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 $1 + \chi(p)^{-1}p$.*