Introduction aux formes automorphes et aux conjectures de Langlands

Cours de Master 2 à Orsay, Février-Avril 2017

Gaëtan Chenevier

Table des matières

Chapitre 1. Motivations : quelques fonctions L d'origine arithmétique 1

Chapitre 2. Formes modulaires 21
1. Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré et réseaux de $\mathbb{C}$ 21
2. Fonctions modulaires et fonctions de réseaux 24
3. Formes modulaires 27
4. q-développement d'une forme modulaire 28
5. Détermination de l'espace M_k 29
6. Quelques q-développements 33

Chapitre 3. Opérateurs de Hecke 37
1. Correspondances de Hecke abstraites 38
2. Correspondances entre réseaux 42
3. Action de l'anneau de Hecke sur les fonctions et formes modulaires 46
4. Exemples et estimées des valeurs propres 48
5. Liens entre coefficients de Fourier et valeurs propres des opérateurs de Hecke 50
6. Fonction L d'une forme modulaire : théorie de Hecke 52
7. Exercices 53

Chapitre 4. Formes automorphes pour $\mathrm{GL}_n(\mathbb{R})$ 55
1. Le groupe de Lie $\mathrm{GL}_n(\mathbb{R})$ 56
2. Algèbres enveloppantes 58
3. Le centre de $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$ 61
4. Formes automorphes pour un sous-groupe discret de $\mathrm{GL}_n(\mathbb{R})$ 64
5. Les formes modulaires sont des formes automorphes 67

Chapitre 5. Propriétés de finitude et $(\mathfrak{g}, K)$-modules 73
1. $(\mathfrak{g}, K)$-modules et énoncés de finitude 74
2. $(\mathfrak{g}, K)$-modules pour $\mathrm{GL}_2(\mathbb{R})$ 78
3. Le théorème d'harmonicité de Harish-Chandra 82
4. Exercices 87

Chapitre 6. L'espace des formes automorphes pour $\mathrm{GL}_2(\mathbb{Z})$ 89
1. Formes paraboliques 90
2. Les formes paraboliques invariantes par $\mathbb{R}^\times$ sont bornées 92
3. Digression sur $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})$ 94
4. Structure de $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$ 97
5. L'intégrabilité entraîne la croissance modérée 102

Chapitre 7. Formes automorphes pour $\mathrm{GL}_n(\mathbb{A})$ 105
1. Groupes et variétés adéliques 106
2. $\mathrm{GL}_n(\mathbb{A}_f)$ et réseaux de $\mathbb{Q}^n$ 110

3. Mesures sur les espaces et groupes localement profinis 112
4. Retour sur les anneaux de Hecke $\mathrm{H}(G, K)$ 119
5. L'isomorphisme de Satake 120
6. Formes automorphes pour $\mathrm{GL}_n(\mathbb{A})$ 127
7. Produits eulériens automorphes 131

CHAPITRE 1

Motivations : quelques fonctions L d'origine arithmétique

Cours 1 Quelques fonctions L d'origine galoisienne (1)

But : Expliquer deux constructions de fonctions L "d'origine arithmétique" : fonctions L d'Artin et fonctions L de courbes elliptiques / c.d.m. (cas particuliers de fonctions L / ξ à la Hasse-Weil). Dans les deux cas elles sont associées à des représentations de Groupes de Galois (ce sera évident pour celles d'Artin). On rappellera quelques conjectures classiques portant sur ces fonctions L (prol. analytique, valeurs spéciales). Dans tous les cas où ces conj. ont été résolues, c'est en montrant qu'elles sont de nature "automorphe" : motivation importante des conj. de Langlands.

I) Rappels sur les Frobenius

(1) $K/\mathbb{Q}$ corps de nombres galoisien sur $\mathbb{Q}$

$p \in \mathbb{Z}$ premier, $\mathcal{P}_p = \{ \mathfrak{P} \subset \mathcal{O}_K$ id. premiers $\mid (p) \}$ (i.e contenant p)

(on a $(p)\mathcal{O}_K = \prod_{\mathfrak{P} \in \mathcal{P}_p} \mathfrak{P}^{e_{\mathfrak{P}}}$)

$G := \mathrm{Gal}(K/\mathbb{Q})$ agit sur $\mathcal{P}_p$: $(\sigma, \mathfrak{P}) \longmapsto \sigma(\mathfrak{P})$

on sait que cette action est transitive ($\Leftrightarrow e_{\mathfrak{P}} = e_p$ ind. de $\mathfrak{P}$)

$G \supset G_{\mathfrak{P}}$ = stabilisateur de $\mathfrak{P}$ dans G = gp. déc. en $\mathfrak{P}$

il agit sur $k_{\mathfrak{P}} := \mathcal{O}_K/\mathfrak{P}$ corps fini $\supset \mathbb{F}_q$ $q = p^{f_{\mathfrak{P}}}$ cor. ?

$\mathrm{red}_{\mathfrak{P}} : G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ un hom. $I_{\mathfrak{P}} = \ker \mathrm{red}_{\mathfrak{P}}$ groupe d'inertie en $\mathfrak{P}$.

(i.e $I_{\mathfrak{P}} = \{ \sigma \in G_{\mathfrak{P}},\ \sigma x \equiv x \ (\mathfrak{P}) \ \forall x \in \mathcal{O}_K \}$.)

Fait 1. $\mathrm{red}_{\mathfrak{P}}$ est surjectif, i.e. $\exists\, \mathrm{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}}$, unique mod $I_{\mathfrak{P}}$, t.q. $\mathrm{red}_{\mathfrak{P}}(\mathrm{Frob}_{\mathfrak{P}}) =$ le frob. de $k_{\mathfrak{P}}/\mathbb{F}_p = x \mapsto x^p$.

autrement dit $\mathrm{Frob}_{\mathfrak{P}}\, x \equiv x^p \ (\mathfrak{P}) \quad \forall x \in \mathcal{O}_K$.

une façon de le voir : (point de vue local sur $G_{\mathfrak{P}}$).

on regarde $K_{\mathfrak{P}}$ = complété de K pour $|x| = q^{-v_{\mathfrak{P}}(x)}$ valuation $\mathfrak{P}$-adique.

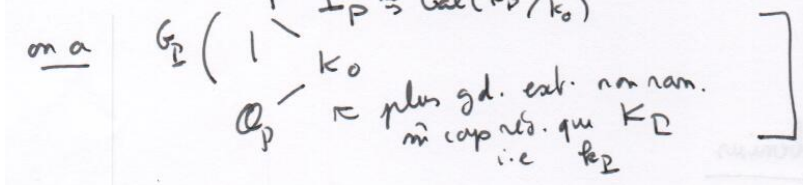
$$= \left(\varinjlim_n \left(\mathcal{O}_K / \mathfrak{P}^n \right) \right) \left[\tfrac{1}{p} \right]$$

c'est une ext. gal. finie de $\mathbb{Q}_p$, $K \longrightarrow K_{\mathfrak{P}}$ inj. à im. dense.

d'où $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(K/\mathbb{Q})$, induit $\mathrm{Gal}(K_{\mathfrak{P}}/\mathbb{Q}_p) \xrightarrow{\sim} G_{\mathfrak{P}}$

$\sigma \longmapsto \sigma|_K$.

on a



Fait 2 (évident) soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, on a $\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\sigma(\mathfrak{P})}$, $\sigma I_{\mathfrak{P}} \sigma^{-1} = I_{\sigma(\mathfrak{P})}$ et $\sigma\, \mathrm{Frob}_{\mathfrak{P}}\, \sigma^{-1} = \mathrm{Frob}_{\sigma(\mathfrak{P})}$ mod $I_{\mathfrak{P}}$

Cor : i) $\forall p$, les $G_{\mathfrak{P}}$ avec $\mathfrak{P} \mid (p)$ sont classe de conj. can. de ss-gps de $\mathrm{Gal}(K/\mathbb{Q})$.

ii) si p non ram dans K, i.e. $p \nmid \mathrm{disc}\, \mathcal{O}_K \Leftrightarrow e = 1$, $\Rightarrow I_{\mathfrak{P}} = 1$, alors $\mathrm{Frob}_p = \{ \mathrm{Frob}_{\mathfrak{P}},\ \mathfrak{P} \in \mathcal{P}_p \}$ classe de conj. dans $\mathrm{Gal}(K/\mathbb{Q})$

Rk : $p \longmapsto \mathrm{Frob}_p \subset G$ contient beaucoup de l'arithm. de K.

$p \nmid \mathrm{disc}\, K$

ex. ordre de $\mathrm{Frob}_{\mathfrak{P}} = f$ l'unique inconnue dans la déc. de (p)

- analogue archimédien : classe de conj. des conjugaisons complexes

$\mathrm{Frob}_\infty = \{ c_\sigma,\ \sigma : K \to \mathbb{C} \}$ où $c_\sigma(x) = \sigma^{-1}(\overline{\sigma(x)})$. ③

Exemple 1 $K = \mathbb{Q}(e^{2i\pi/N})$ ($\zeta = e^{2i\pi/N}$). $N \geq 1$ entier

hom. can. $\varepsilon : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^*$ "car. cycl."

$\sigma \longmapsto$ l'unique k t.q. $\sigma(\zeta) = \zeta^k$

(ex : morph. de gpls. injectif). $p \nmid N \Rightarrow p$ non ram ds K.

on a $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ (singleton : cas abélien).

$$\boxed{\varepsilon(\mathrm{Frob}_p) = p}$$

Car bien connu (Gauss). ε surjectif ! i.e $[K:\mathbb{Q}] = \varphi(N)$.

Exemple 2 soit $Q \in \mathbb{Z}[X]$ unitaire irréd., soit $p \in \mathbb{Z}$

nb premier, $Q \bmod p \equiv \prod Q_i^{e_i}$, $Q_i \in \mathbb{Z}/p\mathbb{Z}[X]$ unit irred.

pb non résolu de comprendre $p \longrightarrow$ type de décomp. de $Q \bmod p$ ex. $\{\deg Q_i\}$?

ex : pour quels p $Q \bmod p$ scindé mod p ? ($p \nmid \mathrm{disc}\, Q$ rem. $e_i = 1\ \forall i$).

. $Q = X^2 - m$ .... solution donnée par la loi de réciprocité quad.

$p \nmid 4m$, m carré mod $p \Leftrightarrow \bar{p} \in H_m \subset (\mathbb{Z}/4m\mathbb{Z})^*$ "où H_m ss groupe d'indice 2 explicite"

Lien avec les Frobenius : K = un corps de déc. de Q.

si $R = \{$racines de Q dans $\mathbb{C}\}$, $K = \mathbb{Q}(R)$

$Q(X) = \prod_{x \in R} (X - x)$ scindé ds $\mathcal{O}_K[X]$.

$\mathrm{Gal}(K/\mathbb{Q})$ agit sur R : $\rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathfrak{S}(R)$

si $p \nmid \mathrm{disc}\, Q$ (donc de K), $\rho(\mathrm{Frob}_P)$ est une permutation de R dont les cycles sont de longueur deg de Q_i !

$P \mid (p)$.

$\Rightarrow$ pt. cas part. de répartition des Frob_p ds $\mathrm{Gal}(K/\mathbb{Q})$.

II Fonctions L d'Artin (Référence : dernier chapitre de Neukirch)

$K/\mathbb{Q}$ c.d.m Galoisien $G = \mathrm{Gal}(K/\mathbb{Q})$ gpe fini.

soit $\rho : G \to GL(V)$ hom. V $\mathbb{C}$-ev de dim finie.

on va définir $L(s,\rho)$ une série de Dirichlet associée.

$$\| \prod_p L_p(s,\rho).$$

cas le plus simple p ∤ disc K, $\mathrm{Frob}_p \subset \mathrm{Gal}(K/\mathbb{Q})$ classe conj. constitué d'éléments 2 à 2 conjugués.

$\rho(\mathrm{Frob}_p) \subset GL(V)$

$\Rightarrow Q_p(X) := \det(1 - X\rho(\mathrm{Frob}_p))$ polynôme bien défini

$= 1 - \mathrm{tr}\,\rho(\mathrm{Frob}_p)X + \dots + (-1)^{\dim V} X^{\dim V} \det\rho(\mathrm{Frob}_p)$

On pose $\boxed{L_p(s,\rho) = \dfrac{1}{Q_p(p^{-s})}}$

- cas général $p \in \mathbb{Z}$, soit $\mathfrak{P} \mid (p)$. on regarde

$$V \supset V^{I_{\mathfrak{P}}} = \{v \in V,\ \rho(g)v = v \ \ \forall g \in I_{\mathfrak{P}}\}$$

ssev. sur lequel agit $G_{\mathfrak{P}}/I_{\mathfrak{P}} = \langle \mathrm{Frob}_{\mathfrak{P}} \rangle$.

on pose $Q_p(X) := \det(1 - X\rho(\mathrm{Frob}_{\mathfrak{P}})|_{V^{I_{\mathfrak{P}}}})$

ne dépend pas du choix de $\mathfrak{P}$ à cause du Fait 2.

($\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ $\sigma(V^{I_{\mathfrak{P}}}) = V^{\sigma I_{\mathfrak{P}} \sigma^{-1}} = V^{I_{\sigma(\mathfrak{P})}}$ ...)

Prop : i) $L(s,\rho)$ conv. abs. pour $\mathrm{Re}\, s > 1$

ii) $L(s,\rho)$ ne dépend que de la classe d'éq. de ρ. (comme rep.)

iii) $L(s,\rho_1 \oplus \rho_2) = L(s,\rho_1)\,L(s,\rho_2)$.

iv) $L(s,\rho) = \sum a_n n^{-s}$, $p \nmid \mathrm{disc}\,K$, $a_p = \mathrm{trace}(\rho(\mathrm{Frob}_p))$

preuve : i) tout élément de G est d'ordre fini, donc les vp. des $\rho(g)$ sont des racines de l'unité $\Rightarrow$ racines de $Q_p(X)$ ds $\mathbb{C}$ sont de module 1 i.e $Q_p(p^{-s})$ est produit de termes de la forme $\frac{1}{1-\alpha_p^{-s}}$. $\Rightarrow |L(s,\rho)| \leq \zeta(Re(s))^{[K:\mathbb{Q}]}$.

ii) iii) iv) évidents ■

Exemple 1 $\rho =$ rep. triviale de dim 1, on a $L(s,\rho) = \zeta(s)$ Riemann.
car $Q_p(X) = 1 - X \quad \forall p$.

Exemple 2 $K =$ corps de déc. de $\underset{\mathbb{Z}[X]}{\overset{\cap}{\mathbb{Q}}} = \mathbb{Q}(R)$ où $R = \{$rac. de $\mathbb{Q}$ ds $\mathbb{C}\}$.

$(\rho, V) = \mathbb{C}[R]$ (rep. de permutation).

alors $L(s,\rho) = \xi_K(s)$ ξ êta de Dedekind.

(laissé en exercice, au moins si $p \nmid$ disc $\mathbb{Q}$ c'est une conséquence immédiate de l'exemple 2 précédent).

Exemple 3 $K = \mathbb{Q}(e^{2i\pi/N})$, $\varepsilon : Gal(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$

et dim $V = 1$. Ops $V = \mathbb{C}$, $\rho = \chi \circ \varepsilon$: $Gal(K/\mathbb{Q}) \longrightarrow GL_1(\mathbb{C}) = \mathbb{C}^\times$

où χ car. de Dirichlet.

Alors $L(s,\rho) = L(s,\chi')$ où χ' est le car. de Dirichlet primitif ↖ fonction L de Dirichlet ass. à χ. i.e χ se factorise en

$$\underbrace{(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times}_{\chi}$$

avec $M \mid N$ minimal.

Laissé en exercice pour $p \mid N$, si $p \nmid N$ c'est une conséquence immédiate de l'Exemple 1 précédent.

En général on doit utiliser le

Lemme : $L / K / \mathbb{Q}$ (Galois / Galois), $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$ rep.

$\tilde{\rho} : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\text{can}} \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$

rep. composée ("inflation de ρ"), alors $L(s, \tilde{\rho}) = L(s, \rho)$.

preuve compatibilité de formation des gpes de déc. / Frob.

$p \in \mathcal{V}$, $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{Q} \subset \mathcal{O}_L$ avec $\mathfrak{Q} \mid \mathfrak{P} \mid p$, on a

$L_{\mathfrak{Q}} / K_{\mathfrak{P}} / \mathbb{Q}_p$

on a $\mathrm{Gal}(L_{\mathfrak{Q}} / \mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(K_{\mathfrak{P}} / \mathbb{Q}_p)$. via

$G_{\mathfrak{Q}} \twoheadrightarrow G_{\mathfrak{P}}$ $\quad \sigma \mapsto \sigma | K$

puis $I_{\mathfrak{Q}} \twoheadrightarrow I_{\mathfrak{P}}$

$\mathrm{Frob}_{\mathfrak{Q}} | K \equiv \mathrm{Frob}_{\mathfrak{P}} \bmod I_{\mathfrak{P}}$ ∎

Conjecture (Artin). ρ arbitraire

i) $L(s, \rho)$ se prolonge méro. à $\mathbb{C}$ tout entier, avec $s = 1$ pour unique pole éventuel, et $\mathrm{ord}_{s=1} L(s, \rho) = \langle 1, \rho \rangle$ ("le seul pole possible est $s=1$ et vient de ζ éventuellement")

ii) soit $n_\pm$ = dim du sp. de V où "Frob_∞" vaut $\pm \mathrm{id}$

$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2)$ avec $\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$.

fonction Γ d'Euler.

alors si on pose $\xi(s, \rho) = \Gamma_{\mathbb{R}}(s)^{n_+} \Gamma_{\mathbb{R}}(s+1)^{n_-} L(s, \rho)$

on a $\boxed{\xi(s, \rho) = \varepsilon \cdot N^{s-1/2} \xi(1-s, \rho^\vee)}$

$\varepsilon \in \mathbb{C}^\times$ (root number). N entier explicite (cond. d'Artin)

Théorème La conj. d'Artin est vraie si $\mathrm{Im}\,\rho$ abélien

Preuve : On a $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$.

ρ se factorise par $\rho' : \mathrm{Gal}(M/\mathbb{Q}) \to GL(V)$ où $M = K^{\ker \rho} \subset K$ et $\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Im}\,\rho$

- Lemme $\Rightarrow$ $L(s,\rho) = L(s,\rho')$

$\Rightarrow$ O.P.S. $\mathrm{Gal}(K/\mathbb{Q})$ abélien.

- Kronecker-Weber : $K \subset \mathbb{Q}(e^{2i\pi/N})$ $N \geq 1$.

Lemme encore $\Rightarrow$ O.P.S. $K = \mathbb{Q}(e^{2i\pi/N})$

- $\mathrm{Im}\,\rho$ ab $\Rightarrow$ ρ somme directe de caractères

Exemple 3 $\Rightarrow$ $L(s,\rho)$ produit de f. L de Dirichlet.

On conclut par les prop de ces fonctions (Riemann, Dirichlet). ●

Remarque (loi de réciprocité). Si $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$ est injective, alors $\rho(g) = 1 \Leftrightarrow g = 1 \Leftrightarrow \mathrm{tr}\,\rho(s) = \dim V$ donc si $p \nmid \mathrm{disc}\,K$, p tel. déc. dans $K \Leftrightarrow \mathrm{tr}\,\rho(\mathrm{Frob}_p) = \dim V$

donc identifier $L(s,\rho) \Longleftrightarrow$ loi de réciprocité généralisée à $\mathrm{Gal}(K/\mathbb{Q})$.

(cette remarque aurait sa place avant !)

Autres choses connues (et difficiles !)

Thm i) $L(s,\rho)$ méro sur $\mathbb{C}$ + ii) connue (Artin, Hecke, Brauer)
(mais on ne connaît pas le pôle dans $0 < \mathrm{Re}(s) < 1$

iii) Si ρ irred. de dim ≥ 2, et $n_+ = 1$,
conjecture connue (Khare-Wintenberger, Wiles, Serre, ...) Langlands, ...

on montre $\Rightarrow$ $L(s,\rho)$ et la fonction L ass. à une forme modul. pour GL_2

si $n_+ \neq 1$, on conj. que $L(s,\rho)$ et la fonction L d'une "forme de Maass" pour GL_2 .... et plus rad !

III Fonction L d'une courbe elliptique sur un c.d.n.

(référence : Tate "arithmetic of elliptic curve" inventiones math.)

Soit k un corps. Une courbe ell. sur k sera ici une courbe projective plane cubique $E \subset \mathbb{P}^2_{/k}$ non singulière, munie d'un point point rationnel $O \in E(k)$ qui est d'inflexion.

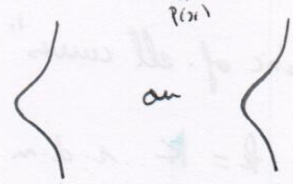
Exemple fondamental (universel, quitte à changer de coord. linéaires $/k$, lorsque $6 \in k^\times$) $E :=$ courbe défini par $Y^2 Z = X^3 + aXZ^2 + bZ^3$

avec $a, b \in k$, et $\Delta_E := 4a^3 + 27b^2 \in k^\times$, et $2 \in k^\times$

munie de $O := (0:1:0)$.

partie affine $E \cap (Z=1)$: $(x:y:1)$ $\qquad y^2 = x^3 + ax + b$ (éq. de Weierstrass) familière.

le lieu singulier vérifiait $2y = 0$ et $P'(x) = 0$ où $P = x^3 + ax + b$ (i.e. $y = 0 = P(x)$ si $2 \in k^\times$) donc vide car $2\Delta_E \in k^\times$.

dessin $k = \mathbb{R}$ O 

partie à ∞ $E \cap (Z=0)$: $\qquad 0 = X^3$ un seul point (triple) qui est $O = (0:1:0)$

point lisse / flex ? on se place sur $Y = 1$
on a $(x:1:z)$ avec $\qquad z = x^3 + axz + bz^3$ cqfd

Prop $\exists!$ loi de groupe sur $E(k)$ de neutre O t.q. $\forall P, Q, R \in E(k)$

$$P + Q + R = O \iff \exists \text{ droite } D \subset \mathbb{P}^2_{/k} \text{ t.q. } D \cap E(k) = \{P, Q, R\}$$
(avec mult.)

Rmq: • $P = -Q \Leftrightarrow \exists$ dte passant par P, Q et O

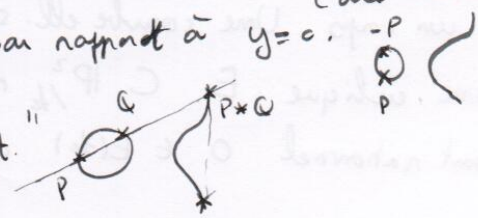
soit $\alpha X + \beta Y + \gamma Z = 0$ une dte générale $\alpha, \beta, \gamma \in k$.

elle passe par $O \Leftrightarrow \beta = 0$. 2 cas: . $\alpha = 0 \Rightarrow$ c'est $Z = 0$

. $\alpha \neq 0 \Rightarrow$ c'est $x = \text{cste}$.

(dte verticale)

$\Rightarrow$ l'opposé de P est le sym. par rapport à $y=0$.



$\Leftrightarrow P + Q =$ l'opposé du "3e pt. d'∩"

• $E(k)$ abélien. L'associativité est la partie la plus difficile.

Citons deux résultats fameux:

Thm (Mordell) k corps de nombres $\Rightarrow E(k)$ gr. ab. type fini

Thm (Hasse) k fini $\Rightarrow \#E(k) = q + 1 - a$

où $q = \#k$ et $|a| \leq 2\sqrt{q}$

Preuves: (cf. Silverman "Arithmetic of ell. curves", ou Tate, pour déno. pour réf.)

On suppose maintenant $k = K$ c.d.n. et E donnée sous forme de Weierstrass avec $a, b \in \mathcal{O}_K$.

Soit $\mathfrak{P}$ premier t.q. $\mathfrak{P} \nmid 2 \operatorname{disc} E$,

$\mathcal{O}_K$

$\Rightarrow E \bmod \mathfrak{P}$ c. ell sur $k_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$. $\#k_{\mathfrak{P}} = N\mathfrak{P}$

Hasse $\Rightarrow \#E(k_{\mathfrak{P}}) = \#k_{\mathfrak{P}} + 1 - a_{\mathfrak{P}}$. avec $|a_{\mathfrak{P}}| \leq 2\sqrt{\#k_{\mathfrak{P}}}$

Def: (Hasse, Weil) $$L(s, E) := \prod_{\mathfrak{P} \nmid 2 \operatorname{disc} E} \frac{1}{1 - a_{\mathfrak{P}} N\mathfrak{P}^{-s} + N\mathfrak{P}^{1-2s}}$$

(code "analytiquement" $a_{\mathfrak{P}}$ $\forall \mathfrak{P}$).

Hasse $1 - a_{\mathfrak{P}} X + NP X^2 = (1 - \alpha_{\mathfrak{P}} X)(1 - \beta_{\mathfrak{P}} X)$

$a_{\mathfrak{P}}^2 - 4NP < 0 \Rightarrow \beta_{\mathfrak{P}} = \overline{\alpha_{\mathfrak{P}}}$ et $|\alpha_{\mathfrak{P}}| = |\beta_{\mathfrak{P}}| = \sqrt{N\mathfrak{P}}$.

ex $\Rightarrow$ $L(s, E)$ cv. abs pour $\mathrm{Re}\, s > 3/2$

Conjectures i) (Hasse-Weil) $L(s, E)$ a un prol. hol. à $\mathbb{C}$ + eq. f. $s \to 2-s$ (convenablement complétée)

ii) (Birch Swinnerton-Dyer) ord$_{s=1} L(s, E) = \dim E(k) \otimes \mathbb{Q}$.

Cas connus : (1) (Wiles – B.C.D.T.) i) connu si $k = \mathbb{Q}$.
ils montrent "E modulaire", ce que l'on peut interpréter comme $L(s, E)$ et la fonction L d'une forme modulaire.

(2) "presque rien" n'est connu sur ii) (mais si $k = \mathbb{Q}$)
(de général...).
cas ord = 1 ou 0

(3) Deuring / Hecke : cas "CM" de i) connus.

IV) Esquisse de preuve du prolongement analytique de $L(s, E)$ pour $E : y^2 = x^3 - x$ / $\mathbb{Q}$ (Hecke, Deuring)

$\Delta_E = -4$. $p \neq 2$.

Lemme 1 $\#E(\mathbb{F}_p) = \begin{cases} p+1 & \text{si } p \equiv 3 \ (4) \\ p+1-\pi-\overline{\pi} & \text{si } p \equiv 1 \ (4) \\ & \text{où } \pi \in \mathbb{Z}[i] \text{ t.q. } \pi\overline{\pi} = p \\ & \text{et } \pi \equiv 1 \ (1+i)^3 \\ & \quad = -2i(1+i) \end{cases}$

(ex. conj de Gauss "last entry", prouvé par Herglotz en 1921)

Preuve • cas $p \equiv 3$ (4) exercice : $x \to -x$, $x^3 - x \to -(x^3 - x)$ et -1 non carré dans $\mathbb{Z}/p\mathbb{Z}$ donc. $\#E(\mathbb{F}_p) = 1 + 3 + \frac{1}{2}(p-3) \times 2$

1 ↗ 0 ; 3 ↗ $x^3 - x = 0$; $\frac{1}{2}(p-3) \times 2$ ↑ $x^3 - x \neq 0$.

Cas $p \equiv 1 (4)$ (esquisse) on se ramène à compter les points de la courbe plane $C := \{(u,v),\ u^2 = v^4 + 4\}$.

En effet, le changement de variables $\begin{cases} y = vx \\ 2x = u + v^2 \end{cases}$ montre que pour tout corps k, $2 \in k^\times$ on a $E(k) - \{O, (0;0;1)\} \xrightarrow{\sim} C(k)$. (exercice !)

$\# C(\mathbb{F}_p)$ se calcule par la méthode des sommes de Jacobi et conduit au résultat (cf. Ireland & Rosen ch. 18 §4)

Lemme 2 i) On a $1 - a_p X + p X^2 = \begin{cases} 1 - (-p) X^2 & \text{si } p \equiv 3 (4) \\ (1 - \pi X)(1 - \bar{\pi} X) & \text{si } p \equiv 1 (4) \end{cases}$ avec $\pi, \bar{\pi}$ comme dans le lemme 7

ii) $L(s, E) = \prod_{\substack{\pi \in \mathbb{Z}[i] \\ \pi \text{ irréd} \equiv 1 (1+i)^3}} \frac{1}{1 - N\bar{\pi}^s \pi} = \sum_{\substack{\pi \in \mathbb{Z}[i] \\ \pi \equiv 1 (1+i)^3}} \frac{\pi}{(N\pi)^s}$

Preuve : i) c'est le lemme 1 !

ii) c'est conséquence du i) et de la classif. bien connue des irréductibles de $\mathbb{Z}[i]$.

Lemme 3 i) La fonction $\vartheta : \mathbb{R}_{>0} \to \mathbb{C}$, définie par

$$\vartheta(t) = \sum_{\substack{z \in \mathbb{Z}[i] \\ z \equiv 1 (1+i)^3}} z\, e^{-\pi t |z|^2}$$

converge abs. $\forall t$ et vérifie $\vartheta(t) \sim_{t \to +\infty} e^{-\pi t}$

ii) On a $\pi^{-s} \Gamma(s) L(s, E) = \int_0^\infty \vartheta(t)\, t^s \frac{dt}{t}$

pour $\mathrm{Re}(s) > 3/2$.

Preuve i) exercice

ii) utilisera que pour $z \in \mathbb{C} - \{0\}$, on a pour $\mathrm{Re}(s) > 0$

$$\int_0^\infty e^{-\pi t |z|^2} t^s \frac{dt}{t} = \pi^{-s} |z|^{-2s} \Gamma(s)$$

$u = \pi t |z|^2$ ∎

Lemme 4 (Lemme clé) Soit $\lambda = (1+i)^3$. On a $|\lambda| = 8^{1/2}$ et la fonction $\underline{\vartheta}(t) := \vartheta(t/|\lambda|)$ vérifie

$$\underline{\vartheta}(t) = t^{-2} \underline{\vartheta}(1/t) \quad \forall t \in \mathbb{R}_{>0}$$

Lemme 4 $\Rightarrow$ Thm :

$$\pi^{-s} \Gamma(s) L(s, E) = \int_0^\infty \vartheta(t) t^s \frac{dt}{t} = |\lambda|^{-s} \int_0^\infty \underline{\vartheta}(t) t^s \frac{dt}{t}$$

$$= |\lambda|^{-s} \int_1^\infty \left(\underline{\vartheta}(t) t^s + \underline{\vartheta}\left(\tfrac{1}{t}\right) t^{-s} \right) \frac{dt}{t}$$

$\underline{\vartheta}(t) t^{2-s}$

cette expression converge $\forall s \in \mathbb{C}$. (plus de sing. en 0), holomorphe, et $|\lambda|^s \pi^{-s} \Gamma(s) L(s, E)$ invariante par $s \to 2-s$ ∎.

Preuve Lemme 4 Soit $t > 0$ réel.

On a $\vartheta(t) = \sum_{z \in \mathbb{Z}[i]} f(z)$ où $f : \mathbb{C} \to \mathbb{C}$ est la f.

$$f(z) = (1 + \lambda z) e^{-t\pi |1+\lambda z|^2}.$$

formule de Poisson : $\vartheta(t) = \sum_{z \in \mathbb{Z}[i]} \hat{f}(z)$

où $\hat{f}(w) := \int_{\mathbb{C}} f(z) e^{-2i\pi \mathrm{Re}\, z\bar{w}} \, dw.$

($\mathbb{C} \simeq \mathbb{R}^2$ $\mathrm{Re}\, z\bar{w} \Leftrightarrow$ prod. scalaire usuel

$1, i \to (1,0), (0,1)$ $\mathbb{Z}[i]$ autodual.

Exercice $\hat{f}(w) = -\frac{i}{|\lambda|^2 t^2}\,\frac{w}{\bar{\lambda}}\, e^{-\pi\frac{|w|^2}{t|\lambda|^2}}\, e^{2i\pi\, \mathrm{Re}\, \bar{w}/\lambda}$

Il faut ensuite étudier $\sum_{z\in\mathbb{Z}[i]} \hat{f}(z)$ et reconnaître $\frac{1}{|\lambda|^2 t^2}\,\vartheta(1/t|\lambda|^2)$

On ne détaille pas tous les calculs, mais disons simplement qu'il est commode d'introduire la fonction

$$\gamma : \mathbb{Z}[i] \longrightarrow \mathbb{C}$$
$$w \longmapsto -\frac{i}{\bar{\lambda}} \sum_{k=0}^{3} i^k\, e^{\frac{2i\pi}{8}\mathrm{Re}(w i^k \lambda)}$$

on observe alors les faits (faciles!) suivants :

- $\gamma(wi) = i^{-1}\gamma(w) \quad \forall\, w \in \mathbb{Z}[i]$
- $\gamma(w+\lambda z) = \gamma(w) \quad \forall\, w, z \in \mathbb{Z}[i]$
- $\gamma(1) = 1$ (calcul)

Comme le groupe $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ agissant sur $\mathbb{Z}[i]/(1+i)^3$ (anneau a 8 éléments) a 1 seule orbite libre, i.e. celle des inversibles, on en déduit $\gamma(w) = 0$ si $w \equiv 0\ (1+i)$

On réécrit ensuite $\sum_{z\in\mathbb{Z}[i]} \hat{f}(z)$ sous la forme

$$\frac{1}{|\lambda|^2 t^2} \sum_{w \equiv 1\,(\lambda)} \gamma(w)\, w\, e^{-\frac{\pi|w|^2}{t|\lambda|^2}} = \frac{1}{|\lambda|^2 t^2}\,\vartheta\left(\frac{1}{t|\lambda|^2}\right) \quad \blacksquare$$

V) Module de Tate d'une courbe elliptique

but : "montrer" que si k c.d.m. et E/k c.ell alors $L(s, E)$ est d'origine galoisienne ("à la Artin")

réf : Tate, Silverman

suite E/k c.ell et L/k ext. corps

$\mathbb{P}^2 \supset$ alors $\mathrm{Aut}_k L$ agit sur $\mathbb{P}^2(L)$ en préservant $E(L)$

$(\sigma(X:Y:Z) = (\sigma X : \sigma Y : \sigma Z)$: il agit par aut. de groupes

$\forall \sigma \in \mathrm{Aut}_k L$: $\sigma O = O$ et $\sigma(P+Q) = \sigma P + \sigma Q$ $\forall P, Q \in E(L)$

Thm | on suppose E/k avec k alg clos, $N \geq 1$ entier inversible dans k.

groupe $E(k)[N] = \{P \in E(k),\ \underbrace{P+P+\dots+P}_{N \text{ fois}} = O\}$ est $\simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^2$

(anal : $N = 2, 3 \dots$)

Preuve : cas particulier $k \hookrightarrow \mathbb{C}$.

$k = \mathbb{C}$ théorie de Weierstrass : $E(\mathbb{C})$ est isom à $\mathbb{C}/\Lambda$, où $\Lambda \subset \mathbb{C}$ réseau bien choisi, entraînant groupe analytique / $\mathbb{C}$.

$\Rightarrow E(\mathbb{C})[N] \simeq \frac{1}{N}\Lambda/\Lambda \simeq \left(\mathbb{Z}/N\mathbb{Z}\right)^2$

si $k \hookrightarrow \mathbb{C}$, $(*)$ $E(k)[N] \subset E(\mathbb{C})[N]$ sous-groupe

si $(x:y:1) \in E(\mathbb{C})[N]$ alors $(\sigma(x) : \sigma(y) : 1) \in E(\mathbb{C})[N]$

par la suite $\forall \sigma \in \mathrm{Aut}_k \mathbb{C} \Rightarrow \{\sigma(x),\ \sigma \in \mathrm{Aut}_k \mathbb{C}\}$ fini (idem avec y)

$\Rightarrow x \in \overline{k} = k$, et $y \in k$ aussi.

donc $(*)$ est une égalité ∎ (le cas des corps finis sera aussi utile dans la suite. On peut en fait se ramener aussi au cas $k \subset \mathbb{C}$ dans ce cas [illegible] la fin du cours)

module de Tate de E/k (k quelconque). $\bar{k} :=$ clôt alg (sép) de

$n \geq 1$, ℓ premier, on regarde

$$0 \to E[\bar{k}][\ell] \longrightarrow E[\bar{k}][\ell^{n+1}] \xrightarrow{\times \ell} E(\bar{k})[\ell^n]$$

thm $\Rightarrow$ $\times \ell$ surjective. On pose $\boxed{T_\ell(E) := \varprojlim_n E(\bar{k})[\ell^n]}$

$T_\ell(E) \simeq \mathbb{Z}_\ell^2$ comme gpe abelien + action $\mathbb{Z}_\ell$-linéaire (suite) de $Gal(\bar{k}/k)$

$\rightsquigarrow$ $\boxed{\rho_{E,\ell} : Gal(\bar{k}/k) \longrightarrow GL_2(\mathbb{Z}_\ell)}$ (unique conj. près).

C'est une "représentation ℓ-adique", elle connaît beaucoup de choses sur E/k, du moins si k de type fini / ss corps premier

<u>Thm</u>' (Hasse) k fini, $\det(X - \rho_{E,\ell}(\varphi)) = X^2 - aX + \# k$

$\hookrightarrow$ du thm. Hasse

$\varphi \in Gal(\bar{k}/k)$

Frob. : $x \to x^{\# k}$ (i.e $\det(1 - \rho_{E,\ell}(\varphi)) = \# E(k)$)

<u>Pour finir</u> $k = K$ est un corps de nombres.

Soit P idéal premier $|p$, on choisit $K_P \longrightarrow \overline{K_P}$, puis.

$\overset{\cap}{\mathcal{O}_K}$

on prolonge arbitrairement $K \longrightarrow K_P \to \overline{K_P}$

en $\bar{K} \longrightarrow \overline{K_P}$. Cela fournit un morphisme

de groupes $Gal(\overline{K_P}/K_P) \longrightarrow Gal(\bar{K}/K)$

(changer de choix $\Leftrightarrow$ conjuguer par $Gal(\bar{K}/K)$)

(exercice)

Thm: 2 Soit E/K c. ell, ℓ premier, $\mathfrak{P} \subset \mathcal{O}_K$ idéal premier.

Alors i) $\rho_{E,\ell} \mid \mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}}) \simeq \rho_{E_{K_{\mathfrak{P}}},\ell}$

↑ E vue comme c. ell $/K_{\mathfrak{P}}$

ii) si E est ss forme de Weierstrass avec $a, b \in \mathcal{O}_K$, et si $\mathfrak{P} \nmid 2\ell \,\mathrm{disc}\, E$, alors

$\rho_{E_{K_{\mathfrak{P}}},\ell}$ est triviale sur le sous-groupe d'inertie de $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}})$ (i.e $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_0)$ où K_0 est l'ext. non ram. max. de $K_{\mathfrak{P}}$ dans $\bar{K}_{\mathfrak{P}}$)

donc se factorise en une rep. de $\mathrm{Gal}(K_0/K_{\mathfrak{P}}) \simeq \mathrm{Gal}(\bar{k}_{\mathfrak{P}}/k_{\mathfrak{P}})$,

et en tant que telle, est isom. à $\rho_{\bar{E},\ell}$,

où $\bar{E} = E \bmod \mathfrak{P}$ (une c. ell / $k_{\mathfrak{P}}$).

Enoncé a rallongé.... il répond au but affiché, d'après Hasse:

si $\mathfrak{P} \times 2\ell \,\mathrm{disc}\, E$, $X^2 - a_{\mathfrak{P}} X + \mathrm{N}\mathfrak{P}$ est un pol. caractéristique de Frobenius, comme dans le cas d'Artin —

Preuves (esquisses : cf Tate, Silvermann)

i) est conséquence immédiate de la suite et du premier thm. (dans les cas démontrés) : on a $T_\ell(E) \xrightarrow{\sim} T_\ell(E_{K_{\mathfrak{P}}})$

(l'isom. étant induit par $\bar{K} \longrightarrow \bar{K}_{\mathfrak{P}}$, et donc commutant à $\mathrm{Gal}(\bar{K}_{\mathfrak{P}}/K_{\mathfrak{P}})$).

ii) plus délicat. On se ramène à l'énoncé suivant :

On dira qu'un groupe abélien A est "uniquement N-divisible" si $A \to A$, $x \mapsto Nx$, est bijective.

Prop: (cf: Tate) Soit F un corps complet pour une val. discrète, $\mathcal{O} \subset F$ l'anneau de val, $k = \mathcal{O}/\mathfrak{m}$ corps résiduel, E/F une c. ell. On suppose que E a un modèle de Weierstrass avec $a, b \in \mathcal{O}$ et $2\text{dis}\, E \in \mathcal{O}^\times$.

On note $\pi : \mathbb{P}^2(F) = \mathbb{P}^2(\mathcal{O}) \longrightarrow \mathbb{P}^2(k)$ l'application can. de réduction mod $\mathfrak{m}$. Alors

π induit un morphisme de groupe $E(F) = E(\mathcal{O}) \to \bar{E}(k)$, où $\bar{E}$ est la c. ell / k définie par réduction mod $\mathfrak{m}$ de E, et ce morphisme est : i) surjectif

ii) de noyau N-divisible $\forall N \in \mathcal{O}^\times$

Preuve i) Le fait que π induise un morph. de groupes $E(F) = E(\mathcal{O}) \to \bar{E}(k)$ est clair : toute droite de $\mathbb{P}^2_{/F}$ peut être choisie à coeff dans $\mathcal{O}$, l'un d'eux étant dans $\mathcal{O}^\times$.

ii) la surjectivité de π vient du fait que $\bar{E}$ est non singulière + lemme de Hensel (+ F complet !)

iii) plus subtile. On note $E_1 \subset E(\mathcal{O})$ le noyau de π.

$P = (x : y : 3) \in E_1 \Rightarrow$ OPS $y = 1$ puis $P = (x : 1 : 3)$, $x, 3 \in \mathfrak{m}$

on rappelle qu'alors $3 = x^3 + axz^2 + bz^3$

on montre que $E_1 \longrightarrow \mathfrak{m}$, $P \mapsto x$ bijection., et on définit la loi de groupe sur $\mathfrak{m}$

↳ induite par E : loi de groupe formel (cf Tate)

On vérifie notamment que la $\times N$ est de la forme

$$x \longmapsto Nx + f(x)x^2 \quad \text{avec} \quad f(x) \in \mathcal{O}[[x]]$$

mais une telle série formelle est inversible (pour la composition !) si $N \in \mathcal{O}^\times$, cqfd. ∎

Cor ① sous les hypothèses de la prop., pour tout $N \geq 1$ avec $N \in \mathcal{O}^\times$, on a $\pi : \quad E(F)[N] \xrightarrow{\sim} \bar{E}(k)[N]$.

preuve : exercice !

Autre Cor : on est maintenant en mesure de prouver le thm. I.1 dans le cas où $k = \bar{\mathbb{F}}_p$. En effet, soit $N \geq 1$ premier à p, $E / \bar{\mathbb{F}}_p$ une c. ell, $\mathcal{O}_0 := W(\bar{\mathbb{F}}_p)$ (vecteurs de Witt), $F_0 = \mathcal{O}_0[1/p]$.

$\mathcal{E} :=$ une courbe ell. arbitraire$/F_0$ ss forme de Weierstrass à coeff. dans $\mathcal{O}_0$ telle que $\bar{\mathcal{E}} = E$ (évidemment possible).

Soit F/F_0 finie telle que $\mathcal{E}(F)[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$
$\qquad = \mathcal{E}(\bar{F})[N]$

(existe car $\bar{F}_0$ se plonge dans $\mathbb{C}$!)

$\mathcal{O}$ = anneau de val. de F a pour corps résiduel $\bar{\mathbb{F}}_p$

(F/F_0 totalement nécessairement ramifiée)

$$\text{Prop (ou Cor ↑)} \Rightarrow \quad \mathcal{E}(F)[N] \xrightarrow{\sim} \bar{\mathcal{E}}(\bar{\mathbb{F}}_p)[N] = E(\bar{\mathbb{F}}_p)[N], \qquad \mathcal{E}(F)[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$$ ∎

Cor ② Soit F, $\mathcal{O}$ et E comme dans l'énoncé de la prop.
Soit $N \geq 1$ un entier $\in \mathcal{O}^\times$.
(On suppose F extension finie de $\mathbb{Q}_p$ si on veut)
soit F^{nr}/F une extension non ramifiée de F

choisie assez grosse de sorte que l'on ait $E(k_{F^{ur}})[N] = E(k_F)[N]$ (fini)

Alors
$$\begin{array}{ccc} E(F^{ur})[N] & \xrightarrow{\pi}_{\sim} & E(k_F)[N] \\ \downarrow \text{inclusion} & \nearrow \text{un isomorphisme} & \\ E(\bar{F})[N] & & \end{array}$$

preuve π isom $\Rightarrow E(F^{ur})[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$

thm 1 $\Rightarrow$ inclusion égalité, cqfd. ■

Cor: $\rho_{E,\ell}$ non ramifiée si $\ell \in \Theta^\times$, sous les mêmes hyp.

et $\rho_{E,\ell} \mid [redacted] \cdot Gal(F^{ur\,max}/F) \xrightarrow{\sim} \rho_{\bar{E},\ell}$:

Cela conclut la démonstration du thm 2.

CHAPITRE 2

Formes modulaires

Une forme modulaire est une fonction analytique sur le demi-plan de Poincaré vérifiant une condition de croissance à l'infini et qui se transforme de manière particulière sous l'action du groupe $\mathrm{SL}_2(\mathbb{Z})$. Nous les aborderons ici d'abord sous cet aspect, traditionnel, à la manière du livre de Serre. Comme nous le verrons, toute forme modulaire admet un développement de Fourier, dont les coefficients ont des rapports très surprenants avec l'arithmétique. De plus, lorsque l'on fixe leur *poids*, l'espace (vectoriel) des formes modulaires est de dimension finie. Cet énoncé de finitude est la source de nombreuses identités remarquables. On rapporte qu'à ce sujet Eichler aurait dit un jour que les formes modulaires constituent la 5ème opération de l'arithmétique (après l'addition, la soustraction, la multiplication et la division).

Il y a plusieurs autres points de vue importants sur la notion de forme modulaire. Comme nous le verrons, une forme modulaire peut aussi être vue comme une fonction sur l'espace des réseaux de $\mathbb{C}$, point de vue qui aura de nombreux avantage, notamment lorsque nous discuterons les opérateurs de Hecke. On aura alors a portée de main un troisième point de vue, le point de vue *groupe*, qui consiste à voir une forme modulaire comme une fonction sur $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$: c'est ce point de vue qui conduit à la notion de forme automorphe, qui fera l'objet de la suite du cours.

Références : Henri Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*,

Jean-Pierre Serre, *Cours d'arithmétique*,

Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*,

D. Zagier, *Elliptic modular forms and their applications*, dans *The 1, 2, 3 of modular forms*, Springer Universitext (2008).

1. Action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré et réseaux de $\mathbb{C}$

1.1. Homographies. Pour tout corps K, le groupe $\mathrm{GL}_2(K)$ agit naturellement sur K^2, et donc sur l'ensemble $\mathrm{P}^1(K)$ des droites vectorielles de ce dernier. On pose

$$\widehat{K} \quad = \quad K \coprod \{\infty\}.$$

Cet ensemble s'identifie à $\mathrm{P}^1(K)$ en envoyant tout élément $z \in K$ sur la droite engendrée par $\begin{pmatrix} z \\ 1 \end{pmatrix}$, et le symbole ∞ sur celle engendrée par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Par transport de structure, on en déduit une action de $\mathrm{GL}_2(K)$ sur $\widehat{K}$, que l'on notera $(g, z) \mapsto gz$.

Si g désigne l'élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(K)$, et si $z \in K$, on constate les égalités

$$g \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \begin{cases} (cz+d) \begin{pmatrix} \frac{az+b}{cz+d} \\ 1 \end{pmatrix} & \text{si } cz+d \neq 0, \\ (az+b) \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } cz+d = 0. \end{cases} \tag{1}$$

On retrouve la formule bien connue $gz = \frac{az+b}{cz+d}$ si $cz+d \neq 0$. Les bijections de $\widehat{K}$ de cette forme sont appelées *homographies*. Elles forment donc un sous-groupe de $\mathfrak{S}(\widehat{K})$ isomorphe à $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^\times$ (une application linéaire préservant toutes les droites étant une homothétie). Par exemple, on a pour $a \in K^\times$ et $b, z \in K$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} z = az+b \ \text{(homographies } \textit{affines}\text{)} \text{ et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z = -1/z \ (\textit{inversion}).$$

Pour utilisation future, mentionnons que l'élément $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(K)$ étant donné, l'application $z \mapsto cz+d, K \to K$, sera notée $\mathrm{j}(g,z)$. La formule (4) ci-dessus montre la relation dite de "cocycle" :

$$\mathrm{j}(gg', z) = \mathrm{j}(g, g'z)\mathrm{j}(g', z),$$

valable pour tout $g, g' \in \mathrm{GL}_2(K)$ et tout $z \in K$.

1.2. Demi-plan de Poincaré. Ces rappels s'appliquent à $K = \mathbb{C}$, auquel cas $\widehat{\mathbb{C}}$ n'est autre que la *sphère de Riemann*. Le sous-groupe $\mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ agit par restriction sur cette sphère, en préservant $\widehat{\mathbb{R}}$, ainsi donc son complémentaire $\mathbb{C} - \mathbb{R}$. Cet ouvert de $\mathbb{C}$ a deux composantes connexes, l'une d'elles étant l'ouvert

$$\mathbb{H} = \{\tau \in \mathbb{C}, \operatorname{Im} \tau > 0\},$$

appelé *demi-plan de Poincaré*, l'autre étant son conjugué complexe $\overline{\mathbb{H}}$. Si g est l'élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{GL}_2(\mathbb{R})$, et si $\tau \in \mathbb{C} - \mathbb{R}$, alors on a $c\tau + d \neq 0$ et on constate l'égalité

$$\operatorname{Im} g\tau = \det g \ \frac{\operatorname{Im} \tau}{|c\tau+d|^2}. \tag{2}$$

En particulier, l'action par homographies du groupe

$$\mathrm{GL}_2(\mathbb{R})^+ := \{g \in \mathrm{GL}_2(\mathbb{R}), \ \det g > 0\}$$

préserve le demi-plan de Poincaré. L'action des homographies de la forme $a\tau + b$ avec $a \in \mathbb{R}_{>0}$ et $b \in \mathbb{R}$, montre que cette action est transitive.

Ces homographies ont des propriétés géométriques remarquables, particulièrement lumineuses lorsqu'on les étudie du point de vue de la géométrie hyperbolique. Par exemple, notons $\mathcal{C}$ l'ensemble des parties de $\mathbb{H}$ qui sont soit de la forme $\operatorname{Re} \tau = a$ ("droites verticales"), soit un demi-cercle de centre dans $\mathbb{R}$ ("perpendiculaire à l'axe réel"). Deux points quelconques de $\mathbb{H}$ appartiennent manifestement à un, et un seul, élément de $\mathcal{C}$. Un fait géométrique important est que $\mathrm{GL}_2(\mathbb{R})^+$ préserve $\mathcal{C}$. Pour le voir, il suffit d'observer que les éléments de $\mathcal{C}$ sont exactement les parties non vides de $\mathbb{H}$ de la forme $\alpha + \beta \operatorname{Re} \tau + \gamma |\tau|^2 = 0$ avec $(\alpha, \beta, \gamma) \in \mathbb{R}^3 - \{0\}$. La vérification de l'assertion précédente est alors un simple exercice ; il suffit même de le vérifier

pour les homographies $\tau \mapsto \tau + \lambda$ et $\tau \mapsto -1/\tau$ (les éléments correspondant de $\mathrm{GL}_2(\mathbb{R})^+/\mathbb{R}_{>0}$ engendrant ce dernier), auquel cas c'est immédiat.

1.3. Action du sous-groupe $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$. Les éléments

$$\mathrm{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } \mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

sont dans le sous-groupe $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ de $\mathrm{GL}_2(\mathbb{R})^+$; ils joueront un rôle très important. On a déjà vu $\mathrm{S}\,\tau = -1/\tau$ et $\mathrm{T}\,\tau = \tau + 1$. On a aussi $\mathrm{S}^2 = -\mathrm{I}_2$ et $\mathrm{ST} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, ainsi donc que l'identité $(\mathrm{ST})^3 = -\mathrm{I}_2$, puis $\mathrm{S}\,i = i$ et $\mathrm{ST}\rho = -1/(\rho+1) = \rho$ où $\rho = e^{2i\pi/3}$. On pose

$$\mathcal{F} = \{\tau \in \mathbb{H},\ |\mathrm{Re}\,\tau| \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}.$$

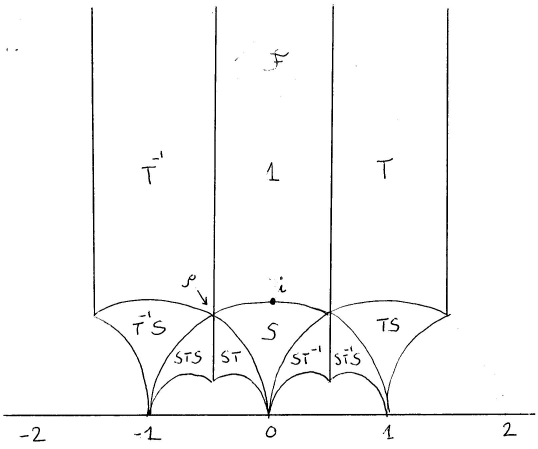


FIGURE 1. Le pavage de $\mathbb{H}$ par la Γ-orbite de $\mathcal{F}$

Théorème 2.1. *(i) Pour tout $\tau \in \mathbb{H}$, l'orbite $\Gamma\tau$ rencontre $\mathcal{F}$.*

(ii) Si τ et τ' sont deux points distincts de $\mathcal{F}$ tels que $\Gamma\tau = \Gamma\tau'$ alors :
- *soit* $\mathrm{Re}\,\tau = \pm\frac{1}{2}$ *et* $\tau' = \tau \pm 1$,
- *soit* $|\tau| = |\tau'| = 1$ *et* $\tau' = -1/\tau$.

(iii) Si $\tau \in \mathcal{F}$ alors le stabilisateur de τ dans Γ est $\{\pm 1\}$, sauf si $\tau = i$ (resp. $\tau = \rho, -\rho^2$), auquel cas c'est le sous-groupe engendré par S (*resp.* ST, TS).

DÉMONSTRATION — Soit $\tau \in \mathbb{H}$. La forme quadratique $\mathbb{R}^2 \to \mathbb{R}$, $(c,d) \mapsto |c\,\tau + d|^2$ est définie positive, elle admet donc un minimum sur $\mathbb{Z}^2 - \{0\}$. D'après la formule (2), il y a donc un sens à considérer l'ensemble $E \subset \Gamma\tau$ des éléments τ' tels que $\mathrm{Im}\,\tau'$ est maximal. Il est invariant par $\tau' \mapsto \tau' + 1$, de sorte qu'il existe $\tau' \in E$ tel que $|\mathrm{Re}\,\tau'| \leq \frac{1}{2}$. Mais $-1/\tau' \in \Gamma\tau$ et $\mathrm{Im}(-1/\tau') = \frac{\mathrm{Im}\tau'}{|\tau'|^2}$, donc $|\tau'| \geq 1$. Ainsi, $\tau' \in \Gamma\tau \cap \mathcal{F}$. Observons que cette démonstration montre en fait $G\tau \cap \mathcal{F} \neq \emptyset$ où G désigne le sous-groupe de Γ engendré par S et T.

Pour montrer (ii) et (iii), considérons $\tau, \tau' \in \mathcal{F}$ (non nécessairement distincts) tels que $\mathrm{Im}\,\tau' \geq \mathrm{Im}\,\tau$ et tels que $\tau' = \gamma\tau$ où

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

On a alors $|c\tau + d| \leq 1$. En particulier, $|c \operatorname{Im}\tau| \leq 1$ et donc $|c| \leq 1$. Si $c = 0$ alors $d = a = \pm 1$ et donc $\pm\gamma$ est une puissance de T et on est dans le premier cas du (ii). Sinon on peut supposer $c = 1$, quitte à remplacer γ par $-\gamma$. On voit sur le dessin que $|\tau + d| \leq 1$ entraîne $|\tau| = 1$, et que l'on est dans l'un des cas suivants :

1. $\tau \neq \rho, -\rho^2$ et $d = 0$. Dans ce cas, $b = -1$ et $\tau' = a - 1/\tau$ puis $a = 0$ car $|\mathrm{Re}(-1/\tau)| < 1/2$. Ainsi, $\gamma = \mathrm{S}$ et $\tau' = \tau = i$.

2. $\tau = \rho$ et $d = 0, -1$. Si $d = 0$ on a encore $b = -1$ et $\tau' = a - 1/\rho = a - \rho^2$. Cela montre que soit $\tau' = -\rho^2$, $a = 0$ et $\gamma = \pm\mathrm{S}$, soit $\tau' = \tau$, $a = -1$ et $\gamma = (\mathrm{ST})^2$.

3. Le cas $\tau = -\rho^2$ et $d = 0, 1$ se traite de manière similaire au cas 2. □

Soit δ l'ensemble des $\tau \in \mathcal{F}$ tels que l'on ait soit $\mathrm{Re}\,\tau = \frac{1}{2}$, soit $|\tau| = 1$ et $\mathrm{Re}\,\tau > 0$. Soit $\mathcal{F}' = \mathcal{F} - \delta$. Les points (i) et (ii) du théorème ci-dessus montrent que pour tout $\tau \in \mathcal{H}$, l'orbite $\Gamma\tau$ rencontre $\mathcal{F}'$ en un et un seul point. On dit aussi que $\mathcal{F}'$ est *un domaine fondamental* de l'action de Γ sur $\mathbb{H}$.

Corollaire 2.2. *Γ est engendré par* S *et* T.

Démonstration — Il ne serait pas difficile de démontrer ce corollaire de manière directe en utilisant des opérations sur les lignes et les colonnes. Déduisons-le plutôt du théorème. Soit G le sous-groupe de Γ engendré par S et T. Soit τ un point de l'intérieur de $\mathcal{F}$. Soit $\gamma \in \Gamma$. D'après la démonstration du (i) ci-dessus (dernière remarque), il existe $g \in G$ tel que $g^{-1}\gamma\tau \in \mathcal{F}$. Ainsi, $g^{-1}\gamma \in \mathrm{SL}_2(\mathbb{Z})$ fixe τ, c'est donc $\pm\mathrm{I}_2$ d'après le (iii). Au final, on a $\gamma \in G$ car $-\mathrm{I}_2 = \mathrm{S}^2 \in G$. □

2. Fonctions modulaires et fonctions de réseaux

2.1. Bases et réseaux de $\mathbb{C}$. (*Où l'on répète d'abord légèrement différemment ce que l'on a déjà dit...*) On note $\mathcal{B}$ l'ensemble des éléments de $\mathbb{C}^2$ de la forme $w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$ tels que $\{w_1, w_2\}$ est une base de $\mathbb{C}$ vu comme $\mathbb{R}$-espace vectoriel ; il est bien sûr équivalent de demander $w_2 \in \mathbb{C}^\times$ et $w_1/w_2 \notin \mathbb{R}$. On notera de plus $\mathcal{B}^+ \subset \mathcal{B}$ le sous-ensemble des bases w telles ques $\mathrm{Im}\ w_1/w_2 > 0$ (bases *directes*).

– L'action naturelle de $\mathbb{C}^\times$ sur $\mathbb{C}^2$ (par homothéties) préserve évidemment $\mathcal{B}$ et $\mathcal{B}^+$. Il est également évident que tout élément w de $\mathcal{B}$ s'écrit de manière unique sous la forme $\lambda \begin{pmatrix} \tau \\ 1 \end{pmatrix}$ avec $\lambda \in \mathbb{C}^\times$ et $\tau \in \mathbb{C} - \mathbb{R}$ (nécessairement $\lambda = w_2$, $z = w_1/w_2$). L'application $\tau \mapsto \begin{pmatrix} \tau \\ 1 \end{pmatrix}$ induit donc des bijections

$$\mathbb{C} - \mathbb{R} \xrightarrow{\sim} \mathbb{C}^\times\backslash\mathcal{B} \quad \text{et} \quad \mathbb{H} \xrightarrow{\sim} \mathbb{C}^\times\backslash\mathcal{B}^+. \tag{3}$$

– L'action naturelle de $\mathrm{GL}_2(\mathbb{R})$ sur $\mathbb{C}^2$ préserve $\mathcal{B}$: pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{GL}_2(\mathbb{R})$ on a (toujours) la (même) formule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} aw_1 + bw_2 \\ cw_2 + dw_2 \end{pmatrix} \tag{4}$$

Cela montre que cette action de $\mathrm{GL}_2(\mathbb{R})$ sur $\mathcal{B}$ est simplement transitive : pour $w, w' \in \mathcal{B}$ il existe un unique $g \in \mathrm{GL}_2(\mathbb{R})$ avec $w' = gw$. Le groupe $\mathrm{GL}_2(\mathbb{R})$ agit sur $\mathbb{C}^2$ en commutant avec l'action de $\mathbb{C}^\times$, et induit donc une action sur $\mathbb{C}^\times\backslash\mathcal{B} \xrightarrow{\sim} \mathbb{C} - \mathbb{R}$ qui n'est autre que celle étudiée au §1, par définition. La formule (2) montre que $g \in \mathrm{GL}_2(\mathbb{R})$ préserve $\mathcal{B}^+$ si, et seulement si, $g \in \mathrm{GL}_2(\mathbb{R})^+$.

Un *réseau de* $\mathbb{C}$ est par définition un sous-groupe engendré par une $\mathbb{R}$-base de $\mathbb{C}$. Si $w \in \mathcal{B}$, on notera $\mathrm{L}(w) := \mathbb{Z}w_1 + \mathbb{Z}w_2 \subset \mathbb{C}$ le réseau engendré. Si $\mathcal{R}$ désigne l'ensemble de tous les réseaux de $\mathbb{C}$, on a donc une surjection canonique

$$\mathcal{B} \longrightarrow \mathcal{R},\ w \mapsto \mathrm{L}(w). \tag{5}$$

Soient $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{GL}_2(\mathbb{R})$ et w dans $\mathcal{B}$. On a $\mathrm{L}(gw) \subset \mathrm{L}(w)$ si, et seulement si, $aw_1 + bw_2$ et $cw_1 + dw_2$ sont dans $\mathrm{L}(w)$. Il est équivalent de demander que a, b, c, d sont dans $\mathbb{Z}$, i.e. $g \in \mathrm{M}_2(\mathbb{Z})$. En particulier, $\mathrm{L}(gw) = \mathrm{L}(w)$ si, et seulement si, on a g et g^{-1} dans $\mathrm{M}_2(\mathbb{Z})$, i.e. $g \in \mathrm{GL}_2(\mathbb{Z})$. On a montré le (i) de la proposition suivante :

Proposition 2.3. *(i) L'application* (5) *induit une bijection* $\mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{B} \xrightarrow{\sim} \mathcal{R}$.
(ii) L'inclusion $\mathcal{B}^+ \to \mathcal{B}$ *induit une bijection* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{B}^+ \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{B}$.

Démonstration — La surjectivité de l'application du (ii) résulte de $\det \mathrm{GL}_2(\mathbb{Z}) = \{\pm 1\}$, et son injectivité de $\mathrm{SL}_2(\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{R})^+$. □

Le groupe $\mathbb{C}^\times$ agit naturellement sur $\mathcal{R}$ par homothéties : $(\lambda, L) \mapsto \lambda L$. La projection (5) est manifestement $\mathbb{C}^\times$-équivariante. En mettant bout-à-bout la bijection (3) et la proposition ci-dessus on en déduit le :

Corollaire 2.4. *L'application* $\tau \mapsto \tau\mathbb{Z} + \mathbb{Z}$ *induit une bijection* $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \xrightarrow{\sim} \mathbb{C}^\times\backslash\mathcal{R}$.

Étant donné que les classes d'homothétie de réseau de $\mathbb{C}$ sont en bijection naturelle avec les classes d'isomorphisme de tores complexes de dimension 1, i.e. de courbes elliptiques complexes, on dit aussi que $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ s'identifie à l'espace des modules grossiers de courbes elliptiques. C'est le point de départ de nombreuses constructions en géométrie algébrique, mais qui ne seront pas abordées dans ce cours.

2.2. Fonctions modulaires de poids χ. Notons $\mathcal{F}(X)$ l'espace vectoriel des fonctions de l'ensemble X dans $\mathbb{C}$. Fixons un morphisme de groupes $\chi : \mathbb{C}^\times \to \mathbb{C}^\times$ et notons $\mathcal{F}_\chi(\mathcal{B}^+) \subset \mathcal{F}(\mathcal{B}^+)$ le sous-espace des fonctions vérifiant $F(\lambda w) = \chi(\lambda)F(w)$ pour tout $\lambda \in \mathbb{C}^\times$ et toute base directe $w \in \mathcal{B}^+$. L'application linéaire

$$\mathcal{F}_\chi(\mathcal{B}^+) \longrightarrow \mathcal{F}(\mathbb{H}), F \mapsto (\tau \mapsto F(\begin{pmatrix} \tau \\ 1 \end{pmatrix}), \tag{6}$$

est évidement bijective, toute base directe s'écrivant de manière unique sous la forme $\lambda\begin{pmatrix} \tau \\ 1 \end{pmatrix}$ avec $\lambda \in \mathbb{C}^\times$ et $\tau \in \mathbb{H}$. Si f est une fonction sur $\mathbb{H}$, on notera $f^\chi \in \mathcal{F}_\chi(\mathcal{B}^+)$ son unique antécédent par cette application.

Le groupe $\mathrm{GL}_2(\mathbb{R})^+$ agit à droite, par translations à gauche !, sur $\mathcal{F}(\mathcal{B}^+) : (g, F)(w) = F(gw)$. Cette action présèrve manifestement $\mathcal{F}_\chi(\mathcal{B}^+)$. Il en résulte une action, également à droite, de $\mathrm{GL}_2(\mathbb{R})^+$ sur $\mathcal{F}(\mathbb{H})$ (dépendant de χ), définie par transport de

structure au moyen de la bijection (6). Cette action est appelée *action de poids* χ de $\mathrm{GL}_2(\mathbb{R})^+$ sur $\mathcal{F}(\mathbb{H})$, et elle est notée $(g,f)\mapsto f_{|\chi}g$. Par définition, elle est donnée par la formule suivante,

$$(f_{|\chi}g)(\tau) := f^\chi(g\begin{pmatrix}\tau\\1\end{pmatrix}) = \chi(c\tau+b)\,f(\frac{a\tau+b}{c\tau+d}) = \chi(\mathrm{j}(g,\tau))f(g\tau). \tag{7}$$

Proposition-Définition 2.5. *Soient $\chi:\mathbb{C}^\times\to\mathbb{C}^\times$ un morphisme de groupes et $f:\mathbb{H}\to\mathbb{C}$ une fonction. Les propriétés suivantes sont équivalentes :*

(i) $f(\frac{a\tau+b}{c\tau+d}) = \chi(c\tau+d)^{-1}f(\tau)$ pour tout τ dans $\mathbb{H}$ et tout $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$,

(ii) $f_{|\chi}\gamma = f$ pour tout $\gamma\in\mathrm{SL}_2(\mathbb{Z})$,

(iii) $f(\tau+1)=f(\tau)$ et $f(-1/\tau)=\chi(\tau)^{-1}f(\tau)$ pour tout $\tau\in\mathbb{H}$,

(iv) $f^\chi:\mathcal{B}^+\to\mathbb{C}$ est invariante par $\mathrm{SL}_2(\mathbb{Z})$,

(v) f^χ se factorise en une fonction $\mathcal{R}\to\mathbb{C}$.

Si elles sont satisfaites, on dit que f est une fonction modulaire de poids χ.

Démonstration — L'équivalence de (i) et (ii) est tautologique. Celle de (ii) et (iii) découle du fait que l'action de poids χ est une action de groupes, et que $\mathrm{SL}_2(\mathbb{Z})$ est engendré par S et T, de sorte que (ii) est équivalent à demander $f_{|\chi}\mathrm{T}=f$ et $f_{|\chi}\mathrm{S}=f$, qui sont les deux équations données. L'équivalence entre (iv) et (ii) est tautologique, par définition de l'action de poids χ (ou par la formule (7)). L'équivalence entre (iv) et (v) est la Proposition 2.3. □

Définition 2.6. *Une* fonction de réseaux de poids χ *une fonction $F:\mathcal{R}\to\mathbb{C}$ telle que $F(\lambda L)=\chi(\lambda)F(L)$ pour tout $\lambda\in\mathbb{C}^*$ et tout $L\in\mathcal{R}$.*

Corollaire 2.7. *Les applications $f\mapsto f^\chi$ et $F\mapsto(\tau\mapsto F(\tau\mathbb{Z}+\mathbb{Z}))$ sont des bijections réciproques entre l'espace des fonctions modulaires de poids χ et celui des fonctions de réseaux de poids χ.*

Remarque 2.8. Pour alléger les notations, on pourra noter par le même symbole une fonction modulaire f de poids χ, la fonction $f^\chi:\mathcal{B}^+\to\mathbb{C}$ correspondante, et la fonction de réseaux $\mathcal{R}\to\mathbb{C}$ qui s'en déduit. Il ne peut en principe y avoir d'ambiguité d'interprétation, puisque les arguments dans chacun des cas sont des objets mathématiques bien différents (un élément de $\mathbb{H}$, un élément de $\mathcal{B}^+$, ou un élément de $\mathcal{R}$).

Les caractères continus $\chi:\mathbb{C}^\times\to\mathbb{C}^\times$ joueront par la suite un rôle naturellement plus important. Ceux sont ceux de la forme $\lambda\mapsto\lambda^k|\lambda|^s$, avec $k\in\mathbb{Z}$ et $s\in\mathbb{C}$ (exercice !). Lorsque χ est le caractère $\lambda\mapsto\lambda^{-k}$ (noter le signe $-$), où $k\in\mathbb{Z}$ est fixé, on utilisera l'expression *de poids k* à la place de *poids χ*, et l'on note traditionnellement $f_{|k}g$ pour $f_{|\chi}g$. Par exemple, une fonction modulaire de poids 0 (i.e. de poids $\chi=1$) est simplement une fonction sur $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

Exemple 2.9. *Soient $k \in \mathbb{Z}$ et $s \in \mathbb{C}$ tels que $k + \mathrm{Re}\, s > 2$. La série d'Eisenstein*

$$\mathrm{G}_{k;s}(L) = \sum_{\lambda \in \mathrm{L} - \{0\}} \frac{1}{\lambda^k |\lambda|^s}$$

est absolument convergente, et définit une fonction modulaire de poids $\lambda \mapsto \lambda^{-k}|\lambda|^{-s}$. Vue comme fonction de $\tau \in \mathbb{H}$, on a $\mathrm{G}_{k;s}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2-\{0\}} \frac{1}{(n\tau+m)^k |n\tau+m|^s}$.

L'assertion de convergence absolue de $\mathrm{G}_{k;s}(L)$ sera justifiée en détail un peu plus loin. Le reste s'en déduit immédiatement.

Exemple 2.10. *La fonction* covol : $\mathcal{R} \to \mathbb{R}_{>0}$, *où* $\mathrm{covol}(L)$ *désigne le covolume du réseau L étant pris disons dans la $\mathbb{R}$-base $1, i$, est modulaire de poids $\lambda \mapsto |\lambda|^2$. Comme fonction sur $\mathcal{B}$, c'est $w \mapsto |\det_{i,1}(w_1, w_2)|$. Comme fonction sur $\mathbb{H}$, c'est la fonction $\tau \mapsto |\det \begin{bmatrix} \mathrm{Im}\,\tau & 0 \\ \mathrm{Re}\tau & \mathrm{Im}\tau \end{bmatrix}| = \mathrm{Im}\,\tau$ (c'est aussi ce qui dit la formule (2) !).*

Exemple 2.11. *Si f est (une fonction) modulaire de poids χ, et si f' est modulaire de poids χ', alors ff' est modulaire de poids $\chi\chi'$. De plus, $|f|$ est modulaire de poids $|\chi|$. Si $|\chi|$ est le caractère $\lambda \mapsto |\lambda|^{-s}$ avec $s \in \mathbb{R}$, alors $|f| \cdot \mathrm{covol}^{s/2}$ est modulaire de poids 0, i.e. $|f(\tau)|(\mathrm{Im}\,\tau)^{s/2}$ définit une fonction $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{R}_{\geq 0}$.*

3. Formes modulaires

Notons $\mathcal{O}(\mathbb{H}) \subset \mathcal{F}(\mathbb{H})$ le sous-espace des fonctions holomorphes. Si $k \in \mathbb{Z}$, l'action de poids k de $\mathrm{GL}_2(\mathbb{R})^+$ sur $\mathcal{F}(\mathbb{H})$ préserve manifestement $\mathcal{O}(\mathbb{H})$.

Définition 2.12. *Une* forme modulaire de poids $k \in \mathbb{Z}$ *est une fonction $f : \mathbb{H} \to \mathbb{C}$ qui est une fonction modulaire de poids*[1] *k, telle que :*

(i) f est holomorphe,

(ii) $f(\tau)$ admet une limite finie quand $\mathrm{Im}\ \tau \longrightarrow +\infty$, *notée $f(\infty)$.*

L'ensemble des formes modulaires de poids k est un sous-espace de $\mathcal{O}(\mathbb{H})$. Suivant Serre, nous le noterons M_k. La relation $f_{|_k} - \mathrm{I}_2 = (-1)^k f$ montre que si $f \in \mathrm{M}_k$ alors $f = (-1)^k f$, de sorte que $\mathrm{M}_k = 0$ si k est impair. Les fonctions constantes sont modulaires de poids 0 : nous verrons plus loin que ce sont les seules. Un premier exemple intéressant de forme modulaire est donné par les *séries d'Eisenstein* (Exemple 2.9), vues ici comme fonction de τ. Si k est un entier ≥ 3, on pose $\mathrm{G}_k = \mathrm{G}_{k;0}$.

Proposition 2.13. *On suppose que k est pair ≥ 4. Alors on a $\mathrm{G}_k \in \mathrm{M}_k$ et $\mathrm{G}_k(\infty) = 2\zeta(k)$. En particulier $\mathrm{G}_k \neq 0$.*

Démonstration — Fixons $A, B \in \mathbb{R}_{>0}$ et notons $\mathcal{D}_{A,B}$ l'ensemble des $\tau \in \mathbb{H}$ tels que $\mathrm{Im}\ \tau > A$ et $|\mathrm{Re}\,\tau| < B$. Vérifions qu'il existe un réel $C > 0$ tel que pour tout $(\mu, \nu) \in \mathbb{R}^2$ et tout $\tau \in \mathcal{D}_{A,B}$ alors

$$|\mu\tau + \nu| \geq C\ \sup(|\mu|, |\nu|).$$

1. ... ce qui signifie donc que l'on a $f(\frac{a\tau+b}{c\tau+d}) = (c\tau + d)^k f(\tau)$ pour tout τ dans $\mathbb{H}$ et tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$.

Soient $\tau \in \mathcal{D}_{A,B}$ et $(\mu,\nu) \in \mathbb{R}^2$. D'une part, on a $|\mu\tau+\nu| \geq |\mathrm{Im}\,(\mu\tau+\nu)| > A|\mu|$. D'autre part, on constate sur un dessin qu'il existe $\delta > 0$ tel que $|\lambda\tau+1| > \delta$ pour tout $\lambda \in \mathbb{R}$ et tout $\tau \in \mathcal{D}_{A,B}$. Ainsi, pour $\nu \neq 0$ on a $|\mu\tau+\nu| = |\nu||\frac{\mu}{\nu}\tau+1| \geq \delta|\nu|$. En conclusion, $C = \mathrm{Min}(A,\delta)$ convient.

Si $s \geq 1$, il y a exactement $4\cdot 2s = 8s$ couples $(m,n) \in \mathbb{Z}^2$ tels que $\sup(|m|,|n|) = s$. On en déduit la majoration

$$\sum_{(m,n)\in\mathbb{Z}^2-\{0\}} \frac{1}{|m\tau+n|^k} \leq \frac{1}{C^k}\sum_{s\geq 1}\frac{8s}{s^k}$$

pour tout $\tau \in \mathcal{D}_{A,B}$. Ainsi, la série de l'énoncé est normalement convergente sur $\mathcal{D}_{A,B}$. En particulier, $\mathrm{G}_k(\tau)$ est une fonction holomorphe de τ. Nous avons déjà justifié dans l'exemple 2.9 que la convergence absolue de la série définissant G_k implique sa modularité de poids k. On peut le re-justifier directement : les bijections $(m,n) \mapsto (m,n+m)$ et $(m,n) \mapsto (n,-m)$ de $\mathbb{Z}^2-\{0\}$ entraînent les identités $\mathrm{G}_k(\tau+1) = \mathrm{G}_k(\tau)$ et $\mathrm{G}_k(-1/\tau) = \tau^k\mathrm{G}_k(\tau)$ pour tout $\tau \in \mathbb{H}$.

Enfin, faisons tendre $\mathrm{Im}\,\tau$ vers l'infini quand $\tau \in \mathcal{D}_{1,1}$. La fonction $\tau \mapsto \frac{1}{(m\tau+n)^k}$ tend vers $\frac{1}{n^k}$ ou 0 selon que $m = 0$ ou non. Par convergence uniforme de G_k sur $\mathcal{D}_{1,1}$, on peut intervertir limite et sommation et l'on obtient que $\mathrm{G}_k(\tau) \to 2\zeta(k)$. On conclut par 1-périodicité de G_k. □

Si $k \geq 4$ est pair, on pose $\mathrm{E}_k = \frac{1}{2\zeta(k)}\mathrm{G}_k \in \mathrm{M}_k$ (série d'Eisenstein "normalisée"), de sorte que l'on ait $\mathrm{E}_k(\infty) = 1$. Bien entendu, cette définition a un sens puisque $\zeta(k) \neq 0$. L'application $\mathrm{M}_k \to \mathbb{C}$, $f \mapsto f(\infty)$, est une application linéaire. Son noyau, noté S_k, est le sous-espace des formes modulaires *paraboliques* ("cuspidal" en anglais). Si $k \geq 4$, il est donc engendré par les éléments de la forme $f - f(\infty)\mathrm{E}_k$.

Corollaire 2.14. *Pour tout entier pair $k \geq 4$, on a $\mathrm{M}_k = \mathrm{S}_k \oplus \mathbb{C}\,\mathrm{E}_k$.*

4. q-développement d'une forme modulaire

Observons que si $z \in \mathbb{C}$ alors $|e^{2i\pi z}| = e^{-2\pi \mathrm{Im} z}$. Soit $\mathrm{D} = \{z \in \mathbb{C},\ |z| < 1\}$. On considère l'application

$$\mathrm{q} : \mathbb{H} \longrightarrow \mathrm{D} - \{0\},\ \ \tau \mapsto e^{2i\pi\tau}.$$

Cette application induit une bijection $\langle \mathrm{T}\rangle\backslash\mathbb{H} \xrightarrow{\sim} \mathrm{D}-\{0\}$. Autrement dit, si $f : \mathbb{H} \to \mathbb{C}$ est telle que $f(\tau+1) = f(\tau)$, il existe une unique fonction $\widetilde{f} : \mathrm{D}-\{0\} \to \mathbb{C}$ telle que $f(\tau) = \widetilde{f}(\mathrm{q})$.

Soit $f : \mathbb{H} \to \mathbb{C}$ telle que $f(\tau+1) = f(\tau)$. Observons que f est une fonction holomorphe si, et seulement si, $\widetilde{f}$ est une fonction holomorphe sur $\mathrm{D}-\{0\}$. En effet, pour tout $\tau_0 \in \mathbb{H}$, l'application q induit une bijection bi-holomorphe entre le voisinage ouvert $\{\tau \in \mathbb{H},\ |\mathrm{Re}(\tau-\tau_0)\,| < 1/2\}$ de τ_0 dans $\mathbb{H}$, et le voisinage ouvert $\mathrm{D} - \mathbb{R}_{\leq 0}\, e^{2i\pi\tau_0}$ de $e^{2i\pi\tau_0}$ dans D (un inverse s'obtient en considérant une branche du logarithme complexe). Si f est holomorphe il y a donc équivalence entre :

– $f(\tau)$ admet une limite quand $\mathrm{Im}\,\tau \longrightarrow \infty$,

– $|f(\tau)|$ est bornée sur $\{\tau \in \mathbb{H},\ \mathrm{Im}\,\tau > 1\}$,

– $|\widetilde{f(q)}|$ est bornée au voisinage de $q = 0$,

– $\widetilde{f}$ se prolonge en une fonction holomorphe sur tout D,

– $\widetilde{f}$ admet un développement en série entière en 0 de rayon de convergence ≥ 1.

(L'implication assertion 3 $\Rightarrow$ assertion 4 est le lemme de prolongement de Riemann). Cela justifie à la proposition-définition suivante.

Proposition-Définition 2.15. *Soit $f \in \mathrm{M}_k$. La forme f admet un unique développement*

$$f(\tau) = \sum_{n \geq 0} \mathrm{a}_n(f)\ \mathrm{q}^n,$$

avec $\mathrm{a}_n(f) \in \mathbb{C}$ pour tout entier $n \geq 0$, normalement convergent sur toute partie de $\mathbb{H}$ de la forme $\mathrm{Im}\,\tau > A$, $A \in \mathbb{R}_{>0}$. Ce développement est appelé développement de Fourier*, ou* q*-développement, de la forme f, et les $\mathrm{a}_n(f)$ sont ses* coefficients de Fourier*. On a $\mathrm{a}_0(f) = f(\infty)$.*

Comme nous le verrons, et de manière un peu surprenante, la suite des coefficients de Fourier de chaque forme modulaire est en général d'un intérêt arithmétique considérable.

5. Détermination de l'espace M_k

5.1. Un théorème de structure. Observons que si $f \in \mathrm{M}_k$ et $g \in \mathrm{M}_{k'}$ alors $fg \in \mathrm{M}_{k+k'}$. On peut donc fabriquer tout un tas de formes modulaires à l'aide des séries d'Eisenstein. Par exemple, si r et s sont des entiers ≥ 0 alors $\mathrm{E}_4^r\mathrm{E}_6^s \in \mathrm{M}_{4r+6s}$.

Théorème 2.16. *Soit $k \in \mathbb{Z}$. L'espace M_k admet pour base les $\mathrm{E}_4^r\mathrm{E}_6^s$, avec $(r, s) \in \mathbb{N}^2$ vérifiant $4r + 6s = k$.*

(La finitude même de $\dim \mathrm{M}_k$ est assez surprenante !)

Observons d'abord que si $f \in \mathrm{M}_k$ alors $f(i) = f_{|k}\mathrm{S}\ (i) = i^{-k}f(i)$. Ainsi, $f(i) = 0$ si $k \not\equiv 0 \bmod 4$. De même $f(\rho) = 0$ si $k \not\equiv 0 \bmod 6$. En particulier, $\mathrm{E}_6(i) = 0$ et $\mathrm{E}_4(\rho) = 0$. Nous démontrerons $\mathrm{E}_4(i) \neq 0$ dans la section suivante (pouvez-vous le démontrer directement ?) et que la famille de l'énoncé est génératrice : admettons-le pour l'instant. Vérifions ici qu'elle est libre. On procède par récurrence sur $k \geq 0$, le cas $k = 0$ étant trivial. Supposons donc pour $k \geq 0$ donné que l'on ait une relation de dépendance linéaire

$$\sum_{4r+6s=k} \lambda_{r,s}\mathrm{E}_4^r\mathrm{E}_6^s = 0.$$

Si k est multiple de 4, l'évaluation en $\tau = i$ de cette formule donne $\lambda_{k/4,0} = 0$ (car on a $\mathrm{E}_4(i) \neq 0$). Dans tous les cas, on a donc "$\lambda_{r,s} \neq 0$ implique $s \neq 0$". Ainsi, soit tous les $\lambda_{r,s}$ sont nuls, soit on a $k \geq 6$ et on peut simplifier l'égalité ci-dessus par E_6 (l'anneau des fonctions holomorphes sur $\mathbb{H}$ étant intègre...), puis conclure par récurrence sur k.□

Définition 2.17. *(Fonction Δ de Jacobi) La fonction $\Delta = \frac{1}{1728}(\mathrm{E}_4^3 - \mathrm{E}_6^2)$ est une forme modulaire parabolique de poids* 12*.*

L'apparition du facteur 1728 sera expliquée plus loin. D'après ce que nous avons dit ci-dessus, $\Delta \neq 0$ car $\Delta(i) = \frac{1}{1728}\mathrm{E}_4(i)^3$.

5.2. Sur les zéros des formes modulaires. Soient $f \in \mathrm{M}_k$ et $P \in \mathbb{H}$. On note $\mathrm{v}_P(f)$ l'ordre d'annulation de f au point P et e_P le cardinal du stabilisateur de P dans $\mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{I}_2\}$. Ces deux quantités, des entiers ≥ 0, ne dépendent que de la Γ-orbite de P (pour $\mathrm{v}_P(f)$, cela vient de la non annulation des $\mathrm{j}(\gamma, \tau)$ quand $\gamma \in \Gamma$ et $\tau \in \mathbb{H}$). De plus, d'après le Théorème 2.1 (iii) on a $\mathrm{e}_i = 2$, $\mathrm{e}_\rho = 3$, et si P n'est pas dans l'orbite de i ou ρ alors $\mathrm{e}_P = 1$. On note aussi $\mathrm{v}_\infty(f)$ l'ordre d'annulation de $\widetilde{f}$ en 0.

Proposition 2.18. (Formule $k/12$) *Soient $k \in \mathbb{Z}$ et $f \in \mathrm{M}_k$ non nulle. On a la relation*

$$\mathrm{v}_\infty(f) + \sum_{P \in \Gamma \backslash \mathbb{H}} \frac{\mathrm{v}_P(f)}{\mathrm{e}_P} = \frac{k}{12}.$$

Il fait partie de l'énoncé que la somme de gauche est en fait une somme finie (nécessairement ≥ 0). Le lecteur préférant voir d'abord comment utiliser cette formule, et par exemple terminer la démonstration du théorème 2.16, peut commencer par lire la sous-section suivante.

Démonstration — Soit $f \in \mathrm{M}_k$ non nulle. Rappelons que la Γ-orbite de tout zéro de f rencontre le domaine $\mathcal{F}$. Si r est un réel > 0 posons $\Omega_r = \{\tau \in \mathbb{H}, \mathrm{Im}\, \tau > r\}$. La fonction $\widetilde{f}$ étant holomorphe en 0, il existe $r > 0$ tel que f n'admet pas de zéro dans Ω_r. La partie $\mathcal{F} - \Omega_r$ étant compacte, la fonction holomorphe f n'y admet qu'un nombre fini de zéros (qui sont isolés). Cela montre que le nombre des Γ-orbites de points constituées de zéros de f est fini (et donc que la somme apparaissant dans la formule $k/12$ a tous ses termes nuls sauf au plus un nombre fini d'entre eux).

Considérons le contour $\mathcal{C}$ indiqué par la figure 2. Sur cette figure, les zéros éventuels de f qui sont dans $\partial\mathcal{F} - \{i, \rho, -\rho^2\}$ et de partie réelle $1/2$ (resp. de module 1) sont notés λ (resp. μ). En particulier, ce contour ne contient aucun zéro de f. On suppose que chaque portion de cercle dessinée est de rayon suffisamment petit de sorte que le disque bordé ne contienne que le point indiqué pour éventuel zéro (i.e $i, \rho, -\rho^2$, l'un des $\lambda, \lambda + 1$, ou l'un des $\mu, -1/\mu$). Nous noterons γ_{XY} le chemin portion de $\mathcal{C}$ allant de X à Y (dans ce sens). Le chemin $\gamma_{D'E}$ est par définition le chemin $\mathrm{T}\,\gamma_{AB}^{\mathrm{opp}}$. De même, on a choisi $\gamma_{C'D} = \mathrm{S}\,\gamma_{B'C}^{\mathrm{opp}}$. Enfin, on suppose que γ_{EA} est de partie imaginaire r suffisamment grande de sorte qu'aucun zéro de f ne soit de partie imaginaire $> r$. L'existence d'un tel contour est justifiée par le paragraphe précédent (zéros isolés).

La formule des résidus appliquée à la 1-forme méromorphe $\frac{\mathrm{d}f}{f} = \frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau$ s'écrit donc

$$\frac{1}{2i\pi} \int_{\mathcal{C}} \frac{f'(\tau)}{f(\tau)} \mathrm{d}\tau = \sum_P \mathrm{v}_P(f)$$

la somme portant sur les Γ-orbites de zéros de f ne contenant ni i ni ρ. Examinons maintenant les contributions des diverses portions du contour. Les fonctions f et f' étant T-invariantes on observe d'abord

$$\int_{\gamma_{AB}} \frac{f'(\tau)}{f(\tau)} \mathrm{d}\tau = \int_{\mathrm{T}\,\gamma_{AB}} \frac{f'(\tau)}{f(\tau)} \mathrm{d}\tau = -\int_{\gamma_{D'E}} \frac{f'(\tau)}{f(\tau)} \mathrm{d}\tau.$$

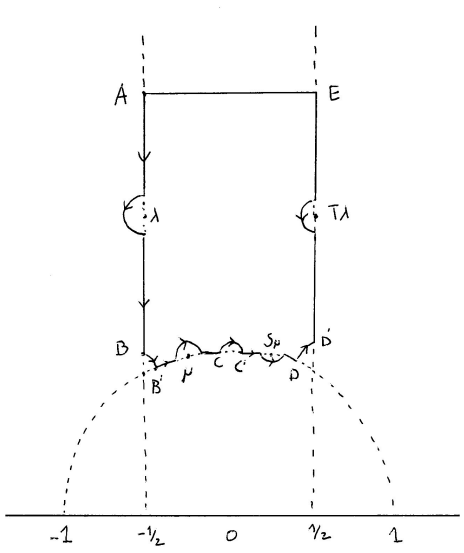


FIGURE 2. Le chemin d'intégration dans la démonstration de la formule $k/12$

Le chemin $\omega(t) := e^{2i\pi\gamma_{EA}(t)}$ est un cercle de centre 0 dans D faisant un tour dans le sens indirect. On a alors

$$\frac{1}{2i\pi}\int_{\gamma_{EA}}\frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau = \frac{1}{2i\pi}\int_{\omega}\frac{\widetilde{f}'(q)}{\widetilde{f}(q)}\mathrm{d}q = -\mathrm{v}_\infty(f).$$

En effet, la première égalité est un simple changement de variables (réelles !), et la seconde est le théorème des résidus appliqué à $\widetilde{f}$, sachant que par hypothèse 0 est le seul zéro éventuel de $\widetilde{f}$ dans le disque de D bordé par ω. De plus, par modularité de f on a $\frac{f'}{f} = -\frac{k}{\tau} + \frac{(f\circ S)'}{f\circ S}$, de sorte que

$$\frac{1}{2i\pi}\int_{\gamma_{B'C}}\frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau = -\frac{1}{2i\pi}\int_{\gamma_{B'C}}\frac{k}{\tau}\mathrm{d}\tau + \frac{1}{2i\pi}\int_{\mathrm{S}\,\gamma_{B'C}}\frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau,$$

avec rappelons-le $\mathrm{S}\,\gamma_{B'C} = \gamma_{C'D}^{\mathrm{opp}}$. Lorsque le point B' tend vers ρ, C tend vers i, et lorsque les portions de cercles autour des points notés μ sont de rayon tendant vers 0, alors l'intégrale de chemin $\frac{1}{i}\int_{\gamma_{B'C}}\frac{\mathrm{d}\tau}{\tau}$ tends vers l'angle orienté défini par ρ, 0 et i, i.e. $-(\frac{2\pi}{3} - \frac{2\pi}{4}) = -\frac{\pi}{6}$. De même, lorsque B et B' tendent vers ρ alors l'intégrale de chemin $\frac{1}{i}\int_{\gamma_{BB'}}\frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau$ tend vers l'angle orienté $\widehat{B\,\rho\,B'} = -\frac{\pi}{3}$ multiplié par $\mathrm{v}_\rho(f)$. Un argument similaire vaut en $-1/\overline{\rho} = \rho + 1$. Enfin, lorsque C et C' tendent vers i alors l'intégrale de chemin $\frac{1}{i}\int_{\gamma_{CC'}}\frac{f'(\tau)}{f(\tau)}\mathrm{d}\tau$ tend vers $-\pi\mathrm{v}_i(f)$. On conclut en mettant toutes ces identités bout à bout. □

5.3. Conséquences de la formule $k/12$. La première conséquence évidente de la formule $k/12$ est l'annulation $\mathrm{M}_k = 0$ si $k < 0$. De plus, on a $\mathrm{S}_k = 0$ si $k < 12$, car $\mathrm{v}_\infty(f) \geq 1$ si $f \in \mathrm{S}_k - \{0\}$. En particulier, on a donc $\mathrm{M}_0 = \mathbb{C}\,1$ (les constantes).

Séparant les orbites de i et ρ des autres, la formule $k/12$ s'écrit aussi

$$\mathrm{v}_\infty(f) + \frac{1}{2}\mathrm{v}_i(f) + \frac{1}{3}\mathrm{v}_\rho(f) + \sum_P \mathrm{v}_P(f) = \frac{k}{12}, \tag{8}$$

la somme portant sur les Γ-orbites de points de $\mathbb{H}$ distinctes de Γi et $\Gamma\rho$. En particulier on a $\mathrm{M}_2 = 0$ car chaque terme de gauche est soit $> 1/6$, soit nul. On a donc montré le :

Corollaire 2.19. *(i) Si $k < 12$ alors $\mathrm{S}_k = 0$.*

(ii) Si $k < 0$ ou $k = 2$ alors $\mathrm{M}_k = 0$.

(iii) $\mathrm{M}_0 = \mathbb{C}\,1$ et si $k = 4, 6, 8, 10$ alors $\mathrm{M}_k = \mathbb{C}\,\mathrm{E}_k$.

Appliquons la formule (8) à $k = 4$ et $f = \mathrm{E}_4$. Dans ce cas on a $\frac{k}{12} = \frac{1}{3}$, mais l'annulation évidente $\mathrm{E}_4(\rho) = 0$ entraîne $\frac{1}{3}\mathrm{v}_\rho(f) \geq 1/3$. Ainsi, la seule Γ-orbite de points qui sont des zéros de E_4 est celle de ρ. En particulier, cela démontre la non-nullité annoncée

$$\mathrm{E}_4(i) \neq 0,$$

puis $\Delta \neq 0$ car on a $\Delta(i) = \frac{1}{1728}\mathrm{E}_4(i)^3$.

Appliquant maintenant (8) à $k = 12$ et $f = \Delta$, on en déduit que Δ ne s'annule pas sur $\mathbb{H}$ et que l'inégalité $\mathrm{v}_\infty(\Delta) \geq 1$ est une égalité. En particulier, si k est quelconque et si $f \in \mathrm{S}_k$ alors la fonction $\frac{f}{\Delta}$ est une forme modulaire de poids $k-12$. On a démontré le corollaire suivant.

Corollaire 2.20. *(i) La fonction Δ ne s'annule pas sur $\mathbb{H}$ et l'on a $\mathrm{v}_\infty(\Delta) = 1$.*

(ii) Si $k \in \mathbb{Z}$ alors $\mathrm{S}_k = \Delta\,\mathrm{M}_{k-12}$. En particulier, $\mathrm{S}_{12} = \mathbb{C}\,\Delta$ est de dimension 1.

Démontrons enfin que M_k est engendré par les $\mathrm{E}_4^r\mathrm{E}_6^s$, où r, s sont des entiers ≥ 0 tels que $4r + 6s = k$. D'après le corollaire 2.19, on peut supposer $k \geq 4$. On procède par récurrence sur k. Observons que k étant pair ≥ 4, il existe des entiers positifs r, s tels que $k = 4r + 6s$: on a soit $k \equiv 0 \bmod 4$, soit $k \equiv 6 \bmod 4$ et $k \geq 6$. Un tel couple (r, s) étant fixé, observons que pour tout $f \in \mathrm{M}_k$ alors $f - f(\infty)\mathrm{E}_4^r\mathrm{E}_6^s \in \mathrm{S}_k$. Mais $\mathrm{S}_k = \Delta\mathrm{M}_{k-12}$ d'après le corollaire 2.20, et $\Delta = \frac{1}{1728}(\mathrm{E}_4^3 - \mathrm{E}_6^2)$. Cela termine la démonstration, ainsi donc que celle du théorème 2.16. □

Les corollaires 2.19 et 2.20 entraînent également immédiatement le corollaire suivant :

Corollaire 2.21. *Supposons $k \geq 0$ pair. La dimension de S_k vaut $[k/12]$ si $k \not\equiv 2 \bmod 12$, $[k/12] - 1$ sinon.*

Remarque 2.22. Comme Δ ne s'annule pas sur $\mathbb{H}$, la fonction $\mathrm{j} := \frac{\mathrm{E}_4^3}{\Delta}$ ("invariant modulaire") est une fonction modulaire de poids 0, manifestement holomorphe sur $\mathbb{H}$. En revanche, $|\mathrm{j}(\tau)|$ tends vers $+\infty$ lorsque $\mathrm{Im}(\tau)$ tend vers l'infini. Ainsi, si l'on avait omise la condition de limite (ii) dans la définition des formes modulaires, l'espace M_0 aurait été de dimension infinie, à cause des polynômes en j. De même, tous les M_k avec k pairs auraient été de dimension infinie (considérer $j^m\frac{\mathrm{E}_{k+12r}}{\Delta^r}$ avec r assez grand et m quelconque).

6. Quelques q-développements

6.1. Séries d'Eisenstein. Si $k \in \mathbb{Z}$ et $n \geq 1$ est un entier, on pose $\sigma_k(n) = \sum_{d|n} d^k$. On rappelle que les nombres de Bernoulli sont définis par la série formelle $\frac{t}{e^t-1} = \sum_{n\geq 0} \frac{\mathrm{B}_n}{n!} t^n$. L'identité suivante est essentiellement due à Euler.

Proposition 2.23. *Soit k un entier pair ≥ 4. On a $\mathrm{E}_k = 1 - \frac{2k}{\mathrm{B}_k} \sum_{n\geq 0} \sigma_{k-1}(n)\mathrm{q}^n$.*

Démonstration — Rappelons qu'Euler a démontré que pour tout $z \in \mathbb{C} - \mathbb{Z}$, on a

$$\frac{\pi}{\tan \pi z} = \frac{1}{z} + \sum_{n\in\mathbb{Z}-\{0\}} (\frac{1}{z-n} + \frac{1}{n}) \tag{9}$$

Justifions brièvement cette identité. Notons $g(z)$ la série de fonctions de droite et posons $f(z) = \frac{\pi}{\tan \pi z}$. Si $|z| \leq r$ et $|n| > r$ alors l'inégalité

$$|\frac{1}{z-n} + \frac{1}{n}| = \frac{|z|}{|n||z-n|} \leq \frac{r}{|n|(|n|-r)}$$

montre que la série de fonctions méromorphes $g(z)$ converge normalement sur tout compact de $\mathbb{C}$. C'est donc une fonction méromorphe sur $\mathbb{C}$, holomorphe sur $\mathbb{C} - \mathbb{Z}$, dont les pôles en les entiers sont simples de résidu 1. La fonction f a les même propriétés que g, de sorte que $f - g$ est holomorphe sur $\mathbb{C}$. Mais f et g, et donc $f - g$, sont 1-périodiques et impaires (c'est un exercice pour g). Pour en déduire que $f - g$ est nulle il suffit d'après Liouville de montrer que f et g restent bornées quand $\mathrm{Im}\tau \to \infty$. C'est clair pour f. Pour g, on observe que $\mathrm{q}\, g(\tau) \to 0$ quand $\mathrm{Im}(\tau) \to +\infty$, d'où l'on tire que $\widetilde{g}$ est holomorphe en 0 (lemme de prolongement de Riemann), ce qui conclut.

Si $\tau \in \mathbb{H}$ on a le développement évident $\frac{\pi}{\tan \pi\tau} = i\pi \frac{\mathrm{q}+1}{\mathrm{q}-1} = i\pi - 2i\pi \sum_{n\geq 0} \mathrm{q}^n$. Soit $k \geq 2$. En dérivant $k-1$ fois par rapport à τ la formule d'Euler, on trouve l'identité

$$\sum_{n\in\mathbb{Z}} \frac{1}{(\tau+n)^k} \;=\; \frac{(-2i\pi)^k}{(k-1)!} \sum_{n\geq 0} n^{k-1}\mathrm{q}^n.$$

Supposons k pair ≥ 4. On applique cette identité à $m\tau$ pour tout m entier ≥ 1, ce qui a pour effet de remplacer q par q^m, et on fait la somme (la convergence absolue du terme de droite ayant déjà été vérifiée). On en déduit, pour $k \geq 4$ pair :

$$\frac{1}{2}\,\mathrm{G}_k(\tau) - \zeta(k) \;=\; \frac{(2i\pi)^k}{(k-1)!} \sum_{n\geq 0} \sigma_{k-1}(n)\mathrm{q}^n.$$

Pour conclure, on utilise une identité fameuse due à Euler :

$$\zeta(k) = -\frac{(2i\pi)^k}{2k!}\mathrm{B}_k.$$

En fait, cette formule est aussi conséquence de l'identité (9). En effet, cette dernière dérivée $k-1$ fois s'écrit

$$(\frac{2i\pi}{e^{2i\pi z}-1} - \frac{1}{z})^{(k-1)} = (-1)^{k-1}\,(k-1)! \sum_{n\neq 0} \frac{1}{(z+n)^k}.$$

Par définition des nombres de Bernoulli on a $\frac{2i\pi}{e^{2i\pi z}-1} - \frac{1}{z} = \sum_{n\geq 1} (2i\pi)^n \frac{\mathrm{B}_n}{n!} z^{n-1}$ au voisinage de $z = 0$. On conclut par évaluation en $z = 0$. □

Observons que le q-développement de E_k est à coefficients dans $\mathbb{Q}$. Mieux, E_4 et E_6 sont à coefficients entiers, comme le montre le tableau suivant.

k	2	4	6	8	10	12	14	16
$-\frac{2k}{\mathrm{B}_k}$	-24	240	-504	480	-264	65520/691	-24	16320/3617

Corollaire 2.24. *Soit* $\mathrm{M}_k(\mathbb{Z}) \subset \mathrm{M}_k$ *le sous-groupe constitué des formes modulaires dont tous les coefficients de Fourier sont dans* $\mathbb{Z}$*. Alors* $\mathrm{M}_k(\mathbb{Z})$ *est libre de rang* $\dim \mathrm{M}_k$*, et engendré sur* $\mathbb{Z}$ *par une* $\mathbb{C}$*-base de* M_k

Démonstration — Soit N un entier $> k/12$. L'application linéaire $u : \mathrm{M}_k \longrightarrow \mathbb{C}^{N+1}$, $f \mapsto (a_n(f))_{n=0}^N$, est injective, car si f non nulle est dans $\ker u$ alors on a $\mathrm{v}_\infty(f) > k/12$, ce qui contredit la formule $k/12$. En particulier, le groupe $\mathrm{M}_k(\mathbb{Z})$ se plonge dans $\mathbb{Z}^{N+1}$: il est donc libre de type fini sur $\mathbb{Z}$. Comme toute famille $\mathbb{Z}$-libre dans $\mathbb{Z}^r$ est $\mathbb{C}$-libre dans $\mathbb{C}^r$, toute famille $\mathbb{Z}$-libre de $\mathrm{M}_k(\mathbb{Z})$ est $\mathbb{C}$-libre dans M_k (appliquer u). Ainsi le $\mathbb{Z}$-rang de $\mathrm{M}_k(\mathbb{Z})$ est $\leq \dim \mathrm{M}_k$. Mais $\mathrm{E}_4^r\mathrm{E}_6^s$ est dans $\mathrm{M}_{4k+6s}(\mathbb{Z})$ d'après l'observation ci-dessus, donc on conclut par le Théorème 2.16. □

6.2. La magie des formes modulaires. En guise d'exemple, considérons E_4^2. C'est un élément de $\mathrm{M}_8 = \mathbb{C}\,\mathrm{E}_8$ (Corollaire 2.19). Comme $\mathrm{E}_4^2(\infty) = \mathrm{E}_8(\infty) = 1$, on a nécessairement

$$\mathrm{E}_4^2 = \mathrm{E}_8.$$

Cette identité est tout à fait non triviale ! En effet, une fois les coefficients de Fourier égalisés elle s'écrit

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m), \quad \forall\ n \geq 1.$$

Par exemple, $1 + 2^7 = 129 = 1 + 2^3 + 120$. Cette méthode de raisonnement a de nombreuses autres applications.

6.3. La fonction Δ. La formule $\Delta = \frac{1}{1728}(\mathrm{E}_4^3 - \mathrm{E}_6^2)$, combinée aux q-développements de E_4 et E_6, permet d'exprimer les coefficients de Fourier de Δ. On trouve (en notant $1728 = 3 \cdot 240 + 2 \cdot 504$)

$$\Delta = \mathrm{q} - 24\,\mathrm{q}^2 + 252\,\mathrm{q}^3 - 1472\,\mathrm{q}^4 + 4830\,\mathrm{q}^5 - 6048\,\mathrm{q}^6 + \cdots$$

Théorème 2.25. (Jacobi) $\Delta = \mathrm{q} \prod_{n\geq 1}(1 - \mathrm{q}^n)^{24}$.

Avant de discuter la démonstration de cet énoncé, faisons quelques remarques de nature historique. Les coefficients de Fourier $\mathrm{a}_n(\Delta)$ de Δ sont notés $\tau(n)$: c'est la fonction τ de Ramanujan. Elle possède une riche histoire. En 1916, Ramanujan avait notamment conjecturé par inspection les deux propriétés suivantes :

(a) si m et n sont premiers entre eux, alors $\tau(mn) = \tau(m)\tau(n)$,

(b) si p est premier, et si $n \geq 1$ alors $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$,

(c) si p est premier, on a $|\tau(p)| \leq 2\,p^{11/2}$.

Par exemple, on a bien $\tau(6) = -6048 = -24 \cdot 252 = \tau(2)\tau(3)$ et $\tau(4) = -1472 = (-24)^2 - 2^{11} = \tau(2)^2 - 2^{11}$. Ces conjectures ont eu une influence considérable sur la théorie des nombres, et se sont avérées très loin d'être anecdotiques, peut-être en dépit de leur apparence. Les deux premières ont été démontrées par Mordell [2]. Ce sont des conséquences simples de l'égalité $\dim \mathrm{S}_{12} = 1$ démontrée ici et de l'existence de certains opérateurs agissant sur les espaces de formes modulaires ; ces opérateurs seront étudiés plus tard de manière systématique par Hecke et feront l'objet du prochain cours (de sorte que nous démontrerons (a) et (b)). La troisième, maintenant un théorème fameux de Deligne, s'est avérée être une manifestation des célèbres conjectures de Weil, elles-même démontrées aussi par Deligne, donnant des estimées précises "à la Hasse" sur le nombre des solutions $(x_1, \ldots, x_d)$ dans $(\mathbb{Z}/p\mathbb{Z})^d$ d'une équation de la forme $P(X_1, \ldots, X_d) = 0$ avec $P \in (\mathbb{Z}/p\mathbb{Z})[X_1, \ldots, X_d]$ un polynôme. Le lien entre les formes modulaires et ces conjectures avait d'ailleurs déjà été suspecté avant Deligne par des mathématiciens comme Eichler, Shimura, Kuga et Sato. Les conjectures de Weil, furent l'une des motivations principale de la refonte de la géométrie algébrique initée par Grothendieck et son école dans les années 60, elles ont été complètement démontrées par Deligne. Nous n'aborderons pas du tout la démontration de Deligne dans ce cours. En revanche, nous verrons que (c) est un cas très particulier d'une conjecture extrêmement générale (est très largement ouverte) en théorie des formes automorphes.

Démonstration — (du Théorème 2.25) Comme $\mathrm{S}_{12} = \mathbb{C}\Delta$, il suffit de montrer que la fonction sur $\mathbb{H}$ définie par $f(\tau) = \mathrm{q}\prod_{n\geq 1}(1-\mathrm{q}^n)^{24}$ est dans S_{12}. C'est manifestement une fonction holomorphe vérifiant $f(\tau+1) = f(\tau)$ et $f(\tau) \to 0$ quand $\mathrm{Im}\,\tau$ tend vers $+\infty$, de sorte qu'il suffirait de vérifier $f(-1/\tau) = \tau^{12} f(\tau)$. Considérons en fait l'identité générale à démontrer, à savoir que pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$ on a

$$\mathrm{j}(\gamma, \tau)^{-12} f(\gamma\tau) = f(\tau). \tag{10}$$

Étant donnée l'écriture en produit de f on va s'intéressee à la dérivée logarithmique de cette identité. La théorie des fonctions holomorphes (voir par exemple le livre de H. Cartan Ch. V §3 Thm. 2, p. 161) montre que la dérivée logarithmique de f est la somme des dérivées logarithmiques de chacun des termes du produit. Celle de q est $2i\pi\mathrm{q}$, et celle de $1-\mathrm{q}^n$ est $-2i\pi\sum_{m\geq 1} nq^{nm}$. On a donc $f'(\tau)/f(\tau) = 2i\pi\,\mathrm{E}_2$ où E_2 est la fonction sur $\mathbb{H}$ définie par

$$\mathrm{E}_2 = 1 - 24\sum_{n\geq 1}\sigma_1(n)\mathrm{q}^n.$$

La notation est bien "compatible" avec celle des E_k pour $k > 2$. Mieux, l'argument d'Euler donné dans la proposition 2.23 montre que l'on a

$$2\zeta(2)\,\mathrm{E}_2(\tau) = \sum_{n\in\mathbb{Z}-\{0\}}\frac{1}{n^2} + 2\sum_{m\geq 1}\Big(\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^2}\Big) \tag{11}$$

(la somme n'est plus absolument convergente, et doit être effectuée dans l'ordre indiqué). D'autre part, la dérivée logarithmique de $\tau \mapsto j(\gamma,\tau) = c\tau + d$ est la

2. *On Mr. Ramanujan's Empirical Expansions*, Proceedings of the Cambridge Philosophical Society, Mathematical and physical sciences (1917).

fonction $-c\mathrm{j}(\gamma,\tau)^{-1}$, et celle de $\tau \mapsto \gamma\tau$ est $\mathrm{j}(\gamma,\tau)^{-2}$. Ainsi, la dérivée logarithmique de l'équation (10) à prouver s'écrit après division par $2i\pi$

$$-\frac{12}{2i\pi}\, c\,\mathrm{j}(\gamma,\tau)^{-1} + j(\gamma,\tau)^{-2}\mathrm{E}_2(\gamma\tau) = \mathrm{E}_2(\tau). \tag{12}$$

Esquissons maintenant seulement la démonstration de cette identité donnée par Zagier (référence citée §2.3), qu'il attribue à Hecke (voir aussi le cours d'arithmétique de Serre pour démonstration directe pour $\gamma = S$, ce qui suffira pour prouver le théorème). On regarde la série d'Eisenstein $\mathrm{G}_{2,s}$, avec disons s réel > 0, introduite dans l'Exemple 2.9. Zagier démontre d'abord que pour tout réseau L, la fonction $s \to \mathrm{G}_{2;s}(L)$ admet une limite quand $s \to 0$ (c'est en fait un cas particulier du fameux prolongement méromorphe à $\mathbb{C}$ des séries d'Eisenstein valable pour tout k, s), que nous noterons G_2. L'argument de régularisation donné par Zagier (avec pour point de départ l'identité (11)) montre que G_2 est relié à E_2 par la formule suivante pour G_2

$$\frac{1}{2\zeta(2)}\mathrm{G}_2(\tau) = \mathrm{E}_2(\tau) - \frac{6}{2\pi}\,\frac{1}{\mathrm{Im}\,\tau}. \tag{13}$$

Comme $\mathrm{G}_{2;s}$ est modulaire de poids $\lambda^{-2}|\lambda|^{-s}$, la fonction G_2 est modulaire de poids 2, par passage à la limite. Ainsi, G_2 n'est pas holomorphe, mais une fonction modulaire de poids 2, alors que la fonction E_2 est holomorphe, mais pas modulaire (comme il se doit !). L'équation (12) résulte alors de l'identité (13) et de l'identité $(\mathrm{G}_2)_{|_2\gamma} = \mathrm{G}_2$, modulo le calcul immédiat suivant

$$\frac{6}{2\pi}\left((\frac{1}{\mathrm{Im}\tau})_{|_2\gamma} - \frac{1}{\mathrm{Im}\,\tau}\right) = \frac{12}{2i\pi}\, c\,\mathrm{j}(\gamma,\tau)^{-1}.$$

On pourra noter que comme $\mathrm{Im}\,\tau$ est modulaire de poids $\chi(\lambda) = |\lambda|^2 = \lambda\overline{\lambda}$, on a

$$(\frac{1}{\mathrm{Im}\tau})_{|_2\gamma} = \chi(\mathrm{j}(\gamma,\tau))\mathrm{j}(\gamma,\tau)^{-2}(\frac{1}{\mathrm{Im}\tau})_{|_\chi\gamma} = \frac{\overline{\mathrm{j}(\gamma,\tau)}}{\mathrm{j}(\gamma,\tau)}\frac{1}{\mathrm{Im}\,\tau}.$$

(sans calcul !), et conclure par $\overline{\mathrm{j}(\gamma,\tau)} - \mathrm{j}(\gamma,\tau) = -2i\,\mathrm{Im}\,\mathrm{j}(\gamma,\tau) = \frac{2}{i}\,c\,\mathrm{Im}\tau$.

Au final, nous avons démontré qu'il existe une constante $\mathrm{C}_\gamma \in \mathbb{C}^\times$ telle que $f_{|_{12}\gamma} = \mathrm{C}_\gamma f$: c'est l'information que l'on obtient en disant que la dérivée logarithmique de (10) est nulle. Autrement dit, f est vecteur propre de Γ pour l'action de poids 12, de "système de valeurs propres les C_γ". Il en résulte que $\gamma \to \mathrm{C}_\gamma, \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^\times$, est un morphisme de groupes. Pour voir qu'il est trivial, il suffit de vérifier $\mathrm{C}_\mathrm{T} = 1$ et $\mathrm{C}_\mathrm{S} = 1$, une remarque que l'on avait déjà faite au début. Mais $\mathrm{C}_\mathrm{T} = 1$ est évident car $f(\tau+1) = f(\tau)$. Enfin, si l'on contemple l'équation

$$\tau^{-12} f(1/\tau) = \mathrm{C}_\mathrm{S} f(\tau),$$

on a pour $\tau = i$ l'identité $f(i) = \mathrm{C}_\mathrm{S} f(i)$. Il ne reste qu'à observer que l'on a $f(i) \neq 0$, ce qui c'est évident ; on constate même sur la formule définissant f que $f(iy)$ est un réel > 0 pour tout $y \in \mathbb{R}_{>0}$. □

CHAPITRE 3

Opérateurs de Hecke

Les opérateurs de Hecke sont certaines correspondances entre réseaux, indexées par les entiers $n \geq 1$ et notées $\mathrm{T}(n)$, qui opèrent de manière naturelle sur les espaces de formes modulaires. Ces opérateurs, étudiés de manière systématique par Hecke dans les années 30 mais dont l'origine est plus ancienne [1], jouissent de propriétés remarquables. Nous verrons par exemple qu'ils commutent deux à deux et (plus tard) qu'ils sont diagonalisables, de sorte que M_k possède une base constituée de formes propres pour tous ces opérateurs simultanément (appelées parfois "formes de Hecke").

L'opérateur $\mathrm{T}(p)$ apparaît à bien des égards comme un analogue de la substitution de Frobenius Frob_p rappelée au Chapitre 1. Par exemple, d'un point de vue élémentaire, nous verrons suivant Hecke qu'à toute forme de Hecke $f \in \mathrm{S}_k$ est associée une série de Dirichlet $\mathrm{L}(s, f)$ possédant à la fois un prolongement analytique à $\mathbb{C}$ tout entier, et un produit Eulerien indexé par tous les nombres premiers, le facteur en p étant donné par une recette simple à partir de la valeur propre $\lambda_p(f)$ de $\mathrm{T}(p)$ sur f. Ces fonctions L présentent des similarités frappantes avec celles introduites au Chapitre 1, bien que leur construction soit très différente. En fait, l'analogie entre Frobenius et opérateurs de Hecke est plus profonde, comme l'ont vu notamment Eichler et Shimura. Elle prend une de ses formes ultimes (?) dans la construction par Deligne de représentations galoisiennes ℓ-adiques de dimension 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ qui sont non ramifiées en tout nombre premier $p \neq \ell$, et dans lesquelles le polynôme caractéristique de Frob_p vaut $X^2 - \lambda_p(f)X + p^{k-1}$ pour tout $p \neq \ell$. Nous ne dirons malheureusement rien de cette construction dans ce cours.

Avant d'agir sur les espaces de formes modulaires, les opérateurs de Hecke existent comme on l'a dit sous forme de correspondances "naturelles" sur l'ensemble des réseaux de $\mathbb{C}$, et en tant que telles, ils forment un anneau intéressant. Le sens du mot "naturel" ici est que ces correspondances commutent à l'action du groupe des automorphisme de $\mathbb{C}$ vu comme $\mathbb{R}$-espace vectoriel. Il s'agit d'un cas particulier d'une construction aussi simple que générale, s'appliquant à tous les ensembles munis d'une action de groupe, et dont l'étude élémentaire sera notre point de départ. Cela nous permettra aussi d'introduire les anneaux de convolution $\mathrm{H}(G, K)$ qui jouent un rôle important en théorie des représentations, et réapparaîtront plus tard dans le cours.

Références : G. Chenevier & J. Lannes, *Formes automorphes et réseaux unimodulaires pairs*, Chapitre 4,

J.-P. Serre, *Cours d'arithmétique*, dernier Chapitre.

1. Par exemple, ils apparaissent dans ce contexte, bien que dans des cas particuliers, mais de manière très claire, dans le travail de Mordell déjà cité (1917), et sont sans doute beaucoup plus anciens.

1. Correspondances de Hecke abstraites

1.1. Correspondances sur un ensemble. Soit X un ensemble. On rappelle que $\mathbb{Z}[X]$ désigne le *groupe abélien libre sur* X. Un élément de $\mathbb{Z}[X]$ s'écrit de manière unique la forme $\sum_{x\in X} n_x\, x$ avec $n_x \in \mathbb{Z}$ et $n_x = 0$ pour tout $x \in X$ hors d'un ensemble fini. Pour éviter les confusions, on notera parfois $[x]$ l'élément $x \in X$ vu dans $\mathbb{Z}[X]$. Soulignons aussi que dans les applications, l'ensemble X sera en général infini.

Définition 3.1. *Une correspondance sur l'ensemble X est un endomorphisme du groupe abélien $\mathbb{Z}[X]$. Les correspondances forment un anneau pour la composition, à savoir l'anneau* $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$.

Faisons quelques observations élémentaires. Soit T une correspondance sur X. Pour tout $y \in X$ on peut écrire

$$T(y) \;=\; \sum_{x\in X} T_{x,y}\; x$$

où les coefficients $T_{x,y}$ sont des éléments de $\mathbb{Z}$ uniquement déterminés, et arbitraires, avec pour unique contrainte que pour tout y l'ensemble des $x \in X$ vérifiant $T_{x,y} \neq 0$ est fini. On peut donc penser à T comme étant la donnée d'une matrice carrée $(\mathrm{T}_{x,y})_{(x,y)\in X\times X}$, n'ayant qu'un nombre fini de termes non nuls dans chaque colonne. Si $T, T' \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$, la matrice associée à un produit $T \circ T'$ n'est manifestement rien d'autre que le produit des matrices de T et T' :

$$(TT')_{x,z} = \sum_{y\in X} T_{x,y}T'_{y,z}, \;\text{ pour tout } x, z \in X. \tag{14}$$

(Observer au passage que la somme de droite est bien finie.) Il sera commode d'introduire, pour $T \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$, la "fonction coefficient associée" $\mathrm{f}_T : X \times X \to \mathbb{Z}$, définie par $\mathrm{f}_T(x, y) = T_{x,y} \;\; \forall\, (x, y) \in X \times X$. Par exemple, si $T = \mathrm{id}$ est l'identité, f_T est la fonction caractéristique de la diagonale de $X \times X$. Mentionnons pour utilisation future le résultat suivant, déjà justifié au début du paragraphe.

Corollaire 3.2. *L'application* $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X]) \longrightarrow \{f : X \times X \to \mathbb{Z}\}$, $T \mapsto \mathrm{f}_T$, *est une injection $\mathbb{Z}$-linéaire dont l'image est le sous-groupe des fonctions ne prenant qu'un nombre fini de valeurs non nulles sur $X \times \{y\}$, pour tout $y \in X$.*

1.2. Correspondances de Hecke. Supposons désormais que le groupe G agit sur X. Ce groupe agit alors naturellement sur $\mathbb{Z}[X]$, de manière $\mathbb{Z}$-linéaire, par la formule $g[x] := [gx]$, pour tous $g \in G$ et $x \in X$.

Définition 3.3. *Soit X un ensemble muni d'une action d'un groupe G. Une correspondance (ou opérateur) de Hecke sur X est un endomorphisme T du groupe abélien $\mathbb{Z}[X]$ qui commute à l'action de G, i.e. vérifiant $T\,(gx) = gT(x)$ pour tout $x \in X$ et tout $g \in G$. L'ensemble de ces correspondances est un sous-anneau de* $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[X])$, *appelé anneau de Hecke de X, et noté* $\mathrm{H}(X)$.

On fait agir le groupe G sur $X \times X$ par la formule $g(x, y) = (gx, gy)$.

Lemme 3.4. *Soit T une correspondance sur X. Alors T est dans* $\mathrm{H}(X)$ *si, et seulement si, f_T est constante sur chaque G-orbite dans $X \times X$.*

Démonstration — En effet, si $g \in G$ on a les égalités évidentes $g^{-1}T(gy) = \sum_{x\in X} T_{x,gy}\ g^{-1}x = \sum_{x\in X} T_{gx,gy}\ x$, la seconde résultant du fait que $x \mapsto gx$ est une bijection de X. □

Soit $\Omega \subset X \times X$ une G-orbite. Soit $T \in \mathrm{H}(X)$. On sait que f_T est constante sur Ω. Si elle y prend une valeur *non nulle*, alors l'ensemble $\Omega \cap (X \times \{y\})$ est fini, par finitude de $\{x \in X, T_{x,y} \neq 0\}$. On dira que Ω est VF (pour *verticalement finie*), si $\Omega \cap (X \times \{y\})$ est fini pour tout $y \in X$. En retour, si Ω est VF alors il existe une unique correspondance de Hecke $\mathrm{c}_\Omega \in \mathrm{H}(X)$ telle que $\mathrm{f}_{\mathrm{c}_\Omega}$ est la fonction caractéristique de Ω (Corollaire 3.2).

Proposition 3.5. *On suppose que l'action de G sur X a un nombre fini d'orbites (par exemple, qu'elle est transitive).*

(i) L'application $T \mapsto \mathrm{f}_T$ est une injection $\mathbb{Z}$-linéaire de $\mathrm{H}(X)$ sur le groupe abélien des fonctions $X \times X \to \mathbb{Z}$ à support dans une réunion finie d'orbites VF.

(ii) Les c_Ω, Ω parcourant les orbites VF *de G dans $X \times X$, forment une $\mathbb{Z}$-base du groupe additif de $\mathrm{H}(X)$.*

Démonstration — (i) ⇒ (ii) est évident. Pour montrer le (i), il ne reste qu'à voir que si T est dans $\mathrm{H}(X)$, alors f_T est nulle hors d'une réunion fini de G-orbites. Fixons $y_1, \ldots, y_n \in X$ des représentants des G-orbites dans X. Toute G-orbite dans $X \times X$ contient donc un élément de la forme (x, y_i). Mais pour chaque i, l'ensemble des $x \in X$ tels que $T_{x,y_i} \neq 0$ étant fini, la fonction f_T est bien nulle hors d'un ensemble fini de G-orbites. □

Terminons par une observation simple concernant les orbites VF. Si $x \in X$ on note $G_x \subset G$ son stabilisateur dans G.

Proposition 3.6. *Soient $(x, y) \in X \times X$ et Ω la G-orbite de (x, y). On a*

$$\Omega \cap (X \times \{y\}) = (G_y \cdot x) \times \{y\}. \tag{15}$$

De plus, les propriétés suivantes sont équivalentes :

(i) Ω est VF*,*

(ii) $\Omega \cap (X \times \{y\})$ est fini,

(iii) la G_y-orbite de x dans X est finie.

Démonstration — Si $g \in G$, l'élément (gx, gy) est dans $X \times \{y\}$ si, et seulement si, on a $g \in G_y$: c'est la formule de l'énoncé. On en déduit immédiatement $(ii) \Leftrightarrow (iii)$. Comme la multiplication par g induit une bijection $\Omega \cap (X \times \{y\}) \xrightarrow{\sim} \Omega \cap (X \times \{gy\})$ (d'inverse la multiplication par g^{-1}), on a $(i) \Leftrightarrow (ii)$. □

Définition 3.7. *On dira que le G-ensemble X est admissible si G agit transitivement sur X, et si toutes les G-orbites de $X \times X$ sont* VF*. D'après le lemme ci-dessus, il est équivalent de demander que G agit transitivement sur X, et que pour tout x dans X, les orbites de G_x dans X sont des ensembles finis.*

Si X est fini, et si G agit transitivement sur X, alors X est évidemment admissible.

1.3. Un exemple élémentaire. Donnons un exemple simple illustrant ces notions. Fixons un carré dans le plan euclidien et prenons pour X l'ensemble de ses 4 sommets. Le groupe G des isométries du carré (en fait, un groupe dihédral à 8 éléments) agit transitivement sur X. On se convainc immédiatement qu'il y a trois G-orbites dans $X \times X$:

$$X \times X = \Omega_1 \coprod \Omega_2 \coprod \Omega_3,$$

définies par :

– $(x, y) \in \Omega_1$ si, et seulement si, $x = y$ (diagonale),

– $(x, y) \in \Omega_2$ si, et seulement si, x et y sont des sommets voisins,

– $(x, y) \in \Omega_3$ si, et seulement si, x et y sont des sommets opposés.

X est évidemment admissible, car il est fini. Posons $\mathrm{T}_i = \mathrm{c}_{\Omega_i} \in \mathrm{H}(X)$. La proposition ci-dessus affirme qu'ils forment une $\mathbb{Z}$-base de $\mathrm{H}(X)$, qui est donc de rang 3.

Soient $P \in X$ est un sommet, Q et R les deux sommets voisins de P, et S le sommet opposé à P. On a par définition : $\mathrm{T}_1(P) = P$, $\mathrm{T}_2(P) = Q + R$ et $\mathrm{T}_3(P) = S$. On constate donc les identités suivantes dans l'anneau $\mathrm{H}(X)$:

$$\mathrm{T}_1 = 1,\ \mathrm{T}_2^2 = 2 + 2\,T_3,\ \mathrm{T}_3^2 = 1 \text{ et } \mathrm{T}_2\mathrm{T}_3 = \mathrm{T}_3\mathrm{T}_2 = \mathrm{T}_2.$$

En particulier, $\mathrm{H}(X)$ est un anneau commutatif (ce qui n'est bien sûr pas toujours le cas). On a en fait $\mathrm{T}_2^3 = 4\mathrm{T}_2$, puis un isomorphisme d'anneaux $\mathbb{Z}[1/2][t]/(t^3 - t) \xrightarrow{\sim} \mathrm{H}(X)[1/2]$, obtenu en voyant t sur $\frac{1}{2}\mathrm{T}_2$. On en déduit :

$$\mathrm{H}(X)[1/2] \simeq \mathbb{Z}[1/2] \times \mathbb{Z}[1/2] \times \mathbb{Z}[1/2].$$

1.4. Une traduction : l'anneau de convolution $\mathrm{H}(G, K)$. On suppose désormais que le groupe G agit transitivement sur l'ensemble X. On fixe un point $x_0 \in X$, et on note $K = G_{x_0} \subset G$ le stabilisateur de x_0 dans G, de sorte que $g \mapsto gx_0$ identifie G/K et X. Soulignons que le couple de groupes (G, K) ainsi obtenu, avec K sous-groupe de G, est bien entendu arbitraire, étant donné que l'on peut toujours poser $X = G/K$ et $x_0 = K$.

Soit Ω une G-orbite dans $X \times X$. Par transitivité de l'action de G sur X, Ω contient un élément de la forme (gx_0, x_0) avec $g \in G$. D'après la formule (15), un tel élément g est même unique modulo translations à droite et à gauche par des éléments de K : l'application $G \to \Omega,\ \ h \mapsto (hx_0, x_0)$, induit une bijection

$$(KgK)/K \xrightarrow{\sim} \Omega \cap (X \times \{x_0\}) \tag{16}$$

En particulier, (16) et la Proposition 3.6 montrent que Ω est VF si, et seulement si, $(KgK)/K$ est fini (ou ce qui revient au même, ssi $K/(K \cap (gKg^{-1}))$ est fini) :

Corollaire 3.8. *Le G-ensemble G/K est admissible si, et seulement si, pour tout $g \in G$ l'ensemble $(KgK)/K$ est fini.*

Remarque 3.9. Si $g \in G$ est tel que $(KgK)/K$ est fini, alors $K\backslash(Kg^{-1}K)$ est également fini, comme on le voit en appliquant $g \mapsto g^{-1}$. En particulier, si G/K est admissible alors pour tout $g \in G$, le sous-ensemble $KgK \subset G$ est non seulement réunion disjointe finie de parties de la forme g_iK, mais il est aussi réunion disjointe finie de parties de la forme Kh_j.

Corollaire 3.10. *On suppose X admissible. Soit $x_0 \in X$ et $K = G_{x_0}$. L'application $\varphi : T \mapsto (g \mapsto T_{gx_0,x_0})$ définit une bijection $\mathbb{Z}$-linéaire entre $\mathrm{H}(X)$ et l'ensemble des fonctions $f : G \to \mathbb{Z}$ vérifiant les propriétés suivantes :*

(i) $f(k'gk) = f(g)$ pour tout $k, k' \in K$ et tout $g \in G$,

(ii) f est nulle hors d'une réunion finie de parties de la forme KgK avec $g \in G$.

De plus, si $\Omega \subset X \times X$ est une G-orbite, et si $g \in G$ est tel que $(gx_0, x_0) \in \Omega$, alors $\varphi(\mathrm{c}_\Omega)$ est la fonction caractéristique de KgK.

Démonstration — D'après la proposition 3.6, l'application $\Omega \mapsto \Omega \cap (X \times \{x_0\})$ induit une bijection entre G-orbites dans $X \times X$ et K-orbites dans X. Toute telle K-orbite est de la forme $KgK\, x_0 = Kgx_0$ pour une unique "double classe" $KgK \subset G$ (bijection (16)). L'énoncé est donc une traduction de la Proposition 3.5. □

Définition 3.11. *Soient G un groupe et K un sous-groupe de G. On note $\mathrm{H}(G, K)$ l'ensemble des fonctions $G \to \mathbb{Z}$ vérifiant les conditions (i) et (ii) du corollaire précédent.*

Supposons le G-ensemble G/K admissible. Soient $f, f' \in \mathrm{H}(G, K)$ et $g \in G$, on définit alors le *produit de convolution*

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

Explications : les deux sommes ci-dessus ont bien un sens, d'une part car f est K-invariante à droite et f' est K-invariante à gauche, et d'autre part car il s'agit en fait de sommes finies d'après la Remarque 3.9 ; le changement de variables bijectif $h \mapsto gh$ de G/K montre alors l'égalité des deux sommes.

Lemme 3.12. *Soit $\varphi : \mathrm{H}(X) \to \mathrm{H}(G, K)$ l'application de l'énoncé du corollaire 3.10. Pour tout $T, T' \in \mathrm{H}(X)$ on a $\varphi(TT') = \varphi(T') * \varphi(T)$.*

Démonstration — Si g est un élément de G, on constate les égalités :

$$\varphi(TT')(g) = (TT')_{gx_0,x_0} = \sum_{y \in X} T_{gx_0,y} T'_{y,x_0} = \sum_{h \in G/K} T_{gx_0,hx_0} T'_{hx_0,x_0}$$

$$= \sum_{h \in G/K} T'_{hx_0,x_0} T_{h^{-1}gx_0,x_0} = (\varphi(T') * \varphi(T))(g).$$

□

Corollaire 3.13. *On suppose G/K admissible.*

(i) Si f et f' sont dans $\mathrm{H}(G, K)$ alors on a $f * f' \in \mathrm{H}(G, K)$.

(ii) La loi $(f, f') \mapsto f * f'$ munit $\mathrm{H}(G, K)$ d'une structure d'anneau associatif de neutre 1_K.

(iii) L'application $T \mapsto (g \mapsto T_{gK,K})$ induit un isomorphisme d'anneaux

$$\mathrm{H}(G/K)^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{H}(G, K).$$

Démonstration — Il ne serait pas difficile (et instructif) de démontrer les assertions (i) et (ii) de cette proposition directement. C'est cependant inutile à ce stade, puisque (i) et (ii) et (iii) se déduisent immédiatement (et sans calcul !) du Corollaire 3.10, du Lemme 3.12 et du fait (évident) que $\mathrm{H}(X)$ est un anneau associatif. □

2. Correspondances entre réseaux

2.1. Correspondances entre réseaux de $\mathbb{Q}^n$. Soit V un $\mathbb{Q}$-espace vectoriel de dimension finie. On appellera *réseau* de V un sous-groupe de V engendré (sur $\mathbb{Z}$) par une $\mathbb{Q}$-base de V (on sait qu'il revient au même de demander que c'est un sous-groupe de type fini engendrant V, le point étant qu'un tel sous-groupe est libre car $\mathbb{Z}$ est principal). On notera $\mathrm{R}(V)$ l'ensemble des réseaux de V. Il est muni d'une action naturelle de $\mathrm{GL}(V)$: $(g, L) \mapsto g(L)$. C'est une action transitive, car $\mathrm{GL}(V)$ permute transitivement les bases de V ; le stabilisateur d'un réseau L est le sous-groupe $\mathrm{GL}(L)$ de tous les automorphismes du groupe abélien L. Dans le cas particulier (essentiellement général) $V = \mathbb{Q}^n$ et $L = \mathbb{Z}^n$, le groupe $\mathrm{GL}(\mathbb{Z}^n)$ n'est autre que le sous-groupe $\mathrm{GL}_n(\mathbb{Z})$ de $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{Q})$, et l'application orbite $g \mapsto g(\mathbb{Z}^n)$ induit donc une bijection

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

La théorie précédente s'applique donc au $\mathrm{GL}(V)$-ensemble $\mathrm{R}(V)$. Donnons des exemples d'opérateur de Hecke dans ce contexte qui joueront un grand rôle par la suite.

– Tout élément $\lambda \in \mathbb{Q}^*$ peut être vu comme un élément du centre $\mathrm{GL}(V)$, à savoir l'homothétie de rapport λ, et définit donc un élément $\mathrm{R}_\lambda \in \mathrm{H}(\mathrm{R}(V))$ par la formule $\mathrm{R}_\lambda([L]) = [\lambda L]$ pour tout $L \in \mathrm{R}(V)$. Il est évident que R_λ est dans le centre de l'anneau $\mathrm{H}(X)$, et qu'il est inversible d'inverse $\mathrm{R}_{\lambda^{-1}}$.

– Si $n \geq 1$ est un entier, on définit un endomorphisme $\mathrm{T}(n)$ de $\mathbb{Z}[\mathrm{R}(V)]$ en posant

$$\mathrm{T}(n)\ L = \sum_{L'} L'$$

où L' parcourt le sous-ensemble des sous-réseaux $L' \subset L$ qui sont d'indice n. Ces réseaux sont bien en nombre fini, car en bijection naturelle avec les sous-groupes du groupe abélien fini de L/nL qui sont d'indice n.

– Si A est un groupe abélien fini, on définit aussi un endomorphisme T_A de $\mathbb{Z}[\mathrm{R}(V)]$ en posant

$$\mathrm{T}_A\ L = \sum_{L'} L'$$

où L' parcourt le sous-ensemble des sous-réseaux $L' \subset L$ tels que L/L' est isomorphe à A (en particulier, un tel L' est d'indice $|A|$, donc la somme est bien finie).

Il est évident que si les groupes A et B sont isomorphes, on a $\mathrm{T}_A = \mathrm{T}_B$. Il est également évident que l'on a $\mathrm{T}(n) = \sum_A \mathrm{T}_A$, où A parcourt l'ensemble des classes d'isomorphisme de groupes abéliens finis ayant n éléments (ensemble qui est donc fini !).

Proposition 3.14. *(i) Pour tout groupe abélien fini A, on a $\mathrm{T}_A \in \mathrm{H}(\mathrm{R}(V))$.*

(ii) Si $|A|$ et $|B|$ sont premiers entre eux alors $\mathrm{T}_A\mathrm{T}_B = \mathrm{T}_{A\times B} = \mathrm{T}_B\mathrm{T}_A$.

(iii) Si n, m sont premiers entre eux, on a $\mathrm{T}(nm) = \mathrm{T}(n)\mathrm{T}(m) = \mathrm{T}(m)\mathrm{T}(n)$.

Démonstration — Le (i) résulte des observations évidentes suivantes : (1) si $g \in \mathrm{GL}(V)$, l'application $g \mapsto g(L)$ induit une bijection de l'ensemble des sous-groupes de L vers l'ensemble des sous-groupes de $g(L)$ (d'inverse g^{-1}), (2) pour $L' \subset L$ un sous-groupe et $g \in \mathrm{GL}(V)$, l'application $v \mapsto gv$ induit un isomorphisme de groupes abéliens $L/L' \xrightarrow{\sim} g(L)/g(L')$ (d'inverse g^{-1}). On a donc $\mathrm{T}_A(gL) = g\mathrm{T}_A(L)$ pour tout $g \in \mathrm{GL}(V)$ et tout $L \in \mathrm{R}(V)$.

Pour le (ii), considérons deux entiers m et n premiers entre eux. Rappelons d'abord que si C est un groupe abélien fini de cardinal mn, et si l'on pose $C_n = \{c \in C, nc = 0\}$, on a une décomposition en somme directe canonique $C = C_n \oplus C_m$, comme on le voit immédiatement en écrivant une relation de Bézout entre n et m. Pour des raisons d'ordre des éléments on a que $|C_n|$ est premier à m, ce qui force $|C_n| = n$ et $|C_m| = m$. Comme un sous-groupe de C d'ordre n contient C_n (Lagrange), on en déduit que C_n est l'unique sous-groupe d'ordre n de C, et l'unique quotient d'ordre m de C est isomorphe à C_m. Considérons maintenant deux réseaux L et L'' de V avec $L'' \subset L$ et $|L/L''| = mn$. Ces remarques appliquées à L/L'' montrent qu'il existe un et un seul sous-réseau $L'' \subset L' \subset L$ tel que $|L'/L''| = n$ (et donc $|L/L'| = m$), et que l'on a $L/L'' \simeq L/L' \times L'/L''$. Cela montre (ii) et (iii) (noter pour (ii) l'isomorphisme $A \times B \simeq B \times A$!). □

Théorème 3.15. *Le* $\mathrm{GL}(V)$*-ensemble* $\mathrm{R}(V)$ *est admissible. Les éléments* $\mathrm{T}_A \mathrm{R}_\lambda$*, avec* λ *parcourant* $\mathbb{Q}_{>0}$ *et* A *parcourant les classes d'isomorphisme de groupes abéliens finis engendrés par au plus* $\dim V - 1$ *éléments, forment une* $\mathbb{Z}$*-base de* $\mathrm{H}(\mathrm{R}(V))$.

Démonstration — Soient L, L' deux réseaux de V. Il existe $M, N \in \mathbb{Z}$ non nuls tel que $ML \subset L' \subset \frac{1}{N}L$. L'ensemble des $g(L')$ avec $g \in \mathrm{GL}(L)$ est donc inclus dans l'ensemble fini des réseaux compris entre ML et $\frac{1}{N}L$. On en déduit que $\mathrm{R}(V)$ est admissible par le (iii) de la Proposition 3.6.

Nous allons appliquer la Proposition 3.5. Pour A un groupe abélien fini et $\lambda \in \mathbb{Q}_{>0}$, et $T = \mathrm{T}_A \mathrm{R}_\lambda$, alors f_T est la fonction caractéristique de l'ensemble $\Omega_{A,\lambda}$ des couples (L', L) tels que $L' \subset \lambda L$ et $(\lambda L)/L' \simeq A$. Il s'agit de voir que toute $\mathrm{GL}(V)$-orbite dans $\mathrm{R}(V) \times \mathrm{R}(V)$ est de la forme $\Omega_{A,\lambda}$, pour un unique couple (A, λ) comme dans l'énoncé. Mais ceci est une traduction de la théorie des diviseurs élémentaires. Développons un peu. En effet, cette dernière affirme que pour tout couple (L', L) de réseaux de V, il existe une, et une seule, famille d'éléments $a_1, \ldots, a_d \in \mathbb{Q}_{>0}$ avec $d = \dim V$ et $a_{i+1} \in a_i\mathbb{Z}$ pour tout $i < d$, appelés *diviseurs élémentaires du couple* (L', L), ayant la propriété suivante : il existe une $\mathbb{Z}$-base $\epsilon_1, \ldots, \epsilon_d$ de L telle que

$$L = \bigoplus_i \mathbb{Z}\epsilon_i \text{ et } L' = \bigoplus_i \mathbb{Z}a_i\epsilon_i. \tag{17}$$

Comme $\mathrm{GL}(V)$ permute transitivement les bases de V, cela montre que la $\mathrm{GL}(V)$-orbite de (L', L) est exactement l'ensemble des (N', N) ayant même diviseurs élémentaires que (L', L). Pour conclure, il suffit d'observer que a_1 est le plus petit élément λ de $\mathbb{Q}_{>0}$ tel que $L' \subset \lambda L$, et que si L, L' sont comme dans (17) on a

$$a_1 L/L' \simeq \prod_{i=2}^{d} \mathbb{Z}/m_i\mathbb{Z}, \text{ avec } m_i = a_i/a_1 \in \mathbb{Z} \text{ pour tout } i = 2, \ldots, d.$$

Les entiers $m_2, \dots, m_d$ ci-dessus vérifient $m_{i+1} \mid m_i$ pour $i < d$, ils sont uniquement déterminés par la structure du groupe abélien $a_1 L/L'$: c'est l'assertion d'unicité dans le théorème de structure des groupes abéliens finis. □

Remarque 3.16. Soient Z un anneau principal tel que Z/nZ est fini pour tout élément $n \in Z - \{0\}$, $Q = \operatorname{Frac} Z$ et V un Q-espace vectoriel de dimension finie. Notons $\mathrm{R}(V)$ l'ensemble des sous-Z-modules de V engendrés par une Q-base de V. Le groupe $\mathrm{GL}(V)$ agit de manière naturelle, et transitive, sur $\mathrm{R}(V)$. La description ci-dessus de $\mathrm{H}(\mathrm{R}(V))$ s'étend immédiatement à ce contexte, le rôle des groupes abéliens finis étant alors joué par les Z-modules finis. Cette généralisation s'applique par exemple (et de manière utile !) dans le cas où l'anneau Z vaut respectivement $\mathbb{Z}_{(p)}$, $\mathbb{Z}_p$, $(\mathbb{Z}/p\mathbb{Z})[T]$, $(\mathbb{Z}/p\mathbb{Z})[[T]]$ etc.. (ici p désigne un nombre premier). L'hypothèse Z principal pourrait même être affaiblie en "Z Dedekind" au prix de modifications mineures (et de connaissances sur les modules de type fini sur un anneau de Dedekind).

La structure multiplicative de $\mathrm{H}(\mathrm{R}(V))$, pour V de dimension arbitraire, sera étudiée plus tard dans le cours. Nous nous contenterons ici d'élucider le cas $\dim V = 2$ (le cas $\dim V = 1$ est trivial : voir les exercices).

2.2. Structure de l'anneau $\mathrm{H}(\mathrm{R}(V))$ dans le cas $\dim V = 2$. Le résultat principal est le suivant (et il est essentiellement dû à Mordell).

Proposition 3.17. ($\dim V = 2$) *Soit p un nombre premier. On a l'égalité*

$$\mathrm{T}(p)\,\mathrm{T}(p^n) \;=\; \mathrm{T}(p^{n+1}) \;+\; p\,\mathrm{R}_p\,\mathrm{T}(p^{n-1}), \quad \forall\, n \;\geq\; 1. \tag{18}$$

En particulier, on a $\mathrm{T}(p^n) \in \mathbb{Z}[\mathrm{R}_p, \mathrm{T}(p)]$ pour tout entier $n \geq 1$, ainsi que l'identité de séries formelles dans $\mathrm{H}(\mathrm{R}(V))[[t]]$:

$$\frac{1}{1 - \mathrm{T}(p)\,t \;+\; p\,\mathrm{R}_p\,t^2} = \sum_{n \geq 0} \mathrm{T}(p^n)\,t^n.$$

Démonstration — Fixons $L \subset V$ un réseau. On a $\mathrm{T}(p)\,\mathrm{T}(p^n)\,L = \sum_{(L'',L')} L''$ la somme portant sur les couples (L'', L') avec L'' d'indice p dans L' et L' d'indice p^n dans L (en particulier, L'' est d'indice p^{n+1} dans L). Soit L'' un sous-réseau quelconque d'indice p^{n+1} dans L. On est dans un, et un seul, des cas suivants :

(i) $L'' \subset pL$ (i.e. $\frac{1}{p}L'' \subset L$). Dans ce cas, il y a exactement $p+1$ sous-groupes L' de L dans lequels L'' est d'indice p : ces sous-groupes sont en bijection avec les droites du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\frac{1}{p}L'')/(L'') \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

(ii) $L'' \subsetneq pL$. Dans ce cas, on a $L/L'' \simeq \mathbb{Z}/(p^{n+1}\mathbb{Z})$ (comme on le voit par exemple sur les diviseurs élémentaires), et il y a donc un unique sous-groupe L' de L dans lequel L'' est d'indice p.

On a donc

$$\mathrm{T}(p)\,\mathrm{T}(p^n)\,L = (p+1) \sum_{L'' \subset pL} L'' + \sum_{L'' \subsetneq pL} L'' = p \sum_{L'' \subset pL} L'' + \sum_{L''} L''$$

chacune des sommes portant sur l'ensemble des sous-groupes L'' d'indice p^{n+1} de L satisfaisant la restriction indiquées. Si L'' est dans pL, alors il est d'indice p^{n+1} dans L, si et seulement si, il est d'indice p^{n-1} dans pL. On a bien démontré

$$\mathrm{T}(p)\,\mathrm{T}(p^n)\,L \;=\; p\,\mathrm{T}(p^{n-1})\,\mathrm{R}_p\,L \;+\; \mathrm{T}(p^{n+1})\,L.$$

(On rappelle que R_p est central dans $\mathrm{H}(\mathrm{R}(V))$. La seconde assertion découle trivialement de la première (exercice !). □

Théorème 3.18. ($\dim V = 2$) *Les* $\mathrm{R}_\lambda\,\mathrm{T}(n)$ *avec* $\lambda \in \mathbb{Q}_{>0}$ *et* $n \geq 1$ *forment une* $\mathbb{Z}$*-base de* $\mathrm{H}(\mathrm{R}(V))$. *L'anneau* $\mathrm{H}(\mathrm{R}(V))$ *est commutatif, et le morphisme d'anneaux*

$$\mathbb{Z}[\{X_p, Y_p, Y_p^{-1}\}_p] \longrightarrow \mathrm{H}(\mathrm{R}(V))$$

envoyant pour tout premier p *la variable* X_p *sur* $\mathrm{T}(p)$, *et* Y_p *sur* R_p, *est un isomorphisme.*

Démonstration — D'après le Théorème 3.15, les $\mathrm{R}_\lambda\,\mathrm{T}_{\mathbb{Z}/n\mathbb{Z}}$ avec $\lambda \in \mathbb{Q}_{>0}$ et $n \geq 1$ forment une $\mathbb{Z}$-base de $\mathrm{H}(\mathrm{R}(V))$. D'autre part, pour des réseaux donnés $L' \subset L$, il y a équivalence entre "$L/L' \simeq \mathbb{Z}/(dm)\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ " et "$L' \subset dL$ et $dL/L' \simeq \mathbb{Z}/m\mathbb{Z}$", de sorte que l'on a la relation

$$\mathrm{T}(n) = \sum_{n=d^2m} \mathrm{R}_d \mathrm{T}_{\mathbb{Z}/m\mathbb{Z}}.$$

On en déduit la première assertion ("système linéaire triangulaire de diagonale 1"). L'existence et unicité de la décomposition d'un entier en produit de facteurs premiers, la Proposition 3.14 (iii), et la Proposition 3.17, montrent alors que les monômes $\prod \mathrm{R}_p^{n_p} \prod \mathrm{T}(p)^{m_p}$, où (n_p) (resp. (m_p)) parcourent les suites d'éléments de $\mathbb{Z}$ (resp. $\mathbb{N}$) indexées par les nombres premiers n'ayant qu'un nombre fini de termes non nuls, est une $\mathbb{Z}$-base de $\mathrm{H}(\mathrm{R}(V))$. Tous ces éléments commutent (Prop. 3.14), le morphisme de l'énoncé est donc bien défini ; c'est un isomorphisme d'après la phrase précédente. □

2.3. Variante : réseaux d'un espace vectoriel réel. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie. On rappelle qu'un réseau de V est un sous-groupe additif $L \subset V$ de la forme $\sum_i \mathbb{Z}e_i$ où e_i est une base de V. On notera $\mathcal{R}(V)$ l'ensemble des réseaux de V. Il est muni d'une action naturelle de $\mathrm{GL}(V) : (g, L) \mapsto g(L)$. C'est une action transitive, car $\mathrm{GL}(V)$ permute transitivement les bases de V ; le stabilisateur d'un réseau L est le sous-groupe $\mathrm{GL}(L)$ de tous les automorphismes $\mathbb{Z}$-linéaires du groupe L. Dans le cas particulier $V = \mathbb{R}^n$ et $L = \mathbb{Z}^n$, on a $\mathrm{GL}(\mathbb{Z}^n)$ n'est autre que le sous-groupe $\mathrm{GL}_n(\mathbb{Z})$ de $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{R})$, et l'application orbite $g \mapsto g(\mathbb{Z}^n)$ induit donc une bijection

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

On observe que les éléments T_A et R_λ définis précédemment ont également un sens dans ce contexte, à l'aide des même formules, à ceci près qu'ici il y a un sens à définir R_λ plus généralement pour $\lambda \in \mathbb{R}^\times$. Notons $\mathrm{H}(\mathrm{R}(V))^{\mathrm{rat}}$ le sous-anneau de $\mathrm{H}(\mathrm{R}(V))$ constitué des T ayant la propriété suivante : pour tout L', L on a $\mathrm{T}_{L',L} = 0$ si L et L' n'engendre pas le même $\mathbb{Q}$-espace vectoriel de V. Bien sûr, on a $\mathrm{R}_\lambda \in \mathrm{H}(\mathrm{R}(V))^{\mathrm{rat}}$ si, et seulement si, $\lambda \in \mathbb{Q}^\times$.

Proposition 3.19. *Soit $W \subset V$ le $\mathbb{Q}$-espace vectoriel engendré par une $\mathbb{R}$-base arbitraire de V. La restriction $T \mapsto T_{|\mathbb{Z}[\mathrm{R}(W)]}$ induit un isomorphisme d'anneaux $\mathrm{H}(\mathrm{R}(V))^{\mathrm{rat}} \xrightarrow{\sim} \mathrm{H}(\mathrm{R}(W))$, envoyant chaque R_λ (resp. T_A) sur R_λ (resp. T_A).*

Démonstration — Cela se déduit immédiatement du fait que l'inclusion $\mathrm{R}(W) \to \mathrm{R}(V)$ induit une injection

$$\mathrm{GL}(W)\backslash(\mathrm{R}(W) \times \mathrm{R}(W)) \longrightarrow \mathrm{GL}(V)\backslash(\mathrm{R}(V) \times \mathrm{R}(V))$$

d'image l'ensemble des couples de réseaux (L', L) tels que L et L' engendrent le même espace vectoriel. Les détails sont laissés au lecteur. □

Mentionnons que le $\mathrm{GL}(V)$-ensemble $\mathrm{R}(V)$ n'est pas admissible si $\dim V > 1$; nous renvoyons à l'exercice 3.6 pour étude de cette question un peu anecdotique, ainsi que pour une description très simple de $\mathrm{H}(\mathrm{R}(V))$ à partir de $\mathrm{H}(\mathrm{R}(V))^{\mathrm{rat}}$. Si $T \in \mathrm{H}(\mathrm{R}(V))$ et si F est une fonction $\mathrm{R}(V) \to \mathbb{C}$, on définit une nouvelle fonction $T(F) : \mathrm{R}(V) \to \mathbb{C}$ en posant, pour tout réseau $L \subset V$,

$$T(F)(L) = \sum_{L'} T_{L',L}\, F(L'). \tag{19}$$

Corollaire 3.20. *(i) L'application $(\mathrm{T}, F) \mapsto T(\mathrm{F})$ est une structure de $\mathrm{H}(\mathrm{R}(V))^{\mathrm{opp}}$-module sur l'espace vectoriel des fonctions $\mathrm{R}(V) \to \mathbb{C}$.*

(ii) L'action naturelle de $\mathrm{GL}(V)$ sur l'espace des fonctions $\mathrm{R}(V) \to \mathbb{C}$ commute à celle de $\mathrm{H}(\mathrm{R}(V))$.

Démonstration — Se donner une fonction $\mathrm{R}(V) \to \mathbb{C}$ est la même chose que se donner une application $\mathbb{Z}$-linéaire $\mathbb{Z}[\mathrm{R}(V)] \to \mathbb{C}$. Mais $\mathrm{H}(\mathrm{R}(V))$ agit par définition par endomorphismes de $\mathbb{Z}[\mathrm{R}(V)]$, et donc sur $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{R}(V)], \mathbb{C})$ par composition à la source (c'est donc une action à droite, d'où le "opp″ de l'énoncé) : c'est exactement l'action donnée par la formule (19). Le (ii) signifie que l'on a $\mathrm{T}(F)(gL) = \mathrm{T}(F \circ g)(L)$, pour tout L, ce qui est la définition même d'un opérateur de Hecke. □

3. Action de l'anneau de Hecke sur les fonctions et formes modulaires

Retournons au cas des formes modulaires : on considère $V = \mathbb{C}$ comme $\mathbb{R}$-espace vectoriel de dimension 2, de sorte que dans nos notations on a $\mathcal{R} = \mathrm{R}(V)$. On dispose donc de l'action définie précédemment de l'anneau $\mathrm{H}(\mathcal{R})^{\mathrm{opp}}$ sur l'espace des fonctions $\mathcal{R} \longrightarrow \mathbb{C}$. Cette action commute à l'action de $\mathrm{GL}(\mathbb{C})$, en donc en particulier à celle du sous-groupe $\mathbb{C}^\times$ de ce dernier, elle préserve donc pour tout caractère $\chi : \mathbb{C}^\times \to \mathbb{C}^\times$ le sous-espace $\mathcal{F}_\chi(\mathcal{R})$ des fonctions de réseaux de poids χ. D'après le Corollaire 2.7, cet espace s'identifie naturellement avec l'espace des fonctions $\mathbb{H} \to \mathbb{C}$ qui sont modulaires de poids χ : ce dernier hérite donc d'une structure de $\mathrm{H}(\mathrm{R})^{\mathrm{opp}}$-module par transport de structure. Par définition, on a donc :

Scholie 3.21. *Soient f une fonction modulaire de poids χ et F la fonction de réseau de poids χ qui lui correspond (reliée à f par la formule $f(\tau) = F(\tau\mathbb{Z} + \mathbb{Z})$ pour tout $\tau \in \mathbb{H}$). Si $T \in \mathrm{H}(\mathcal{R})$ alors $T(f)$ est par définition la fonction*

$$\tau \mapsto (T(F))\,(\tau\mathbb{Z} + \mathbb{Z}).$$

C'est une fonction modulaire de poids χ.

Par exemple, on a manifestement $\mathrm{R}_\lambda(f) = \chi(\lambda)f$ pour tout $\lambda \in \mathbb{R}^\times$. Dans la suite, nous ne considèrerons que l'action du sous-anneau

$$\mathrm{H} := \mathrm{H}(\mathcal{R})^{\mathrm{rat}} \subset \mathrm{H}(\mathcal{R}),$$

que l'on a étudié en détail dans la partie précédente (ce qui ne change pas grand chose en fait comme nous l'avons déjà dit : voir l'exercice 3.6). Nous avons montré que H admet pour $\mathbb{Z}$-base les $\mathrm{R}_\lambda \cdot \mathrm{T}(n)$ avec $\lambda \in \mathbb{Q}^\times$ et $n \geq 1$. Le lemme suivant donne une formule concrète pour l'action des $\mathrm{T}(n)$ avec $n \geq 1$.

Lemme 3.22. *Soit $n \geq 1$ un entier.*

(i) Soient $w \in \mathcal{B}^+$, $g \in \mathrm{GL}_2(\mathbb{R})^+$. Le réseau $\mathrm{L}(gw)$ est un sous-réseau d'indice n de $\mathrm{L}(w)$ si, et seulement si, on a $g \in \mathrm{M}_2(\mathbb{Z})$ et $\det g = n$.

(ii) Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit par translations à gauche sur $\{g \in \mathrm{M}_2(\mathbb{Z}),\ \det g = n\}$. Un système de représentants pour cette action est donné par les matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

dans $\mathrm{M}_2(\mathbb{Z})$ avec $ad = n$ et $0 \leq b \leq d-1$.

Remarquons qu'il y a $\sigma_1(n) = \sum_{d|n} d$ représentants dans l'assertion (ii).

Démonstration — L'assertion (i) est évidente. Pour (ii), faisons d'abord opérer le groupe $\mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{Z}^2$. Si $v \in \mathbb{Z}^2 - \{0\}$, notons $\mathrm{a}(v) \in \mathbb{N}$ le pgcd de ses deux coefficients : c'est aussi le plus petit entier $a \geq 1$ tel que $\frac{1}{a}v \in \mathbb{Z}^2$. D'après la théorie des diviseurs élémentaires, il existe un unique entier $a \geq 1$ tel qu'il existe $g \in \mathrm{GL}_2(\mathbb{Z})$ tel que $gv = \begin{pmatrix} a \\ 0 \end{pmatrix}$. La caractérisation donnée de $\mathrm{a}(v)$ montre $a = \mathrm{a}(v)$. Soit $g \in \mathrm{GL}_2(\mathbb{Z})$ tel que gv est de cette forme. Quitte à remplacer g par $\mathrm{diag}(1,-1)\,g$, on peut supposer $g \in \mathrm{SL}_2(\mathbb{Z})$. Le stabilisateur de gv dans $\mathrm{SL}_2(\mathbb{Z})$ est manifestement celui de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, i.e. le sous-groupe engendré par T. On applique ces observations de la manière suivante. Soit $g \in \mathrm{M}_2(\mathbb{Z})$ avec $\det g = n$. La première colonne de g est $\neq 0$ car $n > 0$. On a vu qu'il existe un $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, unique modulo action de $\langle T \rangle$ à gauche, tel que γg a son coefficient d'indice $(2,1)$ qui est nul. Écrivons $\gamma g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Remplacer γ par $T^{\pm 1}\gamma$ revient à remplacer b par $b \pm d$ (et n'affecte ni a, ni d). Cela conclut. □

Corollaire 3.23. *Soient $f : \mathbb{H} \to \mathbb{C}$ une fonction modulaire de poids χ, $n \geq 1$ un entier, et $T = \mathrm{T}(n)$. La fonction $T(f) : \mathbb{H} \to \mathbb{C}$ est donnée par la formule*

$$\tau \mapsto \sum \chi(d)\, f\Big(\frac{a\tau + b}{d}\Big),$$

la somme portant sur les $(a,b,c) \in \mathbb{N}^3$ avec $ad = n$ et $0 \leq b < d$.

Démonstration — En effet, d'après la proposition appliquée à $w = \begin{pmatrix} \tau \\ 1 \end{pmatrix}$ avec $\tau \in \mathbb{H}$, les sous-réseaux d'indice n de $\tau\mathbb{Z}+\mathbb{Z}$ sont les $(a\tau+b)\mathbb{Z}+d\mathbb{Z}$ avec a, b, d comme dans l'énoncé. Par définition, $T(f)$ envoie donc τ sur la somme des $F((a\tau+b)\mathbb{Z}+d\mathbb{Z})$, indexée par ces mêmes a, b, d. On conclut par $(a\tau + b)\mathbb{Z} + d\mathbb{Z} = d(\frac{a\tau+b}{d}\mathbb{Z} + \mathbb{Z})$. □

Corollaire 3.24. *Pour tout entier $k \in \mathbb{Z}$, et tout $T \in \mathrm{H}$, on a*

$$T(\mathrm{M}_k) \subset \mathrm{M}_k \quad \text{et} \quad T(\mathrm{S}_k) \subset \mathrm{S}_k.$$

Démonstration — D'abord, le cas $T = \mathrm{R}_\lambda$ est évident. Ensuite, le cas $T = \mathrm{T}(n)$ est manifeste sur la formule ci-dessus : si f est holomorphe (resp. admet une limite quand $\mathrm{Im}\,\tau \to +\infty$), il en va de même des fonctions $\tau \mapsto f(a\tau + b)$ pour tout réels a et b avec $a > 0$. On conclut [2] par le Corollaire 3.23. □

L'anneau H des opérateurs de Hecke agit donc de manière naturelle, pour tout entier k, comme (une famille commutative d') endomorphismes des $\mathbb{C}$-espaces vectoriel de dimension finie M_k, tout en préservant S_k. Nous verrons juste après que E_k est un vecteur propre commun pour $k \geq 4$, de sorte qu'ils préservent en fait la décomposition $\mathrm{M}_k = \mathrm{S}_k \oplus \mathbb{C}\mathrm{E}_k$ pour $k \geq 4$. Il sont en particulier co-trigonalisables. Nous verronsplus tard que leur restriction à S_k est auto-adjointe pour un produit hermitien naturel appelé *produit de Petersson.* Cela entraînera qu'ils sont co-diagonalisables, de valeurs propres réelles.

4. Exemples et estimées des valeurs propres

Exemple 3.25. *La droite des fonctions constantes $\mathcal{R} \to \mathbb{C}$ est propre pour $\mathrm{T}(n)$ pour tout $n \geq 1$, de valeur propre $\sigma_1(n) = \sum_{d|n} d$.*

Démonstration — En effet, le lemme 3.22 implique en particulier que tout réseau admet exactement $\sigma_1(n)$ sous-réseaux d'indice $n \geq 1$. Observons, de manière indépendante, que c'est évident si $n = p$ est un nombre premier, car il revient au même de compter les $\mathbb{Z}/p\mathbb{Z}$-droites de $(\mathbb{Z}/p\mathbb{Z})^2$, qui sont au nombre de $p + 1 = \sigma_1(p)$. □

Exemple 3.26. *Soit $k \geq 4$. Pour tout entier $n \geq 1$, la fonction G_k est propre pour $\mathrm{T}(n)$ de valeur propre $n^{1-k}\sigma_{k-1}(n)$.*

Démonstration — Nous nous contenterons de vérifier ici cet énoncé pour $n = p$ premier, en laissant le cas général en exercice (le cas général est aussi conséquence du cas $n = p$ et du Théorème 3.33 démontré plus bas). Par définition, la fonction $\mathrm{T}(p)\,\mathrm{G}_k$ envoie le réseau L de $\mathbb{C}$ sur

$$\sum_{L'} \mathrm{G}_k(L') = \sum_{L',\lambda} \frac{1}{\lambda^k}$$

où L' parcourt les $p+1$ sous-groupe de L d'indice p, et où en outre dans la deuxième somme λ parcourt les éléments de L'. Si $\lambda \in L$, on constate que :

– si $\lambda \in pL$ alors λ est dans chacun des $p + 1$ sous-groupes d'indice p de L,

– si $\lambda \notin pL$ alors il existe un, et un seul, sous-groupe d'indice p de L contenant λ, à savoir $\mathbb{Z}\,\lambda + pL$.

2. L'utilisation de cette proposition est commode à ce stade, mais nous aurions tout à fait pu nous en passer. En effet, une étude de l'action d'un $T \in \mathrm{H}(\mathcal{R})^{\mathrm{rat}}$ général moins précise que celle de $\mathrm{T}(n)$ dans l'énoncé montrerait que $\mathrm{T}(f)$ est toujours combinaison linéaire finie de fonctions de la forme $f(a\tau + b)$ avec a, b dans $\mathbb{Q}$ et $a > 0$. Le point est que tout élément de $\mathrm{GL}_2(\mathbb{Q})$ s'écrit sous la forme γb avec $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ et b triangulaire supérieure.

Ainsi, la somme ci-dessus s'écrit aussi

$$(p+1)\sum_{\lambda\in pL}\frac{1}{\lambda^k}+\sum_{\lambda\in L-pL}\frac{1}{\lambda^k}=p\sum_{\lambda\in pL}\frac{1}{\lambda^k}+\sum_{\lambda\in L}\frac{1}{\lambda^k}=(p^{1-k}+1)\mathrm{G}_k(L).$$

□

Une estimée simple mais intéressante dans le cas des fonctions bornées est la suivante :

Proposition 3.27. *Soient $F:\mathcal{R}\to\mathbb{C}$ une fonction de réseaux de poids χ et s un réel. On suppose que $|F|\,\mathrm{covol}^s$ est bornée et non nulle sur $\mathcal{R}$ et que F est vecteur propre de l'opérateur $\mathrm{T}(p)$ pour p premier, de valeur propre notée λ. On a l'inégalité*

$$|\lambda|\leq(p+1)p^{-s}.$$

Démonstration — Si L' est un sous-réseau d'indice p de L, on a $\mathrm{covol}\,L'=p\,\mathrm{covol}L$. On en déduit que la fonction de réseaux $L\mapsto F(L)\,(\mathrm{covol}L)^s$, qui est de poids $\chi|\cdot|^s$ comme on l'a vu, est vecteur propre de $\mathrm{T}(p)$ pour la valeur propre $p^s\lambda$:

$$\sum_{L'}F(L')(\mathrm{covol}\,L')^s\;=\;p^s\,(\mathrm{covol}\,L)^s\,\mathrm{T}_p(F)(L)\;=\;p^s\lambda\,F(L)\,(\mathrm{covol}\,L)^s.$$

Quitte à remplacer F par $F\,\mathrm{covol}^s$, on peut donc supposer $s=0$, $|F|$ bornée, et on veut alors montrer $|\lambda|\leq p+1$.

On a d'une part $\mathrm{T}_p(F)=\lambda F$ et d'autre part $\mathrm{T}_p\,F(L)=\sum_{L'}F(L')$, la somme portant sur les $p+1$ sous-groupes d'indice p de L. Par hypothèse $M:=\sup_L|F(L)|$ est fini. Pour $L\in\mathcal{R}$ on a donc

$$|\lambda||f(L)|=|\mathrm{T}_pF\,(L)|\leq(p+1)M,$$

puis $|\lambda|M\leq(p+1)M$, et on conclut en divisant par M (un réel >0). □

Nous allons voir que la proposition ci-dessus s'applique aux formes modulaires paraboliques.

Proposition 3.28. *Soient $k\in\mathbb{Z}$ et $f\in\mathrm{S}_k$.*

(i) Pout tout $A\geq 0$, il existe une constante $C>0$ telle que pour tout $\tau\in\mathbb{H}$ vérifiant $\mathrm{Im}\,\tau\geq A$, on a $|f(\tau)|\leq Ce^{-2\pi\mathrm{Im}\,\tau}$.

(ii) La fonction $\tau\mapsto|f(\tau)|(\mathrm{Im}\,\tau)^{k/2}$ (modulaire de poids 0) est bornée sur $\mathbb{H}$.

Démonstration — La fonction $\frac{\widetilde{f}(z)}{z}$ est continue sur le disque ferné $|z|\leq e^{-2\pi A}$ (elle est même analytique sur $|z|<1$!). Si C désigne le maximum de sa valeur absolue sur ce disque, on a pour $\mathrm{Im}\,\tau>A$ l'inégalité $|f(\tau)|\leq C|e^{2i\pi\tau}|=Ce^{-2\pi\mathrm{Im}\,\tau}$. Cela montre le (i).

Pour le (ii), on rappelle que $|f(\tau)|(\mathrm{Im}\,\tau)^{k/2}$ est invariante par $\mathrm{SL}_2(\mathbb{Z})$. Pour la majorer on peut donc supposer que τ est dans $\mathcal{F}=\{\tau\in\mathbb{H},|\tau|\geq 1\text{ et }|\mathrm{Re}\,\tau|\leq 1/2\}$. Mais si $\tau\in\mathcal{F}$ on a $\mathrm{Im}\,\tau\geq\frac{\sqrt{3}}{2}$, et donc d'après le (i) il existe une constante C telle que $|f(\tau)|(\mathrm{Im}\,\tau)^{k/2}\leq Ce^{-2\pi\mathrm{Im}\,\tau}(\mathrm{Im}\,\tau)^{k/2}$. On conclut car $y\mapsto e^{-2\pi y}y^{k/2}$ est bornée sur $[\frac{\sqrt{3}}{2},+\infty[$. □

Corollaire 3.29. *Soit $f \in \mathrm{S}_k$ non nulle et vecteur propre de $\mathrm{T}(p)$ (avec p premier) pour la valeur propre λ. On a $|\lambda| \leq (p+1)p^{-k/2}$.*

Remarquer que l'énoncé analogue pour E_k (avec $k \geq 4$) est faux, car l'inégalité $(1+p^{1-k}) \leq (p+1)p^{-k/2}$ (qui s'écrit aussi $1+p^{k-1} \leq p^{k/2}+p^{k/2-1}$) n'est pas vérifiée.

5. Liens entre coefficients de Fourier et valeurs propres des opérateurs de Hecke

Le Corollaire 3.23 permet aussi de relier les coefficients de Fourier de $\mathrm{T}(n)\,f$ à ceux de f lorsque l'on a $f \in \mathrm{M}_k$.

Proposition 3.30. *Soient $f \in \mathrm{M}_k$, $n \geq 1$ et $g = \mathrm{T}(n)\,f$. Pour tout $m \geq 1$, on a*

$$\mathrm{a}_m(g) = n^{1-k} \sum_{d|n \text{ et } d|m} d^{k-1}\, \mathrm{a}_{\frac{mn}{d^2}}(f). \tag{20}$$

Démonstration — On applique le Corollaire 3.23 à $f = \sum_{r\geq 0} \mathrm{a}_r(f)\,\mathrm{q}^r$. Observons d'abord la somme suivante, dans laquelle l'entier $r \geq 1$ et $\tau \in \mathbb{H}$ sont fixés :

$$\sum_{ad=n} d^{-k} \sum_{b=0}^{d-1} e^{2i\pi r\frac{a\tau+b}{d}} = \sum_{d|n} d^{-k} e^{2i\pi\frac{nr\tau}{d^2}} \sum_{b=0}^{d-1} e^{2i\pi\frac{br}{d}}.$$

Le terme $e^{2i\pi\frac{nr\tau}{d^2}} \sum_{b=0}^{d-1} e^{2i\pi\frac{br}{d}}$ est nul sauf si d divise r, auquel cas il vaut $d\,\mathrm{q}^{\frac{nr}{d^2}}$. Il est donc de la forme $\mu\mathrm{q}^m$ avec $\mu \in \mathbb{C}^*$ et $m \geq 1$ si, et seulement si, on a $r = \frac{d^2m}{n}$ et $d|r$. Noter alors la relation $\frac{r}{d} = \frac{m}{(n/d)}$. Pour tout entier $m \geq 1$, le coefficient de q^m dans le développement de $\mathrm{T}(n)\,f$ vaut donc

$$\sum_{d|n \text{ et } \frac{n}{d}|m} d^{1-k}\, \mathrm{a}_{\frac{d^2m}{n}}(f).$$

Mais $d \mapsto n/d$ induit une bijection de l'ensemble des diviseurs de n, et on a $\frac{d^2m}{n} = \frac{mn}{(n/d)^2}$, donc cette somme coïncide avec la somme de l'énoncé après changement de variable $d \mapsto n/d$. Notons que le regroupement de terme effectué est loisible par absolue convergence de la série $\sum_{n\geq 0} \mathrm{a}_n(f) z^n$ pour $|z| < 1$. □

Pour tout entier $k \in \mathbb{Z}$ et tout entier $n \geq 1$, on définit un endomorphisme T_n de M_k par la formule

$$\mathrm{T}_n = n^{k-1}\mathrm{T}(n)_{|\mathrm{M}_k}. \tag{21}$$

L'intérêt de cette normalisation tient au corollaire suivant.

Corollaire 3.31. *Pour tout $k \geq 1$, et tout entier $n \geq 1$, T_n préserve $\mathrm{M}_k(\mathbb{Z})$. En particulier, le polynôme caractéristique de T_n est à coefficients entiers.*

Démonstration — La première assertion est évidente en contemplant la formule (20). Pour la seconde, elle se déduit du fait que $\mathrm{M}_k(\mathbb{Z})$ admet une $\mathbb{Z}$-base qui est une $\mathbb{C}$-base de M_k d'après la Proposition 2.24, dans laquelle la matrice de T_n est à coefficients entiers. □

Corollaire 3.32. *Soient $f \in \mathrm{M}_k$.*

(i) Soit $n \geq 1$ un entier. Supposons que f est vecteur propre de l'opérateur de Hecke T_n, de valeur propre notée λ_n. On a la relation $\mathrm{a}_n(f) = \lambda_n \mathrm{a}_1(f)$.

(ii) On suppose $k \neq 0$, $f \neq 0$, et que f est vecteur propre de tous les $\mathrm{T}(n)$ avec $n \geq 1$. Alors on a $\mathrm{a}_1(f) \neq 0$.

Démonstration — La relation $\mathrm{T}_n f = \lambda_n f$ entraîne d'abord $\mathrm{a}_1(\mathrm{T}_n f) = \mathrm{a}_1(f)\lambda_n$. La formule (20) appliquée à $m = 1$ sécrit $\mathrm{a}_1(\mathrm{T}_n f) = \mathrm{a}_n(f)$. On a montré le (i). Vérifions le (ii). Supposons par contraposée $\mathrm{a}_1(f) = 0$. Le (i) montre $\mathrm{a}_n(f) = 0$ pour tout $n \geq 1$, i.e. $f(\tau) = \mathrm{a}_0(f) = f(\infty)$: f est une fonction constante. Cela entraîne $k = 0$ ou $f = 0$ (utiliser par exemple $f(-1/\tau) = \tau^k f(\tau)$ pour tout $\tau \in \mathbb{H}$). □

Théorème 3.33. *Soit $f = \sum_{n\geq 0} \mathrm{a}_n \mathrm{q}^n$ une forme modulaire de poids $k \neq 0$. On suppose que f est normalisée, i.e. que l'on a $\mathrm{a}_1 = 1$, et aussi que f est vecteur propre de $\mathrm{T}(n)$ pour tout entier $n \geq 1$. On a*

(i) $\mathrm{a}_{nm} = \mathrm{a}_n \mathrm{a}_m$ pour tous n et m premiers entre eux,

(ii) $\mathrm{a}_{p^{n+1}} = \mathrm{a}_p \mathrm{a}_{p^n} - p^{k-1}\mathrm{a}_{p^{n-1}}$ pour tout p premier et tout entier $n \geq 1$,

(iii) et si f est parabolique, alors pour tout p est premier on a $|\mathrm{a}_p| \leq (1+p)p^{k/2-1}$.

Démonstration — On a vu que M_k est un $\mathrm{H}^{\mathrm{opp}}$-module. Les propriétés (i) et (ii) découlent donc du Corollaire 3.32 (i), de l'hypothèse $\mathrm{a}_1(f) = 1$ et des identités $\mathrm{T}_{nm} = \mathrm{T}_n\mathrm{T}_m = \mathrm{T}_m\mathrm{T}_n$ et $\mathrm{T}_{p^{n+1}} = \mathrm{T}_p\mathrm{T}_{p^n} - p^{k-1}\mathrm{T}_{p^{n-1}}$, qui se déduisent de l'identité $\mathrm{T}_n = n^{k-1}\mathrm{T}(n)$ et de la Proposition 3.17. D'après le Corollaire 3.29, la valeur propre de $\mathrm{T}(p)$ sur f, qui n'est autre que $p^{1-k}\mathrm{a}_p(f)$ d'après le Corollaire 3.32 (i), est $\leq (1+p)p^{-k/2}$ en valeur absolue : cela montre le (iii). □

La (feu) conjecture de Ramanujan-Petersson, démontrée par Deligne, affirme que sous les hypothèses ci-dessus on a en fait $|\mathrm{a}_p| \leq 2p^{(k-1)/2}$. La borne naïve obtenue au (c) ci-dessus s'écrit aussi $(\sqrt{p} + \frac{1}{\sqrt{p}})p^{(k-1)/2}$. Notons que ces estimées sont spécifiques aux formes paraboliques, comme le montre l'exemple de E_k.

Corollaire 3.34. *Les conjectures (a) et (b) de Ramanujan sont vraies.*

Démonstration — En effet, l'espace S_{12} est de dimension 1, donc son générateur Δ est nécessairement propre pour les opérateurs de Hecke. On conclut car Δ est trivialement une forme normalisée ($\tau(1) = 1$). □

6. Fonction L d'une forme modulaire : théorie de Hecke

Pour des raisons de temps, nous ne considèrerons que le cas (le plus intéressant) des formes paraboliques.

Lemme 3.35. *Soient $k \in \mathbb{Z}$ et $f \in \mathrm{S}_k$. Il existe $C > 0$ tel que pour tout $n \geq 1$, on a $|\mathrm{a}_n(f)| \leq C\, n^{k/2}$.*

Démonstration — Soit $n \geq 1$. On observe qu'à $y > 0$ donné, le n-ème coefficient de Fourier de la fonction 1-périodique $x \mapsto f(x+iy)$ est vaut $\mathrm{a}_n(f)e^{-2\pi ny}$. Si $M > 0$ est la constante donnée par la proposition 3.28 (ii), on a la majoration naive $|\mathrm{a}_n(f)|e^{-2\pi ny} \leq My^{-k/2}$ pour tout $y > 0$. On conclut en prenant $y = 1/n$ et $C = e^{2\pi}M$. □

Soient $f \in \mathrm{S}_k$ et $s \in \mathbb{C}$. On pose, suivant Ramanujan et Hecke,

$$\mathrm{L}(s, f) = \sum_{n \geq 1} \frac{\mathrm{a}_n(f)}{n^s}.$$

D'après le lemme ci-dessus, cette série converge absolument pour $\mathrm{Re}\, s > \frac{k}{2} + 1$.

Théorème 3.36. *On suppose $f \in \mathrm{S}_k$ normalisée et vecteur propre de tous les opérateurs de Hecke dans* H. *On a*

$$\mathrm{L}(s, f) = \prod_p \frac{1}{1 - \mathrm{a}_p(f)\, p^{-s} + p^{k-1-2s}},$$

pour $\mathrm{Re}\, s > \frac{k}{2} + 1$ (et le produit Eulerien ci-dessus est absolument convergent).

Démonstration — En effet, c'est la conséquence des points (i) et (ii) du Théorème 3.33 (voir aussi la proposition 3.17). (La convergence absolue du produit Eulerien découle de celle de la série $\mathrm{L}(s, f)$). □

Théorème 3.37. *Si $f \in \mathrm{S}_k$ alors la fonction $\Lambda(s, f) := (2\pi)^{-s}\, \Gamma(s)\, \mathrm{L}(s, f)$, définie a priori pour $\mathrm{Re}\, s > k/2 + 1$, admet un prolongement holomorphe à $\mathbb{C}$ tout entier. Ce prolongement vérifie $\Lambda(s, f) = (-1)^k \Lambda(k - s, f)$ pour tout $s \in \mathbb{C}$.*

Démonstration — Le point de départ est que pour $\mathrm{Re}\, s > k/2 + 1$ on a l'identité :

$$\int_0^\infty f(iy)\, y^s\, \frac{\mathrm{d}y}{y} = \sum_{n \geq 1} \mathrm{a}_n(f) \int_0^\infty e^{-2\pi ny} y^s \frac{\mathrm{d}y}{y} = (2\pi)^s\, \Gamma(s)\, \mathrm{L}(s, f).$$

En effet, le changement de variable $2\pi ny = t$ montre $\int_0^\infty e^{-2\pi ny} y^s \frac{\mathrm{d}y}{y} = (2\pi)^{-s}\Gamma(s)n^s$ pour $\mathrm{Re}\, s > 0$. On conclut par une interversion somme-intégrale, justifiée pour $\mathrm{Re}\, s > k/2 + 1$ par la convergence absolue de la série $\sum_{n \geq 1} \frac{\mathrm{a}_n(f)}{n^s}$.

Le changement de variables $y \mapsto 1/y$ entraîne (toujours pour $\mathrm{Re}\, s > k/2+1$) l'égalité

$$\int_0^1 f(iy) y^s \frac{\mathrm{d}y}{y} = \int_1^\infty f(i/y) y^{-s} \frac{\mathrm{d}y}{y} = i^k \int_1^\infty f(iy) y^{k-s} \frac{\mathrm{d}y}{y},$$

la seconde égalité venant de $f(i/y) = f(-1/(iy)) = i^k f(iy)$ par modularité de f. On a alors

$$\int_0^\infty f(iy)\, y^s\, \frac{\mathrm{d}y}{y} = \int_0^1 f(iy)\, y^s\, \frac{\mathrm{d}y}{y} + \int_1^\infty f(iy)\, y^s\, \frac{\mathrm{d}y}{y} = \int_1^\infty f(iy)(y^s + i^k\, y^{k-s})\frac{\mathrm{d}y}{y}.$$

La Proposition 3.28 (i) montre que pour tout $s \in \mathbb{C}$ la fonction $y \mapsto f(iy)(y^s + i^k\, y^{k-s})/y$ est intégrable sur $[1, +\infty[$ (et dominée uniformément par une fonction intégrable lorsque s reste dans un compact de $\mathbb{C}$). La fonction $\int_1^\infty f(iy)(y^s + i^k\, y^{k-s})\frac{\mathrm{d}y}{y}$ est donc une fonction entière de $s \in \mathbb{C}$, qui fournit le prolongement de $\Lambda(s, f)$ cherchée, ainsi que l'identité $\Lambda(s, f) = i^k \Lambda(k-s, f)$ (noter que l'on peut supposer k pair, auquel cas on a $i^k = \pm 1$). □

7. Exercices

Exercice 3.1. *On suppose que le groupe G agit sur l'ensemble X. Si A est un anneau commutatif unitaire. On définit $A[X]$ comme étant le A-module libre sur X (il s'identifie à $A \otimes_{\mathbb{Z}} \mathbb{Z}[X]$). Le groupe G agit naturellement A-linéairement sur $A[X]$, et on note $\mathrm{H}(X; A)$ le sous-anneau des endomorphismes du A-module $A[X]$ commutant à l'action de G. On suppose que G agit transitivement sur X.*

(i) Montrer que l'application naturelle $\mathrm{H}(X) \to \mathrm{H}(X; A)$ est injective si $\mathbb{Z} \to A$ l'est.

(ii) On suppose que G n'a qu'un nombre fini d'orbites dans X. Montrer que cette même application induit un isomorphisme de A-algèbres $\mathrm{H}(X) \otimes A \xrightarrow{\sim} \mathrm{H}(X; A)$.

L'exercice suivant repose sur l'Exercice 3.1.

Exercice 3.2. *On suppose que le groupe fini G agit sur l'ensemble fini X. On voit $\mathbb{C}[X]$ comme une représentation linéaire de G de dimension finie. On se propose de montrer que $\mathrm{H}(X)$ est commutatif si, et seulement si, cette représentation est sans multiplicité (i.e. chacune des représentations irréductibles de G n'apparaît au plus qu'une fois dans sa décomposition en irréductible).*

(i) Montrer que $\mathrm{H}(X)$ est commutatif si, et seulement si, $\mathrm{H}(X; \mathbb{C})$ l'est.

(ii) On écrit $\mathbb{C}[X] \simeq \oplus_{i=1}^r V_i^{n_i}$ où les V_i sont des représentations irréductibles de G deux-à-deux non isomorphes, et les n_i sont des entiers ≥ 1. Montrer que $\mathrm{H}(X; \mathbb{C})$ est isomorphe comme $\mathbb{C}$-algèbre à $\prod_{i=1}^r \mathrm{M}_{n_i}(\mathbb{C})$.

(iii) Conclure.

Exercice 3.3. *Soit n un entier ≥ 4 et X l'ensemble des parties à 2 éléments de $\{1, 2, \ldots, n\}$. Le groupe symétrique $G = \mathrm{S}_n$ agit transitivement sur X. Montrer que les orbites de S_n sur $X \times X$ sont les parties $\Omega_i = \{(P, Q), |P \cap Q| = i\}$, avec $i = 0, 1, 2$. Déterminer $\mathrm{c}_{\Omega_i}\mathrm{c}_{\Omega_j}$.*

Exercice 3.4. *Montrer que V est un $\mathbb{Q}$-espace vectoriel de dimension 1, alors l'anneau $\mathrm{H}(\mathrm{R}(V))$ est canoniquement isomorphe à l'anneau de groupe $\mathbb{Z}[\mathbb{Q}_{>0}]$ (où $\mathbb{Q}_{>0}$ est vu comme groupe multiplicatif).*

Exercice 3.5. *On se propose de montrer que l'anneau* $\mathrm{H}(\mathrm{R}(V))$*, V étant un $\mathbb{Q}$-espace vectoriel de dimension finie, ne dépend canoniquement que de* $\dim V$*. On fixe pour cela U et V deux $\mathbb{Q}$-espaces vectoriel de même dimension.*

(i) Soit $\varphi : U \to V$ un isomorphisme. On note $\mathrm{m}_\varphi : \mathbb{Z}[\mathrm{R}(U)] \xrightarrow{\sim} \mathbb{Z}[\mathrm{R}(V)]$ l'application linéaire envoyant $[L]$ sur $[\varphi(L)]$. Vérifier que l'application $T \mapsto \mathrm{m}_\varphi^{-1} \circ T \circ \mathrm{m}_\varphi$ définit un morphisme d'anneaux $\mathrm{H}(\varphi) : \mathrm{H}(V) \longrightarrow \mathrm{H}(U)$.

(i) Montrer que $\mathrm{H}(\varphi)$ ne dépend pas du choix de φ : si $\varphi' : U \to V$ un second isomorphisme, on a $\mathrm{H}(\varphi') = \mathrm{H}(\varphi)$.

Exercice 3.6. *Soit $L \subset \mathbb{R}^n$ un réseau tel que $\{g(L), g \in \mathrm{GL}_n(\mathbb{Z})\}$ est fini. On se propose de montrer qu'il existe $\lambda \in \mathbb{R}^\times$ tel que $\lambda L \subset \mathbb{Z}^n$. On notera $\mathrm{E}_{i,j}$ l'élément de $\mathrm{M}_n(\mathbb{Z})$ dont le seul coefficient $\neq 0$ est 1, et d'indice (i,j).*

(i) Montrer qu'il existe un entier $N \geq 1$ tel que $g^N L \subset L$ pour tout $g \in \mathrm{GL}_n(\mathbb{Z})$.

(ii) (suite) En déduire $(\mathrm{I}_n + N\,\mathrm{E}_{i,j})\,L \subset L$ pour $i \neq j$, puis $\mathrm{M}_n(\mathbb{Z})\,N^2 L \subset L$.

(iii) Soit $P \in \mathrm{GL}_n(\mathbb{R})$ vérifiant $P\,\mathrm{M}_n(\mathbb{Q})\,P^{-1} = \mathrm{M}_n(\mathbb{Q})$. Montrer qu'il existe $\lambda \in \mathbb{R}^\times$ avec $\lambda P \in \mathrm{GL}_n(\mathbb{Q})$.

(iv) Conclure.

(Application) *En déduire que si V est un $\mathbb{R}$-espace vectoriel de dimension finie, tout élément de $\mathrm{H}(\mathrm{R}(V))$ est une combinaison linéaire à coefficients dans $\mathbb{Z}$ d'éléments de la forme $\mathrm{R}_\lambda T$ avec $T \in \mathrm{H}(\mathrm{R}(V))^{\mathrm{rat}}$ et $\lambda \in \mathbb{R}^\times$.*

Exercice 3.7. *Soient $k \in \mathbb{Z}$ et $s \in \mathbb{C}$ avec $\mathrm{Re}\, s + k > 2$. On pose $\chi(\lambda) = \lambda^{-k}|\lambda|^{-s}$. Montrer que $\mathrm{G}_{k;s}$ est vecteur propre de $\mathrm{T}(p)$ de valeur propre $1 + \chi(p)^{-1}p$.*

CHAPITRE 4

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

Dans ce chapitre, nous introduisons la notion de forme automorphe, au sens donné par Harish-Chandra (voir la référence ci-dessous). Dans un cadre très général, on fixe un groupe de Lie réel G qui est linéaire et réductif, ce que l'on peut traduire en disant que G se plonge comme sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$ stable par $g \mapsto {}^t g$, ainsi qu'un sous-groupe discret $\Gamma \subset G$ d'origine arithmétique. La problématique à laquelle s'intéresse Harish-Chandra, tout comme d'autres mathématiciens de l'époque comme Selberg, Gelfand, Piatetski-Shapiro et Langlands, est de décrire "à la Fourier" l'espace des fonctions de carré intégrable $\mathrm{L}^2(\Gamma\backslash G)$ (pour la mesure de Haar), en tant que représentation du groupe G pour les translations à droite. Les formes automorphes sont les fonctions spéciales qui interviennent dans la description finale du résultat. C'est en étudiant l'exemple important des séries d'Eisenstein que Langlands a découvert les conjectures très générales qui portent sont nom entre formes automorphes et fonctions L.

La définition précise d'une forme automorphe est relative à un choix (inessentiel) d'un sous-groupe compact maximal K de G. Une forme automorphe de G pour le sous-groupe Γ est alors une fonction $f : G \to \mathbb{C}$ de classe $\mathcal{C}^\infty$ telle que :

(1) $f(\gamma g) = f(g)$ pour tout $\gamma \in \Gamma$ et tout $g \in G$ (invariance à gauche sous Γ),

(2) les translatés à droite de f par tous les éléments de K engendrent un sous-espace de dimension finie (symétrie "maximale" vis-à-vis de l'action de K),

(3) les fonctions $z.f$, où z parcourt les opérateurs différentiels bi-invariants sur G, forment un sous-espace de dimension finie (système d'équations différentielles),

(4) f et toutes ses dérivées par rapport à $\mathrm{Lie}\, G$ sont à croissance modérée (condition de croissance).

Pour éviter trop de rappels en théorie de Lie, théorie qui ne sera pas supposée ici, nous nous restreindrons au cas (essentiel) du groupe $G = \mathrm{GL}_n(\mathbb{R})$. La première partie du chapitre aura alors pour but principal de déchiffrer la condition (3) dans ce contexte. Dans la seconde partie du chapitre, nous montrerons que les formes modulaires étudiées aux chapitres 2 et 3 ne sont rien d'autre que des formes automorphes particulières de $\mathrm{GL}_2(\mathbb{R})$ pour le sous-groupe $\mathrm{GL}_2(\mathbb{Z})$.

Références : D. Bump, *Automorphic forms and representations* (1996),

W. Casselman, *Analysis on* SL(2), notes de cours.

Harish-Chandra, *Automorphic forms on semisimple Lie groups* (1968),

J. Dixmier, *Algèbres enveloppantes* (1974),

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

1. Le groupe de Lie $\mathrm{GL}_n(\mathbb{R})$

Soit $n \geq 1$ un entier. On considère le groupe $G = \mathrm{GL}_n(\mathbb{R})$. C'est un groupe topologique, et même un groupe de Lie, de manière naturelle. En effet, c'est une variété différentiable en tant qu'ouvert de l'espace vectoriel $\mathrm{M}_n(\mathbb{R})$ (défini par $\det \neq 0$), et la multiplication $(g,h) \to gh$ et l'inversion $g \to g^{-1}$ sont des applications de classe $\mathcal{C}^\infty$: elles sont même polynomiales en les coefficients $g_{i,j}$ de g, et en la fonction $g \mapsto \det(g)^{-1}$.

L'algèbre de Lie $\mathfrak{g}$ de G s'identifie de manière naturelle à l'espace des matrices $\mathrm{M}_n(\mathbb{R})$, muni de son crochet de Lie usuel $[X,Y] = XY - YX$. En particulier, l'exponentielle de matrices $X \mapsto e^X = \sum_{n\geq 0} \frac{X^n}{n!}, \mathfrak{g} \to G$, est une application de classe $\mathcal{C}^\infty$ qui est un difféomorphisme d'un voisinage ouvert assez petit de $0 \in \mathfrak{g}$ sur un voisinage ouvert de 1 dans G (une réciproque étant donnée par le logarithme matriciel, sur un voisinage assez petit de 1).

On note $\mathcal{C}^\infty(G)$ l'espace vectoriel des fonctions $G \to \mathbb{C}$ qui sont de classes $\mathcal{C}^\infty$. Si $g \in G$ et $f \in \mathcal{C}^\infty(G)$, la fonction $h \mapsto f(hg)$ est dans $\mathcal{C}^\infty(G)$, on la note $\mathrm{R}_g f$. L'application $(g,f) \mapsto \mathrm{R}_g f$ définit une représentation linéaire de G sur $\mathcal{C}^\infty(G)$ (“translations à droite"). On définit de même une autre représentation de G sur $\mathcal{C}^\infty(G)$ par $(g,f) \mapsto \mathrm{L}_g f$ ("translations à gauche") où $\mathrm{L}_g f$ désigne la fonction $h \mapsto f(g^{-1}h)$). Ces opérations commutent manifestement : on $\mathrm{R}_g \circ \mathrm{L}_h = \mathrm{L}_h \circ \mathrm{R}_g$ pour tous $g,h \in G$.

Par différenciation, on en déduit des actions de $\mathfrak{g}$ sur $\mathcal{C}^\infty(G)$ de la manière suivante. Il nous suffira dans la suite de considérer l'action par translations à droite (l'autre cas étant de toutes façons similaire). Soient $X \in \mathfrak{g}$, $f \in \mathcal{C}^\infty(G)$ et $g \in G$. La fonction d'une variable réelle $t \mapsto f(ge^{tX})$ est $\mathcal{C}^\infty$ (comme composée !) et on pose

$$(\mathrm{R}_X f)(g) = \frac{\partial}{\partial t}_{|t=0} f(ge^{tX}) = \lim_{t\to 0} \frac{f(ge^{tX}) - f(g)}{t}.$$

La fonction $G \times \mathbb{R} \to \mathbb{C}, (g,t) \mapsto f(ge^{tX})$ étant de classe $\mathcal{C}^\infty$, on a $\mathrm{R}_X f \in \mathcal{C}^\infty(G)$. Pour $g \in \mathrm{GL}_n(\mathbb{R})$ et $X \in \mathrm{M}_n(\mathbb{R})$, la formule $ge^{tX} = g + tgX + O(t^2)$ quand $t \to 0$ montre que l'on a en fait

$$\mathrm{R}_X f(g) = \mathrm{d}f_g(gX), \tag{22}$$

où $\mathrm{d}f_g : \mathrm{M}_n(\mathbb{R}) \to \mathbb{C}$ désigne la différentielle de f au point g.

Proposition 4.1. *L'application $\mathfrak{g} \times \mathcal{C}^\infty(G) \to \mathcal{C}^\infty(G)$, $(X,f) \mapsto \mathrm{R}_X f$ définit une représentation de l'algèbre de Lie $\mathfrak{g}$ sur $\mathcal{C}^\infty(G)$: c'est une application bilinéaire, et l'on a pour tout $X,Y \in \mathfrak{g}$ la relation $\mathrm{R}_X \circ \mathrm{R}_Y - \mathrm{R}_Y \circ \mathrm{R}_X = \mathrm{R}_{[X,Y]}$. De plus, pour tout $g \in G$ et tout $X \in \mathfrak{g}$ on a les identités*

$$\mathrm{L}_g \circ \mathrm{R}_X = \mathrm{R}_X \circ \mathrm{L}_g \text{ et } \mathrm{R}_g \circ \mathrm{R}_X \circ \mathrm{R}_g^{-1} = \mathrm{R}_{gXg^{-1}}.$$

Démonstration — La $\mathbb{R}$-bilinéarité de $(X,f) \mapsto \mathrm{R}_X f$ est claire sur la formule (22). Vérifions l'égalité $\mathrm{R}_X\mathrm{R}_Y - \mathrm{R}_Y\mathrm{R}_X = \mathrm{R}_{[X,Y]}$ pour $X,Y \in \mathfrak{g}$. Fixons pour cela $g \in G$ ainsi que $X,Y \in \mathrm{M}_n(\mathbb{R})$. Regardons l'application $\varphi_{X,Y} : \mathbb{R}\times\mathbb{R} \to \mathbb{C}, (u,v) \mapsto f(ge^{uX}e^{vY})$. Elle est manifestement de classe $\mathcal{C}^\infty$. Par définition $(\mathrm{R}_X\mathrm{R}_Y f)(g)$ est la

dérivée en $u=0$ de la fonction $u \mapsto (\mathrm{R}_Y f)(ge^{uX}) = \frac{\partial \varphi_{X,Y}}{\partial v}(u,0)$. On a donc

$$(\mathrm{R}_X \mathrm{R}_Y f)(g) = \frac{\partial^2}{\partial u \partial v} \varphi_{X,Y}(0,0). \tag{23}$$

Écrivons maintenant le développement de Taylor de f au point $g \in \mathrm{M}_n(\mathbb{R})$. On a

$$f(g+H) = f(g) + \mathrm{d}f_g(H) + \mathrm{Q}f_g(H) + \mathrm{o}(||H||^2)$$

pour $H \to 0$ dans $\mathrm{M}_n(\mathbb{R})$, où $\mathrm{Q}f_g : \mathrm{M}_n(\mathbb{R}) \to \mathbb{C}$ est la $\mathbb{R}$-forme quadratique Hessienne au point g. Posons $P_{X,Y}(u,v) = uv\,XY + \frac{u^2}{2}\,X^2 + \frac{v^2}{2}\,Y^2$, c'est un polynôme homogène de degré 2 de $\mathbb{R}^2$ dans $\mathrm{M}_n(\mathbb{R})$; il vérifie la relation $e^{uX}e^{vY} = 1 + uX + vY + \mathrm{q}_{X,Y}(u,v) + o(||(u,v)||^2)$ pour $(u,v) \to (0,0)$. On peut donc écrire :

$$\varphi_{X,Y}(u,v) \;=\; f(g) + \mathrm{d}f_g(u\,gX + v\,gY + g\,\mathrm{P}_{X,Y}(u,v)\,) + \mathrm{Q}f_g(\,u\,gX + v\,gY\,) + \mathrm{o}(||(u,v)||^2).$$

L'identité $P_{X,Y}(u,v) - P_{Y,X}(u,v) = uv[X,Y]$ entraîne au final

$$\varphi_{X,Y}(u,v) - \varphi_{Y,X}(u,v) \;=\; uv\,(\mathrm{R}_{[X,Y]}f)(g) \;+\; \mathrm{o}\,(||(u,v)||^2),$$

ce qui conclut l'égalité $\mathrm{R}_X\mathrm{R}_Y - \mathrm{R}_Y\mathrm{R}_X = \mathrm{R}_{[X,Y]}$ par la Formule (23). Les deux identités de la dernière assertion découlent trivialement de la définition. □

Notons que l'action de $\mathfrak{g}$ sur $\mathcal{C}^\infty(G)$ ainsi définie est très concrète. Pour $1 \leq p,q \leq n$, notons $\mathrm{E}_{p,q} \in \mathrm{M}_n(\mathbb{R})$ la matrice élémentaire d'indice (p,q) : on a $\mathrm{E}_{p,q} = (m_{i,j})$ avec $m_{i,j} = 0$ si $(i,j) \neq (p,q)$ et $m_{p,q} = 1$. La relation $e^{tE_{p,q}} = 1 + tE_{p,q} + o(t)$ pour tout $t \in \mathbb{R}$, et une application directe de la définition, montrent que dans les coordonnées $(m_{i,j})$ évidentes sur $\mathrm{M}_n(\mathbb{R})$ on a pour $f \in \mathcal{C}^\infty(G)$

$$\mathrm{R}_{E_{p,q}}\, f \;=\; \sum_{i=1}^{n} m_{i,p}\, \frac{\partial\, f}{\partial\, m_{i,q}}. \tag{24}$$

L'endomorphisme $f \mapsto \mathrm{R}_{E_{p,q}} f$, ainsi donc que tous les R_X qui ne sont que des combinaisons linéaires à coefficients dans $\mathbb{R}$ de ceux-ci, est un opérateur différentiel de degré 1 à coefficients polynomiaux en les $(m_{i,j})$, qui a la propriété remarquable d'être invariant par translations à gauche comme on l'a vu.

Proposition 4.2. *(Poincaré-Birkhoff-Witt) Soient $X_1, \ldots, X_r$ les $r := n^2$ éléments de $\mathfrak{g}$ de la forme $\mathrm{E}_{p,q}$, ordonnés de manière arbitraire. Alors les éléments $\mathrm{R}_{X_\alpha} := \mathrm{R}_{X_1}^{\alpha_1} \circ \mathrm{R}_{X_2}^{\alpha_2} \circ \cdots \circ \mathrm{R}_{X_r}^{\alpha_r}$, avec $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r) \in \mathbb{N}^r$, sont des endomorphismes $\mathbb{C}$-linéairement indépendants de $\mathcal{C}^\infty(G)$.*

Démonstration — Pour tout $i = 1, \ldots, r$, il existe un unique (p,q) tel que $X_i = \mathrm{E}_{p,q}$, et l'on note x_i la fonction $G \to \mathbb{C}$ définie par $x_i(g) = g_{p,q} - \delta_{p,q}$. Autrement dit, les x_i ne sont autres que les fonctions coordonnées naturelles sur G (coefficients matriciels) translatées de sorte que l'on ait $x_i(1) = 0$ pour tout i. La formule (24) montre que l'on a une expression de la forme

$$\mathrm{R}_{X_i} = \frac{\partial}{\partial x_i} + D_i$$

où D_i est une somme finie d'opérateurs de la forme $x_k \frac{\partial}{\partial x_l}$. Introduisons le sous-anneau $A = \mathbb{C}[x_1, \ldots, x_r] \subset \mathcal{C}^\infty(G)$ (fonctions polynomiales en les coefficients matriciels), ainsi que son idéal $I = (x_1, \ldots, x_r)$ des fonctions dans A qui s'annulent en $1 \in G$. L'anneau A est manifestement préservé par R_{X_i} pour tout i. Mieux, on a

$$D_i(I^k) \subset I^k \ \textit{et} \ \frac{\partial}{\partial x_i} I^k \subset I^{k-1}$$

pour tout $i = 1, \ldots, r$ et pour tout $k \geq 0$ (en posant $I^0 = I^{-1} = A$). On en déduit que pour des indices arbitraires $1 \leq i_1, \ldots, i_h \leq d$, et pour $f \in I^k$ avec $k \geq h$, on a

$$\mathrm{R}_{X_{i_1}} \circ \mathrm{R}_{X_{i_2}} \circ \cdots \circ \mathrm{R}_{X_{i_h}} f - \frac{\partial^h}{\partial x_{i_1} \cdots \partial x_{i_h}} f \ \in \ I^{k-h+1}. \tag{25}$$

Supposons enfin que l'on ait une relation de dépendance linéaire finie de la forme

$$\sum_\alpha \lambda_\alpha \mathrm{R}_{X_\alpha} = 0$$

dans les endomorphismes de $\mathcal{C}^\infty(G)$. Soit $h \geq 0$ l'entier maximal tel qu'il existe un multi-indice α avec $\lambda_\alpha = 0$ et $h = \sum_i \alpha_i$. Soit β un multi-indice arbitraire tel que $\sum_i \beta_i \leq h$. On applique la formule (25) à R_{X_β}, $k = h$ et $f = \prod_i x_i^{\alpha_i}$. On en déduit $\mathrm{R}_{X_\beta} f \in I$ pour $\beta \neq \alpha$, et $\mathrm{R}_{X_\alpha} f - \prod_i (\alpha_i!) \in I$. On en tire que la constante $\lambda_\alpha \prod_{i=1}^r (\alpha_i!)$ est dans I, puis $\lambda_\alpha \prod_{i=1}^r (\alpha_i!) = 0$ (évaluation en 1) : une contradiction. □

Ce résultat a des conséquences intéressantes sur la structure de la sous-$\mathbb{C}$-algèbre de $\mathrm{End}(\mathcal{C}^\infty(G))$ engendrée par les R_X avec $X \in \mathfrak{g}$.

2. Algèbres enveloppantes

Dans cette partie, k désignera un corps de caractéristique 0. On rappelle qu'une k-algèbre de Lie sur est la donnée d'un k-espace vectoriel $\mathfrak{g}$ muni d'une application k-bilinéaire $(x, y) \to [x, y], \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ (appelée *crochet de Lie*) vérifiant $[x, x] = 0$ et $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ pour tous $x, y, z \in \mathfrak{g}$ (*identités de Jacobi*). On dispose d'une notion évidente de sous-algèbre de Lie (=sous-espace vectoriel stable par le crochet), de somme directe d'algèbres de Lie (somme directe des espaces munie de la somme des crochets), de morphisme $\mathfrak{g} \to \mathfrak{h}$ entre k-algèbres de Lie (=application k-linéaire f vérifiant $f([x, y]) = [f(x), f(y)]$) etc...

Pour toute k-algèbre associative A, $[x, y] := xy - yx$ munit le k-espace vectoriel A d'une structure de k-algèbre de Lie ; qui sera notée $\underline{A}$. En particulier, V est un k-espace vectoriel, on dispose de la k-algèbre de Lie $\underline{\mathrm{End}_k(V)}$, souvent notée $\mathfrak{gl}(V)$, et même $\mathfrak{gl}_n(k)$ si $V = k^n$. Bien entendu, $\mathfrak{gl}_n(k)$ n'est autre que le k-espace vectoriel $\mathrm{M}_n(k)$ des matrices carrées de taille n, munie répétons-le du crochet $(x, y) \mapsto xy - yx$.

Une *représentation* de la k-algèbre de Lie $\mathfrak{g}$ est la donnée d'un espace vectoriel V et d'un morphisme $\mathfrak{g} \longrightarrow \mathfrak{gl}(V)$. Par définition, il est équivalent de se donner un tel morphisme et une application k-bilinéaire $(x, v) \mapsto xv$ vérifiant $x(yv) - y(xv) = [x, y]v$ pour tout $x, y \in \mathfrak{g}$ et tout $v \in V$. Il est utile de remarquer que les identités de Jacobi sont équivalentes à demander que le crochet $(x, y) \mapsto [x, y]$ est une représentation de $\mathfrak{g}$ sur elle-même ; c'est la *représentation adjointe*.

Définition 4.3. *Si $\mathfrak{g}$ est une k-algèbre de Lie, son* algèbre enveloppante *est le quotient de la k-algèbre tensorielle (associative, mais non commutative en général)*

$$\bigoplus_{n\geq 0} \mathfrak{g}^{\otimes n}$$

son idéal bilatère engendré par tous les éléments de la forme $x\otimes y - y\otimes x - [x,y]$ avec $x, y \in \mathfrak{g}$ (vus comme éléments de degré 1 dans l'algèbre tensorielle). C'est une k-algèbre associative notée $\mathrm{U}(\mathfrak{g})$, munie d'un morphisme canonique $\mathfrak{g} \to \underline{\mathrm{U}(\mathfrak{g})}$.

En composant les propriétés universelles de l'algèbre tensorielle et celle d'un quotient, on obtient la propriété universelle suivante pour $\mathrm{U}(\mathfrak{g})$:

Scholie 4.4. *Si A est une k-algèbre associative, tout morphisme $\mathfrak{g} \to \underline{A}$ s'étend de manière unique en un morphisme de k-algèbres $\mathrm{U}(\mathfrak{g}) \to A$, et l'application ainsi définie $\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g}, \underline{A}) \to \mathrm{Hom}_{k-\mathrm{Alg}}(\mathrm{U}(\mathfrak{g}), A)$ est bijective.*

En particulier, se donner une représentation de $\mathfrak{g}$ sur le k-espace vectoriel V est la même chose que se donner une structure de $\mathrm{U}(\mathfrak{g})$-module sur V (c'est le cas particulier $A = \mathrm{End}_k V$), de sorte que l'on retombe dans un monde familier.

Si an a $x_1, x_2, \ldots, x_p \in \mathfrak{g}$, on note en général $x_1 x_2 \ldots x_p$ leur produit dans $\mathrm{U}(\mathfrak{g})$, plûtot que $x_1 \otimes x_2 \otimes \cdots \otimes x_p$. On prendra garde, dans le cas $\mathfrak{g} = \mathrm{gl}_n(k) = \underline{\mathrm{M}_n(k)}$, que ce produit n'est pas le produit des matrices $x_1, \cdots, x_p$. Par la propriété universelle ci-dessus appliquée à l'identité de $\underline{\mathrm{M}_n(k)}$, on dispose bien d'une surjection canonique $\mathrm{U}(\mathfrak{gl}_n(k)) \to \mathrm{M}_n(k)$, mais on verra ci-après que $\mathrm{U}(\mathfrak{g})$ est de dimension infinie sur k en général.

Si $n \geq 0$ est un entier, on note $\mathrm{U}_n(\mathfrak{g})$ le sous-espace vectoriel engendré par les produits $x_1 x_2 \ldots x_p$ avec $p \leq n$ et $x_i \in \mathfrak{g}$ pour tout i. On convient $\mathrm{U}_{-1}(\mathfrak{g}) = 0$. Les propriétés suivantes sont immédiates :

(a) $\mathrm{U}(\mathfrak{g})$ est la réunion croissante des $\mathrm{U}_n(\mathfrak{g})$ pour $n \geq 0$,

(b) $\mathrm{U}_n(\mathfrak{g})\mathrm{U}_m(\mathfrak{g}) \subset \mathrm{U}_{n+m}(\mathfrak{g})$ pour tout $n, m \geq 0$,

(c) $\mathrm{U}_1(\mathfrak{g})^n$ engendre k-linéairement $\mathrm{U}_n(\mathfrak{g})$ pour $n \geq 0$,

(d) pour tout $u \in \mathrm{U}_n(\mathfrak{g})$ et $v \in \mathrm{U}_m(\mathfrak{g})$, on a $uv - vu \in \mathrm{U}_{n+m-1}(\mathfrak{g})$.

Cette dernière se démontre par récurrence immédiate à partir de la relation $xy - yx = [x,y] \in \mathrm{U}_1$ pour $x, y \in \mathfrak{g}$. Considérons l'espace vectoriel gradué associé $\mathrm{gr}\,\mathrm{U}(\mathfrak{g}) = \bigoplus_{n\geq 0} \mathrm{U}_n(\mathfrak{g})/\mathrm{U}_{n-1}(\mathfrak{g})$. Les observations ci-dessus montrent que la multiplication dans $\mathrm{U}(\mathfrak{g})$ induit une structure de k-algèbre commutative sur $\mathrm{gr}\,\mathrm{U}(\mathfrak{g})$. L'application naturelle $\mathfrak{g} \to \mathrm{U}_1(\mathfrak{g}) \to \mathrm{gr}(\mathrm{U}(\mathfrak{g}))$ induit donc par construction un homomorphisme de k-algèbres

$$\mathrm{Sym}\,\mathfrak{g} \longrightarrow \mathrm{gr}\,\mathrm{U}(\mathfrak{g}). \tag{26}$$

qui est surjectif par (c).

Théorème 4.5. *(Poincaré-Birkhoff-Witt) On suppose $k = \mathbb{C}$ et $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{C})$. Alors :*

(a) l'homomorphisme (26) *est un isomorphisme,*

(b) si $X_1, \ldots, X_r$ une $\mathbb{C}$-base de $\mathfrak{g}$ alors les $X_\alpha := X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$, avec $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, forment une $\mathbb{C}$-base de $\mathrm{U}(\mathfrak{g})$,

(c) le morphisme naturel $\mathrm{U}(\mathfrak{g}) \longrightarrow \mathrm{End}(\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{R})))$, défini par la structure de $\mathfrak{gl}_n(\mathbb{C}) = \mathfrak{gl}_n(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C}$-module sur $\mathcal{C}^\infty(G)$ donnée par la Proposition 4.2, est injectif.

Démonstration — Soit $X_1, \ldots, X_r$ une base de $\mathfrak{g}$ provenant d'une $\mathbb{R}$-base de $\mathrm{gl}_n(\mathbb{R})$ comme dans l'énoncé de la proposition 4.2. Les X_α associés engendrent manifestement $\mathrm{U}(\mathfrak{g})$. Mais cette proposition montre qu'ils sont linéairement indépendants, car c'est le cas de leur image dans $\mathrm{End}\,(\mathcal{C}^\infty(\mathrm{GL}_n(\mathbb{R})))$. On a montré (c) ainsi que (b) pour la base spécifique ci-dessus.

Il est clair que si $X_1, \ldots, X_r$ est une k-base quelconque de $\mathfrak{g}$, la propriété (d) précédent l'énoncé du théorème montre que les monômes X_α de l'énoncé avec $\sum_i \alpha_i \leq n$ forment une famille génératrice de $\mathrm{U}_n(\mathfrak{g})$. Ainsi, l'assertion (b) est vraie pour une base $X_1, \ldots, X_r$ si, et seulement si, les images dans $\mathrm{U}_n(\mathfrak{g})/\mathrm{U}_{n-1}(\mathfrak{g})$ des X_α avec $\sum_i \alpha_i = n$ forment une base de ce dernier espace. Comme ces images l'engendrent, if faut et il suffit que la dimension de $\mathrm{U}_n(\mathfrak{g})/\mathrm{U}_{n-1}(\mathfrak{g})$ soit le nombre de α avec $\sum_i \alpha_i = n$. Comme cela ne dépend pas du choix de la base, et qu'on l'a montré pour les $\mathrm{E}_{p,q}$, on a montré (b). L'application k-linéaire sous-jacente à (26) est la somme directe des surjections $\mathrm{Sym}^n \mathfrak{g} \to \mathrm{U}_n(\mathfrak{g})/\mathrm{U}_{n-1}(\mathfrak{g})$. Mais on vient de voir que la source et l'arrivée d'une telle application ont même dimension. □

Notons que si $\mathfrak{h}$ est une sous-algèbre de Lie de $\mathfrak{g}$, on dispose d'un morphisme de k-algèbres évident $\mathrm{U}(\mathfrak{h}) \to \mathrm{U}(\mathfrak{g})$ (autrement dit, la construction $\mathrm{U}(-)$ est un foncteur des algèbres de Lie vers les algèbres associatives). La proposition ci-dessous se déduit immédiatement du point (b) de l'énoncé ci-dessus.

Corollaire 4.6. *Soit $\mathfrak{g} = \mathrm{gl}_n(\mathbb{C})$. Alors :*

(i) l'application canonique $\mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ est injective,

(iii) si $\mathfrak{h}$ est une sous-algèbre de Lie de $\mathfrak{g}$, l'application naturelle $\mathrm{U}(\mathfrak{h}) \to \mathrm{U}(\mathfrak{g})$ est injective,

(iv) supposons que l'on a une décomposition en sous-espaces vectoriels $\mathfrak{g} = \oplus_{i=1}^s \mathfrak{g}_i$ où chaque $\mathfrak{g}_i$ est stable par crochets (i.e. est une sous-algèbre de Lie). Alors l'application naturelle $\mathrm{U}(\mathfrak{g}_1) \otimes \mathrm{U}(\mathfrak{g}_2) \otimes \cdots \otimes \mathrm{U}(\mathfrak{g}_s) \longrightarrow \mathrm{U}(\mathfrak{g})$ est un isomorphisme de $\mathbb{C}$-espaces vectoriels.

Il ne serait pas difficile à ce stade d'étendre le corollaire ci-dessus à toute k-algèbre de Lie de dimension finie sur k qui se plonge dans $\mathrm{gl}_n(k)$ (exercice !), et donc à toute k-algèbre de Lie de dimension finie sur k par le théorème d'Ado.

Exemple : l'algèbre enveloppante de $\mathfrak{gl}_2(\mathbb{C})$

Le centre de l'algèbre de Lie $\mathfrak{gl}_n(\mathbb{C})$ est bien sûr de dimension 1 et engendré par la matrice identité, que nous noterons $Z \in \mathfrak{gl}_n(\mathbb{C})$. On a une décomposition en somme directe

$$\mathfrak{gl}_n(\mathbb{C}) = \mathbb{C}Z \oplus \mathfrak{sl}_n(\mathbb{C})$$

où $\mathfrak{sl}_n(\mathbb{C})$ est la sous-algèbre de Lie constituée des matrices de trace nulle. En particulier, Z est dans le centre de $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$, et le théorème de Poincaré-Birkhoff-Witt

entraîne alors que l'on a un isomorphisme d'algèbres $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C})) \simeq \mathbb{C}[Z] \otimes_{\mathbb{C}} \mathrm{U}(\mathfrak{sl}_n(\mathbb{C}))$. On a bien sûr $\mathrm{U}(\mathfrak{gl}_1(\mathbb{C})) = \mathbb{C}[Z]$, de sorte que le premier cas intéressant est $n = 2$. On pose traditionnellement

$$h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ et } f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Ces éléments e, f et h forment une base de $\mathfrak{sl}_2(\mathbb{C})$ et on a les relations évidentes

$$[h, e] = 2e,\ \ [h, f] = -2f \ \text{ et } \ [e, f] = h,$$

qui déterminent entièrement la structure de l'algèbre de Lie de $\mathfrak{sl}_2(\mathbb{C})$. Par définition de $\mathrm{U}(-)$ on en déduit la présentation suivante (de $\mathbb{C}$-algèbre associative unitaire non nécessairement commutative)

$$\mathrm{U}(\mathfrak{sl}_2(\mathbb{C})) = \mathbb{C}\{e, f, h\}/\langle he - eh = 2e, hf - fh = -2f, ef - fe = h\rangle.$$

D'après le théorème de Poincaré-Birkhoff-Witt, les monômes de la forme $f^a h^b e^c$, avec $(a, b, c) \in \mathbb{N}^3$, forment une base de $\mathrm{U}(\mathfrak{sl}_2(\mathbb{C}))$.

3. Le centre de $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$

Définition 4.7. *Si $\mathfrak{g}$ est une k-algèbre de Lie, on note $\mathfrak{z}(\mathfrak{g})$ le centre de l'algèbre enveloppante $\mathrm{U}(\mathfrak{g})$. C'est une k-algèbre commutative.*

On s'intéresse dans cette partie au cas $\mathfrak{g} := \mathfrak{gl}_n(\mathbb{C})$. Le groupe $\mathrm{GL}_n(\mathbb{C})$ agit naturellement sur $\mathrm{M}_n(\mathbb{C})$ par conjugaison. Cette action est linéaire et définit une représentation de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathrm{M}_n(\mathbb{C})$ appelée *représentation adjointe* et notée $(g, X) \mapsto \mathrm{ad}_g(X) = gXg^{-1}$. La relation $g[X, Y]g^{-1} = [gXg^{-1}, gYg^{-1}]$ montre que ad_g est un automorphisme de l'algèbre de Lie $\mathfrak{g}$. Par fonctorialité de $\mathrm{U}(-)$, $\mathrm{GL}_n(\mathbb{C})$ agit donc par automorphismes de $\mathbb{C}$-algèbres de $\mathrm{U}(\mathfrak{g})$. Cette représentation de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathrm{U}(\mathfrak{g})$ préserve le sous-espace de dimension finie $\mathrm{U}_m(\mathfrak{g})$ pour tout $m \geq 0$.

Proposition 4.8. *L'ensemble des invariants $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))^{\mathrm{GL}_n(\mathbb{C})}$ coincide avec $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$.*

Démonstration — Soient $u \in \mathrm{U}_m(\mathfrak{g})$ et $X \in \mathfrak{g}$. Vérifions que l'élément $uX - Xu$ de $\mathrm{U}(\mathfrak{g})$ est la dérivée en $t = 0$ de la fonction $\mathbb{C} \to \mathrm{U}_m(\mathfrak{g}), t \mapsto \mathrm{ad}_{e^{tX}} u$ (et en particulier que cette dérivée existe, au sens complexe). En effet, c'est immédiat si l'on a $u \in \mathfrak{g}$ étant donnée la relation $e^{tX} u e^{-tX} = u + t(Xu - uX) + O(t^2)$. En général, on peut supposer $u = u_1 \cdots u_m$ avec les $u_i \in \mathfrak{g}$ par multilinéarité, et dans ce cas on constate que la dérivée en question vaut ("dérivée d'un produit") $\sum_{i=1}^m u_1 \cdots u_{i-1}(Xu_i - u_i X)u_{i+1} \cdots u_m$, qui se simplifie bien en $Xu - uX$ (somme télescopique).

On en déduit d'abord que si u est fixe par $\mathrm{GL}_n(\mathbb{C})$, alors on a $Xu = uX$ pour tout $X \in \mathfrak{gl}_n(\mathbb{C})$, ce qui est équivalent à dire que u est dans le centre de $\mathrm{U}(\mathfrak{g})$. Réciproquement, si u est dans le centre de $\mathrm{U}(\mathfrak{g})$ alors la formule ci-dessus montre que la fonction analytique $\varphi(t) := \mathrm{ad}_{e^{tX}}.u$ est donc constante : sa dérivée en $t = 0$ est nulle et on a $\varphi'(t) = e^{tX}.\varphi'(0)$. On a donc $\mathrm{ad}_{e^X} u = u$ pour tout $X \in \mathrm{M}_n(\mathbb{C})$. On conclut car $X \mapsto e^X, \mathrm{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective. □

Nous avons déjà vu que l'élément identité $Z \in \mathfrak{g}$ est dans le centre de l'algèbre $\mathrm{U}(\mathfrak{g})$. Donnons un exemple plus intéressant : l'élément de Casimir. Considérons la trace $\mathrm{M}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$, $(X, Y) \mapsto \mathrm{Tr}(XY)$. C'est une forme bilinéaire symmétrique non dégénérée. Si l'on fait agir $\mathrm{GL}_n(\mathbb{C})$ trivialement sur $\mathbb{C}$, et par la représentation adjointe sur chaque facteur $\mathrm{M}_n(\mathbb{C})$, on constate que la trace est $\mathrm{GL}_n(\mathbb{C})$-équivariante : $\mathrm{Tr}(gXg^{-1} \cdot gYg^{-1}) = \mathrm{Tr}(XY)$. Autrement dit, elle induit un isomorphisme entre la représentation adjointe et sa duale,

$$\mathrm{tr} : \mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*,\ X \mapsto (Y \mapsto \mathrm{Tr}(XY)).$$

On a donc des isomorphismes $\mathrm{GL}_n(\mathbb{C})$-équivariants :

$$\mathfrak{g} \otimes \mathfrak{g} \xrightarrow{1\otimes \mathrm{tr}} \mathfrak{g} \otimes \mathfrak{g}^* \overset{\mathrm{can}}{\xrightarrow{\sim}} \mathrm{End}_{\mathbb{C}}(\mathfrak{g}),$$

le dernier étant l'isomorphisme naturel général $V \otimes_k V^* \simeq \mathrm{End}_k(V)$ existant pour tout k-espace vectoriel de dimension finie. Notons que dans cet isomorphisme, l'identité de V correspond à $\sum_i x_i \otimes x_i^*$, où (x_i) est une base quelconque de V et (x_i^*) est la base duale. L'élément identité de $\mathrm{End}_{\mathbb{C}}(\mathfrak{g})$ étant manifestement $\mathrm{GL}_n(\mathbb{C})$-invariant, il correspond via les isomorphismes ci-dessus à un élément $\mathrm{GL}_n(\mathbb{C})$-invariant $C' \in \mathfrak{g}\otimes\mathfrak{g}$. Compte tenu de la Proposition 4.8, nous avons donc démontré le corollaire suivant.

Corollaire-Définition 4.9. *L'image dans* $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$ *de l'élément* $C' \in \mathfrak{g}l_n(\mathbb{C}) \otimes \mathfrak{g}l_n(\mathbb{C})$ *défini ci-dessus est un élément de* $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$ *appelé* élément de Casimir *(quadratique). Il est noté* C. *Si* (X_i) *est une base de* $\mathfrak{gl}_n(\mathbb{C})$, *et si* (Y_i) *désigne la base duale de* (X_i) *pour la forme trace, alors on a la formule* $C = \sum_i X_i Y_i$.

En guise d'exemple, considérons la base Z, e, f, h de $\mathrm{M}_2(\mathbb{C})$. Sa base duale relativement à la trace est respectivement $\frac{Z}{2}$, $f, e, \frac{h}{2}$. On a donc

$$C = \frac{1}{2}(Z^2 + h^2) + ef + fe. \tag{27}$$

Plus généralement, considérons la base des $\mathrm{E}_{p,q}$ de $\mathrm{M}_n(\mathbb{C})$. Sa base duale relativement à la trace est manifestement celle des $(\mathrm{E}_{q,p})_{p,q}$, de sorte que l'on a

$$C = \sum_{p,q} \mathrm{E}_{p,q}\mathrm{E}_{q,p}. \tag{28}$$

Théorème 4.10. *Le morphisme de* $\mathbb{C}$*-algèbres* $\mathbb{C}[X, Y] \to \mathfrak{z}(\mathfrak{g}l_2(\mathbb{C}))$ *envoyant* X *sur* Z *et* Y *sur* C *est un isomorphisme.*

La fin de cette partie est consacrée à la démonstration de ce théorème. L'entier $n \geq 1$ sera pour l'instant quelconque. On commence par étudier une version graduée de $\mathfrak{z}$: on pose $\mathfrak{z}_m = \mathfrak{z}(\mathfrak{g}) \cap \mathrm{U}_m(\mathfrak{g})$. On dispose encore d'une algèbre graduée associée

$$\mathrm{gr}\,\mathfrak{z} \ = \ \oplus_{m\geq 0}\, \mathfrak{z}_m/\mathfrak{z}_{\mathfrak{m}-1}.$$

Par définition, c'est une sous-algèbre de $\mathrm{gr}\,\mathrm{U}(\mathfrak{g})$ constituée d'éléments $\mathrm{GL}_n(\mathbb{C})$-invariants. L'isomorphisme $\mathrm{Sym}\,\mathfrak{g} \xrightarrow{\sim} \mathrm{gr}\,\mathrm{U}(\mathfrak{g})$ du théorème de Poincaré-Birkhoff-Witt commute manifestement aux actions naturelles de $\mathrm{GL}_n(\mathbb{C})$ des deux côtés. On s'intéresse donc aux $\mathrm{GL}_n(\mathbb{C})$-invariants de l'anneau $\mathrm{Sym}\,\mathfrak{g}$.

Si V est un espace vectoriel de dimension finie sur $\mathbb{C}$, on note $\mathrm{Pol}(V)$ l'algèbre des fonctions polynomiales en les formes linéaires sur V. Elle s'identifie naturellement à l'algèbre symétrique $\mathrm{Sym}\,V^*$ (de manière comptible aux actions naturelles de $\mathrm{GL}(V)$). La $\mathbb{C}$-algèbre $\mathrm{Sym}\,\mathfrak{g}$ s'identifie donc naturellement à $\mathrm{Pol}(\mathfrak{g}^*)$, et même à

$\mathrm{Pol}(\mathfrak{g}) = \mathrm{Pol}(\mathrm{M}_n(\mathbb{C}))$ si l'on utilise l'isomorphisme $\mathrm{tr} : \mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$ plus haut (qui est $\mathrm{GL}_n(\mathbb{C})$-équivariant rappelons-le).

Nous allons utiliser le lemme classique suivant, qui vaut pour tout entier $n \geq 1$. On note $\mathfrak{h} \simeq \mathbb{C}^n \subset \mathrm{M}_n(\mathbb{C})$ le sous-espace des matrices diagonales, et on considère l'action par conjugaison de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathrm{Pol}(\mathrm{M}_n(\mathbb{C}))$, et l'action naturelle du groupe symétrique S_n sur $\mathrm{Pol}(\mathfrak{h}) \simeq \mathbb{C}[t_1, \ldots, t_n]$ par permutation des coordonnées.

Lemme 4.11. *La restriction naturelle* $\mathrm{Pol}(\mathrm{M}_n(\mathbb{C})) \to \mathrm{Pol}(\mathfrak{h})$ *induit un isomorphisme* $\mathrm{Pol}(\mathrm{M}_n(\mathbb{C}))^{\mathrm{GL}_n(\mathbb{C})} \xrightarrow{\sim} \mathrm{Pol}(\mathfrak{h})^{\mathrm{S}_n}$.

Démonstration — L'application est injective car les matrices diagonalisables sont denses dans $\mathrm{M}_n(\mathbb{C})$. Elle est surjective car les coefficients du polynôme caractéristique sont des éléments de $\mathrm{Pol}(\mathrm{M}_n(\mathbb{C}))^{\mathrm{GL}_n(\mathbb{C})}$ qui s'envoient sur les fonctions symmétriques élémentaires, dont il est bien connu qu'elles engendrent $\mathrm{Pol}(\mathfrak{h})^{\mathrm{S}_n}$ (sans relation polynomiale). □

Autrement dit, $\mathrm{Pol}(\mathrm{M}_n(\mathbb{C}))^{\mathrm{GL}_n(\mathbb{C})}$ est exactement l'algèbre des polynômes en les coefficients (d'indice $< n$) du polynôme caractéristique, et ces derniers ne satisfont pas de relation polynomiale non triviale. Nous avons défini ci-dessus un homomorphisme naturel injectif

$$\gamma : \mathrm{gr}\,\mathfrak{z} \longrightarrow \mathrm{Pol}(\mathfrak{g})^{\mathrm{GL}_n(\mathbb{C})}$$

obtenu en composant l'inclusion $\mathrm{gr}\,\mathfrak{z} \subset \mathrm{gr}\,\mathrm{U}(\mathfrak{g})$ et les isomorphismes $\mathrm{gr}\,\mathrm{U}(\mathfrak{g}) \to \mathrm{Pol}(\mathfrak{g}^*)$ (PBW) et $\mathrm{Pol}(\mathfrak{g}^*) \xrightarrow{\sim} \mathrm{Pol}(\mathfrak{g})$ (via tr).

Lemme 4.12. *Soient* $\overline{Z}$ *et* $\overline{\mathrm{C}}$ *les images respectives de* Z *et* C *dans* $\mathfrak{z}_1/\mathfrak{z}_0$ *et* $\mathfrak{z}_2/\mathfrak{z}_1$. *Alors pour tout* $X \in \mathfrak{g}$ *on a* $\gamma(\overline{Z})(X) = \mathrm{Tr}(X)$ *et* $\gamma(\overline{\mathrm{C}})(X) = \mathrm{Tr}(X^2)$.

Démonstration — L'application m-linéaire symétrique $\mathfrak{g}^m \to \mathrm{Pol}(\mathfrak{g})$ induite par composition de l'application naturelle $\mathfrak{g}^m \to \mathrm{Pol}(\mathfrak{g}^*)$ avec l'isomorphisme tr est $(X_1, \ldots, X_m) \mapsto (M \mapsto \mathrm{Tr}(X_1 M) \ldots \mathrm{Tr}(X_m M))$. On en déduit $\gamma(\overline{Z})(X) = \mathrm{Tr}(X)$ pour $m = 1$. Pour $m = 2$, la Formule (28) montre donc :

$$\gamma(\overline{\mathrm{C}})(X) = \sum_{1 \leq p,q \leq n} \mathrm{Tr}(X\mathrm{E}_{p,q})\,\mathrm{Tr}(X\mathrm{E}_{q,p}) = \mathrm{Tr}(X^2).$$

□

Supposons enfin $n = 2$. Le Lemme 4.12 montre que γ est surjectif, car l'anneau des invariants $\mathrm{Pol}(\mathrm{M}_2(\mathbb{C}))^{\mathrm{GL}_2(\mathbb{C})}$ est engendré par $\mathrm{tr}(X)$ et $\mathrm{tr}(X^2)$ d'après le Lemme 4.11. Comme γ est injectif, c'est un isomorphisme, et $\mathrm{gr}\,\mathfrak{z}$ est l'anneau de polynômes $\mathbb{C}[\overline{Z}, \overline{C}]$. Les éléments $\overline{Z}$ et $\overline{C}$ sont algébriquement indépendants sur $\mathbb{C}$ car c'est le cas de $\mathrm{tr}(X)$ et $\mathrm{tr}(X^2)$ dans $\mathrm{Pol}(\mathrm{M}_2(\mathbb{C}))^{\mathrm{GL}_2(\mathbb{C})}$. On en déduit facilement $\mathfrak{z} = \mathbb{C}[Z, C]$, puis le théorème. □

Remarque 4.13. En exhibant d'autres éléments convenables dans $\mathfrak{z}$ on pourrait démontrer que γ est surjectif (et donc un isomorphisme) pour tout entier $n \geq 1$, puis que $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$ est isomorphe à une $\mathbb{C}$-algèbre de polynômes sur n variables (Harish-Chandra).

4. Formes automorphes pour un sous-groupe discret de $\mathrm{GL}_n(\mathbb{R})$

Soient $n \geq 1$ et $G = \mathrm{GL}_n(\mathbb{R})$.

4.1. Le groupe K. On munit $\mathbb{R}^n$ du produit scalaire standard $(x_i) \cdot (y_i) = \sum_i x_i y_i$ et on note $|x| = \sqrt{x \cdot x}$ la norme euclidienne associée. On note $\mathrm{O}(n)$ le groupe orthogonal de cet espace euclidien. C'est le sous-groupe des éléments $g \in G$ tels que ${}^t g\, g = \mathrm{I}_n$. C'est un sous-groupe compact de G, car il est fermé et borné dans $\mathrm{M}_n(\mathbb{R})$, et pour cette raison on le notera aussi K. Son algèbre de Lie $\mathfrak{k} \subset \mathfrak{gl}_n(\mathbb{R})$ est le sous-espace des matrices $X \in \mathrm{M}_n(\mathbb{R})$ vérifiant $e^{tX} \in K$ pour tout $t \in \mathbb{R}$: c'est la sous-algèbre de Lie des matrices anti-symétriques.

La proposition suivante résume quelques unes des propriétés essentielles de K. On note $S \subset \mathrm{GL}_n(\mathbb{R})$ le sous-ensemble des matrices symétriques définies positives et $A \subset S$ le sous-ensemble des matrices diagonales $a = \mathrm{diag}(a_1, \ldots, a_n)$ avec $a_1 \geq a_2 \geq \cdots \geq a_n$. L'ensemble S est stable par inversion, par conjugaison par K, et A stable par produits.

Proposition 4.14. *(i) (Décomposition polaire) Tout élément de G s'écrit de manière unique sous la forme $g = sk$ avec $s \in S$ et $k \in K$,*

(ii) (Décomposition de Cartan) $G = \coprod_{a \in A} KaK$,

(iii) K est un sous-groupe compact maximal de G (pour l'inclusion),

(iv) Tout sous-groupe compact de G est conjugué dans G à un sous-groupe de K.

Démonstration — Un point clé, bien connu, est que tout élément s de S est diagonalisable en base orthonormée (théorème spectral), i.e. $s = kak^{-1}$ avec $a \in A$ et $k \in K$. En particulier, s est le carré de $s' = k\sqrt{a}k^{-1} \in \mathrm{S}$ avec $\sqrt{a} \in A$ l'unique élément vérifiant $\sqrt{a}^2 = a$. On en tire le (i) : si g est dans G on écrit ${}^t g\, g$ (qui est dans S) sous la forme $s^2 = {}^t s\, s$ avec $s \in S$, puis $gs^{-1} \in K$. De plus, (i) et le théorème spectral impliquent $G = \bigcup_{a \in A} KaK$. Pour le caractère *disjoint* de cette dernière réunion, on constate que si $g = kak'$ avec $a = \mathrm{diag}(a_1, \ldots, a_n) \in A$ et $k, k' \in K$, alors on a $a_1 = \mathrm{Sup}_{|x|=1} |g(x)|$. L'unicité des a_i avec $i > 1$ résulte, par récurrence, d'un argument similaire effectué dans l'espace euclidien $\Lambda^i \mathbb{R}^n$, et conclut le (vi). Si $a \in A$ est tel que $\{a^n, n \in \mathbb{Z}\}$ est borné dans G, alors on constate que l'on a $a = 1$, de sorte que (iii) se déduit de $G = \bigcup_{a \in A} KaK$. Il ne reste qu'à vérifier (iv). Soit $H \subset G$ un sous-groupe compact. Si $\mathrm{d}h$ désigne une mesure de Haar (à droite !) sur H, on constate que

$$\langle x, y \rangle = \int_H hx \cdot hy \, \mathrm{d}h$$

est un produit scalaire sur $\mathbb{R}^n$ qui est invariant par H. Si $g \in G$ désigne un élément envoyant une base orthonormée arbitraire pour $\langle x, y \rangle$ sur la base canonique de $\mathbb{R}^n$, on a $\langle x, y \rangle = gx \cdot gy$ pour tous $x, y \in \mathbb{R}^n$, puis $gHg^{-1} \subset K$. □

La théorie des représentations continues et unitaires des groupes compacts sur des espaces de Hilbert est un chapitre classique des mathématiques, avec des contributions fameuses et importantes de Hermann Weyl. Une telle représentation est la donnée d'un espace de Hilbert V et d'un morphisme de groupes $\rho : G \to \mathrm{U}(V)$ tel que pour tout $v \in V$ l'application orbite $G \to V, g \mapsto \rho(g)v$, est continue. Un résultat central de cette théorie est qu'une telle représentation est toujours somme orthogonale Hilbertienne de sous-représentations irréductibles et de dimension finie. Dans le cas particulier, mais crucial, où V est l'espace des fonctions de carré intégrable sur K pour une mesure de Haar, et où $K = \mathrm{O}(n)$, c'est une conséquence relativement simple du théorème de Stone-Weierstrass : les polynômes en les coefficients matriciels forment une sous-algèbre dense (et ce même pour la norme sup.). C'est l'esprit de la définition suivante (pour laquelle nous pouvons oublier ce que l'on vient de dire).

Définition 4.15. (Vecteurs K-finis) *Soit V un $\mathbb{C}$-espace vectoriel muni d'une représentation linéaire du groupe K. Un vecteur $v \in V$ est K-fini si le sous-espace vectoriel de V engendré de par les $k \cdot v$ avec $k \in K$ est de dimension finie sur $\mathbb{C}$. L'ensemble des vecteurs K-finis de V est un sous-espace vectoriel stable par K.*

De même, si V est un module sur une $\mathbb{C}$-algèbre A, un vecteur $v \in V$ est A-fini si le sous-espace vectoriel de V constitué des éléments de la forme $a \cdot v$ avec $a \in A$ est de dimension finie sur $\mathbb{C}$. L'ensemble des vecteurs A-finis de V est un sous-A-module de V.

Cette définition s'applique en particulier à la restriction à K de l'action de G par translations à droite sur $\mathcal{C}^\infty(G)$, via $(g, f) \mapsto \mathrm{R}_g f$. Autrement dit, la fonction $f \in \mathcal{C}^\infty(G)$ est K-finie (à droite, si l'on veut rappeler que l'on s'intéresse aux translations à droite) si le sous-espace vectoriel de $\mathrm{C}^\infty(G)$ engendré par tous les translatés $\mathrm{R}_k f$, avec k parcourant K, est de dimension finie. De même, on a vu que la dérivation des translations à droite par G permet de munir $\mathrm{C}^\infty(G)$ d'une structure de $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$-module de manière naturelle, et donc à fortiori de $\mathfrak{z}$-module. Une fonction $f \in \mathcal{C}^\infty(G)$ est donc $\mathfrak{z}$-finie (pour cette action) si le sous-espace vectoriel $\mathfrak{z}.f \subset \mathrm{C}^\infty(G)$ est de dimension finie.

4.2. Définition des formes automorphes. Nous sommes désormais en mesure de donner la définition d'une forme automorphe. On fixe un sous-groupe discret Γ de G. Les exemples importants pour la suite sont $\Gamma = \mathrm{GL}_n(\mathbb{Z})$, ou Γ un sous-groupe d'indice fini de $\mathrm{GL}_n(\mathbb{Z})$ (voire un sous-groupe de congruence).

Définition 4.16. *Une fonction $f \in \mathcal{C}^\infty(G)$ est une forme automorphe pour Γ si elle vérifie les conditions suivantes :*

(AF1) $f(\gamma g) = f(g)$ pour tout $\gamma \in \Gamma$ et pour tout $g \in G$,

(AF2) f est K-finie à droite,

(AF3) f est $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$-finie,

(AF4) Pour tout $u \in \mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$, la fonction $u.f$ est à croissance modérée.

Les formes automorphes pour Γ forment un sous-espace vectoriel de $\mathcal{C}^\infty(G)$ noté $\mathrm{A}(G\,;\Gamma)$.

Pour que cette définition ait un sens, il ne reste qu'à expliquer ce qu'est une fonction à croissance modérée sur G. Pour cela, on commence par plonger $\mathrm{GL}_n(\mathbb{R})$ dans $\mathrm{M}_{n+1}(\mathbb{R})$ de la manière diagonale évidente $\iota(g) = (g, \det(g)^{-1})$. On voit $\mathrm{M}_{n+1}(\mathbb{R})$ comme espace euclidien pour le produit scalaire $(A, B) \mapsto \mathrm{Tr}({}^t AB)$, et l'on considère $||\cdot|| : \mathrm{M}_{n+1}(\mathbb{R}) \to \mathbb{R}$ la norme euclidienne associée :

$$||M||^2 = \mathrm{Tr}\,({}^t M\, M) = \sum_{1 \leq i,j \leq n} M_{i,j}^2.$$

Pour $g \in G$ on note simplement $||g||$ l'élément $||\iota(g)||$. Signalons quelques propriétés élémentaires [1] vérifiées par la fonction $||.||$:

(i) $||gh|| \leq ||g||\,||h||$ pour tout $g, h \in G$,

(ii) $||g|| \geq 1$ pour tout $g \in G$,

(iii) $||gk|| = ||kg|| = ||g||$ pour tout $g \in G$ et $k \in K$,

(iv) il existe des réels $c, N > 0$ tels que $||g^{-1}|| \leq c\,||g||^N$ pour tout $g \in G$.

Définition 4.17. *Une fonction $f : G \to \mathbb{C}$ est dite à* croissance modérée *s'il existe des réels $c, N > 0$ tels que $|f(g)| \leq c\,||g||^N$ pour tout $g \in G$.*

La propriété (ii) montre que les fonctions à croissance modérée forment un sous-espace vectoriel.

Proposition 4.18. *L'espace $\mathrm{A}(G\,;\,\Gamma)$ est stable par les actions de K et de $\mathrm{U}(\mathfrak{gl}_n(\mathbb{C}))$.*

Démonstration — Soient $f \in \mathrm{A}(G\,;\,\Gamma)$, $k \in K$ et $X \in \mathfrak{gl}_n(\mathbb{C})$. Il faut voir que $\mathrm{R}_k\, f$ et $\mathrm{R}_X\, f$ sont dans $\mathrm{A}(\,G, \Gamma)$.

– La propriété (AF1) découle dans les deux cas du fait que L_γ et R_k (resp. R_X) commutent.

– Soit $W \subset \mathcal{C}^\infty(G)$ l'espace (de dimension finie) engendré par les $\mathrm{R}_{k'}\, f$ avec $k' \in K$. Il est évidemment K-stable, et il contient $\mathrm{R}_k f$, donc f satisfait (AF2). On a pour tout $k' \in K$ la relation $\mathrm{R}_{k'}\,\mathrm{R}_X\, f = \mathrm{R}_{k'Xk'^{-1}}\,\mathrm{R}_k\, f \subset \sum_{Y \in \mathfrak{g}} \mathrm{R}_Y\, W$ (de dimension finie car W et $\mathfrak{g}$ le sont), donc $\mathrm{R}_X f$ satisfait (AF2).

– L'action de $\mathfrak{z}$ commute évidemment avec R_X, et aussi avec R_k par la Proposition 4.8 et la formule $\mathrm{R}_k\, z = \mathrm{ad}_k(z)\,\mathrm{R}_k$, de sorte que $\mathrm{R}_X\, f$ et $\mathrm{R}_k\, f$ satisfont (AF3).

– Enfin, il est évident que $\mathrm{R}_X f$ satisfait (AF4). Concernant $\mathrm{R}_k\, f$, on choisit d'abord des constantes c et N telles que $|f(g)| \leq C||g||^N$, et on conclut par l'inégalité $|\mathrm{R}_k(f)(g)| = |f(gk)| \leq C||gk||^N = C||g||^N$. □

L'espace $\mathrm{A}(G\,;\Gamma)$ n'est en revanche pas stable par les R_g avec $g \in G$ en général. Sa propriété importante, du point de vue de la théorie des représentations, est que c'est un $(\mathfrak{g}, K)$-module au sens de Harish-Chandra (notion qui sera vue au prochain chapitre).

1. Pour le (ii), on pourra observer, pour tout $M \in \mathrm{M}_{n+1}(\mathbb{R})$, que l'on a l'inégalité $||M||^2 \geq (n+1)|\det M|^{2/(n+1)}$. En effet, on peut supposer M symétrique définie positive, puis appliquer l'inégalité arithmético-géométrique. Pour le (iv), utiliser que M^{-1} est la transposée de la comatrice de g pour $\mathrm{M} \in \mathrm{SL}_{n+1}(\mathbb{R})$, et observer que pour tout polynome $P \in \mathbb{C}[X_{i,j}]$, il existe des constantes $c, N > 0$ telles que $|P(M_{i,j})| \leq c||M||^N$ (car c'est vrai pour $P = X_{i,j}$).

5. Les formes modulaires sont des formes automorphes

On considère ici le cas $n = 2$ et $\Gamma = \mathrm{GL}_2(\mathbb{Z})$. On note $P \subset \mathrm{GL}_2(\mathbb{R})^+$ le sous-groupe constitué des matrices de la forme $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)$ (donc, avec $y > 0$), $Z \simeq \mathbb{R}_{>0}$ le sous-groupe central des homothéties de facteur > 0, et on pose

$$K^+ = K \cap \mathrm{GL}_2(\mathbb{R})^+ = \mathrm{SO}(2)$$

(matrices de la forme $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ avec $a^2 + b^2 = 1$). Pour tout $\lambda \in \mathbb{C}^\times$, écrit sous la forme $\lambda = a + bi$ avec $a, b \in \mathbb{R}$, on pose

$$\mathrm{s}_\lambda = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) \in ZK^+.$$

(C'est la similitude de rapport $\overline{\lambda}$ si l'on identifie $\mathbb{R}^2$ à $\mathbb{C}$ au moyen de la base $(i, 1)$.) Tout élément de K^+Z est de la forme s_λ pour un unique λ.

Proposition 4.19. *(i) Le stabilisateur du point $i \in \mathbb{H}$ dans $\mathrm{GL}_2(\mathbb{R})^+$ est K^+Z.*

(ii) L'application $g \mapsto \mathrm{j}(g, i)$ induit un isomorphisme de groupes $K^+Z \xrightarrow{\sim} \mathbb{C}^\times$. On a $\mathrm{j}(\mathrm{s}_\lambda, i) = \lambda$ pour tout $\lambda \in \mathbb{C}^\times$.

(iii) On a $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) \cdot i = x + iy$ pour tout $x \in \mathbb{R}$ et tout $y > 0$. De plus, tout élément de g s'écrit de manière unique sous la forme $p\,\mathrm{s}_\lambda$ avec $p \in P$ et $\lambda \in \mathbb{C}^\times$.

Démonstration — L'équation $\frac{ai+b}{ci+d} = i$ étant équivalente à $b = -c$ et $a = d$, le stabilisateur de i est K^+Z, d'où le (i). Ce stabilisateur est aussi le sous-groupe des $g \in \mathrm{GL}_2(\mathbb{R})^+$ préservant la droite $\mathbb{C}\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right)$ dans $\mathbb{C}^2$, l'élément $\mathrm{j}(g, i)$ étant alors la valeur propre associée. Cela montre que $g \mapsto \mathrm{j}(g, i)$ est un morphisme de groupes. L'identité $\mathrm{j}(\mathrm{s}_\lambda, i) = \lambda$ est claire. Le (iii) est évident. □

On a vu au chapitre 2 que l'ensemble $\mathcal{B}$ des $\mathbb{R}$-bases $\omega = \left(\begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix}\right)$ de $\mathbb{C}$ est muni d'une action simplement transitive de $\mathrm{GL}_2(\mathbb{R})$. Choisissons pour base de référence la base directe $\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right) \in \mathcal{B}^+$ de $\mathbb{C}$. L'application $g \mapsto g\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right)$ induit des bijections $\mathrm{GL}_2(\mathbb{R}) \xrightarrow{\sim} \mathcal{B}$ et $\mathrm{GL}_2(\mathbb{R})^+ \xrightarrow{\sim} \mathcal{B}^+$.

Fixons un caractère χ de $\mathbb{C}^\times$, i.e. un morphisme de groupes $\mathbb{C}^\times \longrightarrow \mathbb{C}^\times$, et une fonction $f : \mathbb{H} \to \mathbb{C}$ qui est modulaire de poids χ. On rappelle que f est de la forme $F(\left(\begin{smallmatrix} \tau \\ 1 \end{smallmatrix}\right))$ pour une, et une seule, fonction $F : \mathcal{B} \to \mathbb{C}$ vérifiant $F(\gamma\lambda\omega) = \chi(\lambda)F(w)$ pour tout $\omega \in \mathcal{B}^+$, tout $\gamma \in \mathrm{GL}_2(\mathbb{Z})$, et tout $\lambda \in \mathbb{C}^\times$. On associe à χ et f et la fonction

$$\Phi_f : \mathrm{GL}_2(\mathbb{R}) \longrightarrow \mathbb{C}, \quad g \mapsto F(g\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right)). \tag{29}$$

Il résulte de cette définition et du §2.2 que pour tout g dans $\mathrm{GL}_2(\mathbb{R})^+$ on a la formule $\Phi_f(g) = \chi(\mathrm{j}(g, i))f(g.i)$.

Proposition 4.20. *Soit χ un caractère de $\mathbb{C}^\times$. L'application $f \mapsto \Phi_f$ induit une bijection $\mathbb{C}$-linéaire entre l'espace des fonctions $\mathbb{H} \to \mathbb{C}$ qui sont modulaires de poids χ et l'espace des fonctions $\Phi : \mathrm{GL}_2(\mathbb{R}) \longrightarrow \mathbb{C}$ vérifiant :*

(i) $\Phi(\gamma g) = \Phi(g)$ *pour tout* $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ *et tout* $g \in \mathrm{GL}_2(\mathbb{R})$,

(ii) $\Phi(gs_\lambda) = \chi(\lambda)\Phi(g)$ *pour tout* $g \in \mathrm{GL}_2(\mathbb{R})$ *et tout* $\lambda \in \mathbb{C}^*$.

De plus, on a $\Phi_f(\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)) = f(x+iy)$ *pour tout* $x \in \mathbb{R}$ *et tout* $y \in \mathbb{R}_{>0}$.

Démonstration — C'est une traduction de la Proposition 2.5 (compte tenu de la bijection $g \mapsto g\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right)$, $\mathrm{GL}_2(\mathbb{R}) \xrightarrow{\sim} \mathcal{B}$) et de la Proposition 4.19 (ii). □

Si $\tau \in \mathbb{H}$ on note $\mathrm{p}_\tau \in P$ l'élément $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)$ vérifiant $\tau = x + iy$. Observons que la bijection $\mathbb{H} \times \mathbb{C}^\times \to \mathrm{GL}_2(\mathbb{R})^+$, $(\tau, \lambda) \mapsto \mathrm{p}_\tau \mathrm{s}_\lambda$ est un $\mathcal{C}^\infty$-difféomorphisme. En effet, elle est manifestement de classe $\mathcal{C}^\infty$, et son inverse est donnée par la formule

$$g \mapsto (\, g.i,\, \mathrm{j}(s(g), i)), \;\text{ avec } s(g) \,=\, \mathrm{p}_{g.i}^{-1}\, g,$$

qui est manifestement de classe $\mathcal{C}_\infty$ également.

Lemme 4.21. *Soit* χ *un caractère de* $\mathbb{C}^\times$ *et* $\Phi : \mathrm{GL}_2(\mathbb{R}) \longrightarrow \mathbb{C}$ *vérifiant les assertions (i) et (ii) de la proposition 4.20. La fonction* Φ *est de classe* $\mathcal{C}^\infty$ *si, et seulement si :*

(i) la fonction $\lambda \mapsto \chi(\lambda), \mathbb{C}^\times \to \mathbb{C}$,

(ii) et la fonction $\tau \mapsto \Phi(\mathrm{p}_\tau)$, $\mathbb{H} \to \mathbb{C}$,

sont de classes $\mathcal{C}^\infty$.

Démonstration — La relation $\Phi(\gamma g) = \Phi(g)$ pour un $\gamma \in \mathrm{GL}_2(\mathbb{Z}) - \mathrm{SL}_2(\mathbb{Z})$ montre que Φ est de classe $\mathcal{C}^\infty$ si, et seulement si, c'est le cas de sa restriction à $\mathrm{GL}_2(\mathbb{R})^+$. On conclut immédiatement par la relation (ii) vérifiée par χ et par l'observation précédent le lemme. □

Lemme 4.22. *Un caractère* χ *de* $\mathbb{C}^\times$ *est* $\mathcal{C}^\infty$ *si, et seulement si, il est de la forme* $\lambda \mapsto \lambda^m |\lambda|^s$ *avec* $m \in \mathbb{Z}$ *et* $s \in \mathbb{C}$.

Démonstration — Exercice ! □

On s'intéresse maintenant à l'action de $\mathfrak{gl}_2(\mathbb{C})$ sur les Φ_f. On pourrait utiliser la base Z, e, f, h mais ce ne serait pas très judicieux car elle n'est pas adaptée à la propriété (ii) de Φ_f vis à vis du sous-groupe K^+. On considère plutôt la base Z, e', f', h' avec

$$ih' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\; e' = \frac{1}{2}\begin{bmatrix} 1 & -i \\ -i & -1 \end{bmatrix} \text{ et } f' = \frac{1}{2}\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} = \overline{e'}.$$

On vérifierait aisément que les relations $[h', e'] = 2e'$, $[h', f'] = -2f'$ et $[e', f'] = h'$ valent encore. L'origine de cette nouvelle base[2] de $\mathrm{sl}_2(\mathbb{C})$ est la suivante. Tout

2. Une manière alternative, bien que similaire, de penser à la base e', f', h' est de raisonner dans la base $\left(\begin{smallmatrix} i \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -i \\ 1 \end{smallmatrix}\right)$ de $\mathbb{C}^2$, dans laquelle K agit diagonalement. Autrement dit, on conjugue

d'abord la matrice anti-symétrique $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] = ih'$ est un générateur de l'algèbre de Lie de K : on a pour tout $t \in \mathbb{R}$ la formule

$$\exp(tih') = \mathrm{s}_{e^{it}}. \tag{30}$$

L'action par conjugaison de K sur $\mathrm{M}_2(\mathbb{R})$ préserve $\mathbb{R}(ih')$, $\mathbb{R}Z$, et aussi le plan des matices symétriques de trace nulle, i.e des $\left[\begin{smallmatrix} u & v \\ v & -u \end{smallmatrix}\right]$ avec u, v dans $\mathbb{R}$. L'action sur ce plan se diagonalise après extension des scalaires à $\mathbb{C}$, les éléments e' et f' étant choisis comme étant une base de vecteurs propres (et ensuite normalisés correctement). On a précisément

$$\mathrm{ad}_{\mathrm{s}_\lambda} e' = (\lambda/|\lambda|)^2\, e' \text{ et } \mathrm{ad}_{\mathrm{s}_\lambda} f' = (\lambda/|\lambda|)^{-2}\, f'. \tag{31}$$

Proposition 4.23. *Soit χ le caractère $\lambda \mapsto \lambda^m|\lambda|^s$, $m \in \mathbb{Z}$ et $s \in \mathbb{C}$. Soit $\Phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{C}$ de classe $\mathcal{C}^\infty$ vérifiant $\Phi(g\,\mathrm{s}_\lambda) = \chi(\lambda)\Phi(g)$ pour tout $g \in \mathrm{GL}_2(\mathbb{R})$ et tout $\lambda \in \mathbb{C}^*$, et $f : \mathbb{H} \to \mathbb{C}$ la fonction $\tau \mapsto \Phi(\mathrm{p}_\tau)$ (de classe $\mathcal{C}^\infty$ aussi). On a les formules suivantes :*

(i) $\mathrm{R}_Z\Phi = (m+s)\,\Phi$,

(ii) $\mathrm{R}_{h'}\Phi = m\,\Phi$,

(iii) $(\mathrm{R}_{e'}\Phi)(\,\mathrm{p}_\tau\,\mathrm{s}_\lambda\,) = \lambda^{m+2}\,|\lambda|^{s-2}\,\big((\overline{\tau}-\tau)\,\frac{\partial}{\partial\overline{\tau}}f(\tau) - \frac{s}{2}\,f(\tau)\big)$,

(iv) $(\mathrm{R}_{f'}\Phi)(\,\mathrm{p}_\tau\,\mathrm{s}_\lambda\,) = \lambda^{m-2}\,|\lambda|^{s+2}\,\big((\tau-\overline{\tau})\,\frac{\partial}{\partial\tau}f(\tau) - (m+\frac{s}{2})\,f(\tau)\big)$.

Démonstration — Pour $t \in \mathbb{R}$ on a $e^{tZ} = s_{e^t}$, puis $\Phi(ge^{tZ}) = e^{(m+s)t}\Phi(g)$, dont l'assertion (i) découle en dérivant en $t = 0$. De même, la formule (30) montre $\Phi(ge^{ith'}) = e^{imt}\Phi(g)$, puis $\mathrm{R}_{ih'}\,\Phi = i\,m\,\Phi$, et donc (par $\mathbb{C}$-linéarité) $\mathrm{R}'_h\Phi = m\Phi$. Le (iii) est plus subtile. On commence par observer que l'on a $(\mathrm{R}_{e'}\Phi)(\,\mathrm{p}_\tau\,\mathrm{s}_\lambda\,) = (\mathrm{R}_{s_\lambda}\mathrm{R}_{e'}\Phi)(p_\tau)$. La formule générale $\mathrm{R}_{s_\lambda}\,\mathrm{R}_{e'} = \mathrm{R}_{\mathrm{ad}_{s_\lambda}e'}\mathrm{R}_{s_\lambda}$, l'identité $\mathrm{ad}_{s_\lambda}e' = (\lambda/|\lambda|)^2 e'$, et la relation évidente $\mathrm{R}_{s_\lambda}\Phi = \lambda^m|\lambda|^s\Phi$, entraînent donc l'égalité

$$(\mathrm{R}_{e'}\Phi)(\,\mathrm{p}_\tau\,\mathrm{s}_\lambda\,) = \lambda^{m+2}|\lambda|^{s-2}(\mathrm{R}_{e'}\Phi)(p_\tau).$$

Pour calculer $\mathrm{R}_{e'}\Phi(\mathrm{p}_\tau)$ sans effort il paraît naturel de décomposer d'abord e comme somme d'un élément de l'algèbre de Lie de P et d'un élément de l'algèbre de Lie de K^+Z. Concrètement on a

$$e' = \frac{1}{2}(h' - Z) + \mathrm{E}_{1,1} - i\,\mathrm{E}_{1,2}.$$

Les assertions (i) et (ii) déjà montrées entraînent déjà

$$\mathrm{R}_{(h'-Z)/2}\,\Phi = \frac{s}{2},\Phi,$$

de sorte que nous n'avons plus qu'à déterminer $(\mathrm{R}_{|rmE_{1,i}}\Phi)(\mathrm{p}_\tau)$ pour $i = 1, 2$. On pose $\tau = x + iy$, on a pour $t \in \mathbb{R}$:

$$\Phi(\mathrm{p}_\tau \exp(t\mathrm{E}_{1,1})) = \Phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} e^t & 0 \\ 0 & 1 \end{pmatrix}) = \Phi(\begin{pmatrix} e^t y & x \\ 0 & 1 \end{pmatrix}) = f(x + ie^t y),$$

$\mathrm{GL}_2(\mathbb{R})$ dans $\mathrm{GL}_2(\mathbb{C})$ par C^{-1} avec $C = \left[\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right]$ (c'est la "transformation de Cayley"). L'application $M \mapsto C^{-1}MC$ avec $C = \left[\begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix}\right]$ envoit respectivement h', e' et f' sur $-h, e$ et f.

d'où la formule

$$\mathrm{R}_{\mathrm{E}_{1,1}}\Phi(p_\tau) = \mathrm{Im}\,\tau\,\frac{\partial f}{\partial y}(\tau)$$

en dérivant en $t = 0$. Dans cette dernière formule, nous voyons bien entendu f comme une fonction de deux variables (x, y) (comme en théorie des fonctions holomorphes) via $(x, y) \mapsto f(x + iy)$. De même, on a pour $t \in \mathbb{R}$:

$$\Phi(\mathrm{p}_\tau \exp(t\mathrm{E}_{1,2})) = \Phi(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}) = \Phi(\begin{pmatrix} y & ty+x \\ 0 & 1 \end{pmatrix}) = f(x + ty + iy),$$

puis la formule

$$\mathrm{R}_{\mathrm{E}_{1,2}}\Phi(p_\tau) = \mathrm{Im}\,\tau\,\frac{\partial f}{\partial x}(\tau).$$

En terme des opérateurs différentiels d'ordre 1 sur $\mathcal{C}^\infty(\mathbb{H})$ définis par les formules

$$\frac{\partial}{\partial\tau} = \frac{1}{2}\frac{\partial}{\partial x} - i\frac{1}{2}\frac{\partial}{\partial y} \text{ et } \frac{\partial}{\partial\overline{\tau}} = \frac{1}{2}\frac{\partial}{\partial x} + i\frac{1}{2}\frac{\partial}{\partial y},$$

familiers en analyse complexe, et en utilisant la formule $-2\,i\mathrm{Im}\,\tau = \overline{\tau} - \tau$, on a la relation $\mathrm{Im}\,\tau(\frac{\partial}{\partial y} - i\frac{\partial}{\partial x}) = (\overline{\tau} - \tau)\frac{\partial}{\partial\overline{\tau}}$. On a donc montré

$$(\mathrm{R}_{\mathrm{E}_{1,1} - i\,\mathrm{E}_{1,2}}\Phi)(\mathrm{p}_\tau) = (\overline{\tau} - \tau)\frac{\partial}{\partial\tau}f(\tau),$$

ce qui termine la démonstration du (iii). L'assertion (iv) se montre de la même manière, en utilisant $\mathrm{ad}_{s_\lambda} f' = (\lambda/|\lambda|)^{-2} f'$ et $f' = \overline{e'} = \frac{1}{2}(-h' - Z) + \mathrm{E}_{1,1} + i\,\mathrm{E}_{1,2}$. □

Corollaire 4.24. *On se place sous les hypothèses de la Proposition 4.23 et on suppose de plus $s = 0$. Les assertions suivantes sont vérifiées :*

(i) On a $\mathrm{R}_{e'}\,\Phi = 0$ si, et seulement si, f est holomorphe sur $\mathbb{H}$.

(ii) Si f est holomorphe, on a $C\,\Phi = m(m+1)\,\Phi$.

(iii) Si $m = s = 0$, on a $(C\,\Phi)\,(\mathrm{p}_\tau) = -2\,(\mathrm{Im}\,\tau)^2\,\frac{\partial^2}{\partial\tau\partial\overline{\tau}}f(\tau)$.

Démonstration — Le (i) résulte immédiatement de la formule pour $\mathrm{R}_{e'}\Phi$, et du fait que f est holomorphe si, et seulement si, on a $\frac{\partial f}{\partial\overline{\tau}} = 0$ (équations de Cauchy-Riemann). Pour le (ii), on utilise la formule

$$C = ((h')^2 + Z^2)/2 + e'f' + f'e' = ((h')^2 + Z^2)/2 + h' + 2f'e'$$

et les relations $\mathrm{R}_{e'}\Phi = 0$ et $\mathrm{R}_Z\,\Phi = \mathrm{R}_{h'}\,\Phi = m\,\Phi$. Pour le (iii), on pose $\Phi' = \mathrm{R}_{e'}\,\Phi$. On a $\Phi'(\mathrm{p}_\tau \mathrm{s}_\lambda) = (\lambda/|\lambda|)^2\,(\overline{\tau} - \tau)\frac{\partial f}{\partial\overline{\tau}}$, de sorte que Φ' satisfait les hypothèses de la proposition avec $m = 2$ et $s = -2$. On en déduit

$$\mathrm{R}_{f'}\Phi'(\mathrm{p}_\tau) = (\tau - \overline{\tau})\frac{\partial f}{\partial\tau}((\overline{\tau} - \tau)\frac{\partial f}{\partial\overline{\tau}}) - (\overline{\tau} - \tau)\frac{\partial f}{\partial\overline{\tau}} = -\,(\mathrm{Im}\,\tau)^2\,\frac{\partial^2}{\partial\tau\partial\overline{\tau}}f(\tau).$$

(on rappelle que l'on a par définition $\frac{\partial f}{\partial\tau}(\tau) = 1$ et $\frac{\partial f}{\partial\tau}(\overline{\tau}) = 0$). □

Théorème 4.25. *Soit $k \in \mathbb{Z}$. L'application $f \mapsto \Phi_f$ induit une bijection entre l'espace M_k des formes modulaires et l'espaces des formes automorphes $\Phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{C}$ pour $\mathrm{GL}_2(\mathbb{Z})$ vérifiant les conditions suivantes :*

(i) $\Phi(g\,\mathrm{s}_\lambda) = \lambda^{-k}\,\Phi(g)$ *pour tout* $\lambda \in \mathbb{C}^*$ *et tout* $g \in \mathrm{GL}_2(\mathbb{R})$,

(ii) $\mathrm{R}_{e'}\,\Phi = 0$,

(iii) $\mathrm{C}\,\Phi = k(k+1)\,\Phi$.

Démonstration — On part de la Proposition 4.20 appliquée à $\chi(\lambda) = \lambda^{-k}$. Soit $f : \mathbb{H} \to \mathbb{C}$ une fonction modulaire de poids $k \geq 0$. Notons que Φ_f est propre sous l'action de K^+ ; comme ce dernier est d'indice 2 dans K, on en déduit que Φ_f est K-finie. On a vu que f est de classe $\mathcal{C}^\infty$ si, et seulement si, on a $\Phi_f \in \mathcal{C}^\infty(G)$, puis que f est holomorphe si, et seulement si, $\mathrm{R}_{e'}\Phi_f = 0$. Si f est holomorphe, on a vu aussi que Φ_f est propre sous l'action de Z et de C, elle est donc $\mathfrak{z}(\mathrm{gl}_2(\mathbb{C}))$-finie d'après le Théorème 4.10. Nous allons maintenant vérifier que si f est holomorphe, $f(\tau)$ admet une limite pour $\mathrm{Im}\,\tau \to +\infty$ si, et seulement si, Φ_f est à croissance modérée, et qu'auquel cas elle satisfait (AF4).

Soit $g = \mathrm{p}_\tau \mathrm{s}_\lambda \in \mathrm{GL}_2(\mathbb{R})^+$. On a $|\Phi_f(g)| = |\lambda||f(\tau)|$. En particulier, si Φ_f est à croissance modérée, il existe des constantes C, m telles que l'on ait

$$|f(\tau)| = |\Phi_f(\mathrm{p}_\tau)| \leq C||\mathrm{p}_\tau||^m = C(|\tau|^2 + 1 + (\mathrm{Im}\,\tau)^{-2})^{m/2}.$$

Cela entraîne que la série de Laurent $\widetilde{f} : \mathrm{D} - \{0\} \to \mathbb{C}$, qui rappelons-le vérifie $\widetilde{f}(\mathrm{q}) = f(\tau)$, satisfait $|\widetilde{f}(z)| \leq |P(\log(|z|)|$ où $P \in \mathbb{R}[X, X^{-1}]$ est un polynôme bien choisi (observer que l'on peut écrire $z = e^{2i\pi\tau}$ avec $|\mathrm{Re}(\tau)| \leq 1$, auquel cas on a $|\tau|^2 \leq (\mathrm{Im}\,\tau)^2 + 1$ et $|\log(|z|)| = 2\pi\mathrm{Im}\,\tau$). Cela implique que $|z\widetilde{f}(z)|$ est bornée au voisinage de $z = 0$, et tend vers 0 en 0 : $\widetilde{f}$ est holomorphe en 0, *i.e.* f est une forme modulaire.

Étudions enfin la réciproque. Observons d'abord que si $g \in \mathrm{GL}_2(\mathbb{R})^+$ est de la forme $\mathrm{p}_\tau \mathrm{s}_\lambda$, on a les égalités $|\det g| = |\lambda|^2 \mathrm{Im}\,\tau$ et

$$||\mathrm{p}_\tau \mathrm{s}_\lambda||^2 = ||\mathrm{p}_\tau|\lambda|||^2 = |\lambda|^2(|\tau|^2 + 1) + |\det g|^{-2}.$$

En particulier, on a $|\lambda|\mathrm{Im}\,\tau \leq ||g||$, $|\lambda|^{-2}(\mathrm{Im}\,\tau)^{-1} \leq ||g||$, $|\lambda|^{-1} \leq ||g||^2$ et $|\mathrm{Im}\,\tau| \leq ||g||^3$.

Ssupposons enfin que $f(\tau)$ admet une limite quand $\mathrm{Im}\,\tau \to +\infty$. En particulier, $|f(\tau)|$ est bornée sur le domaine fondamental $\mathcal{F}$ par une certaine constante $C > 0$. Mais tout $g \in \mathrm{GL}_2(\mathbb{R})$ est de la forme $g = \gamma \mathrm{p}_\tau \mathrm{s}_\lambda$ avec $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ et τ dans $\mathcal{F}$. Comme Φ_f est $\mathrm{GL}_2(\mathbb{Z})$-invariante à gauche, on a donc $|\Phi_f(g)| = |\lambda|^{-k}|f(\tau)| \leq C|\lambda|^{-k}$. Les observations ci-dessus (et $k \geq 0$) montrent $|\lambda|^{-k} \leq ||\mathrm{p}_\tau \mathrm{s}_\lambda||^{2k}$. On conclut par le lemme 4.26.

Vérifions maintenant que $u\Phi_f$ est à croissante modérée pour tout $u \in \mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$. Cela concluera la démonstration. Il suffit de le faire pour des éléments de la forme $(f')^a(h')^b(e')^c Z^d$ avec a, b, c, d des entiers ≥ 0. D'après les relations $\mathrm{R}_Z\Phi_f = \mathrm{R}_{h'}\Phi_f = m\Phi_f$ et $\mathrm{R}_{e'}\Phi_f = 0$, il suffit de le vérifier pour la fonction $\Psi_m := \mathrm{R}_{(f')^m}\Phi_f$ avec $m \geq 0$.

D'après la Proposition 4.23 (iv), elle vérifie $\Psi_m(\mathrm{p}_\tau \mathrm{s}_\lambda) = \lambda^{-k}(\lambda/|\lambda|)^{-2m} f_m(\tau)$, où $f_0 = f$ et pour $m \geq 1$ on a

$$f_m(\tau) = (\tau - \overline{\tau})\frac{\partial f_{m-1}(\tau)}{\partial \tau} + (k - m + 1) f_{m-1}(\tau).$$

On constate aisément que $f_m(\tau)$ est une combinaison linéaire finie de fonctions de la forme $(\tau - \overline{\tau})^i f^{(j)}(\tau)$ avec $i \leq m$. En particulier, $|f_m(\tau)|$ est majorée sur $\mathcal{F}$ par un polynôme en $\mathrm{Im}\,\tau$ dont le degré est $\leq m$. Le même argument que ci-dessus montre alors que Ψ_m est à croissance modérée. □

Le lemme suivant est dû à Borel et Harish-Chandra. On note $\Pi \subset \mathrm{GL}_2(\mathbb{R})$ l'ensemble des éléments de la forme $\mathrm{p}_\tau \mathrm{s}_\lambda$ avec $\tau \in \mathcal{F}$ et $\lambda \in \mathbb{C}^*$.

Lemme 4.26. *Il existe une constante $\delta > 0$ telle que pour tout $g \in \Pi$ on a*

$$\delta ||g|| \leq \inf_{\gamma \in \mathrm{GL}_2(\mathbb{Z})} ||\gamma g|| \leq ||g||.$$

Démonstration — Fixons $g = \mathrm{p}_\tau \mathrm{s}_\lambda$ avec $\tau \in \mathcal{F}$. Soit $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. On pose $\tau' = \gamma \mathrm{p}_\tau(i) = \gamma\tau \in \mathbb{C} - \mathbb{R}$. On a $\gamma \mathrm{p}_\tau = \mathrm{p}_{\tau'} \mathrm{s}_{\lambda'}$ pour un unique $\lambda' \in \mathbb{C}$, où la définition de p_z pour $z \in \mathbb{C} - \mathbb{R}$ va de soi. En appliquant $h \mapsto |\det h|$ on obtient l'égalité $\mathrm{Im}\,\tau = \mathrm{Im}\,\tau' \, |\lambda'|^2$. On a donc

$$||\gamma\, g||^2 \,=\, ||\mathrm{p}_{\tau'}\, \mathrm{s}_{\lambda\lambda'}||^2 = ||\mathrm{p}_{\tau'}\, |\lambda\lambda'|\, ||^2 \,=\, |\lambda\lambda'|^2\, (|\tau'|^2 + 1) \,+\, |\det g|^{-2}.$$

Écrivons $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. On a $|\lambda'| = |c\tau + d|$ et $\tau' = (a\tau + b)/(c\tau + d)$, puis

$$|\lambda'|^2(|\tau'|^2 + 1) = |a\tau + b|^2 + |c\tau + d|^2 \geq (a^2 + c^2)\,(\mathrm{Im}\,\tau)^2 \geq (\mathrm{Im}\,\tau)^2.$$

Mais on vérifie immédiatement que pour $\tau \in \mathcal{F}$, et plus généralement pour $|\mathrm{Re}\,\tau| \leq 1/2$ et $\mathrm{Im}\,\tau \geq \sqrt{3}/2$, on a l'inégalité $(\mathrm{Im}\,\tau)^2 \geq \frac{3}{8}\,(|\tau|^2 + 1)$. Cela montre

$$||\gamma g||^2 \,\geq\, \frac{3}{8}\, ||g||^2,$$

et conclut la démonstration (avec $\delta^2 = 3/8$). □

Remarque 4.27. Le Lemme 4.26 s'étend à $\mathrm{GL}_n(\mathbb{Z}) \subset \mathrm{GL}_n(\mathbb{R})$, et même à des sous-groupes d'indice fini de ces derniers, si l'on remplace Π par un *domaine de Siegel* convenable : voir le premier chapitre du livre de Borel *Introduction aux groupes arithmétiques*.

CHAPITRE 5

Propriétés de finitude et $(\mathfrak{g}, K)$-modules

Dans ce chapitre, on s'intéresse aux propriétés de finitude des espaces de formes automorphes $\mathrm{A}(G;\Gamma)$. Ces espaces sont munis d'actions naturelles de K et $\mathfrak{g}$ compatibles en un certain sens : c'est un exemple de $(\mathfrak{g}, K)$-module (ou *module de Harish-Chandra*). Dans une première partie, nous étudierons abstraitement ces $(\mathfrak{g}, K)$-modules et introduirons trois notions de finitude naturelles les concernant : admissibilité, engendrement fini, longueur finie. Un résultat dû à Harish-Chandra affirme l'équivalence de ces trois notions pour un $(\mathfrak{g}, K)$-module donné si ce dernier est annulé par un idéal de codimension finie de $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$. Dans la seconde partie, nous démontrerons cet énoncé dans le cas $G = \mathrm{GL}_2(\mathbb{R})$, et nous classifierons essentiellement les $(\mathfrak{g}, K)$-modules admissibles irréductibles dans ce cas, un résultat fameux dû à Bargmann qui est un ingrédient important dans la classification du dual unitaire de $\mathrm{GL}_2(\mathbb{R})$.

Fixons Γ un sous-groupe d'indice fini de $\mathrm{GL}_n(\mathbb{Z})$ et I un idéal de codimension finie de $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$. Un résultat central dû à Harish-Chandra est l'admissibilité du $(\mathfrak{g}, K)$-module $\mathrm{A}(\mathrm{GL}_n(\mathbb{R});\Gamma)[I]$ constitué des formes automorphes $f \in \mathrm{A}(\mathrm{GL}_n(\mathbb{R});\Gamma)$ annulées par I. Cet énoncé peut être vu comme une vaste généralisation du fait que les espaces M_k étudiés au chapitre 2 sont de dimension finie. Nous en donnerons une démonstration complète (et au chapitre suivant) que dans le cas $n = 2$ et $\Gamma = \mathrm{GL}_2(\mathbb{Z})$, cas qui présentera toutefois déjà de nombreuses difficultés et idées du cas général. Un énoncé intermédiaire qui jouera un rôle important est le théorème "d'harmonicité" de Harish-Chandra, étudié ici en section 3. Il permet notamment de montrer que les formes automorphes sont à croissance uniformément modérée (et d'affaiblir substantiellement l'hypothèse (A4)).

Références :

[BK], T. Bailey, A. Knapp ed., *Representation theory and automorphic forms*, Edinburgh, AMS P.S.P.M. 61 (1996),

[B], A. Borel, *Automorphic forms on* $\mathrm{SL}_2(\mathbb{R})$, Cambridge Tract in Math. 130 (1997),

W. Casselman, *Analysis on* SL(2), notes de cours,

Harish-Chandra, *Automorphic forms on semisimple Lie groups* (1968),

L. Hörmander, *The analysis of linear partial differential equations* (1983),

A. Knapp, *Representation Theory of semisimple Lie groups*, Princeton University Press (1986), Chapitres I, III et VIII.

1. $(\mathfrak{g}, K)$-modules et énoncés de finitude

Si G est un groupe, on rappelle qu'une représentation linéaire de G sur un $\mathbb{C}$-espace vectoriel V est la donnée d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$, ou ce qui revient au même d'une structure de $\mathbb{C}[G]$-module sur V. Si $g \in G$ et $v \in V$ on note aussi $g.v$ pour $\rho(g).v$. Les représentations de G forment une catégorie de manière évidente : celle des $\mathbb{C}[G]$-modules. Une représentation (ρ, V) est dite irréductible (ou simple) si l'on a $V \neq 0$, et si les seuls sous-espaces de V stable par $\rho(G)$ sont $\{0\}$ et V, autrement dit si le $\mathbb{C}[G]$-module associé est simple.

On suppose désormais que G est un groupe topologique. On rappelle que tout $\mathbb{C}$-espace vectoriel *de dimension finie* est muni d'une topologie canonique (équivalence des normes). Une représentation (ρ, V) de G avec $\dim V < \infty$ est dite *continue* si ρ l'est en tant qu'application $G \to \mathrm{GL}(V)$, où $\mathrm{GL}(V)$ est vu comme un ouvert de l'espace de dimension finie $\mathrm{End}(V)$. Il est équivalent de demander que pour tout $v \in V$, l'application "orbite" $g \mapsto g.v$, $G \to V$, est continue. En effet, cette propriété est évidemment nécessaire, et pour la réciproque il suffit de l'appliquer aux vecteurs v d'une base donnée de V. On note $\mathrm{Irr}(G)$ l'ensemble des classes d'isomorphisme de représentations continues et irréductibles de G sur des espaces de dimension finie (c'est évidemment un ensemble car on peut supposer que l'espace sous-jacent est $\mathbb{C}^n$ pour un entier $n \geq 0$).

Pour tout $\tau \in \mathrm{Irr}(G)$, et toute représentation linéaire (ρ, V) de G, on note $V_\tau \subset V$ le sous-espace engendré par les sous-représentations de V qui sont isomorphes à τ. Un argument à la Zorn montre que la représentation V_τ est isomorphe à une somme directe (éventuellement infinie) de représentations isomorphes à τ. L'égalité évidente $\mathrm{Hom}_{\mathbb{C}[G]}(V_\tau, V'_\tau) = 0$ pour $\tau \neq \tau'$ entraîne que les sous-espaces V_τ avec $\tau \in \mathrm{Irr}(G)$ sont en somme directe dans V. Cette somme est toutefois strictement incluse dans V en général (donner un exemple avec $G = \mathbb{R}$ et $\dim V = 2$).

Proposition 5.1. *Soient G un groupe topologique compact et (ρ, V) une représentation de G. On a équivalence entre :*

(i) $V = \bigoplus_{\tau \in \mathrm{Irr}(G)} V_\tau$,

(ii) V est réunion de sous-représentations de dimension finie et continues,

(iii) pour tout $v \in V$, l'application $g \mapsto \rho(g).v$ prend ses valeurs dans un sous-espace de dimension finie W de V, et induit une application continue $G \to W$.

Démonstration — Les conditions (ii) et (iii) sont trivialement équivalentes, et (i) implique (ii). Supposons (ii) vérifiée et montrons $V \subset \sum_{\tau \in \mathrm{Irr}(G)} V_\tau$ (la seule chose restant à monter par les rappels ci-dessus). Par le (ii), il suffit de voir que si $U \subset V$ est une sous-représentation de dimension finie et continue, on a $U \subset \sum_{\tau \in \mathrm{Irr}(G)} U_\tau$ (car on a $U_\tau \subset V_\tau$). On peut donc supposer que V est de dimension finie.

Rappelons que G étant compact, il possède une unique mesure borélienne de volume total 1 invariante par translation des deux côtés, notée $\mathrm{d}g$: c'est la mesure de Haar. [1] Cette mesure permet de munir V d'un produit hermitien (défini positif)

1. Nous n'utiliserons pas son unicité ici, et en ce qui concerne son existence, le seul exemple que nous considèrerons sérieusement ici est le cas ridiculement simple du groupe $G = \mathrm{SO}(2)$. Dans ce cas, le morphisme de groupes $\pi : \mathbb{R} \to \mathrm{SO}(2)$, $x \mapsto s_{e^{2i\pi x}}$, est un revêtement surjectif de

pour lequel on a $G \subset \mathrm{U}(V)$ (groupe unitaire de V). En effet, on part d'un produit hermitien $\langle x, y\rangle$ arbitraire et on observe que la fomule

$$x.y \,=\, \int_G \langle\, g.x, g.y\,\rangle \,\mathrm{d}g$$

est bien définie et convient. Il en résulte que tout sous-espace U de V qui est G-stable admet un supplémentaire G-stable, à savoir l'orthogonal de U pour le produit hermitien ci-dessus. En particulier, V est somme directe de sous-représentations irréductibles, ce qui conclut. □

Considérons le cas du groupe compact $G = \mathrm{SO}(2)$. Il sera commode de noter $\epsilon : \mathrm{SO}(2) \to \mathbb{C}^\times$ le morphisme de groupes vérifiant $\epsilon(\mathrm{s}_\lambda) = \lambda$ pour $\lambda \in \mathbb{C}^\times$ avec $|\lambda| = 1$, c'est un isomorphisme (topologique) sur son image qui est le cercle unité S^1. C'est un groupe commutatif, donc ses représentations irréductibles de dimension finie (continues ou non) sont de dimension 1 (noter que si ρ est de dimension finie alors $\rho(G)$ est "co-trigonalisable", donc possède une droite stable). L'ensemble $\mathrm{Irr}(\mathrm{SO}(2))$ est donc en bijection avec l'ensemble des morphismes continus $\mathrm{SO}(2) \to \mathbb{C}^\times$ (ou "caractères"). C'est un exercice classique de vérifier que les caractères de S^1 sont les $\lambda \mapsto \lambda^m$ avec $m \in \mathbb{Z}$, on a donc

$$\mathrm{Irr}(\mathrm{SO}(2)) = \{\epsilon^m, m \in \mathbb{Z}\}.$$

Si V est une représentation linéaire de $\mathrm{SO}(2)$, et si $m \in \mathbb{Z}$, on notera

$$V_m := V_{\epsilon^m} = \{v \in V,\ g.v \,=\, \epsilon(g)^m\, v \ \ \forall g \in \mathrm{SO}(2)\}.$$

On a démontré le corollaire suivant (qui s'applique en particulier aux représentations linéaires de $\mathrm{O}(2)$ qui sont réunion de sous-représentations continues de dimension finie) :

Corollaire 5.2. *Si V est une représentation linéaire de $\mathrm{SO}(2)$ qui est réunion de sous-représentations continues de dimension finie, alors on a $V = \bigoplus_{m\in\mathbb{Z}} V_m$.*

La définition ci-dessous aurait un sens (et un intérêt) pour tout groupe de Lie G et tout sous-groupe fermé $K \subset G$. Nous ne l'utiliserons que dans le cas $G = \mathrm{GL}_n(\mathbb{R})$ et $K = \mathrm{O}(n)$, ce que l'on suppose désormais pour fixer les idées. On pose $\mathfrak{g} = \mathfrak{gl}_n(\mathbb{R})$ et note $\mathfrak{k} \subset \mathfrak{g}$ le sous-espaces des matrices $X \in \mathrm{M}_n(\mathbb{R})$ avec $e^{tX} \in K$ pour tout $t \in \mathbb{R}$, i.e. des matrices antisymétriques (c'est l'algèbre de Lie de K). On pose aussi $\mathfrak{g}_\mathbb{C} = \mathfrak{g} \otimes_\mathbb{R} \mathbb{C} = \mathfrak{gl}_n(\mathbb{C})$.

Définition 5.3. *Un* $(\mathfrak{g}, K)$-module *(ou* module de Harish-Chandra*) est la donnée d'un $\mathbb{C}$-espace vectoriel V muni à la fois d'une structure de $\mathrm{U}(\mathfrak{g}_\mathbb{C})$-module et d'une représentation linéaire de K telles que :*

(HC1) en tant que représentation de K on a $V = \bigoplus_{\tau\in\mathrm{Irr}(K)} V_\tau$,

---

groupe $\mathbb{Z}$. Ainsi, si λ désigne la mesure de Lebesgue sur $\mathbb{R}$ telle que $\lambda([0,1[) = 1$, l'invariance par translation de λ entraîne immédiatement que la mesure borélienne sur $\mathrm{SO}(2)$ définie par $\mu(X) = \lambda(\,[0,1[\cap \pi^{-1}(X)\,)$ est une mesure de Haar sur $\mathrm{SO}(2)$ (c'est ce que l'on fait en analyse de Fourier traditionnelle !). Si G est un groupe de Lie, comme $G = \mathrm{O}(n)$ ou (d'après Cartan) tout sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$, on dispose également d'un construction assez simple de la mesure de Haar à l'aide des formes volumes.

(HC2) pour tout $X \in \mathfrak{k}$ et tout $v \in V$, l'application $t \mapsto e^{tX}.v$ est dérivable en $t = 0$ et de dérivée $X.v$,

(HC3) pour tout $X \in \mathfrak{g}$, $k \in K$ et $v \in V$ on a $k \cdot (X \cdot v) = \mathrm{ad}_k(X) \cdot (k \cdot v)$.

La condition (HC2) a bien un sens car d'après (i) l'application $t \mapsto e^{tX}.v$ prend ses valeurs dans un espace de dimension finie. En fait, l'existence de la dérivée en question est automatique : c'est un exercice [2] de voir que tout morphisme de groupes continu $\mathbb{R} \to \mathrm{GL}_n(\mathbb{C})$ est de la forme $t \mapsto e^{At}$ pour un unique $A \in \mathrm{M}_n(\mathbb{C})$.

Les $(\mathfrak{g}, K)$-modules forment une catégorie de manière évidente : un morphisme est une application $\mathbb{C}$-linéaire commutant aux actions de K et $\mathfrak{g}_{\mathbb{C}}$, on a des sommes directes évidentes, une notion de sous-$(\mathfrak{g}, K)$-module (=un sous-espace vectoriel stable par K et $\mathfrak{g}$), etc.. C'est une catégorie abélienne, qui est même munie d'un produit tensoriel (voir l'exemple (d) ci-dessous). Un $(\mathfrak{g}, K)$-module V est dit irréductible s'il est non nul et s'il ne possède pas de sous-$(\mathfrak{g}, K)$-module autre que 0 et V.

Exemple 5.4. (a) Le sous-espace $\mathcal{C}^\infty(G)_{K-\mathrm{fini}}$ des éléments K-finis de $\mathcal{C}^\infty(G)$ pour les translations à droite est un $(\mathfrak{g}, K)$-module (bien entendu, pour la représentation de $\mathfrak{g}$ donnée par les R_X et la Proposition 4.1). Pour vérifier l'axiome (HC2), on pourra observer que si $W \subset \mathcal{C}^\infty(G)$ est un sous-espace vectoriel de dimension finie, on peut trouver un nombre fini d'éléments $g_i \in G$ tels que les formes linéaires $f \mapsto f(g_i)$ engendrent W^*.

(b) Pour tout sous-groupe discret $\Gamma \subset G$, l'espace des formes automorphes $\mathrm{A}(G; \Gamma)$ est un sous-$(\mathfrak{g}, K)$-module de $\mathcal{C}^\infty(G)_{K-\mathrm{fini}}$ (Proposition 4.18).

(c) Soit V un espace vectoriel de dimension finie et $\rho : G \to \mathrm{GL}(V)$ une représentation de classe $\mathcal{C}^\infty$. Alors l'espace V est muni d'une structure naturelle de $(\mathfrak{g}, K)$-module noté $\mathrm{d}V$: l'action de K est celle donnée par ρ, et l'action $\mathrm{d}\rho$ de $\mathfrak{g}$ est définie par $\mathrm{d}\rho(X)v = \frac{\partial}{\partial t_{|t=0}} e^{tX}.v$. La Proposition 4.1 appliquée aux coefficients matriciels de ρ, i.e. aux fonctions $g \mapsto \varphi(\rho(g).v)$ avec $v \in V$ et $\varphi \in V^*$, montre que $\mathrm{d}\rho$ est une représentation de $\mathfrak{g}$ et que $\mathrm{d}V$ est un $(\mathfrak{g}, K)$-module.

(d) Si V_1 et V_2 sont des $(\mathfrak{g}, K)$-modules, il existe une unique structure de $(\mathfrak{g}, K)$-module sur $V_1 \otimes_{\mathbb{C}} V_2$ telle que pour tout $X \in \mathfrak{g}$, tout $k \in K$, et tout $v, w \in V$ on ait $k.(v \otimes w) = (k.v) \otimes (k.w)$ et $X.(v \otimes w) = (X.v) \otimes w + v \otimes (X.w)$.

Remarque 5.5. (Remarques informatives mais non utilisées dans la suite)

(i) On peut montrer la réciproque suivante de l'exemple (c) : tout $(\mathfrak{g}, K)$-module W *de dimension finie* provient d'une et une seule représentation $G \to \mathrm{GL}(W)$ de classe $\mathcal{C}^\infty$ (plutôt que seulement du revêtement simplement connexe de $\mathrm{GL}_n(\mathbb{R})^+$ comme le donnerait la théorie de Lie). Un fait trivial mais utile est l'égalité $G = \mathrm{GL}_n(\mathbb{R})^+ K$.

2. En effet, soit f un tel morphisme. On choisit $\varphi : \mathbb{R} \to \mathbb{R}_{\geq 0}$ une fonction de classe $\mathcal{C}^\infty$, à support compact telle que l'intégrale $I = \int_{\mathbb{R}} \varphi(t) f(t) \mathrm{d}t$ est dans $\mathrm{GL}_n(\mathbb{R})$. On a alors pour tout $x \in \mathbb{R}$ la relation $f(x)\, I = \int_{\mathbb{R}} \varphi(t) f(x+t) \mathrm{d}t = \int_{\mathbb{R}} \varphi(t-x) f(t) \mathrm{d}t$, qui montre que f est de classe $\mathcal{C}^\infty$. On peut donc dériver l'égalité $f(t+x) = f(t)f(x)$ en $t = 0$, et on obtient $f'(x) = Af(x)$ avec $A = f'(0) \in \mathrm{M}_n(\mathbb{C})$, puis $f(x) = e^{Ax}$.

(ii) La construction donnée au (c) s'étend avec peu de modifications aux *représentations unitaires* $\rho : G \to \mathrm{U}(V)$ sur un espace de Hilbert V (rappelons que cela signifie que pour tout $v \in V$ l'application $g \mapsto \rho(g).v$ est continue). On prend dans ce cas pour espace sous-jacent à $\mathrm{d}V$ le sous-espace $V' \subset V$ constitué des vecteurs v qui sont K-finis et tels que $g \mapsto \rho(g).v$ est de classe $\mathcal{C}^\infty$ (en tant que fonction sur G à valeurs dans V), et les mêmes actions de K et de $\mathfrak{g}$. Un argument basé sur de la convolution montre que V' est dense dans V (Gärding, Peter-Weyl). Harish-Chandra montre que $V \mapsto \mathrm{d}V$ est une bijection entre classe d'isomorphisme de représentations unitaires de G et classes d'isomorphisme de $(\mathfrak{g}, V)$-modules unitaires (en un sens assez évident). Nous renvoyons à l'introduction de l'article de Casselman sus-cité, à l'article de W. Baldoni dans le livre [BK] référencé pour un survol de la théorie, et aux chapitres I,III, et VI du livre de Knapp référencé pour un exposé complet. La Proposition 5.21 de ce chapitre est un énoncé clef dans ces directions.

Définition 5.6. *Un $(\mathfrak{g}, K)$-module V est dit admissible si on a $\dim V_\tau < \infty$ pour tout $\tau \in \mathrm{Irr}(K)$.*

On véifie aisément qu'un sous-module (resp. un quotient) d'un $(\mathfrak{g}, K)$-module admissible est encore admissible (voir l'exercice 5.2). Avant d'énoncer le premier théorème de finitude dont nous aurons besoin, nous devons faire deux observations. Soient V un $(\mathfrak{g}, K)$-module et $v \in V$.

(a) La propriété (HC3) montre que le sous-espace $\mathrm{U}(\mathfrak{g}_\mathbb{C}) \cdot \mathbb{C}[K] \cdot v$ est stable par K (et évidemment par $\mathfrak{g}_\mathbb{C}$) : c'est le sous-$(\mathfrak{g}, K)$-module *engendré* par v. Le plus petit sous-$(\mathfrak{g}, K)$-module de V contenant une famille d'éléments v_i de V est donc $\sum_i \mathrm{U}(\mathfrak{g}_\mathbb{C}) \cdot \mathbb{C}[K] \cdot v_i$ ("sous $(\mathfrak{g}, K)$-module engendré par les v_i").

(b) Il est équivalent de demander que v est $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$-fini, et de demander qu'il existe un idéal de codimension finie $I \subset \mathfrak{z}(\mathfrak{g}_\mathbb{C})$ tel que $I.v =$. En effet, on a un isomorphisme $\mathfrak{z}(\mathfrak{g}_\mathbb{C}).v \simeq \mathfrak{z}(\mathfrak{g}_\mathbb{C})/I_v$ où $I_v = \{z \in \mathfrak{z}(\mathfrak{g}_\mathbb{C}), zv = 0\}$ est l'idéal annulateur de v dans $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$. En utilisant d'une part que l'action de $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$ commute à K et à $\mathrm{U}(\mathfrak{g}_\mathbb{C})$, et d'autre part qu'une intersection finie d'idéaux de codimension finie est de codimension finie, on constate que si V est engendré par un nombre fini d'éléments $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$-finis, alors il existe un idéal $I \subset \mathfrak{z}(\mathfrak{g}_\mathbb{C})$ de codimension finie tel que $IV = 0$ (i.e. I annule tout élément de V).

Théorème 5.7. (Harish-Chandra) *Soit V un $(\mathfrak{gl}_n(\mathbb{R}), \mathrm{O}(n))$-module annulé par un idéal de codimension finie de $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$. Les assertions suivantes sont équivalentes :*

(i) V est de longueur finie : il existe une suite finie de sous-$(\mathfrak{gl}_n(\mathbb{R}), \mathrm{O}(n))$-module $V_0 = 0 \subset V_1 \subset \cdots \subset V_m = V$ avec V_i/V_{i-1} irréductible pour $i = 1, \ldots, m$,

(ii) V est engendré par un nombre fini d'éléments,

(iii) V est admissible.

La seule implication évidente dans ce théorème est (i) ⇒ (ii). De plus, le théorème tout entier est facile et laissé en exercice au lecteur dans le cas $n = 1$. Nous le démontrerons pour $n = 2$ dans la section suivante.

Le second résultat de finitude suivant, également dû à Harish-Chandra, est central en théorie des formes automorphes. Si I est un idéal de $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$, on pose $V[I] = \{v \in V,\, I\, v\, = 0\}$. C'est un sous-$(\mathfrak{g}, K)$-module de V (utiliser, encore, que $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$-commute avec K et $\mathrm{U}(\mathfrak{g}_{\mathbb{C}})$).

Théorème 5.8. (Harish-Chandra) *Si Γ est un sous-groupe d'indice fini de $\mathrm{GL}_n(\mathbb{Z})$, et si I est un idéal de codimension finie de $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$, alors $\mathrm{A}(G;\Gamma)[I]$ est admissible (et donc de longueur finie).*

La démonstration de ce théorème est difficile (sauf pour $n = 1$, où c'est un exercice !). Dans ce cours, on se propose de le démontrer complètement uniquement dans le cas $n = 2$ et $\Gamma = \mathrm{GL}_2(\mathbb{Z})$. Nous renvoyons au chapitre 1 du livre de Harish-Chandra référencé pour le cas général. Harish-Chandra démontre en fait *loc. cit.* un énoncé encore plus général, dans lequel on a $G = \underline{G}(\mathbb{R})$ et Γ d'indice fini dans $\underline{G}(\mathbb{Z})$, où $\underline{G}$ est un schéma en groupes affine et de type fini sur $\mathbb{Z}$ supposé réductif sur $\mathbb{C}$.

Terminons par un énoncé général et utile dont la démonstration est élémentaire.

Proposition 5.9. *Soit V un $(\mathfrak{g}, K)$-module admissible et irréductible. Il existe un morphisme de $\mathbb{C}$-algèbres $\eta : \mathfrak{z}(\mathfrak{g}_{\mathbb{C}}) \to \mathbb{C}$ tel que $z.v = \eta(z)\, v$ pour tout $v \in V$ et tout $z \in \mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$.*

Démonstration — Soit τ avec $V_\tau \neq 0$. L'action de $\mathfrak{z}$ commute à K (axiome (HC3) et Proposition 4.8), elle préserve donc V_τ et forme une famille commutative d'endomorphismes de ce dernier. Comme V_τ est de dimension finie sur $\mathbb{C}$ par hypothèse, il existe un vecteur $e \in V_\tau - \{0\}$ propre pour tous les éléments de $\mathfrak{z}$ ("cotrigonalisation"). On pose $z.e = \eta(z)\, e$. Le sous-$\mathrm{U}(\mathfrak{g}_{\mathbb{C}})$-module $\mathrm{U}(\mathfrak{g}).V_\tau$ est stable par K (axiome (HC3)), c'est donc V tout entier, et z y agit par multiplication par $\eta(z)$. □

Définition 5.10. *Soit V un $(\mathfrak{g}, K)$-module admissible et irréductible. L'homomorphisme $\eta : \mathfrak{z}(\mathfrak{g}_{\mathbb{C}}) \to \mathbb{C}$ de la proposition 5.9 est appelé caractère infinitésimal de V. On le notera η_V.*

Remarque 5.11. Observons que si V est irréductible admissible, alors $\ker \eta_V$ est un idéal de codimension finie de $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$ annulant V, on a même $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})/(\ker \eta_V) \simeq \mathbb{C}$. On en déduit que tout $(\mathfrak{g}, K)$-module admissible de longueur finie est annulé par un idéal de codimension finie dan $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$. En effet, soit $V_0 \subset V_1 \subset \cdots \subset V_m = V$ une suite croissante de sous-$(\mathfrak{g}, K)$-modules avec V_i/V_{i-1} irréductibles pour $i = 1, \ldots, m$. L'admissibilité de V entraîne celle des V_i/V_{i-1}. On pose $I_i = \ker \eta_{V_i/V_{i-1}}$. L'idéal $\prod_{i=1}^m I_i$ annule V ; il est de codimension finie car $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$ est de type fini sur $\mathbb{C}$ (fait que nous n'avons montré entièrement que pour $n \leq 2$).

2. $(\mathfrak{g}, K)$-modules pour $\mathrm{GL}_2(\mathbb{R})$

Dans toute cette partie on a $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{R})$ et $K = \mathrm{O}(2)$. On pose aussi $\mathfrak{z} = \mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$. On se propose de démontrer dans ce cas le Théorème 5.7. Au passage nous classifierons, suivant Bargmann, les $(\mathfrak{g}, K)$-modules admissibles irréductibles pour $\mathrm{GL}_2(\mathbb{R})$. Fixons un $(\mathfrak{g}, K)$-module V. On a la décomposition

$$V_{|\mathrm{SO}(2)} = \bigoplus_{m \in \mathbb{Z}} V_m, \tag{32}$$

qui découle de l'axiome (HC1) et du Corollaire 5.2. On rappelle aussi la base Z, h', e', f' de $\mathfrak{gl}_2(\mathbb{C})$ introduite au chapitre pécédent, on les renomme ici simplement Z, h, e, f pour ne pas multiplier les "primes". Faisons quelques observations élémentaires :

(O1) $h.\,v = m\,v$ pour tout $v \in V_m$,

En effet, c'est une conséquence directe de l'axiome (HC2).

(O2) $e\,V_m \subset V_{m+2}$ et $f\,V_m \subset V_{m-2}$ pour tout $n \in \mathbb{Z}$,

En effet, la relation $[h, e] = 2e$ montre que pour $v \in V_m$ on a $hev = (eh + [h, e])\,v = eh\,v + 2\,ev = (m+2)v$ et donc $v \in V_{m+2}$ par la formule (32) et (O1). L'argument est similaire pour $f\,V_m \subset V_{m-2}$ en utilisant $[h, f] = -2f$.

(O3) Posons $C' = C - Z^2/2 \in \mathfrak{z}$ et notons P le polynôme $P(X) = X^2/2 + X = \frac{1}{2}((X+1)^2 - 1)$. On a les égalités suivantes dans $\mathrm{U}(\mathfrak{g}_{\mathbb{C}})$:

$$2\,fe = C' - P(h) \text{ et } 2\,ef = C' - P(h-2). \tag{33}$$

En particulier, pour tout $m \in \mathbb{Z}$ et tout $v \in V_m$, on a

$$2\,fe\,v = (C' - P(m))\,v \text{ et } 2\,ef\,v = (C' - P(m-2))\,v. \tag{34}$$

(O4) Si s_0 désigne l'élément $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ de $\mathrm{O}(2)$, on a $\mathrm{O}(2) = \mathrm{SO}(2) \coprod s_0\,\mathrm{SO}(2)$ et $s_0 \mathrm{s}_\lambda s_0^{-1} = \mathrm{s}_{\overline{\lambda}}$ pour tout $\lambda \in \mathbb{C}^\times$, et $\mathrm{ad}(s_0)$ échange e et f. En particulier, on a $s_0(V_m) = V_{-m}$ pour tout $m \in \mathbb{Z}$.

Pour $v \in V$, on pose $W(v) = \sum_{n\geq 1} \mathbb{C}e^n v + \mathbb{C}v + \sum_{n\geq 1} \mathbb{C}f^n v$. On a $\mathrm{s}_0(W(v)) = W(\mathrm{s}_0(v))$ par (O4).

Lemme 5.12. *Soient V un $(\mathfrak{g}, K)$-module engendré un élément $v_{m_0} \in V_{m_0}$, et $W = W(v_{m_0})$. Alors $\mathfrak{z}W$ est stable par $\mathrm{SO}(2)$ et $\mathfrak{g}$, et on a $V = \mathfrak{z}\,W + \mathfrak{z}\,s_0\,W$.*

Démonstration — $\mathfrak{z}W$ est évidemment stable par Z. Les identités (O1) et (O2) montrent de plus qu'il est stable par h et $\mathrm{SO}(2)$. L'identité (O3) montre que pour $v \in V_m$, on a $ef\,v \in \mathbb{C}[C'].v \subset \mathfrak{z}v$, et aussi $fe\,v \in \mathfrak{z}v$. Cela implique que pour $n \geq 1$ on a $fe^n v_{m_0} \subset \mathbb{C}[C, Z]e^{n-1}v_{m_0}$, et un énoncé similaire en échangeant e et f : on a bien $eW \subset \mathfrak{z}W$ et $fW \subset \mathfrak{z}W$. □

Corollaire 5.13. *L'implication (ii) ⇒ (iii) du Théorème 5.7 est vraie pour $n = 2$.*

Démonstration — Supposons V finiment engendré et annulé par l'idéal de codimension finie $I \subset \mathfrak{z}$. Comme une somme directe finie de $(\mathfrak{g}, K)$-modules admissible est admissible, et comme un quotient d'un $(\mathfrak{g}, K)$-module admissible est admissible, on peut supposer que V est engendé par un seul élément, et même que cet élément dans V_{m_0} pour un certain $m_0 \in \mathbb{Z}$, on le note v_{m_0}. Lemme montre que pour $m \in \mathbb{Z}$ on a $V_m \subset \mathfrak{z}W_m + \mathfrak{z}W_{-m}$, où $W = W(v_0)$. Mais on constate sur la définition de $W(v_0)$ que W_m est de dimension ≤ 1 pour tout $m \in \mathbb{Z}$. Comme W_m est annulé par l'idéal de codimension finie $I \subset \mathfrak{z}$, on a bien $\dim \mathfrak{z}W_m < \infty$. □

Corollaire-Définition 5.14. *Si V est un $(\mathfrak{g}, K)$-module, on note $\mathrm{m}(V)$ l'ensemble des entiers $m \in \mathbb{Z}$ avec $V_m \neq 0$. Si V est irréductible, ou plus généralement si V est engendré par un élément $v \in V_m$ pour un certain $m \in \mathbb{Z}$, alors on a $\mathrm{m}(V) \subset m + 2\mathbb{Z}$.*

Démonstration — C'est une conséquence immédiate du Lemme 5.12 si l'on remarque que pour tout $n \in \mathbb{Z}$ on a $\mathfrak{z} V_n \subset V_n$ et $\mathrm{s}_0(V_n) = V_{n-2n}$. □

Proposition 5.15. *Soient V un $(\mathfrak{g}, K)$-module. On suppose qu'il existe un entier $k > 0$ et un élément $v \in V_{-k}$ engendrant V et vérifiant les relations : $ev = 0$ et $Zv = sv$ pour un certain $s \in \mathbb{C}$.*

Alors V est irréductible et sa classe d'isomorphisme est uniquement déterminée par s et k. De plus, on a $\dim V_m \leq 1$ pour tout $m \in \mathbb{Z}$ et $\mathrm{m}(V)$ et l'ensemble de tous les entiers $m \in \mathbb{Z}$ vérifiant $m \equiv k \bmod 2$ et $|m| \geq k$.

Démonstration — Les relations $hv = -kv$, $ev = 0$ et $C' = P(h) + 2fe$ entraînent $C'v = P(-k)v$. En particulier, on a $z.v = \eta(z)v$ avec η l'unique morphisme d'algèbres $\mathfrak{z} = \mathbb{C}[C', Z] \to \mathbb{C}$ tel que $\eta(Z) = s$ et $\eta(C') = P(-k)$. L'égalité $z.w = \eta(z)w$ vaut alors pour tout $w \in V$ car v engendre V. On a manifestement $W(v) = \sum_{n \geq 0} \mathbb{C} f^n v$, ainsi donc que $\mathrm{s}_0 W(v) = \sum_{n \geq 0} \mathbb{C} e^n \mathrm{s}_0(v)$ par (O4), et aussi $V = W(v) \oplus W(\mathrm{s}_0\, v)$ par le lemme 5.12. D'après (O3), on a pour tout $n \geq 0$,

$$2\, ef^n\, v \;=\; (\eta(C') - P(-k-2n))\, f^{n-1}\, v. \tag{35}$$

Cette formule et l'inégalité $P(a) > P(b)$ pour $a < b \leq -1$ montrent que $f^n v$ est non nul pour tout $n \geq 0$ (par récurrence sur n). L'assertion sur $\mathrm{m}(V)$ et les $\dim V_m$ s'en déduisent. On observe aussi que la classe d'isomorphisme de V est entièrement déterminée par k et s. L'assertion d'irréductibilité est évidente : tout sous-$(\mathfrak{g}, K)$-module $U \subset V$ vérifie $U_m \neq 0$ pour un certain $m \in \mathbb{Z}$, et l'on peut même supposer $m \leq 0$ à cause de s_0 ; contient donc $f^n v$ pour un certain entier $n \geq 0$, il contient donc $e^n f^n v$ qui est un multiplie non nul de v par la formule (35). □

Cette proposition s'applique par exemple au $(\mathfrak{g}, K)$-module engendré par la fonction $\Phi_f(g) |\det(g)|^{(k+s)/2} \in \mathcal{C}^\infty(G)$ pour tout $f \in \mathrm{M}_k$ et tout $s \in \mathbb{Z}$, par le Théorème 4.25. Cela montre que pour tout k pair > 2, et tout $s \in \mathbb{C}$, il existe un $(\mathfrak{g}, K)$-module satisfaisant les hypothèses de l'énoncé ci-dessus (prendre $f = \mathrm{E}_k$). Il ne serait pas difficile de montrer qu'un tel $(\mathfrak{g}, K)$-module existe dans tous les autres cas (i.e. k impair et $k = 2$) ; on note $\mathrm{D}_{k,s}$ ce $(\mathfrak{g}, K)$-module. Noter en particulier que deux formes modulaires de même poids engendrent des $(\mathfrak{g}, K)$-modules isomorphes (à savoir $\mathrm{D}_{k,-k}$).

Théorème 5.16. (Bargmann) *Soit V un $(\mathfrak{gl}_2(\mathbb{R}), \mathrm{O}(2))$-module admissible irréductible. On pose $\eta = \eta_V$ et $s = \eta(Z)$. On est dans un, et un seul, des cas suivants :*

(i) $\eta(C')$ est de la forme $P(-k)$ avec $k \geq 1$.

Dans ce cas, soit V est isomorphe à $\mathrm{D}_{k,s}$, soit on a $k \geq 2$ et V est le $(\mathfrak{g}, K)$-module associé à la représentation $(\mathrm{Sym}^{k-2} \mathbb{C}^2) \otimes |\det|^{(s-k)/2} \chi$ de $\mathrm{GL}_2(\mathbb{R})$, où χ est l'un des deux caractères $\mathrm{GL}_2(\mathbb{R}) \to \{\pm 1\}$.

(ii) $\eta(C')$ n'est pas de la forme $P(m)$ avec $m \in \mathrm{m}(V)$.

Dans ce cas on a soit $\mathrm{m}(V) = 2\mathbb{Z}$ *(cas "pair"), soit* $\mathrm{m}(V) = 2\mathbb{Z}+1$ *(cas "impair"), ainsi que* $\dim V_m \leq 1$ *pour tout* $m \in \mathbb{Z}$*. La classe d'isomorphisme de* V *est uniquement déterminée par* η_V *et par une donnée supplémentaire définie ci-dessous qui ne peut prendre que deux valeurs. Dans le cas pair, cette donnée est simplement la valeur propre de* s_0 *sur la droite* V_0 *(un signe* ± 1*).*

Démonstration — Supposons d'abord que la multiplication par e est injective dans V. La relation $\mathrm{ad}_{\mathrm{s}_0} e = f$ montre qu'il en va de même de la multiplication par f, et donc de celle par ef, qui préserve V_m pour tout m. Les Formules (33) montrent que $\eta(C')$ n'est pas de la forme $P(m)$ avec $m \in \mathrm{m}(V)$ et que les multiplications par e et f sont bijectives dans V. En particulier, on a $\mathrm{m}(V) \cap \{0,1\} \neq \emptyset$.

Si $0 \in \mathrm{m}(V)$, i.e. $V_0 \neq 0$, on peut choisir un élément $v \in V_0 - \{0\}$ vecteur propre de s_0 ; on a alors $\mathrm{s}_0(v) = \pm v$. On constate que $W(v)$ est stable par $\mathrm{O}(2)$ et $\mathfrak{g}$, donc $V = W(v)$, et on en déduit le (ii) dans le cas pair.

Si $1 \in \mathrm{m}(V)$, on choisit cette fois-ci $v \in V_1$ vecteur propre de l'endomorphisme bijectif $\mathrm{s}_0 f : V_1 \to V_1$. Le carré de cet endomorphisme est $\mathrm{s}_0 f \mathrm{s}_0 f = ef$ (car $\mathrm{ad}_{s_0}(f) = e$), et (35) montre que $2ef$ coincide avec la multiplication par $\lambda := \eta(C') - P(-1)$ sur V_1, un scalaire qui est non nul par hypothèse. On a donc $\mathrm{s}_0 f v = \mu v$ avec $2\mu^2 = \lambda$ (au plus deux possibilités pour μ, et $V = W(v)$: on conclut comme précédemment.

Faisons maintenant l'hypothèse, restante, que la multiplication par e n'est pas injective dans V. Soient $m \in \mathbb{Z}$ et $v \in V_m - \{0\}$ avec $ev = 0$. La formule $C' = 2fe + P(h)$ montre $C'v = P(m)v$. Si $m = -k$ avec $k \geq 1$, la Proposition 5.15 montre $V \simeq \mathrm{D}_{k,s}$ avec $s = \eta(Z)$. On peut donc supposons que l'on a $m \geq 0$.

Les relations $\eta(C') = P(m)$, $2ef^{m+1} v = (\eta(C') - P(-m-2))\, f^m v$ et $P(X) = P(-X-2)$ montrent $2\, ef^{m+1} v = 0$. La Proposition 5.15 appliquée au sous-$(\mathfrak{g}, K)$-module U engendré par l'élément $f^{m+1}v$ de V_{-m-2} montre $U_k = 0$ pour $|k| \leq m$ et donc $v \notin U$. On en déduit $U = 0$ par irréductibilité de V, i.e. $f^{m+1}v = 0$. Cela montre que $W(v)$ est de dimension finie, et aussi $e\mathrm{s}_0 f^m v = \mathrm{s}_0 f^{m+1} v = 0$. Les Formules (34) montrent enfin $f^i v \neq 0$ pour $0 \leq i \leq m$. En particulier, on a montré que $u(x) := \mathrm{s}_0 f^m x$ est un automorphisme du sous-espace (non nul) de V_m constitué des vecteurs annulés par e. On peut donc choisir $v \in V_m - \{0\}$ vecteur propre de u pour une certaine valeur propre μ, i.e. vérifiant $\mathrm{s}_0 f^m v = \mu v$. Mais u^2 n'est autre que la multiplication par $e^m f^m$, i.e. par le scalaire non nul $2^{-m}\lambda = \prod_{n=1}^{m} (P(m) - P(m-2n)$, de sorte qu'il n'y a que deux choix pour μ. Au final, on a $U = W(v)$. Posons $k - 2 = m$. Alors U est manifestement irréductible de dimension $k-1$, vérifie $\nu(C') = P(m) = P(-k)$, et sa structure de $(\mathfrak{g}, K)$-module ne dépend que de l'entier $k \geq 2$, du complexe $\eta(Z) \in \mathbb{C}$, et de la racine carrée μ de λ. Nous laissons au lecteur le soin de vérifier que les représentations de l'énoncés fournissent effectivement de tels $(\mathfrak{g}, K)$-modules, le choix de χ correspondant à celui de μ. □

Il ne serait pas difficile de montrer que les $(\mathfrak{g}, K)$-modules suggérés par le (ii) du théorème ci-dessus existent vraiment (voir, par exemple, les notes de Casselman référencées). Par exemple, pour tout morphisme d'algèbre $\eta : \mathfrak{z} \to \mathbb{C}$ avec $\eta(C') \notin P(2\mathbb{Z})$, et pour tout signe $\varepsilon \in \{\pm 1\}$, il existe un $(\mathfrak{g}, K)$-module irréductible admissible $\mathrm{P}_{\eta,\varepsilon}$ (unique à isomorphisme près d'après le théorème ci-dessus) ayant les propriétés suivantes : son caractère infinitésimal est η, V_0 est de dimension 1 et s_0 y agit par multiplication par ε, et $\mathrm{m}(V) = 2\mathbb{Z}$. On voit que tout $(\mathfrak{g}, K)$-module V est

engendré par un vecteur $v \in V_0 - \{0\}$ tel que $\mathrm{s}_0 v = \epsilon v$, et tel que $z.v = \eta(z)v$ avec $\eta(C') \notin P(2\mathbb{Z})$, est irréductible et isomorphe à $\mathrm{P}_{\eta,\varepsilon}$.

Remarque 5.17. (Formes de Maass) Soient $\eta : \mathfrak{z} \to \mathbb{C}$ avec $\eta(C') \notin P(2\mathbb{Z})$ et $\epsilon = \pm 1$; on pose $s = \eta(Z)$. Supposons que $\Phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{C}$ est une forme automorphe pour $\mathrm{GL}_2(\mathbb{Z})$ invariante par $\mathrm{SO}(2)$ et engendrant un $(\mathfrak{g}, K)$-module isomorphe à $\mathrm{P}_{\eta,\varepsilon}$. La fonction $f : \mathbb{H} \to \mathbb{C}$, $\tau \mapsto \Phi(\mathrm{p}_\tau)$ a les propriétés suivantes :

(i) f est modulaire de poids $|\cdot|^s$ et vérifie $f(-\overline{\tau}) = \epsilon f(\tau)$,

(ii) f est de classe $\mathcal{C}^\infty$ et vérifie $-2(\mathrm{Im}\,\tau)^2 \frac{\partial^2}{\partial\tau\partial\overline{\tau}} f(\tau) = \eta(C) f(\tau)$ (Corollaire 4.24),

(iii) il existe une constante $N > 0$ telle que l'on ait $|f(\tau)| = \mathrm{O}(\mathrm{Im}\,\tau)^N$ quand $\mathrm{Im}\,\tau$ tend vers l'infini.

Une telle fonction est appelée *forme de Maass*. Un argument similaire à celui du paragraphe §5 Chap. 4 montrerait réciproquement que pour toute forme de Maass f, la fonction Φ_f engendre un $(\mathfrak{g}, K)$-module isomorphe à $\mathrm{P}_{\eta,\varepsilon}$.

Théorème 5.18. *Il n'existe qu'un nombre fini de $(\mathfrak{gl}_2(\mathbb{R}), \mathrm{O}(2))$-modules admissibles irréductibles ayant un caractère infinitésimal donné (en fait, il y en a au plus 3). L'implication (ii) ⇒ (iii) du Théorème 5.7 est vraie pour $n = 2$.*

Démonstration — Le premier point résulte par inspection du théorème précédent. Pour le second, un dévissage simple (voir l'exercice 5.3) permet de supposer que le $(\mathfrak{g}, K)$-module admissible V admet un caractère infinitésimal η (et on veut montrer que V est de longueur finie). Il en va alors de même de tous ses sous-quotients. Étant donné qu'il n'y a qu'un nombre fini de $(\mathfrak{g}, K)$-modules admissibles irréductibles de caractère infinitésimal η d'après le premier point du théorème, il ne reste qu'à voir que tout $(\mathfrak{g}, K)$-module non nul U admet un sous-quotient irréductible. Soit $u \in U - \{0\}$, on considère d'une part $U' \subset U$ le sous-$(\mathfrak{g}, K)$-module engendré par u, et d'autre part $U'' \subset U'$ un sous-$(\mathfrak{g}, K)$-module maximal ne contenant pas u (existence assurée par Zorn) : le $(\mathfrak{g}, K)$-module U'/U'' est manifestement irréductible (cet argument est très similaire à celui montrant que tout module sur un anneau admet un sous-quotient simple). □

3. Le théorème d'harmonicité de Harish-Chandra

Soient $n \geq 1$ est un entier, $G = \mathrm{GL}_n(\mathbb{R})$, $K = \mathrm{O}(n) \subset G$, $\mathfrak{g} = \mathrm{gl}_n(\mathbb{R})$ et $\mathfrak{g}_\mathbb{C} = \mathfrak{gl}_n(\mathbb{C})$.

Comme tout groupe topologique localement compact, le groupe G admet des mesures de Haar des deux côtés. L'existence d'une telle mesure dans le cas d'espèce est très simple. En effet, la multiplication par g, aussi bien à droite qu'à gauche, est un $\mathcal{C}^\infty$-difféomorphisme (linéaire !) de $\mathrm{M}_n(\mathbb{R})$, dont le Jacobien est constant et manifestement égal à $|\det g|^n$. En effet, chacune des n colonnes C de $\mathrm{M}_n(\mathbb{R})$ est un sous-espace vectoriel G-stable (pour les translations à gauche), et on a $C \simeq \mathbb{R}^n$ en tant que représentation de G. La mesure borélienne > 0 sur G définie par la formule

$$\mathrm{d}g = \frac{\prod_{i,j} \mathrm{d}g_{i,j}}{|\det g|^n}$$

est donc invariante par multiplication à droite et à gauche par des éléments de G : c'est une mesure de Haar (à droite et à gauche), et G est *unimodulaire*. Lorsque $n = 1$, c'est la mesure invariante bien connue $\frac{\mathrm{d}x}{|x|}$ sur le groupe multiplicatif $\mathbb{R}^\times$.

Soient $f, f' : G \to \mathbb{C}$ deux fonctions continues avec f' à support compact. On peut définir le *produit de convolution*

$$(f * f')(g) = \int_G f(gh) f'(h^{-1}) \mathrm{d}h = \int_G f(h) f'(h^{-1} g) \mathrm{d}h.$$

Il suffirait même de supposer que f est intégrable sur G pour la convergence absolue de la première intégrale, et l'égalité avec la seconde résulte de l'invariance de $\mathrm{d}h$ par $h \mapsto gh$ pour tout $g \in G$. Pour tout $g \in G$ on a manifestement :

$$\mathrm{R}_g(f * f') \;=\; f * (\mathrm{R}_{g'} f'). \tag{36}$$

La multiplication $G \times G \to G$ étant de classe $\mathcal{C}^\infty$, on observe de manière classique que si f ou f' est dans $\mathcal{C}^\infty(G)$, alors on a $f * f' \in \mathcal{C}^\infty(G)$. De plus, pour tout $f' \in \mathcal{C}^\infty(G)$ et tout $X \in \mathfrak{g}$, on a la formule

$$\mathrm{R}_X(f * f') = f * (\mathrm{R}_X\, f'). \tag{37}$$

Par récurrence sur le degré, on en déduit que cette égalité vaut encore si l'on remplace R_X par un élément quelconque de $\mathrm{U}(\mathfrak{g}_\mathbb{C})$.

On notera $\mathrm{I}_c^K(G) \subset \mathrm{C}^\infty(G)$ le sous-espace des fonctions φ à support compact, et invariante par conjugaison par K, c'est-à-dire vérifiant $\varphi(kgk^{-1}) = \varphi(g)$ pour tout $g \in G$ et tout $k \in K$. Le résultat suivant affirme que les fonctions K-finies et $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$-finie se comportent un peu comme des fonctions harmoniques.

Théorème 5.19. (Harish-Chandra) *Soit $f \in \mathcal{C}^\infty(G)$. On suppose que :*

(i) f est K-finie (pour les translations à droite),

(ii) f est $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$-finie.

Alors pour tout voisinage U de 1 dans G, il existe $\varphi \in \mathrm{I}_c^K(G)$ nulle en dehors de U vérifiant $f = f * \varphi$.

Avant de discuter la démonstration de ce théorème, mentionnons la conséquence importante suivante pour les formes automorphes. Elle montre d'une part qu'il suffit de supposer f à croissance modérée dans l'axiome (AF4) de la définition des formes automorphes, et d'autre part que l'exposant de croissance peut être choisi de manière uniforme tout les $u.f$ avec $u \in \mathrm{U}(\mathfrak{g}_\mathbb{C})$: on dit parfois que les formes automorphes sont à croissance *uniformément modérée*. Ce second point jouera un rôle crucial pour voir que les formes automorphes "cuspidales unitaires" sont bornées.

Corollaire 5.20. *Soit $f \in \mathcal{C}^\infty(G)$ une fonction K-finie (à droite) et $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$-finie. On suppose qu'il existe des réels $c, N > 0$ tels que $|f(g)| \leq c\,||g||^N$ pour tout $g \in G$. Alors pour tout $u \in \mathrm{U}(\mathfrak{g}_\mathbb{C})$ il existe un réel $c(u) > 0$ telle que l'on ait*

$$|(u.f)(g)| \;\leq\; c(u)\,||g||^N, \quad \forall\, g \;\in\; G.$$

En particulier, $u.f$ est à croissance modérée pour tout $u \in \mathrm{U}(\mathfrak{g}_\mathbb{C})$.

Démonstration — Soit $\psi : G \to \mathbb{C}$ une fonction continue et à support dans un compact $\Omega \subset G$. L'inégalité $||gh|| \leq ||g|||h||$ montre

$$|f * \psi(g)| \leq \int_\Omega |f(gh)\psi(h^{-1})|\mathrm{dg} \leq \mathrm{vol}(\Omega)\, M_1\, M_2\, c\, ||g||^N,$$

où on a posé $M_1 = \sup_{h\in\Omega}|\psi(h)|$ et $M_2 = \sup_{h\in\Omega}||h||$. Autrement dit, $f*\psi$ est à croissance modérée, avec le même exposant que f, et pour la constante $\mathrm{vol}(\Omega)\, M_1\, M_2\, c$. Écrivons maintenant $f = f*\varphi$ avec $\varphi \in \mathrm{I}_c^K(G)$ à support dans un voisinage compact U de 1. Pour $u \in \mathrm{U}(\mathfrak{g}_\mathbb{C})$ on a $u \cdot f = f * (u.\varphi)$ par la formule 37, et $u \cdot \varphi$ est bien entendu continue à support compact (par définition, elle est nulle hors d'un ouvert arbtraire contenant U). On conclut en appliquant le premier paragraphe à $\psi = u \cdot \varphi$. □

La démonstration du Théorème 5.19 est difficile. La méthode que nous suivons est inspirée de l'exposition de Borel dans le chapitre 2 de [B]. Un ingrédient important de l'argument est l'assertion (ii) ⇒ (iii) du Théorème 5.7 (que nous n'avons démontré que pour $n \leq 2$). Un autre est le suivant, dans lequel l'espace vectoriel $\mathcal{C}^\infty(G)$ est muni de sa structure naturelle d'espace de Fréchet (on n'utilise ici que la structure de G comme variété différentielle, en l'occurence un ouvert de $\mathrm{M}_n(\mathbb{R})$). On rappelle que sa topologie est métrisable et qu'une suite de fonctions $f_n \in \mathcal{C}^\infty(G)$ converge si, et seulement si, elle converge uniformément sur tout compact de G, ainsi que ses dérivées partielles de tout ordre (par exemple, relativement aux n^2 coordonnées $m_{i,j}$).

Proposition 5.21. *Soient $W \subset \mathcal{C}^\infty(G)_{\mathrm{K-fini}}$ un sous-$(\mathfrak{g}, K)$-module et V l'adhérence de W dans $\mathcal{C}^\infty(G)$.*

(i) Si W est annulé par un idéal de codimension finie dans $\mathfrak{z}(\mathfrak{g}_\mathbb{C})$, alors V est stable par R_g pour tout $g \in G$.

(ii) Si W est admissible alors tout vecteur K-fini de V est dans W.

Démonstration — Le point (i), le plus délicat, sera démontré plus bas. Vérifions le (ii). Pour $f : G \to \mathbb{C}$ continue, $m \in \mathbb{Z}$ et $g \in G$, on pose $\mathrm{P}_m(f)(g) = \int_{\mathrm{SO}(2)} \epsilon(k)^{-m} f(gk)\,\mathrm{d}k$ (où $\mathrm{d}k$ est la mesure de Haar évidente sur $\mathrm{SO}(2)$). Il est clair que P_m définit un endomorphisme continu de $\mathcal{C}^\infty(G)$ qui est un projecteur d'image $\mathrm{C}^\infty(G)_m$. Par définition de V, $\mathrm{P}_m(V)$ est dans l'adhérence de $\mathrm{P}_m(W) = W_m$. Mais comme W_m est de dimension finie par hypothèse, il est fermé dans le Fréchet $\mathcal{C}^\infty(G)$, et donc $\mathrm{P}_m V \subset W_m$. □

Montrons que cette proposition implique le Théorème 5.19. On l'applique au $(\mathfrak{g}, K)$-module W engendré par la fonction f ; et on note encore V l'adhérence de W dans $\mathcal{C}^\infty(G)$. Comme l'application $G \times \mathcal{C}^\infty(G) \to \mathcal{C}^\infty(G)$, $(g, v) \mapsto \mathrm{R}_g v$, est manifestement continue, et comme $\mathcal{C}^\infty(G)$ est espace de Fréchet, il y a un sens à définir l'intégrale[3] $\int_G \psi(h^{-1})\mathrm{R}_h.v\,\mathrm{d}h$ pour tout $v \in \mathcal{C}^\infty(G)$. Cette intégrale n'est

3. On se ramène par exemple au cas de l'inégration à valeurs dans un Banach, traité par Lang dans son cours "Real and functional analysis" à $\mathcal{C}^\infty(G)$ en raisonnant dans les Banach des fonctions de classe $\mathcal{C}^k$ sur un compact arbitraire Ω de G, pour un entier k arbitraire. La formation de cette intégrale commute aux applications linéaires continues sur l'image. Nous renvoyons à l'exposé de Garrett pour des références ainsi qu'un autre point de vue sur ces questions.

autre que $v * \psi$ comme on le constate en l'évaluant en tout $g \in G$, et elle est par construction dans l'adhérence du sous-espace vectoriel engendré par les $\mathrm{R}_h.v$ avec $h \in G$. On en déduit en particulier que V est stable par $v \mapsto v*\varphi$ pour toute fonction $\varphi \in \mathcal{C}^\infty(G)$ continue à support compact. En particulier, pour tout $\varphi \in \mathrm{I}_c^K(G)$ on a $f * \varphi \in V$.

Observons maintenant que pour tout $\varphi \in \mathrm{I}_c^K(G)$ et $\psi \in \mathcal{C}^\infty(G)_m$, alors on a $\psi * \varphi \in \mathcal{C}^\infty(G)_m$. En effet, si $k \in \mathrm{SO}(2)$ cela découle des égalités suivantes

$$\int_G f(gkh)\varphi(h^{-1})dh = \int_G f(gh)\varphi(h^{-1}k)dh$$

$$= \int_G f(gh)\varphi(kh^{-1})dh = \int_G f(ghk)\varphi(h^{-1})dh,$$

la première résultant du changement de variables $h \mapsto k^{-1}h$, la seconde de la propriété de φ, et la troisième du changement de variables $h \mapsto hk$. Mais W est admissible d'après le Théorème 5.7 (ii) $\Rightarrow$ (iii). La seconde partie de la Proposition 5.21 s'applique donc et montre

$$W_m * \varphi \subset W_m \ \ \forall m \in \mathbb{Z}, \ \ \forall \varphi \in \mathrm{I}_c^K(G). \tag{38}$$

Fixons un entier $N \geq 0$ assez grand de sorte que la fonction f soit dans l'espace $W' = \oplus_{|n|\leq N} W_n$; W' est de dimension finie par admissibilité de W. L'observation ci-dessus affirme que la convolution par $\mathrm{I}_c^K(G)$ préserve W'. Considérons une suite de Dirac en l'élément $1 \in G$ constituée de fonctions φ_n dans $\mathrm{I}_c^K(G)$. Une telle suite existe bien :

Lemme 5.22. *Soit U un voisinage ouvert de 1 dans G. Il existe $\varphi \in \mathrm{I}_c^K(G)$ à valeurs ≥ 0, à support dans U, et vérifant $\int_G \varphi(h^{-1})\mathrm{d}h = 1$.*

Démonstration — C'est un résultat classique si l'on n'impose pas à φ d'être invariante par conjugaison par K (G est un ouvert de $\mathrm{M}_n(\mathbb{R})$). On se ramène à ce cas de la manière suivante. L'application $K \times G \to G$, $(k, g) \mapsto kgk^{-1}$ étant continue, en particulier aux points de la forme $(k, 1)$, la compacité de K montre que l'on peut trouver un voisinage $1 \in U' \subset U$ vérifiant $kU'k^{-1} \subset U$ pour tout $k \in K$. Soit $\psi \in \mathcal{C}_\infty(G)$ une fonction ≥ 0, à support dans U', vérifiant $\psi(1) > 0$. La fonction $\varphi(g) = \int_K \psi(kgk^{-1})\mathrm{d}k$, multipliée éventuellement par une constante > 0, a toutes les conditions requises. □

Pour $\varphi \in \mathrm{I}_c^K(G)$ notons enfin $u(\varphi) \in \mathrm{End}(W')$ l'endomorphisme $w \mapsto w * \varphi$. Les φ_n formant une suite de Dirac, on constate que pour tout $w \in W'$ et tout $g \in G$, la suite des $u(\varphi_n)(w)(g)$ converge vers $w(g)$. L'espace W' étant de dimension finie, on en déduit que $u(\varphi_n)$ converge vers l'identité dans $\mathrm{End}(W')$. Le sous-espace vectoriel de $\mathrm{End}(W')$ constitué des $u(\varphi)$ est trivialement fermé (dimension finie), contient donc $\mathrm{id}_{W'}$ dans son adhérence : il contient donc $\mathrm{id}_{W'}$. Cela terminer la démonstration du théorème, admettant le (i) de la Proposition 5.21. □

Démonstration — (Démonstration de la Proposition 5.21) D'après le théorème de Hahn-Banach (valable dans tout Fréchet), il suffit de montrer que si Λ est une forme linéaire continue sur $\mathcal{C}^\infty(G)$ qui est nulle sur V (i.e. sur W), alors elle est nulle sur $\mathrm{R}_g V$ pour tout $g \in G$. Par continuité des endomorphismes R_g de $\mathcal{C}^\infty(G)$, il suffit de

voir que Λ est nulle sur $\mathrm{R}_g W$. Soit $w \in W$. Pour des raisons générales (voir l'exercice 5.5), la fonction $\varphi_w : G \to \mathbb{C}$, $g \mapsto \Lambda(\mathrm{R}_g w)$ est de classe $\mathcal{C}^\infty$ et l'on a

$$\mathrm{R}_g\, \varphi_w \;=\; \varphi_{\mathrm{R}_g w} \;\text{ et }\; \mathrm{R}_X\, \varphi_w \;=\; \varphi_{\mathrm{R}_X\, w}$$

pour tous $g \in G$ et $X \in \mathfrak{g}$ (ces assertions valent pour tout $w \in \mathcal{C}^\infty(G)$ et toute forme linéaire continue Λ sur $\mathcal{C}^\infty(G)$). On en déduit que la fonction φ_w est K-finie car w l'est, et aussi que l'on a

$$(u.\varphi_w)(1) = \varphi_{u.w}(1) = \Lambda(u.w) = 0,$$

pour tout $u \in \mathrm{U}(\mathfrak{g}_{\mathbb{C}})$). On en déduit (par exemple en contemplant la formule (22)) que toutes les dérivées partielles (d'ordre quelconque) en $g = 1$ de la fonction φ_w sont nulles. Mais d'après le lemme 5.23 suivant, φ_w est analytique réelle : elle est donc nulle sur la composante connexe de 1 dans $\mathrm{GL}_n(\mathbb{R})$, i.e. sur $\mathrm{GL}_n(\mathbb{R})^+$. Mais cela vaut pour tout $w \in W$, donc $\mathrm{R}_k(\varphi_w) = \varphi_{\mathrm{R}_k w}$ est également nulle sur $\mathrm{GL}_n(\mathbb{R})^+$, i.e. φ_w est nulle sur $\mathrm{O}(n)\mathrm{GL}_n(\mathbb{R})^+ = G$. □

Il ne reste qu'à démontrer le lemme suivant.

Lemme 5.23. (Analyticité des fonctions K-finies et $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$-finies)*Soit $f \in \mathcal{C}^\infty(G)$ supposée K-finie (à droite) et $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$-finie. Alors f est une fonction analytique réelle.*

Démonstration — On suppose $n = 2$ (mais la démonstration donnée s'adapterait aisément au cas où n est quelconque). Comme les hypothèses sont encore satisfaites par $\mathrm{L}_g f$ pour tout $g \in G$, il suffit de voir que f est analytique (=donnée par une série entière normalement convergente) dans un voisinage de 1. On peut supposer qu'il existe $m \in \mathbb{Z}$ avec $f \in \mathcal{C}^\infty(G)_m$. Si l'on pose $X = \mathrm{E}_{2,1} - \mathrm{E}_{1,2}$, cela entraîne $\mathrm{R}_X f \;=\; i\, m\, f$, et donc $X^2.f = -m^2 f$. Contemplons l'opérateur

$$D := C + X^2 = \mathrm{E}_{1,1}^2 + \mathrm{E}_{2,2}^2 + \mathrm{E}_{2,1}^2 + \mathrm{E}_{1,2}^2 \in \mathrm{U}(\mathfrak{g}).$$

En tant qu'opérateur différentiel sur $\mathrm{C}^\infty(G)$, il est de la forme

$$\sum_{1 \le i,j \le 4} a_{i,j}\, \frac{\partial^2}{\partial x_i \partial x_j} + D'$$

où les $x_i : \mathrm{M}_n(\mathbb{R}) \to \mathbb{C}$ sont les coordonnées affines centrées en 1 déjà utilisées dans la démonstration de la Proposition 4.2, où $a_{i,j}$ est un polynôme en les x_k vérifiant $a_{i,j}(1) = \delta_{i,j}$ (symbole de Kronecker), où $D' \in \mathbb{C}[x_i, \frac{\partial}{\partial x_j}]$ est un opérateur différentiel de degré ≤ 1. La matrice des $(a_{i,j}(x))$ est donc symmétrique définie positive pour x dans un voisinage assez petit de 1 : D est un *opérateur différentiel elliptique* dans un voisinage de $1 \in G$. Ses coefficients, dans les coordonnées x_i, sont polynomiaux, et donc en particulier analytiques réels. Le *théorème de régularité elliptique* (qui sera rappelé plus tard dans le cours : voir le lemme 6.21 (ii) et les rappels qui le précèdent) montre alors que toute équation de la forme $P(D).u = 0$ avec $P \in \mathbb{C}[T]$ non nul entraîne que u est analytique dans un voisinage de 1. Mais comme l'ensemble des $P(D).f$ est contenu dans $\mathfrak{z}(\mathfrak{g}_{\mathbb{C}}).f$ qui est de dimension finie, il existe un polynôme non nul vérifiant $P(D).f = 0$. □

4. Exercices

Exercice 5.1. *Pour $n \in \mathbb{Z}$ on pose $\mathrm{I}_n = \mathrm{Ind}_{\mathrm{SO}(2)}^{\mathrm{O}(2)} \epsilon^n$ (une représentation linéaire continue de dimension 2 de $\mathrm{O}(2)$). On note $\det : \mathrm{O}(2) \to \mathbb{C}^\times$ le morphisme déterminant.*

(i) *Montrer que l'on a $\mathrm{I}_n \simeq \mathrm{I}_{-n}$, $\mathrm{I}_0 \simeq 1 \oplus \det$, et que I_n est irréductible pour $n \neq 0$.*

(ii) *Montrer toute représentation irréductible, continue, de dimension finie de $\mathrm{O}(2)$ est isomophe à 1, $\det$, où à I_n pour un unique entier $n \geq 1$.*

Exercice 5.2. *Soit G un groupe topologique compact et V une représentation de G réunion de sous-représentations continues de dimension finie. Soit $U \subset V$ une sous-représentation de V.*

(i) *Monter que U et V/U sont réunion de sous-représentations continues de dimension finie de G.*

(ii) *Montrer qu'il existe une sous-représentation $W \subset V$ telle que $V = U \oplus W$. En déduire qu'il existe un isomorphisme de représentations $V \simeq U \oplus V/U$.*

Exercice 5.3. *Soient V un $(\mathfrak{gl}_n(\mathbb{R}), \mathrm{O}(n))$-module, $\mathfrak{z}(\mathfrak{gl}_n(\mathbb{C}))$, et $I \subset \mathfrak{z}$ un idéal de co-dimension finie. On suppose que l'on a $IV = 0$.*

(i) *En raisonnant dans la $\mathbb{C}$-algèbre (artinienne) de dimension finie $\mathfrak{z}/I$ montrer qu'il existe une suite d'idéaux maximaux $m_1, m_2, \ldots, m_r \subset \mathfrak{z}$ avec $m_1 m_2 \ldots m_r \subset I$ et $\mathfrak{z}/m_i \simeq \mathbb{C}$ pour tout i.*

(ii) *On pose $V_0 = 0$ et $V_i = m_i V_{i-1}$ pour $i = 1, \ldots, r$. Montrer que l'on a $V_r = 0$ et que V_{i-1}/V_i admet un caractère infinitésimal pour tout $i = 1, \ldots r$.*

(iii) *Montrer que si les V_i/V_{i-1} pour $i = 1, \ldots, r$ sont de longueur finie, il en va de même de V.*

(iv) *En utilisant l'exercice 5.2, montrer que si les V_i/V_{i-1} pour $i = 1, \ldots, r$ sont admissibles, il en va de même de V.*

(v) *Montrer que si V est engendré comme $(\mathfrak{gl}_n(\mathbb{R}), \mathrm{O}(n))$-module par un nombre fini d'éléments, il en va de même des V_i/V_{i-1} pour $i = 1, \ldots, r$ (on pourra observer que $m_i/(m_i \cap I)$ est de dimension finie sur $\mathbb{C}$).*

Exercice 5.4. *Donner un exemple de $(\mathfrak{gl}_2(\mathbb{R}), \mathrm{O}(2))$-module V non admissible et engendré par un élément $v \in V_0$.*

Exercice 5.5. *Soit $G = \mathrm{GL}_n(\mathbb{R})$. C'est un ouvert de $\mathrm{M}_n(\mathbb{R})$, de sorte que $\mathcal{C}^\infty(G)$ est un espace de Fréchet de manière naturelle.*

(i) *Montrer que l'application $G \times \mathcal{C}^\infty(G) \to \mathcal{C}^\infty(G)$ est continue.*

(ii) *Soient* $f \in \mathcal{C}^\infty(G)$ *et* Λ *une forme linéaire continue sur* $\mathcal{C}^\infty(G)$. *Montrer que la fonction* $\varphi_f : G \to \mathbb{C}$, $g \mapsto \Lambda(\mathrm{R}_g f)$ *est dans* $\mathcal{C}^\infty(G)$, *et que l'on a*

$$\mathrm{R}_g \, \varphi_f \, = \, \varphi_{\mathrm{R}_g f} \text{ et } \mathrm{R}_X \, \varphi_f \, = \, \varphi_{\mathrm{R}_X \, f}$$

pour tous $g \in G$ *et* $X \in \mathfrak{g}$.

CHAPITRE 6

L'espace des formes automorphes pour $\mathrm{GL}_2(\mathbb{Z})$

Dans cette partie, on s'intéresse à la structure du $(\mathfrak{gl}_2(\mathbb{R}), \mathrm{O}(2))$-module

$$\mathcal{A} := \mathcal{A}(\mathrm{GL}_2(\mathbb{R})\,;\mathrm{GL}_2(\mathbb{Z}))$$

des formes automorphes de $\mathrm{GL}_2(\mathbb{R})$ pour le sous-groupe $\mathrm{GL}_2(\mathbb{Z})$. En particulier, on se propose de démontrer que pour tout idéal de codimension finie I de $\mathfrak{z} = \mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$, le $(\mathfrak{g}, K)$-module $\mathcal{A}[I]$ est admissible.

Nous commencerons pour cela par introduire plusieurs espaces annexes, dont celui $\mathcal{A}_{\mathrm{cusp}} \subset \mathcal{A}$ des formes *paraboliques*, ainsi qu'un autre espace très concret $\mathcal{A}_P$ (espace des "termes constants") ; ils sont tels que l'on dispose d'une suite exacte naturelle de $(\mathfrak{g}, K)$-modules

$$0 \longrightarrow \mathcal{A}_{\mathrm{cusp}} \longrightarrow \mathcal{A} \longrightarrow \mathcal{A}_P$$

L'admissibilité des $\mathcal{A}_P[I]$ est élémentaire, et ramène l'admissibilité de $\mathcal{A}[I]$ à celle des $\mathcal{A}_{\mathrm{cusp}}[I]$. L'espace $\mathcal{A}_{\mathrm{cusp}}$ lui-même admet une description très simple en terme de son sous-espace $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ des formes paraboliques invariantes par l'action du centre $\mathbb{R}^\times$ de $\mathrm{GL}_2(\mathbb{R})$. Une propriété importante des telles formes paraboliques est qu'elles sont bornées sur $\mathrm{GL}_2(\mathbb{R})$, ce que l'on démontrera dans une seconde partie.

On étudie ensuite l'espace homogène quotient $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$, ou plutôt le quotient $X = \mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R})$, où $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}$ est le sous-groupe (encore discret) engendré par $\mathrm{GL}_2(\mathbb{Z})$ et l'homothétie $e^{1/2}$. On montre que X est muni d'un mesure invariante naturelle héritée de la mesure de Haar sur $\mathrm{GL}_2(\mathbb{R})$ (introduite concrètement au chapitre précédent) et surtout qu'il est de volume finie : ce volume vaut même $\zeta(2)$, un cas particulier de la célèbre formule du volume de Siegel.

Cette finitude entraîne que les éléments de $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ sont de carré intégrable sur X, et permet l'utilisation de méthodes hilbertiennes. Le fait que l'espace $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}[I]_m$ est de dimension finie est alors conséquence du fait qu'il est fermé dans $\mathrm{L}^2(X)$ et constitué de fonctions bornées (critère de Godement). Le caractère fermé n'est pas immédiat : il requiert un argument de régularité elliptique. Le théorème principal est alors que $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ est une somme *directe* de $(\mathfrak{g}, K)$-modules irréductibles, chacun d'entre eux intervenant avec une multiplicité finie.

Références :

[B1], A. Borel, *Automorphic forms on* $\mathrm{SL}_2(\mathbb{R})$, Cambridge Tract in Math. 130 (1997),

[B2], A. Borel, *Introduction aux groupes arithmétiques*, Institut de Math. de l'université de Strasbourg (1969),

W. Casselman, *Analysis on* SL(2), notes de cours,

Harish-Chandra, *Automorphic forms on semisimple Lie groups* (1968),

L. Hörmander, *The analysis of linear partial differential equations* (1983),

1. Formes paraboliques

On pose $G = \mathrm{GL}_2(\mathbb{R})$, $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{R})$, $K = \mathrm{O}(2)$, $\mathfrak{z} = \mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$, $\Gamma = \mathrm{GL}_2(\mathbb{Z})$ et

$$\mathcal{A} := \mathcal{A}(\mathrm{GL}_2(\mathbb{R})\,;\mathrm{GL}_2(\mathbb{Z})).$$

On rappelle que P est le sous-groupe des éléments de $\mathrm{GL}_2(\mathbb{R})$ de la forme p_τ avec $\tau \in \mathbb{H}$. Il contient comme sous-groupe le groupe

$$N = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{R}\},$$

ce dernier étant naturellement isomorphe au groupe additif de $\mathbb{R}$ via l'application $x \mapsto \mathrm{n}_x$, où n_x désigne la matrice $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ pour $x \in \mathbb{R}$. On constate que n_1 n'est autre que l'élément noté $\mathrm{T} \in \mathrm{SL}_2(\mathbb{Z})$, ainsi que les égalités

$$N \cap \Gamma \,=\, \{n_x, x \in \mathbb{Z}\} \,=\, \langle T\rangle \,\xrightarrow{\sim}\, \mathbb{Z}.$$

Définition 6.1. *Soit $f : G \to \mathbb{C}$ une fonction continue vérifiant $f(\mathrm{T}g) = f(g)$ pour tout $g \in G$. Pour tout $g \in G$ on pose*

$$f_P(g) \,=\, \int_0^1 f(\mathrm{n}_x\, g)\,\mathrm{d}x.$$

La fonction $f_P : G \to \mathbb{C}$ est appelée terme constant de f le long de P. *C'est une fonction continue vérifiant $f_P(ng) = f_P(g)$ pour tout $n \in N$. On a aussi $(f_P)_P = f_P$.*

Supposons $f \in \mathcal{C}^\infty(G)$ et $f(\mathrm{T}g) = f(g)$ pour tout $g \in G$. À $g \in G$ fixé, la fonction $x \mapsto f(n_x\, g)$ est une fonction $\mathcal{C}^\infty$ et 1-périodique sur $\mathbb{R}$, elle admet donc un "développement de Fourier" absolument convergent

$$f(n_x g) \,=\, \sum_{m\in\mathbb{Z}} \mathrm{c}_m(f;g)e^{2i\pi mx},$$

avec $\mathrm{c}_0(f;g) = f_P(g)$, d'où la terminologie.

Exemple 6.2. Si $f \in \mathrm{M}_k$ on a $\Phi_f(n_x \mathrm{p}_\tau \mathrm{s}_\lambda) = \Phi_f(\mathrm{p}_{\tau+x}\mathrm{s}_\lambda) = \lambda^{-k} f(\tau + x) = \lambda^{-k}(\sum_{m\geq 0} \mathrm{a}_m(f)e^{2i\pi m\tau}e^{2i\pi mx})$. On a donc $\mathrm{c}_m(\Phi_f; \mathrm{p}_\tau \mathrm{s}_\lambda) = \lambda^{-k}\mathrm{a}_m(f)e^{2i\pi m\tau}$, puis

$$(\Phi_f)_P(\mathrm{p}_\tau \mathrm{s}_\lambda) = \lambda^{-k}\mathrm{a}_0(f).$$

Ce cas est atypique : en général, le terme constant d'un $f \in \mathcal{A}$ dépendra de τ.

Supposons toujours $f \in \mathcal{C}^\infty(G)$ et $f(\mathrm{T}g) = f(g)$ pour tout $g \in G$. La fonction $\mathbb{R} \times G \to \mathbb{C}$, $f \mapsto f(\mathrm{n}_x g)$ étant de classe $\mathcal{C}^\infty$, on a aussi $f_P \in \mathcal{C}^\infty(G)$. De plus, si $h \in G$ et $X \in \mathfrak{gl}_2(\mathbb{R})$, les fonctions $\mathrm{R}_h f$ et $\mathrm{R}_X f$ sont encore invariantes à gauche par T, et on a les relations

$$(\mathrm{R}_h f)_P \,=\, \mathrm{R}_h(f_P) \quad \text{et} \quad (\mathrm{R}_X f)_P \,=\, \mathrm{R}_X(f_P), \tag{39}$$

de sorte que l'on peut aussi remplacer R_X par un élément arbitraire de $\mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$ dans la seconde relation ci-dessus.

Définition 6.3. *On note $\mathcal{A}_P$ le sous-espaces des fonctions $f \in \mathcal{C}^\infty(G)$ qui sont K-finies (à droite), $\mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$-finies, invariantes à gauche par N et le sous-groupe $D \subset \mathrm{GL}_2(\mathbb{Z})$ constitué des matrices diagonales.*

On a bien entendu $D \simeq \mathrm{GL}_1(\mathbb{Z}) \times \mathrm{GL}_1(\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Remarquons que D normalise N, et que si f est continue et invariante à gauche par $\mathrm{GL}_2(\mathbb{Z})$, et que si $d = \mathrm{diag}(d_1, d_2)$ on a $f(n_x dg) = f(\, n_{d_2/d_1\, x}\, g)$ puis $f_P(dg) = f_P(g)$. Étant données les Formules (39) on a démontré le lemme suivant :

Lemme 6.4. *$\mathcal{A}_P$ est un sous-$(\mathfrak{g}, K)$-module de $\mathrm{C}^\infty(G)_{K-\mathrm{fini}}$, et l'application $f \mapsto f_P$ est un morphisme de $(\mathfrak{g}, K)$-modules $\mathcal{A} \to \mathcal{A}_P$.*

Corollaire-Définition 6.5. *Une forme automorphe $f \in \mathcal{A}$ est dite parabolique si l'on a $f_P = 0$. Les formes paraboliques forment un sous-$(\mathfrak{g}, K)$-module de $\mathcal{A}$ noté $\mathcal{A}_{\mathrm{cusp}} \subset \mathcal{A}$.*

La structure du $(\mathfrak{g}, K)$-module $\mathcal{A}_P$ est en fait relativement simple, de sorte que nous seront ramenés en première approche à l'étude de $\mathcal{A}_{\mathrm{cusp}}$. Notons $A \subset G$ le sous-groupe des matrices diagonales de la forme $\mathrm{diag}(a_1, a_2)$ avec $a_1 > 0$ et $a_2 > 0$ (on ne demande pas $a_1 \geq a_2$ ici). Tout élément de G s'écrit alors sous la forme $n\, d\, a\, k$ avec $n \in N$, $d \in D$, $a \in A$ et $k \in \mathrm{SO}(2)$. On voit A comme un ouvert de $\mathbb{R}^2$ de manière évidente. On considère la restriction

$$\rho : \mathcal{A}_P \to \mathcal{C}^\infty(A),\ \ f \mapsto (a \mapsto f(a)).$$

Pour $i = 1, 2$ on a clairement la relation

$$\rho(\mathrm{R}_{E_{i,i}} f) \ = \ \mathrm{D}_i\, \rho(f) \ \text{ avec } \ \mathrm{D}_i = a_i \frac{\partial}{\partial a_i}. \tag{40}$$

Lemme 6.6. *(i) Pour tout $f \in \mathcal{A}_P$ on a $\rho(\mathrm{R}_{\mathrm{E}_{1,2}}\, f) = 0$.*

(ii) Soit $\xi : \mathfrak{z}(\mathfrak{gl}_2(\mathbb{C})) \to \mathbb{C}[D_1, D_2]$ le morphisme de $\mathbb{C}$-algèbres envoyant Z sur $D_1 + D_2$ et C sur $D_1^2 + D_2^2 + D_2 - D_1$. On a $\rho(z\, f) = \xi(z)\rho(f)$ pour tout $f \in \mathcal{A}_P$ et tout $z \in \mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$.

(iii) Si I est un idéal de codimension finie de $\mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$, l'idéal de $\mathbb{C}[D_1, D_2]$ engendré par $\xi(I)$ est aussi de codimension finie.

(iv) Soient $\varphi \in \mathcal{C}^\infty(A)$ et $P_1, P_2 \in \mathbb{C}[X] - \{0\}$ avec $P_1(D_1)(\varphi) = P_2(D_2)(\varphi) = 0$. Alors φ une combinaison linéaire finie de fonctions de la forme

$$(a_1, a_2) \mapsto (\log a_1)^{n_1}\, a_1^{s_1}\, (\log a_2)^{n_2}\, a_2^{s_2},$$

où les n_i sont des entiers avec $0 \leq n_i < P_i$, et où les s_i sont des nombres complexes tels que $P_i(s_i) = 0$.

Démonstration — Si $a \in A$ et $t \in \mathbb{R}$ on a $e^{t\mathrm{E}_{1,2}} = n_t$ et $a\, n_t \ = \ n_{a_1/a_2\, t}\, a$. Si $f \in \mathcal{A}_P$, la fonction $t \mapsto f(a\mathrm{n}_t)$ est donc constante, ce qui montre le (i).

Montrons le (ii). La relation $[\mathrm{E}_{2,1}, \mathrm{E}_{1,2}] = \mathrm{E}_{2,2} - \mathrm{E}_{1,1}$ montre que l'on a

$$C = \mathrm{E}_{1,1}^2 + \mathrm{E}_{2,2}^2 + \mathrm{E}_{2,2} - \mathrm{E}_{1,1} + 2\, \mathrm{E}_{1,2}\mathrm{E}_{2,1}.$$

Si $f \in \mathcal{A}_P$ alors on a $\mathrm{R}_{E_{2,1}} f \in \mathcal{A}_P$, et donc $\rho(\mathrm{E}_{1,2}\mathrm{E}_{2,1} f) = 0$ d'après le (i). La formule (40) entraîne que pour tout $f \in \mathcal{A}_P$ on a les égalités $\rho(C\, f) = \xi(C)\rho(f)$ et $\rho(\mathrm{R}_Z f) = \xi(Z)\rho(f)$, qui entraîne le (ii) car C et Z engendrent $\mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$.

Le (iii) est un énoncé purement algébrique. Si I est un idéal de codimension finie de $\mathfrak{z}$, il existe des polynômes $Q_i \in \mathbb{C}[X] - \{0\}$ avec $Q_1(C) \in I$ et $Q_2(Z) \in I$. Soit J

l'idéal de $\mathbb{C}[X,Y]$ engendré par les polynômes $Q_1(X^2+Y^2+Y-X)$ et $Q_2(X+Y)$. Cet idéal est manifestement de codimension finie dans $\mathbb{C}[X,Y]$, puisque le lieu de ses zéros $(x,y)\in\mathbb{C}^2$ est fini : les éléments $t=x+y$ et $x^2+y^2+y-x=y^2+2(1-t)y+t^2-t$ sont des racines respectives de Q_1 et Q_2 et ne prennent donc qu'un nombre fini de valeurs, ainsi donc que y et x.

Le (iv) est une équation différentielle linéaire ordinaire très classique. On se ramène par Bézout (lemme des noyaux) au cas $P_1=(X-s_1)^{n_1}$ et $P_2=(X-s_2)^{n_1}$. La fonction $\varphi(a_1,a_2)$, à a_2 fixé, est annulée par $(a_1\frac{\partial}{\partial a_1}-s_1)^{n_1}$, c'est donc une combinaison linéaire finie de la forme $\sum_{i=0}^{n_1-1}\lambda_i(a_2)(\log a_1)^i a_1^{s_1}$, avec $\lambda_i(a_2)\in\mathbb{C}$ uniquement déterminée. Les fonctions $a_2\to\lambda_i(a_2)$ sont donc de classe $\mathcal{C}^\infty$ sur $\mathbb{R}_{>0}$ et annulées par $(a_2\frac{\partial}{\partial a_2}-s_2)^{n_2}$, et on conclut par le même argument que précédemment. □

Corollaire 6.7. *Soit I un idéal de codimension finie de $\mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$. Le $(\mathfrak{g},K)$-module $\mathcal{A}_P[I]$ est admissible. De plus, $\mathcal{A}[I]$ est admissible si, et seulement si, $\mathcal{A}_{\mathrm{cusp}}[I]$ l'est.*

Démonstration — Soit $m\in\mathbb{Z}$. La décomposition $G=NDAK^+$ montre que l'application ρ induit une injection $(\mathcal{A}_P)_m\longrightarrow\mathcal{C}^\infty(A)$. Soit ξ comme dans l'énoncé du Lemme 6.6 (ii) et J l'idéal de $\mathbb{C}[D_1,D_2]$ engendré par $\xi(I)$; on en déduit que ρ induit une injection $(\mathcal{A}_P)_m[I]\longrightarrow\mathcal{C}^\infty(A)[J]$. Par le (iii) du même lemme, J est de codimension finie dans $\mathbb{C}[D_1,D_2]$, il existe donc $P_i\in\mathbb{C}[X]-\{0\}$ avec $P_i(D_i)\in J$ pour $i=1,2$. Par le point (iv), $\mathcal{C}^\infty(A)[J]$ est de dimension finie, ainsi donc que $(\mathcal{A}_P)_m[I]$, ce qui montre l'admissibilité de $\mathcal{A}_P[I]$. Le dernier point résulte alors de la suite exacte $0\to\mathcal{A}_{\mathrm{cusp}}[I]\to\mathcal{A}[I]\to\mathcal{A}_P[I]$ (tout sous-$(\mathfrak{g},K)$-module d'un $(\mathfrak{g},K)$-module admissible est admissible, et une extension d'un $(\mathfrak{g},K)$-module admissible par un $(\mathfrak{g},K)$-module admissible est admissible). □

Nous allons donc nous concentrer sur l'étude de $\mathcal{A}_{\mathrm{cusp}}$.

2. Les formes paraboliques invariantes par $\mathbb{R}^\times$ sont bornées

Lemme 6.8. ("Estimée fondamentale") *Soit $f\in\mathcal{C}^\infty(G)$ vérifiant $f(\mathrm{T}g)=f(g)$ pour tout $g\in G$. Soit $X_1,\dots,X_4$ une $\mathbb{R}$-base de $\mathfrak{g}$. Il existe une constante $c>0$ telle que pour tout $g\in G$ on ait $|f(g)-f_P(g)|\leq c\,|\mathrm{Im}\,g.i|^{-1}\sum_{j=1}^4|\mathrm{R}_{X_j}f|_P(g)$.*

Démonstration — Fixons $g\in G$ et posons $\varphi(t)=f(g)-f(\mathrm{n}_t g)$ (c'est une fonction $\mathcal{C}^\infty$ sur $\mathbb{R}$). On a d'abord $\int_0^1\varphi(t)\mathrm{d}t=f(g)-f_P(g)$. La majoration évidente $|\varphi(t)|\leq\int_0^s|\varphi'(s)|\mathrm{d}s\leq\int_0^1|\varphi'(s)|\mathrm{d}s$ (noter $\varphi(0)=0$) entraîne

$$|f(g)-f_P(g)|\leq\int_0^1|\varphi'(t)|\mathrm{d}t. \tag{41}$$

D'autre part, on a $\mathrm{n}_{t+h}\,g=\mathrm{n}_t\,g\,e^{h\,\mathrm{ad}_{g^{-1}}\mathrm{E}_{1,2}}$ pour tout $t,h\in\mathbb{R}$. Écrivons g sous la forme $\mathrm{p}_\tau\mu k$ avec $\tau=g.i=x+iy\in\mathbb{C}-\mathbb{R}$, $\mu\in\mathbb{R}_{>0}$ et $k\in\mathrm{SO}(2)$. On a $\mathrm{p}_\tau=\mathrm{n}_x\,\mathrm{diag}(y,1)$, $\mathrm{ad}_n\mathrm{E}_{1,2}=\mathrm{E}_{1,2}$ pour tout $n\in N$, et $\mathrm{ad}_{\mathrm{diag}(y,1)^{-1}}(\mathrm{E}_{1,2})=y^{-1}\mathrm{E}_{1,2}$. Si l'on

pose $\mathrm{ad}_{k^{-1}}\mathrm{E}_{1,2} = \sum_{j=1}^4 a_j(k)X_i$, ce qui définit uniquement les fonctions $a_j : K \to \mathbb{R}$, on a donc une identité de la forme

$$\mathrm{ad}_{g^{-1}}\,\mathrm{E}_{1,2} \;=\; y^{-1}\sum_{j=1}^4 a_j(k)X_j.$$

Les fonctions $|a_j|$ sont continues sur le compact $\mathrm{SO}(2)$; elles sont donc majorées par une même constante $c > 0$. Si l'on met tout bout-à-bout on a montré pour $t \in \mathbb{R}$:

$$|\varphi'(t)| \;\leq c\,|\mathrm{Im}\, g.i|^{-1}\sum_{j=1}^4 |\mathrm{R}_{X_j}f|(n_t g),$$

et on conclut par l'inégalité (41). □

Théorème 6.9. *Soit $f \in \mathcal{A}_{\mathrm{cusp}}$.*

(i) (Décroissance rapide des formes cuspidales) *Pour tout entier $N \geq 1$ et tout $A > 0$, il existe un réel $c > 0$ tel que pour tout $\tau \in \mathbb{H}$ avec $\mathrm{Im}\,\tau \geq A$, et tout $k \in \mathrm{SO}(2)$, on ait $|f(\mathrm{p}_\tau k)| \leq c\,|\mathrm{Im}\,\tau|^{-N}$.*

(ii) Si on a $|f(zg)| = |f(g)|$ pour tout $z \in \mathbb{R}_{>0}$ et tout $g \in G$, alors $|f|$ est bornée sur G.

Démonstration — (Démonstration du Théorème 6.9) Observons que si f satisfait les hypothèses du Lemme 6.8, et si $f_P = 0$, la conclusion de ce lemme entraîne qu'il existe un réel $c = c_f > 0$ tel que $|f(ng)| \leq c_f\,|\mathrm{Im}\, g.i|^{-1}\sum_{j=1}^4 |\mathrm{R}_{X_j}f|_P(g)$ pour tout $g \in G$ et tout $n \in N$ (noter $\mathrm{Im}\, ng.i = \mathrm{Im}\, g.i$). On en déduit

$$|f|_P(g) \;\leq\; c_f\,|\mathrm{Im}\, g.i|^{-1}\sum_{j=1}^4 |\mathrm{R}_{X_j}f|_P(g), \quad \forall\, g \in G. \tag{42}$$

Mais les fonctions $\mathrm{R}_{X_j}f$ vérifient encore les hypothèses du lemme, et aussi $(\mathrm{R}_{X_j}\,f)_P = \mathrm{R}_{X_j}\,f_P \;=\; 0$, de sorte qu'ils vérifient une inégalité de la forme (42) (pour une autre constante que c_f à priori). On en déduit par récurrence que pour tout entier $m \geq 1$ on a

$$\sum_{j=1}^4 |\mathrm{R}_{X_j}f|_P(g) \;\leq\; c_{f,m}\,|\mathrm{Im}\, g.i|^{1-m}\sum_{u\in B_m} |u.f|_P(g) \;\; \forall g \in G,$$

où $\mathrm{B}_m \in \mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$ désigne la famille des 4^m de monômes " de degré m" en les X_j. Supposons maintenant $f \in \mathcal{A}_{\mathrm{cusp}}$. D'après le Corollaire 5.20, f est à croissance uniformément modérée : il existe $n \geq 0$ (fixé dans toute la suite) tel que pour tout $u \in \mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$ il existe $C(u,f) > 0$ avec $|u.f|(g) \leq C(u,f)||g||^n$ pour tout $g \in G$. En particulier on a

$$|u.f|_P(g) \;=\; \int_0^1 |u.f|(\mathrm{n}_x\, g)\mathrm{d}x \leq C(u,f)\,||g||^n M$$

avec $M = \int_0^1 ||\mathrm{n}_x||^n \mathrm{dx}$. On en déduit que pour tout $m \geq 1$ il existe $C_{f,m} > 0$ avec

$$|f(g)| \;\leq\; C_{f,m}\,|\mathrm{Im}\, g.i|^{-m}\,||g||^n \quad \forall g \in G, \tag{43}$$

(on peut prendre $C_m = c_f c_{f,m}(\sum_{u\in \mathrm{B}_m} C(u,f))M$.)

Montrons maintenant le (i). On peut supposer $|\mathrm{Re}\,\tau| \leq 1$ car $f(\mathrm{p}_\tau k) = f(\mathrm{T}\mathrm{p}_\tau k) = f(\mathrm{p}_{\tau+1}k)$ pour tout $\tau \in \mathbb{H}$. On a alors

$$||\mathrm{p}_\tau k||^2 \,=\, ||\mathrm{p}_\tau||^2 \,=\, |\tau|^2 + 1 + (\mathrm{Im}\,\tau)^{-2} \leq\, (\mathrm{Im}\,\tau)^2 + 2 + A^{-2} \,\leq\, \alpha\,(\mathrm{Im}\tau)^2,$$

avec $\alpha = (A^2 + 2 + A^{-2})A^{-2}$, pour $\mathrm{Im}\,\tau \geq A$. La majoration (43) entraîne donc

$$|f(\mathrm{p}_\tau k)| \,\leq\, \sqrt{\alpha}\, C_{f,m}\, |\mathrm{Im}\,\tau|^{n-m}.$$

On conclut en prenant $m > N + n$.

Montrons le (ii). Le (i) et l'hypothèse entraînent que $|f|$ est bornée sur l'ensemble Π des éléments de la forme $\mathrm{p}_\tau \mathrm{s}_\lambda$ avec $\tau \in \mathcal{F}$ et $\lambda \in \mathbb{C}^*$. On conclut car $|f|$ est invariante à gauche par $\mathrm{GL}_2(\mathbb{Z})$ et on a $\mathrm{GL}_2(\mathbb{Z}).\Pi = \mathrm{GL}_2(\mathbb{R})$ d'après le Théorème 2.1. □

Remarque 6.10. Le (i) du Théorème 6.9 permet de montrer plus généralement que si $f \in \mathcal{A}_{\mathrm{cusp}}$ et $f' \in \mathcal{A}$ sont tels que la fonction $g \mapsto |f(g)f(g')|, G \to \mathbb{R}_{\geq 0}$, est $\mathbb{R}_{>0}$ invariante, alors $g \mapsto |f(g)f'(g)|$ est bornée sur G.

Définition 6.11. *On note $\mathcal{A}^{\mathrm{unit}} \subset \mathcal{A}$ le sous-espace des formes automorphes qui vérifient $f(zg) = f(g)$ pour tout $z \in \mathbb{R}_{>0}$ et tout $g \in G$. C'est un sous-$(\mathfrak{g}, K)$-module. On pose aussi $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}} = \mathcal{A}_{\mathrm{cusp}} \cap \mathcal{A}^{\mathrm{unit}}$.*

Pour tout entier $n \geq 0$ et tout $s \in \mathbb{C}$, on pose $e_{n,s}(g) \,=\, (\log|\det g|)^n\, |\det g|^{s/2}$. Le lemme facile suivant ramène la structure de $\mathcal{A}_{\mathrm{cusp}}$ à celle de $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$.

Lemme 6.12. *Pour tout entier $N \geq 0$ et tout $s \in \mathbb{C}$ on a*

$$\mathcal{A}[(\mathrm{R}_Z - s)^N] = \bigoplus_{0 \leq n \leq N} e_{n,s}\, \mathcal{A}^{\mathrm{unit}}.$$

En particulier, on a $\mathcal{A} = \bigoplus_{n \geq 0, s \in \mathbb{C}} e_{n,s}\, \mathcal{A}^{\mathrm{unit}}$ (et idem en remplaçant $\mathcal{A}$ par $\mathcal{A}_{\mathrm{cusp}}$).

Démonstration — Soit $f \in \mathcal{C}^\infty(G)$ annulée par $(\mathrm{R}_Z - s)^n$. Pour $h \in G$ on constate que la fonction $t \mapsto f(th)$, $\mathbb{R}_{>0} \to \mathbb{C}$, est annulée par $(t\frac{\partial}{\partial t} - s)^N$. Il existe donc des uniques scalaires $\lambda_n(h)$ tels que pour tout $t > 0$ on a $f(th) \,=\, \sum_{n=0}^{N-1} (\log t)^n\, t^s\, \lambda_n(h)$. On conclut aisément en prenant $t = |\det g|^{1/2}$ et $h = g/|\det(g)|^{1/2}$ (et donc $th = g$). □

3. Digression sur $\mathrm{GL}_n(\mathbb{Z})\backslash\mathrm{GL}_n(\mathbb{R})$

Considérons temporairement le groupe $\mathrm{GL}_n(\mathbb{R})$ avec $n \geq 1$ quelconque. Il sera peu élégant mais commode de considérer le sous-groupe

$$\mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}} \subset \mathrm{GL}_n(\mathbb{R})$$

engendré par $\mathrm{GL}_n(\mathbb{Z})$ et l'homothétie $e^{1/n}$ ("e" comme "étendu"). C'est un sous-groupe discret de $\mathrm{GL}_n(\mathbb{R})$: si U désigne un voisinage de 1 dans $\mathrm{GL}_n(\mathbb{R})$ assez petit de sorte que l'on ait $1/e < |\det g| < e$ et $|g_{i,j} - \delta_{i,j}| < 1$ pour tout $g \in U$, on constate que l'on a $U \cap \mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}} = \{1\}$. Quitte à remplacer U par un sous-ensemble ouvert contenant 1, on peut même supposer $UU^{-1} \cap \mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}} = \{1\}$. On en déduit que

pour tout $g \in G$ la réunion $\bigcup_{\gamma\in\mathrm{GL}_n(\mathbb{Z})_e} \gamma\, U\, g$ est disjointe, et donc que la projection naturelle

$$\pi : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{GL}_n(\mathbb{Z})_e\backslash\mathrm{GL}_n(\mathbb{R})$$

est un revêtement. Cela permet l'espace quotient $\mathrm{GL}_n(\mathbb{Z})_e\backslash\mathrm{GL}_n(\mathbb{R})$ (un espace topologique manifestement localement compact, séparé, et réunion dénombrable de compacts) d'une mesure $\overline{\lambda} = \mathrm{d}\overline{g}$ héritée de la mesure de Haar $\lambda = \mathrm{d}g$ sur $\mathrm{GL}_n(\mathbb{R})$ introduite au §3 Chap. 5 :

Lemme 6.13. *Il existe une unique mesure borélienne $\overline{\lambda}$ sur $\mathrm{GL}_n(\mathbb{Z})_e\backslash\mathrm{GL}_n(\mathbb{R})$ telle que pour tout borélien $X \subset \mathrm{GL}_n(\mathbb{R})$ vérifiant $\lambda(X \cap \gamma X) = 0$ pour tout $\gamma \in \Gamma - \{1\}$ on ait $\overline{\lambda}(\pi(X)) = \lambda(X)$. La mesure $\overline{\lambda}$ est invariante par translations à droite par G.*

Démonstration — On pose $\Gamma = \mathrm{GL}_n(\mathbb{Z})_e$ et $G = \mathrm{GL}_n(\mathbb{R})$. Un argument de compacité montre que $\Gamma\backslash G$ est réunion dénombrable de compacts, disons K_n avec $n \geq 1$, au dessus desquels le revêtement π est trivial. En particulier, il existe un compact $U_n \subset G$ avec $\pi^{-1}\, K_n = \coprod_{\gamma\in\Gamma} \gamma\, U_n$. Les boréliens $K'_n = K_n - \cup_{1\leq k<n} K_k$ avec $n \geq 1$ forment une partition dénombrable de $\Gamma\backslash G$, et si l'on pose $U'_n = \pi^{-1} K'_n \cap U_n$, on a

$$G = \coprod_{\gamma\in\Gamma} \gamma U', \quad \text{avec } U' = \coprod_{n\geq 1} U'_n. \tag{44}$$

Si $\overline{\lambda}$ existe avec la propriété du lemme, on a pour tout borélien Y de $\Gamma\backslash G$ l'égalité

$$\overline{\lambda}(Y) = \sum_{n\geq 1} \overline{\lambda}(Y \cap K'_n) = \sum_{n\geq 1} \lambda(\pi^{-1}(Y) \cap U'_n) = \lambda(\pi^{-1}(Y) \cap U') \tag{45}$$

ce qui montre son unicité. Réciproquement, définissons $\overline{\lambda}$ par cette formule, i.e.

$$\overline{\lambda}(Y) = \lambda(\pi^{-1}(Y) \cap U')$$

pour tout borélien Y de $\Gamma\backslash G$. Pour voir qu'elle satisfait la condition de l'énoncé, observons que si A et B sont deux boréliens de G avec $\lambda(A \cap \gamma A) = \lambda(B \cap \gamma B) = 0$ pour tout $\gamma \neq 1$, et si on a $C \cup \bigcup_{\gamma\in\Gamma} \gamma A = C \cup \bigcup_{\gamma\in\Gamma} \gamma B$ avec C négligeable, alors on a $\lambda(A) = \lambda(B)$. En effet, la dénombrabilité de Γ et l'invariance de λ à gauche par Γ entraînent

$$\lambda(A) = \sum_{\gamma\in\Gamma} \lambda(A \cap \gamma B) = \sum_{\gamma\in\Gamma} \lambda(\gamma^{-1} A \cap B) = \lambda(B). \tag{46}$$

Soient $B \subset G$ un borélien quelconque et $A = (\pi^{-1}\pi(B)) \cap U'$. On a $\pi(A) = \pi(B)$ d'après (44), i.e.

$$\bigcup_{\gamma\in\Gamma} \gamma A = \bigcup_{\gamma\in\Gamma} \gamma B.$$

Si $B = X$ est comme dans l'énoncé du lemme, on a donc $\lambda(X) = \lambda(A) = \overline{\lambda}(\pi(X))$ (par définition de $\overline{\lambda}$), comme affirmé dans l'énoncé. L'invariance par translations à droite découle de la même propriété pour λ : pour $g \in G$, Y borélien de $\Gamma\backslash G$, et $X = \pi^{-1} Y \cap U'$, on a $\overline{\lambda}(Yg) = \overline{\lambda}(\pi(Xg)) = \lambda(Xg) = \lambda(X) = \overline{\lambda}(Y)$. □

On note $\overline{\lambda} = \mathrm{d}\overline{g}$ la mesure définie par le lemme ci-dessus sur $\mathrm{GL}_n(\mathbb{Z})_e\backslash\mathrm{GL}_n(\mathbb{R})$. Nous appellerons *domaine fondamental* pour l'action de $\mathrm{GL}_n(\mathbb{Z})_e$ sur $\mathrm{GL}_n(\mathbb{R})$ tout borélien $X \subset \mathrm{GL}_n(\mathbb{R})$ vérifiant $\lambda(X \cap \gamma X) = 0$ pour $\gamma \in \Gamma - \{1\}$ et tel que $\mathrm{GL}_n(\mathbb{R}) - \bigcup_{\gamma\in\Gamma} \gamma X$ est négligeable. La démonstration ci-dessus montre qu'un tel

domaine existe toujours : par exemple, la partie U' définie dans la démonstration ci-dessus en est un d'après (44). De plus, nous avons aussi montré (Formule (46)) que tous les domaines fondamentaux ont même mesure, à savoir $\overline{\lambda}(\mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_n(\mathbb{R}))$.

Théorème 6.14. *L'espace* $\mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_n(\mathbb{R})$ *est de mesure finie. Mieux, on a*

$$\overline{\lambda}(\mathrm{GL}_n(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_n(\mathbb{R})) = \prod_{k=2}^{n}\zeta(k).$$

On ne va démontrer ce résultat que pour $n \leq 2$. Pour $n = 1$, l'ensemble $[1, e] \subset \mathbb{R}^\times$ est un domaine fondamental, et on a donc $\overline{\lambda}(\mathrm{GL}_1(\mathbb{Z})\backslash\mathrm{GL}_1(\mathbb{R})) = \int_1^e \frac{\mathrm{d}z}{z} = 1$ (conformément à la formule ci-dessus). Dans le cas $n = 2$, notons $\mathcal{F} \subset \mathbb{H}$ la partie introduite au Chapitre 2 §1, et $\mathcal{F}_0$ son intérieur. Le Théorème 6.14 et la Proposition 4.19 montrent que l'ouvert

$$\Pi_0 = \{\mathrm{p}_\tau\,\mathrm{s}_\lambda \mid \tau \in \mathcal{F}_0,\ 1 < |\lambda| < e^{1/2},\ 0 < \arg\lambda < \pi\} \subset \mathrm{GL}_2(\mathbb{R}) \tag{47}$$

est un domaine fondamental. En effet, l'ensemble $C \subset \mathrm{GL}_2(\mathbb{R})$ constitué des éléments de la forme $\mathrm{p}_\tau\mathrm{s}_\lambda$ avec $\tau \in \partial\mathcal{F}$ et $\lambda \in \mathbb{C}^*$ est négligeable pour $\mathrm{d}g$ (ce sera particulièrement évident une fois démontré le Lemme 6.15 ci-dessous). Pour déterminer son volume, nous aurons besoin d'une formule pour $\mathrm{d}g$ adaptée à la décomposition $G = NAZK$. On considère la variété différentielle $M = \mathbb{R} \times \mathbb{R}^\times \times \mathbb{R}_{>0} \times \mathbb{R}/(2\pi\mathbb{Z})$ munie de la mesure

$$\mathrm{d}m = \frac{\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z\,\mathrm{d}t}{z\,y^2}.$$

On pose $\mathrm{a}_y = \mathrm{diag}(y, 1)$ pour $y \in \mathbb{R}^\times$. On a déjà justifié que l'application

$$\varphi : M \to \mathrm{GL}_2(\mathbb{R}),\ (x, y, z, t) \mapsto \mathrm{n}_x\,\mathrm{a}_y\,z\,\mathrm{s}_{e^{it}},$$

est un $\mathcal{C}^\infty$-difféomorphisme.

Lemme 6.15. *Soit* $f : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{C}$. *On a* $f \in \mathrm{L}^1(\mathrm{GL}_2(\mathbb{R}), \mathrm{d}g)$ *si, et seulement si,* $f \circ \varphi \in \mathrm{L}^1(M, \mathrm{d}m)$, *et si ces assertions sont satisfaites on a l'égalité*

$$\int_{\mathrm{GL}_2(\mathbb{R})} f(g)\,\mathrm{d}g \;=\; \int_M f\circ\varphi(x, y, z, t)\ \mathrm{d}m.$$

Démonstration — On pose $G = \mathrm{GL}_2(\mathbb{R})$ (vu comme ouvert de $\mathrm{M}_2(\mathbb{R})$). Le théorème du changement de variables montre que pour toute fonction $f : G \to \mathbb{C}$ la fonction $f(g)\,|\det g|^{-2}$ sommable sur G pour la mesure $\prod_{i,j}\mathrm{d}g_{i,j}$ si, et seulement si, $f(\varphi(x, y, z, t))\,y^{-2}\,z^{-4}\,\mathrm{Jac}_\varphi(x, y, z, t)$ est sommable sur M, et qu'alors on a l'égalité

$$\int_G f(g)\,|\det g|^{-2}\ \prod_{i,j}\mathrm{d}g_{i,j} \;=\; \int_M f(\varphi(x, y, z, t))\,z^{-4}\,y^{-2}\,\mathrm{Jac}_\varphi(x, y, z, t)\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z\,\mathrm{d}t,$$

En particulier, on a

$$\mathrm{d}g \;=\; J(x, y, z, t)\,\mathrm{d}x\,\frac{\mathrm{d}y}{|y|}\,\frac{\mathrm{d}z}{z}\,\mathrm{d}t \quad \text{avec} \quad J(x, y, z, t) \;=\; \mathrm{Jac}_\varphi(x, y, z, t)\,|y|^{-1}\,z^{-3}.$$

On pourrait calculer de manière directe le Jacobien ci-dessus pour conclure, mais ce n'est pas nécessaire par le raisonnement suivant. En effet, $\mathrm{d}g$ est invariante à droite par $\mathrm{SO}(2)$, mais multiplier à droite par $e^{2i\pi t'}$ sur G revient à appliquer le changement de variables $(x, y, z, t) \mapsto (x, y, z, t + t')$; comme $\mathrm{d}t$ est invariante par translations, la fonction J est indépendante de t. De même, comme $\mathrm{d}g$ est invariante à gauche,

et puisque la multiplication à gauche par $\mathrm{n}_{x'z'}$ revient à appliquer le changement de variables $(x,y,z,t) \mapsto (x+x', y, zz', t)$, J est également indépendante de x et z. Mais pour $y' \in \mathbb{R}^\times$ on a

$$\mathrm{a}_{y'}\,\varphi(x,y,z,t) = \varphi(y'x, y'y, z, t).$$

Comme $\mathrm{d}y/|y|$ est invariante par translations sur $\mathbb{R}^\times$, et comme on a $\mathrm{d}(y'x) = |y'|\mathrm{d}x$, on a donc $J(y'x,y'y,z,t)|y'| = J(x,y,z,t)$ pour tous x,y,y',z,t, puis (avec $y' = 1/y$)

$$J(x,y,z,t) \;=\; J(0,1,1,0)\,|y|^{-1} \;\text{ avec }\; J(0,1,1,0) = \mathrm{Jac}_\varphi(0,1,1,0).$$

La différentielle en de φ en $(0,1,1,0)$ (d'image $1 \in G$) est l'application linéaire

$$(u,v,w,t) \mapsto \begin{pmatrix} w+v & u-t \\ t & w \end{pmatrix},$$

d'où l'on tire $J(0,1,1,0) = 1$. □

Il ne reste qu'à montrer le :

Lemme 6.16. *On a* $\lambda(\Pi_0) = \pi^2/6 = \zeta(2)$.

Démonstration — Par définition, Π_0 est l'ensemble des $\mathrm{n}_x\,\mathrm{a}_y\,z\,\mathrm{s}_{\mathrm{e}^{it}}$ avec $x+iy \in \overset{\circ}{\mathcal{F}}$, $1 < z < e^{1/2}$ et $0 < t < \pi$. Le Lemme 6.15 appliqué à la fonction caractéristique de Π_0 entraîne donc

$$\begin{aligned}\lambda(\Pi_0) \;&=\; \int_1^{e^{1/2}} \frac{\mathrm{d}z}{z} \times \int_0^{\pi} \mathrm{d}t \times \int_{|x|<1/2,\,\sqrt{1-x^2}<y} \frac{\mathrm{d}x\,\mathrm{d}y}{y^2} \\ &=\; \frac{\pi}{2}\int_{-1/2}^{1/2}\left(\int_{\sqrt{1-x^2}}^{\infty}\frac{\mathrm{d}y}{y^2}\right)\mathrm{d}x \;=\; \frac{\pi}{2}\int_{-1/2}^{1/2}\frac{\mathrm{d}x}{\sqrt{1-x^2}}\end{aligned}$$

et on conclut car on a $\arcsin(1/2) - \arcsin(-1/2)) = 2\pi/6 = \pi/3$. □

Remarque 6.17. Le Théorème 6.14 est dû à Siegel ; sa démonstration pour n général ne repose pas sur la détermination d'un domaine fondamental explicite. La finitude de $\overline{\lambda}(\mathrm{GL}_n(\mathbb{Z})_e\backslash\mathrm{GL}_n(\mathbb{R}))$ peut se démontrer assez simplement en utilisant les domaines fondamentaux "approchés" aussi introduits par Siegel ("domaines de Siegel", voir le premier chapitre du livre de Borel "Introductions aux groupes arithmétiques").

4. Structure de $\mathcal{A}_{\text{cusp}}^{\text{unit}}$

Nous sommes enfin en mesure de démontrer le :

Théorème 6.18. *Si I est un idéal de codimension finie de $\mathfrak{z}$ alors $\mathcal{A}_{\text{cusp}}^{\text{unit}}[I]$ est admissible. En outre, $\mathcal{A}_{\text{cusp}}[I]$ et $\mathcal{A}[I]$ sont également admissibles.*

La dernière assertion résulte de la première, du Corollaire 6.7 et du Lemme 6.12 (noter que I contient toujours un polynôme non nul en Z). Montrons la première. Pour cela, on munit $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R})$ de la mesure $\overline{\lambda}$ définie dans le Lemme 6.13. C'est une mesure invariante pour les translations à droite de volume total fini. En particulier, toute fonction continue et bornée sur $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R})$ est de carré intégrable pour cette mesure. Le Théorème 6.9 (ii) entraîne donc :

$$\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}} \subset \mathrm{L}^2(\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash \mathrm{GL}_2(\mathbb{R})). \tag{48}$$

Lemme 6.19. *(Godement) Soit (X, μ) un espace mesuré avec $\mu \geq 0$ et $\mu(X) < \infty$. Soit $V \subset \mathrm{L}^2(X)$ un sous-espace fermé. Si tout élément de V est essentiellement borné alors V est de dimension finie.*

Démonstration — (preuve de Hörmander) Comme $\mu(X)$ est fini on a $||f||_2 \leq \mu(X)||f||_\infty$ pour tout $f \in \mathrm{L}^2(X)$. Observons que V est complet pour $||.||_\infty$. En effet, si f_n est une suite de Cauchy pour $||.||_\infty$ avec $f_n \in V$ pour tout n, alors il existe $f : X \to \mathbb{C}$ telle que f_n converge uniformément vers f hors d'un sous-ensemble de X de mesure 0. L'inégalité $||f||_2 \leq \mu(X)||f||_\infty$ montre $f \in \mathrm{L}^2(X)$ et $||f_n - f||_2 \to 0$, donc $f \in V$ car V est fermé dans L^2 par hypothèse. Ainsi, V est un Banach pour $||.||_\infty$ et $||.||_2$, et l'identité $(V, ||.||_2) \to (V, ||.||_\infty)$ est continue (de norme $\leq \mu(X)$). Le théorème de l'application ouverte implique alors que c'est un homéomorphisme, i.e. qu'il existe $c > 0$ avec

$$||f||_\infty \leq c\,||f||_2 \quad \forall v \in V.$$

Soit $f_1, \ldots, f_n$ une base orthonormée dans le Hilbert $(V, ||.||_2)$. Nous allons montrer $n \leq c^2\mu(X)$. Pour $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$ donné, on a

$$|\sum_{i=1}^{n} \lambda_i f_i(x)| \leq c\,(\sum_{i=1}^{n} |\lambda_i|^2)^{1/2}$$

pour presque tout x. Soit $C \subset \mathbb{C}$ un sous-ensemble dense et dénombrable. Il existe donc un ensemble négligeable $Z \subset X$ tel que pour tout $x \in X - Z$, et tout $(\lambda_1, \ldots, \lambda_n) \in C^n$, on ait l'inégalité ci-dessus. Mais du coup cette inégalité vaut pour tout $x \in X - Z$ et tout $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}^n$. On l'applique à $x \in X - Z$ arbitraire et à $\lambda_i = \overline{f_i(x)}$, on obtient

$$\sum_{i=1}^{n} |f_i(x)|^2 \leq c^2 \quad \forall x \in X - Z,$$

puis en intégrant $n \leq c^2\mu(X)$. On a donc $\dim V \leq c^2\mu(X)$. □

Compte tenu du Théorème 6.9 (ii) et du Théorème 6.14 (et donc de l'inclusion (48)), il suffit de montrer le :

Lemme 6.20. *Soit $I \subset \mathfrak{z}$ un idéal de codimension finie et $m \in \mathbb{Z}$. Alors $(\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}})_m[I]$ est fermé dans $\mathrm{L}^2(\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash \mathrm{GL}_2(\mathbb{R}))$.*

L'ingrédient important pour démontrer ce lemme sera un énoncé de régularité elliptique. Sa formulation nécessite quelques remarques préliminaires. Fixons $\Omega \subset \mathbb{R}^n$ un ouvert non vide ; on note $\mathcal{C}^\infty(\Omega)$ les fonctions $\Omega \to \mathbb{C}$ de classe $\mathcal{C}^\infty$, et $\mathcal{C}_c^\infty(\Omega)$ son sous-espace des fonctions à support compact. Soit $m \geq 0$ un entier. Un *opérateur différentiel* (linéaire, à coefficients $\mathcal{C}^\infty$) d'ordre $\leq m$ sur Ω est un endomorphisme P de l'espace $\mathcal{C}^\infty(\Omega)$ de la forme

$$P(f) = \sum_{|\alpha| \leq m} a_\alpha\, \partial^\alpha f, \quad \forall f \in \mathcal{C}^\infty(\Omega). \tag{49}$$

Dans cette formule, α parcourt les multi-indices $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ avec $|\alpha| := \sum_i \alpha_i \leq m$, et les a_α sont des éléments de $\mathcal{C}^\infty(\Omega)$ indépendants de f. Bien sûr, ∂^α désigne aussi l'opérateur usuel $\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_n}}{\partial x_n^{\alpha_n}}$. Les coefficients a_α sont uniquement déterminés par P (appliquer P aux monômes x^β évidents). On dit que P est *elliptique* d'ordre m s'il est d'ordre $\leq m$ et si la fonction $\Omega \times \mathbb{R}^n \to \mathbb{C}$

$$(x, y) \mapsto \sum_{|\alpha|=m} a_\alpha(x) y^\alpha,$$

où y^α désigne le monôme $\prod_i y_i^{\alpha_i}$, ne s'annule pas sur $\Omega \times (\mathbb{R}^n - \{0\})$ (observer que cette fonction est un polynôme homogène de degré m en les y_i, à coefficients dans $\mathcal{C}^\infty(\Omega)$). Par exemple, l'opérateur différentiel $\sum_{1 \leq i,j \leq n} a_{i,j}(x) \frac{\partial^2}{\partial x_i \, \partial x_j}$ est elliptique d'ordre 2 si, et seulement si, la matrice symétrique $(a_{i,j}(x))_{1 \leq i,j \leq n}$ est définie (positive ou négative) pour tout $x \in \Omega$. Observons aussi que si P est elliptique il en va de même de $Q(P)$ pour tout $Q \in \mathbb{C}[X]$.

Les opérateurs différentiels agissent par définition sur $\mathcal{C}^\infty(\Omega)$. Ils agissent aussi naturellement sur l'espace $\mathcal{D}(\Omega)$ des distributions sur Ω par la formule suivante, dans laquelle P est un opérateur différentiel sur Ω, $D \in \mathcal{D}(\Omega)$ et $\varphi \in \mathcal{C}_c^\infty(\Omega)$:

$$\langle P(D), \varphi \rangle := \langle D, P^*(\varphi) \rangle$$

où P^* désigne l'opérateur "adjoint", i.e. $P^*(f) = \sum_{|\alpha| \leq m} (-1)^{|\alpha|} \, \partial^\alpha(a_\alpha f)$ lorsque P est donné par (49). Si D est la distribution associée à une fonction $f \in \mathcal{C}^\infty(\Omega)$, alors $P(D)$ est la distribution associée à $P(f)$ (cela résulte du cas $P = \frac{\partial}{\partial x_i}$ et d'une intégration par partie). On rappelle enfin que toute (classe de) fonction $f \in \mathrm{L}^1_{\text{loc}}(\Omega)$ définit une distribution par la formule $\varphi \mapsto \int_\Omega f \, \varphi \, dx$.

Lemme 6.21. (Théorèmes de régularité elliptique) *Soient Ω un ouvert de $\mathbb{R}^n$, P un opérateur différentiel elliptique sur Ω, $f \in \mathrm{L}^1_{\text{loc}}(\Omega)$, et D la distribution associée à f. On suppose $\mathrm{P}(D) = 0$. Alors :*

(i) (la classe de) f est dans $\mathcal{C}^\infty(\Omega)$,

(ii) si les coefficients de P sont des fonctions analytiques réelles, alors f est analytique réelle.

Démonstration — Le (i) est le Théorème 8.3.1 du livre de Hörmander référencé (la démonstration est très courte et auto-contenue). Le (ii), plus difficile, est démontré quelques pages plus loin dans ce même livre (Théorème 8.6.1). □

Démonstration — (du Lemme 6.20) Supposons que f_n est une suite d'éléments de $\mathcal{A}_{\text{cusp}}^{\text{unit}}[I]_m$ qui converge dans $\mathrm{L}^2(\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}} \backslash \mathrm{GL}_2(\mathbb{R})))$ vers une limite f. On peut représenter (la classe de) f par une fonction borélienne $\mathrm{GL}_2(\mathbb{R}) \to \mathbb{C}$ invariante à gauche par $\mathrm{GL}_2(\mathbb{Z})_e$, de carré intégrable sur tout domaine fondamental (par exemple sur Π_0). En particulier, f est dans $\mathrm{L}^1_{\text{loc}}(G)$ (Cauchy-Schwarz).

On considère l'espace des distributions $\mathcal{D}(G)$ sur l'ouvert $G \subset \mathrm{M}_2(\mathbb{R})$. Pour toute fonction $F \in \mathrm{L}^1_{\text{loc}}(G)$ on note $\mathrm{D}_F \in \mathcal{D}(G)$ la distribution $\mathrm{D}_F(\varphi) = \int_G F(g)\varphi(g)\mathrm{d}g$ pour tout $\varphi \in \mathcal{C}_c^\infty(G)$ (autrement dit, la distribution associée traditionnellement à $F|\det g|^{-n}$). Les actions de G et $\mathfrak{gl}_2(\mathbb{R})$ sur $\mathcal{C}^\infty(G)$ induisent des actions naturelles correspondantes sur $\mathcal{D}(G)$: pour $D \in \mathcal{D}(G)$, $g \in G$ et $X \in \mathfrak{gl}_2(\mathbb{R})$ on définit $\mathrm{R}_g D$ et

$\mathrm{R}_X D$ par les formules suivantes, dans lesquelles φ est une "fonction test" arbitraire dans $\mathcal{C}_c^\infty(G)$ (fonctions de classe $\mathcal{C}^\infty$ et à support compact)

$$\langle \mathrm{R}_g D, \varphi\rangle = \langle D, \mathrm{R}_{g^{-1}}\varphi\rangle \quad \text{et} \quad \langle \mathrm{R}_X D, \varphi\rangle = \langle D, \mathrm{R}_{-X}\varphi\rangle. \tag{50}$$

On alors bien $\mathrm{R}_g D_F = D_{\mathrm{R}_g F}$ et $\mathrm{R}_X D_F = \mathrm{D}_{\mathrm{R}_X F}$ pour $F \in \mathcal{C}^\infty(G) \cap \mathrm{L}^1_{\mathrm{loc}}(G)$, par invariance à droite de $\mathrm{d}g$. L'action de $\mathfrak{gl}_2(\mathbb{R})$ sur $\mathcal{D}(G)$ ainsi définie est aussi une représentation, et définit donc une structure de $\mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$-module sur $\mathcal{D}(G)$. On constate que l'on a $\langle uD, \varphi\rangle = \langle D, u^*\varphi\rangle$ pour tout D et tout $u \in \mathrm{U}(\mathfrak{gl}_2(\mathbb{C}))$, où $u \mapsto u^*$ est l'unique anti-automorphisme de l'algèbre enveloppante vérifiant $X^* = -X$ pour $X \in \mathfrak{gl}_2(\mathbb{R})$ (la propriété universelle de $\mathrm{U}(\mathfrak{g})$ montre son existence pour toute k-algèbre de Lie $\mathfrak{g}$: c'est *l'anti-automorphisme de Chevalley*).

La convergence de f_n vers f dans $\mathrm{L}^2(\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R}))$ entraîne celle de $\langle D_{f_n}, \varphi\rangle$ vers $\langle D_f, \varphi\rangle$ pour tout $\varphi \in \mathcal{C}_c^\infty(G)$, car tout compact de G est inclus dans une réunion finie de domaines fondamentaux pour $\mathrm{GL}_2(\mathbb{Z})_e$ (voir la Remarque 6.22). On en déduit $\mathrm{R}_k D_f = \epsilon(k)^m \mathrm{D}_f$, puis $H^2\,\mathrm{D}_f = -m^2\,\mathrm{D}_f$ avec $H = \mathrm{E}_{1,2} - \mathrm{E}_{2,1}$, et $ID_f = 0$ par les propriétés analogues des D_{f_n}. En particulier, l'espace vectoriel $\mathfrak{z}[H^2].\mathrm{D}_f$ est de dimension finie, de sorte que D_f est annulée par un polynôme non nul en l'élément

$$u = C + H^2 = \sum_{1\le p,q\le 2} \mathrm{E}_{p,q}^2.$$

On a vu expliqué dans le Lemme 5.23 que l'opérateur différentiel u sur G est elliptique dans un voisinage de $1 \in G$. Cela implique qu'il l'est au voisinage de tout point car il commute aux translations à gauche. Le théorème de régularité elliptique (Lemme 6.21 (i)) affirme alors que D_f, a priori seulement $\mathrm{L}^1_{\mathrm{loc}}(G)$, est représentée par une fonction de classe $\mathcal{C}^\infty$, autrement dit on peut supposer $f \in \mathcal{C}^\infty(G)$. Mais alors les relations prouvées sur D_f entraînent d'une part $\mathrm{R}_k f = \varepsilon(k)^m f$ pour tout $k \in K$, et d'autre part $I.f = 0$. Comme f est de carré intégrable sur $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R})$, cela entraîne en fait que f est à croissance modérée : nous reportons à la Proposition 6.25 la vérification de cette propriété.

Il ne reste qu'à voir $f_P = 0$. À l'aide de la formule du Lemme 6.15, il suffit de voir que pour toute fonction $\psi = \psi(y, z, t)$ continue à support compact $\Omega \subset \mathbb{R}^\times \times \mathbb{R}_{>0} \times \mathbb{R}/(2\pi\mathbb{Z})$, on a

$$\int_{[0,1]\times\Omega} f(\mathrm{n}_x\,\mathrm{a}_y\,z\,\mathrm{s}_{e^{it}})\,\psi(y, z, t)\,\mathrm{d}m = 0.$$

Mais une telle identité vaut avec f remplacée par f_n pour tout entier n car on a $(f_n)_P = 0$. Justifions que cette annulation passe à la limite en n. L'image dans G du compact $[0, 1] \times \Omega$ de M est incluse dans une réunion finie, disons $N \ge 1$, de domaines fondamentaux (Remarque 6.22). On a alors pour tout entier n

$$\int_{[0,1]\times\Omega} |f - f_n| \circ \varphi\,\mathrm{d}m \le N \int_X |f - f_n|\,\overline{\lambda} \le C\,N\,\overline{\lambda}(X)^{1/2}\Big(\int_X |f - f_n|^2\,\overline{\lambda}\Big)^{1/2},$$

la seconde inégalité résultant de Cauchy-Schwarz. On conclut car ψ est bornée. □

Remarque 6.22. Nous avons utilisé à deux reprises que toute partie compacte de $G = \mathrm{GL}_2(\mathbb{R})$ est incluse dans une réunion finie de domaines fondamentaux de $\mathrm{GL}_2(\mathbb{Z})_e$. Cela se déduit en effet d'un argument de compacité et du fait que pour tout $g \in G$ il existe un domaine fondamental (borélien) $X \subset G$ tel que g est dans

l'intérieur de X (considérer un translaté à droite convenable de Π_0 par un élément de $\mathrm{GL}_2(\mathbb{R})$).

Théorème 6.23. *Le $(\mathfrak{g}, K)$-module $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$ est une somme directe de $(\mathfrak{g}, K)$-modules irréductibles, chacun d'entre eux intervenant avec une multiplicité finie.*

Nous ferons usage du fait que l'espace $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$ est muni d'un produit hermitien

$$\langle f, f' \rangle = \int_{\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}} \backslash \mathrm{GL}_2(\mathbb{R})} \overline{f(g)} f'(g)\, \overline{\lambda},$$

(appelé *produit de Petersson*), d'après l'inclusion (48). On vérifie immédiatement que l'invariance de $\overline{\lambda}$ pour les translations à droite entraîne pour tout $f, f' \in \mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$ les relations

$$\text{(51)} \qquad \begin{cases} \langle \mathrm{R}_k f, \mathrm{R}_k f' \rangle = \langle f, f' \rangle, & \forall k \in K, \\ \\ \langle \mathrm{R}_X f, f' \rangle = -\langle f,\ \mathrm{R}_X f' \rangle, & \forall X \in \mathfrak{gl}_2(\mathbb{R}). \end{cases}$$

(c'est la notion naturelle de produit hermitien *invariant* sur un $(\mathfrak{g}, K)$-module).

Démonstration — Fixons tout d'abord un idéal $I \subset \mathfrak{z}(\mathfrak{g}_{\mathbb{C}})$ de codimension finie et considérons le $(\mathfrak{g}, K)$-module $V = \mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}[I]$. On a démontré que V est admissible (Théorème 6.18). Montrons qu'il est semi-simple, i.e. que pour tout sous-$(\mathfrak{g}, K)$-module $U \subset V$ il existe un supplémentaire U' de U dans V qui est un sous-$(\mathfrak{g}, K)$-module. Les relations (51) montrent que l'orthogonal $U^{\perp}$ de U dans V est stable par $\mathfrak{gl}_2(\mathbb{R})$ et K, et il est clair que l'on a aussi $U \cap U^{\perp} = 0$, de sorte qu'il ne reste qu'à vérifier $V = U + U^{\perp}$. Ce n'est pas immédiat car V n'est pas complet pour le produit de Petersson en général. Soit $m \in \mathbb{Z}$. L'espace V_m est de dimension finie car on sait que V est admissible, de sorte qu'on a $V_m = U_m \oplus (U^{\perp}_m \cap V_m)$. Mais les relations (51) montrent que V_m et $V_{m'}$ sont orthogonaux pour $m \neq m'$, et donc $U^{\perp}_m \cap V_m = U^{\perp} \cap V_m$, puis $V_m \subset U_m + (U^{\perp})_m$ pour tout $m \in \mathbb{Z}$, ce qui conclut.

Un argument classique du type "modules semisimples" (voir Algebra de Lang Chapitre XIII) montre alors que V est somme de $(\mathfrak{g}, K)$-modules irréductibles, ainsi donc que $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$ (réunion de V), puis que ce dernier est somme directe de $(\mathfrak{g}, K)$-modules irréductibles. Si un facteur irréductible W apparaît une infinité de fois, et si $I = \ker \eta_W$, cela contredit l'admissibilité de $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}[I]$. □

Terminons par quelques remarques. Tout d'abord, l'invariance des éléments de $\mathcal{A}^{\mathrm{unit}}$ par le sous-groupe central $\mathbb{R}^{\times}$ (noter que -1 est dans $\mathrm{GL}_2(\mathbb{Z})$) montre que si un $(\mathfrak{g}, K)$-module irréductible V intervient dans la décomposition de $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}$, on a $\eta_V(Z) = 0$ et $V_m = 0$ pour $m \equiv 1 \bmod 2$ (i.e. V est de poids pairs). Suivant la classification de Bargmann (Théorème 5.16), les cas possibles sont donc :

(i) $V \simeq \mathrm{D}_{k,0}$ avec $k \geq 2$ pair,

(ii) $V \simeq \mathrm{P}_{\eta,\epsilon}$,

(iii) $\dim V$ est finie (et impaire).

(1) D'après le Théorème 4.25 et la Proposition 5.15, la multiplicité du $(\mathfrak{g}, K)$-module $\mathrm{D}_{k,0}$ dans $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ est exactement $\dim \mathrm{M}_k$ (considérer les $\Phi_f(g)|\det g|^{k/2}$ avec $f \in \mathrm{M}_k$).

(2) De même, d'après la Remarque 5.17, la multiplicité du $(\mathfrak{g}, K)$-module $\mathrm{P}_{\eta,\epsilon}$ est exactement la dimension de l'espace de formes de Maass de type (η, ϵ) (espace qui est donc de dimension finie). On sait montrer que cet espace est non nul pour une infinité dénombrable de (η, ϵ), mais un fait remarquable est que l'on connaît aucune valeur exacte de (η, ϵ) intervenant.

(3) Le cas (iii) ne se produit pas. En effet, il n'est pas difficile de voir que l'existence d'un produit hermitien invariant sur V rajoute quelques contraintes supplémentaires dans les cas (ii) et (iii) (voir par exemple les notes de Casselman Ch. I §5). Par exemple, si V est de dimension finie, alors $\dim V = 1$, et donc V est le $(\mathfrak{g}, K)$-module associé à la représentation triviale de $\mathrm{GL}_2(\mathbb{R})$. Mais un tel V serait engendré par une fonction non nulle $f \in \mathcal{A}_{\mathrm{cusp}}$ annulée par R_X pour tout X, et donc serait constante sur chaque composante connexe de $\mathrm{GL}_2(\mathbb{R})$, puis sur tout $\mathrm{GL}_2(\mathbb{R})$ par $\mathrm{GL}_2(\mathbb{Z})$-invariance à gauche. Mais les fonctions constantes non nulles ne sont pas paraboliques (car elles sont égales à leur terme constant).

Remarque 6.24. Le Théorème 6.23 et le Lemme 6.12 décrivent entièrement la structure du $(\mathfrak{g}, K)$-module $\mathcal{A}_{\mathrm{cusp}}$. D'après la remarque 6.10, le produit de Petersson $\langle f, f' \rangle$ est bien défini plus généralement pour $f \in \mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ et $f' \in \mathcal{A}^{\mathrm{unit}}$. L'argument ci-dessus montre alors que l'orthogonal $\mathcal{E}^{\mathrm{unit}}$ de $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$ dans $\mathcal{A}^{\mathrm{unit}}$ est un supplémentaire $(\mathfrak{g}, K)$-stable, puis que l'on a une décomposition naturelle

$$\mathcal{A}_{\mathrm{cusp}} \oplus \mathcal{E} = \mathcal{A}$$

où $\mathcal{E}$ désigne le sous-espace engendré par les fonctions $|\det g|^s (\log|\det(g)|)^n f$ avec $s \in \mathbb{C}$, $n \in \mathbb{N}$ et $f \in \mathcal{E}^{\mathrm{unit}}$. Pour étudier la structure de $\mathcal{E}$, il aurait fallu examiner les séries d'Eisenstein Φ_f avec $f = \mathrm{G}_{k,s}$ définies au chapitre 2, qui en sont des éléments naturels, ainsi que leur terme constant et leur prolongement analytique comme fonction de s. La structure de $\mathcal{E}^{\mathrm{unit}}$ est plus subtile que celle de $\mathcal{A}_{\mathrm{cusp}}^{\mathrm{unit}}$: il n'est pas semi-simple.

5. L'intégrabilité entraîne la croissance modérée

Lors de la démonstration de Lemme 6.20, nous avons utilisé le résultat suivant :

Proposition 6.25. (Harish-Chandra) *Soit $f \in \mathcal{C}^\infty(\mathrm{GL}_2(\mathbb{R}))$ une fonction K-finie à droite et $\mathfrak{z}(\mathfrak{gl}_2(\mathbb{C}))$-finie. On suppose que f est invariante à gauche par $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}$ et de carré intégrable sur $\mathrm{GL}_2(\mathbb{Z})_{\mathrm{e}}\backslash\mathrm{GL}_2(\mathbb{R})$. Alors f est une forme automorphe (i.e. f est à croissance modérée).*

Cette proposition résultera du théorème d'harmonicité de Harish-Chandra et de l'éstimée ci-dessous (due à Borel).

Lemme 6.26. *Il existe des constantes $c, N > 0$ telles que pour tout $t \in \mathbb{R}_{>0}$ on ait*

$$|\{\, \gamma \in \mathrm{GL}_2(\mathbb{Z}),\ ||\gamma|| \leq t \,\}| \ \leq\ c\, t^N.$$

Démonstration — Posons $\Gamma = \mathrm{GL}_2(\mathbb{Z})$ et $G_t = \{g \in \mathrm{GL}_2(\mathbb{R}), ||g|| \leq t\}$ pour t réel > 0. On cherche à majorer $|\Gamma \cap G_t|$. On a $G_t = \emptyset$ pour $t < 1$, on peut donc supposer

$t \geq 1$. Soient $\mu = \mathrm{d}g$ la mesure de Haar déjà introduite sur $\mathrm{GL}_2(\mathbb{R})$, V un voisinage compact de 1 dans $\mathrm{GL}_2(\mathbb{R})$ avec $VV^{-1} \cap \Gamma = \{1\}$, de sorte que la réunion des γV, portant sur les $\gamma \in \Gamma$, est disjointe, et soit enfin $m = \sup_{v \in V} ||v||$. Le sous-ensemble $\coprod_{\gamma \in \Gamma \cap G_t} \gamma V$ est de mesure $|\Gamma \cap G_t| \mu(V)$ et il est inclus dans G_{mt}. Il suffit donc de montrer qu'il existe des constantes $c, N > 0$ avec $\mu(G_t) \leq ct^N$.

Rappelons que tout élément $g \in G$ s'écrit de manière unique sous la forme $g = \mathrm{n}_x \, \mathrm{a}_y \, z \, \mathrm{s}_{e^{it}}$ avec $(x, y, z, t) \in M$ (§3). Dans ces coordonnées, on a

$$||g||^2 = ||\mathrm{p}_{x+iy} z||^2 = z^2(x^2 + y^2 + 1) + z^{-4} y^{-2}.$$

Donc l'inégalité $||g|| \leq t$ entraîne $|z|, |zx|, |zy| \leq t$ et $|z^{-2} y^{-1}| \leq t$, puis $|z^{-1}| \leq t^2$, $|x|, |y|^{\pm 1} \leq t^3$, et $t^{-2} \leq z \leq t$. La formule d'intégration du Lemme (6.15) entraîne donc l'inégalité

$$\mu(G_t) \leq 2\pi \, (\int_{|x| \leq t^3} \mathrm{d}x \,) \, (\int_{t^{-3} \leq |y| \leq t^3} \frac{\mathrm{d}y}{y^2} \,) \, (\int_{t^{-2} \leq z \leq t} \frac{\mathrm{d}z}{z}).$$

L'intégrale de droite vaut $2\,\pi \cdot 2\,t^3 \cdot 2\,(t^3 - t^{-3}) \cdot 3 \log t$, qui est bien $\leq c\,t^7$ pour une constante $c > 0$ adéquate. □

Démonstration — Démontrons maintenant la Proposition 6.25. On pose encore $G = \mathrm{GL}_2(\mathbb{R})$ et $\Gamma = \mathrm{GL}_2(\mathbb{Z})$. D'après le théorème d'harmonicité de Harish-Chandra, il existe une fonction continue et à support compact φ sur G vérifiant $f = f * \varphi$. Considérons la fonction

$$\psi : G \times G \longrightarrow \mathbb{C}, \;\; (h, g) \mapsto \sum_{\gamma \in \Gamma} \varphi(h^{-1} \gamma g).$$

Soit $\Omega \subset G$ un compact hors duquel φ est nulle. À $g, h \in G$ donnés, la somme ci-dessus est nulle pour γ qui n'est pas dans $h\Omega g^{-1}$. Mais $\Gamma \cap h\Omega g^{-1}$ est fini, car discret et compact : la somme ci-dessus est finie, et ce même uniformément lorsque g et h restent dans un compact de G, de sorte que ψ est bien définie et continue. On a pour tout $g \in G$

$$f(g) \;=\; \int_G f(h) \varphi(h^{-1} g) \mathrm{d}h \;=\; \sum_{\gamma \in \Gamma} \int_{\gamma \Pi_0} f(h) \varphi(h^{-1} g) \mathrm{d}h$$

$$= \sum_{\gamma \in \Gamma} \int_{\Pi_0} f(h) \varphi(h^{-1} \gamma^{-1} g) \mathrm{d}h \;=\; \int_{\Pi_0} f(h) \psi(h, g) \mathrm{d}h.$$

L'échange des sommations est justifié car d'une part f est intégrable sur Π_0, car de carré intégrable et $\mu(\Pi_0) < \infty$, et d'autre part $h \mapsto \psi(h, g)$ est continue et bornée. En effet, nous allons montrer plus précisément la majoration

$$\text{Il existe } \; c, N > 0 \; \text{ avec } \; \psi(h, g) \leq c ||g||^N. \tag{52}$$

Elle entraînera $|f(g)| \leq c||g||^N (\mu(\Pi_0) \int_{\Pi_0} |f(h)|^2 \mu)^{1/2}$, et donc la proposition.

Notons M un majorant de $|\varphi|$ sur G. Observons que si on a $h^{-1} \gamma g \in \Omega$ et $h^{-1} \gamma' g \in \Omega$ avec $\gamma, \gamma' \in \Gamma$ et $h, g \in G$, alors on a $g^{-1} \gamma^{-1} \gamma' g \in \Omega^{-1} \Omega$. En particulier, si ω désigne le sup des $||a||$ avec a variant dans le compact $\Omega^{-1}\Omega$ de G, on a

$$|\gamma^{-1} \gamma'| \;\leq\; ||g||\,||g^{-1}||\,\omega.$$

Rappelons qu'il existe des réels $c_0, N_0 > 0$ avec $||g^{-1}|| \leq c_0||g||^{N_0}$ pour tout $g \in G$. On en déduit que pour tout $h, g \in G$ on a

$$\psi(h,g) \leq M(1 + |\{\gamma \in \mathrm{GL}_2(\mathbb{Z}), ||\gamma|| \leq c_0||g||^{N_0+1}\}|).$$

La relation (52) découle alors du Lemme 6.26. □

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), $A \mapsto \mathrm{O}_n(A) = \{m \in \mathrm{M}_n(A), {}^t m m = \mathrm{I}_n\}$ (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

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

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 $\mathrm{Spec}\, \mathbb{Z}[T_1, \ldots, T_m]$, 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

$$U_N \,=\, N\widehat{\mathbb{Z}} \,=\, \{(N\,x_p)_p,\ x \in \mathbb{A}_f\} \,=\, \left(\prod_{p|N} N\mathbb{Z}_p\right) \times \prod_{p \not| N} \mathbb{Z}_p,$$

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

$$\begin{array}{ccccc} G(\mathbb{Z}_p) & \xrightarrow{\mathrm{i}} & \mathbf{A}^m(\mathbb{Z}_p) & \xrightarrow{\sim} & \mathbb{Z}_p^m \\ \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{can}} \\ G(\mathbb{Z}_p/N\mathbb{Z}_p) & \xrightarrow{\mathrm{i}} & \mathbf{A}^m(\mathbb{Z}_p/N\mathbb{Z}_p) & \xrightarrow{\sim} & (\mathbb{Z}_p/N\mathbb{Z}_p)^m \end{array}$$

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 $\mathrm{i} : X \to \mathbf{A}^m$ 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. □

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 $UK \subset U$ alors U/K est fini et K est compact,

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

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 uK 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, uK est fermé et donc compact pour tout $u \in U$. Choisissant $u \in U$ (qui est non vide), cela montre que $K = u^{-1}uK$ 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 $UV \subset U$. 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 $UK \subset U$, 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 $UK \subset U$. Alors U est réunion disjointe de $|U/K| < \infty$ parties de la forme uK, 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

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

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 $\mu(1 + p\mathrm{M}_n(\mathbb{Z}_p)) = \mu(p\mathrm{M}_n(\mathbb{Z}_p)) = p^{-n^2}$. □

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 $(g^{-1}\operatorname{Supp} f) \cap H$ de H. Il a donc un sens à poser $f_H(g) = \int_{h\in H} f(gh)\mathrm{d}h$ 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

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

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 $\mathrm{Supp}\,\varphi \;=\; \coprod_{i=1}^m K\,g\,h_i$ 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. □

4. Retour sur les anneaux de Hecke 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, 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 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 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 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

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

Comme $\mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G/K])$ agit à droite sur le membre de gauche, l'anneau opposé H(G, K) y agit à gauche, ce qui fait de V^K un 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 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* 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 $\mathrm{H}(\mathrm{R}(\mathbb{Q}_p))=\mathbb{Z}[\mathrm{R}_p^{\pm 1}]$, 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 $\mathrm{H}(G,K)\xrightarrow{\sim}\mathrm{H}(\mathrm{R}(\mathbb{Q}_p^n))$ 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 $\varphi: G\xrightarrow{\sim}G^{\mathrm{opp}}$, 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 $n \mapsto t^{-1}t'n'^{-1}t'^{-1}tn$. □

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). □

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

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

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

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

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*

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

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 $\sigma \in \mathfrak{S}_n$

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

(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 $s = n-1$). □

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 $\mathrm{vol} = \mathrm{d}n$. 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. □

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 $i = 1, \dots, n$, considérons l'élément (contenant i fois 1)

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

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 $\mathrm{b}_{\omega_i} = \Sigma_i(X_1, \dots, X_n)$ ($i$ème polynôme symétrique élémentaire). On a donc la formule

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

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

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

(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 $(i, j) \in \{1, \dots, n\}^2$ 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 $\gamma \in \mathrm{GL}_n(\mathbb{Q})$, $i \in \{1, \dots, h\}$ 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 $|f(h, g_f)| \leq c||\gamma^{-1}||^N||h||^N = c'||h||^N$. □

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 $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}(n)$, 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 $\mathcal{A}^{\mathrm{unit}}_{\mathrm{cusp}}(n)$, 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

$$\mathrm{L}(s, \rho, f) \;=\; \prod_{p \not| N} \det(\mathrm{I}_n - p^{-s}\rho(\mathrm{c}_p(f)))^{-1}.$$

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*

$$(T - \pi_p(T))^r f = 0 \quad \forall p \not| N,\ \forall T \in \mathrm{H}_p.$$

.

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. □

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