Université Paris Sud — Année 2019–2020

L3/S6 M305 — Algèbre II

TD n° IV

Facteurs invariants et bases adaptées

Exercice A : (Décomposition canonique des p-groupes abéliens)
Soit p un nombre premier, et G un p-groupe abélien de cardinal p^k $k \in \mathbb{N}^*$.

1) Rappeler pourquoi il existe $r \in \mathbb{N}$ et $a_{k\ ,1 \leq k \leq r}$ tels que

$$G \cong \mathbb{Z}/p^{a_1} \times \ldots \times \mathbb{Z}/p^{a_r} \text{ et } \forall 1 \leq k \leq r-1,\ a_{k+1} \leq a_k \ .$$

On dira que G admet une « décomposition canonique » $(r, a_{k\ ,1\leq k\leq r})$.
On notera

$$\underline{p} : G \to G \ , \ x \mapsto p \cdot x$$

la multiplication par p dans G. On suppose désormais que G a deux décompositions canoniques

$(r, a_{k\ ,1\leq k\leq r})$ et $(s, b_{k\ ,1\leq k\leq s})$, (r **n'étant pas nécessairement égal à** s .)

Soient

$$u := \#\big(\{i \in [1;r] \ ; \ a_i = 1\}\big) \text{ et } v := \#\big(\{i \in [1;s] \ ; \ b_i = 1\}\big) \ .$$

2) Montrer que $\#(\operatorname{Im} \underline{p}) < \#(G)$.

3) Écrire des décompositions canoniques de $\operatorname{Im} \underline{p}$ données par $(r, a_{k\ ,1\leq k\leq r})$ et $(s, b_{k\ ,1\leq k\leq s})$.

4) Montrer que

$$p^u \cdot \prod_{1 \leq i \leq r, a_i > 1} p^{a_i} = p^v \cdot \prod_{1 \leq i \leq w, b_i > 1} p^{b_i} \ .$$

5) Montrer finalement par récurrence sur $\#(G)$ qu'un p-groupe abélien G possède une unique décomposition canonique.

Exercice B : (Décomposition canonique pour un groupe abélien fini quelconque)
Soit G un groupe abélien fini.

1) Rappeler pourquoi il existe

$$r \in \mathbb{N} \text{ et } n_{k\ ,1\leq k\leq r} \text{ tels que } G \cong \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_r \ , \ \forall 1 \leq k \leq r-1,\ n_k | n_{k+1} \ .$$

On dit alors qu'on a une décomposition canonique de G : $(r, n_{k\ ,1\leq k\leq r})$.
Dans la suite, on suppose donnée une décomposition canonique $(r, n_{k\ ,1\leq k\leq r})$ **pour** G.

2) Soit p un nombre premier tel que $p|n_1$ ($v_p(n_1) > 0$.) Montrer que l'entier r peut être caractérisé en terme de la décomposition canonique du p-groupe $G[p^\infty]$ et utiliser les résultats de l'exercice A pour montrer que r ainsi que les $v_p(n_k)_{\ ,1 \leq k \leq r}$ sont uniquement déterminés par G.

3) En déduire l'unicité d'une décomposition canonique pour un groupe abélien G fini quelconque.

Exercice C : (Structure des groupes finis(cf. TD n° VIII, exercice A.))

1) Parmi les groupes suivants, lesquels sont isomorphes (vous devez justifier votre réponse) :

$$\begin{aligned} G_1 &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \\ G_2 &= \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_3 &= \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ G_4 &= (\mathbb{Z}/25\mathbb{Z})^\times \times \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

Lesquels sont cycliques ?

2) Combien y a-t-il de classes d'isomorphismes de groupes abéliens de cardinal 1400 et possédant au moins un sous-groupe non cyclique d'ordre une puissance de 2 ? Donner leurs invariants (ou diviseurs élémentaires).

3) Soient r, s et t trois entiers positifs. On désire calculer en fonction de r, s et t les invariants $(d_1, d_2, \ldots, d_k)$ du groupe abélien

$$A \;:=\; \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/t\mathbb{Z}\ .$$

a) Que vaut d_1 ?

b) Calculer de deux manières le nombre d'éléments d'ordre divisant d_k et montrer que $k \leq 3$ et que d_3 est le **Pgcd** de r, s et t.

c) Montrer que

$$d_2 \;=\; \mathrm{PPCM}\big((r \wedge s), (s \wedge t), (t \wedge r)\big)\ .$$

4) Montrer que si A et B sont des groupes abéliens finis et

$$A \times A \;\cong\; B \times B, \text{ alors } \;\cong\; AB\ .$$

Exercice D : Soient

$$v_1 \;:=\; (1, 4, 2, 5)\ ,\ v_2 \;:=\; (3, 7, 11, 6)\ ,\ v_3 \;:=\; (4, 13, 10, 2)\ ,\ v_4 \;:=\; (5, 11, 9, 7)$$

des éléments de $\mathbb{Z}^4$.

Déterminer le sous-groupe A de $\mathbb{Z}^4$ engendré par les éléments $v_{i\ ,1\leq i\leq 4}$ c'est-à-dire donner une base adaptée pour A.

Exercice E : Déterminer à isomorphisme près les groupes abéliens de cardinal 300.

Exercice F : Cet exercice reprend les étapes de l'étude des sous-groupes d'un groupe abélien libre de type fini de manière effective.

Soit A le groupe abélien libre $\mathbb{Z}^2$ et B le sous-groupe de A engendré par les éléments $b_1 = (-4, 12)$ et $b_2 = (-8, 12)$. On désire calculer les facteurs invariants (diviseurs élémentaires) de A/B.

1) Donner un homomorphisme f de A dans $\mathbb{Z}$ tel que l'image de B soit maximale.

2) On note d un générateur de $f(B)$. Donner un élément a_2 de A tel que da_2 soit dans B et tel que $f(a_2) = 1$.

3) Calculer une base a_1 du noyau de f. Calculer l'intersection B' du noyau de f avec B et exprimer un générateur de B' d'une part en fonction de a_1 et d'autre part dans le système générateur de B.

4) Calculer les facteurs invariants de A/B.

Exercice G : **1)** Soit $A = \mathbb{Z}^2$ et B le sous-groupe de A engendré par $b_1 = (14, 2)$ et $b_2 = (2, 4)$. Calculer une base de A adaptée à B. Donner la structure du quotient A/B.

2) Soit G un groupe abélien (noté additivement) et possédant deux générateurs a et b tels que $14a+2b = 0_G$ et $2a+4b = 0_G$. Montrer que G est isomorphe à un quotient d'un groupe d'ordre 52 dont on donnera la structure.

Exercice H : Soit $e_1 = (a_1, \ldots, a_n)$ un élément de $\mathbb{Z}^n$ tel que le pgcd des a_i vaille 1. Montrer qu'il existe une base $(e_1, \ldots, e_n)$ de $\mathbb{Z}^n$ dont le premier vecteur est e_1. Que peut-on dire du quotient $\mathbb{Z}^n/\mathbb{Z}e_1$?

Adapter l'exercice en ne supposant plus que le pgcd vaut 1.