CHAPITRE 7

Formes automorphes pour $\mathrm{GL}_n(\mathbb{A})$

Le but de ce dernier chapitre est de définir la notion de forme automorphe pour $\mathrm{GL}_n(\mathbb{A})$, ainsi que les produits eulériens associés par Langlands aux formes propres pour les opérateurs de Hecke [L2]. Cela nous permettra d'énoncer quelques conjectures importantes (et largement ouvertes) dues à Langlands [L1,L2], dont certaines avaient déjà évoquées informellement au Chapitre 1.

Pour parvenir à ces buts, nous aurons besoin de plusieurs études préliminaires. Nous commencerons par étudier les groupes et variétés adéliques, en particulier leur topologie, dans un contexte assez général. Ensuite, nous ferons quelques rappels sur la théorie de la mesure (très élémentaire !) sur ces espaces, et plus généralement sur les espaces topologiques séparés localement profinis (ℓ-espaces). Nous exposerons en particulier la construction des mesures de Haar, et des mesures invariantes sur les espaces homogènes, dans ce contexte. Ces constructions jetterons un regard nouveau sur les anneaux de Hecke introduits au Chapitre 3. Ces préliminaires étant établis, nous serons en mesure de démontrer l'isomorphisme de Satake [Sa, Ca], qui est le résultat central de ce chapitre. Il s'agit d'un isomorphisme canonique

$$\mathrm{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p)) \xrightarrow{\sim} \mathbb{C}[X_1^{\pm 1}, X_2^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n}$$

qui conduit à un analogue du Frobenius Frob_p en théorie des formes automorphes. C'est la clé de la définition des produits eulériens de Langlands [L2].

Références :

[BC] A. Borel & W. Casselman ed., *Automorphic forms, representations and L-functions, Part I & II*, Proc. Symp. in Pure Math. XXXIII, Oregon State Univ., Corvallis, Ore., Providence, R.I., Amer. Math. Soc. (1977).

A. Borel & H. Jacquet, *Automorphic forms and automorphic representations*, dans [BC] Part. II, 189–203.

[Ca] P. Cartier, *Representations of p-adic groups : a survey*, dans [BC] Part. I, 111–157.

B. Conrad, *Weil and Grothendieck approaches to adelic points*, Enseign. Math. (2) 58 61–97 (2012),

[L1] R. Langlands, *Problems in the theory of automorphic forms*, dans le volume *Lectures in modern analysis and applications III*, Lecture Notes in Mathematics 170, Springer-Verlag, (1970)

[L2]. Langlands, *Euler products*, Yale Math. Monographs 1, Yale University Press (1971),

[Sa] I. Satake, *Theory of spherical functions on reductive algebraic groups over p-adic fields*, Publ. Math. I.H.É.S. (1963),

J.-L. Waldspurger, *Formes automorphes pour* GL_n, notes d'un cours de M2,

A. Weil, *Integration dans les groupes topologiques et ses applications*, Hermann (1953).

1. Groupes et variétés adéliques

1.1. Rappels sur les schémas en groupes affines de type fini sur $\mathbb{Z}$. Il sera naturel de considerer des *foncteurs en groupes* sur la catégorie Ann des anneaux commutatifs, autrement dit des foncteurs covariants de Ann vers la catégorie Gro des groupes. Par exemple, $A \to \mathbb{G}_a(A) = (A,+)$ (groupe additif), $A \mapsto \mathbb{G}_m(A^\times, \times)$ (groupe multiplicatif),

$$A \mapsto \mathrm{GL}_n(A) = \{m \in \mathrm{M}_n(A),\ \det m \in A^\times\}$$

(groupe linéaire), $A \mapsto \mathrm{O}_n(A) = \{m \in \mathrm{M}_n(A), m\,{}^{\mathrm{t}}m = \mathrm{I}_n\}$ (groupe orthogonal standard) etc... sont des foncteurs en groupes de manière évidente, et d'un intérêt également évident. Tous ces foncteurs, vus à valeurs dans la catégorie Ens des ensembles, sont de plus représentables par des anneaux de type fini sur $\mathbb{Z}$, i.e. isomorphes à un foncteur de la forme $A \mapsto \mathrm{Hom}_{\mathrm{Ann}}(R, A)$ où R est un anneau de type fini sur $\mathbb{Z}$. Conformément à l'usage en géométrie algébrique, ce dernier foncteur $\mathrm{Hom}_{\mathrm{Ann}}(R,-)$ sera aussi noté $\mathrm{Spec}\,R$. Par exemple on a manifestement des isomorphismes de foncteurs

$$\mathbb{G}_a \simeq \mathrm{Spec}\,\mathbb{Z}[T],\ \mathbb{G}_m \simeq \mathrm{Spec}\,\mathbb{Z}[T,T^{-1}],\ \mathrm{GL}_n \simeq \mathrm{Spec}\,\mathbb{Z}[\{T_{i,j}\}_{1\leq i,j\leq n}][\det(T_{i,j})^{-1}].$$

Toujours conformément à l'usage (et l'intuition !) en géométrie algébrique, on appellera *schéma affine* tout foncteur Ann $\to$ Ens isomorphe à un foncteur de la forme $\mathrm{Spec}\,R$. Le très général (et facile !) *lemme de Yoneda* affirme que tout morphisme (de foncteurs) $\mathrm{Spec}\,R \to \mathrm{Spec}\,S$ est induit par un unique morphisme d'anneaux $S \to R$. Un schéma affine est dit de type fini s'il est isomorphe à $\mathrm{Spec}\,R$ avec R anneau de type fini sur $\mathbb{Z}$. L'*espace affine de dimension* m est par définition $\mathrm{Spec}\,\mathbb{Z}[T_1,\dots,T_m]$, on le note $\mathbf{A}^m$. Si X et Y sont deux schémas affines, respectivement représentés par les anneaux R et S, alors le foncteur $X \times Y$, défini par $A \mapsto X(A) \times Y(A)$, est encore un schéma affine, représenté par $R \otimes S$. Une *immersion fermée* entre schémas affines est un morphisme de foncteurs $X \to Y$, disons avec $X \simeq \mathrm{Spec}\,R$ et $Y \simeq \mathrm{Spec}\,S$, tel que le morphisme d'anneaux associé $S \to R$ est *surjectif.* Si $X \to Y$ est une immersion fermée entre schémas affine, alors pour tout anneau A l'application $X(A) \to Y(A)$ est *injective.*

Un schéma en groupes affine (resp. affine de type fini sur $\mathbb{Z}$) est un foncteur G : Ann $\to$ Gro tel que le foncteur sous-jacent Ann $\to$ Ens est un schéma affine (resp. affine de type fini sur $\mathbb{Z}$). Si G est un schéma en groupes, notons que l'on dispose en particulier de morphismes $G \times G \to G$ (donné par la multiplication) et $G \to G$ (donné par l'inversion).

1.2. Variétés adéliques affines. Soient P l'ensemble des nombres premiers et $\mathrm{V} = \mathrm{P} \cup \{\infty\}$. L'ensemble V s'identifie à l'ensemble des places (=classes d'équivalences de valuations) de $\mathbb{Q}$ de manière évidente. On note $\mathbb{Q}_v$ le complété de $\mathbb{Q}$ en $v \in \mathrm{V}$, de sorte que l'on a $\mathbb{Q}_v = \mathbb{Q}_p$ (corps des p-adiques) si v est le nombre premier p, $\mathbb{Q}_v = \mathbb{R}$ si v est la place archimédienne ∞. On rappelle que *l'anneau des adèles* de $\mathbb{Q}$ est le sous-anneau

$$\mathbb{A} \subset \prod_{v\in\mathrm{V}} \mathbb{Q}_v$$

constitué des éléments (x_v) tels que $x_p \in \mathbb{Z}_p$ *pour presque tout nombre premier* p, ce qui signifiera "pour tout p sauf éventuellement un nombre fini". De même, l'anneau des *adèles finis* est le sous-anneau

$$\mathbb{A}_f \subset \prod_p \mathbb{Q}_p$$

constitué des (x_p) avec $x_p \in \mathbb{Z}_p$ pour presque tout $p \in \mathrm{P}$. On a $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$. Le corps $\mathbb{Q}$ se plonge diagonalement dans $\mathbb{A}$ et $\mathbb{A}_f$, ce qui fait de ces derniers des $\mathbb{Q}$-algèbres. On posera

$$\widehat{\mathbb{Z}} = \prod_{p \in \mathrm{P}} \mathbb{Z}_p,$$

c'est un sous-anneau de $\mathbb{A}_f$.

Soit X un schéma affine de type fini sur $\mathbb{Z}$. Écrivons $X \simeq \operatorname{Spec} \mathbb{Z}[T_1, \ldots, T_n]/I$ pour un certain idéal I dans $\mathbb{Z}[T_1, \ldots, T_n]$, de sorte que X s'identifie au fermé Zariski défini par $I = 0$ de l'espace affine A^n de dimension n sur $\mathbb{Z}$. L'ensemble $X(A)$ s'identifie donc fonctoriellement en l'anneau A à celui des n-uples $(t_1, \ldots, t_n) \in A^n$ avec $P(t_1, \ldots, t_n) = 0$ pour tout $P \in I$. La finitude du nombre n des coordonnées entraîne manifestement le :

Lemme 7.1. *Si X est un schéma affine de type fini sur $\mathbb{Z}$, l'application*

$$X(\mathbb{A}) \to \prod_{v \in V} X(\mathbb{Q}_v), \tag{53}$$

induite par les projections $\mathbb{A} \to \mathbb{Q}_v$, est une bijection d'image le sous-ensemble des (x_v) avec $x_p \in X(\mathbb{Z}_p)$ pour presque tout p.

(Noter que le cas où $X = \operatorname{Spec}(\mathbb{Z}[T])$ est la droite affine est même tautologique !). On a bien sûr une description similaire de $X(\mathbb{A}_f)$ dans laquelle P remplace V. Enfin, on a tautologiquement $X(\widehat{\mathbb{Z}}) = \prod_p X(\mathbb{Z}_p)$ et $X(\mathbb{A}) = X(\mathbb{R}) \times X(\mathbb{A}_f)$. De plus, le plongement naturel de $X(\mathbb{Q})$ dans $X(\mathbb{A})$, induit par $\mathbb{Q} \to \mathbb{A}$, devient le plongement diagonal lorsqu'on le compose avec (53).

Le sorite ci-dessus s'applique en particulier au cas où $X = G$ est un schéma en groupes affine de type fini sur $\mathbb{Z}$. Dans ce cas le groupe $G(\mathbb{A})$ est évidemment un sous-groupe du groupe produit $\prod_{v \in V} G(\mathbb{Q}_v)$: c'est le *groupe adélique* associé à G, idem pour $G(\mathbb{A}_f)$ en remplaçant V par P. Dans ce cas, on identifiera parfois $G(\mathbb{Q}_v)$ au sous-groupe de $G(\mathbb{A})$ constitué des éléments (g_w) avec $g_w = 1$ pour tout $w \neq v$, idem pour $\mathrm{G}(\mathbb{A}_f)$.

1.3. Topologies. Expliquons maintenant comment munir les variétés et groupes adéliques de topologies naturelles. Tout d'abord, pour tout $v \in \mathrm{V}$, le corps $\mathbb{Q}_v$ est un corps topologique localement compact pour la topologie définie par v. Il se trouve que l'on peut munir également les anneaux $\mathbb{A}$ et $\mathbb{A}_f$ d'une topologie naturelle (localement compacte et séparée). Il suffit de l'expliquer pour $\mathbb{A}_f$, car on munira alors $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$ de la topologie produit. On constate que les sous-groupes $U_N \subset \mathbb{A}_f$, avec N un entier ≥ 1, définis par

$$U_N \;=\; N\widehat{\mathbb{Z}} \;=\{(N\,x_p)_p,\; x \in \mathbb{A}_f\} \;=\; \left(\prod_{p \mid N} N\mathbb{Z}_p\right) \times \prod_{p \nmid N} \mathbb{Z}_p,$$

vérifient $U_N \cap U_M \supset U_{MN}$ et $U_N \cdot U_M = U_{NM}$ pour tous $N, M \geq 1$. De plus, pour tout $x \in \mathbb{A}_f$ et tout $M \geq 1$, il existe $N \geq 1$ tel que $xU_N \subset U_M$. On en déduit que les $x + U_N$, avec $x \in \mathbb{A}_f$ et $N \geq 1$, forment donc une base d'une unique topologie d'anneaux [1] sur $\mathbb{A}_f$. Par définition, le sous-anneau $U_1 = \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ est ouvert dans $\mathbb{A}_f$, et la topologie de U_1 induite par $\mathbb{A}_f$ est la topologie produit. C'est donc un sous-anneau compact, et même profini car U_N est un idéal ouvert de U_1 vérifiant $U_1/U_N \simeq \mathbb{Z}/N\mathbb{Z}$ pour tout $N \geq 1$.

Ces topologies sur les $\mathbb{Q}_v$ et sur $\mathbb{A}_f$ sétendent à toutes les variétés/groupes adéliques pour une raison très simple et générale, qui prend la forme du lemme suivant. [2] Dans cet énoncé, R est un anneau topologique quelconque, et on munit R^m de la topologie produit pour tout entier $m \geq 1$.

Lemme 7.2. *Soit R un anneau topologique.*

(i) Il existe un unique foncteur des schémas affines de type fini sur $\mathbb{Z}$ vers les espaces topologiques qui est de la forme $X \mapsto X(R)$, et tel que si $X \subset \mathbf{A}^m$ est fermé alors le sous-ensemble $X(R) \subset R^m$ est fermé.

On muni désormais $X(R)$ de cette topologie pour tout schéma affine X de type fini sur $\mathbb{Z}$ et tout anneau topologique R.

(ii) Si X et Y sont deux shémas affines de type fini sur $\mathbb{Z}$, la bijection naturelle $(X \times Y)(R) \to X(R) \times Y(R)$ est alors un homéomorphisme.

(iii) Si G est un schéma en groupes affine et de type fini sur $\mathbb{Z}$, alors $G(R)$ est un groupe topologique.

(iv) Si $R = R_1 \times R_2$ avec R_1 et R_2 des anneaux topologiques, et si X est affine de type fini sur $\mathbb{Z}$, alors l'isomorphismes naturel $X(R) \xrightarrow{\sim} X(R_1) \times X(R_2)$ est un homéomorphisme.

Démonstration — Comme tout X se réalise comme fermé d'un espace affine, l'unicité est évidente. Pour justifier l'existence, supposons d'abord $X = \operatorname{Spec} A$ avec A un anneau de type fini sur $\mathbb{Z}$. Pour tout élément $f \in A$, on dispose d'une évaluation tautologique $\mathrm{ev}_f : X(R) \to R$, $x \mapsto f(x)$ (rappelons qu'au sens strict x est un morphisme d'anneaux de A vers R, et que l'on a posé $f(x) = x(f)$!). On munit $X(R)$ de la topologie $\mathcal{T}$ la plus faible rendant ev_f continue pour tout $f \in A$. Choisir une immersion fermée $X \to \mathbf{A}^m$ revient à choisir des générateurs $x_1, \ldots, x_m$ de l'anneau R. La topologie $\mathcal{T}'$ de $X(R)$ induite par l'inclusion $X(R) \subset R^m$ est alors la topologie faible donnée par les ev_{x_i} pour $i = 1, ..., m$. On a évidemment $\mathcal{T}' \subset \mathcal{T}$. Mais tout $f \in R$ est un polynôme à coefficients entiers en les x_i. Comme les applications polynomiales $R^m \to R$ sont continues, l'application ev_f est continue pour $\mathcal{T}'$ pour tout $f \in A$: on a donc $\mathcal{T} \subset \mathcal{T}'$ puis $\mathcal{T} = \mathcal{T}'$: ce que l'on voulait démontrer. Le fait que $X \mapsto X(R)$ est un foncteur satisfaisant (i) s'en déduit trivialement, car tout morphisme $\operatorname{Spec} A \to \operatorname{Spec} B$ provient d'un unique morphisme d'anneaux $B \to A$.

---

1. Rappelons qu'un anneau topologique est un anneau muni d'une topologie telle que $(x, y) \mapsto x + y$, $(x, y) \mapsto xy$ et $x \mapsto -x$ soient continues. En particulier, pour tout élément a l'application $x \mapsto x + a$ est un homéomorphisme.

2. Voir l'article de B. Conrad *Weil and Grothendieck approaches to adelic points*, Enseign. Math. (2) 58 61–97 (2012), pour de nombreux développements de cette méthode, notamment dans des contextes non affines.

Pour le (ii), on peut supposer que X et Y sont respectivement plongés dans $\mathbf{A}^n$ et $\mathbf{A}^m$, et on invoque simplement que l'application évidente $R^n \times R^m \to R^{n+m}$ est un homéomorphisme.

Pour le (iii), on note que l'inversion $G(R) \to G(R)$ est continue par le (i), ainsi que la multiplication $G(R) \times G(R) = (G \times G)(R) \to G(R)$ par (i) et (ii).

Pour le (iv), on se ramène encore à montrer que la bijection naturelle $R_1^m \times R_2^m \to (R_1 \times R_2)^m$ est un homéomorphisme, ce qui est évident. □

On munira dorénavant sans commentaire les ensembles $\mathrm{X}(\mathbb{Q}_v)$, $X(\mathbb{A}_f)$ et $X(\mathbb{A})$, pour X affine de type fini sur $\mathbb{Z}$, des topologies données par le lemme ci-dessus. Par le (iv) l'application évidente $X(\mathbb{A}) \xrightarrow{\sim} X(\mathbb{R}) \times X(\mathbb{A}_f)$ est un homéomorphisme. De plus, tous ces espaces sont des espaces localement compact séparés, car c'est le cas de $\mathbb{Q}_v$ et de $\mathbb{A}_f$ (et donc des $\mathbb{Q}_v^m$ et $\mathbb{A}_f^m$).

Remarque 7.3. Si $X \to Y$ est une immersion *ouverte* entre schémas de type fini sur $\mathbb{Z}$ (au sens de la théorie des schémas, par exemple de la forme $\operatorname{Spec} A[1/f] \to \operatorname{Spec} A$ avec $f \in A$), et si R anneau topologique, il n'est pas vrai en général que $X(R)$ est un ouvert de $Y(R)$. Par exemple si $X = \mathbb{G}_m \subset \mathbf{A}^1 = Y$, alors $\mathbb{A}_f^\times$ (les idèles) n'est pas un ouvert de $\mathbb{A}_f$ (mais, bien sûr, il s'identifie au fermé de $\mathbb{A}_f^2$ défini par $xy = 1$).

Soit G est un schéma en groupes de type fini sur $\mathbb{Z}$. Pour $N \geq 1$ et p premier on note $\mathrm{G}(\mathbb{Z}_p)_{(N)}$ le noyau du morphisme $G(\mathbb{Z}_p) \to G(\mathbb{Z}_p/N\mathbb{Z}_p)$. C'est un sous-groupe distingué d'indice fini dans $G(\mathbb{Z}_p)$; il est égale à $G(\mathbb{Z}_p)$ si p ne divise pas N. On pose enfin $G(\mathbb{A}_f)_{(N)} = \prod_p G(\mathbb{Z}_p)_{(N)}$. C'est un sous-groupe distingué et d'indice fini dans $G(\mathbb{A}_f)_{(1)} = G(\widehat{\mathbb{Z}})$.

Corollaire 7.4. *Soient G un schéma en groupes affine et de type fini sur $\mathbb{Z}$.*

- *(i) Si $p \in \mathrm{P}$, les $G(\mathbb{Z}_p)_{(N)}$ avec $N \geq 1$ forment un système fondamental de voisinages de 1 dans $G(\mathbb{Q}_p)$ constitué de sous-groupes ouverts et compacts, distingués et d'indice fini dans $G(\mathbb{Z}_p)$.*
- *(ii) les sous-groupes $G(\mathbb{A}_f)_{(N)}$ avec $N \geq 1$, forment un système fondamental de voisinages de 1 dans $G(\mathbb{A}_f)$ constitué de sous-groupes ouverts et compacts, distingués et d'indice fini dans $G(\widehat{\mathbb{Z}})$.*

Démonstration — Soit $\mathrm{i} : G \to \mathbf{A}^m$ une immersion fermée. Quitte à la composer par $x \mapsto x - i(1)$ (où $1 \in G(\mathbb{Z})$ est l'élément neutre de G, et donc $\mathrm{i}(1) \in \mathbb{Z}^m$), on peut supposer que l'on a $\mathrm{i}(1) = 0$. On observe que l'on a tautologiquement

$$G(\mathbb{Z}_p)_{(N)} = \mathrm{i}^{-1}(N\mathbb{Z}_p) \quad \text{et} \quad G(\mathbb{A}_f)_{(N)} = \mathrm{i}^{-1}(N\widehat{\mathbb{Z}}).$$

En effet, pour justifier par exemple la première égalité il suffit de contempler le diagramme commutatif naturel

$$\begin{tikzcd}
G(\mathbb{Z}_p) \arrow[r, "\mathrm{i}"] \arrow[d, "\mathrm{can}"'] & \mathbf{A}^m(\mathbb{Z}_p) \arrow[r, "\sim"] \arrow[d, "\mathrm{can}"] & \mathbb{Z}_p^m \arrow[d, "\mathrm{can}"] \\
G(\mathbb{Z}_p/N\mathbb{Z}_p) \arrow[r, "\mathrm{i}"] & \mathbf{A}^m(\mathbb{Z}_p/N\mathbb{Z}_p) \arrow[r, "\sim"] & (\mathbb{Z}_p/N\mathbb{Z}_p)^m
\end{tikzcd}$$

et d'utiliser l'injectivité des applications induites par i horizontales (vraies car i est une immersion fermée). On conclut car les plongements $G(\mathbb{Q}_p) \to \mathbb{Q}_p^m$ et $G(\mathbb{A}_f) \to \mathbb{A}_f^m$ induits par i sont fermés puisque i est une immersion fermée, et car les $N\mathbb{Z}_p$ (resp. $N\widehat{\mathbb{Z}}$) avec $N \geq 1$ forment une base de voisinage de 0 dans $\mathbb{Q}_p$ (resp. $\mathbb{A}_f$). □

Ce corollaire montre que la topologie que nous avons mise ici sur $G(\mathbb{Q}_p)$ et $G(\mathbb{A}_f)$ coïncide avec celle que l'on trouve dans diverses autres références sur le sujet. Terminons par une propriété cruciale du plongement $\mathbb{Q} \to \mathbb{A}$, qui font que les adèles sont à $\mathbb{Q}$ ce que $\mathbb{R}$ est à $\mathbb{Z}$.

Proposition 7.5. *Si X est un schéma affine de type fini sur $\mathbb{Z}$, alors $X(\mathbb{Q})$ est discret dans $X(\mathbb{A})$.*

Démonstration — Soit i : $X \to \mathbf{A}^m$ une immersion fermée. Elle induit donc une injection fermée $X(\mathbb{A}) \to \mathbb{A}^m$ qui envoie $X(\mathbb{Q})$ dans $\mathbb{Q}^m$. Il suffit donc de voir que $\mathbb{Q}^m$ est discret dans $\mathbb{A}^m$, ce pour quoi on peut même supposer $m = 1$. Comme $\mathbb{Q}$ est un sous-groupe de $\mathbb{A}$, il suffit de voir qu'il existe un voisinage V de 0 dans $\mathbb{A}$ avec $V \cap \mathbb{Q} = \{0\}$. On conclut car $V =]-1, 1[\times\widehat{\mathbb{Z}}$ convient. □

2. $\mathrm{GL}_n(\mathbb{A}_f)$ et réseaux de $\mathbb{Q}^n$

Définition 7.6. *Soit G un schéma en groupes affine et de type fini sur $\mathbb{Z}$. On note* $\mathrm{Cl}(G)$ *l'ensemble des doubles classes $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$ et on pose* $\mathrm{h}(G) = |\mathrm{Cl}(G)$.

Un résultat fameux de Borel[3], vaste généralisation de la finitude du nombre des classes d'idéaux d'un corps de nombres, affirme que $\mathrm{h}(G)$ est toujours fini. Par exemple, on a $\mathrm{h}(\mathbb{G}_a) = 1$. En effet, tout adèle $a \in \mathbb{A}_f$ s'écrit manifestement sous la forme $\lambda + x$ avec $\lambda \in \mathbb{Q}$ et $x \in \widehat{\mathbb{Z}}$. De même, on a $\mathbb{A}_f^\times = \mathbb{Q}^\times \cdot \widehat{\mathbb{Z}}^\times$ et $\mathrm{h}(\mathbb{G}_m) = 1$. Nous allons étudier ici le cas $G = \mathrm{GL}_n$.

Proposition 7.7. *Pour tout $n \geq 1$ on a* $\mathrm{h}(\mathrm{GL}_n) = 1$, *autrement dit*

$$\mathrm{GL}_n(\mathbb{A}_f) = \mathrm{GL}_n(\mathbb{Q}).\mathrm{GL}_n(\widehat{\mathbb{Z}}).$$

Avant de démontrer cette proposition, commençons par une observation sur les réseaux de l'espace vectoriel $\mathbb{Q}^n$, dont l'ensemble a été noté $\mathrm{R}(\mathbb{Q}^n)$ au chapitre 3. Si $L \subset \mathbb{Q}^n$ est un réseau, alors son image dans le $\mathbb{Q}_p$-espace vectoriel $\mathbb{Q}_p^n$ engendre un $\mathbb{Z}_p$-réseau L_p pour tout premier p. On note $\mathrm{R}(\mathbb{Q}_p^n)$ l'ensemble des $\mathbb{Z}_p$-réseaux de $\mathbb{Q}_p^n$

Lemme 7.8. (Eichler, Weil) *L'application* $\mathrm{R}(\mathbb{Q}^n) \to \prod_p \mathrm{R}(\mathbb{Q}_p^n)$, *$L \mapsto (L_p)$, est une injection d'image l'ensemble des collections (L_p) vérifiant $L_p = \mathbb{Z}_p^n$ pour presque tout* $p \in \mathrm{P}$.

Démonstration — Soit $L \in \mathrm{R}(\mathbb{Q}^n)$. Il existe un entier $N \geq 1$ tel que l'on a $N\mathbb{Z}^n \subset L \subset \frac{1}{N}\mathbb{Z}^n$. Cela entraîne $N\mathbb{Z}_p^n \subset L_p \subset \frac{1}{N}\mathbb{Z}_p^n$ pour tout premier p. En

3. Voir *Some finiteness properties of adele groups over number fields*, Publ. Math, IHES (1963).

particulier, on a $L_p = (\mathbb{Z}_p)^n$ pour tout p ne divisant pas N (et donc pour presque tout p). De plus, par Bézout on a un isomorphisme canonique

$$(\frac{1}{N}\,\mathbb{Z}^n)/(N\mathbb{Z}^n) \xrightarrow{\sim} \prod_{p|N}(\frac{1}{N}\,\mathbb{Z}_p^n)/(N\mathbb{Z}_p^n),$$

qui envoit manifestement L sur le produit des $L_p/(N\mathbb{Z}_p^n)$: L est uniquement déterminé par la collection des L_p (c'est même l'intersection de tous les L_p en un sens évident), et l'application de l'énoncé est injective. Enfin, si on a (L_p) avec $L_p = \mathbb{Z}_p^n$ pour presque tout p, on peut trouver un entier $N \geq 1$ tel que $N\mathbb{Z}_p^n \subset L_p \subset \frac{1}{N}\mathbb{Z}_p^n$ pour tout p. L'isomorphisme ci-dessus montre encore que l'image inverse des $L_p/(N\mathbb{Z}_p^n)$ est un sous-réseau $N\mathbb{Z}^n \subset L' \subset \frac{1}{N}(\mathbb{Z}^n)$ vérifiant $L'_p = L_p$ pour tout p : c'est la surjectivité annoncée. □

Il résulte de ce lemme que l'on peut définir une action de $\mathrm{GL}_n(\mathbb{A}_f)$ sur $\mathrm{R}(\mathbb{Q}^n)$: si $g \in \mathrm{GL}_n(\mathbb{A}_f)$, et si $L \in \mathrm{R}(\mathbb{Q}^n)$, on note $g.L \in \mathrm{R}(\mathbb{Q}^n)$ l'unique réseau vérifiant

$$(g.L)_p = g_p L_p$$

pour tout premier p (observer que l'on a bien $g_p L_p = \mathbb{Z}_p^n$ pour presque tout p si $g \in \mathrm{GL}_n(\mathbb{A})$). C'est trivialement une action de groupe, qui de plus est transitive, car $\mathrm{GL}_n(\mathbb{Q}_p)$ agit transitivement sur $\mathrm{R}(\mathbb{Q}_p^n)$ pour tout premier p. Le stabilisateur de $\mathbb{Z}^n$ pour cette action est manifestement $\prod_{p\in\mathrm{P}} G(\mathbb{Z}_p) = G(\widehat{\mathbb{Z}})$, et nous avons démontré que $g \mapsto g(\mathbb{Z}^n)$ induit une bijection

$$\mathrm{GL}_n(\mathbb{A}_f)/\mathrm{GL}_n(\widehat{\mathbb{Z}}) \xrightarrow{\sim} \mathrm{R}(\mathbb{Q}^n).$$

Mais d'autre part, on a aussi une action naturelle, et également transitive, de $\mathrm{GL}_n(\mathbb{Q})$ sur $\mathrm{R}(\mathbb{Q}^n)$, compatible avec l'action précédente et l'inclusion de $\mathrm{GL}_n(\mathbb{Q})$ dans $\mathrm{GL}_n(\mathbb{A}_f)$: on a bien démontré

$$\mathrm{GL}_n(\mathbb{A}_f) = \mathrm{GL}_n(\mathbb{Q}) \cdot \mathrm{GL}_n(\widehat{\mathbb{Z}}),$$

ce qui démontre la Proposition 7.7.

Corollaire 7.9. *L'application $g \mapsto (g, 1)$, $\mathrm{GL_n}(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{A})$ induit un homéomorphisme entre espaces topologiques quotients*

$$\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A})/\mathrm{GL}_n(\widehat{\mathbb{Z}}).$$

Démonstration — L'application de l'énoncé induit manifestement une application $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{Q})\backslash\mathrm{GL}_n(\mathbb{A})/\mathrm{GL}_n(\widehat{\mathbb{Z}})$, à savoir $g \mapsto \mathrm{GL}_n(\mathbb{Q})(g\times 1)\mathrm{GL}_n(\widehat{\mathbb{Z}})$. Cette application est trivialement injective, et elle est surjective d'après la Proposition 7.7. Elle est continue car l'inclusion $G(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{A})$ l'est. Elle est ouverte car si Ω est un ouvert de $\mathrm{GL}_n(\mathbb{R})$ alors $\Omega \times \mathrm{GL}_n(\widehat{\mathbb{Z}})$ est un ouvert de $\mathrm{GL}_n(\mathbb{A})$, ainsi donc que $\mathrm{GL}_n(\mathbb{Q})(\Omega \times \mathrm{GL}_n(\widehat{\mathbb{Z}}))$ (réunion d'ouverts). □

3. Mesures sur les espaces et groupes localement profinis

Nous appellerons *ℓ-espace* un espace topologique séparé [4] dans lequel tout élément possède une base de voisinages à la fois ouverts et compacts. Par exemple, les espaces produits $\mathbb{A}_f^m$ et $\mathbb{Q}_p^m$ sont des ℓ-espaces pour tout $m \geq 1$. Plus généralement, si X est un schéma affine de type fini sur $\mathbb{Z}$, et si p est premier, alors $X(\mathbb{A}_f)$ et $X(\mathbb{Q}_p)$ sont des ℓ-espaces par le Lemme 7.2.

Lemme 7.10. *Soient X un ℓ-espace et U, V deux ouverts compacts de X. Alors $U \cup V, U \cap V$ et $U - V$ sont des ouverts compacts de X.*

Démonstration — C'est évident pour $U \cup V$. Pour les autres, cela se déduit du fait qu'un fermé d'un compact est compact, et que dans un espace séparé tout compact est fermé. $\square$

Si X est un ℓ-espace, on notera $\mathrm{OC}(X)$ l'ensemble des parties de X qui sont à la fois ouvertes et compactes.

Définition 7.11. *Une petite mesure sur le ℓ-espace X est une fonction $\mu : \mathrm{OC}(X) \to \mathbb{C}$ vérifiant $\mu(U \cup V) = \mu(U) + \mu(V)$ pour tout $U, V \in \mathrm{OC}(X)$ avec $U \cap V = \emptyset$ (et donc $\mu(\emptyset) = 0$). Les petites mesures forment un $\mathbb{C}$-espace vectoriel de manière évidente, que l'on notera $\mathrm{PM}(X)$. Une petite mesure $\mu \in \mathrm{PM}(X)$ sera dite positive, et on notera $\mu \geq 0$, si l'on a $\mu(U) \geq 0$ pour tout $U \in \mathrm{OC}(X)$.*

Un énoncé classique de théorie de la mesure (théorème d'extension de Caratheodory [5]) implique que les petites mesures positives sont la même chose que les mesures boréliennes lorsque le ℓ-espace X est réunion dénombrable de compacts.

Proposition 7.12. *(Carathéodory) Soit X un ℓ-espace supposé réunion dénombrable de compacts. Alors toute petite mesure positive sur X sétend de manière unique en une mesure borélienne positive sur X.*

Notons que cette proposition s'applique aux ℓ-espaces de la forme $X(\mathbb{Q}_p)$ ou $X(\mathbb{A}_f)$ car $\mathbb{Q}_p$ et $\mathbb{A}_f$ sont réunion dénombrable de compacts. Ceci étant dit, les petites mesures suffiseront aux besoins de ce chapitre.

Nous appellerons *ℓ-groupe* un groupe topologique dont l'espace topologique sous-jacent est un ℓ-espace. Notre premier but sera d'expliquer une construction très simple des (petites) mesures de Haar pour les ℓ-groupes. Si G est affine de type fini sur $\mathbb{Z}$ alors $G(\mathbb{A}_f)$ et les $G(\mathbb{Q}_p)$ sont des exemples de ℓ-groupes. Dans ces exemples, nous avons vu qu'il existe une base de voisinages de 1 constituée de sous-groupes ouverts compacts, c'est un fait général :

Lemme 7.13. *Soient G un ℓ-groupe et U un ouvert compact non vide de G.*

---

4. Rappelons que cela signifie que pour tout $x, y \in X$ avec $x \neq y$, il existe des ouverts U et V avec $x \in U$, $y \in V$ et $U \cap V = \emptyset$.

5. Voir le blog de Terence Tao https://terrytao.wordpress.com/2009/01/03/254a-notes-0a-an-alternate-approach-to-the-caratheodory-extension-theorem/ pour une démonstration assez courte de ce théorème.

(i) Si K est un sous-groupe ouvert de G vérifiant $U\,K \subset U$ alors U/K est fini et K est compact,

(ii) il existe un sous-groupe ouvert compact K de G vérifiant $U\,K \subset U$ (et donc $U\,K = U$).

En particulier, G admet une base de voisinages de 1 constituée de sous-groupes ouverts compacts, et si K et K' sont deux sous-groupes compacts ouverts de G alors $K \cap K'$ est d'indices finis dans K (des deux côtés).

Démonstration — Montrons le (i). L'ensemble U est réunion disjointes de K-orbites, i.e. de parties de la forme $u\,K$ avec $u \in U$, donc ouvertes car K l'est. Par compacité de U, ces K-orbites sont en nombre fini. Comme le complémentaire d'une K-orbite dans U est une réunion de K-orbites, $u\,K$ est fermé et donc compact pour tout $u \in U$. Choisissant $u \in U$ (qui est non vide), cela montre que $K = u^{-1}\,u\,K$ est compact.

Montrons le (ii). Par continuité de la multiplication dans G, pour tout $x \in U$ il existe un voisinage ouvert compact U_x de x dans U, et un voisinage ouvert compact V_x de 1 dans G, tels que $U_x\,V_x \subset U$. Par compacité de U, il existe $x_1, \dots, x_n \in U$ avec $U = \cup_{i=1}^{n} U_{x_i}$. On en déduit que le voisinage ouvert compact $V = \cap_{i=1}^{n} V_{x_i}$ de 1 dans G vérifie $U\,V \subset U$. Par continuité de l'inversion, il existe un voisinage ouvert $W \subset V$ de 1 dans G avec $W^{-1} \subset V$. Le sous-groupe K de G engendré par W est ouvert (car $W \subset K$) et vérifie $U\,K \subset U$, donc K est compact par le (i), et on a montré le (ii).

Pour la dernière assertion, on applique le (ii) à un voisinage U de 1 et on observe $K \subset U$. L'assertion sur $K \cap K'$ découle du (i). □

Si G est un ℓ-groupe, alors G agit naturellement par translations à droite et à gauche sur $\mathrm{OC}(G)$. En effet, si $U \in \mathrm{OC}(G)$ et $g \in G$ alors gU et Ug sont dans $\mathrm{OC}(G)$. Pour $\mu \in \mathrm{PM}(G)$ et $g \in G$ on note $\mathrm{R}_g\mu$ (resp. $\mathrm{L}_g\mu$) est la petite mesure sur G définie par $U \mapsto \mu(Ug)$ (resp. $U \mapsto \mu(g^{-1}U)$) ; ce sont des petites mesures pour des raisons évidentes, et $g \mapsto \mathrm{R}_g$ et L_g sont deux actions à gauche de G sur $\mathrm{OC}(G)$ qui commutent entre elles. L'énoncé suivant traite des mesures de Haar à gauche : le cas “à droite” se traite de manière similaire, ou mieux se ramène à celui-là en considérant le groupe opposé.

Proposition 7.14. *(Mesures de Haar à gauche) Soient G un ℓ-groupe. Il existe une petite mesure positive non nulle μ sur G, unique à un scalaire dans $\mathbb{R}_{>0}$ près, vérifiant $\mathrm{L}_g\,\mu = \mu$ pour tout $g \in G$. Elle vérifie de plus $\mu(U) > 0$ pour tout $U \in \mathrm{OC}(G)$ non vide.*

(Notons que l'extension de Carathéodory d'une petite mesure de Haar est également invariante, par la propriété d'unicité de celle-là.)

Démonstration — Supposons l'existence d'une petite mesure sur G invariante à droite. Soient $U \in \mathrm{OC}(G)$ et K un sous-groupe ouvert compact de G tels que $U\,K \subset U$. Alors U est réunion disjointe de $|U/K| < \infty$ parties de la forme $u\,K$, et on a donc

$$\mu(U) = |U/K|\,\mu(K). \tag{54}$$

Soit K' un sous-groupe compact ouvert de G. Cette observation appliquée à $U = K'$, qui est stable par le compact ouvert $K \cap K'$, montre aussi

$$\mu(K') = |K'/(K \cap K')| \, \mu(K \cap K') \tag{55}$$

pour tous sous-groupes ouverts compacts K, K' de G. En particulier, on a $\mu(K) = |K/K'| \, \mu(K')$ pour $K' \subset K$. On en déduit de (54) que si μ est non nulle, alors $\mu(K)$ est non nul pour au moins un sous-groupe compact ouvert K de G, puis pour tous les sous-groupes compacts ouverts de G par (55), puis que $\mu(U)$ est non nul pour tout $U \in \mathrm{OC}(G)$ non vide par (54) appliqué une seconde fois. D'autre part, (54) et (55) montrent que μ est uniquement déterminée par sa valeur sur un compact ouvert donné de G, d'où l'assertion d'unicité.

Il ne reste que la question de l'existence de μ, mais elle est dictée par l'analyse précédente. Fixons un sous-groupe ouvert compact $K_0 \subset G$ (in fine, nous aurons $\mu(K_0) = 1$). Soit $U \in \mathrm{OC}(G)$. On choisit un sous-groupe compact ouvert $K \subset K_0$ vérifiant $U\,K_0 \subset U$ (intersecter avec K_0 un sous-groupe donné par le Lemme 7.13 (ii)), puis on pose

$$\mu(U) = |U/K| \, |K_0/K|^{-1}.$$

Alors $\mu(U)$ ne dépend pas du choix de K. En effet, si l'on a $U\,K' \subset U$, alors on a $U\,(K \cap K') \subset U$, de sorte que l'on peut supposer $K' \subset K$, auquel cas on conclut par les égalités évidentes

$$|U/K'| = |K/K'| \, |U/K| \quad \text{et} \quad |K_0/K'| = |K/K'| \, |K_0/K|.$$

On a bien $\mu(gU) = \mu(U)$ pour tout $U \in \mathrm{OC}(G)$ et tout $g \in G$ en vertu de l'égalité $|gU/K| = |U/K|$. Enfin, pour $U, V \in \mathrm{OC}(G)$ avec $U \cap V = \emptyset$, on peut choisir $K \subset K_0$ avec $U\,K \subset U$ et $V\,K \subset V$, auquel cas $\mu(U \coprod V) = \mu(U) + \mu(V)$ car $(U \coprod V)/K = U/K \coprod V/K$. □

Si μ est une mesure de Haar à gauche sur le ℓ-groupe G, et si $g \in G$, alors $\mathrm{R}_g\mu$ en est encore une : elle est donc de la forme $\delta_G(g)\mu$ pour un unique scalaire $\delta_G(g) \in \mathbb{R}_{>0}$ (clairement indépendant du choix de μ). Comme $g \mapsto \mathrm{R}_g$ est une action de groupes, $\delta_G : G \mapsto \mathbb{R}_{>0}$ est un morphisme de groupes. Il est trivial sur tout sous-groupe compact ouvert K de G : pour $k \in K$ on a $\mu(K) = \mu(Kk) = \delta_G(k)\mu(K)$ et donc $\delta_G(k) = 1$ car $\mu(K) \neq 0$. En particulier, l'application δ_G est continue pour la topologie discrète sur $\mathbb{R}$:

Corollaire-Définition 7.15. *Pour tout ℓ-groupe G, il existe un unique homomorphisme continu $\delta_G : G \to \mathbb{R}_{>0}$, appelé* module *de G, tel que pour toute mesure de Haar à gauche μ sur G, pour tout $g \in G$, et tout $U \in \mathrm{OC}(G)$, on ait $\mu(Ug) = \mu(g^{-1}Ug) = \delta_G(g)\mu(U)$. On dit que G est* unimodulaire *si l'on a $\delta_G = 1$, dans ce cas toute mesure de Haar à gauche sur G est aussi une mesure de Haar à droite.*

Exemple 7.16. (i) Les ℓ-groupes commutatifs (resp. simples, resp. compacts) sont trivialement unimodulaires.

(ii) (Mesure de Haar standard sur $\mathbb{Q}_p$) La (petite) mesure de Haar sur le ℓ-groupe additif $\mathbb{Q}_p^m$ normaliée par $\mu(\mathbb{Z}_p^m) = 1$ sera notée $\prod_{i=1}^m \mathrm{d}x_i$.

(iii) Le groupe $\mathrm{GL}_n(\mathbb{Q}_p)$ est unimodulaire.

Démonstration — Seul le (iii) reste à justifier. Posons $G = \mathrm{GL}_n(\mathbb{Q}_p)$, $H = \mathrm{SL}_n(\mathbb{Q}_p)$ et $Z = \mathbb{Q}_p^\times$. On a $\delta_G(ZH) = 1$ car H est égal à son groupe dérivé et Z est central. Comme ZH est d'indice fini dans G, le sous-groupe $\delta_G(G) \subset \mathbb{R}_{>0}$ est fini : il est donc trivial. □

Pour construire des mesures, il est commode d'adopter le point de vue fonctionnel suivant. On notera $\mathcal{C}_c(X)$ l'espace vectoriel des fonctions $X \to \mathbb{C}$ qui sont localement constantes (autrement dit, continues pour la topologie discrète sur $\mathbb{C}$) et à support compact. Une telle fonction ne prend qu'un nombre fini de valeurs, de sorte que pour tout $\lambda \in \mathbb{C}$ l'ensemble $f^{-1}(\{\lambda\})$ est un ouvert fermé de X, compact si l'on a $\lambda \neq 0$ (car dans $\mathrm{Supp}\, f$). En particulier, les fonctions caractéristiques 1_U avec $U \in \mathrm{OC}(X)$ forment une famille génératrice de l'espace $\mathcal{C}_c(X)$. Elles ne forment pas une base en général, à cause par exemple des relations de la forme $1_U + 1_V = 1_{U\cup V} + 1_{U\cap V}$ pour $U, V \in \mathrm{OC}(X)$ (nous allons voir plus bas que ce sont essentiellement les seules relations). Toute forme linéaire $\Lambda : \mathcal{C}_c(X) \to \mathbb{C}$ définit une petite mesure μ_Λ sur X en posant $\mu_\Lambda(U) = \Lambda(1_U)$. L'application

$$\mathcal{C}_c(X)^* \longrightarrow \mathrm{PM}(X), \quad \Lambda \mapsto \mu_\Lambda, \tag{56}$$

ainsi définie est linéaire est injective.

Lemme 7.17. *L'application* (56) *est bijective.*

Démonstration — Reste à montrer la surjectivité. Fixons donc une petite mesure μ sur X. Soient $f \in \mathcal{C}_c(X)$ et Ω un ouvert compact de X contenant $\mathrm{Supp} f$. Supposons que l'on ait deux décompositions $\Omega = \coprod_{i\in I} U_i = \coprod_{j\in J} V_j$ où les U_i et les V_j sont des ouverts compacts sur lesquels f est constante (de valeur notée $f(U_i)$ resp. $f(V_j)$), avec I et J finis. Observons que l'on a

$$\sum_{i\in I} f(U_i)\,\mu(U_i) \;= \sum_{i\in I} f(U_i)\,(\sum_{j\in J}\mu(U_i\cap V_j)) \;=\; \sum_{i\in I, j\in J} f(U_i\cap V_j)\,\mu(U_i\cap V_j),$$

la première égalité résultant de l'additivité de μ appliquée à la partition finie $U_i = \coprod_{j\in J} U_i \cap V_j$ et la seconde des égalités évidentes $f(U_i\cap V_j) = f(U_i) = f(V_j)$. Autrement dit, la somme $\sum_{i\in I} f(U_i)\mu(U_i)$ ne dépend que de f et Ω. En fait, elle ne dépend pas non plus de Ω, car pour $\Omega' \subset \Omega$ on a $f(\Omega' - \Omega) = 0$. On la note $\Lambda(f)$. En particulier, on a $\Lambda(f) = \sum_{\lambda\in f(X)-\{0\}} \lambda\,\mu(f^{-1}(\{\lambda\}))$. Il est évident que l'on a $\Lambda(1_A) = \mu(A)$ pour tout $A \in \mathrm{OC}(X)$, et aussi $\Lambda(\mu f) = \mu\Lambda(f)$. Il ne reste qu'à prouver $\Lambda(f+g) = \Lambda(f) + \Lambda(g)$ pour $f, g \in \mathcal{C}_c(X)$. Fixons donc deux telles fonctions f et g. Posons $\Omega = \mathrm{Supp} f \cup \mathrm{Supp} g$. D'après les observations précédentes, il suffit de voir qu'il existe une partition finie $\Omega = \coprod_k W_k$ où f et g sont toutes les deux constantes sur chaque W_k. Pour cela, on choisit des décompositions finies $\Omega = \coprod_{i\in I} U_i = \coprod_{j\in J} V_j$ avec f constante sur les U_i et g constante sur les V_j, et on observe que la partition de Ω donnée par les $U_i \cap V_j$, $(i,j) \in I \times J$, convient. □

Remarque 7.18. Si Λ est la forme linéaire associée à la petite mesure μ, et si $f \in \mathcal{C}_c(X)$, on note souvent $\Lambda(f) = \int_X f(x)\mu$. Ainsi, pour $f = \sum_{i=1}^n \lambda_i 1_{U_i}$ on a $\int_X f(x)\mu = \sum_{i=1}^n \lambda_i \mu(U_i)$: ce n'est rien d'autre qu'une somme finie, mais l'écriture est suggestive. Lorsque μ est positive et X réunion dénombrable de compacts, de sorte que μ s'étend canoniquement en une mesure borélienne d'après Carathéodory, cette notation est compatible avec celle en théorie de l'intégration.

Exercice 7.1. ("Petit Fubini") Soient X et Y des ℓ-espaces, ainsi que $\mu \in \mathrm{PM}(X)$ et $\nu \in \mathrm{PM}(Y)$. Alors $X \times Y$ est un ℓ-espace, et il existe un unique $\lambda \in \mathrm{PM}(X \times Y)$ avec $\lambda(U \times V) = \mu(U)\nu(V)$ pour tout $U \in \mathrm{OC}(X)$ et $V \in \mathrm{OC}(Y)$, on note $\lambda = \mu\nu$ ou $\lambda = \mu \times \nu$. Pour tout $f \in \mathrm{C}_c(X \times Y)$ on a

$$\int_X (\int_Y f(x,y)\nu)\mu = \int_{X\times Y} f(x,y)\mu \times \nu = \int_Y (\int_X f(x,y)\mu)\nu.$$

Donnons un exemple. Soit $\mu = \prod_{1\leq i,j\leq n} \mathrm{d}m_{i,j}$ la mesure standard sur le $\mathbb{Q}$-espace vectoriel $V = \mathrm{M}_n(\mathbb{Q}_p)$. Le ℓ-groupe $G = \mathrm{GL}_n(\mathbb{Q}_p)$ est manifestement un ouvert de V, défini par $\det \neq 0$. On a donc $\mathrm{OC}(G) \subset \mathrm{OC}(V)$ et la (petite) mesure μ définit une petite mesure sur G encore notée μ. On peut voir cette mesure comme une forme linéaire sur $\mathcal{C}_c(G)$, et en tant que telle on peut la “multiplier” par la fonction localement constante (mais pas à support compact) $m \mapsto |\det m|^{-n}$, i.e. considérer la forme linéaire sur $\mathcal{C}_c(G)$

$$f \mapsto \int_G f(m)\,|\det m|^{-n} \prod_{1\leq i,j\leq n} \mathrm{d}m_{i,j}. \tag{57}$$

Nous avons noté $|x|$ la norme de $x \in \mathbb{Q}_p$, normalisée par $|p| = 1/p$.

Proposition 7.19. *La Formule* (57) *définit une mesure de Haar des deux côtés sur* $\mathrm{GL}_n(\mathbb{Q}_p)$ *pour laquelle* $\mathrm{GL}_n(\mathbb{Z}_p)$ *est de volume* $p^{-n^2}|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = \prod_{i=1}^n (1-p^{-i})$.

Démonstration — Le groupe G agit sur $\mathrm{PM}(V)$ par $(\mathrm{i}_g\mu)(U) = \mu(g^{-1}U)$. On a pour $v \in V$ et $g \in G$

$$(\mathrm{R}_v\,\mathrm{i}_g\,\mu)(U) \;=\; \mathrm{i}_g\,\mu(U+v) \;=\; \mu(g^{-1}(U+v)) \;=\; \mu(g^{-1}U + g^{-1}v) \;=\; \mathrm{i}_g\,(U)$$

donc $\mathrm{i}_g(U)$ est une mesure de Haar sur V, et le même argument que pour δ_G montre que l'on a un homomorphisme $d : G \to \mathbb{R}_{>0}$ trivial sur $\mathrm{GL}_n(\mathbb{Z}_p)$ et vérifiant $\mathrm{i}_g\mu = \mathrm{d}(g)\mu$. Il s'agit de démontrer que l'on a

$$\mathrm{d}(g) \;=\; |\det g|^{-n} \;\; \forall g \in G. \tag{58}$$

Comme l'homomorphisme d est nécessairement trivial sur $\mathrm{SL}_n(\mathbb{Q}_p)$ (on peut aussi invoquer le fait qu'une transvection $g \in G$ vérifie manifestement $\mathrm{d}(g) = 1$), ainsi que sur $\mathrm{GL}_n(\mathbb{Z}_p)$, on peut supposer $g = \mathrm{diag}(p, 1, \ldots, 1)$. Mais dans ce cas on a manifestement $\mu(g^{-1}\mathrm{M}_n(\mathbb{Z}_p)) = p^n$. La dernière assertion découle de la surjectivité de $\mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et de l'égalité $\mu(1 + p\mathrm{M}_n(\mathbb{Z}_p)) = \mu(p\mathrm{M}_n(\mathbb{Z}_p)) = p^{-n^2}$. $\square$

Nous avons montré au passage le fait que $\frac{\mathrm{d}x}{|x|}$ est une mesure de Haar sur $\mathbb{Q}_p^\times$ (cas $n = 1$). Notons $B_n \subset \mathrm{GL}_n$ (resp. N_n, resp. T_n) le sous-schéma en groupes des éléments triangulaires supérieurs (resp. unipotents supérieurs, resp. diagonaux). Chacun de ces groupes s'identifie naturellement à un ouvert d'un sous-espace vectoriel de $\mathrm{M}_n(\mathbb{Q}_p)$, et on démontre aisément la proposition suivante par la même méthode que ci-dessus :

Proposition 7.20. *(i) La mesure* $\prod_{i=1}^n \frac{\mathrm{d}m_{i,i}}{|m_{i,i}|}$ *est une mesure de Haar (des deux côtés) sur* $T_n(\mathbb{Q}_p)$.

(ii) La mesure $\prod_{1\leq i<j\leq n} \mathrm{d}m_{i,j}$ *est une mesure de Haar (des deux côtés) sur* $N_n(\mathbb{Q}_p)$.

(iii) La mesure $\prod_{i=1}^n |m_{i,i}|^{n+1-i} \prod_{1\leq i\leq j\leq n} \mathrm{d}m_{i,j}$ *est une mesure de Haar à gauche sur* $B = B_n(\mathbb{Q}_p)$, *et on a* $\delta_B(m) = \prod_{i=1}^n |m_{i,i}|^{n+1-2i}$ *pour tout* $m \in B$.

Nous allons terminer cette partie par une discussion de mesures sur les espaces homogènes (qui nous sera utile pour démontrer l'isomorphisme de Satake).

Proposition 7.21. *Soient* G *un* ℓ*-groupe et* H *un sous-groupe fermé avec* $(\delta_G)_{|H} = \delta_H$. *Il existe une (petite) mesure* $\mathrm{d}\overline{g}$ *non nulle sur* G/H, *unique à un scalaire dans* $\mathbb{R}_{>0}$ *près, qui est invariante à gauche par* G. *De plus, si* dg *et* dh *sont des (petites) mesures de Haar à gauche respectives sur* G *et* H, *il existe un unique choix pour* $\mathrm{d}\overline{g}$ *de sorte que l'on ait*

$$\int_G f(g)dg = \int_{G/H} (\int_H f(gh)\mathrm{d}h)\mathrm{d}\overline{g}$$

pour toute fonction $f \in \mathcal{C}_c(G)$.

Démonstration — Il y a plusieurs choses à vérifier, dont certaines sont sous-entendues dans l'énoncé. Tout d'abord, notons que H est un ℓ-groupe en tant que fermé de G. De plus, l'espace topologique quotient G/H est également un ℓ-espace. En effet, il est séparé, car G est séparé et H est fermé. D'autre part, la projection canonique $\pi : G \to G/H$ est à la fois ouverte et continue par définition, de sorte que si V est un voisinage de Hg dans G/H, $\pi^{-1}(V)$ est ouvert et contient donc un voisinage ouvert compact U de g dans G : $\pi(U)$ est un ouvert compact de V contenant g.

Fixons $\lambda = \mathrm{d}h$ une mesure de Haar à gauche sur H comme dans l'énoncé. Soit $f \in \mathcal{C}_c(G)$. Observons que pour $g \in G$, la fonction $h \mapsto f(gh)$ est évidemment continue, et nulle hors de l'ouvert compact $(\, g^{-1}\,\mathrm{Supp}\, f) \,\cap H$ de H. Il a donc un sens à poser $f_H(g) = \int_{h\in H} f(gh)\mathrm{dh}$ pour tout $g \in G$. On a $f_H(gh) = f_H(g)$ pour $g \in G$ et $h \in H$ car $\mathrm{d}h$ est invariante à gauche. De plus, si f est constante sur les ouverts compacts U_i (en nombre fini), et nulle hors de leur réunion, alors f_H est constante sur chaque ouvert U_iH, et nulle hors de la réunion des U_iH. Autrement dit, la fonction f_H, vue comme fonction sur G/H, est localement constante et à support compact. On a construit une application manifestement $\mathbb{C}$-linéaire

$$\mathcal{C}_c(G) \to \mathcal{C}_c(G/H), \;\; f \mapsto f_H. \tag{59}$$

Lemme 7.22. *L'application* (59) *est surjective.*

Démonstration — Les ouverts compacts de la forme Kg avec $g \in G$ et $K \subset G$ sous-groupe ouvert compact forment une base de la topologie de G, et donc les ouverts compacts $\pi(Kg) = KgH$ forment une base de la topologie de G/H. En particulier, les fonctions caractéristiques des KgH engendrent $\mathcal{C}_c(G/H)$. Fixons $g_0 \in G$ et K sous-groupe ouvert compact de G et étudions la fonction $(1_{Kg_0})_H$. Elle est manifestement nulle hors de Kg_0H, car pour $h \in H$ et $G \in G$, alors $gh \in Kg_0$ entraîne $g \in Kg_0K$. Comme elle est H-invariante à droite, il suffit de calculer $(1_{Kg_0})_H(g)$ pour $g \in Kg_0$. Dans ce cas, on a $gh \in Kg_0$ si, et seulement si, $h \in g_0^{-1}Kg_0$, et on a montré

$$(1_{Kg_0})_H \;=\; \lambda(H \cap (g_0^{-1}Kg_0))\, 1_{Kg_0H}, \tag{60}$$

ce qui conclut. □

L'unicité de $\overline{\mu}$, si elle existe, ainsi que $\overline{\mu}(U) > 0$ pour tout $U \in \mathrm{OC}(G/H)$ non vide, se démontrent comme dans le cas des mesures de Haar sur G, en observant que les gKH $(= gKg^{-1}gH)$, avec $g \in G$ et K sous-groupe ouvert compact de G, forment une base de la topologie de G/H constituée d'ouverts compacts. De plus, toujours supposant l'existence de $\overline{\mu}$, on constate que l'application linéaire $\mathcal{C}_c(G) \to \mathbb{C}$, $f \mapsto \int_{G/H} f_H\overline{\mu}$ est manifestement G-invariante par translations à gauche, et définit donc une mesure de Haar à gauche sur G (elle est manifestement ≥ 0 et $\neq 0$) : c'est donc un multiple de $\mu = \mathrm{d}g$. Quitte à remplacer $\overline{\mu}$ par un multiple, la Formule (60) montre que pour tout $g \in G$ et tout sous-groupe compact ouvert K de G on a

$$\lambda(H \cap g^{-1}Kg)\,\overline{\mu}(KgH) \;=\; \mu(Kg)$$

(et donc aussi $\lambda(H \cap K)\,\overline{\mu}(KH) \;=\; \mu(K)\,!$). Observer que si g est remplacé par gh avec $h \in H$, le terme de gauche est multiplié par $\delta_H(h)$ et celui de droite par $\delta_G(h)$, de sorte que l'hypothèse $\delta_H(h) = \delta_G(h)$ pour tout $h \in H$ est une condition nécessaire à l'existence de $\overline{\mu}$.

Montrons enfin l'existence de $\overline{\mu}$. Nous voulons poser, pour $f \in \mathcal{C}_c(G/H)$,

$$\int_{G/H} f\,\overline{\mu} \;:=\; \int_G \widetilde{f}\,\mu,$$

où $\widetilde{f} \in \mathcal{C}_c(G)$ vérifie $\widetilde{f}_H \;=\; f$. On a vu qu'une telle fonction $\widetilde{f}$ existe ; il ne reste donc qu'à vérifier que le terme de droite ne dépend pas du choix de $\widetilde{f}$, autrement dit que si $\varphi \in \mathcal{C}_c(G)$ vérifie $\varphi_H = 0$ alors on a $\int_G \varphi\mu = 0$.

Fixons donc $\varphi \in \mathcal{C}_c(G)$ avec $\varphi_H = 0$. Notons que l'on peut trouver un sous-groupe compact ouvert $K \subset G$ tel que φ est invariante à gauche par K. En effet, si on choisit des ouverts compacts U_i sur lesquels φ est constante, et hors desquels elle est nulle, on peut trouver des sous-groupes compacts ouverts $K_i \subset G$ avec $K\,U_i \subset U_i$ (Lemme 7.13 (ii) appliqué à U_i^{-1}) : le sous-groupe $K = \cap_i K_i$ convient. Écrivons la fonction φ comme une somme finie de fonctions φ_j dont le support est inclus dans une double classe de la forme $K\,g_j\,H$ avec $g_j \in G$. La fonction $(\varphi_j)_H$ est nulle hors de Kg_jH, et coïncide du coup avec φ_H sur Kg_jH : on a donc $(\varphi_j)_H = 0$ pour tout j : on peut supposer que φ est à support dans une unique double classe KgH, avec $g \in G$.

Écrivons $\operatorname{Supp}\varphi \;=\; \coprod_{i=1}^m K\,g\,h_i$ et $\varphi \;=\; \sum_{i=1}^m \varphi(gh_i)\,1_{Kgh_i}$. On a pour tout i l'égalité $\lambda(H \cap (gh_i)^{-1}Kgh_i) \;=\; \delta_H(h_i)\lambda(H \cap g^{-1}Kg)$. La Formule (60) et $\varphi_H \;=\; 0$ montrent que l'on a donc

$$\lambda(H \cap g^{-1}Kg) \sum_{i=1}^m \varphi(gh_i)\,\delta_H(h_i) = 0.$$

Mais d'autre part on a

$$\int_G \varphi(g)\mathrm{d}g \;=\; \sum_{i=1}^m \varphi(gh_i)\mu(Kgh_i) = \mu(Kg) \sum_{i=1}^m \varphi(gh_i)\delta_G(h_i),$$

qui est bien nulle par l'hypothèse sur δ_H et δ_G. Cela termine la démonstration de la Proposition 7.21. $\square$

4. Retour sur les anneaux de Hecke $\mathrm{H}(G,K)$

Soient G un ℓ-groupe et K un sous-groupe compact ouvert de G.

Pour tout $g \in G$, la double classe $KgK \subset G$ est une partie compacte (image de $K \times K \to G$, $(k,k') \mapsto kgk'$) manifestement ouverte de G, de sorte que les deux ensembles de classes $(KgK)/K$ et $K\backslash(KgK)$ sont finis : le G-ensemble G/K est admissible au sens du chapitre 3 §1.2, d'après le Corollaire 3.8.

D'autre part, $\mathrm{H}(G,K)$ n'est autre que le groupe des fonctions $f \in \mathcal{C}_c(G)$ à valeurs dans $\mathbb{Z}$ et invariantes par K des deux côtés. Nous avons vu que $\mathrm{H}(G,K)$ s'identifie naturellement à l'anneau de Hecke

$$\mathrm{H}(G/K) = \mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/K])^{\mathrm{opp}}$$

dont il hérite une structure d'anneau, le produit induit étant le produit de convolution $*$ introduit *loc. cit.* Soient $\mu = \mathrm{d}g$ la mesure de Haar à gauche sur G vérifiant $\mu(K) = 1$, ainsi que $f, f' \in \mathrm{H}(G,K)$ et $g \in G$, on a par définitions :

$$f*f'(g) = \sum_{h \in G/K} f(gh)\, f'(h^{-1})\, \mu(K) = \int_G f(gh)\, f'(h^{-1})\, \mathrm{d}h = \int_G f(h) f'(h^{-1}g)\, \mathrm{dh}.$$

(Une fonction manifestement K-invariante des deux côtés et à support dans le produit de $\mathrm{Supp}\, f$ par lui-même). L'associativité du produit de convolution serait aussi conséquence immédiate d'une version (immédiate !) de Fubini pour les petites mesures.

L'anneau $\mathrm{H}(G,K)$ apparaît dans la théorie des représentations de G de la manière suivante. Si V est un $\mathbb{Z}[G]$-module, on note $V^K = \{v \in V,\ kv = v\ \forall k \in V\}$ le sous-groupe des éléments K-invariants. On dispose d'une bijection naturelle

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/K], V) \overset{\sim}{\to} V^K, \varphi \mapsto \varphi([K]). \tag{61}$$

Comme $\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/K])$ agit à droite sur le membre de gauche, l'anneau opposé $\mathrm{H}(G,K)$ y agit à gauche, ce qui fait de V^K un $\mathrm{H}(G,K)$-module par transport de structure. Concrètement, la fonction $f \in \mathrm{H}(G,K)$ correspond à l'unique opérateur de Hecke T vérifiant $T_{gK,K} = f(g)$ pour tout $g \in G$, et donc si $v \in V^K$ et $f \in \mathrm{H}(G,K)$ on constate la formule

$$f \cdot v := \sum_{h \in G/K} f(h)\, hv. \tag{62}$$

Nous aurions pu, bien entendu, définir directement une structure de $\mathrm{H}(G,K)$-module sur V^K par cette formule : le fait $f.v \in V^K$ pour $v \in V^K$ et $f \in \mathrm{H}(G,K)$ est d'ailleurs évident, et la vérification des axiomes de modules assez aisée. La bijection (61) montre plus généralement le :

Corollaire 7.23. *$V \mapsto V^K$ est un foncteur des $\mathbb{Z}[G]$-modules vers les $\mathrm{H}(G,K)$-modules.*

Remarque 7.24. Nous n'irons pas plus loin dans ce cours au sujet des représentations de G, mais mentionnons tout de même qu'il n'est pas difficile de montrer que : (i) si V est un $\mathbb{C}[G]$-module avec $V^K \neq 0$, alors le $\mathbb{C}[G]$-module V est simple si, et seulement si, le $\mathrm{H}(G,K)\otimes\mathbb{C}$-module V^K l'est, (ii) $V\mapsto V^K$ induit une bijection entre l'ensemble des classes d'isomorphismes de $\mathbb{C}[G]$-modules simples vérifiant $V^K\neq 0$, et celui des classes d'isomorphismes de $\mathrm{H}(G,K)\otimes\mathbb{C}$-modules simples.

5. L'isomorphisme de Satake

On fixe désormais un entier $n\geq 1$ et on pose $G=\mathrm{GL}_n(\mathbb{Q}_p)$ et $K=\mathrm{GL}_n(\mathbb{Z}_p)$. Dans ce cas, $\mathrm{H}(G,K)$ s'identifie à l'opposé de l'anneau de Hecke du G-ensemble $G/K\simeq\mathrm{R}(\mathbb{Q}_p^n), g\mapsto g(\mathbb{Z}_p^n)$, des $\mathbb{Z}_p$-réseaux de $\mathbb{Q}_p^n$, un anneau déjà étudié au Chapitre 3. Par exemple, il est aisé de vérifier que l'on a $\mathrm{H}(\mathrm{R}(\mathbb{Q}_p))=\mathbb{Z}[\mathrm{R}_p^{\pm1}]$, et une variante immédiate du Théorème 3.18 montre

$$\mathrm{H}(\mathrm{R}(\mathbb{Q}_p^2))=\mathbb{Z}[\mathrm{R}_p,\mathrm{R}_p^{-1},\mathrm{T}_{\mathbb{Z}/p\mathbb{Z}}].$$

Rappelons d'abord la structure additive de $\mathrm{H}(G,K)$. Pour $\lambda=(\lambda_1,\dots,\lambda_n)\in\mathbb{Z}^n$, nous noterons $p^\lambda\in T$ l'élément diagonal

$$p^\lambda=\mathrm{diag}(p^{\lambda_1},\dots,p^{\lambda_n}).$$

Nous noterons aussi $\mathbb{Z}^{n,+}\subset\mathbb{Z}^n$ le sous-monoide des éléments $(\lambda_1,\dots,\lambda_n)$ croissants, i.e. vérifiant $\lambda_1\leq\cdots\leq\lambda_n$. La théorie des diviseurs élémentaires (modules de types fini sur l'anneau principal $\mathbb{Z}_p$) affirme que l'on a

$$\mathrm{GL}_n(\mathbb{Q}_p)=\coprod_{\lambda\in\mathbb{Z}^{n,+}}\mathrm{GL}_n(\mathbb{Z}_p)p^\lambda\mathrm{GL}_n(\mathbb{Z}_p).$$

Pour $\lambda\in\mathbb{Z}^n$ on note $\mathrm{c}_\lambda\in\mathrm{H}(G,K)$ la fonction caractéristique de $Kp^\lambda K$. La décomposition ci-dessus et un argument déjà détaillé dans la démonstration du Théorème 3.15 montrent le :

Proposition 7.25. *Les c_λ avec $\lambda\in\mathbb{Z}^{n,+}$ forment une $\mathbb{Z}$-base de $\mathrm{H}(G,K)$. De plus, l'isomorphisme naturel $\mathrm{H}(G,K)\overset{\sim}{\to}\mathrm{H}(\mathrm{R}(\mathbb{Q}_p^n))$ envoit c_λ sur l'opérateur $\mathrm{R}_{p^{\lambda_1}}\mathrm{T}_A$ avec $A=\prod_{i=2}^n\mathbb{Z}/(p^{\lambda_i-\lambda_1}\mathbb{Z})$.*

Donnons d'abord une astuce due à Gelfand montrant la commutativité de $\mathrm{H}(G,K)$ pour tout $n\geq 1$. On rappelle qu'un *anti-automorphisme* d'un groupe G est un isomorphisme de groupes $\varphi: G\overset{\sim}{\to}G^{\mathrm{opp}}$, i.e. une bijection de G vérifiant $\varphi(1)=1$ et $\varphi(gh)=\varphi(h)\varphi(g)$ pour tous $g,h\in G$.

Proposition 7.26. (Gelfand) *Soient G un ℓ-groupe et K un sous-groupe compact ouvert. On suppose que G possède un anti-automorphisme φ vérifiant $\varphi(KgK)=KgK$ pour tout $g\in G$ (en particulier $\varphi(K)=K$). Alors $\mathrm{H}(G,K)$ est un anneau commutatif.*

Démonstration — Fixons $f,f'\in\mathrm{H}(G,K)$ et $g\in G$. On a

$$(f*f')(\varphi(g))=\sum_{h\in G/K}f(h)f'(h^{-1}\varphi(g))$$

$$=\sum_{h\in G/K}f(\varphi(h)^{-1})f'(\varphi(h)\varphi(g))=\sum_{h\in G/K}f(\varphi(h)^{-1})f'(\varphi(gh))=(f'\circ\varphi)*(f\circ\varphi)(g)$$

En effet, les première et quatriéme égalités valent par définition, la seconde utilise le fait que $g\mapsto\varphi(g)^{-1}$ induit une bijection de G/K (car $\varphi(K)=K$, φ bijectif et

$\varphi(ab) = \varphi(ba)$ pour $a, b \in G$) et la troisième utilise $\varphi(gh) = \varphi(h)\varphi(g)$. On n'a pas encore utilisé $\varphi(KgK) = KgK$ pour tout $g \in G$, mais cela entraîne $f \circ \varphi = f$ pour tout $f \in \mathrm{H}(G, K)$. On a donc $f * f' = f' * f$. □

Ce lemme s'applique à $G = \mathrm{GL}_n(\mathbb{Q}_p)$, $K = \mathrm{GL}_n(\mathbb{Z}_p)$ et $\varphi(g) = {}^t g$, si l'on remarque que l'on a $\varphi(KtK) = K\varphi(t)K = KtK$ pour tout $t \in T_n(\mathbb{Q}_p)$, et en particulier pour $t = p^\lambda$.

Corollaire 7.27. *L'anneau* $\mathrm{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p))$ *est commutatif.*

Nous allons préciser sensiblement cet énoncé en démontrant le fameux *isomorphisme de Satake*. Définir cet homomorphisme nécessite un peu de préparation. On pose $B = B_n(\mathbb{Q}_p)$, $T = T_n(\mathbb{Q}_p)$ et $N = N_n(\mathbb{Q}_p)$. Si $H \subset G$ est un sous-groupe fermé, on posera aussi $H^0 = H \cap K$. On a en particulier

$$G^0 = K,\ B^0 = B_n(\mathbb{Z}_p),\ T^0 = T_n(\mathbb{Z}_p)\ \text{ et }\ N^0 = N_n(\mathbb{Z}_p).$$

Lemme 7.28. *On a* $G = BK$ *et la restriction* $f \mapsto f_{|B}$ *est un morphisme d'anneaux injectif* $\mathrm{H}(G, K) \to \mathrm{H}(B, B^0)$.

Démonstration — Notons ϵ_i la base canonique de $\mathbb{Q}_p^n$ et $W_i \subset \mathbb{Q}_p^n$ le sous-espace vectoriel engendré par les ϵ_j avec $1 \leq j \leq i$. Si L est un réseau de $\mathbb{Q}_p^n$, alors $L_i = L \cap W_i$ est un réseau de W_i et L_{i+1}/L_i est libre de rang 1. On peut donc choisir une $\mathbb{Z}_p$-base $f_1, \ldots, f_n$ de L vérifiant $L_{i+1} = L_i + \mathbb{Z}_p f_{i+1}$ pour $1 \leq i < n$. L'élément $g \in \mathrm{GL}_n(\mathbb{Q}_p)$ envoyant f_i sur ϵ_i est dans B, et vérifie $gL = \mathbb{Z}_p^n$: on a montré que B agit transitivement sur $\mathrm{R}(\mathbb{Q}_p^n)$, et donc $G = BK$.

Notons que B étant fermé dans G, l'application de l'énoncé est bien définie. D'après le premier point, on peut voir le G-ensemble transitif $\mathrm{R}(\mathbb{Q}_p^n)$ comme un B-ensemble transitif. Mais l'inclusion évidente $\mathrm{End}_{\mathbb{Z}[G]}(\mathrm{R}(\mathbb{Q}_p^n)) \subset \mathrm{End}_{\mathbb{Z}[B]}(\mathrm{R}(\mathbb{Q}_p^n))$ s'identifie tautologiquement à $\mathrm{H}(G, K) \to \mathrm{H}(B, B \cap K)$, $f \mapsto f_{|B}$. □

La seconde étape consiste à utiliser le dévissage $B = TN$ (produit semi-direct). Nous notons $\mathrm{d}n$, $\mathrm{d}t$ et $\mathrm{d}b$ les mesures de Haar à gauche respectives sur N, T et B pour lesquelles le volume de N^0 (resp. T^0, resp. B^0) vaut 1 ; par exemple, $\mathrm{d}n$ est exactement la mesure de Haar de la Proposition 7.20 (ii). On rappelle que N étant fermé dans B, on a défini une application $f \mapsto f_N$, $\mathcal{C}_c(B) \to \mathcal{C}_c(B/N)$, avec $f_N(b) = \int_N f(bn)\mathrm{d}n$ (Formule (59)). Comme la multiplication $T \times N \to B$, $(t, n) \mapsto tn$ est un homéomorphisme, on a un isomorphisme naturel $\mathcal{C}_c(B/N) \xrightarrow{\sim} \mathcal{C}_c(T)$. En particulier, la fonction $t \mapsto f_N(t)$ est dans $\mathcal{C}_c(T)$ pour $f \in \mathcal{C}_c(B)$.

Lemme 7.29. *L'application* $f \mapsto f_N$ *est un morphisme d'anneaux* $\mathrm{H}(B, B^0) \longrightarrow \mathrm{H}(T, T^0)$.

Démonstration — Il est évident que pour $f \in \mathrm{H}(B, B^0)$ alors $f_N(t)$ est invariante à droite par T^0, ainsi qu'à gauche par commutativité de T. Observons que l'on a

$$\int_B \psi(b)\,\mathrm{d}b = \int_{T \times N} \psi(tn)\,\mathrm{d}n\,\mathrm{d}t \quad \forall \psi \in \mathcal{C}_c(B) \tag{63}$$

En effet, on peut voir B comme un espace homogène (principal) sur le groupe $T \times N^{\mathrm{opp}}$, agissant à gauche par $((t,n),b)) \mapsto tbn)$. L'espace B possède donc une unique mesure $T \times N^{\mathrm{opp}}$-invariante à gauche μ pour laquelle $T^0.1.N^0 = B^0$ est de volume 1. Mais la mesure $\mathrm{d}b$ sur B est invariante à gauche par T, et à droite par N (car $\delta_B(N) = 1$), et attribue à B^0 le volume 1 : on a donc $\mu = \mathrm{d}b$. On conclut la Formule (63) par la Proposition 7.21 appliquée à $G = T \times N^{\mathrm{opp}}$, $H = 1$, $G/H = B$ et $f(t,n) = \psi(tn)$ (noter que N est unimodulaire). Pour $f, f' \in \mathrm{H}(B, B^0)$ et $t \in T$ on a donc

$$(f * f')_N(t) = \int_{N\times B} f(b)f'(b^{-1}tn)\,\mathrm{d}b\,\mathrm{d}n = \int_{N\times T\times N} f(t'n')f'(n'^{-1}t'^{-1}tn)\,\mathrm{d}n\,\mathrm{d}n'\,\mathrm{d}t'$$
$$= \int_{N\times T\times N} f(t'n')f'(tt'^{-1}n)\,\mathrm{d}n\,\mathrm{d}n'\,\mathrm{d}t' = \int_T f_N(t')f'_N(t'^{-1}t)\,\mathrm{d}t' = (f_N * f'_N)(t),$$

la troisième égalité résultant du changement de variables $n \mapsto t^{-1}t'n'^{-1}t'^{-1}tn$. $\square$

Corollaire-Définition 7.30. (Homomorphisme de Satake) *Si* $f \in \mathrm{H}(G,K)$ *on note* $\mathrm{S}(f) \in \mathrm{H}(T,T^0)[p^{-1/2}]$ *la fonction définie par*

$$\mathrm{S}(f)(t) = \delta_B(t)^{1/2} f_N(t).$$

L'application $f \mapsto \mathrm{S}(f)$ *est un morphisme d'anneaux* $\mathrm{H}(G,K) \to \mathrm{H}(T,T^0)[p^{-1/2}]$.

Démonstration — L'application $f \mapsto \mathrm{S}(f)$ est un morphisme d'anneaux, comme composée de trois morphismes : d'une part, la restriction $\mathrm{H}(G,K) \to \mathrm{H}(B,B^0)$, $f \mapsto f_{|B}$, d'autre part l'application $\mathrm{H}(B,B^0) \to \mathrm{H}(T,T^0)$, $f \mapsto f_N$, et enfin l'application $\mathrm{H}(T,T^0)[p^{-1/2}] \to \mathrm{H}(T,T^0)[p^{-1/2}]$, $f \mapsto (t \mapsto f(t)\delta_B(t)^{1/2})$ (c'est un morphisme d'anneaux car δ_B est un morphisme de groupes). On a utilisé $\delta_B(T) \subset p^{\mathbb{Z}}$, fait par exemple évident sur la formule 7.20 (iii). $\square$

Notons que par commutativité de T, $\mathrm{H}(T,T^0)$ est l'espace des fonctions à support fini sur le groupe abélien T/T^0. De plus, l'application naturelle $T/T^0 \to \mathrm{H}(T,T^0)$, envoyant tT^0 sur la fonction caractéristique de tT^0, est trivialement multiplicative, et induit un isomorphisme

$$\mathbb{Z}[T/T^0] \xrightarrow{\sim} \mathrm{H}(T,T^0).$$

L'application $\mathbb{Z}^n \longrightarrow T/T^0, \lambda \mapsto p^\lambda T^0$, est un isomorphisme de groupes (discrets) commutatifs ; elle induit un isomorphisme d'anneaux

$$\mathbb{Z}[T/T^0] \xrightarrow{\sim} \mathbb{Z}[X_1, X_1^{-1}, X_2, X_2^{-1}, \dots, X_n, X_n^{-1}],$$

faisant correspondre à $[p^\lambda T^0]$ le monôme $X^\lambda := \prod_{i=1}^n X_i^{\lambda_i}$. L'application S peut donc alternativement être vue comme un morphisme d'anneaux

$$\mathrm{S}' : \mathrm{H}(G,K) \to \mathbb{Z}[p^{-1/2}, X_1^{\pm 1}, \dots, X_n^{\pm 1}], \quad f \mapsto \sum_{\lambda \in \mathbb{Z}^n} \mathrm{S}(f)(p^\lambda)\ X^\lambda.$$

Le groupe $\mathfrak{S}_n$ agit naturellement sur T par permutation des coordonnées (en préservant manifestement T^0), ainsi donc que sur $\mathrm{H}(T,T^0)$ et $T/T^0 \simeq \mathbb{Z}^n$ (permutation évidente des X_i).

Théorème 7.31. *(Satake)* S' *définit un isomorphisme d'anneaux*

$$\mathrm{H}(G,K) \otimes \mathbb{Z}[p^{-1/2}] \xrightarrow{\sim} \mathbb{Z}[p^{-1/2}, X_1^{\pm 1}, \dots, X_n^{\pm 1}]^{\mathfrak{S}_n}.$$

La démonstration comporte plusieurs étapes. La partie la plus difficile, et qui expliquera la présence du facteur $\delta_B^{1/2}$ dans la définition de S, consiste à montrer que $\mathrm{S}'(f)$ est bien invariant par $\mathfrak{S}_n$. La preuve de Satake repose sur la formule d'intégration suivante, variante p-adique d'une formule du Harish-Chandra dans le cas réel. Dans l'énoncé suivant, $\mathrm{d}g$ et $\mathrm{d}t$ sont les mesures de Haar sur G et T affectant à K et T^0 la mesure 1, et $\mathrm{d}\overline{g}$ est la mesure G-invariantes sur G/T associée par la proposition 7.21 (noter que T est unimodulaire car commutatif).

Lemme 7.32. *(Satake) Soient $t = \mathrm{diag}(t_1, \dots, t_n) \in T$ avec $t_i \neq t_j$ pour tout $i \neq j$, et $f \in \mathcal{C}_c^\infty(G)$ telle que $f(kgk^{-1}) = f(g)$ pour tout $g \in G$ et tout $k \in K$. On a*

$$|\det t|^{(1-n)/2} \prod_{1 \leq i < j \leq n} |t_i - t_j| \int_{G/T} f(gtg^{-1})\mathrm{d}\overline{g} = \delta_B(t)^{1/2} \int_N f(tn)\mathrm{d}n.$$

Montrons d'abord comment cet énoncé implique l'invariance de $\mathrm{S}(f)$ par $\mathfrak{S}_n$ pour $f \in \mathrm{H}(G, K)$ (et donc invariante par conjugaison sous K). Le groupe $\mathfrak{S}_n$ se plonge naturellement dans G (matrices de permutations) en normalisant T, il agit donc sur la droite sur l'espace homogène G/T, puis sur $\mathrm{PM}(G/T)$ en commutant aux translations à gauche par G, et préservant la positivité. En utilisant l'unicité à un réel > 0 près de la mesure invariante $\mathrm{d}\overline{g}$, et le fait que tout homomorphisme $\mathfrak{S}_n \to \mathbb{R}_{>0}$ est trivial (c'est vrai pour tout groupe fini), on en déduit que $\mathrm{d}\overline{g}$ est invariante à droite par $\mathfrak{S}_n$. Ainsi, l'intégrale de gauche dans l'énoncé reste inchangée si t est remplacé par $\sigma t \sigma^{-1}$ pour $\sigma \in \mathfrak{S}_n$. Comme c'est également vrai pour le terme (non nul) $\prod_{i=1}^n |t_i - t_j|$, c'est encore vrai pour $\mathrm{S}(f)(t) = \delta_B(t)^{1/2} \int_N f(tn)\mathrm{d}n$ pour tout $t \in T$ *régulier*, i.e. vérifiant $t_i \neq t_j$ pour $i \neq j$. On conclut car pour tout $t \in T$ on peut toujours trouver $u \in T^0$ avec tu régulier, et on a pour $\sigma \in \mathfrak{S}_n$

$$\mathrm{S}(f)(t) \;=\; \mathrm{S}(f)(tu) \;=\; \mathrm{S}(f)(\sigma t u \sigma^{-1}) \;=\; \mathrm{S}(f)(\sigma t \sigma^{-1} \sigma u \sigma^{-1}) \;= \mathrm{S}(f)(\sigma t \sigma^{-1})$$

(noter $\sigma u \sigma^{-1} \in T^0$).

Démonstration — (du Lemme 7.32) Soit d_r la mesure de Haar à droite sur B (i.e. la mesure de Haar à gauche sur B^{opp}) affectant à B^0 le volume 1. Montrons d'abord que pour toute fonction $\psi \in \mathcal{C}_c(G)$ on a

$$\int_G \psi(g)\mathrm{d}g \;=\; \int_{K \times B} \psi(kb)\mathrm{d}k\,\mathrm{d}_r b \;=\; \int_{K \times T \times N} \psi(knt)\mathrm{d}k\,\mathrm{d}n\,\mathrm{d}t. \tag{64}$$

En effet, G peut être vu comme un espace homogène sous $K \times B^{\mathrm{opp}}$ via $((k, b), g) = kgb$. Le stabilisateur de 1 est le sous-groupe compact des (x, x^{-1}) avec $x \in B^0$, donc unimodulaire, donc il existe une unique mesure $K \times B^{\mathrm{opp}}$-invariante sur G affectant à $KB^0 = K$ le volume 1 : c'est nécessairement la mesure de Haar de G (qui convient !). La première égalit'e résulte alors de la proposition 7.21 appliquée à la fonction $\varphi(k, b) = \psi(kb)$ (noter que φ est invariante à droite par les (x, x^{-1}) avec $x \in B^0$, donc $\varphi = \varphi_{B_0}$). Cela montre la première égalité. La seconde s'en déduit par le même argument que celui prouvant la formule (63) (i.e. le même argument que précédement en plus simple !). On déduit de (64) que l'on a

$$\int_{G/T} \psi'(g)\,\mathrm{d}\overline{g} \;=\; \int_{K \times N} \psi'(kn)\,\mathrm{d}k\,\mathrm{d}n \quad \forall\, \psi' \in \mathcal{C}_c(G/T) \tag{65}$$

En effet, cela vaut pour ψ' de la forme ψ_T avec $\psi \in \mathrm{C}_c(G)$ par (64), mais on a vu que tout ψ' est de cette forme, par surjectivité de l'application (59). Appliquons cette identité à $\psi'(g) = f(gtg^{-1})$. Cette fonction est manifestement continue sur G et T-invariante à droite. Le centralisateur de t dans G est exactement T par hypothèse sur les t_i, de sorte que l'application continue naturelle $j : G/T \to G$, $gT \mapsto gtg^{-1}$ est une bijection sur la classe de conjugaison C de t dans G. Mais cette dernière est fermée : si $R \subset \mathbb{Q}_p$ désigne l'ensemble des t_i (on a donc $|R| \leq n$) alors C est le fermé de G défini par les équations $\prod_{r\in R}(r-g) = 0$ et $\det(r-g) = 0$ pour tout $r \in R$. Une application classique du théorème de Baire montre que j est un homéomorphisme de G/T dans C. Comme f est à support compact on en déduit que ψ' est à support compact. Comme f est invariante par conjugaison par K on a donc

$$\int_{G/T} f(gtg^{-1})\mathrm{d}\overline{g} = \int_N f(ntn^{-1})\mathrm{d}n. \tag{66}$$

Remarquons que l'élément $t^{-1}ntn^{-1}$ est dans N pour tout $n \in N$ et $t \in T$. Si l'on pose $\Delta(t) = |\det t|^{(1-n)/2}\prod_{1\leq i<j\leq n}|t_i - t_j|$, il ne reste qu'à montrer

$$\delta_B^{1/2}(t)\int_N \psi(n)\mathrm{d}n = \Delta(t)\int_N \psi(t^{-1}ntn^{-1})\mathrm{dn}, \quad \forall \psi \in \mathcal{C}_c(N). \tag{67}$$

(Appliquer cette formule à $\psi(n) = f(tn)$). Notons que la définition de $\Delta(t)$ et la formule $\delta_B(t) = |t_1|^{n-1}|t_2|^{n-3}|\cdots|t_n|^{1-n}$ (Proposition 7.20 (iii)) montrent

$$\Delta(t) = \prod_{1\leq i<j\leq n}|t_j/t_i - 1|\prod_{i=1}^{n}|t_i|^{n-i-\frac{n-1}{2}} = \delta_B(t)^{1/2}\prod_{1\leq i<j\leq n}|t_j/t_i - 1|,$$

de sorte que l'identité à montrer est

$$\int_N \psi(n)\mathrm{d}n = \prod_{1\leq i<j\leq n}|t_j/t_i - 1|\int_N \psi(t^{-1}ntn^{-1})\mathrm{dn}, \quad \forall \psi \in \mathcal{C}_c(N). \tag{68}$$

Observons que cette identité est facile à voir en dimension $n = 2$ (et intuitive en général). En effet, dans ce cas N s'identifie naturellement à $\mathbb{Q}_p$ via $x \mapsto n_x$, $\mathrm{d}n$ à $\mathrm{d}x$, et on a $t^{-1}n_x t n_{-x} = n_{(t_2/t_1-1)x}$. On conclut car la multiplication par $t \in \mathbb{Q}_p^*$ multiplie la mesure par $|t|$ sur $\mathbb{Q}_p$ (cas très particulier de l'analyse faite dans la Prop. 7.19). Nous reportons à la fin de cette partie la démonstration du cas général de l'identité (68) (c'est le Lemme 7.36 dans le cas $s = n-1$). $\square$

Pour terminer la démonstration du Théorème 7.31, nous allons démontrer que les $\mathrm{S}(\mathrm{c}_\lambda)$ avec $\lambda \in \mathbb{Z}^{n,+}$ forment une $\mathbb{Z}[p^{-1/2}]$-base de l'anneau $R = (\mathrm{H}(T,T^0)[p^{-1/2}])^{\mathfrak{S}_n}$. Pour tout $\lambda \in \mathbb{Z}^n$, on note $\mathrm{b}_\lambda \in R$ la fonction caractéristique de l'orbite $\mathfrak{S}_n\lambda \subset \mathbb{Z}^n$. Toute $\mathfrak{S}_n$-orbite dans $\mathbb{Z}^n$ rencontrant $\mathbb{Z}^{n,+}$ en un et un seul point, il est clair que les b_λ avec $\lambda \in \mathbb{Z}^{n,+}$ forment une $\mathbb{Z}[p^{-1/2}]$-base de R. Considérons la relation d'ordre $\prec$ sur $\mathbb{Z}^n$ définie par

$$\lambda \prec \mu \ \Leftrightarrow\ \sum_{k=i}^{n}\lambda_k \leq \sum_{k=i}^{n}\mu_k \text{ pour } 1 < i \leq n, \text{ et } \sum_{k=1}^{n}\lambda_k = \sum_{k=1}^{n}\mu_k.$$

L'élément $\mu \in \mathbb{Z}^{n,+}$ étant donné, il n'y a qu'un nombre fini de $\nu \in \mathbb{Z}^{n,+}$ avec $\nu \prec \mu$. Pour $\lambda \in \mathbb{Z}^{n,+}$, il existe des uniques $d_{\lambda,\mu} \in \mathbb{Z}[p^{-1/2}]$, pour μ parcourant $\mathbb{Z}^{n,+}$, vérifiant

$$\mathrm{S}(\mathrm{c}_\lambda) = \sum_{\mu\in\mathbb{Z}^{n,+}} d_{\lambda,\mu}\,\mathrm{b}_\mu.$$

Lemme 7.33. *(i) Pour tout* $\lambda \in \mathbb{Z}^{n,+}$ *on a* $d_{\lambda,\lambda} = \delta_B(p^\lambda)^{1/2}$, *et en particulier,* $d_{\lambda,\lambda} \in \mathbb{Z}[p^{-1/2}]^\times$.

(ii) Pour tous $\lambda, \mu \in \mathbb{Z}^{n,+}$ *avec* $d_{\lambda,\mu} \neq 0$ *on a* $\mu \prec \nu$.

Ce lemme entraîne que les $\mathrm{S}(\mathrm{c}_\lambda)$ s'expriment en fonction des b_μ avec $\mu \prec \lambda$ en résolvant un système linéaire triangulaire (fini) sur $\mathbb{Z}[p^{-1/2}]$ dont la diagonale est inversible. Il concluera donc la démonstration du théorème de Satake.

Démonstration — (du Lemme 7.33) Fixons $\lambda \in \mathbb{Z}^{n,+}$. Pour $\mu \in \mathbb{Z}^{n,+}$ on a par définitions

$$d_{\lambda,\mu} = \delta_B^{1/2}(p^\mu) \int_N \mathrm{c}_\lambda(p^\mu n)\mathrm{d}n = \delta_B^{1/2}(p^\mu)\,\mathrm{vol}(N \cap (p^{-\mu}Kp^\lambda K))$$

où vol $= \mathrm{d}n$. Le volume ci-dessus est non nul si, et seulement si, on a

$$N \cap (p^{-\mu}Kp^\lambda K) \neq \emptyset.$$

Cette propriété vaut si $\mu = \lambda$ car $p^{-\lambda}Kp^\lambda K$ contient K. Supposons $N \cap (p^{-\mu}Kp^\lambda K)$ non vide. En prenant le déterminant on trouve $\sum_{i=1}^n \mu_i = \sum_{i=1}^n \lambda_i$, et de plus il existe $g \in N$ avec $p^\mu\, g \in Kp^\lambda K$. En particulier on a pour $i = 1, \ldots, n$

$$p^\mu\, g\, \Lambda^i\, \mathbb{Z}_p^n \subset Kp^\lambda\, \Lambda^i \mathbb{Z}_p^n \subset\, p^{\lambda_1+\lambda_2+\cdots+\lambda_k}\, \Lambda^i \mathbb{Z}_p^n. \tag{69}$$

Soit $\epsilon_1, \ldots, \epsilon_n$ la base canonique de $\mathbb{Z}_p^n$. L'identité (69) pour $i = 1$ entraîne $p^{\mu_1}\epsilon_1 \subset p^{\lambda_1}\mathbb{Z}_p^n$. Plus généralement, on a pour $i = 1, \ldots n$

$$p^{\mu_1+\mu_2+\cdots+\mu_i}\epsilon_1 \wedge \cdots \wedge \epsilon_i \subset p^{\lambda_1+\lambda_2+\cdots+\lambda_i}\Lambda^i \mathbb{Z}_p^n.$$

On a donc $\mu_1 + \mu_2 + \cdots + \mu_i \geq \lambda_1 + \lambda_2 + \cdots + \lambda_i$ pour $i = 1, \ldots, n$. Compte tenu de l'égalité $\sum_{i=1}^n \mu_i = \sum_{i=1}^n \lambda_i$, on a montré $\mu \prec \lambda$. Cela prouve le (ii).

Pour terminer la démonstration du (i), il ne reste qu'à montrer $N \cap (p^{-\lambda}Kp^\lambda K) = N \cap K$. Soient $g \in N \cap (p^{-\lambda}Kp^\lambda K)$. Observons que la formule (69) pour $i = 1$ et $\lambda = \mu$ montre que pour tout $1 \leq j \leq n$ l'élément $p^\lambda g(\epsilon_j) = \sum_{i \leq j} p^{\lambda_i} g_{i,j}\epsilon_i$ est dans $p^{\lambda_1}\mathbb{Z}_p^n$. En particulier, le coefficient $g_{1,j}$ est dans $\mathbb{Z}_p$ pour tout j. Plus généralement, cette même formule appliquée à i quelconque et à $p^\lambda\, g(\epsilon_1 \wedge \epsilon_2 \wedge \cdots \wedge \epsilon_{i-1} \wedge \epsilon_j)$ pour $j \geq i$ montre $g_{i,j} \in \mathbb{Z}_p$. □

Corollaire 7.34. *L'isomorphisme de Satake induit des bijections canoniques entre :*

(i) l'ensemble des morphismes d'anneaux $\mathrm{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p)) \to \mathbb{C}$,

(ii) l'ensemble des orbites de $\mathfrak{S}_n$ *sur* $(\mathbb{C}^\times)^n$,

(iii) l'ensemble $\mathrm{GL}_n(\mathbb{C})_{\mathrm{ss}}$ *des classes de conjugaison d'éléments diagonalisables dans* $\mathrm{GL}_n(\mathbb{C})$.

Démonstration — L'isomorphisme de Satake (disons dans sa version S′) identifie canoniquement le premier ensemble aux homomorphismes de $\mathbb{C}$-algèbres

$$\mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]^{\mathfrak{S}_n} \to \mathbb{C},$$

ce qui montre l'équivalence entre (i) et (ii). En effet, pour tout groupe fini G d'automorphismes d'une $\mathbb{C}$-algèbre commutative de type fini on a une bijection canonique entre $G\backslash \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(A, \mathbb{C})$ et $\mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(A^G, \mathbb{C})$: on applique ceci à $A = \mathbb{C}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$ et $G = \mathfrak{S}_n$. La bijection naturelle sous-entendue entre (ii) et (iii) est celle associant à une classe de conjugaison de matrice diagonalisable la collection non ordonnée de ses valeurs propres. $\square$

Les classes de conjugaison du (iii) seront des analogues des Frobenius en théorie des formes automorphes. Les énoncés ci-dessus, ainsi que les démonstrations, se généralisent à $\mathrm{H}(G(\mathbb{Q}_p), G(\mathbb{Z}_p))$ pour tout schéma en groupe G affine, de type fini, et réductif, sur $\mathbb{Z}_p$ (voir les articles référencés de Satake et Cartier, ou encore l'article de survol de Gross *"On the Satake isomorphism"*). Le groupe $\mathrm{GL}_n(\mathbb{C})$ dans le (iii) ci-dessus est alors remplacé par un certain groupe réductif complexe appelé *dual de Langlands de G*. C'est l'un des points de départ de la théorie de Langlands (voir *Euler Products*).

Remarque 7.35. Pour $i = 1, \ldots, n$, considérons l'élément (contenant i fois 1)

$$\omega_i = (0, \ldots, 0, 1, 1, \ldots, 1) \in \mathbb{Z}^{n,+}.$$

On vérifie sans difficulté que ω_i est minimal pour $\prec$: si $\mu \prec \omega_i$ avec $\mu \in \mathbb{Z}^{n,+}$ alors $\mu = \omega_i$. D'autre part, on a $\delta_B(p^{\omega_i})^{1/2} = p^{\frac{i(n-i)}{2}}$ (Prop. 7.20 (iii)), et on a évidemment $\mathrm{b}_{\omega_i} = \Sigma_i(X_1, \ldots, X_n)$ ($i$ème polynôme symétrique élémentaire). On a donc la formule

$$\mathrm{S}(\mathrm{c}_{\omega_i}) = p^{\frac{i(n-i)}{2}} \Sigma_i(X_1, \ldots, X_n). \tag{70}$$

De plus, l'isomorphisme naturel $\mathrm{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p)) \xrightarrow{\sim} \mathrm{H}(\mathrm{R}(\mathbb{Q}_p^n))$ envoit c_{ω_i} sur l'opérateur $\mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^i}$ pour $i < n$, et sur R_p pour $i = n$ (Prop. 7.25). La théorie des polynômes symétriques élémentaires montre donc que l'on a

$$\mathrm{H}(\mathrm{R}(\mathbb{Q}_p^n))[p^{-1/2}] = \mathbb{Z}[p^{-1/2}, \mathrm{R}_p^{\pm 1}, \mathrm{T}_{\mathbb{Z}/p\mathbb{Z}}, \ldots, \mathrm{T}_{(\mathbb{Z}/p\mathbb{Z})^{n-1}}]$$

(sans autres relations). On a généralisé le Théorème 3.18. On pourrait même montrer qu'en fait il n'est pas nécessaire de rajouter $p^{-1/2}$ dans cet isomorphisme.

Terminons par une démonstration de la formule (68) utilisée dans la preuve du Lemme 7.32.[6] Pour $0 \leq s < n$, on notera I_s l'ensemble des couples $(i,j) \in \{1, \ldots, n\}^2$ avec $j - i \geq n - s$, puis N_s le sous-groupe fermé de N constitué des éléments de la forme $(n_{i,j})$ avec $n_{i,j} = 0$ pour $i \neq j$ et $(i,j) \notin \mathrm{I}_s$. C'est un sous-groupe distingué de B ; on a par exemple $N_{n-1} = N$ et $N_0 = \{1\}$. On notera $\mathrm{d}n$ la mesure $\prod_{(i,j)\in \mathrm{I}_s} \mathrm{d}n_{i,j}$: c'est une mesure de Haar à droite et à gauche affectant à N_s^0 le volume 1. Pour $1 \leq s < n$ on a bien entendu $N_s \supset N_{s-1}$, et la surjection $\pi_s : N_s \to \mathbb{Q}_p^s$, $n \mapsto (n_{i,n+i-s})_{i=1}^s$, est un morphisme de groupes de noyau N_{s-1} (bien entendu, $\mathbb{Q}_p^s$ est vu ici comme groupe additif). La surjection π_s admet une unique section

6. L'argument donné dans l'article original de Satake utilise une construction des mesures de Haar en terme de formes différentielles invariantes, point de vue non abordé ici. Un autre argument, utilisé par exemple dans les notes de Waldspurger et par Harish-Chandra dans le cas réel, serait d'utiliser un calcul de jacobien de l'application $n \mapsto tnt^{-1}n^{-1}$ et une formule de changement variables dans le cadre des mesures sur des variétés analytiques sur $\mathbb{Q}_p$ (théorie de Weil), point de vue non abordé ici également. Nous suivrons plutôt ici l'indication de Cartier consistant à faire le calcul par dévissage sur des sous-groupes distingués naturels de N, qui a l'avantage d'être élémentaire, bien que de mise en place un peu pénible.

(manifestement continue) $\beta_s : \mathbb{Q}_p^s \to N_s$ vérifiant $\beta_s(x)_{i,j} = 0$ pour $j - i > n - s$. La Prop. 7.21 implique la formule suivante, dans laquelle on a $1 < s < n$ et $f \in \mathcal{C}_c(N_s)$:

$$\int_{N_s} f(n)\mathrm{d}n \;=\; \int_{\mathbb{Q}_p^s \times N_{s-1}} f(\beta_s(x)n)\mathrm{d}x\mathrm{d}n. \tag{71}$$

Lemme 7.36. *Soient* $0 \leq s < n$, $t = \mathrm{diag}(t_1, \ldots, t_n) \in T$ *et* $f \in \mathcal{C}_c(N_s)$. *On a*

$$\prod_{(i,j)\in \mathrm{I}_s} |t_j/t_i - 1| \int_{N_s} f(t^{-1}\, n\, t\, n^{-1})\mathrm{d}n \;=\; \int_{N_s} f(n)\mathrm{d}n.$$

Démonstration — Posons $\alpha_t : N \to N$, $n \mapsto t^{-1}ntn^{-1}$. On a bien $\alpha_t(N_s) \subset N_s$ pour tout s, de sorte que l'énoncé a un sens. On procède par récurrence sur s, le cas $s = 0$ étant évident (l'identité cherchée s'écrivant $f(1) = f(1)$). Supposons $s > 0$ et fixons $y \in N_s$. On a pour $n \in N_{s-1}$ l'identité (de commutateurs) $\alpha_t(yn) = \alpha_t(y)y\alpha_t(n)y^{-1}$. L'hypothèse de récurrence montre donc

$$\prod_{(i,j)\in \mathrm{I}_{s-1}} |t_j/t_i - 1| \int_{N_{s-1}} f(\alpha_t(yn))\mathrm{d}n \;=\; \int_{N_{s-1}} f(\alpha_t(y)yny^{-1})\mathrm{d}n.$$

L'intégrale de droite est aussi égale à $\int_{N_{s-1}} f(\alpha_t(y)n)\mathrm{d}n$. En effet, la mesure $\mu = \mathrm{d}n$ sur N_{s-1} est invariante par conjugaison par N_s, et même par N. On peut le justifier ainsi : comme N_{s-1} est distingué dans B, des arguments déjà vu montrent qu'il existe un homomorphisme $a : B \to \mathbb{R}_{>0}$ avec $\mu(bUb^{-1}) = a(b)\mu(U)$ pour tout $U \in \mathrm{OC}(N_{s-1})$ et tout $b \in B$. Mais N étant le groupe dérivé de B, cet homomorphisme a est nécessairement trivial sur N. Observons enfin que l'on a $\int_{N_{s-1}} f(\alpha_t(y)n)\mathrm{d}n = \int_{N_{s-1}} f(y'n)\mathrm{d}n$ pour tout $y' \in N_s$ congru à $\alpha_t(y)$ modulo N_{s-1}. Appliquons ces analyses à $y = \beta_s(x)$ où $x = (x_i) \in \mathbb{Q}_p^s$. Dans ce cas on constate en appliquant l'homomorphisme π_s que l'on peut prendre $y' = \beta_s(t \cdot x)$ où $t \cdot x \in \mathbb{Q}_p^s$ désigne l'élément avec $(t \cdot x)_i = (t_{n-i+s}/t_i - 1)x_i$. On a montré

$$\prod_{(i,j)\in \mathrm{I}_{s-1}} |t_j/t_i - 1| \int_{N_s} f(\alpha_t(n))\mathrm{d}n \;=\; \int_{\mathbb{Q}_p^s \times N_{s-1}} f(\beta_s(t \cdot x)n)\mathrm{d}x\mathrm{d}n.$$

On peut (petit Fubini) intégrer d'abord en x le terme de droite. On trouve l'intégrale $\int_{\mathbb{Q}_p^s} f(\beta_s(x)n)\mathrm{d}x$ après multiplication par le produit des $|t_j/t_i - 1|$ où (i,j) parcourt les couples avec $i + j = n - s$. On conclut car la réunion de cet ensemble de couples avec I_{s-1} est I_s. □

6. Formes automorphes pour $\mathrm{GL}_n(\mathbb{A})$

6.1. Définitions. On dit qu'une fonction $\varphi : \mathrm{GL}_n(\mathbb{A}) \to \mathbb{C}$ est *lisse* au point $g \in \mathrm{GL}_n(\mathbb{A})$, avec disons $g = (g_\infty, g_f) \in \mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{A}_f)$, s'il existe :

– un voisinage ouvert U_∞ de g_∞ dans $\mathrm{GL}_n(\mathbb{R})$ et une fonction $\psi : U_\infty \to \mathbb{C}$ de classe $\mathcal{C}^\infty$ sur U_∞,

– un voisinage ouvert U_f de g_f dans $\mathrm{GL}_n(\mathbb{A}_f)$,

tels que l'on a $f(x) = \psi(x_\infty)$ pour tout $x = (x_\infty, x_f)$ dans $U_\infty \times U_f$. Il est clair qu'alors f est continue sur le voisinage ouvert $U_\infty \times U_f$ de g dans $\mathrm{GL}_n(\mathbb{A})$, et lisse en tout point de cet ouvert. Il est également clair que toute combinaisons linéaire finie de fonctions lisses en g est encore lisse en g.

Définition 7.37. *On note* $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ *le sous-espace vectoriel complexe des fonctions* $\mathrm{GL}_n(\mathbb{A}) \to \mathbb{C}$ *qui sont lisses en tout point de* $\mathrm{GL}_n(\mathbb{A})$.

L'espace de toutes les fonctions $\mathrm{GL}_n(\mathbb{A}) \to \mathbb{C}$ est muni d'une représentation naturelle de $\mathrm{GL}_n(\mathbb{A})$ par translations à droite, que l'on notera encore $(g, \varphi) \mapsto \mathrm{R}_g\varphi$, définie par $(\mathrm{R}_g\varphi)(h) = \varphi(hg)$. Le sous-espace $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ en est manifestement une sous-représentation.

Si $v \in \mathrm{V}$, le groupe $\mathrm{GL}_n(\mathbb{Q}_v)$ s'identifie de manière naturelle au sous-groupe de $\mathrm{GL}_n(\mathbb{A})$ constitué des éléments (g_w) avec $g_w = 1$ pour $w \neq v$. Pour $v \neq w$, $g \in \mathrm{GL}_n(\mathbb{Q}_v)$ et $h \in \mathrm{GL}_n(\mathbb{Q}_w)$, on a évidemment $gh = hg$ (où g et h sont bien entendus vus comme éléments de $\mathrm{GL}_n(\mathbb{A})$ par le plongement précédent). De même, l'identification $\mathrm{GL}_n(\mathbb{A}) = \mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{A}_f)$ permet d'identifier $\mathrm{GL}_n(\mathbb{A}_f)$ au sous-groupe $1 \times \mathrm{GL}_n(\mathbb{A}_f)$ de $\mathrm{GL}_n(\mathbb{A})$. Il commute à $\mathrm{GL}_n(\mathbb{R})$, contient $\mathrm{GL}_n(\mathbb{Q}_p)$ pour tout $p \in \mathrm{P}$, et il est même engendré par ces derniers et $\mathrm{GL}_n(\widehat{\mathbb{Z}})$.

Toute représentation de $\mathrm{GL}_n(\mathbb{A})$ définit donc par restriction des représentations des sous-groupes $\mathrm{GL}_n(\mathbb{Q}_v)$ pour tout $v \in \mathrm{V}$, ainsi que de $\mathrm{GL}_n(\mathbb{A}_f)$. Cela s'applique en particulier à $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$. Observons que l'action de $\mathrm{GL}_n(\mathbb{R})$ qui s'en déduit sur $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ est différentiable : si $X \in \mathfrak{g} = \mathfrak{gl}_n(\mathbb{R})$, $f \in \mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$, et $g = (g_\infty, g_f) \in \mathrm{GL}_n(\mathbb{A})$, il y a un sens à poser

$$(\mathrm{R}_X f)(g) = \frac{\partial}{\partial t}_{t=0} f(g_\infty e^{tX}, g_f).$$

Si on a $f(g) = \psi(g_\infty)$ avec $\psi \in \mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{R}))$ dans un voisinage de g, on a $(\mathrm{R}_X f)(g) = (\mathrm{R}_X\psi)(g_\infty)$ dans ce même voisinage. En particulier, $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ est un $(\mathfrak{g}, \mathrm{O}(n))$-module de manière naturelle.

Définition 7.38. *Une forme automorphe pour* $\mathrm{GL}_n(\mathbb{A})$ *est une fonction* φ *dans* $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ *ayant les propriétés suivantes :*

(i) $\varphi(\gamma g) = \varphi(g)$ *pour tout* $\gamma \in \mathrm{GL}_n(\mathbb{Q})$ *et tout* $g \in \mathrm{GL}_n(\mathbb{A})$,

(ii) il existe un sous-groupe compact ouvert $K \subset \mathrm{GL}_n(\mathbb{A}_f)$ *tel que* $\mathrm{R}_k\varphi = \varphi$ *pour tout* $k \in K$,

(iii) φ *est* $\mathrm{O}(n)$*-finie et* $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$*-finie,*

(iv) pour tout $g_f \in \mathrm{GL}_n(\mathbb{A}_f)$, *la fonction* $g_\infty \mapsto \varphi(g_\infty, g_f)$ *est à croissance modérée sur* $\mathrm{GL}_n(\mathbb{R})$.

On note $\mathcal{A}(n) \subset \mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ *l'espace des formes automorphes pour* $\mathrm{GL}_n(\mathbb{A})$. *C'est un sous-*$(\mathfrak{g}, \mathrm{O}(n))$*-module de* $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ *stable par les translations à droite par* $\mathrm{GL}_n(\mathbb{A}_f)$.

Justifions la dernière assertion. Le fait que $\mathcal{A}(n)$ est stable par $\mathfrak{g}$ est conséquence du théorème d'harmonicité de Harish-Chandra appliqué aux fonctions du (iv) (qui sont $\mathrm{O}(n)$-finies et $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$-finies par le (iii)). Le fait qu'il est stable par translations à droite par $\mathrm{GL}_n(\mathbb{A}_f)$ vient de l'observation suivante : si $g \in \mathrm{GL}_n(\mathbb{A}_f)$ et $\varphi \in \mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ est K-invariante à droite avec $K \subset \mathrm{GL}_n(\mathbb{A}_f)$ sous-groupe compact ouvert, alors $\mathrm{R}_g f$ est invariante à droite par le sous-groupe compact ouvert $g^{-1}Kg$ de $\mathrm{GL}_n(\mathbb{A}_f)$.

6.2. Lien avec les espaces considérés antérieurement. Éxaminons la définition de $\mathcal{A}(n)$. On a $\mathcal{A}(n) = \bigcup_{K\subset \mathrm{GL}_n(\mathbb{A}_f)} \mathcal{A}(n)^K$ où K parcourt les sous-groupes ouverts compacts de $\mathrm{GL}_n(\mathbb{A}_f)$. Notons que si $K \subset \mathrm{GL}_n(\mathbb{A}_f)$ un sous-groupe ouvert compact, il en va de même de $K \cap \mathrm{GL}_n(\widehat{\mathbb{Z}})$, de sorte que l'on a aussi :

$$\mathcal{A}(n) = \bigcup_{K\subset \mathrm{GL}_n(\widehat{\mathbb{Z}})} \mathcal{A}(n)^K,$$

où K parcourt les sous-groupes ouverts compacts de $\mathrm{GL}_n(\widehat{\mathbb{Z}})$.

Fixons K un sous-groupe ouvert compact de $\mathrm{GL}_n(\widehat{\mathbb{Z}})$. Il est d'indice fini dans $\mathrm{GL}_n(\widehat{\mathbb{Z}})$, de sorte que par la Proposition 7.7, il existe des éléments $\gamma_1, \ldots, \gamma_h \in \mathrm{GL}_n(\widehat{\mathbb{Z}})$ vérifiant $\mathrm{GL}_n(\mathbb{A}_f) = \coprod_{i=1}^h \mathrm{GL}_n(\mathbb{Q})\,\gamma_i\, K$. En particulier, on a une décomposition

$$\mathrm{GL}_n(\mathbb{A}) = \coprod \mathrm{GL}_n(\mathbb{Q})\gamma_i(\mathrm{GL}_n(\mathbb{R}) \times K) \tag{72}$$

(où γ_i signifie $1 \times \gamma_i$). Soit $f : \mathrm{GL}_n(\mathbb{A}) \to \mathbb{C}$ une fonction pour l'instant arbitraire vérifiant $f(gk) = f(g)$ pour $g \in G$ et $k \in K$. Pour $i = 1, \ldots, h$, on définit une fonction $f_i : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{C}$ par

$$f_i(h) = f(h \times \gamma_i). \tag{73}$$

La fonction f est $\mathrm{GL}_n(\mathbb{Q})$-invariante à gauche si, et seulement si, chaque fonction f_i est invariante à gauche par le sous-groupe

$$\Gamma_i = \mathrm{GL}_n(\mathbb{Q}) \cap \gamma_i K \gamma_i^{-1}$$

de $\mathrm{GL}_n(\mathbb{Q})$. Observons que comme $\gamma_i K \gamma_i^{-1}$ est un sous-groupe ouvert de $\mathrm{GL}_n(\widehat{\mathbb{Z}})$, il est d'indice fini dans ce dernier, de sorte que Γ_i est en fait d'indice fini [7] dans $\mathrm{GL}_n(\mathbb{Q}) \cap \mathrm{GL}_n(\widehat{\mathbb{Z}}) = \mathrm{GL}_n(\mathbb{Z})$. Réciproquement la décomposition (72) montre toute collection g_i de fonctions sur $\mathrm{GL}_n(\mathbb{R})$ invariantes à gauche par Γ_i provient d'une et une seule fonction sur $\mathrm{GL}_n(\mathbb{A})$ invariante à gauche par $\mathrm{GL}_n(\mathbb{Q})$ et à droite par K.

Proposition 7.39. *Soient $K \subset \mathrm{GL}_n(\widehat{\mathbb{Z}})$ un sous-groupe ouvert compact, ainsi que des éléments $\gamma_i \in \mathrm{GL}_n(\widehat{\mathbb{Z}})$ vérifiant* (72) *pour $i = 1, \ldots, h$. On pose $\Gamma_i = \mathrm{GL}_n(\mathbb{Q}) \cap \gamma_i K \gamma_i^{-1}$ et on définit f_i par la formule* (73)*. L'application $f \mapsto (f_i)$ est un isomorphisme de $(\mathfrak{g}, \mathrm{O}(n))$-modules*

$$\mathcal{A}(n)^K \xrightarrow{\sim} \prod_{i=1}^h \mathrm{A}(\mathrm{GL}_n(\mathbb{R}), \Gamma_i).$$

7. Ce n'est pas un sous-groupe d'indice fini quelconque. En effet, K contient par définition de la topologie de $\mathrm{GL}_n(\widehat{\mathbb{Z}})$ un sous-groupe "de congruence", i.e. de la forme $\mathrm{GL}_n(\widehat{\mathbb{Z}})_{(N)}$ avec $N \geq 1$. Ce sous-groupe étant distingué, Γ_i contient $\mathrm{GL}_n(\mathbb{Q}) \cap \mathrm{GL}_n(\widehat{\mathbb{Z}})_{(N)}$, qui est le noyau de $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$.

Démonstration — Comme $\mathrm{GL}_n(\mathbb{R}) \times K$ est un sous-groupe ouvert de $\mathrm{GL}_n(\mathbb{A})$, chacun des termes de la partition (72) est un ouvert de $\mathrm{GL}_n(\mathbb{A})$. On en déduit que f est dans $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$ si, et seulement si, les f_i sont dans $\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{R}))$. Il est évident que l'application $f \mapsto (f_i)$ commute aux actions de $\mathrm{O}(n)$ et $\mathfrak{g}$ pour $f \in \mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{A}))$. En particulier, la finitude du nombre h des indices montre que pour f satisfaisant (i) et (ii), alors f satisfait (iii), si et seulement si, tous les f_i sont $\mathrm{O}(n)$-finis et $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$-finis. Enfin, il est évident que si f satisfait (i), (ii) et (iv) alors les f_i sont à croissance modérée. Réciproquement, si $g_f \in \mathrm{GL}_n(\mathbb{A}_f)$ est quelconque on écrit $g_f = \gamma\gamma_i k$ pour certains $\gamma \in \mathrm{GL}_n(\mathbb{Q})$, $i \in \{1, \ldots, h\}$ et $k \in K$. On a donc pour $h \in \mathrm{GL}_n(\mathbb{R})$

$$f(h, g_f) = f(\gamma^{-1}h, g_i) = f_i(\gamma^{-1}h).$$

Si on a $|f_i(g)| \leq c||g||^N$ on en déduit bien $|f(h, g_f)| \leq c||\gamma^{-1}||^N||h||^N = c'||h||^N$. $\square$

La proposition précédente montre que du point de vue de l'action de $(\mathfrak{g}, \mathrm{O}(n))$, l'espace $\mathcal{A}(n)$ renferme essentiellement la même information que les $\mathrm{A}(\mathrm{GL}_n(\mathbb{R}), \Gamma)$ introduits précédemment, où Γ parcourt les sous-groupes de congruences (voir la remarque ci-dessus). Ce que l'on a gagné c'est que l'on dispose gratuitement d'une action des anneaux de Hecke $\mathrm{H}(\mathrm{GL}_n(\mathbb{A}_f), K)$ sur les $\mathcal{A}(n)^K$, pour tout sous-groupe ouvert compact $K \subset \mathrm{GL}_n(\mathbb{A}_f)$. Nous reviendrons juste après sur cette structure. Notons d'abord le corollaire immédiat suivant du Théorème 5.8 de Harish-Chandra et de la Proposition 7.39.

Théorème 7.40. *Pour tout sous-groupe compact ouvert $K \subset \mathrm{GL}_n(\mathbb{A}_f)$, et tout idéal de codimension finie $I \subset \mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$, le $(\mathfrak{g}, \mathrm{O}(n))$-module $\mathcal{A}(n)^K[I]$ est admissible. Autrement dit, pour tout $\tau \in \mathrm{Irr}(\mathrm{O}(n))$ on a*

$$\dim_{\mathbb{C}} \, \mathcal{A}(n)^K_\tau[I] \; < \; \infty.$$

Notons que l'espace $\mathcal{A}(n)^K_\tau[I]$ est le sous-espace de $\mathcal{A}(n)$ des fonctions annulées par I, invariantes par K, et dans la composante isotypiques de τ pour l'action de $\mathrm{O}(n)$. Comme les actions de $\mathfrak{z}$, $\mathrm{O}(n)$ et K commutent entre elles, l'ordre dans lequel on effectue les opérations $-^K$, $-_\tau$ et $-[I]$ est sans importance.

6.3. Remarques. Bien que comme nous l'avons dit le théorème 7.40 se déduit des énoncés d'Harish-Chandra, il est en fait aussi agréable de le démontrer directement dans le cadre adélique (point de vue adopté par Jacquet-Langlands pour GL(2), ou encore dans les notes de Waldspurger). Cela a plusieurs avantages, notamment le fait que le groupe discret Γ est fixé et égal à $\mathrm{GL}_n(\mathbb{Q})$. Ce dernier est le groupe des points rationnels d'un groupe algébrique sur un corps, dont la structure est assez classique, contrairement à celle des sous-groupes d'indices fini de $\mathrm{GL}_n(\mathbb{Z})$. Un autre exemple important de simplification est le fait qu'il n'y a qu'une seule "pointe" dans le cadre adélique, et donc qu'un domaine de Siegel, comme dans le cas du groupe $\mathrm{GL}_2(\mathbb{Z})$ voire même de $\mathrm{GL}_n(\mathbb{Z})$ ("tous les sous-groupes de Borel sont conjugués dans $\mathrm{GL}_n(\mathbb{Q})$"). Enfin, les propriétés des opérateurs de Hecke sont sensiblement plus transparentes dans ce contexte, et ouvrent la voie à l'utilisation de la théorie des représentations de $\mathrm{GL}_n(\mathbb{Q}_p)$. Dans le cadre adélique, on peut alors imiter de manière assez directe de nombreuses étapes de la démonstration donnée ici pour $\mathrm{GL}_2(\mathbb{Z})$, qu'il aurait été pédagogique (avec plus de temps à notre disposition...) d'étendre d'abord à $\mathrm{GL}_n(\mathbb{Z})$ pour dégager les difficultés combinatoires à résoudre en dimension > 2.

Donnons toutefois quelques définitions importantes dans ce contexte. Tout d'abord, comme dans le cas $\mathrm{GL}_2(\mathbb{Z})$, l'espace $\mathcal{A}(n)$ s'exprime très simplement (et facilement) en fonction de son sous-espace $\mathcal{A}^{\mathrm{unit}}(n)$ constitué des fonctions invariantes par les homothéties $\mathbb{R}_{>0}$ (à la place archimédienne). Un rôle central est encore joué par les formes paraboliques, que l'on définit maintenant. Pour chaque couple (a, b) d'entiers ≥ 0 vérifiant $a + b = n$, notons $N_{a,b} \subset \mathrm{GL}_n$ le sous-schéma en groupes constitué des éléments de la forme

$$n_x = \begin{pmatrix} \mathrm{I}_a & x \\ 0 & \mathrm{I}_b \end{pmatrix},$$

où x est une matrice de taille $a \times b$. L'application $x \mapsto n_x$ est un isomorphisme du groupe additif $\mathrm{M}_{a,b}$ des matrices de tailles $a \times b$ sur $N_{a,b}$. Une forme automorphe $f \in \mathcal{A}(n)$ est dite *parabolique* si on a

$$\int_{N_{a,b}(\mathbb{A})/N_{a,b}(\mathbb{Q})} f(ng)\,\mathrm{d}n = 0 \quad \forall\, g \in \mathrm{GL}_n(\mathbb{A}),$$

pour tout couple (a, b) avec $a + b = n$ et $ab \neq 0$. Noter que l'intégrale ci-dessus est une intégrale sur ab copies de l'espace compact $\mathbb{A}/\mathbb{Q}$, que l'on munit de la mesure invariante évidente. On vérifie immédiatement que c'est un sous-$(\mathfrak{g}, K) \times \mathrm{GL}_n(\mathbb{A}_f)$-module de $\mathcal{A}(n)$, noté $\mathcal{A}_{\mathrm{cusp}}(n)$. On démontre alors d'abord que $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}(n) := \mathcal{A}_{\mathrm{cusp}}(n) \cap \mathcal{A}^{\mathrm{unit}}(n)$ est constitué de fonctions bornées sur $\mathrm{GL}_n(\mathbb{Q})_{\mathrm{e}}\backslash\mathrm{GL}_n(\mathbb{A})$ et que ce dernier admet une mesure invariante finie. [8] De plus, les termes constants, indexés cette fois-ci par les couples (a, b), permettent d'exprimer $\mathcal{A}(n)/\mathcal{A}_{\mathrm{cusp}}(n)$ en fonction des espaces de formes automorphes des GL_a avec $0 < a < n$ (et donc de procéder par récurrence sur n). On démontre au passage le :

Théorème 7.41. $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}(n)$ *est somme directe avec multiplicité finie (en fait* 1*) de* $(\mathfrak{g}, \mathrm{O}(n)) \times \mathrm{GL}_n(\mathbb{A}_f)$*-modules.*

Les $(\mathfrak{g}, \mathrm{O}(n)) \times \mathrm{GL}_n(\mathbb{A}_f)$-modules intervenant ci-dessus sont les *représentations automorphes cuspidales* de $\mathrm{GL}_n(\mathbb{A})$.

7. Produits eulériens automorphes

Soient $N \geq 1$ un entier. Une forme automorphe f sera dite *de niveau* N si on a $f \in \mathcal{A}(n)^{K_N}$ où K_N désigne le sous-groupe de congruence $\mathrm{GL}_n(\widehat{\mathbb{Z}})_{(N)}$. Il est évident que si f est de niveau N alors elle est de niveau M pour tout entier M multiple de N.

L'espace $\mathcal{A}(n)^{K_N}$ des formes automorphes de niveau N est muni d'une action naturelle de l'anneau de Hecke $\mathrm{H}(G, K_N)$ commutant à l'action de $(\mathfrak{g}, \mathrm{O}(n))$. Soit p un nombre premier ne divisant pas N. On a manifestement

$$K_N = \mathrm{GL}_n(\mathbb{Z}_p) \times K_N^p, \ \text{ avec } K_N^p = \prod_{\ell \neq p} \mathrm{GL}_n(\mathbb{Z}_\ell)_{(N)},$$

de sorte que l'anneau commutatif

$$\mathrm{H}_p := \mathrm{H}(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p))$$

8. Si l'on munit $\mathrm{GL}_n(\mathbb{A})$ du "produit infini" des mesures naturelles sur $\mathrm{GL}_n(\mathbb{R})$ et sur chacun des $\mathrm{GL}_n(\mathbb{Q}_p)$ divisée par $1 - 1/p$ (sans quoi cela diverge), le volume de $\mathrm{GL}_n(\mathbb{Q})_{\mathrm{e}}\backslash\mathrm{GL}_n(\mathbb{A})$ devient même exactement égal à 1 par la Formule 6.14 et les Propositions 7.19 et 7.7. C'est un exemple de nombre de *Tamagawa*.

agit naturellement sur $\mathcal{A}(n)^{K_N}$. En effet, ce dernier est l'espace des $\mathrm{GL}_n(\mathbb{Z}_p)$-invariants du $\mathrm{GL}_n(\mathbb{Q}_p)$-module $\mathcal{A}(n)^{K_N^p}$, et on applique le §4. Il est évident que les actions des H_p, pour des premiers p distincts ne divisant pas N, commutent deux à deux. Par exemple, l'espace $\mathcal{A}(n)^{K_1}$ des formes automorphes de niveau 1, qui est naturellement isomorphe à $\mathrm{A}(\mathrm{GL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{Z}))$ d'après la Proposition 7.39 (on a $h = 1$ par la Proposition 7.7, et on peut prendre $\gamma_1 = 1$), est muni d'actions concommutantes de H_p pour tout premier p.

Soit $f \in \mathcal{A}(n)$ de niveau N et vecteur propre commun de tous les opérateurs $T \in \mathrm{H}_p$ pour tout p premier à N (ce qui sous-entend $f \neq 0$). Soit p premier ne divisant pas N. Comme $\mathcal{A}(n)^{K_N}$ est un H_p-module, il existe un unique morphisme d'anneaux $\pi_p : \mathrm{H}_p \to \mathbb{C}$ tel que $T.f = \pi_p(T)f$ pour tout $T \in \mathrm{H}_p$. L'isomorphisme de Satake associe alors à π_p une unique classe de conjugaison $\mathrm{c}_p(f) \in \mathrm{GL}_n(\mathbb{C})$ (appelée *paramètre de Satake de f en p*). Il y a donc un sens à considérer le produit Eulérien suivant :

$$\mathrm{L}(s, f) = \prod_{p \nmid N} \det(\mathrm{I}_n - p^{-s}\mathrm{c}_p(f))^{-1}.$$

(Il n'est pas difficile de voir que lorsque l'on a $n = 2$ et f est associée à une forme modulaire propre et normalisée, cette définition coïncide avec celle de Hecke). L'énoncé ci-dessous récapitule quelques résultats importants connus sur $\mathrm{L}(s, f)$ et les $\mathrm{c}_p(f)$.

Théorème 7.42. *Soient $f \in \mathcal{A}(n)$ de niveau N et propre pour les H_p avec p ne divisant pas N.*

(i) (Langlands) le produit eulérien $\mathrm{L}(s, f)$ converge absolument pour $\mathrm{Re}\, s$ assez grand,

(ii) (Langlands) il existe une décomposition $n = n_1 + \ldots, n_r$, et des formes automorphes cuspidales $f_i \in \mathcal{A}_{\mathrm{cusp}}(n_i)$ de niveau une puissance de N et propres pour les H_p avec p ne divisant pas N, vérifiant

$$\mathrm{L}(s, f) = \prod_{i=1}^{r} \mathrm{L}(s, f_i).$$

(iii) (Godement-Jacquet) si f est parabolique alors $\mathrm{L}(s, f)$ admet un prolongement méromorphe à $\mathbb{C}$ tout entier, holomorphe si $\mathrm{L}(s, f) \neq \prod_{p \nmid N}(1 - p^{-s})^{-1}$ (et en particulier si $n > 1$).

(iv) (Jacquet-Shalika) si f est dans $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}(n)$, les modules des valeurs propres des $\mathrm{c}_p(f)$ sont dans $]p^{-1/2}, p^{1/2}[$.

Les points (i) et (ii) ne seraient pas très difficiles à démontrer. Le (iv) est une version faible, mais remarquablement général, de la *conjecture de Ramanujan généralisée* : si f est dans $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}(n)$, de niveau N, et propre pour H_p avec p ne divisant pas N, alors les valeurs propres des $\mathrm{c}_p(f)$ sont de module 1.

Pour faire court : *Langlands conjecture que toutes les fonctions L d'origine arithmétique, comme toutes celles rencontrées au chapitre 1, sont de la forme $\mathrm{L}(s, f)$, avec*

f comme ci-dessus. Par exemple, la conjecture suivante est une immense généralisation de la loi de réciprocité quadratique (noter que dans cet énoncé, les propriétés analytiques des fonctions L ci-dessus ne jouent pas de rôle) :

Conjecture 7.43. *(Conjecture de réciprocité de Langlands) Soient K un corps de nombres galoisien sur $\mathbb{Q}$ et $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ une représentation (d'Artin). Il existe une forme automorphe $f \in \mathcal{A}(n)$ de niveau une puissance de $\mathrm{disc}\, K$, et propre pour les opérateurs de Hecke dans H_p pour p non ramifié dans K, vérifiant*

$$\det(X - \rho(\mathrm{Frob}_p)) = \det(X - \mathrm{c}_p(f))$$

pour tout premier p non ramifié dans K. De plus, f est cuspidale si, et seulement si, ρ est irréductible.

Noter que l'énoncé entraîne l'égalité de $\mathrm{L}(s, f)$ et de la fonction L-partielle $\mathrm{L}(s, \rho)$ (hors de N), et donc la conjecture d'Artin d'après Godement et Jacquet.

Ce n'est pas tout. On peut faire diverses opérations simples sur les fonctions L d'origine arithmétique qui n'ont pas d'analogues évidents sur les formes automorphes. Cela a conduit Langlands à conjecturer des énoncés internes aux formes automorphes, dont sa célèbre conjecture de fonctorialité. L'énoncé suivant n'est pas le plus général, mais sans doute l'un des plus importants (et à l'heure actuelle, semble-t-il, inaccessible). Soit $f \in \mathcal{A}(n)$ de niveau N et propre pour les H_p avec p ne divisant pas N. Soit $\rho : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_m(\mathbb{C})$ un morphisme de groupes polynomial. Langlands pose

$$\mathrm{L}(s, \rho, f) \;=\; \prod_{p \nmid N} \det(\mathrm{I}_n - p^{-s}\rho(\mathrm{c}_p(f)))^{-1}.$$

Conjecture 7.44. *(Conjecture de fonctorialité de Langlands) Pour tout $f \in \mathcal{A}(n)$ de niveau N et propre, et pour tout mophisme $\rho : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_m(\mathbb{C})$ comme ci-dessus, il existe une forme automorphe $f' \in \mathcal{A}(m)$ de niveau une puissance de N et propre, vérifiant $\mathrm{L}(s, \rho, f) = \mathrm{L}(s, f')$.*

On ne connaît actuellement que des cas très partiels (mais dans chacun des cas très importants !) de cette conjecture. Par exemple, le cas $n = 2$ et $\rho = \mathrm{Sym}^2$ est dû à Gelbart et Jacquet. Il y aurait beaucoup de plus à dire sur ces conjectures et leurs raffinements divers, incluant par exemple la définition de facteurs eulériens aux p divisant N, ou la considérations d'autres groupes que GL_n... Nous nous arrêterons toutefois ici ! Terminons par une proposition très simple.

Proposition 7.45. *Pour tout entier $N \geq 1$, l'espace vectoriel $\mathcal{A}(n)^{K_N}$ possède une base constituée de formes automorphes f ayant la propriété suivante : il existe une collection d'homomorphismes d'anneaux $\pi_p : \mathrm{H}_p \to \mathbb{C}$ pour tout p ne divisant pas N, et un entier $r \geq 1$, vérifiant*

$$(T - \pi_p(T))^r f = 0 \;\; \forall p \nmid N, \; \forall T \in \mathrm{H}_p.$$

.

Démonstration — En effet, il suffit de voir que $\mathcal{A}(n)^{K_N}$ est engendré par de telles fonctions. Mais $\mathcal{A}(n)^{K_N}$ est engendré par les espaces de dimension finie $\mathcal{A}(n)^{K_N}_{\tau}[I]$, qui sont stables par H_p pour tout $p \not| N$. Comme les H_p sont commutatifs, et commutent entre eux, leur action sur chaque $\mathcal{A}(n)_\tau^{K_N}[I]$ est co-trigonalisable, ce qui conclut aisément. $\square$

En utilisant le produit scalaire de Petersson adélique on pourrait même montrer que $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}(n)^{\mathrm{K}_\mathrm{N}}$ possède en fait une base de formes propres pour tous les H_p avec $p \not| N$.