

# PARTITION D'UN ENTIERS ET STRUCTURE DES GROUPES ABÉLIENS FINIS

## DEVOIR L3

Le but de ce sujet est de présenter ce que l'on appelle le *nombre de partitions* d'un entier et de montrer qu'il intervient dans différents domaines de l'algèbre (algèbre linéaire, théorie des groupes). On étudiera ensuite la structure des groupes abéliens finis.

### 0. INTRODUCTION ET NOTATIONS

Le nombre qui va nous intéresser dans ce sujet est le nombre de façons différentes d'écrire un entier naturel comme somme d'autres entiers naturels. Par exemple :

$$\begin{aligned}4 &= 1 + 1 + 1 + 1 \\ &= 1 + 1 + 2 \\ &= 1 + 3 \\ &= 2 + 2 \\ &= 4\end{aligned}$$

Du fait de la commutativité de l'addition dans  $\mathbb{N}$ , on considèrera que deux décompositions sont égales si elles sont composées des mêmes entiers sommés dans des ordres différents. Les entiers qui apparaissent dans la décomposition ne doivent pas être nuls : par exemple la décomposition  $4 = 1 + 1 + 2 + 0 + 0$  est comptée comme étant la même que  $4 = 1 + 1 + 2$  (et que  $4 = 1 + 2 + 1\dots$ ).

**Définition 1.** Une *partition* de  $n \in \mathbb{N}^*$  est une famille d'entiers naturels non nuls  $i_1, \dots, i_r$  vérifiant  $i_1 + i_2 + \dots + i_r = n$  avec  $i_1 \leq \dots \leq i_r$ .

La dernière inégalité est là pour dire qu'on ne tient pas compte de l'ordre des éléments : on peut donc les supposés classés par ordre croissant. La question qui nous intéresse en premier lieu est de savoir combien il existe de telles décompositions de  $n$ . On notera dans toute la suite  $P(n)$  le nombre de partition de  $n \in \mathbb{N}^*$ .

Malheureusement, il n'existe pas de formule explicite pour calculer  $P(n)$ . On a par exemple un théorème pour donner un équivalent de  $P(n)$  à l'infini :

**Théorème 1** (Ramanujan et Hardy).  $P(n) \sim_{n \rightarrow +\infty} \frac{\exp(\pi\sqrt{\frac{2n}{3}})}{4n\sqrt{3}}$

Nous allons voir à présent que ce nombre apparaît à beaucoup d'endroits en algèbre.

### 1. ALGÈBRE LINÉAIRE

On se place dans  $\mathbf{M}_n(\mathbb{C})$ . On rappelle que deux matrices  $A$  et  $B$  sont dites **semblables** si et seulement si il existe  $P \in \mathbf{GL}_n(\mathbb{C})$  telle que  $A = PBP^{-1}$ .

On va s'intéresser aux classes de similitudes, c'est-à-dire aux classes d'équivalences de  $\mathbf{M}_n(\mathbb{C})$  par la relation « être semblable ». On va alors montrer le résultat suivant :

**Théorème 2.** *Le nombre de classes de similitude contenant des endomorphismes nilpotents est  $P(n)$ .*

On rappelle qu'un bloc de Jordan nilpotent de taille  $r$  est une matrice de la forme :

$$J_{r,0} = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix}$$

- (1) Montrer que la relation « être semblable » est une relation d'équivalence.
- (2) Soit  $f$  un endomorphisme de  $\mathbb{C}^n$ . Montrer que si  $f$  est semblable à un endomorphisme nilpotent  $\nu$ , alors  $f$  est nilpotent.
- (3) Soit  $M \in \mathbf{M}_n(\mathbb{C})$  une matrice nilpotente. Donner la décomposition de Jordan de  $M$ . Que pensez-vous de la réciproque de la question précédente ?
- (4) En raisonnant sur la taille des blocs de Jordan dans la décomposition de  $M$ , en déduire le théorème.

Un peu hors de propos, mais un résultat à connaître :

- (5) **(Question Bonus)** Montrer que deux matrices  $M$  et  $N$  sont semblables si et seulement si elles ont même décomposition de Jordan.

## 2. PERMUTATIONS

On note  $S_n$  le groupe symétrique d'ordre  $n$ . Nous allons voir que  $P(n)$  est le nombre de classes de conjugaison de  $S_n$ .

- (6) Rappeler ce qu'est la classe de conjugaison d'une permutation  $\sigma \in S_n$ .
- (7) Montrer que le nombre de classes de conjugaison de  $S_n$  est  $P(n)$ .

## 3. GROUPES ABÉLIENS FINIS

Le but de cette section va être de voir que le nombre de groupes abéliens finis d'un cardinal donné à isomorphisme près est  $P(n)$ .

- (8) Soit  $G$  un ordre cyclique d'ordre  $n$ . Montrer que  $G \cong \mathbb{Z}/n\mathbb{Z}$ .

Dans cette partie, on admettra le théorème de structure des groupes abéliens de type fini. Dans la section suivante, on démontrera une version un peu plus faible du théorème (quand  $G$  est fini).

**Théorème 3.** *Soit  $G$  un groupe abélien engendré par un nombre fini d'éléments. Il existe une unique suite d'entiers  $d_1, d_2, \dots, d_p$ , avec  $d_i \mid d_{i+1}$ , et un unique entier  $s \in \mathbb{N}$  tels que*

$$G \cong \mathbb{Z}^s \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_p\mathbb{Z}.$$

- (9) Montrer que si  $G$  est fini, alors nécessairement  $s = 0$ .

Donnons la décomposition de  $n$  en facteurs premiers. Il existe  $p_1, \dots, p_r$  des nombres premiers distincts et  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$  des entiers tels que

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

- (10) Nous allons montrer que le nombre de groupes abéliens d'ordre  $n$  à isomorphisme près vaut  $P(\alpha_1) \cdots P(\alpha_r)$ .
- (a) Montrer le résultat dans le cas où  $r = 1$ .
- (b) Si  $r \geq 2$ , considérer une partition  $\{\beta_{i,j}\}_{j=1}^{s_i}$  de chaque exposant  $\alpha_i$ . Rajouter alors des 0 au début des partitions pour qu'elles aient toutes la même taille  $s = \max_{i=1,\dots,r}(s_i)$ . Considérer alors  $d_j = p_1^{\beta_{1,j}} \cdots p_r^{\beta_{r,j}}$  pour  $j \in \{1, \dots, s\}$  et conclure.
- (11) Déterminer tous les groupes abéliens d'ordre 250 à isomorphisme près.

#### 4. STRUCTURE DES GROUPES ABÉLIENS FINIS

Le but de cette partie est de démontrer le théorème 3 dans le cas où  $G$  est fini, puisque l'on s'en est servi dans la partie précédente. Pour cela, nous allons d'abord définir l'exposant d'un groupe, les caractères d'un groupe et dévisser un sous-groupe de  $G$  par rétraction.

**4.1. Exposant d'un groupe.** Soit  $G$  un groupe abélien fini d'ordre  $n$ . On appelle l'**exposant** d'un groupe  $G$  le plus petit commun multiple des ordres de ses éléments. On va montrer que l'exposant de  $G$  est atteint, i.e.

$$\exists h \in G, o(h) = \text{ppcm}_{g \in G} o(g).$$

Donnons la décomposition de  $n$  en facteurs premiers. Il existe  $p_1, \dots, p_r$  des nombres premiers distincts et  $\alpha_1, \dots, \alpha_r \in \mathbb{N}$  des entiers tels que

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

- (12) Pourquoi la forme de l'ordre d'un élément  $g \in G$  quelconque est  $\prod_{i=1}^r p_i^{\gamma_i}$  ?
- (13) Pour tout  $i$ , on va considérer parmi les éléments d'ordre  $p_i$ , un élément  $h_i$  telle que cette puissance soit maximale, disons  $o(h_i) = p_i^{\beta_i}$ . On pose alors

$$h_0 = h_1 \cdots h_r.$$

Quel est l'ordre de  $h_0$  ?

- (14) Vérifions que cet élément convient. Soit un élément  $g$  d'ordre  $\prod_{i=1}^r p_i^{\gamma_i}$ . De quel ordre est  $g^{\prod_{i=1, i \neq j}^r p_i^{\gamma_i}}$  pour  $j \in \{1, \dots, r\}$  ? Conclure.

**4.2. Dévissage de groupes à l'aide d'une rétraction.** Soit  $H$  un sous-groupe d'un groupe  $G$  abélien et  $\rho: G \rightarrow G$  une **rétraction** de  $G$  sur  $H$ , i.e. un morphisme vérifiant

$$\begin{cases} \rho|_H = \text{id}_H \\ \rho(G) \subset H \end{cases}$$

On notera  $\pi: G \rightarrow G/H$  la projection canonique. On va montrer que le morphisme

$$\begin{aligned} \pi \times \rho: G &\longrightarrow G/H \times H \\ g &\longmapsto (\pi(g), \rho(g)) \end{aligned}$$

est bijectif.

- (15) Montrer l'injectivité.

- (16) Soient  $g' \in G$  et  $h' \in H$ . On cherche un  $g \in G$  tel que  $\pi \times \rho(g) = (\pi(g'), h')$ . Montrer par équivalence que

$$\begin{cases} \pi(g) = \pi(g') \\ \rho(g) = h' \end{cases} \iff \begin{cases} g = hg' \\ h = \frac{h'}{\rho(g')} \end{cases}$$

et conclure.

- (17) La propriété  $G \cong G/H \times H$  est très alléchante d'un point de vue formel, mais n'est pas du tout vraie en général. Expliciter un contre exemple.

**4.3. Prolongement des caractères.** On appelle **caractère** d'un groupe  $G$  tout morphisme de groupes  $\chi: G \rightarrow \mathbb{C}^*$ .

On va montrer que si  $G$  est un groupe abélien fini et  $H$  un sous-groupe de  $G$ , alors tout caractère de  $H$  se prolonge en un caractère de  $G$ .

- (18) On va essayer de prolonger  $\chi$  petit à petit, en rajoutant à  $H$  un élément  $a \notin H$ . Si l'on y parvient, il suffira de répéter l'opération pour conclure. Qu'est-ce qui assure que le procédé est assuré de terminer ?
- (19) On veut donc prolonger  $\chi$  à  $\langle H, a \rangle$  (le sous-groupe engendré par  $H$  et  $a \notin H$ ).
- (a) Pourquoi existe-t-il un ordre  $n$  de  $a$  tel que  $a^n \in H$  ?
- (b) Soit  $\alpha \in \mathbb{C}^*$  tel que  $\alpha^n = \chi(a^n)$ . Posons alors, pour tous  $r \in \mathbb{Z}$  et  $h \in H$ ,

$$\bar{\chi}(ha^r) = \chi(h)\alpha^r$$

Sous cette forme, il est clair que  $\bar{\chi}$  prolonge  $\chi$ , mais rien n'affirme que la formule ci-dessus est valide. Soient deux écritures  $ha^r = h'a^{r'}$  d'un même élément dans  $\langle H, a \rangle$ , on veut montrer que

$$\chi(h')\alpha^{r'} = \chi(h)\alpha^r.$$

- (i) Montrer que  $ha^r = 1 \Rightarrow \chi(h)\alpha^r = 1$ .
- (ii) En déduire le résultat.

**4.4. Structure des groupes abéliens finis.** Soit  $G$  un groupe abélien fini. À l'aide des trois parties précédentes, on va montrer que  $G$  est isomorphe à un produit de  $\mathbb{Z}/d_i\mathbb{Z}$  avec les relations de divisibilité  $d_i \mid d_{i+1}$  et unicité de tels  $d_i$  :

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

*Existence.*

- (20) Si le résultat à montrer est juste, quel est l'exposant de  $G$  (en fonction des  $d_i$ ) ?
- (21) On peut voir l'amorce d'une récurrence en dévissant successivement  $G$  à l'aide des  $\mathbb{Z}/d_i\mathbb{Z}$ . Le point délicat est donc d'exhiber la rétraction. Soit  $a \in G$  d'ordre  $e$  l'exposant de  $G$ .
- (a) Pourquoi  $a$  existe-t-il ?
- (b) Pourquoi  $H$  est-il isomorphe au groupe  $\mu_e$  des racines  $e$ -ièmes de l'unité ? On notera  $\chi: H \rightarrow \mu_e$  cet isomorphisme.
- (c) Montrer qu'il existe un caractère  $\bar{\chi}: G \rightarrow \mathbb{C}^*$ . Déterminer  $\text{Im}(\bar{\chi})$ .
- (d) Vérifier qu'alors  $\chi^{-1} \circ \bar{\chi}$  est une rétraction de  $G$  sur  $H$ .

(e) On en déduit donc un dévissage

$$G \cong G/H \times H \cong G' \times \mathbb{Z}/e\mathbb{Z}$$

où  $G' = G/H$ . Pour conclure de la récurrence, vérifiez que l'exposant  $e'$  de  $G'$  divise  $e$ .

(22) Conclure.

*Unicité.* L'unicité est essentiellement une affaire de combinatoire.

(23) Pour tous  $a, b \in \mathbb{Z}$ , montrer l'isomorphisme suivant :

$$a(\mathbb{Z}/b\mathbb{Z}) \cong \mathbb{Z}/(b/\text{pgcd}(a, b))\mathbb{Z}.$$

(24) Supposons à présent que  $G$  se décompose de deux manières

$$\prod_{i=1}^m \mathbb{Z}/c_i\mathbb{Z} \cong G \cong \prod_{j=1}^n \mathbb{Z}/d_j\mathbb{Z}$$

avec les divisibilités  $c_i \mid c_{i+1}$  et  $d_j \mid d_{j+1}$ .

(a) Montrer que

$$\prod_{i=1}^m \mathbb{Z}/(c_i/\text{pgcd}(d_1, c_i))\mathbb{Z} \cong \prod_{j=1}^n \mathbb{Z}/(d_j/d_1)\mathbb{Z}.$$

(b) Pourquoi  $\prod_{i=1}^m c_i = \prod_{j=1}^n d_j$ ? En déduire en prenant le cardinal de ce qui précède que

$$d_1^n = \prod_{i=1}^m \text{pgcd}(c_i, d_1)$$

et donc que  $n \leq m$ . On a donc  $n = m$  par symétrie.

(c) En déduire que  $\text{pgcd}(c_1, d_1) = d_1$ , d'où  $c_1 = d_1$ .

(d) Conclure.