Polynômes de Hall

Travail Encadré de Recherche

Max Reh

encadré par M. Jérôme Germoni

Université Claude Bernard Lyon 1
Master 1 Mathématiques Générales

2013-2014

Table des matières

1 Rappels

1.1 Groupes

Définition 1.1. Soient G un groupe abélien et $(H_i)_{i\in I)} \neq \emptyset$ une famille de sous-groupes de G. Si

$$\forall j \in I, H_j \cap \sum_{i\in I, i\neq j} H_i = \{0\}$$

le sous-groupe $\sum_{i\in I} H_i$ est **somme directe** des sous-groupes H_i et est noté $\bigoplus_{i\in I} H_i$.

Définition 1.2. Soit G un groupe abélien et $H \subseteq G$.H est appelé **facteur direct** de G s'il existe un $K \subseteq G$ tel que $G = H \oplus K$.

Proposition 1.3. *Soient G un groupe abélien, $H \subseteq G$ et i l'injection canonique de H dans G. Alors H est un facteur direct de G si et seulement s'il existe un $p \in Hom(G, H)$ tel que $p \circ i = id_H$*

Démonstration. " $\Leftarrow$ " : On suppose qu'il existe $p \in \mathrm{Hom}(G, H)$ tel que $p \circ i = \mathrm{id}_H$ et on pose $h = p(g)$ pour tout $g \in G$. Alors on a $h = p \circ i(h) = p(h)$, i.e. $(g - h) \in \mathrm{Ker}(p)$. On a $g = h + (g - h)$ et pour $x \in H \cap \mathrm{Ker}(p)$, $x = p(x) = 0$. Donc $G = H \oplus \mathrm{Ker}(p)$.

" $\Rightarrow$ " : On suppose que $G = H \oplus K$. Donc tout $g \in G$ s'écrit de manière unique $g = h + k$, $h \in H$ et $k \in K$. Si on prend $p(g) = h$ pour p, on a le résultat. □

Définition 1.4. Un groupe abélien est dit **libre** s'il est somme directe de groupes monogènes infinis.

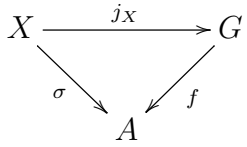
On peut aussi dire que G est libre si on peut trouver un ensemble I et une famille d'éléments de G, $X = \{x_i\}_{i\in I}$ tels que

$$G = \bigoplus_{i\in I} \langle x_i \rangle \quad \text{et} \quad \langle x_i \rangle \cong \mathbb{Z}, \quad \forall i \in I$$

On dit que X est une **base** de G.

Theorème 1.5 (propriété universelle d'un groupe abélien libre)**.** *Soient G un groupe abélien, X une partie de G et j_X l'inclusion canonique de X dans G. Alors G est abélien libre de base X si et seulement si, pour tout groupe*

abélien A et toute application $\sigma : X \to A$, il existe un unique morphisme de groupes $f : G \to A$ tel que $f \circ j_X = \sigma$.



Démonstration. On suppose que le groupe abélien G est libre de base X.

Existence de f : On note $X = \{x_i\}_{i\in I}$ la base donnée de G. Tout élément x de G s'écrit de manière unique $x = \sum_{i\in I} n_i x_i$, où les n_i sont des entiers nuls sauf pour un nombre fini de $i \in I$. Alors, si on pose $f(x) = \sum_{i\in I} n_i \sigma(x_i)$, cette somme est bien définie. On voit facilement que l'application f ainsi définie est un morphisme de groupes et vérifie $f \circ j_X = \sigma$.

Unicité de f : On suppose $f' : G \to A$ un autre morphisme de groupes vérifiant $f' \circ j_X = \sigma$. On a donc $f(x_i) = f'(x_i)$ pour tout élément $x_i \in X$, d'où $f(x) = f'(x)$ pour tout élément x de G.
Maintenant on suppose que le groupe abélien G est tel que pour tout groupe abélien A et toute application $\sigma : X \to A$, il existe un unique morphisme de groupes $d : G \to A$ tel que $f \circ j_X = \sigma$. C'est en particulier vérifié si $A = \mathbb{Z}^{(X)}$ est libre de base X et $\sigma = i_X$ est l'injection de X dans $\mathbb{Z}^{(X)}$. Le début de la démonstration montre qu'il existe un morphisme de groupes $g : A \to G$ tel que $g \circ i_X = j_X$. Les morphismes f et g sont réciproques l'un de l'autre. Donc ce sont des isomorphismes. □

Corollaire 1.6. *Tout groupe abélien est isomorphe à un quotient d'un groupe abélien libre.*

Démonstration. Soit X une partie génératrice d'un groupe abélien G et σ l'inclusion de X dans G. On considère le groupe libre de base X, $\mathbb{Z}^{(X)}$ et j_X l'inclusion de X dans $\mathbb{Z}^{(X)}$. D'après le théorème 1.5, il existe un morphisme de groupes $f : \mathbb{Z}^{(X)} \to G$ tel que $f \circ j_X = \sigma$. Tout élément x de G s'écrit

$$x = \sum_{1\le l\le k} n_i \sigma(x_{i_l}) = \sum_{1\le l\le k} n_l f(j_X(x_{i_l})) = f\left(\sum_{1\le l\le k} n_l j_X(x_{i_l})\right).$$

Donc f est surjectif. On en déduit que le groupe G est isomorphe au groupe $\mathbb{Z}^{(X)}/\mathrm{Ker}(f)$. □

Corollaire 1.7. *Soit G un groupe abélien, G' un groupe abélien libre et $p : G \to G'$ un homomorphisme (de groupes abéliens) surjectif. Alors il existe un homomorphisme (de groupes abéliens) $s : G' \to G$ tel que $p \circ s = id_{G'}$. En particulier, $s(G')$ est un facteur direct de G.*

Démonstration. Soit X une base de G'. Comme p est sujectif, il existe une application $j : X \to G$ telle que $p \circ j = id_X$. D'après le théorème 1.5, il existe un morphisme de groupes $s : G' \to G$ tel que $p \circ s = id_{G'}$. On déduit de la proposition 1.3 que $s(G')$ est facteur direct dans G. □

Remarque. Le morphisme s est injectif car $p \circ s = \mathrm{id}_{G'}$ et ça implique que G' et $s(G') \subseteq G$ sont isomorphe. De ce fait on peut dire que G' est isomorphe à un facteur direct du G sous les hypothèses du corollaire 1.6.
On a $G = \mathrm{Ker}(p) \oplus s(G')$ sous les hypothèses ci-dessus (cf proposition 1.3 et corollaire 1.7).
Dans ce cas on apelle s une **section** de p.

Définition 1.8. On dit qu'un groupe est de **type fini** s'il est engendré par une partie finie.

Définition 1.9. On appelle le cardinal d'une base d'un groupe abélien libre G le **rang** de G.

Définition 1.10. Soit G un groupe abélien. G est dit **de torsion** si tout $g \in G$ est d'ordre fini. Il est dit **sans torsion** si tout $g \in G$, différent de l'élément neutre, est d'ordre infini.

Proposition 1.11. *Soit G un groupe abélien. Les éléments de G d'ordre fini de G forment un sous-groupe,*

On note $T(G)$ l'ensemble des éléments d'ordre fini de G et on l'appelle le **sous-groupe de torsion** de G.

Démonstration. Il y a trois cas :
Si G est un groupe sans torsion alors $T(G) = 0$, si G est un groupe de torsion alors $T(G) = G$; dans ces ceux cas le résultat est trivial.
On suppose que G soit un groupe tel que $T(G)$ soit distinct de G et de $\{0\}$. Soient x et y deux éléments de $T(G)$; on note p (resp. q) l'ordre de x (resp. y). On a $pq(x - y) = 0$, donc $(x - y) \in T(G)$ et $T(G)$ est un sous-groupe de G. soit $\overline{x}$ un élément du groupe $G/T(G)$. S'il existe $p \in \mathbb{N}^*$ tel que $p\overline{x} = 0$, on a $px \in T(G)$ et $\overline{x} = 0$, d'où $G/T(G)$ est un groupe sans torsion. □

Définition 1.12. Soient G un groupe abélien et p un nombre premier. La **composante p-primaire** $G(p)$ de G est l'ensemble des éléments de G dont l'ordre est une puissance de p.

Proposition 1.13. *Soient G un groupe abélien et p un nombre premier. La composante p-primaire $G(p)$ est un sous-groupe de G.*

Theorème 1.14. *Soient G un groupe abélien de torsion et $\mathcal{P}$ l'ensemble des nombres premiers. Alors $G = \bigoplus_{p\in\mathcal{P}} G(p)$.*

Démonstration. Soit x un élément d'ordre n de G. On considère $n = p_1^{r_1} \cdots p_k^{r_k}$ la décomposition en facteurs premiers de n et on pose $n_i = n/p_i^{r_i}$, $1 \leq i \leq k$. Les nombres entiers n_i sont premiers entre eux dans leur ensemble donc, d'après le théorème de Bezout, il existe des nombres entiers $a_1, \ldots, a_k$ tels que $\sum_{1\leq i\leq k} a_i n_i = 1$. On en déduit que

$$x = 1x = a_1(n_1x) + \ldots + a_k(n_kx),$$

où, pour $1 \leq i \leq k$, n_ix est d'ordre $p_i^{r_i}$. Par conséquent,

$$x \in \sum_{1\leq i\leq k} G(p_i) \subseteq \sum_{\mathcal{P}} G(p),$$

d'où $G \subseteq \sum_{\mathcal{P}} G(p)$. Comme l'inclusion dans l'autre sens est évidente, on a

$$G = \sum_{\mathcal{P}} G(p).$$

On va montrer que cette somme est directe. Soit p_0 un élément de $\mathcal{P}$ et soit

$$x \in G(p_0) \cap \sum_{p\neq p_0, p\in\mathcal{P}} G(p).$$

Il existe $\{p_1, \ldots, p_n\} \subset (\mathcal{P}\setminus\{p_0\})$ tel que $x = x_1 + \ldots + x_n$ avec $x_i \in G(p_i)$. Chaque x_i, $1 \leq i \leq k$, est d'ordre $p_i^{s_i}$ et, puisque les p_i sont premiers et que le groupe G est abélien, x est d'ordre $p_1^{s_1}, \cdots p_n^{s_n}$. Mais, puisque $x \in G(p_0)$, il est aussi d'ordre $p_0^{s_0}$, d'où $x = 0$. On a donc

$$G = \bigoplus_{p\in\mathcal{P}} G(p).$$

□

Proposition 1.15. *Soit G un groupe abélien de type fini. Alors,*
(i) G est de torsion si et seulement si G est fini,
(ii) G est sans torsion si et seulement si G est libre.

Démonstration. (i) "⇐" Il est clair que tout groupe fini est de torsion.

"⇒" Soit G un groupe abélien de type fini de torsion et soit $\{x_1, \ldots, x_n\}$ une famille génératrice de G. Chaque élément x_i, $1 \leq i \leq n$ est d'ordre fini

p_i. Par conséquent, dans toute écriture d'un élément x quelconque de G, $x = \sum_{1\leq i\leq n} n_i x_i$ on peut supposer que $0 \leq n_i \leq p_i - 1$. On a donc

$$G = \left\{ \sum_{1\leq i\leq n} n_i x_i \right\}$$

où les n_i ne prennent qu'un nombre fini de valeurs, par conséquent le groupe G est fini.

(ii) "$\Leftarrow$" Il est clair qu'un groupe abélien libre est sans torsion

"$\Rightarrow$" Soit G un groupe abélien de type fini sans torsion et soit $\{x_1, \ldots, x_s\}$ une famille génératrice de G. On va raisonner par récurrence sur s.
(Initialisation :) Si $s = 1$, G est isomorphe à $\mathbb{Z}$ et donc libre de rang 1.
(Hérédité :) On suppose le résultat vrai pour les groupes engendrés par $r \leq s - 1$ éléments. Si la famille $\{x_1, \ldots, x_s\}$ est libre, c'est une base et le groupe G est libre. Sinon, on considère une combinaison linéaire nulle liant les générateurs de G,

$$\sum_{1\leq i\leq s} n_i x_i = 0.$$

Les coefficients n_i étant dans $\mathbb{Z}$ et le groupe G étant sans torsion, on peut supposer que les n_i sont premiers entre eux dans leur ensemble (sinon, on met en facteur le *pgcd* de n_i et on utilie l'hypothèseque le groupe est sans torsion).
Si l'un des coefficients, par exemple n_k, est égal à 1, on a

$$x_k = \sum_{1\leq i\leq s, i\neq k} n_i x_i$$

et le groupe G est engendré par les $s - 1$ éléments $(x_i)_{1\leq i\leq s, i\neq k}$. Il est donc libre par hypothèse de récurrence.
si tous les coefficients n_i sont distincts de 1, il existe au moins deux coefficients n_j et n_k tels que $|n_j| > |n_k| > 0$. En faisant la division euclidienne de n_j par n_k, on a $|n_j - qn_k| < |n_k|$. On pose $x'_k = x_k + qx_j$; il est clair que $\{x_1, \ldots, x_j, \ldots, x'_k, \ldots, x_s\}$ est une partie génératrice de G. D'autre part, on a

$$n_1 x_1 + \ldots + (n_j - qn_k)x_j + \ldots + n_k x'_k + \ldots + n_s x_s = 0$$

où les coefficients sont premiers entre eux dans leur ensemble et $|n_j - qn_k| < |n_j|$. Alors, ou bien $|n_j - qn_k| = 1$ et on est ramené au cas précédent, ou bien $|n_j - qn_k| > 1$ et on réitère le procédé. Comme ce procédé converge vers le *pgcd* des n_i, on arrivera, en un nombre fini d'étapes, à ce que l'un des coefficients soit égal à 1.
Dans tous les cas, on se ramène à une famille génératrice constituée de $(s-1)$ éléments au plus et, par hypothèse de récurrence, le groupe G est libre. □

1.2 Anneaux

Définition 1.16. Un anneau est dit **principal** s'il est un anneau intègre (i.e. un anneau commutatif unitaire différent de l'anneau nul et qui ne possède aucun diviseur de zéro) dont chaque idéal est un idéal principal, i.e. engendré par un unique élément.

Définition 1.17. Un **anneau de valuation discrète** est un anneau principal, qui ne possède qu'un idéal maximal et tel que cet idéal soit non nul.

Définition 1.18. Un **corps résiduel** d'un anneau commutatif A est le quotient de A par un idéal maximal. Comme l'idéal est maximal, l'anneau issu du quotient a une structure de corps.

2 Structure des groupes abéliens de type fini

Proposition 2.1 (sans démonstration)**.** *Si G est un groupe abélien de type fini, alors il est somme directe d'un groupe libre de rang fini et d'un groupe fini (qui est son sous-groupe de torsion $T(G)$).*

Comme cette décomposition est unique à isomorphisme près, le rang du groupe libre F est parfaitement déterminé et donc le groupe F aussi.

Theorème 2.2 (de la base adaptée)**.** *Soient G un groupe abélien libre, $rg(G) = n$ et H un sous-groupe. Alors :*

i) Il existe une base $(e_1, \ldots, e_n)$ de G, un entier $q \leq n$ et une famille d'entiers positifs $a_1, \ldots, a_q$ tels que
   a) pour $1 \leq i \leq q-1$, a_i divise a_{i+1},
   b) $(a_1 e_1, \ldots, a_q e_q)$ forme une base de H.

ii) Les entiers q, $a_q, \ldots, a_q$ qui vérifient ces conditions sont uniquement déterminés par G et H.

Démonstration. i) Il y a deux cas.
Premier cas : $H = \{0\}$. Dans ce cas, le résultat est trivial.
Deuxieme cas : $H \neq \{0\}$. Dans ce cas, on va faire la preuve par récurrence sur n.
(Initialisation :) Pour $n = 1$, G est isomorphe à $\mathbb{Z}$ et on connait déjà le résultat.
(Hérédité :) On suppose que le théorème est vrai si le rang (du groupe libre) est inférieur ou égal à $(n-1)$.
Soit G muni d'une base $(x_i)_{1 \leq i \leq n}$ et soit $(\pi_i)_{1 \leq i \leq n}$ les fonctions coordonnées associées à cette base. Chaque $x \in G$ s'écrit de manière unique sous la forme $x = \sum_{1 \leq i \leq n} n_i x_i$ et on pose $\pi_i(x) = n_i$.
Comme $u(H)$ est un sous-groupe de $\mathbb{Z}$ pour tout $u \in \mathrm{Hom}(G, \mathbb{Z})$, c'est de la forme $\mathbb{Z}\alpha_u$. Donc on a trouvé un ensemble d'entiers positifs ou nuls (α_u). Il existe au moins une fonction coordonnée qui s'annule pas sur H, car H est non nul, alors il existe des $\alpha_u \neq 0$. On pose

$$a = \inf_{\substack{u \in \mathrm{Hom}(G,\mathbb{Z}) \\ \alpha_u \neq 0}} (\alpha_u).$$

On note f un élément de $\mathrm{Hom}(G, \mathbb{Z})$ qui correspond à a tel que $f(H) = \mathbb{Z}a$. On écrit $h = \sum_{1 \leq i \leq n} h_i x_i$ pour $h \in H$ tel que $f(h) = a$.

Lemme 2.3. *L'entier a divise h_i pour tout i, $1 \leq i \leq n$*

Démonstration. Soit d le plus grand commun diviseur de a et h_i. D'après le théorème des restes chinois existent des entiers r et s tels que

$$d = rh_i + sa = r\pi_i(h) + sf(h) = (r\pi_i + sf)(h).$$

Puisque $(r\pi_i + sf) \in \mathrm{Hom}(G, \mathbb{Z})$, il existe un α tel que $(r\pi_i + sf)(H) = \mathbb{Z}\alpha$. Alors $\mathbb{Z}d \subseteq \mathbb{Z}\alpha$. Et comme d divise a, on a $\mathbb{Z}a \subseteq \mathbb{Z}d$ et alors $\mathbb{Z}a \subseteq \mathbb{Z}\alpha$. On en déduit que α divise a et, car a est minimal, $\alpha = a$. Alors $\mathbb{Z}d = \mathbb{Z}a$, donc a divise d et conséquemment a divise h_i. □

En conséquence de ce lemme, il existe $g_i \in \mathbb{Z}$ tel que $h_i = ag_i$ pour tout i, $1 \leq i \leq n$. On pose $g = \sum_{1 \leq i \leq n} g_i x_i$ et on a $h = ag$, donc $f(h) = f(ag) = af(g)$ et car $f(h) = a$, on a $f(g) = 1$. Alors le morphisme $f : G \to \mathbb{Z}$ admet une section λ, qui est définie par $\lambda(1) = g$. Le groupe $\lambda(\mathbb{Z})$ est libre de rang 1 comme il est isomorphe à $\mathbb{Z}$ et il s'identifie à $\langle g \rangle$. Il est donc aussi libre de rang 1. Du corollaire 1.6 et de la remarque après le corollaire 1.7 on déduit que $G = \langle g \rangle \oplus \mathrm{Ker}(f)$. Alors $\mathrm{Ker}(f)$ est un groupe libre de rang $n-1$ et on a

$$H = (\langle g \rangle \cap H) \oplus (\mathrm{Ker}(f) \cap H).$$

En plus, on a $f(y) = ba$, $b \in \mathbb{Z}$ pour tout $y \in H$, donc $y = bh + (y - bag)$ et comme $f(g) = 1$, on a $(y - bag) \in \mathrm{Ker}((f) \cap H)$. Ça et le fait que tout élément de H a une écriture unique en fonction de la décomposition en somme directe (donnée ci-dessus) donne que $\langle g \rangle \cap H = \langle h \rangle$. Alors

$$H = \langle h \rangle \oplus (H \cap \mathrm{Ker}(f)).$$

Par hypothèse de récurrence appliquée au $\mathrm{Ker}(f)$ et $(\mathrm{Ker}(f) \cap H) \subseteq \mathrm{Ker}(f)$, il existe une base $(e_1 \ldots, e_n)$ de $\mathrm{Ker}(f)$, un entier $q \geq 2$ et des entiers positifs $a_2, \ldots, a_q$ avec $a_2 | a_3 | \ldots | a_q$ tels que $(a_2 e_2, \ldots, a_q e_q)$ soit une base de $\mathrm{Ker}(f) \cap H$.
Avec $a_1 = a$ et $e_1 = g$ (i.e. $a_1 e_1 = h$) $(a_1 e_1, a_2 e_2, \ldots, a_q e_q)$ est une base de H. Pour montrer que a_1 divise a_2 on considère le morphisme $v : G \to \mathbb{Z}$, $v(e_1) = v(e_2) = 1$ et $v(e_i) = 0$ pour $i \geq 3$. Donc on a $a = a_1 = v(a_1 e_1) = v(h)$ et $\mathbb{Z}a \subseteq \mathbb{Z}\beta$ car $v(H) = \mathbb{Z}\beta$. Par minimalité de a, $\mathbb{Z}\beta = \mathbb{Z}a = \mathbb{Z}a_1$. D'un autre côté, $a_2 = v(a_2 e_2) \in v(H) = \mathbb{Z}\beta$, alors$a_2 \in \mathbb{Z}a_1$, d'où le résultat que a_1 divise a_2.

ii) Pour la démonstration de cette partie, on a besoin du théorème **de structure des groupes abéliens de type fini**. □

Theorème 2.4. *Soit G un groupe abélien de type fini. Alors il existe un $p \in \mathbb{Z}$ et une unique famille $(a_1, \ldots, a_r)$ d'entiers supérieurs ou égaux à 2, où a_i divise a_{i+1} pour $1 \leq i \leq r-1$, tels que*

$$G \cong \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}.$$

Démonstration. *Existence :* G a une famille génératrice $(x_1, \ldots, x_n)$ et il existe un morphisme surjectif $f : \mathbb{Z}^n \to G$ tel que $G \cong \mathbb{Z}^n/\mathrm{Ker}(f)$. Comme

on a vu dans le théoreme précédent 2.2, il existe une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$, un entier $1 \leq q \leq n$ et des entiers $a_1, \ldots, a_q$ avec $a_i | a_{i+1}$ pour $1 \leq i \leq q-1$ tels que $(a_1 e_1, \ldots, a_q e_q)$ soit une base de $\mathrm{Ker}(f)$. On a

$$\mathbb{Z}^n/\mathrm{Ker}(f) \cong \bigoplus_{1 \leq i \leq n} (\mathbb{Z}e_i/\mathbb{Z}a_i e_i)$$

si on pose $a_{q+1} = \ldots = a_n = 0$. Mais on a aussi $\mathbb{Z}e_i/\mathbb{Z}a_i e_i \cong \mathbb{Z}/a_i\mathbb{Z}$ pour tout i et $\mathbb{Z}/a_i\mathbb{Z} = \mathbb{Z}$ pour $a_i = 0$. On pose $p = (n-q)$ et élimine les a_i éventuellement $= 1$, on obtient

$$G \cong \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}$$

ce qui prouve l'existence.

Unicité : On suppose qu'il existe deux familles de nombres entiers $(p, a_1, \ldots, a_r)$ et $(q, b_1, \ldots, b_s)$ telles que

$$G \cong \mathbb{Z}^p \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_r\mathbb{Z}$$
$$G \cong \mathbb{Z}^q \oplus \mathbb{Z}/b_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/b_s\mathbb{Z}.$$

Ces deux sommes sont tous les deux une décomposition de G en la somme directe d'un groupe libre de rang fini et d'un groupe fini. On sait que cette décomposition est unique (proposition 2.2), alors $\mathbb{Z}^p \cong \mathbb{Z}^q$, i.e. $p = q$ et

$$\bigoplus_{1 \leq i \leq r} \mathbb{Z}/a_i\mathbb{Z} \cong T(G) \cong \bigoplus_{1 \leq i \leq s} \mathbb{Z}/b_i\mathbb{Z}.$$

On a

$$T(G) = \bigoplus_{1 \leq i \leq k} G(p_i)$$

si $|T(G)| = p_1^{t_1} \cdots p_k^{t_k}$ d'après le théorème 2.12.
On admet provisoirement que pour $1 \leq i \leq k$ l'unicité de la décomposition en somme directe de ce théorème soit vérifiée pour les $G(p_i)$ et on montre que cela implique l'unicité de la décomposition pour $T(G)$.
Alors on a

$$\bigoplus_{1 \leq i \leq r} \mathbb{Z}/a_i\mathbb{Z} \cong T(G) \cong \bigoplus_{1 \leq i \leq s} \mathbb{Z}/b_i\mathbb{Z}.$$

avec $a_1 | a_2 | \ldots | a_r$ et $b_1 | b_2 | \ldots | b_s$.
Pour $1 \leq i \leq r$ on note x_i un générateur de $\mathbb{Z}/a_i\mathbb{Z}$. Donc l'ordre de x_i, $o(x_i) = a_i$ divise $|T(G)|$. Alors

$$a_i = p_1^{w_{i,1}} \cdots p_k^{w_{i,k}} \quad \text{avec} \quad 0 \leq w_{i,j} \leq t_j$$

et

$$t_j = \sum_{1\leq i\leq r} w_{i,j} \quad \text{avec} \quad w_{i,j} \leq w_{i+1,j} \quad \text{car} \quad a_i | a_{i+1}.$$

Alors on a $\langle x_i \rangle = \bigoplus_{1\leq i\leq k} \langle x_{i,j} \rangle$ où $o(x_{i,j}) = p_j^{w_{i,j}}$ pour tout $1 \leq i \leq r$ et en conséquence

$$T(G) = \bigoplus_{1\leq i\leq r} \left(\bigoplus_{1\leq j\leq k} \langle x_{i,j} \rangle \right) = \bigoplus_{1\leq j\leq k} \left(\bigoplus_{1\leq i\leq r} \langle x_{i,j} \rangle \right).$$

Puisque $| \bigoplus_{1\leq i\leq r} \langle x_{i,j} \rangle | = p_j^{w_{1,j}+\ldots+w_{r,j}} = p_j^{t_j}$ on a

$$\bigoplus_i \mathbb{Z}/(w_{i,j})\mathbb{Z} = \bigoplus_{1\leq i\leq r} \langle x_{i,j} \rangle = G(p_j)$$

qui a une unique décomposition en somme directe de groupes cycliques comme on l'a admis provisoirement.
Maintenant on prend l'autre décomposition de $T(G)$, on note y_i un générateur de $\mathbb{Z}/b_i\mathbb{Z}$ et le même raisonnement donne

$$b_i = p_1^{w'_{i,1}} \cdots p_k^{w'_{i,k}} \quad \text{avec} \quad 0 \leq w'_{i,j} \leq t_j,$$

$$t_j = \sum_{1\leq i\leq s} w'_{i,j} \quad \text{et} \quad w'_{i,j} \leq w'_{i+1,j} \quad \text{car} \quad b_i | b_{i+1}$$

et

$$T(G) = \bigoplus_{1\leq j\leq k} \left(\bigoplus_{1\leq i\leq s} \langle y_{i,j} \rangle \right)$$

avec

$$\bigoplus_i \mathbb{Z}/(w'_{i,j})\mathbb{Z} = \bigoplus_{1\leq i\leq s} \langle y_{i,j} \rangle = G(p_j).$$

Pour terminer la preuve, il suffit de montrer que pour tout j, on a : $\forall i, w_{i,j} = w'_{i,j}$. En effet, cela entraîne que $\forall i, a_i = b_i$ puis que $r = s$. Pour le voir, on énonce un lemme.

Lemme 2.5. *Soit P un p-groupe abélien fini avec p premier tel que*

$$P \cong \bigoplus_{1\leq i\leq r} \mathbb{Z}/a_i\mathbb{Z} \cong \bigoplus_{1\leq j\leq s} \mathbb{Z}/b_i\mathbb{Z}$$

avec $a_1|a_2|\ldots|a_r$ et $b_1|b_2|\ldots|b_s$. Alors $r = s$ et $a_i = b_i$ pour tout $1 \leq i \leq r$.

Démonstration. On a nécessairement $a_i = p^{\alpha_i}$ et $b_j = p^{\beta_j}$ pour $\alpha_i, \beta_j \in \mathbb{N}$ convenables, alors les relations de divisibilité se traduisent par $0 < \alpha_1 \leq \ldots \leq \alpha_r$ et $0 < \beta_1 \leq \ldots \leq \beta_s$ et la conclusion par $r = s$ et $\alpha_i = \beta_i$ pour tout $1 \leq i \leq r$.
On écrit $|P| = p^t$ et va faire le raisonnement par récurrence sur t.
(Initialisation :) Pour $t = 1$ on a $r = s = 1$ et $\alpha_1 = \beta_1 = 1$ car $|P| = p^{\sum \alpha_i} = p^{\sum \beta_j}$.
(Hérédité :) Si $t > 1$ on suppose le résultat est vrai pour les p-groupe d'ordre p^u avec $u \leq (t-1)$. Les éléments de P qui sont d'ordre p forment un sous-groupe, qu'on note H_p. $x \in H_p$ s'écrit de manière unique

$$x = \sum_{1 \leq i \leq r} n_i x_i, \text{ avec } x_i \text{ générateur de } \mathbb{Z}/p^{\alpha_i}\mathbb{Z}, 0 \leq n_i \leq p^{\alpha_i}, 1 \leq i \leq r$$

Pour tout i, $1 < i \leq r$, on a $pn_i x_i = 0$, i.e. $p^{\alpha_i} | pn_i$, car $px = 0$ donc $n_i = m_i p^{(\alpha_i - 1)}$ et on a $0 \leq m_i < p$ car $0 \leq n_i < p^{\alpha_i}$.
Alors on a $H_p = \sum_{1 \leq i \leq r} m_i x_i$, $0 \leq m_i < p$ et donc $|H_p| = p^r$.
Avec le même raisonnement pour l'autre décomposition de P en somme directe on déduit $|H_p| = p^s$ et donc que $r = s$.
On considère

$$K_p = \{x \in P | \exists x' \in P, x = px'\}.$$

Un élément$x \in P$ appartient a K_p si et seulement s'il s'écrit $x = \sum_{1 \leq i \leq r} pn_i x_i$.
Alors

$$K_p = \sum_{1 \leq i \leq r} \langle px_i \rangle .$$

Un élément$x_i \in H_p$ si et seulement si $\alpha_i = 1$ donc on suppose que $\alpha_1 = \ldots = \alpha_h = 1$ et $1 < \alpha_{h+1} \leq \ldots \leq \alpha_r$. Alors

$$K_p = \bigoplus_{(h+1) \leq i \leq r} \langle px_i \rangle$$

et $|px_i| = p^{(\alpha_i - 1)}$.
Pour l'autre décomposition de P en somme directe on obtient

$$K_p = \bigoplus_{(h'+1) \leq j \leq r} \langle py_j \rangle$$

et $|py_j| = p^{(\beta_j - 1)}$.
Quand $\alpha_i = 0$ pour tout i, $K_p = o$ et donc $h' = r$ et $\beta_i = 1$ pour tout $1 \leq i \leq r$, d'où le résultat.
Pour $h < r$, le groupe K_p est d'ordre p^u, $1 \leq u < t$ car c'est un sous-groupe propre de P. On applique l'hypothèse de récurrence à K_p et on obtient $h' = h$ et $\alpha_i = \beta_i$ pour $(h+1) \leq i \leq r$ ce qui démontre le lemme. □

□

Démonstration. (du théorème 2.2ii)) Soit H le sous-groupe de G de base $(e_i)_{1\leq i\leq q}$. Il est clair que $H \subseteq H'$. Comme $a_1|\dots|a_q$, on a

$$H' = \{x \in G | \exists \lambda \in \mathbb{Z}, \lambda x \in H\}.$$

Donc H'/H est le sous-groupe de torsion de G/H et comme ça, H' est déterminé de manière unique et son rang q aussi.
D'autre part, on a

$$H'/H \cong \left(\bigoplus_{1\leq i\leq q} \mathbb{Z}e_i\right) / \left(\bigoplus_{1\leq i\leq q} \mathbb{Z}a_i e_i\right) \cong \bigoplus_{1\leq i\leq q} (\mathbb{Z}/a_i\mathbb{Z}).$$

L'unicité des éléments $(a_i)_{1\leq i\leq q}$ est donnée par le théorème 2.4. □

On appelle **décomposition canonique** la décomposition en somme directe d'un groupe abélien de type fini donnée par le théorème 2.4.

Définition 2.6. On appelle les éléments (a_i), $1 \leq i \leq q$ du théorème 2.2 les **facteurs invariants de H dans G**. Pour $H = G$ on les appelle les **facteurs invariants de G**.

Définition 2.7. Les entiers $d_{i,j} = p_j^{w_{i,j}}$ sont appelés les **diviseurs élémentaires** de G pour $1 \leq i \leq q$ et $1 \leq j \leq k$.

Définition 2.8. Soit G un groupe abélien fini. Si on écrit les diviseurs élémentaires de G dans l'ordre croissant, chacun d'entre eux étant écrit un nombre de fois égal au nombre de fois où il apparaît dans l'écriture des facteurs invariants de G, on obtient une suite finie de nombres entiers qui est appelée le **type** de G.

Exemple. Soit $G \cong \mathbb{Z}/20\mathbb{Z}\oplus\mathbb{Z}/30\mathbb{Z}$. On cherche la décomposition canonique de G, ça veut dire les facteurs invariants (les diviseurs élémentaires). On a

$$20 = 2^2 \cdot 5$$
$$30 = 2 \cdot 3 \cdot 5$$

donc G est de type $(2, 3, 2^2, 5, 5)$. Alors

$$G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

et en groupant les composantes c'est égal à

$$G \cong (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^2\mathbb{Z}) \oplus \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}).$$

Le nombre premier qui apparaît le plus grand nombre de fois dans le type est 2 ou 5 qui apparaissent deux fois, donc on sait qu'il y a deux facteurs invariants, a_1 et a_2. Maintenant, il y a deux possibilités pour la décomposition. La premiere est

$$G \cong \mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$$

avec $a_1 = 2 \cdot 3 \cdot 5 = 30$ et $a_2 = 4 \cdot 5 = 20$, mais 30 ne divise pas 20, donc on ce n'est pas la solution. Par conséquence, la décomposition canonique de G est

$$G \cong \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z}$$

avec $a_1 = 2 \cdot 5 = 10$ et $a_2 = 2^2 \cdot 3 \cdot 5 = 60$.

3 Forme normale de Smith

Dans ce chapitre, on va montrer, comment on peut calculer les facteurs invariants de H dans G (cf. théorème 2.2). On va regarder ce problème aussi dans un autre contexte et en faisant ça, on va aussi voir quand deux matrices sont équivalentes.
Pour pouvoir calculer effectivement les facteurs invariants du théorème de la base adaptée 2.2, on va utiliser des matrices : Si $y_1, \ldots, y_n$ est une base quelconque de G et $x_1, \ldots, x_m$ un système de générateurs de H, on note A la matrice dont la $j^{\text{ème}}$ colonne est formée des composantes de x_j dans la base $y_1 \ldots, y_n$, $1 \leq j \leq m$.
Inversement, si $A \in \mathbb{Z}$, note G_A le quotient de $\mathbb{Z}^m$ par le sous-groupe engendré par les colonnes de A (i.e. $\phi_A \in \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}^m), G_A = \mathrm{coker}\varphi_A = \mathbb{Z}^m/\mathrm{Im}\varphi_A$).

Rappel (Opérations élémentaires sur des matrices)**.** Une matrice $\in \mathbb{Z}^{m\times n}$ peut être vu comme un systeme de m vecteurs lignes ou un system de n vecteurs colonnes. On décrit les opérations élémentaires sur l'un ou l'autre en utilisant les letrres L pour les lignes, C pour les colonnes, suivies de l'indice :
$L_i \leftarrow kL_i$: multiplier la ligne i par k.
$L_i \leftarrow L_i + kL_j$: ajouter k fois la ligne j à la ligne i.
$L_i \leftarrow L_j$: échanger la ligne i avec la ligne j.
De même pour les colonnes.

Proposition 3.1. *Soit $A \in \mathbb{Z}^{m\times n}$. On peut , par des opérations élémentaires sur des matrices, ramener A à la forme*

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & a_q & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

où $a_1|a_2|\ldots|a_q$. Les a_i sont parfaitement déterminés : ce sont les facteurs invariants.

Définition 3.2. On dit que cette matrice est en **forme normale de Smith**.

Proposition 3.3. *Deux matrices à coefficients dans $\mathbb{Z}$ sont équivalentes si et seulement si elles ont même rang et mêmes facteurs invariants.*

Démonstration. "⇐" On suppose que $rg(A) = rg(B) = r$ et que $a_1 = b_1, \dots a_r = b_r$ où les a_i (resp. les b_i) sont les facteurs invariants de A (resp. B). D'après la proposition précédent 3.1,

$$A \sim \begin{pmatrix} a_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} \text{ et } B \sim \begin{pmatrix} b_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Comme $a_i = b_i$, $1 \leq i \leq r$,

$$\begin{pmatrix} a_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} b_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

donc $A \sim B$.

"⇒" On suppose que A et B sont équivalentes. Il existe alors des matrices inversibles U et V à coefficients dans $\mathbb{Z}$ telles que $B = UAV$. D'après la proposition 3.1

$$A \sim A' := \begin{pmatrix} a_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

et

$$B \sim B' := \begin{pmatrix} b_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & b_{q'} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

donc $B' \sim UA'V =: A''$.

Remarque. Une matrice $B \in \mathbb{Z}^{m\times n}$ est appelée forme normale de Smith de A, si B est en forme normale de Smith et équivalente à A.

D'après la remarque, B' est la forme normale de Smith de $A'' \sim A$ et A'' celle de $B' \sim B$. Donc $\mathrm{rg}(B) = q' = q = \mathrm{rg}(A)$ et $b_i = a_i$, $1 \le i \le q$. □

Algorithme pour la forme normale de Smith :
Entrée : Une matrice $A \in \mathbb{Z}^{m\times n}$.
Sortie : Une forme normale de Smith B de A.

(1) Poser $B := A$, écrire $B = (b_{i,j})$.
(2) Si $B = 0$, B est en forme normale de Smith, retourner B.
(3) Choisir $i \in \{1, \dots, m\}$ et $j \in \{1, \dots, n\}$ avec $b_{i,j} \neq 0$ tels que $|b_{i,j}|$ soit minimal.
(4) Changer la ligne i et la ligne 1 et la colonne j et la colonne 1 de façon que l'élément $\neq 0$ qui a la valeur absolue minimale devienne $b_{1,1}$.
(5) Si $b_{1,1} < 0$, multiplier la première ligne par -1. Après, $b_{1,1}$ est positif.
(6) Pour $j = 2, \dots n$ effectuer les étapes suivantes.
  (6i) Appliquer la division euclidienne :

$$b_{1,j} = b_{1,1} \cdot q + r$$

  avec $r \in \mathbb{Z}$ tel que $|r| < |b_{1,1}|$.
  (6ii) Soustraire q-fois la première colonne de la colonne j. Maintenant, $b_{1,j} = r$.
  (6iii) Si $b_{1,i} \neq 0$, aller au pas (3).
(7) Appliquer l'étape (6) aux lignes de B.
(8) Arrivé à cet étape, tous les coefficients de la première ligne et la première colonne sont égaux à 0, sauf $b_{1,1}$.
  Si $m = 1$ ou $n = 1$, B est en forme normale de Smith, retourner B.

(9) S'il existe $i, j > 1$ tels que $b_{1,1}$ ne divise pas $b_{i,j}$, additionner les lignes i et 1 et aller au pas (6). (Maintenant, une division euclidienne ne va pas être exacte.)

(10) Calculer une forme normale de Smith D' de $B' = (b_{i,j})_{i,j\geq 2} \in \mathbb{Z}^{(m-1)\times(n-1)}$ par un appel récursif.

(11) La matrice

$$\left(\begin{array}{c|ccc} b_{1,1} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & D' & \\ 0 & & & \end{array}\right) \in \mathbb{Z}^{m\times n}$$

est en forme normale de Smith, la retourner.

Exemple. On va maintenant utiliser cet algorithme pour calculer la forme normale de Smith de la matrice

$$A = \begin{pmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{pmatrix}$$

On va expliquer les premières pas explicitement et après, on va juste appliquer l'algorithme sans expliquation de chaque pas.
On pose $B := A$ et écrit $B = (b_{i,j})$. On cherche $i \in \{1, \dots m\}, j \in \{1, \dots, n\}$, $b_{i,j} \neq 0$ tel que $|b_{i,j}|$ soit minimal et on trouve $i = j = 1 : b_{1,1} = 9$, donc on peut sauter le pas (4) et, car $9 > 0$, aussi le pas (5). La division euclidienne donne $-36 = 9 \cdot (-4) + 0$, alors on soustrait -4-fois la première colonne de la deuxième et on obtient :

$$B = \begin{pmatrix} 9 & 0 & 30 \\ -36 & 48 & -180 \\ 30 & -60 & 180 \end{pmatrix}$$

Maintenant, on continue à suivre les instructions de l'algorithme :

$$B = \begin{pmatrix} 9 & 0 & 30 \\ -36 & 48 & -180 \\ 30 & -60 & 180 \end{pmatrix} \overset{30=9\cdot 3+3}{\longrightarrow} \begin{pmatrix} 9 & 0 & 3 \\ -36 & 48 & -72 \\ 30 & -60 & 90 \end{pmatrix} \overset{3<9}{\to} \begin{pmatrix} 3 & 0 & 9 \\ -72 & 48 & -36 \\ 90 & -60 & 30 \end{pmatrix}$$

$$\overset{9=3\cdot 3+0}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ -72 & 48 & 180 \\ 90 & -60 & -240 \end{pmatrix} \overset{-72=3\cdot(-24)+0}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 48 & 180 \\ 90 & -60 & -240 \end{pmatrix} \overset{90=3\cdot 30+0}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 48 & 180 \\ 0 & -60 & -240 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 48 & 180 \\ -60 & -240 \end{pmatrix} \overset{180=48\cdot 3+36}{\longrightarrow} \begin{pmatrix} 48 & 36 \\ -60 & -60 \end{pmatrix} \overset{36<48}{\to} \begin{pmatrix} 36 & 48 \\ -60 & -60 \end{pmatrix} \overset{48=36\cdot 1+12}{\longrightarrow} \begin{pmatrix} 36 & 12 \\ -60 & 0 \end{pmatrix}$$

$$\overset{12<36}{\to} \begin{pmatrix} 12 & 36 \\ 0 & -60 \end{pmatrix} \overset{36=12\cdot 3+0}{\longrightarrow} \begin{pmatrix} 12 & 0 \\ 0 & -60 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -60 \end{pmatrix} \overset{\cdot(-1)}{\to} \begin{pmatrix} 60 \end{pmatrix}$$

et l'algorithme termine et retourne

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 60 \end{pmatrix}$$

comme forme normale de Smith. On vérifie $3|12|60$.

4 Partitions

Définitions 4.1. Une séquence

$$\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r, \ldots)$$

(finie ou infinie) avec $0 \leq \lambda_i \in \mathbb{Z}$ et

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r \geq \ldots$$

qui ne contient qu'un nombre fini de termes $\neq 0$ est appelé une **partition**.
On ne distingue pas deux telles séquences qui ne diffèrent que d'une chaîne de zéros à la fin.
On appelle les $\lambda_i \neq 0$ les **parts** de λ. Le nombre de parts est la **longueur** de λ qu'on note $\ell(\lambda)$; et la somme des parts $\sum_i \lambda_i$ est le **poids** de λ, noté $|\lambda|$.
Si $|\lambda| = n$, on dit que λ est une **partitition de** n. On note $\mathscr{P}_n$ l'ensemble de toutes les partitions de n et $\mathscr{P}$ l'ensemble de toutes les partitions. En particulier, $\mathscr{P}_0$ est un singleton : $\mathscr{P}_0 = \{(0)\}$ où (0) est la partition unique de zéro.
Parfois on utilise la notation

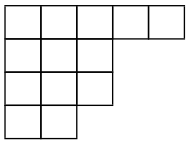
$$\lambda = (1^{m_1} 2^{m_2} \ldots r^{m_r} \ldots)$$

qui indique le nombre de fois où chaque entier apparaît comme part ; il y a m_i parts dans λ qui sont égal à i. On appelle m_i la **multiplicité** de i dans λ :

$$m_i = m_i(\lambda) = \text{card}\{j : \lambda_j = i\}.$$

Remarque. On peut représenter λ comme **diagramme de Young**, un arrangement des cases : Le diagramme de $\lambda = (\lambda_1, \lambda_2, \ldots)$ a λ_1 cases dans la première ligne, λ_2 dans la deuxième etc., qui sont toutes alignées à gauche. On utilise le même symbole pour la partition et le diagramme.

Exemple. Le diagramme de la partition $\lambda = (5332)$ est



Remarque. Si on remplit les cases du diagramme de Young avec des symboles d'un alphabet, on obtient un **tableau de Young**.

Définition 4.2. La **conjuguée** λ' de la partition λ est la partition dont le diagramme est le transposé du diagramme λ, i.e. λ' s'obtient par symétrie axiale par rapport à la diagonale principale. Donc λ'_i est égal au nombre de cases dans la colonne i de λ :

$$\lambda'_i = \text{card}\{j : \lambda_j \geq i\}.$$

En particulier, on a $\lambda'_1 = \ell(\lambda)$ et $\lambda_1 = \ell(\lambda')$ et clairement $\lambda'' = \lambda$.

Exemple. Soit $\lambda = (5332)$. Alors $\lambda' = (44311)$.

Remarque. On déduit de la définition de m_i et celle de λ'_i que

$$m_i(\lambda) = \lambda'_i - \lambda'_{i+1}.$$

Définition 4.3. Pour chaque partition λ, on définit

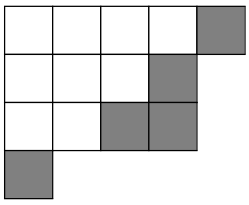
$$n(\lambda) = \sum_{i \geq 1} (i-1)\lambda_i,$$

de sorte que $n(\lambda)$ est la somme des nombres obtenus en ajoutant un zéro à chaque case dans la ligne la plus haute du diagramme de λ, un 1 à chaque case dans la deuxième ligne et ainsi de suite.

Remarque. Si λ, μ sont des partitions, on écrit $\lambda \supset \mu$ si le diagramme de λ contient celui de μ, i.e. si $\lambda_i \geq \mu_i$ pour tout $i \geq 1$.

Définition 4.4. La différence ensembliste (set-theoretic) $\theta = \lambda - \mu$ est appelé **"'skew diagram"'**.

Exemple. Soit $\lambda = (5441)$ et soit $\mu = (432)$, alors le "'skew diagram"' $\lambda - \mu$ est la partie en gris dans le diagramme ci-dessous :



Définitions 4.5. La **conjuguée** d'un "skew diagram" $\theta = \lambda - \mu$ est $\theta' = \lambda' - \mu'$. Soit $\theta_i = \lambda_i - \mu_i$, $\theta'_i = \lambda'_i - \mu'_i$ et

$$|\theta| = \sum \theta_i = |\lambda| - |\mu|.$$

Un "skew diagram" θ est une m-**bande horizontale** (resp. une m-**bande verticale**) si $|\theta| = m$ et $\theta'_i \leq 1$ (resp. $\theta_i \leq 1$) pour tout $i \geq 1$. Autrement dit, une bande horizontale (resp. verticale) a au plus une case dans chaque colonne (resp. ligne).

Définition 4.6. Soit L_n **l'ordre lexicographique inverse** sur l'ensemble $\mathscr{P}_n$: L_n est le sous-ensemble de $\mathscr{P}_n \times \mathscr{P}_n$ qui contient tous les (λ, μ) tels que soit $\lambda = \mu$, soit la première différence non nulle $\lambda_i - \mu_i$ est positive. L_n est un ordre total.

Exemple. Soit $n = 5$. L'ordre L_5 arrange $\mathscr{P}_5$ comme suit :

$$(5), (41), (32), (31^2), (2^21), (21^3), (1^5).$$

Remarque. Il existe un autre ordre total, L'_n, qui est l'ensemble de tous les (λ, μ) tels que soit $\lambda = \mu$, soit la première différence non nulle $\lambda^*_i - \mu^*_i$ est negative, où $\lambda^*_i = \lambda_{n+1-i}$. Pour $n \geq 6$, L_n et L'_n sont distincts.

Proposition 4.7. *Soient $\lambda, \mu \in \mathscr{P}_n$. Alors*

$$(\lambda, \mu) \in L'_n \Leftrightarrow (\mu', \lambda') \in L_n.$$

Démonstration. " $\Rightarrow$ " : On suppose que $(\lambda, \mu) \in L'_n$ et que $\lambda \neq \mu$. Donc il existe $i \geq 1$ tel que $\lambda_i < \mu_i$ et $\lambda_j = \mu_j$ pour $j > i$. Si on pose $k = \lambda_i$ et considère les diagrammes de λ et de μ on voit clairement que $\lambda'_j = \mu'_j$ pour $1 \leq j \leq k$ et que $\lambda'_{k+1} < \mu'_{k+1}$ donc $(\mu', \lambda') \in L_n$.
" $\Leftarrow$ " : Cette preuve se fait de façon similaire. □

Définition 4.8. On appelle N_n **l'ordre (partiel) de domination** sur $\mathscr{P}_n$. Il est défini comme suit :

$$(\lambda, \mu) \in N_n \Leftrightarrow \lambda_1 + \ldots + \lambda_i \geq \mu_1 + \ldots + \mu_i \quad \forall i \geq 1.$$

Pour $n \geq 6$, N_n n'est pas un ordre total.
On écrit $\lambda \geq \mu$ pour $(\lambda, \mu) \in N_n$.

Proposition 4.9. *Soient $\lambda, \mu \in \mathscr{P}$. Alors*

$$\lambda \geq \mu \Rightarrow (\lambda, \mu) \in L_n \cap L'_n.$$

Démonstration. On suppose que $\lambda \geq \mu$. Alors soit $\lambda_1 > \mu_1$ et donc $(\lambda, \mu) \in L_n$ soit $\lambda_1 = \mu_1$. Dans ce cas, soit $\lambda_2 > \mu_2$ et donc encore $(\lambda, \mu) \in L_n$, soit $\lambda_2 = \mu_2$. Si on continue comme ça, on s'assure que $(\lambda, \mu) \in L_n$.
Pour tout $i \geq 1$ on a également

$$\lambda_{i+1} + \lambda_{i+2} + \ldots = n - (\lambda_1 + \ldots + \lambda_i) \leq n - (\mu_1 + \ldots + \mu_i) = \mu_{i+1} + \mu_{i+2} + \ldots$$

Donc le même raisonnement montre que $(\lambda, \mu) \in L'_n$. □

Exemple. En général, $N_n \neq L_n \cap L'_n$: Soit $n = 12$, $\lambda = (63^2)$ et $\mu = (5^2 1^2)$. Alors $(\lambda, \mu) \in L_{12} \cap L'_{12}$, mais $(\lambda, \mu) \notin N_{12}$.

Proposition 4.10. *Soient $\lambda, \mu \in \mathscr{P}_n$. Alors*

$$\lambda \geq \mu \Leftrightarrow \mu' \geq \lambda'.$$

Démonstration. Il suffit de montrer une direction.

" $\Rightarrow$ " : On va faire une démonstration par contraposition : On suppose que $\mu' \not\geq \lambda'$. Alors on trouve $i \geq 1$ tel que

$$\lambda'_1 + \ldots + \lambda'_j \leq \mu'_1 + \ldots + \mu'_j \quad (1 \leq j \leq i-1)$$

et

$$\lambda'_1 + \ldots + \lambda'_i > \mu'_1 + \ldots + \mu'_i \tag{4.1}$$

d'où $\lambda'_i > \mu'_i$.
Soit $l = \lambda'_i$, $m = \mu'_i$. L'inégalité (4.1) implique

$$\lambda'_{i+1} + \lambda'_{i+2} + \ldots < \mu'_{i+1} + \mu'_{i+2} + \ldots \tag{4.2}$$

Maintenant, $\lambda'_{i+1} + \lambda'_{i+2} + \ldots$ est égal au nombre de cases dans le diagramme de λ qui sont situé à droite de la colonne i, donc

$$\lambda'_{i+1} + \lambda'_{i+2} + \ldots = \sum_{j=1}^{\ell} (\lambda_j - i).$$

De même

$$\mu'_{i+1} + \mu'_{i+2} + \ldots = \sum_{j=1}^{m} (\mu_j - i).$$

Alors on déduit de l'inégalité (6.4) que

$$\sum_{j=1}^{m} (\mu_j - i) > \sum_{j=1}^{\ell} (\lambda_j - i) \geq \sum_{j=1}^{m} (\lambda_j - i). \tag{4.3}$$

Ici, l'inégalité à droite est vrai car $l > m$ et $\lambda_j \geq i$ pour $1 \leq j \leq l$. Enfin, (4.3) donne

$$\mu_1 + \ldots + \mu_m > \lambda_1 + \ldots + \lambda_m$$

et conséquemment $\lambda \not\geq \mu$. □

Exemple. L'ensemble $\mathcal{P}_n$ des partitions de n est un treillis (lattice) en ce qui concerne l'ordre de domination. Autrement dit, chaque paire λ, μ de partitions de n a une borne supérieure $\sigma = \sup(\lambda, \mu)$ et une borne inférieure $\tau = \inf(\lambda, \mu)$.

5 Fonctions symétriques

5.1 L'anneau des fonctions symétriques

Définition 5.1. Soient n un entier et $\mathbb{Z}[x_1, \ldots, x_n]$ l'anneau des polynômes en n indéterminées $x_1, \ldots, x_n$ à coefficients dans $\mathbb{Z}$. Le groupe symétrique $\mathfrak{S}_n$ agit sur cet anneau en permutant les variables. On dit qu'un polynôme est **symétrique** s'il est invariant sous l'action de $\mathfrak{S}_n$. Les polynômes symétriques forment un sous-anneau

$$\Lambda_n = \mathbb{Z}[x_1, \ldots, x_n]^{\mathfrak{S}_n}.$$

Remarque. L'annneau Λ_n est un anneau gradué :

$$\Lambda_n = \bigoplus_{k \geq 0} \Lambda_n^k$$

où Λ_n^k se compose des polynômes symétriques homogènes de degré k avec le polynôme nul.

Pour tout $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ on note x^α le monôme

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

Soit λ une partition quelconque de longueur $\leq n$. Le polynôme

$$m_\lambda(x_1, \ldots, x_n) = \sum x^\alpha$$

qui est sommé sur toutes les permutations distinctes α de $\lambda = (\lambda_1, \ldots, \lambda_n)$, est symétrique et les m_λ forment une $\mathbb{Z}$-base de Λ_n. Ainsi, les m_λ tels que $\ell(\lambda) \leq n$ et $|\lambda| = k$ forment une $\mathbb{Z}$-base de Λ_n^k ; en particulier, dès que $n \geq k$, les m_λ avec $|\lambda| = k$ forment une $\mathbb{Z}$-base de Λ_n^k.

Définition 5.2. Les polynômes m_λ sont appelés les **fonctions monomiales symétriques**.

Exemple. Pour $n = 3$, on a :

$$m_{(1,1)} = x_1x_2 + x_1x_3 + x_2x_3,$$
$$m_{(2,0)} = x_1^2 + x_2^2 + x_3^2.$$

Après avoir travaillé avec n variables, on veut généraliser maintenant. Dans la théorie des fonctions symétriques, le nombre des variables est insignifiant en général, à condition qu'il soit assez grand. Souvent c'est plus pratique de

travailler avec un nombre infini de variables.
Soit $m \geq n$. On considère l'homomorphisme

$$\mathbb{Z}[x_1, \ldots, x_m] \to \mathbb{Z}[x_1, \ldots, x_n]$$

qui envoie x_i sur x_i pour $i \leq n$ et sur zéro pour $n+1 \leq i \leq m$.
Si on le restreint à Λ_m, on a un homomorphisme

$$\rho_{m,n} : \Lambda_m \to \Lambda_n$$

qui envoie $m_\lambda(x_1, \ldots, x_m)$ sur $m_\lambda(x_1, \ldots, x_n)$ si $\ell(\lambda) \leq n$ et sur zéro si $\ell(\lambda) > n$. Alors, $\rho_{m,n}$ est surjectif.
Par restriction sur Λ_m^k on a des homomorphismes

$$\rho_{m,n}^k : \Lambda_m^k \to \Lambda_n^k$$

pour tout $k \geq 0$ et $m \geq n$. Ces homomorphismes sont toujours surjectifs et bijectifs pour $m \geq n \geq k$ (car les m_λ avec $|\lambda| = k$ forment une $\mathbb{Z}$-base de Λ_n^k dès que $n \geq k$).
Maintenant, on forme la limite projective

$$\Lambda^k = \varprojlim_n \Lambda_n^k$$

des $\mathbb{Z}$-modules Λ_n^k par rapport aux homomorphismes $\rho_{m,n}^k$: un élement de Λ^k est par définition une suite $f = (f_n)_{n \geq 0}$, où chaque $f_n = f_n(x_1, \ldots, x_n)$ est un polynôme symétrique homogène de degré k en $x_1, \ldots, x_n$ avec $f_m(x_1, \ldots, x_n, 0, \ldots, 0) = f_n(x_1, \ldots, x_n)$ à tout moment où $m \geq n$. Comme $\rho_{m,n}^k$ est un isomorphisme pour $m \geq n \geq k$, la projection

$$\rho_n^k : \Lambda^k \to \Lambda_n^k$$

qui envoie f sur f_n, est aussi un isomorphisme pour tout $n \geq k$. En conséquence, Λ^k a une $\mathbb{Z}$-base qui se compose des m_λ (pour toutes les partitions λ de k) défini par

$$\rho_n^k(m_\lambda) = m_\lambda(x_1, \ldots, x_n)$$

pour tout $n \geq k$. Alors Λ^k est un $\mathbb{Z}$-module libre de rang $p(k)$, où $p(k)$ est le nombre des partitions de k.
Soit

$$\Lambda = \bigoplus_{k \geq 0} \Lambda^k.$$

Comme ça, Λ est un $\mathbb{Z}$-module libre et engendré par les m_λ pour *toutes* les partitions λ.
On a des homomorphismes surjectifs

$$\rho_n = \bigoplus_{k\geq 0} \rho_n^k : \Lambda \to \Lambda_n$$

pour tout $n \geq 0$. Pour $k \leq n$, ρ_n est un isomorphisme.
L'anneau Λ a la structure d'un anneau gradué, les ρ_n sont des homormophismes d'anneaux.

Définition 5.3. L'anneau gradué Λ comme défini ci-dessus est appelé **l'anneau des fonctions symétriques** en un nombre dénombrable des variables indépendantes $x_1, x_2, \ldots$

Remarque. On peut remplacer $\mathbb{Z}$ par un anneau commutatif A quelconque ; au lieu de Λ, on obtient $\Lambda_A \cong \Lambda \otimes_{\mathbb{Z}} A$.

5.2 Fonctions symétriques élémentaires et complètes

Définition 5.4. La r-ième **fonction symétrique élémentaire** e_r est, pour tout entier $r \geq 0$, la somme de tous les produits de r variables distinctes x_i telle que $e_0 = 1$ et

$$e_r = \sum_{i_1<i_2<\ldots<i_r} x_{i_1} x_{i_2} \cdots x_{i_r} = m_{(1^r)}$$

pour $r \geq 1$.

La fonction génératrice des e_r est

$$E(t) = \sum_{r\geq 0} e_r t^r = \prod_{i\geq 1} (1 + x_i t) \tag{5.1}$$

Remarque. Si le nombre des variables est fini, disons n, alors $e_r = 0$ pour tout $r \geq n$ et la fonction génératrice (5.1) est de la forme

$$\sum_{r=0}^{n} e_r t^r = \prod_{i=1}^{n} (1 + x_i t).$$

Les deux côtés sont des éléments de $\Lambda_n[t]$.

On définit

$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots$$

pour chaque partition $\lambda = (\lambda_1, \lambda_2, \ldots)$.

Exemple. Pour $n = 3$, on a :

$$e_{(1,1)} = (x_1 + x_2 + x_3)^2,$$
$$e_{(2,0)} = x_1x_2 + x_1x_3 + x_2x_3.$$

Proposition 5.5. *Soient λ une partition et λ' sa conjuguée. Alors*

$$e_{\lambda'} = m_\lambda + \sum_\mu a_{\lambda\mu} m_\mu$$

où les $a_{\lambda\mu}$ sont des entiers positifs ou nuls et la somme porte sur les partitions $\mu < \lambda$ dans l'ordre de domination.

Démonstration. Si on développe le produit $e_{\lambda'} = e_{\lambda'_1} e_{\lambda'_2} \cdots$, on obtient une somme de monômes qui sont tous de la forme

$$(x_{i_1} x_{i_2} \ldots)(x_{j_1} x_{j_2} \ldots) \ldots = x^\alpha,$$

où $i_1 < i_2 < \ldots < i_{\lambda'_1}$, $j_1 < j_2 < \ldots < j_{\lambda'_2}$ etc.
Imaginons le diagramme de λ. Si on inscrit les nombres $i_1, i_2, \ldots, i_{\lambda'_1}$ dans la première colonne, dans l'ordre et vers le bas et les nombres $j_1, j_2, \ldots, j_{\lambda'_2}$ dans la deuxième colonne, aussi dans l'ordre et vers le bas et ainsi de suite, il est clair que tous les symboles $\leq r$ pour $r \geq 1$ doivent se trouver dans les r lignes les plus hautes. Donc $\alpha_1 + \ldots + \alpha_r \leq \lambda_1 + \ldots + \lambda_r$ pour tout $r \geq 1$, i.e. $\alpha \leq \lambda$.

Pour pouvoir terminer la preuve, on a besoin d'un petit aparté :
Dans ce passage, on ne travaille pas avec des partitions mais avec des vecteurs entiers $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$. Le groupe symétrique $\mathfrak{S}_n$ agit sur $\mathbb{Z}^n$ en permutant les coordonnées, et l'ensemble

$$P_n = \{b \in \mathbb{Z}^n | b_1 \geq b_2 \geq \ldots \geq b_n\}$$

est un domaine fondamental pour cette action, i.e. l'orbite de chaque $a \in \mathbb{Z}^n$ sous $\mathfrak{S}_n$ rencontre P_n en exactement un point, qu'on note a^+. Ainsi a^+ est obtenu en réarrangant les $a_1, \ldots, a_n$ en ordre décroissant de la magnitude.
Pour $a, b \in \mathbb{Z}^n$, on définit $a \geq b$ comme avant :

$$a_1 + \ldots + a_i \geq b_1 + \ldots + b_i \quad (1 \leq i \leq n).$$

Lemme 5.6. *Soit $a \in \mathbb{Z}^n$. Alors*

$$a \in P_n \Leftrightarrow a \geq wa \quad \textit{pour tout } w \in \mathfrak{S}_n.$$

Démonstration. On suppose que $a \in P_n$, i.e. $a_1 \geq \ldots \geq a_n$. Si $wa = b$, alors $(b_1, \ldots, b_n)$ est une permutation de $(a_1, \ldots, a_n)$, et donc

$$a_1 + \ldots + a_i \geq b_1 + \ldots + b_i \quad (1 \leq i \leq n),$$

alors $a \geq b$.
Réciproquement, si $a \geq wa$ pour tout $w \in \mathfrak{S}_n$ on a en particulier

$$(a_1, \ldots, a_n) \geq (a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n)$$

pour $1 \leq i \leq n-1$, ce qui implique

$$a_1 + \ldots + a_{i-1} + a_i \geq a_1 + \ldots + a_{i-1} + a_{i+1},$$

i.e. $a_i \geq a_{i+1}$. Par conséquent $a \in P_n$. □

Par la proposition ci-dessus 5.6, il vient :

$$e_{\lambda'} = \sum_{\mu \geq \lambda} a_{\lambda\mu} m_\mu$$

avec $a_{\lambda\mu} \geq 0$ pour tout $\mu \geq \lambda$, et l'argument ci-dessus de l'aparté montre aussi que le monôme x^λ apparaît exactement une fois, de sorte que $a_{\lambda\lambda} = 1$. □

Proposition 5.7. *On a*

$$\Lambda = \mathbb{Z}[e_1, e_2, \ldots]$$

et les e_r sont algébriquement indépendants sur $\mathbb{Z}$.

Démonstration. On sait que les m_λ forment une $\mathbb{Z}$-base de Λ et la proposition 5.5 montre que les e_λ forment une autre $\mathbb{Z}$-base. Autrement dit, chaque élément de Λ peut s'exprimer comme polynôme en $e_1, e_2, \ldots, e_r, \ldots$ d'une manière unique. □

Définition 5.8. Pour tout $r \geq 0$, la r-ième **fonction symétrique complète** h_r est la somme de tous les monômes en $x_1, x_2, \ldots$ de degré total r telle que

$$h_r = \sum_{|\lambda|=r} m_\lambda.$$

En particulier, $h_0 = 1$ et $h_1 = e_1$. Pour $r < 0$, on définit $h_r = e_r = 0$.
La fonction génératrice des h_r est

$$H(t) = \sum_{r \geq 0} h_r t^r = \prod_{i \geq 1} (1 - x_i t)^{-1}. \tag{5.2}$$

Corollaire 5.9. *Les fonctions génératrices (5.1) et (5.2) donnent*

$$H(t)E(-t) = 1$$

ce qui est équivalent à

$$\sum_{r=0}^{n}(-1)^r e_r h_{n-r} = 0 \tag{5.3}$$

pour tout $n \geq 1$. C'est une trace de la ***dualité de Koszul****.*

Comme les e_r sont algébriquement indépendants d'après la proposition 5.7, on peut définir un homomorphisme d'anneau gradué

$$\omega : \Lambda \to \Lambda$$

par

$$\omega(e_r) = h_r$$

pour tout $r \geq 0$. La symétrie des relations (5.3) entre les e_r et les h_r montre le corollaire suivant.

Corollaire 5.10. *Le morphisme ω est une involution, i.e. ω^2 est l'application identité.*

Cela implique que ω est une automorphisme de Λ. Alors la proposition 5.7 implique la proposition suivante.

Proposition 5.11. *On a :*

$$\Lambda = \mathbb{Z}[h_1, h_2, \ldots]$$

et les h_r sont algébriquement indépendants sur $\mathbb{Z}$.

On définit

$$h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots$$

pour chaque partition $\lambda = (\lambda_1, \lambda_2, \ldots)$.

Exemple. Pour $n = 3$, on a :

$$h_{(1,1)} = (x_1 + x_2 + x_3)^2,$$
$$h_{(2,0)} = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3.$$

D'après la proposition 5.11, les h_λ forment une $\mathbb{Z}$-base de Λ. Maintenant, on a trois $\mathbb{Z}$-bases de Λ : les m_λ, les e_λ et les h_λ. Si on définit

$$f_\lambda = \omega(m_\lambda)$$

pour toute partition λ, les f_λ forment une quatrième $\mathbb{Z}$-base de Λ. (On appelle les f_λ les fonctions symétriques "oubliées".)

Exemple. Soit $x_i = q^{i-1}$ pour $1 \leq i \leq n$, et $x_i = 0$ pour $i > n$, où q est une indéterminée. Alors

$$E(t) = \prod_{i=0}^{n-1}(1+q^i t) = \sum_{r=0}^{n} q^{r(r-1)/2} \begin{bmatrix} n \\ r \end{bmatrix} t^r$$

où $\begin{bmatrix} n \\ r \end{bmatrix}$ désigne le polynôme de Gauß

$$\begin{bmatrix} n \\ r \end{bmatrix} = \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-r+1})}{(1-q)(1-q^2)\cdots(1-q^r)},$$

et

$$H(t) = \prod_{i=0}^{n-1}(1-q^i t)^{-1} = \sum_{r=0}^{\infty} \begin{bmatrix} n+r-1 \\ r \end{bmatrix} t^r.$$

5.3 Fonctions de Schur

Rappel. Pour la partition $\delta = (k-1, k-2, \ldots, 0)$, on a le **déterminant de Vandermonde**

$$a_\delta(x_1, x_2, \ldots, x_k) = \prod_{1 \leq i < j \leq k} (x_i - x_j).$$

Définition 5.12. Il existe une cinquième base, la plus importante peut-être, qu'on va définir maintenant. Ce sont les **fonctions de Schur** définies comme suit :

$$s_\lambda = \frac{|x_j^{\lambda_i+k-i}|}{|x_j^{k-i}|} = \frac{|x_j^{\lambda_i+k-i}|}{\Delta}, \tag{5.4}$$

où $\Delta = \prod_{i<j}(x_i - x_j)$ est le discriminant et $|a_{i,j}|$ désigne le déterminant d'une matrice $(a_{i,j})$ de taille $k \times k$.

Remarque. On a aussi que $s_\lambda = \frac{a_{\lambda+\delta}}{a_\delta}$.

Exemple. Pour $n = 3$, on a :

$$s_{(1,1)} = x_1x_2 + x_1x_3 + x_2x_3,$$
$$s_{(2,0)} = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3.$$

Pour commencer, on va décrire quelque relations entre tous ces fonctions symétriques qu'on a rencontré dans ce chapitre jusqu'ici. L'exemple suivant est facile à voir.

Exemple. On a :

$$\begin{aligned} s_{(1,1)} &= e_{(2,0)} = h_1^2 - h_2, \\ s_{(2,0)} &= h_{(2,0)} = e_1^2 - e_2, \\ s_{(1,0)} \cdot s_{(1,0)} &= s_{(1,1)} + s_{(2,0)}. \end{aligned}$$

Ce sont des cas spéciaux de trois formules importantes comportant les fonctions de Schur. Les deux premières sont connues sous le nom **"determinantal formulas"**. La première est aussi appelée **l'identité de Jacobi-Trudy**. En géométrie, les deux premiers apparaissent sous le nom de **formules de Giambelli** et la troisième de **formule de Pieri**.
On a

$$s_\lambda = |h_{\lambda_i+j-i}| = \begin{vmatrix} h_{\lambda_1} & h_{\lambda_1+1} & \dots & h_{\lambda_1+k-1} \\ h_{\lambda_2-1} & h_{\lambda_2} & \dots & \\ \vdots & & & \\ h_{\lambda_k-k+1} & \dots & & h_{\lambda_k} \end{vmatrix}.$$

La deuxième :

$$s_\lambda = |e_{\mu_i+j-i}| = \begin{vmatrix} e_{\mu_1} & e_{\mu_1+1} & \dots & e_{\mu_1+l-1} \\ e_{\mu_2-1} & e_{\mu_2} & \dots & \\ \vdots & & & \\ e_{\mu_1-l+1} & \dots & & e_{\mu_l} \end{vmatrix}.$$

Démonstration. cf. [1, p. 462] □

Proposition 5.13 (formule de Pieri)**.** *La troisième formule, la formule de Pieri, explique comment on peut multiplier une fonction de Schur s_λ avec une fonction de Schur élémentaire $s_{(m)} = h_m$:*

$$s_\lambda s_{(m)} = \sum_\nu s_\nu, \tag{5.5}$$

la somme porte sur tous les ν dont le diagramme de Young peut être obtenu de celui de λ en ajoutant m cases aux lignes, mais sans ajouter deux cases à la même colonne, i.e. les $\nu = (\nu_1, \dots, \nu_k)$ avec

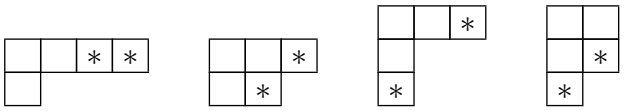
$$\nu_1 \geq \lambda_1 \geq \nu_2 \geq \lambda_2 \geq \dots \geq \nu_k \geq \lambda_k \geq 0,$$

et $\sum \nu_j = \sum \lambda_j + m = d + m$. (La somme porte sur tous les ν de sorte que $\nu - \lambda$ est une m-bande horizontale.)

Exemple. On a :

$$s_{(2,1)} \cdot s_{(2)} = s_{(4,1)} + s_{(3,2)} + s_{(3,1,1)} + s_{(2,2,1)}$$

comme on peut voir par les diagrammes



En applicant l'involution ω (corollaire 5.10) à (5.5), on obtient

$$s_\lambda e_m = \sum_\nu s_\nu \tag{5.5a}$$

où la somme porte sur tous les ν de sorte que $\nu - \lambda$ est une $m-$bande verticale.

Démonstration. On considère (pour un ensemble fini de variables $x_1, \ldots, x_k$) le produit

$$a_{\lambda+\delta} e_m = \sum_{w \in \mathfrak{S}_k} \epsilon(w) x^{w(\lambda+\delta)} \sum_\alpha x^\alpha = \sum_\alpha a_{\lambda+\alpha+\delta}$$

où la somme porte sur tous les $\alpha \in \mathbb{Z}^k$ tels que $\alpha_i = 0$ ou 1, et $\sum \alpha_i = m$. Pour un tel α, la suite

$$\lambda + \alpha + \delta = (\lambda_1 + \alpha_1 + k - 1, \lambda_2 + \alpha_2 + k - 2, \ldots, \lambda_k + \alpha_k)$$

est en ordre descendant, donc on doit seulement retirer les α pour lesquels deux termes consécutifs sont égaux. Il reste les α pour lesquels $\nu = \lambda + \alpha$ est une partition, i.e. de sorte que $\nu - \lambda$ est une m-bande verticale. Cela prouve (5.5a) et aussi (5.5) par dualité. □

On peut multiplier deux fonctions de Schur quelconques en utilisant la formule de Pieri, mais il existe une formule plus directe qui généralise la formule de Pieri. C'est la **règle de Littlewood-Richardson** :

$$s_\lambda \cdot s_\mu = \sum c^\lambda_{\mu\nu} s_\nu.$$

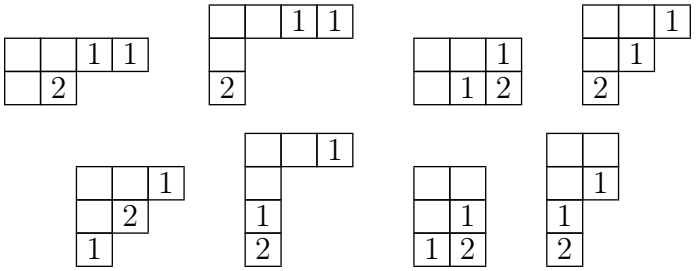
λ est une partition de d, μ une partition de m et la somme porte sur toutes les partitions ν de $d+m$ (chacune avec k parts au maximum). Les $c^\lambda_{\mu\nu}$ sont appelés les **nombres** ou **coefficients de Littlewood-Richardson**. La règle dit que $c^\lambda_{\mu\nu}$ est le nombre des possibilités de transformer le diagramme de Young de λ en le diagramme de Young de ν en n'utilisant que des μ-expansions.
Si $\mu = (\mu_1, \ldots, \mu_k)$, une μ-**expansion** d'un diagramme de Young est obtenu en ajoutant premièrement μ_1 cases, selon la description de la formule de Pieri

ci-dessus, et en inscrivant des entiers 1 dans chacune de ces cases ; puis en ajoutant μ_2 cases avec un 2 de la même façon, en continuant jusqu'à ce que finalement μ_k cases ont été ajoutées avec l'entier k.
On dit que l'expansion est **stricte** si, quand les entiers dans les cases sont listés de droite à gauche, en commencant par la ligne la plus haute, puis en descendant, et on regarde les t premiers coefficients ($1 \leq t \leq \mu_1 + \ldots + \mu_k$) dans cette liste, chaque entier p entre 1 et $k-1$ apparaît au moins autant de fois que l'entier suivant $p+1$.

Exemple. On peut voir l'équation

$$s_{(2,1)} \cdot s_{(2,1)} = s_{(4,2)} + s_{(4,1,1)} + s_{(3,3)} + 2s_{(3,2,1)} + s_{(3,1,1,1)} + s_{(2,2,2)} + s_{(2,2,1,1)}$$

en listant les $(2,1)$-expansions strictes du diagramme de Young  :



Appliquer la formule (5.5) inductivement à $h_\lambda = h_{\lambda_1} \cdots h_{\lambda_k} = s_{(\lambda_1)} \cdots s_{(\lambda_k)}$ donne :

Proposition 5.14. *Pour λ partition,*

$$h_\lambda = \sum k_{\mu\lambda} s_\mu, \tag{5.6}$$

où $k_{\mu\lambda}$ est le nombre de possibilités de remplir les cases du diagramme de Young de μ avec λ_1 fois 1, λ_2 fois 2 jusqu'à λ_k fois k, de telle façon que les entrées de chaque ligne sont non-décroissantes et les entrées de chaque colonne sont strictement croissantes.

Définitions 5.15. Un tel diagramme, comme décrit dans la proposition 5.14, est appelé **tableau semi-standard sur μ de type λ**.
Les entiers $k_{\mu\lambda}$ sont positifs ou nuls avec

$$k_{\lambda\lambda} = 1 \quad \text{et} \quad k_{\mu\lambda} = 0 \quad \text{si} \quad \lambda > \mu$$

i.e. la première différence $\lambda_i - \mu_i$ qui est non nulle, est positive. De plus, $k_{\mu\lambda} = 0$ si λ a plus de termes non nuls que μ.
Les entiers $k_{\mu\lambda}$ sont appelés **nombres de Kostka**.

Exemple. Soit $\mu = (3,2)$ et $\lambda = (1,1,2,1)$. Il y a trois tableaux semi-standard de forme μ et de poids λ, donc $k_{(3,2)(1,1,2,1)} = 3$.

1	3	3
2	4	

1	2	3
3	4	

1	2	4
3	3	

Remarque. Si $\lambda = (1,1,\ldots,1)$, $k_{\mu(1,\ldots,1)}$ est le nombre des tableaux standards sur le diagramme de μ.

Définition 5.16. Un **tableau standard** est un tableau de Young où les coefficients sont les entiers de 1 jusqu'au nombre total de cases, distincts deux à deux et strictement croissants dans les lignes et dans les colonnes.

Soient k un entier et $x_1,\ldots,x_k$ et $y_1,\ldots,y_k$ deux ensembles d'indéterminées. On va voir maintenant une autre formule impliquant les fonctions de Schur qui vient d'une identité de Cauchy :

Lemme 5.17.

$$\det\left|\frac{1}{1-x_iy_j}\right| = \frac{\Delta(x)\Delta(y)}{\prod_{i,j}(1-x_iy_j)}. \tag{5.7}$$

Démonstration. On va faire la preuve par récurrence sur k. Pour calculer le déterminant, on commence par soustraire la première ligne de toutes les autres lignes, en notant que

$$\frac{1}{1-x_iy_j} - \frac{1}{1-x_1y_j} = \frac{x_i-x_1}{1-x_1y_j}\cdot\frac{y_j}{1-x_iy_j}.$$

Dans chaque ligne, on factorise $x_i - x_1$ pour $i \geq 2$ et dans chaque colonne, on factorise $\frac{1}{1-x_1y_j}$ pour $j = 1$ à n. On obtient la matrice

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \frac{y_1}{1-x_2y_1} & \frac{y_2}{1-x_2y_2} & \ldots & \frac{y_k}{1-x_2y_k} \\ \vdots & \vdots & & \vdots \\ \frac{y_1}{1-x_ky_1} & \frac{y_2}{1-x_ky_2} & \ldots & \frac{y_k}{1-x_ky_k}. \end{vmatrix}.$$

On continue en soustrayant la première colonne de toutes les autres colonnes. Cette fois, on utilise l'équation suivante pour exclure les facteurs communs :

$$\frac{y_j}{1-x_iy_j} - \frac{y_1}{1-x_iy_1} = \frac{y_j-y_1}{1-x_iy_1}\cdot\frac{1}{1-x_iy_j}.$$

Dans chaque colonne, on factorise $y_j - y_1$ pour $j \geq 2$ et dans chaque ligne, on factorise $\frac{1}{1-x_iy_1}$ pour $i \geq 2$. Maintenant on a une matrice dont la première

ligne est égale à $(1, 0, \ldots, 0)$ et dont le carré inférieur à droite se compose encore des coefficients initiaux. Donc on a

$$\Delta_k = \Delta_{k-1} \cdot \frac{\prod_{j\geq 2}(y_j - y_1)}{\prod_{i\geq 2}(1 - x_i y_1)} \cdot \frac{\prod_{i\geq 2}(x_i - x_1)}{\prod_{j=1}^{n}(1 - x_1 y_j)}.$$

La formule s'ensuit par induction (cf. [5, p. 202]). □

Voici une autre forme de l'identité de Cauchy :

Corollaire 5.18.

$$\frac{1}{\prod_{i,j}(1 - x_i y_j)} = \sum_{\lambda} s_\lambda(x) s_\lambda(y), \tag{5.8}$$

la somme porte sur toutes les partitions λ avec k termes au maximum.

Démonstration. On développe le déterminant dont le coefficient i, j est égal à $(1 - x_i y_j)^{-1} = 1 + x_i y_j + x_i^2 y_j^2 + \ldots$. On voit que pour tout $l_1 > \ldots > l_k$, le coefficient de $y_1^{l_1} y_2^{l_2} \cdots y_k^{l_k}$ est égal au déterminant $|x_j^{l_i}|$. Par symétrie des variables x et y, on a

$$\det \left| \frac{1}{1 - x_i y_j} \right| = \sum_{l} |x_j^{l_i}| \cdot |y_j^{l_i}|.$$

La combinaison de cette équation avec (5.4) donne (5.8). □

Le développement du membre gauche de 5.8 donne :

$$\frac{1}{\prod_{i,j}(1 - x_i y_j)} = \prod_{j} \left(\sum_{m=0}^{\infty} h_m(x) y_j^m \right) = \sum_{\lambda} h_\lambda(x) m_\lambda(y). \tag{5.9}$$

Définition 5.19. Puisque les fonctions h_λ ainsi que les m_λ forment une base des fonctions symétriques, on peut définir une **forme bilinéaire** $\langle\ ,\ \rangle$ sur l'espace des fonctions symétriques homogènes de degré d en k indéterminées, en exigant que

$$\langle h_\lambda, m_\mu \rangle = \delta_{\lambda,\mu},$$

où $\delta_{\lambda,\mu}$ est le symbole de Kronecker, i.e. $\delta_{\lambda,\mu}$ est égal à 1 si $\lambda = \mu$ et à 0 sinon.

Proposition 5.20. *Les fonctions de Schur forment une base orthonormée pour*

$$\langle s_\lambda, s_\mu \rangle = \delta_{\lambda,\mu}. \tag{5.10}$$

En particulier, ceci implique que $\langle\ ,\ \rangle$ est symétrique.

Démonstration. On peut déduire l'équation (5.10) facilement des équations précédentes comme suit : On écrit $s_\lambda = \sum a_{\lambda\gamma} h_\gamma = \sum b_{\gamma\lambda} m_\gamma$ avec $(a_{\lambda\gamma})$ et $(b_{\gamma\lambda})$ des matrices à coefficients entiers. Alors

$$\langle s_\lambda, s_\mu \rangle = \sum_\gamma a_{\lambda\gamma} b_{\gamma\mu}. \tag{5.11}$$

Afin que

$$\sum_\lambda s_\lambda(x) s_\lambda(y) = \sum_{\lambda,\gamma,\rho} a_{\lambda\gamma} h_\gamma(x) b_{\rho\lambda} m_\rho(y)$$

soit égal à $\sum_\gamma h_\gamma(x) m_\gamma(y)$, ce que l'on sait par (5.8) et (5.9), on doit avoir

$$\sum_\lambda b_{\rho\lambda} a_{\lambda\gamma} = \delta_{\rho,\gamma}.$$

Ceci est équivalent à l'équation $\sum_\gamma a_{\lambda\gamma} b_{\gamma\mu} = \delta_{\lambda,\mu}$, ce qui implique (5.10) par (5.11). □

Corollaire 5.21. *À cause de cette dualité, la formule (5.6) est équivalente à*

$$s_\mu = \sum_\lambda k_{\mu\lambda} m_\lambda,$$

ce qui nous donne une autre formule pour les nombres de Kostka : $k_{\mu\lambda}$ est le coefficient de x^λ dans s_λ où $x^\lambda = x_1^{\lambda_1} \cdots x_k^{\lambda_k}$.

6 Polynômes de Hall

6.1 $\mathfrak{o}$-modules finis

Soit $\mathfrak{o}$ un anneau (commutatif) de valuation discrète , $\mathfrak{p}$ son idéal maximal et $k = \mathfrak{o}/\mathfrak{p}$ le corps résiduel. Pour le moment, ce n'est pas nécessaire que k soit un corps fini, mais plus tard on va l'exiger. On va s'intéresser aux $\mathfrak{o}$-modules **finis** M, c'est-à-dire des modules M qui possèdent une suite de composition finie, ou de manière équivalente des $\mathfrak{o}$-modules M de type fini tels que $\mathfrak{p}^r M = 0$ pour un $r \geq 0$. Si k est un corps fini, alors les $\mathfrak{o}$-modules finis sont justement ceux qui ont un nombre fini d'éléments.

Exemple. Soit p un nombre premier et M un p-groupe abélien fini. Alors $p^r M = 0$ pour r assez grand, de sorte qu'on peut regarder M comme module sur l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ pour tout r grand, et donc comme module sur l'anneau $\mathfrak{o} = \mathbb{Z}_p$ des entiers p-adiques. Le corps résiduel est $k = \mathbb{F}_p$.

Exemple. Soit k un corps, M un espace vectoriel de dimension finie et T un endomorphisme nilpotent de M. Alors M peut être regardé comme $k[t]$-module où t est une indéterminée en définissant $tx = Tx$ pour tout $x \in M$. Puisque T est nilpotent, on a $t^r M = 0$ pour r grand et par conséquent, on peut regarder M comme module sur l'anneau des séries entières $\mathfrak{o} = k[[t]]$, qui est un anneau de valuation discrète dont le corps résiduel est k.

Remarques. L'anneau $\mathfrak{o}$ dans les deux exemples précédents est un anneau de valuation discrète complet. En général, si M est un $\mathfrak{o}$-module fini, on a $\mathfrak{p}^r M = 0$ pour tout r assez grand, de sorte que M est un $\mathfrak{o}/\mathfrak{p}^r$-module et ainsi un module sur la complétion $\mathfrak{p}$-adique $\hat{\mathfrak{o}}$ de $\mathfrak{o}$, qui a le même corps résiduel k que $\mathfrak{o}$. Donc on peut supposer sans perte de généralité que $\mathfrak{o}$ est complet.
On suppose maintenant que k est fini. Les anneaux de valuation discrète complets qui ont un corps résiduel fini sont exactement les anneaux des entiers (des corps) $\mathfrak{p}$-adiques et un corps $\mathfrak{p}$-adique K est soit une extension finie du corps $\mathbb{Q}_p$ des nombres $\mathfrak{p}$-adiques (si la caractéristique de K est 0), soit un corps de séries formelles $k((t))$ sur un corps fini (si la caractéristique de K est > 0). Les deux exemples ci-dessus (avec k fini) sont donc typiques.

Comme $\mathfrak{o}$ est un anneau principal, tout $\mathfrak{o}$-module de type fini peut s'écrire comme somme directe de $\mathfrak{o}$-modules cycliques. Pour un $\mathfrak{o}$-module fini M, ça signifie qu'il y a une décomposition en somme directe de M de la forme

$$M \cong \bigoplus_{i=1}^{r} \mathfrak{o}/\mathfrak{p}^{\lambda_i} \tag{6.1}$$

où les λ_i sont des entiers positifs qu'on peut supposer d'être arrangés en ordre décroissant : $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r > 0$. Autrement dit, $\lambda = (\lambda_1, \ldots, \lambda_r)$ est une *partition*.

Proposition 6.1. *Soit $\mu_i = dim_k(\mathfrak{p}^{i-1}M/\mathfrak{p}^i M)$. Alors $\mu = (\mu_1, \mu_2, \ldots)$ est la conjuguée de la partition λ.*

Démonstration. Soit x_j un générateur de $\mathfrak{o}/\mathfrak{p}^{\lambda_i}$ en (6.1) et π un générateur de $\mathfrak{p}$. Alors $\mathfrak{p}^{i-1}$ est engendré par ceux des $\pi^{i-1}x_j$ qui ne s'annulent pas, i.e. ceux avec $\lambda_j \geq i$. Ainsi μ_j est égal au nombre d'indices j tels que $\lambda_j \geq i$ et donc $\mu_i = \lambda'_i$. □

Définitions 6.2. La proposition 6.1 implique que la partition λ est uniquement déterminée par le module M et on apelle λ le **type** de M.
Par unicité de la décomposition (6.1), on a que deux $\mathfrak{o}$-modules finis sont isomorphes si et seulement s'ils ont le même type, et chaque partition λ apparaît comme un type.
Si λ est le type de M, alors $|\lambda| = \sum \lambda_i$ est la **longueur** $\ell(M)$ de M, i.e. la longueur d'une suite de composition de M.
La longueur est une application additive de M. Ceci signifie que si

$$0 \to M' \to M \to M'' \to 0$$

est une suite exacte courte de $\mathfrak{o}$-modules finis, alors

$$\ell(M') - \ell(M) + \ell(M'') = 0.$$

Si N est un sous-module de M, le **cotype** de N dans M est le type de M/N.

Définitions 6.3. On remarque qu'un $\mathfrak{o}$-module M est **cyclique** (i.e. engendré par un seul élément) si et seulement si son type est une partition (r) qui se compose d'une seule part $r = \ell(M)$. On dit que M est **élémentaire** si le type de M est (1^r).

Dire que M est élémentaire est équivalent au fait que $\mathfrak{p}M = 0$. Dans ce cas M est un espace vectoriel sur k et $\ell(M) = \dim_k M = r$.

Soit π un générateur de l'idéal maximal $\mathfrak{p}$. Si $m \leq n$, la multiplication par π^{n-m} est un $\mathfrak{o}$-homomorphisme injectif de $\mathfrak{o}/\mathfrak{p}^m$ dans $\mathfrak{o}/\mathfrak{p}^n$. Soit E la limite inductive :

$$E = \varinjlim \mathfrak{o}/\mathfrak{p}^n.$$

Alors E est un $\mathfrak{o}$-module injectif qui contient $\mathfrak{o}/\mathfrak{p} = k$ et est l'enveloppe injective de k, i.e. le plus petit $\mathfrak{o}$-module qui est injectif et contient k comme

sous-module. Si maintenant M est un $\mathfrak{o}$-module fini, le **dual** de M est défini comme suit :

$$\hat{M} = \mathrm{Hom}_{\mathfrak{o}}(M, E).$$

Le dual $\hat{M}$ est un $\mathfrak{o}$-module fini, isomorphe à M, donc de même type que M. (Pour voir ça, on observe que $M \mapsto \hat{M}$ commute avec les sommes directes ; il suffit donc de vérifier que $\hat{M} \simeq M$ quand M est cyclique (et fini), ce qui est facile.)
Comme E est injectif, une suite exacte

$$0 \to N \to M \to M/N \to 0$$

(où N est un sous-module de M) donne lieu à une suite exacte

$$0 \leftarrow \hat{N} \leftarrow \hat{M} \leftarrow \widehat{(M/N)} \leftarrow 0$$

et $\widehat{(M/N)}$ est l'annulateur N^0 de N dans $\hat{M}$, i.e. l'ensemble de tous les $\xi \in \hat{M}$ tels que $\xi(N) = 0$. L'application naturelle $M \to \hat{\hat{M}}$ est un isomorphisme pour tout $\mathfrak{o}$-module fini M et identifie N avec N^{00}. D'où la proposition suivante.

Proposition 6.4. *$N \leftrightarrow N^0$ est une bijection entre les sous-modules de M, $\hat{M}$ respectivement, qui envoie l'ensemble de tous les $N \subset M$ de type ν et cotype μ sur l'ensemble de tous les $N^0 \subset \hat{M}$ de type μ et cotype ν.*

On suppose que le corps résiduel k est fini, avec q éléments. Si M est un $\mathfrak{o}$-module fini et x est un élément non nul de M, on dira que x est de **hauteur** r ($\mathrm{ht}(x) = r$) si $\mathfrak{p}^r x = 0$ et $\mathfrak{p}^{r-1} x \neq 0$. On dit que l'élément nul de M est de hauteur 0. On note M_r le sous-module de M qui consiste en les éléments de hauteur $\leq r$, de sorte que M_r est l'annulateur de $\mathfrak{p}^r$ dans M.

Proposition 6.5. *Le nombre des automorphismes d'un $\mathfrak{o}$-module fini M de type λ est*

$$a_\lambda(q) = q^{|\lambda| + 2n(\lambda)} \prod_{i \geq 1} \varphi_{m_i(\lambda)}(q^{-1}),$$

où $\varphi_m(t) = (1-t)(1-t^2)\cdots(1-t^m)$ et $(m_i(\lambda))$ est définie par $\lambda = 1^{m_1} 2^{m_2} \cdots r^{m_r} \cdots$, ($m_i(\lambda) = 0$ si $i \gg 0$ et $\varphi_0(t) = 1$).

Le nombre des automorphismes de M est égal au nombre des suites $(x_1, \ldots, x_r)$ d'éléments de M tels que x_i est de hauteur λ_i ($1 \leq i \leq r$) et M est la somme directe des sous-modules cycliques $\mathfrak{o}x_i$.Pour énumérer ce genre de suites, on utilisera le lemme suivant.

Lemme 6.6. *Soit N un sous-module de M, engendré par des éléments de hauteur $\leq r$, et $x \in M$. Alors les conditions suivantes sont équivalentes :*

(i) x est de hauteur r et $\mathfrak{o}x \cap N = 0$;
(ii) $x \in M_r \backslash (M_{r-1} + N_r)$.
De plus, le nombre de $x \in M$ qui satisfont à ces conditions équivalentes est

$$q^{\lambda'_1+\ldots+\lambda'_r}(1 - q^{\nu'_r-\lambda'_r}) \tag{6.2}$$

si ν est le type de N.

Démonstration. "$(i) \Rightarrow (ii)$" Si x satisfait à (i), clairement $x \in M$. Si $x \in M_{r-1} + N_r$, alors $0 \neq \mathfrak{p}^{r-1}x \subset N_r \subset N$, donc $\mathfrak{o}x \cap N \neq 0$ ce qui contredit l'hypothèse.
"$(ii) \Rightarrow (i)$" Si x satisfait à (ii), il est clair que $\mathrm{ht}(x) = r$. Si $\mathfrak{o}x \cap N \neq 0$, alors on peut prendre $m < r$, m minimal, tel qu'on a $\mathfrak{p}^m x \subset N$ et donc $\mathfrak{p}^{r-1}x$ est contenu dans le socle N_1 de N. Puisque N est engendré par les éléments de hauteur $\geq r$, il s'ensuit que $\mathfrak{p}^{r-1}x = \mathfrak{p}^{r-1}y$ pour un élément $y \in N$ convenable ; d'où $x - y \in M_{r-1}$ et donc $x \in (M_{r-1} + N) \cap M_r = M_{r-1} + N_r$.
On a $M/M_r \simeq \mathfrak{p}^r M$ et donc

$$\ell(M_r) = \ell(M) - \ell(\mathfrak{p}^r M) = \sum_{i=1}^{r} \ell(\mathfrak{p}^{i-1}M/\mathfrak{p}M) = \lambda'_1 + \ldots + \lambda'_r$$

d'après la proposition 6.1. Également

$$\begin{aligned} \ell(M_{r-1} + N_r) &= \ell(M_{r-1}) + \ell((M_{r-1} + N_r)/M_{r-1}) \\ &= \ell(M_{r-1}) + \ell(N_r/N_{r-1}) \\ &= \lambda'_1 + \ldots + \lambda'_{r-1} + \nu'_r \end{aligned}$$

ce qui prouve (6.2). □

Le nombre des automorphismes de M est donc le produit des nombres (6.2) pour $r = \lambda_1, \lambda_2, \ldots$, où $\nu = (\lambda_1, \ldots, \lambda_{k-1}$ si $r = \lambda_k$. Ce n'est pas difficile de voir que le produit est égal à $a_\lambda(q)$ tel qu'il est défini dans la proposition 6.5.

6.2 L'algèbre de Hall

Dans cette partie on suppose que le corps résiduel k est fini.
Soient $\lambda, \mu^{(1)}, \ldots, \mu^{(r)}$ des partitions, et soit M un $\mathfrak{o}$-module fini de type λ. On définit

$$G^{\lambda}_{\mu^{(1)}\ldots\mu^{(r)}}(\mathfrak{o})$$

comme le nombre des chaînes des sous-modules de M :

$$M = M_0 \supset M_1 \supset \ldots \supset M_r = 0$$

telles que M_{i-1}/M_i est de type $\mu^{(i)}$, pour $1 \leq i \leq r$. En particulier, $G^{\lambda}_{\mu\nu}(\mathfrak{o})$ est le nombre des sous-modules N de M qui sont de type ν et de cotype μ. Comme $\ell(M) = \ell(M/N) + \ell(N)$, le corollaire suivant est clair.

Corollaire 6.7. *On a $G^{\lambda}_{\mu\nu}(\mathfrak{o}) = 0$ sauf si $|\lambda| = |\mu| + |\nu|$.*

L'idée de Philip Hall était d'utiliser les nombres $G^{\lambda}_{\mu\nu}(\mathfrak{o})$ comme les constantesde structure de la multiplication d'un anneau, comme suit. Soit $H = H(\mathfrak{o})$ le $\mathbb{Z}$-module libre sur une base (u_λ) indexé par toutes les partitions λ. On définit un produit dans H par la règle

$$u_\mu u_\nu = \sum_\lambda G^{\lambda}_{\mu\nu}(\mathfrak{o}) u_\lambda.$$

D'après le corollaire 6.7, la somme à droite n'a qu'un nombre fini des termes non nuls.

Proposition 6.8. *L'anneau $H(\mathfrak{o})$ est commutatif et associatif et possède un élément neutre.*

Démonstration. L'élément neutre est u_0, où 0 est la partition vide correspondant au module $\mathfrak{o}$. L'associativité découle du fait que le coefficient de u_λ dans $u_\mu(u_\nu u_\rho)$, comme dans $(u_\mu u_\nu)u_\rho$ est juste $G^{\lambda}_{\mu\nu\rho}$. La commutativité découle de la proposition 6.4, qui montre que $G^{\lambda}_{\mu\nu} = G^{\lambda}_{\nu\mu}$ (car on a une bijection qui change type et cotype). □

Définition 6.9. L'anneau $H(\mathfrak{o})$ est l'**algèbre de Hall** de $\mathfrak{o}$.

Proposition 6.10. *L'anneau $H(\mathfrak{o})$ est engendré (comme $\mathbb{Z}$-algèbre) par les éléments $u_{(1^r)}$ $(r \geq 1)$, et ils sont algébriquement indépendants sur $\mathbb{Z}$.*

Démonstration. On va écrire v_r au lieu de $u_{(1^r)}$ et on considère le produit

$$v_{\lambda'} = v_{\lambda'_1} v_{\lambda'_2} \cdots v_{\lambda'_s} \tag{6.3}$$

où $\lambda' = (\lambda'_1, \ldots \lambda'_s)$ est la conjuguée de λ comme d'habitude. Ce produit $v_{\lambda'}$ est une combinaison linéaire des u_μ,

$$v_{\lambda'} = \sum_\mu a_{\lambda\mu} u_\mu \tag{6.4}$$

où le coefficient $a_{\lambda\mu}$ est, par définition, égal au nombre de chaînes

$$M = M_0 \supset M_1 \supset \ldots \supset M_s = 0$$

dans un $\mathfrak{o}$-module M fini fixé de type μ, tel que M_{i-1}/M_i est de type $(1^{\lambda'_i})$, i.e. élémentaire de longueur λ'_i, pour $1 < i < s$. Si une telle chaîne existe (c'est-à-dire, si $a_{\lambda\mu} \neq 0$) on a forcément $\mathfrak{p}M_{i-1} \subset M_i$ $(1 \leq i \leq s)$ et donc $\mathfrak{p}^i M \subset M_i$ pour $1 < i < s$. D'où

$$\ell(M/\mathfrak{p}^i M) \geq \ell(M/M_i)$$

ce qui nous donne, en vertu de la proposition 6.1, l'inégalité suivante pour $1 \leq i \leq s$:

$$\mu'_1 + \ldots + \mu'_i \geq \lambda'_1 + \ldots + \lambda'_i.$$

Alors $\mu' \geq \lambda'$ et donc d'après la proposition 4.10, $\mu \leq \lambda$.
De plus, le même raisonnement montre que si $\mu = \lambda$, il y a qu'une seule chaîne possible : $M_i = \mathfrak{p}^i M$.
Ensuite, on a $a_{\lambda\mu} = 0$ sauf si $\mu \leq \lambda$, et $a_{\lambda\lambda} = 1$. Autrement dit, la matrice $(a_{\lambda\mu})$ est strictement triangulaire supérieure et on peut résoudre les équations (6.3) pour exprimer les u_μ comme combinaisons linéaires des $v_{\lambda'}$. Les $v_{\lambda'}$ forment donc une $\mathbb{Z}$-base de $H(\mathfrak{o})$, ce qui prouve la proposition 6.10. □

Remarque. De la proposition précédente 6.10, il s'ensuit que l'algèbre de Hall $H(\mathfrak{o})$ est isomorphe à l'anneau des fonctions symétriques Λ (chapitre 5).

6.3 Suite LR d'un sous-module

Soit T un tableau de la forme $\lambda - \mu$ et de poids $\nu = (\nu_1, \ldots, \nu_r)$. Alors T détermine (et est déterminé par) une suite des partitions

$$S = (\lambda^{(0)}, \lambda^{(1)}, \ldots, \lambda^{(r)})$$

de manière que $\lambda^{(0)} = \mu$, $\lambda^{(r)} = \lambda$ et $\lambda^{(i)} \supset \lambda^{(i-1)}$ pour $1 \leq i \leq r$, par la condition que $\lambda^{(i)} - \lambda^{(i-1)}$ est le "'skew diagram"' (cf. définition 4.4) qui se compose des cases qui sont occupées par le symbole i dans T (et donc est une bande horizontale, car T est un tableau).

Définition 6.11. Une suite de partitions S comme ci-dessus sera appelé **suite LR** ("suite de Littlewood-Richardson") **de type** $(\mu, \nu; \lambda)$ si

(LR1) $\lambda^{(0)} = \mu$, $\lambda^{(r)} = \lambda$, et $\lambda^{(i)} \supset \lambda^{(i-1)}$ pour $1 \leq i \leq r$;

(LR2) $\lambda^{(i)} - \lambda^{(i-1)}$ est une bande horizontale de longueur ν_i, pour $1 \leq i \leq r$. (Ces deux conditions assurent que S détermine le tableau T.)

(LR3) Le mot $w(T)$ obtenu en lisant T de droite à gauche, en commencant par la ligne la plus haute, puis en descendant, est une "lattice" permutation (chapitre 4).

Pour que (LR3) soit satisfait, il est nécessaire est suffisant que, pour $i \geq 1$ et $k \geq 0$, le nombre de symboles i dans les k premières lignes de T est supérieur ou égal au nombre de symboles $i+1$ dans les $k+1$ premières lignes de T. Autrement dit, une condition équivalente à (LR3) est la condition suivante :

$$\sum_{j=1}^{k}(\lambda_j^{(i)} - \lambda_j^{(i-1)}) \geq \sum_{j=1}^{k+1}(\lambda_j^{(i+1)} - \lambda_k^{(i)}) \qquad \text{(LR3')}$$

pour tout $i \geq 1$ et $k \geq 0$.

Dans cette section, on va montrer que chaque sous-module N d'un $\mathfrak{o}$-module fini M donne lieu à un suite LR de type $(\mu', \nu'; \lambda')$, où λ, μ, ν sont les types de M, M/N, et N respectivement. Mais avant de faire la preuve, on a besoin de certains lemmes. Dans cette section, ce n'est pas nécessaire de supposer que le corps résiduel de $\mathfrak{o}$ est fini.

Lemme 6.12. *Soit M un $\mathfrak{o}$-module fini de type λ et soit N un sous-module de type ν et de cotype μ dans M. Alors $\mu \subset \lambda$ et $\nu \subset \lambda$.*

Démonstration. Puisque

$$\frac{\mathfrak{p}^{i-1}(M/N)}{\mathfrak{p}^i(M/N)} \simeq \frac{\mathfrak{p}^{i-1}M + N}{\mathfrak{p}^i M + N} \simeq \frac{\mathfrak{p}^{i-1}M}{\mathfrak{p}^{i-1}M \cap (\mathfrak{p}^i M + N)}$$

et comme également $\mathfrak{p}^{i-1}M \cap (\mathfrak{p}^i M + N) \supset \mathfrak{p}^i M$, il s'ensuit que

$$\ell(\mathfrak{p}^{i-1}(M/N)/\mathfrak{p}^i(M/N)) \leq \ell(\mathfrak{p}^{i-1}M/\mathfrak{p}^i M)$$

et donc que $\mu_i' \leq \lambda_i'$ par la proposition 6.1. Par conséquent $\mu \subset \lambda$. Par dualité (cf. proposition 6.4), il découle aussi que $\nu \subset \lambda$. □

Soit M un $\mathfrak{o}$-module de type λ, N un sous-module élémentaire de M. Alors $\mathfrak{p}N = 0$, de sorte que $N \subset S$ où

$$S = \{x \in M | \mathfrak{p}x = 0\}$$

est le socle de M, i.e. le plus grand sous-module élémentaire de M.

Lemme 6.13. *Le type de M/S est $\tilde{\lambda} = (\lambda_1 - 1, \lambda_2 - 1, \ldots)$.*

Démonstration. Si $M = \bigoplus \mathfrak{o}/\mathfrak{p}^{\lambda_i}$, alors clairement $S = \bigoplus \mathfrak{p}^{\lambda_i - 1}/\mathfrak{p}^{\lambda_i}$, d'où $M/S \simeq \bigoplus \mathfrak{o}/\mathfrak{p}^{\lambda_i - 1}$. □

Lemme 6.14. *Soit M un $\mathfrak{o}$-module fini de type λ et N un sous-module élémentaire de M, de cotype μ. Alors $\lambda - \mu$ est une bande verticale (i.e. $\lambda_i - \mu_i = 0$ or 1 pour tout i).*

Démonstration. On a $N \subset S$, donc $M/S \simeq (M/N)/(S/N)$ et alors $\tilde{\lambda} \subset \mu \subset \lambda$ par les lemmes 6.12 et 6.13. Ainsi

$$0 \leq \lambda_i - \mu_i \leq \lambda_i - \tilde{\lambda}_i = 1$$

et d'après cela, $\lambda - \mu$ est une bande verticale. □

Remarque. Si $\mu \subset \lambda$, alors $\lambda - \mu$ est une bande verticale si et seulement si $\tilde{\lambda} \subset \mu$.

Proposition 6.15. *Soit M un $\mathfrak{o}$-module fini de type λ et soit N un sous-module de M, de type ν et de cotype μ. Pour tout $i \geq 0$, soit $\lambda^{(i)}$ le cotype de $\mathfrak{p}^i N$. Alors la suite*

$$S(N) = (\lambda^{(0)\prime}, \lambda^{(1)\prime}, \ldots, \lambda^{(r)\prime})$$

(où $\mathfrak{p}^r N = 0$) est une suite LR de type $(\mu', \nu'; \lambda')$.

Démonstration. Il est clair que $\lambda^{(0)} = \mu$ et $\lambda^{(r)} = \lambda$, et $\lambda^{(i)} \supset \lambda^{(i-1)}$ par le lemme 6.12 appliqué au module $M/\mathfrak{p}^i N$ et au sous-module $\mathfrak{p}^{i-1}N/\mathfrak{p}^i N$. Alors (LR1) est satisfait. Puisque $\mathfrak{p}^{i-1}N/\mathfrak{p}^i N$ est un $\mathfrak{o}$-module élémentaire, il s'ensuit du lemme 6.14 que $\lambda^{(i)} - \lambda^{(i-1)}$ est une bande verticale et donc que $\lambda^{(i)\prime} - \lambda^{(i-1)\prime}$ est une bande horizontale, de longueur égale à $\ell(\mathfrak{p}^{i-1}N/\mathfrak{p}^i N) = \nu'_i$ (par la proposition 6.1). Donc (LR2) est satisfait.
Quant à (LR3'), on a

$$\lambda_j^{(i)\prime} = \ell(\mathfrak{p}^{j-1}(M/\mathfrak{p}^i N)/\mathfrak{p}^j(M/\mathfrak{p}^i N))$$

(encore par la proposition 6.1), de sorte que

$$\sum_{j=1}^{k} \lambda_j^{(i)\prime} = \ell((M/\mathfrak{p}^i N)/\mathfrak{p}^k(M/\mathfrak{p}^i N)) = \ell(M/(\mathfrak{p}^k M + \mathfrak{p}^i N))$$

et donc

$$\sum_{j=1}^{k} (\lambda_j^{(i)\prime} - \lambda_j^{(i-1)\prime}) = \ell(V_{ki})$$

où $V_{ki} = (\mathfrak{p}^k M + \mathfrak{p}^{i-1}N)/(\mathfrak{p}^k M + \mathfrak{p}^i N)$. De même

$$\sum_{j=1}^{k+1} (\lambda_j^{(i+1)\prime} - \lambda_j^{(i)\prime}) = \ell(V_{k+1,i+1}).$$

Comme la multiplication par un générateur de $\mathfrak{p}$ induit un homomorphisme de V_{ki} sur $V_{k+1,i+1}$, il s'ensuit que $\ell(V_{ki}) \geq \ell(V_{k+1,i+1})$, et donc (LR3') est satisfait. □

6.4 Le polynôme de Hall

Dans cette section, on va calculer les constantes de structure $G^\lambda_{\mu\nu}$ de l'algèbre de Hall. (Le corps résiduel de $\mathfrak{o}$ est supposé fini.) Soit S une suite LR de type $(\mu', \nu'; \lambda')$ et soit M un $\mathfrak{o}$-module fini de type λ. On note par $G_S(\mathfrak{o})$ le nombre de sous-modules N de M dont la suite LR associée $S(N)$ est S. Par la proposition 6.15, chaque tel N est de type ν et de cotype μ.
On note par q le nombre d'éléments du corps résiduel de $\mathfrak{o}$ et on se rappelle que $n(\lambda) = \sum(i-1)\lambda_i$ pour chaque partition λ (définition 4.3). Alors on a la proposition suivante.

Proposition 6.16. *Pour chaque suite LR S de type $(\mu', \nu'; \lambda')$, il existe un polynôme unitaire $g_S(t) \in \mathbb{Z}[t]$ de degré $n(\lambda) - n(\mu) - n(\nu)$, indépendant de $\mathfrak{o}$, de sorte que*

$$g_s(q) = G_S(\mathfrak{o}).$$

(Autrement dit, $G_S(\mathfrak{o})$ est un "polynôme en q".)

Maintenant on définit pour toutes les trois partitions λ, μ, ν

$$g^\lambda_{\mu\nu}(t) = \sum_S g_S(t)$$

où la somme porte sur toutes les suites LR S de type $(\mu', \nu'; \lambda')$.

Définition 6.17. Ce polynôme est appelé le **polynôme de Hall** correspondant à λ, μ, ν.

Proposition 6.18. *(i) Si $c^\lambda_{\mu\nu} = 0$, le polynôme de Hall $g^\lambda_{\mu\nu}$ est (identiquement) zéro. (En particulier, $g^\lambda_{\mu\nu}(t) = 0$ sauf si $|\lambda| = |\mu| + |\nu|$ et $\mu, \nu \subset \lambda$.)*
(ii) Si $c^\lambda_{\mu\nu} \neq 0$, alors $g^\lambda_{\mu\nu}(t)$ est de degré $n(\lambda) - n(\mu) - n(\nu)$ est le coefficient principal est $c^\lambda_{\mu\nu}$.
(iii) Dans les deux cas, $G^\lambda_{\mu\nu}(\mathfrak{o}) = g^\lambda_{\mu\nu}(q)$.
(iv) $g^\lambda_{\mu\nu}(t) = g^\lambda_{\nu\mu}(t)$.

On va faire la preuve d'une version légèrement affaiblie de 6.18, qui est la suivante :

Proposition 6.19. *Pour chaque triplet des partitions λ, μ, ν, il existe un polynôme $g^\lambda_{\mu\nu}(t) \in \mathbb{Z}[t]$ de sorte que $G^\lambda_{\mu\nu}(\mathfrak{o}) = g^\lambda_{\mu\nu}(q)$. De plus, $g^\lambda_{\mu\nu}(t)$ est de degré $\leq n(\lambda) - n(\mu) - n(\nu)$, et le coefficent de $t^{n(\lambda)-n(\mu)-n(\nu)}$ est égal à $c^\lambda_{\mu\nu}$.*

La preuve est basée sur une interpretation combinatoire des coefficients $a_{\lambda\mu}$ de la formule (6.4). On a besoin de quelques définitions.

Définitions 6.20. Une **composition** est une suite $\alpha = (\alpha_1, \alpha_2, \ldots)$ d'entiers positifs ou nuls qui n'a qu'un nombre fini de termes non nuls. Une partition est donc une composition de sorte que $\alpha_1 \geq \alpha_2 \geq \ldots$. Le groupe S_∞ de permutations finies de $\mathbb{N}^+$ agit sur les compositions par $w\alpha = (\alpha_{w^{-1}(1)}, \alpha_{w^{-1}(2)}, \ldots)$. On va écrire $\alpha \sim \beta$ si α et β sont conjuguée sous cette action : chaque S_∞-orbite contient exactement une partition.
Les compositions ont des diagrammes, comme les partitions : le diagramme de α est défini comme l'ensemble $\{(i,j) \in \mathbb{Z}^2 | 1 \leq j \leq \alpha_i\}$ et est graphiquement représenté comme une superposition de lignes qui contiennent α_i cases dans la i-ème ligne.
Si α et β sont deux compositions, une **table** [1] de forme α et de poids β est une numérotation des cases du diagramme de α par des entiers positifs de sorte que pour chaque $i \geq 1$, il y a β_i cases numéroté par i (une table est une application $A : \alpha \to \mathbb{N}^+$ telle que $\mathrm{card}(A^{-1}(i)) = \beta_i$ pour tout $i \geq 1$; on va supposer que A est défini sur tout $\mathbb{Z}^+ \times \mathbb{Z}^+$ avec $A(i,j) = +\infty$ si $j > \alpha_i$). Pour tout $x = (i,j) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ soit $x^{\rightarrow} = (i, j+1)$. Une table α est appelé **ordonnée selon les lignes** (osl) (resp. **strictement osl**) si $A(x^{\rightarrow}) \geq A(x)$ (resp. $A(x^{\rightarrow}) > A(x)$) pour tout $x \in \alpha$. On définit les tables (strictement) ordonnées selon les colonnes de la même manière.
Sur $\mathbb{N}^+ \times \mathbb{N}^+$, on définit un ordre total par

$$(i,j) <_L (i',j') \Leftrightarrow \text{soit } j < j', \text{ soit } j = j' \text{ et } i > i'.$$

Enfin, pour chaque table strictement osl A de forme α, on définit

$$d(A) = \mathrm{Card}\left\{(x,y) \in \alpha \times \alpha | y <_L x, A(x) < A(y) < A(x^{\rightarrow})\right\}.$$

Proposition 6.21. *Soient λ, μ des partitions et α, β des compositions de sorte que $\alpha \sim \mu$ et $\beta \sim \lambda'$. Alors le coefficient $\alpha_{\lambda\mu}$ (formule (6.4)) est égal à*

$$\alpha_{\lambda\mu} = \sum_A q^{d(A)}$$

où la somme porte sur toutes les tables strictement osl A de forme α et de poids β.

Avant la preuve de cette proposition 6.21, on en déduit la proposition 6.19. Par la proposition 6.21, le polynôme

$$\sum_A t^{d(A)} \in \mathbb{Z}[t],$$

où la somme est la même que dans la proposition 6.21, ne dépend que de λ et μ ; on va le noter $\alpha_{\lambda\mu}(t)$.

1. On utilise "table" pour faire la différence avec "tableau" qui comporte plus de contraintes.

Proposition 6.22. *(a) Les coefficients de $\alpha_{\lambda\mu}(t)$ sont ≥ 0.*

(b) $\alpha_{\lambda\mu}(1)$ est égal au nombre de matrices dont les coefficients sont 0 ou 1 avec des sommes sur les lignes $\mu_1, \mu_2, \ldots$ et des sommes sur les colonnes $\lambda'_1, \lambda'_2, \ldots$.

(c) $\alpha_{\lambda\mu}(0) = 0$ sauf si $\mu \leq \lambda$. De plus, $\alpha_{\lambda\lambda}(t) = 1$.

Démonstration. "(a)" évident.

"(b)" Il suffit de créer une bijection entre des tables strictement osl de forme μ et de poids λ', et des $(0,1)$-matrices avec "row sums" $\mu_1, \mu_2, \ldots$ et "column sums" $\lambda'_1, \lambda'_2, \ldots$. Pour cela, étant donnée une table A, on lui associe la matrice (c_{ij}) , où $c_{ij} = 1$ si la i-ème ligne de A contient j, et $c_{ij} = 0$ sinon ; ceci est la bijection demandée.

"(c)" La preuve de la partie (c) exige le théorème de Gale-Ryser (cf. [4, p. 119]) qu'on n'a pas vu, et est donc sautée. □

Par la proposition ci-dessus 6.22, $(\alpha_{\lambda\mu}(t))$ est une matrice unitriangulaire supérieure sur $\mathbb{Z}[t]$. C'est donc inversible est son inverse est de la même forme. Alors, les coefficients des matrices de passage entre les bases $(v_{\lambda'})$ et (u_λ) dans $H(\mathfrak{o})$ sont des polynômes entiers en q. Puisque la loi de multiplication dans $H(\mathfrak{o})$, exprimée dans la base $(v_{\lambda'})$, ne dépend pas de q, il s'ensuit que les constantes de structure dans la base (u_λ) sont des polynômes entiers en q. Cela prouve l'existence des polynômes de Hall $g^\lambda_{\mu\nu} \in \mathbb{Z}[t]$. Il reste à trouver leurs degrés et coefficients principaux.

Proposition 6.23. *$\alpha_{\lambda\mu}(t)$ est de degré $\leq n(\mu) - n(\lambda)$, et le coefficient de $t^{n(\mu)-n(\lambda)}$ est égal à $k_{\mu'\lambda'}$.*

Cette proposition 6.23 s'ensuit immédiatement du lemme combinatoire suivant.

Lemme 6.24. *Pour chaque table strictement osl A de forme μ et de poids λ' on note $\tilde{d}(A)$ le nombre de paires $(x, y) \in \mu \times \mu$ telles que y est au-dessus de x (dans la même colonne) et $A(x) < A(y) < A(x^{\rightarrow})$. Alors*

(a) $d(A) + \tilde{d}(A) = n(\mu) - n(\lambda)$;

(b) $\tilde{d}(A) = 0$ si et seulement si A est ordonnée selon les colonnes.

Démonstration. "(a)" Soient

$$\begin{aligned} D(A) &= \{(x,y) \in \mu \times \mu | y <_L x, A(x) \leq A(y) < A(x^{\rightarrow})\}, \\ N(\mu) &= \{(x,y) \in \mu \times \mu | y \text{ est au dessus de } x\}, \\ \tilde{D}(A) &= \{(x,y) \in N(\mu) | A(x) < A(y) < A(x^{\rightarrow})\}; \end{aligned}$$

alors on a

$$\mathrm{card}(D(A)) = d(A) + \sum_{i\geq 1} \binom{\lambda'_i}{2} = d(A) + n(\lambda),$$

$$\mathrm{card}(N(\mu)) = \sum_{i\geq 1} \binom{\mu'_i}{2} = n(\mu),$$

et

$$\mathrm{card}(\tilde{D}(A)) = \tilde{d}(A).$$

Maintenant, on va construire une application $\varphi : D(A) \to N(\mu)$. Soit $(x, y) \in D(A)$. On suppose que $x = (i_1, j_1)$, $y = (i_2, j_2)$. Il est clair que $i_1 \neq i_2$; soit $i = \max(i_1, i_2)$, $i' = \min(i_1, i_2)$, $j = \min(j_1, j_2)$ et finalement $\varphi(x, y) = ((i, j), (i', j))$. L'application φ définie ainsi est une bijection de $D(A)$ dans $N(\mu)\backslash\tilde{D}(A)$. On va visualiser φ ; il y a trois cas :

(a) $\boxed{x'} < \boxed{x}$ $\quad$ $\boxed{y}$

(b) $\boxed{y}$ $\quad$ $\boxed{x'} < \boxed{x}$

(c) $\boxed{x}$ $\quad$ $\boxed{y}$

Pour le cas (a), on a $\varphi(x, y) = (y, x')$, pour le cas (b) $\varphi(x, y) = (x', y)$ et pour le cas (c) $\varphi(x, y) = (y, x)$.
Pour voir que φ est une bijection, on cherche une application $\psi : N(\mu)\backslash\tilde{D}(A) \to D(A)$. Soit $(x', y') \in N(\mu)\backslash\tilde{D}(A)$. Ici, il y a deux cas.

(1) "$A(y') \leq A(x')$" : Soit x la case de la même ligne que y' telle que $A(x) \leq A(x') < A(x^{\rightarrow})$. On pose $\psi(x', y') = (x, x')$. Alors $\varphi(x, x') = (x', y')$ par (a) ou (c).

(2) "$A(y') \geq A(x'^{\rightarrow})$" : Soit x la case de la même ligne que x' telle que $A(x) \leq A(y') < A(x^{\rightarrow})$ (la case x est strictement plus à droite que x' car $A(x'^{\rightarrow}) \leq A(y)$). On pose $\psi(x', y') = (x, y')$. Alors $\varphi(x, y') = (x', y')$ par (b).
On a donc trouvé $\psi : N(\mu)\backslash\tilde{D}(A) \to D(A)$ de sorte que $\psi \circ \varphi = \mathrm{id}_{D(A)}$ et $\varphi \circ \psi = \mathrm{id}_{N(\mu)\backslash\tilde{D}(A)}$.

"(b)" "$\Rightarrow$" évident.

"$\Leftarrow$" On suppose que A est ordonné selon les colonnes : c'est-à-dire qu'il existe $x = (i, j)$, $y = (i', j') \in \mu$ de sorte que $i > i'$ et $A(x) < A(y)$. On choisit un tel couple avec j le plus petit possible ; il est clair que ce couple appartient à $\tilde{D}(A)$, donc $\tilde{d}(A) \neq 0$. □

Maintenant, soit $\tilde{a}_{\lambda\mu}(t) = t^{n(\mu)-n(\lambda)}\alpha_{\lambda\mu}(t^{-1})$. De la proposition 6.23 et du lemme 6.24, on obtient le corollaire suivant.

Corollaire 6.25.

$$\tilde{a}_{\lambda\mu}(t) = \sum_A t^{\tilde{d}(A)}$$

où la somme porte sur toutes les tables strictement osl de forme μ et de poids λ' ; en particulier, $\tilde{a}_{\lambda\mu} \in \mathbb{Z}[t]$. De plus, $\tilde{a}_{\lambda\mu}(0) = k_{\mu'\lambda'}$.

Maintenant, on considère l'anneau $\Lambda[t] = \Lambda_{\mathbb{Z}[t]}$ de polynômes en t avec coefficients dans Λ ; on va écrire les éléments de $\Lambda[t]$ comme $P(x;t)$. Il est clair que $\Lambda[t]$ est un $\mathbb{Z}[t]$-module libre ayant pour base (e_λ). Par 6.22(c), la matrice $(\tilde{a}_{\lambda\mu}(t))$ est unitriangulaire supérieure. Les équations

$$e_{\lambda'} = \sum_\mu \tilde{a}_{\lambda\mu}(t) P_\mu(x;t)$$

déterminet donc uniquement des éléments $P_\mu(x;t) \in \Lambda[t]$, et ceux-ci forment une $\mathbb{Z}[t]$-base de $\Lambda[t]$. Soient $f^\lambda_{\mu\nu}(t)$ les constantes de structure de $\Lambda[t]$ dans cette base, i.e.

$$P_\mu(x;t)P_\nu(x;t) = \sum_\lambda f^\lambda_{\mu\nu}(t) P_\lambda(x;t);$$

il est clair que $f^\lambda_{\mu\nu}(t) \in \mathbb{Z}[t]$ pour tout λ, μ, ν.

Corollaire 6.26 (sans démonstration)**.** *(a) $g^\lambda_{\mu\nu}(t) = t^{n(\lambda)-n(\mu)-n(\nu)} f^\lambda_{\mu\nu}(t^{-1})$.*
(b) $P_\lambda(x;0) = s_\lambda(x)$. En particulier, $f^\lambda_{\mu\nu}(0) = c^\lambda_{\mu\nu}$ sont les constantes de structure de Λ dans la base (s_λ).

Par ce corollaire 6.26, $g^\lambda_{\mu\nu}(t)$ est de degré $\leq n(\lambda) - n(\mu) - n(\nu)$, et le coefficient de cette puissance de t est égal à $f^\lambda_{\mu\nu}(0) = c^\lambda_{\mu\nu}$. Ça termine la preuve de la proposition 6.19.

Il reste à prouver la proposition 6.21. Pour ça, on va reformuler les définitions d'une table et de $d(A)$ en termes de(s) suites de compositions. Si α et β sont deux compositions, on écrit $\beta \dashv \alpha$ si $\alpha_i - 1 \leq \beta_i \leq \alpha_i$ pour tout $i \geq 1$. Si $\beta \dashv \alpha$, alors on définit $d(\alpha, \beta)$ comme le nombre de paires (i, j) telles que $\beta_i = \alpha_i$, $\beta_j = \alpha_j - 1$ et $(j, \alpha_j) <_L (i, \alpha_i)$.

Proposition 6.27. *Soient α et β deux compositions et on suppose que $\beta_i = 0$ pour $i > r$. Il existe une bijection naturelle entre des tables strictement osl A de forme α et de poids β et des suites de compositions $(\alpha^{(0)}, \alpha^{(1)}, \ldots, \alpha^{(r)})$ de sorte que $0 = \alpha^{(0)} \dashv \alpha^{(1)} \dashv \ldots \dashv \alpha^{(r)} = \alpha$ et $|\alpha^{(i)}| - |\alpha^{(i-1)}| = \beta_i$ pour $i \geq 1$. De plus, cette bijection transforme $d(A)$ en $\sum_{i\geq 1} d(\alpha^{(i)}, \alpha^{(i-1)})$.*

Démonstration. On associe à une table A la suite $(\alpha^{(i)})$, où $\alpha^{(i)} = A^{-1}(\{1, 2, \ldots, i\})$. On sait que $d(A) = \text{card}\,\{(x, y) \in \alpha \times \alpha | y <_L x, A(x) < A(y) < A(x^{\rightarrow})\}$. Le nombre $d(\alpha^{(i)}, \alpha^{(i-1)})$ est égal au nombre de couples de cases (x, y) tq

(1) x est au bord de $\alpha^{(i)}$ et de $\alpha^{(i-1)}$,
(2) y est au bord de $\alpha^{(i)}$ mais pas de $\alpha^{(i-1)}$,
(3) $y <_L x$.

Le couple (x, y) "contribue" à $d(\alpha^{(i)}, \alpha^{(i-1)})$ si et seulement si $y <_L x$ et $A(x) < A(y) < A(x^{\rightarrow})$. D'où $d(A) = \sum_{i \geq 1} d(\alpha^{(i)}, \alpha^{(i-1)})$. □

On rappelle la définition de $\alpha_{\lambda\mu}$ (formule (6.4)) et on voit qu'une induction évidente réduit la preuve de la proposition 6.21 à la proposition suivante.

de l'induction évidente. On fait la démonstration par récurrence sur le nombre de parts de λ'.
(Initialisation :) Si $k = 1$, $\lambda'_1 = (r)$. Il existe un seul tableau A de forme μ et de poids λ' et $d(A) = 0$ car $A(x) = A(y)$ pour toutes cases x, y.
(Hérédité :) Si c'est vérifié pour k, on a

$$u_{(1^{\lambda'_1})} \cdots u_{(1^{\lambda'_k})} = v_{\lambda'_1} \cdots v_{\lambda'_k} = \sum_{\mu} \left(\sum_{\mathfrak{a}} q^{d(\mathfrak{a})} \right) u_\mu$$

où $\mathfrak{a} = (\alpha^{(l)})_{0 \leq l \leq k}$, $\alpha^{(k)} = \mu$ et $|\alpha(l)| - |\alpha^{(l-1)}| = \lambda'_l$. Par la proposition 6.28 on a

$$v_{\lambda'_1} \cdots v_{\lambda'_k} v_{\lambda'_{k+1}} = \sum_{\mu} \left(\sum_{\mathfrak{a}} q^{d(\mathfrak{a})} \right) u_\mu v_{(1^{\lambda'_{k+1}})} = \sum_{\mathfrak{a}} q^{d(\mathfrak{a})} \sum_{\substack{\mu \dashv \beta \\ |\beta| = |\mu| + \lambda'_{k+1}}} q^{d(\beta,\mu)} u_\beta.$$

On a $\mathfrak{a} = (0 = \alpha^{(0)} \dashv \ldots \dashv \alpha^{(k)} = \mu)$ et $\mu \dashv \beta$. En posant $\alpha^{(k+1)} = \beta$, on obtient $\tilde{\mathfrak{a}} = (0 = \alpha^{(0)} \dashv \ldots \dashv \alpha^{(k)} \dashv \alpha^{(k+1)})$. Comme $q^{d(\mathfrak{a})} q^{d(\beta,\mu)} = q^{d(\tilde{\mathfrak{a}})}$, on arrive à

$$v_{\lambda'_1} \cdots v_{\lambda'_k} v_{\lambda'_{k+1}} = \sum_{\nu} \sum_{\tilde{\mathfrak{a}}} q^{d(\tilde{\mathfrak{a}})} u_\nu.$$

□

Proposition 6.28. *Soient λ, μ des partitions avec $|\lambda| = |\mu| + r$, et soit α une composition de sorte que $\alpha \sim \lambda$. Alors*

$$G^{\lambda}_{\mu(1^r)}(\mathfrak{o}) = \sum_{\beta} q^{d(\alpha,\beta)}$$

où la somme porte sur toutes les compositions β de sorte que $\beta \dashv \alpha$ et $\beta \sim \mu$.

Démonstration. Soit M un $\mathfrak{o}$-module fini de type λ. On rappelle que $G^{\lambda}_{\mu(1^r)}(\mathfrak{o})$ est le nombre de sous-modules $N \subset M$ de type (1^r) et de cotype μ. La condition que N est de type (1^r) signifie que N est un k-sous-espace vectoriel de dimension r du socle S de M. On note $G_r(S)$ l'ensemble de ces sous-espaces. Pour compter le nombre des N, on va utilisier la décomposition en cellules de Schubert. Si $(v_i)_{i\in I}$ est une base de S donnée (i.e. $S = \bigoplus_{i\in I} kv_i$), où I est totalement ordonné, $|I| = s$, alors les cellules de Schubert correspondants C_J dans $G_r(S)$ sont paramétrisées par r-sous-ensembles $J \subset I$. Les coordonnées des éléments de C_J sont $(c_{ij} \in k | j \in J, i \in I\backslash J, j < i)$; le sous-espace correspondant à (c_{ij}) a la base $(v_j + \sum_i c_{ij}v_i)_{j\in J}$. L'ensemble $G_r(S)$ est la réunion disjointe des C_J. De plus, on a $\mathrm{card}(C_J) = q^{d(J)}$, où $d(J)$ est le nombre de pairs (i, j) de sorte que $j \in J$, $i \in I\backslash J$ et $j < i$.
Maintenant, on va exprimer M dans la forme $M_\lambda = \bigoplus_i^s \mathfrak{o}e_i$ où $e_i^{\lambda_i} = 0$.

Remarque. M_λ/N ne dépend que de J. On a $M_\lambda/N \simeq M_{\lambda-\delta_J}$ où $\delta_J = (\delta_{J,i})_{i\geq 1}$ avec $\delta_{J,i} = 1$ si $i \in J$ et 0 sinon

Pour définir un ordre sur I on dit que j est avant i si et seulement si $(j, \alpha_j) <_L (i, \alpha_i)$. On considère la décomposition correspondant de $G_r(S)$ en cellules de Schubert. Les sous-ensembles $J \subset I$ sont en bijection naturelle avec les compositions $\beta \dashv \alpha$: à un sous-ensemble J correspond une composition β telle que $\beta_i = \alpha_i - 1$ pour $i \in J$ et $\beta_i = \alpha_i$ pour $i \in I\backslash J$. Il est clair que cette bijection transforme $d(J)$ en $d(\alpha, \beta)$. Enfin, on a $M_\alpha = \bigoplus_i^s \mathfrak{o}e_i \simeq M_\lambda$ si $\alpha \sim \lambda$. Pour $N \in C_J$, on a $M_\alpha/N \simeq M_{\alpha-\delta_J}$ et il existe $q^{d(\alpha,\beta)}$ sous-espaces vectoriels N de ce genre. On note $\alpha - \delta_J := \beta$. Or, $M_\beta \simeq M_\mu$ si et seulement si $\beta \sim \mu$, d'où la proposition 6.28. □

Références

[1] William Fulton, Joe Harris : *Representation Theory : A First Course*. Springer, 1991.

[2] Daniel Guin, Thomas Hausberger : *Algèbre : Tome 1 : Groupes, corps et théorie de Galois*. EDP Sciences, 2008.

[3] Wolfgang Kinzner : *Ferienkurs zur Linearen Algebra 2, Kapitel 15 : Die Smith-Normalform*. München, 2012.

[4] Ian Grant Macdonald : *Symmetric Functions and Hall Polynomials*. Oxford Science Publications, 1995.

[5] Hermann Weyl : *Classical Groups*. Princeton University Press, Princeton, 1946.