UNIVERSITÉ DE LORRAINE L3 Mathématiques – Site Nancy, S5 – 2021/22

Algèbre 2 – Feuille 4

Décomposition des groupes abéliens finis

Exercice 1. Pour les groupes suivants, déterminer la décomposition primaire, calculer le type, puis la décomposition cyclique.

(a) $G = (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$.
(b) $G = (\mathbb{Z}/84\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$.
(c) $G = (\mathbb{Z}/40\mathbb{Z}) \times (\mathbb{Z}/42\mathbb{Z}) \times (\mathbb{Z}/120\mathbb{Z})$.

Solution de l'exercice 1. Suivre l'exemple 5.6(1) du chapitre 3 (pages 10-11)

(a) Le groupe $G = \mathbb{Z}_{12} \times \mathbb{Z}_{90}$ est abélien et d'ordre $12 \times 90 = 2^3 \cdot 3^3 \cdot 5$. D'où sa décomposition primaire $G = G_2 \times G_3 \times G_5$.

La composante primaire G_2 associé au facteur premier 2 est un sous-groupe d'ordre $2^3 = 8$, donné par

$$G_2 \quad = \{(\bar{k}, \tilde{h}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{90} \mid 2^3(\bar{k}, \tilde{h}) = (\bar{0}, \tilde{0})\}$$

Or,

$$\left\{\begin{array}{ll} 2^3k & \equiv 0[12 = 2^2 \cdot 3] \\ 2^3h & \equiv 0[90 = 3^3 \cdot 2 \cdot 5] \end{array}\right. \iff \left\{\begin{array}{ll} 2k & \equiv 0[3] \\ 2^2h & \equiv 0[45] \end{array}\right. \iff \left\{\begin{array}{ll} k & \equiv 0[3] \\ h & \equiv 0[45] \end{array}\right.$$

Donc

$$G_2 = 3\mathbb{Z}/12\mathbb{Z} \times 45\mathbb{Z}/90\mathbb{Z} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2.$$

On montre de même que la composante primaire G_3 associée au facteur premier 3 est

$$G_3 = 4\mathbb{Z}/12\mathbb{Z} \times 10\mathbb{Z}/90\mathbb{Z} \simeq \mathbb{Z}_3 \times \mathbb{Z}_9.$$

Enfin, la composante primaire G_5 est

$$G_5 = 12\mathbb{Z}/18\mathbb{Z} \times 18\mathbb{Z}/90\mathbb{Z} \simeq \{\bar{0}\} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z}$$

On peut prévoir ce résultat, car G_5 est un groupe cyclique d'ordre premier 5, donc isomorphe à $\mathbb{Z}_5$. Ainsi

$$\mathbb{Z}_{12} \times \mathbb{Z}_{90} \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_9) \times \mathbb{Z}_5$$

Or un produit de deux groupes cycliques d'ordres premiers entre eux est un groupe cyclique. On va donc regrouper les différents groupes cycliques de la décomposition précédente pour former une décomposition cyclique :

$$\begin{aligned} G &\simeq (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5) \\ &\simeq \mathbb{Z}_6 \times \mathbb{Z}_{180} \quad \text{avec } \ 6|180 \end{aligned}$$

Ainsi $\mathbb{Z}_6 \times \mathbb{Z}_{180}$ est la décomposition cyclique de $\mathbb{Z}_{12} \times \mathbb{Z}_{90}$ et $(6, 180)$ est sa suite des invariants.

On fait de même pour les question (b) et (c).

Exercice 2. Donner la décomposition primaire du groupe abélien $\mathbb{Z}/851\mathbb{Z}$. En déduire la structure du groupe $Aut(\mathbb{Z}/851\mathbb{Z})$.

Solution de l'exercice 2. La décomposition primaire de 851 et $851 = 23 \times 37$. Donc d'après le théorème chinois, $\mathbb{Z}_{851} \simeq \mathbb{Z}_{23} \times \mathbb{Z}_{37}$.

On en déduit que $Aut(\mathbb{Z}_{851}) \simeq Aut(\mathbb{Z}_{23}) \times Aut(\mathbb{Z}_{37})$. Or si p est premier, $Aut(\mathbb{Z}/p\mathbb{Z})$ est un groupe cyclique isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. Donc $Aut(\mathbb{Z}_{851}) \simeq \mathbb{Z}_{22} \times \mathbb{Z}_{36}$. La décomposition cyclique de ce groupe est (voir exercice 6)

$$\begin{aligned} Aut(\mathbb{Z}_{851}) &\simeq \mathbb{Z}_{22} \times \mathbb{Z}_{36} \\ &\simeq \mathbb{Z}_{\mathrm{pgcd}(22,36)} \times \mathbb{Z}_{\mathrm{ppcm}(22,36)} \\ &\simeq \mathbb{Z}_2 \times \mathbb{Z}_{396} \end{aligned}$$

Ainsi $Aut(\mathbb{Z}_{851})$ est un groupe abélien fini d'invariant $(2, 396)$.

Exercice 3. Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre :

(a) 600.
(b) 720.
(c) 3240.

Solution de l'exercice 3. (c) Déterminons tous les groupes abéliens d'ordre 3240.

Si G est un groupe abélien d'ordre $3240 = 2^3 \cdot 3^4 \cdot 5$, alors sa décomposition primaire est $G = G_2 \times G_3 \times G_5$, où G_2, G_3 et G_5 sont les composantes primaires associé aux facteurs premiers 2, 3 et 5.

$|G_2| = 2^3$ et 3 admet trois partitions qui sont (3), $(1, 2)$ et $(1, 1, 1)$. Donc G_2 est isomorphe à l'un des groupes

$$\begin{array}{l} \mathbb{Z}_{2^3} \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \end{array}$$

$|G_3| = 3^4$ et 4 admet cinq partitions qui sont (4), $(1,3)$, $(2,2)$, $(1,1,2)$ et $(1,1,1,1)$. Donc G_3 est isomorphe à l'un des groupes

$$\begin{array}{l} \mathbb{Z}_{3^4} \\ \mathbb{Z}_3 \times \mathbb{Z}_{3^3} \\ \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2} \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \end{array}$$

Enfin G_5 est un groupe d'ordre 5 (donc cyclique), il est isomorphe à

$$\mathbb{Z}_5.$$

Il y a donc au total à isomorphisme près $3 \times 5 \times 1 = 15$ groupes abéliens d'ordre 3240 :

$$\begin{array}{rl} \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_5 & \simeq \mathbb{Z}_{3240} \\ \mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_{3^3}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5) \\ & \simeq \mathbb{Z}_3 \times \mathbb{Z}_{1080} \\ \mathbb{Z}_{2^3} \times (\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_{3^2} \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5) \\ & \simeq \mathbb{Z}_9 \times \mathbb{Z}_{360} \\ \mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2}) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \\ & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{360} \\ \mathbb{Z}_{2^3} \times (\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5 & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_5) \\ & \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{120} \end{array}$$

etc... (à compléter par l'étudiant).

D'où les listes des invariants possible pour G :

$$(2340), (3,1080), (9,360), (3,3,360), (3,3,3,120), etc... \text{ (à compléter par l'étudiant).}$$

On faitd e même pour les question (a) et (b).

Exercice 4. Parmi les groupes suivants, tous abéliens d'ordre 180, déterminer lesquels sont isomorphes entre eux :

$$\begin{array}{ll} (1) & \mathbb{Z}/180\mathbb{Z} \\ (2) & (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z}) \\ (3) & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z}) \\ (4) & (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/20\mathbb{Z}) \\ (5) & (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z}) \\ (6) & (\mathbb{Z}/15\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ (7) & (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \\ (8) & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z}) \\ (9) & (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z}) \\ (10) & (\mathbb{Z}/181\mathbb{Z})^\times \\ (11) & (\mathbb{Z}/19\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \\ (12) & (\mathbb{Z}/209\mathbb{Z})^\times \end{array}$$

Solution de l'exercice 4. Deux groupes de cette liste sont isomorphes s'ils ont la même suite d'invariants.

Un groupe d'ordre $180 = 2^2 \times 3^2 \times 5$ admet trois composantes primaires
G_2 d'ordre 2^2, isomorphe à $\mathbb{Z}_4$ ou à $\mathbb{Z}_2 \times \mathbb{Z}_2$.
G_3 d'ordre 3^2, isomorphe $\mathbb{Z}_9$ ou à $\mathbb{Z}_3 \times \mathbb{Z}_3$.
G_5 d'ordre 5, isomorphe à $\mathbb{Z}_5$.

Donc un groupe abélien d'ordre 180 est isomorphe à l'un des groupes

$$\begin{array}{lll} (A) & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_6 \times \mathbb{Z}_{30} & \text{d'invariants } (6,30) \\ (B) & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{90} & \text{d'invariants } (2,90) \\ (C) & \mathbb{Z}_4 \times \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{60} & \text{d'invariants } (6,30) \\ (D) & \mathbb{Z}_4 \times \times \mathbb{Z}_9 \times \times \mathbb{Z}_5 \simeq \mathbb{Z}_{180} & \text{d'invariant } (180) \end{array}$$

– Le groupe (1) de la liste est d'invariant (180) ;
– Le groupe (2) : (on utilise l'exercice 6) $\mathbb{Z}_{12} \times \mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{60}$ est d'invariants (3,60) ;
– Le groupe (3) : $\mathbb{Z}_2 \times \mathbb{Z}_{90}$ est d'invariants (2,90) ;
– Le groupe (4) : $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{20} \simeq \mathbb{Z}_3 \times \mathbb{Z}_{3\times 20} \times \simeq \mathbb{Z}_3 \times \mathbb{Z}_{60}$ est d'invariants (3,60) ;
– Le groupe (5) : (on utilise le lemme chinois ou exercice 6) $\mathbb{Z}_5 \times \mathbb{Z}_{45} \times \simeq \mathbb{Z}_{5\times 45} \simeq \mathbb{Z}_{180}$ est d'invariant (180) ;
– Le groupe (6) : (on utilise le lemme chinois ou exercice 6) $\mathbb{Z}_{15} \times \mathbb{Z}_6 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{15\times 2} \times \mathbb{Z}_6 \simeq \mathbb{Z}_6 \times \mathbb{Z}_{30}$ est d'invariants (6,30) ;

– Le groupe (7) : $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{2\times 9\times 5} \times \mathbb{Z}_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{90}$ est d'invariants (2,90) ;

– Le groupe (8) : $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{9\times 10} \times \simeq \mathbb{Z}_2 \times \mathbb{Z}_{90}$ est d'invariants (2,90) ;

– Le groupe (9) : $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{4\times 3\times 5} \times \simeq \mathbb{Z}_3 \times \mathbb{Z}_{60}$ est d'invariants (3,60) ;

– Le groupe (10) : puisque 181 est premier, $(\mathbb{Z}_{181})^\times \simeq \mathbb{Z}_{180}$ est d'invariant (180) ;

– Le groupe (11) : puisque 19 et 11 sont premiers, $(\mathbb{Z}_{19})^\times \times (\mathbb{Z}_{11})^\times \simeq \mathbb{Z}_{18} \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{90}$ (par l'exercice 6) est d'invariants (2,90) ;

– Le groupe (12) : $(\mathbb{Z}_{209})^\times = (\mathbb{Z}_{19\times 11})^\times \simeq (\mathbb{Z}_{19})^\times \times (\mathbb{Z}_{11})^\times \simeq \mathbb{Z}_{18} \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{90}$ est d'invariants (2,90).

En conclusion, on a

$$(1) \simeq (5) \simeq (10)$$

$$(2) \simeq (4) \simeq (6) \simeq (9)$$

$$(3) \simeq (7) \simeq (8) \simeq (11) \simeq (12)$$

Exercice 5. Montrer que dans tout groupe abélien d'ordre 40, il y a au moins un élément d'ordre 10.
Existe-t-il un groupe abélien d'ordre 40 dans lequel l'ordre de tout élément divise 10 ?

Solution de l'exercice 5. Pour la première question, utilisez le théorème de Cauchy. Pour le deuxième question, déterminer à iso près les groupes abéliens d'ordre 40 (il y en a trois), puis regardez dans le(s)quel(s) l'ordre de tout élément divise 10.

Exercice 6. (a) Soient $k \geq 2$ et $n \geq 2$ des entiers. Posons $d = \operatorname{pgcd}(k,n)$ et $m = \operatorname{ppcm}(k,n)$.
Montrer que $G = (\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ et c'est, à isomorphisme près, la seule expression de G sous la forme $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$ avec p divisant q (décomposition cyclique, avec (p,q) l'invariant de G).

(b) Application : $G = (\mathbb{Z}/18\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$.

Solution de l'exercice 6. (a) Considérons les décompositions en facteurs premiers de k et de n :

$$k = p_1^{\alpha_1} \cdots p_s^{\alpha_s} q_1^{\beta_1} \cdots q_t^{\beta_t} \quad , \quad n = p_1^{\gamma_1} \cdots p_s^{\gamma_s} r_1^{\delta_1} \cdots r_u^{\delta_u}$$

où $p_1, \ldots, p_s$ sont communs à k et n et où $q_1, \ldots, q_t$ (resp. $r_1, \ldots, r_u$) sont facteurs premiers de k et pas de n (resp. de n et pas de k). Pour $1 \leq i \leq s$, posons

$$\lambda_i = \min(\alpha_i, \gamma_i) \quad , \quad \mu_i = \max(\alpha_i, \gamma_i)$$

On a alors $d = p_1^{\lambda_1} \cdots p_s^{\lambda_s}$ et $m = p_1^{\mu_1} \cdots p_s^{\mu_s} q_1^{\beta_1} \cdots q_t^{\beta_t} r_1^{\delta_1} \cdots r_u^{\delta_u}$. Les composantes primaires de $\mathbb{Z}/k\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}$ sont cycliques (3-3, prop.) donc

$$\mathbb{Z}/k\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}) \times \left(\mathbb{Z}/q_1^{\beta_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/q_t^{\beta_t}\mathbb{Z}\right)$$
$$\mathbb{Z}/n\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\gamma_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\gamma_s}\mathbb{Z}) \times \left(\mathbb{Z}/r_1^{\delta_1}\mathbb{Z}\right) \times \cdots \times (\mathbb{Z}/r_u^{\delta_u}\mathbb{Z})$$
$$\mathbb{Z}/d\mathbb{Z} \simeq \left(\mathbb{Z}/p_1^{\lambda_1}\mathbb{Z}\right) \times \cdots \times (\mathbb{Z}/p_s^{\lambda_s}\mathbb{Z})$$

$$\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\mu_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\mu_s}\mathbb{Z}) \times \left(\mathbb{Z}/q_1^{\beta_1}\mathbb{Z}\right) \times \cdots \times (\mathbb{Z}/r_u^{\delta_u}\mathbb{Z})$$

Pour $1 \leq i \leq s$, le produit $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}) \times (\mathbb{Z}/p_i^{\gamma_i}\mathbb{Z})$ est isomorphe à $\left(\mathbb{Z}/p_i^{\lambda_i}\mathbb{Z}\right) \times (\mathbb{Z}/p_i^{\mu_i}\mathbb{Z})$ car $\{\alpha_i, \gamma_i\} = \{\lambda_i, \mu_i\}$ donc $(\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes. En outre, $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ est l'expression canonique du groupe G et d, m sont ses invariants car $d \mid m$, d'où l'unicité de cette expression de G.

(b) Comme $\operatorname{pgcd}(18,45) = 9$ et $\operatorname{ppcm}(18,45) = 90$, les invariants de $(\mathbb{Z}/18\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$ sont $(9, 90)$.