II . −Structure des groupes abéliens de type fini

II.0 . −Introduction

le but de ce chapitre (II,) est d'établir de manière rigoureuse qu'un groupe abélien est essentiellement constitué d'une partie du type $\mathbb{Z}^r$ et d'une autre qui est un produit de groupes cycliques. Un énoncé précis sera obtenu au théorème II.6.4. il est dès lors nécessaire d'étudier les groupes abéliens libres (de type fini) (cf. II.3.2,) d'une part, et les groupes abéliens de type fini et de torsion (*i.e.* finis,) (cf. II.5.2.vi).) c

Les premiers ressemblent assez à des espaces vectoriels, mais qu'on ne sy 'laisse pas prendre : le théorème II.4.6 semble déjà suffisamment délicat à obtenir pour qu'on puisse douter que la situation de deux groupes abéliens libres inclus l'un dans l'autre soit aussi simple que celle de deux espaces vectoriels emboîtés. De fait le résultat optimal qui pourra être obtenu est celui dit du théorème de la base adaptée (théorème II.11.12 qui est tout de même assez éloigné, de ce qui lui est cependant le plus proche à savoir le théorème de la base incomplète en algèbre linéaire.

Les groupes abéliens de type finni et de torsion recevront quant à eux une description complète en termes des plus élémentaires d'entre eux, à savoir les groupes cycliques, au théorème II.10.5. le résultat en réalité le plus susceptible d'être utilisé dans le paragraphe II.10 est le corollaire II.10.7 qui permet de déterminer quand deux groupes abéliens de type fini sont isomorphes. À noter que le théorème II.8.3 s'il est un ingrédient clef de la construction aboutissant au théorème de structure II.10.5, est déjà un résultat significatif en soi et qui fournit une première description des groupes de torsion. **Dans ce chapitre (II,) les notations suivantes seront couramment utilisées :**

Notation II.0.1 Pour tout $n \in \mathbb{Z}$, on notera $\mathbb{Z}/n\mathbb{Z}$ ou même simplement $\mathbb{Z}/n$ le quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$ et

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n \text{ la surjection canonique.}$$

Notation II.0.2 (Éléments irréductibles, nombres premiers) On notera $\mathbb{P}_{\mathbb{Z}}$ ou simplement $\mathbb{P}$ l'ensemble des nombres premiers *i.e.* l'ensemble des éléments irréductibles de $\mathbb{Z}$ contenus dans $\mathbb{N}^*$.

Notation II.0.3 (Valuations p-adiques) Pour tout nombre premier

$$p \in \mathbb{P} \text{ et tout entier relatif } a \in \mathbb{Z}, \text{ on note } v_p(a)$$

sa *valuation p-adique* définie comme en I.13.5.5. On note encore

$$\mathcal{S}(a) := \{p \in \mathbb{P} \,;\, v_p(a) \neq 0\}$$

dont on rapelle que c'est un ensemble fini.

Notation II.0.4 (Décomposition en produit d'irréductibles) Pour tout $a \in \mathbb{Z} \setminus \{0\}$, on a

$$a = u \prod_{p \in \mathbb{P}} p^{v_p(a)} = \prod_{p \in \mathcal{S}(a)} p^{v_p(a)}, \; u \in \mathbb{Z}^\times, \textit{i.e. } u = \pm 1 \text{ (cf. I.13.5.3 ;)}$$

le produit ci-dessus étant en fait fini puisque $v_p(a) \neq 0$ pour un nombre fini de $p \in \mathbb{P}$ seulement.

II.1 . −Groupes abéliens de type fini

Dans ce paragraphe (II.1,) A **est un anneau commutatif.**

Rappel II.1.1 (Partie génératrice) Pour un groupe abélien $(X,+)$ (resp. un A-module $(X,+,\cdot),$) un sous-ensemble $S \subset X$ est une *partie génératrice* (cf. I.4.2 (resp. A.4.2,)) si $X = < S >$. On dit alors que X est *engendré* par S.

Remarque II.1.2 Pour un groupe abélien X, et $S \subset X$, il est équivalent de dire que X est engendré par S en tant que groupe abélien ou en tant que $\mathbb{Z}$-module.

Lemme II.1.3 *Soient X un groupe abéliens (resp. A-module.)*

i) Un morphisme de groupes abéliens (resp. A-modules,) $f : X \to Y$ est surjectif si et seulement s'il existe une partie S de X telle que $f(S)$ est une partie génératrice de Y ; si et seulement si l'image par f de toute partie génératrice de X est une partie génératrice de Y.

ii) Toute partie T de X contenant une partie génératrice S est génératrice.

Exemple II.1.4 a) Le groupe abélien $\mathbb{Z}$ est engendré par $\{1\}$ ou $\{-1\}$.

b) L'anneau A lui-même vu comme A-module comme en A.1.2.b) engendré par $\{1\}$ ou par $\{u\}$ pour tout $u \in A^\times$.

c) Plus généralment, pour tout entier $n \in \mathbb{N}$, le groupe abélien (resp. A-module,) $\mathbb{Z}^n$ (resp. A^n,) (cf. I.7,) est engendré par la famille $\varepsilon_i\ ,1\leq i\leq n$ où

$$\varepsilon_i = (0,\dots,0,1,0,\dots,0) \text{ ou encore } \varepsilon_i(j) = \delta_i^j\ \forall 1\leq i\leq n,\ \forall 1\leq j\leq n,\ .$$

d) Dans l'anneau $A[X]$ des polynômes à une indéterminée et à coefficients dans A,

$$\text{la famille } X^n\ ,n\in\mathbb{N}$$

est une famille génératrice (cf. III.2.5.v).a).)

Définition II.1.5 (Groupe abélien (resp. Module) de type fini) Un groupe abélien (resp. A-module,) X est *de type fini* s'il possède une partie génératrice finie.

Exemple II.1.6 a) On constate sur l'exemple II.1.4.a) que $\mathbb{Z}$ est un groupe abélien de type fini et sur l'exemple II.1.4.b) que A est un A-module de type fini. De même l'exemple II.1.4.c) montre que $\mathbb{Z}^n$ (resp. A^n,) est un groupe abélien (resp. un A-module) de type fini.

b) En revanche la famille $X^n\ ,n\in\mathbb{N}$ de $A[X]$ n'est pas finie. On pourrait cependant se demander s'il n'existe pas une famille génératrice finie du A-module $A[X]$ (que A soit un corps $\mathbb{K}$ ou non.) L'exercice A.8.4 apporte une réponse à cette question.

Définition II.1.7 (Groupe monogène) Pour X un groupe abélien (resp. A-module,) et $x \in X$, le sous-groupe (resp. sous- A-module,)

$$< \{x\} > = \{a \cdot x \ , \ a \in \mathbb{Z} \text{ (resp. } A)\} \, ,$$

engendré par $\{x\}$ est usuellement noté

$$\mathbb{Z} \cdot x \text{ (resp. } A \cdot x, \text{)}$$

ou même simplement

$$\mathbb{Z}x \text{ (resp. } Ax \text{ .)}$$

En particulier pour $a \in A$, l'idéal engendré par $\{a\}$ est noté Aa. Cette notation rappelle celle utilisée pour les $\mathbb{K}$-espaces vectoriels et qui consiste à noter $\mathbb{K}v$ la droite engendrée par le vecteur v.

Si $X = < \{x\} >$ on dit que X est *monogène*.

Lemme II.1.8 *Étant donnés un groupe abélien (resp. un A-module,) X, un entier $n \in \mathbb{N}^*$ et un n-uplet $x_{i \ ,1 \leq i \leq n} \in X$ d'éléments de X, il existe un morphismes de groupes (resp. de A-modules,)*

$$\phi \ : \ \mathbb{Z}^n (\text{resp. } A^n) \ \to \ X \ , \ \varepsilon_i \ \mapsto \ x_i$$

(où les éléments $\varepsilon_{i \ ,1 \ \leq \ i \ \leq \ n}$ sont les éléments introduits en II.1.4.c).) La généralisation de ce lemme donnée en II.2.10 assure même que ϕ est unique.

Preuve *: Si un tel morphisme existe,*

$$\forall a_{i \ ,1 \leq i \leq n} \in \mathbb{Z}^n (\text{resp. } A^n), \ \phi\big(\sum_{i=1}^{n} a_i \varepsilon_i\big) \ = \ \sum_{i=1}^{n} a_i \cdot x_i \ .$$

Il est tout à fait élémentaire de voir que cette formule définit bien un morphisme.

Proposition II.1.9 *Étant donné un groupe abélien (resp. A-module,) X, les assertions suivantes sont équivalentes :*

a) X est de type fini.

b) Il existe un entier $r \in \mathbb{N}$, et un morphisme surjectif

$$p \ : \ \mathbb{Z}^r (\text{resp. } A^r) \ \to \ X \ .$$

c) Il existe un groupe abélien (resp. A-module,) de type fini Y et un morphisme surjectif $p \ : \ Y \ \to \ X$.

Preuve *:*

*i) (**a**) $\Rightarrow$ **b**))*

Si X est de type fini, il possède une partie génératrice fini $S := \{s_1, \ldots, s_r\}$. Il existe alors, en vertu du lemme II.1.8 un morphisme de groupes (resp. A-modules,)

$$\phi \ : \ A^r \ \to \ X \ , \ \varepsilon_i \ \mapsto \ s_{i \ ,1 \ \leq \ i \ \leq \ r}$$

(où ε_i) et défini comme dans l'exemple II.1.4.c). Il résulte alors du lemme II.1.3.i), que ϕ est surjectif.

ii) ***(b)*** $\Rightarrow$ ***c))***
(cf. II.1.4.c).)

iii) ***(c)*** $\Rightarrow$ ***a))***
Si Y est de type fini, il existe une partie génératrice finie S de Y. Si $p : Y \to X$ est un morphisme surjectif, il résulte du lemme II.1.3.i) que $p(S)$ est une partie génératrice de X finie qui plus est.

Remarque II.1.10 On constate avec la proposition ci-dessus qu'il est presque tautologique qu'un quotient d'un groupe abélien
(resp. A-module,) de type fini est de type fini mais qu'on n'a rien affirmé concernant les sous-groupes (resp. sous-A-modules.) Ceci semble d'autant plus contre intuitif qu'on sait depuis longtemps que la dimension est croissante pour les $\mathbb{K}$-espaces vectoriels. Des résultats positifs seront cependant exposés au paragraphe II.4.

Proposition II.1.11 *Étant donné deux groupes abéliens (resp. A-modules,) de type fini X_1 et X_2,*

i) le groupe abélien (resp. A-module,) $X_1 \times X_2$ est de type fini ;

ii) si X_1 et X_2 sont des sous-groupes (resp. sous-A-modules,) d'un groupe abélien (resp. A-module,) X tels que $X = X_1 + X_2$, X est de type fini ;

iii) si X est un groupe abélien (resp. A-module,) tel qu'il existe une suite exacte

$$0 \to X_1 \xrightarrow{i} X \xrightarrow{p} X_2 \to 0$$

X est de type fini.

Preuve *: Étant donnée une partie génératrice finie de X_2, on note X_2 un ensemble de relèvement de ces générateurs dans X. Alors X_2 est une partie finie de X, et si l'on note $Y_2 := < X_2 >$ le sous-groupe (resp. sous- A-moduled)e X engendré par X_2, tout élément de X_2 possède un relèvement dans Y_2. Ainsi, pour tout $x \in X$, $p(x)$ possède un relèvement $y \in Y_2$. Il en résulte que*

$$p(x - y) = p(x) - p(y) = 0,$$

c'est-à-dire que $x - y \in i(X_1)$.
Il s'ensuit que $X = Y_2 + i(X_1)$ (cette somme n'ayant aucune raison d'être directe en général.)
Il suffit donc d'aplliquer le point ii).

II.2 . −Groupes abéliens (resp. A-modules) libres

Définition II.2.1 (Famille libre) Une partie $L \subset X$ d'un groupe abélien (resp. A-module,) est *libre* si, pour tout entier n, tout n-uplet $\lambda_{i\ ,1\leq i\leq n} \in L$ d'éléments deux à deux distincts de L, tout n-uplet $a_{i\ ,1\leq i\leq n}$ d'éléments de $\mathbb{Z}$ (resp. A,)

$$\sum_{i=1}^{n} a_i\lambda_i \ = \ 0 \ \Rightarrow \ \forall 1 \leq i \leq n,\ a_i \ = \ 0\ .$$

Remarque II.2.2 Dans la définition II.2.1 ci-dessus, il revient au même de dire que

$$< L > = \sum_{\lambda \in L} \mathbb{Z} \cdot \lambda (\text{resp. } A \cdot \lambda) \text{ est une somme directe (cf. I.4.8.ii) (resp. A.4.6.ii).))}$$

Lemme II.2.3 *Soit X un groupe abélien (resp. A-module.)*

i) si $f : X \to Y$ est un morphisme injectif de groupe abéliens (resp. A-modules) l'image de toute partie libre de X est une partie libre de Y.

ii) Pour toute partie libre L de X tout sous-ensemble de L est libre.

Exemple II.2.4 Dans l'anneau $A[[X]]$ (cf. III.1,) (ainsi d'ailleurs que dans le groupe abélien (resp. A-module,) $A[X]$,) la famille $X^{n}{}_{,n\ \in\ \mathbb{N}}$ est libre.

Définition II.2.5 (Base) Une partie $\mathcal{B}$ d'un groupe abélien (resp. A-module,) X est une *base* de X si c'est une partie libre et génératrice.

Exemple II.2.6 a) Dans les exemples II.1.4.b) à II.1.4.d) les partie génératrices qu'on a mises en évidence sont en fait des bases.

b) Si $A = \mathbb{Z}x = < x >$ est un groupe monogène (cf. II.1.7,) $\{x\}$ est tautologiquement une partie génératrice de A, cependant, contrairement à ce qui se passe dans le cas des espaces vectoriels, il ne suffit pas que $x \neq 0$ pour que x soit une base de A. Les paragraphes II.5 et A.7 précisent cette question en introduisant la notion d'éléments *de torsion*.

Si $X = x_{i\ ,1\leq i\leq r}$ est une partie finie de X, le sous-groupe (resp. sous- A-module,) $< X >$ de X engendré par X est (cf. I.4.8(resp. A.4.6,))

$$< X > = \sum_{i=1}^{r} A \cdot x_i\ .$$

Là encore il est difficile de donner, en toute généralité, des conditions dans lesquelles cette somme est directe.

Remarque II.2.7 La définition d'une base donnée ci-dessus n'est en rien différente de celle donnée pour les $\mathbb{K}$-espaces vectoriels. Plus précisément encore, une base d'un $\mathbb{K}$-espace vectoriel E est une base de E en tant que $\mathbb{K}$-module.

Si, comme nous allons le voir, les bases des groupes abéliens (resp. A-modules) bénéficient de bonnes propriétés, leur plus grand défaut est, contrairement à la situation rencontrée pour les $\mathbb{K}$-espaces vectoriels, de ne pas toujours exister. Dans le groupe abélien ($\mathbb{Z}$-module) $\mathbb{Z}/n\mathbb{Z}$, par exemple, $n\cdot\alpha = 0$ pour tout $\alpha \in \mathbb{Z}/n\mathbb{Z}$. Aucune famille de $\mathbb{Z}/n\mathbb{Z}$ n'est donc libre.

Certains groupes abéliens (modules,) ne possédant donc pas de base, on est motivé à donner la définition suivante :

Définition II.2.8 (Groupe abélien (resp. A-module,) libre) On dira qu'un groupe abélien (resp. A-module,) X est *libre* s'il admet une base.

Pour un groupe abélien il revient au même d'être libre au sens ci-dessus ou d'être libre en tant que $\mathbb{Z}$-module.

Exemple II.2.9 Ainsi les modules considérés dans les exemples II.1.4.b) à II.1.4.d) sont des modules libres.

Bien entendu, si $\mathbb{K}$ est un corps un $\mathbb{K}$-espace vectoriel est un $\mathbb{K}$-module libre.

Lemme II.2.10 *Étant donné un groupe abélien (resp. A-module,) X possédant une base $\mathcal{B} := \beta_{i\,,1\leq i\leq n}$, pour tout groupe abélien (resp. A-module,) Y et tout n-uplet $\gamma_{i\,,1\leq i\leq n} \in Y$ d'éléments de Y, il existe un unique morphisme de groupes (resp. A-modules,)*

$$\phi \,:\, X \,\to\, Y\,,\ \beta_k i \,\mapsto\, \gamma_{i\,,1\leq i\leq n}\ .$$

Preuve *: Pour tout $x \in X$, il existe, puisque $\mathcal{B}$ est une base de X, $a_{i\,,1\leq i\leq n} \in A$, tel que $x = \sum_{i=1}^{n} a_i\beta_i$. Si donc ϕ existe, nécessairement,*

$$\phi(x) \,=\, \phi\big(\sum_{i=1}^{n} a_i\beta_i\big) \,=\, \sum_{i=1}^{n} a_i\phi(\beta_i) \,=\, \sum_{i=1}^{n} a_i\gamma_i\ .$$

Ceci établit l'unicité de ϕ.

Reste à voir que la formule ci-dessus définit bien, sans ambiguïté un morphisme de groupes abélienss (resp. A-modules.)

Remarque II.2.11 i) Le lemme II.2.10 est bien connu dans le cas des espaces vectoriels, et la preuve donnée ici n'est pas sensiblement différente de celle qu'on peut donner pour les espaces vectoriels et les applications linéaires. Une fois encore dès que l'on dispose d'une base pour un groupe abélien (resp. A-module,) un certain nombre de résultats établis dans le cas des espaces vectoriels peuvent se transposer aisément au cas des groupes abéliens (resp. modules.) Mais outre que l'on ne dispose pas toujours d'une base, un certain nombre de résultats ne s'étendront pas au cas des groupes abéliens (resp. A-modules.)

ii) Dans le lemme II.2.10 on n'est pas obligé de supposer que la base $\mathcal{B}$ est de cardinal fini mais c'est essentiellement la situation que nous allons rencontrer. Voir l'exercice II.12.2 pour un résultat plus général.

Lemme II.2.12 *Si $f : X \cong Y$ est un isomorphisme de groupes, entre groupes abéliens (resp. A-modules,) pour toute base $\mathcal{B}$ de X, $f(\mathcal{B})$ est une base de Y.*

II.3 . −Groupes abéliens (resp. A-modules,) libres de type fini

Proposition II.3.1 (Modules libres de type fini) *Pour un groupe abélien (resp. A-module,) X, les conditions suivantes sont équivalentes :*

a) X possède une base de cardinal fini $n \in \mathbb{N}^*$.

b) Il existe un isomorphisme

$$X \cong \mathbb{Z}^n (\text{resp. } A^n)$$

(cf. II.1.6.a).)

c) X est un groupe abélien (resp. A-module,) à la fois libre et de type fini.

***Preuve** :*

*i) (**a)** $\Rightarrow$ **b**))*
Soit $\mathcal{B} := \beta_{i\ ,1\leq i\leq n}$ une base de X et $\varepsilon_{i\ ,1\leq i\leq n}$ la base de $\mathbb{Z}^n$ (resp. A^n) introduite dans l'exemple II.1.4.c). En vertu du lemme II.2.10, il existe un unique couple de morphismes de groupes (resp. A-modules,)

$$\begin{aligned} & \phi \ : \ X \ \to \ \mathbb{Z}^n (\text{resp. } A^n) \ , \ \beta_i \ \mapsto \ \varepsilon_{i\ ,1\leq i\leq n} \\ \text{et} \quad & \psi \ : \ \mathbb{Z}^n (\text{resp. } A^n) \ \to \ X \ , \ \varepsilon_i \ \mapsto \ \beta_{i\ ,1\leq i\leq n} \quad . \end{aligned}$$

Comme

$$\forall 1 \leq i \leq n, \ \psi(\phi(\beta_i)) \ = \ \beta_i \ = \ \mathrm{Id}_X(\beta_i)$$

le lemme II.1.8 assure encore que

$$\psi \ \circ \ \phi \ = \ \mathrm{Id}_X \ .$$

Le même argument assure que

$$\phi \ \circ \ \psi \ = \ \mathrm{Id}_{\mathbb{Z}^n (\text{resp. } A^n)} \ .$$

*ii) (**b)** $\Rightarrow$ **a**))*
Il suffit d'appliquer le lemme II.2.12.

*iii) (**a)** $\Rightarrow$ **c**))*
Est tautologique.

*iv) (**c)** $\Rightarrow$ **a**))*
Soit $\mathcal{B}$ une base de X et $S := \{s_1, \ldots, s_r\}$ une famille génératrice finie de X. Puisque $\mathcal{B}$ est une base, pour tout $1 \leq i \leq r$, il existe une partie finie $\mathcal{B}_i$ de $\mathcal{B}$ et une application

$$a_i \ : \ \mathcal{B}_i \ \to \ \mathbb{Z} (\text{resp. } A)$$

tels que

$$s_i \ = \ \sum_{\beta \ \in \ \mathcal{B}_i} a_i(\beta)\beta \ .$$

Or S étant une famillle génératrice de X, pour tout $x \in X$, il existe un

$$r - \text{uplet } x_{i\ ,1\leq i\leq r} \ \in \ \mathbb{Z} (\text{resp. } A),$$

d'éléments de $\mathbb{Z}$ (resp. A,) tel que

$$x \;=\; \sum_{i=1}^{r} x_i s_i \;.$$

Il en résulte que

$$x \;=\; \sum_{i=1}^{r} \sum_{\beta \,\in\, \mathcal{B}_i} x_i a_i(\beta)\beta \;.$$

Cela signifie exactement que $\bigcup_{i=1}^{r} \mathcal{B}_i$ est une famille génératrice de X. Comme c'est une union finie d'ensemble finis c'est un ensemble fini. Comme de plus c'est un sous-ensemble de $\mathcal{B}$ c'est une famille libre en vertu du lemme II.2.3.ii). C'est donc une base de cardinal fini de X.

Définition II.3.2 (Groupe abélien (resp. A-Module,) libre de type fini) Un groupe abélien (resp. A-module,) X vérifiant les assertions équivalentes de la proposition II.3.1 est dit *libre de type fini*.

Proposition II.3.3 *Étant donné un groupe abélien (resp. un A-module,) X, les assertions II.1.9.a) à II.1.9.c) sont encore équivalente au fait qu'il existe un groupe abélien (resp. A-module,) libre de type fini L et un morphisme surjectif $f \;:\; L \;\to\; X$.*

Proposition II.3.4 *Soient $(r, s) \;\in\; \mathbb{N} \times \mathbb{N}$ il existe un isomorphisme*

$$\phi \;:\; \mathbb{Z}^r \;\cong\; \mathbb{Z}^s \;(\textit{resp.}\; \phi \;:\; A^r \;\cong\; A^s$$

si et seulement si $r \;=\; s$.

***Preuve** : (cf. TD n° III, exercice B.)*

Corollaire II.3.5 *Si X est un groupe abélien (resp. A-module,) libre de type fini, il existe un entier $r \;\in\; \mathbb{N}$ et un isomorphisme*

$$X \;\cong\; \mathbb{Z}^r (\textit{resp.}\; A^r) \;.$$

L'entier r est alors uniquement déterminé par X.

Définition II.3.6 (Rang d'un groupe abélien (resp. A-module,) libre de type fini) Si X est un groupe abélien
(resp. A-module,) libre de type fini, l'entier r donné par le corollaire II.3.5 est appelé le *rang* de X noté $\mathrm{rg}(X)$. Il est égal au nombre d'éléments d'une base de X.

Remarque II.3.7 Il serait tentant ici encore de faire jouer au rang d'un groupe abélien (resp. A-module,) libre de type fini le rôle de la dimension d'un $\mathbb{K}$-espace vectoriel mais le rang n'a malheureusement pas d'aussi bonnes propriétés : par exemple deux groupes abéliens (resp. A-modules,) $Y \;\subset\; X$ de même rang ne sont pas nécessairement égaux (cf. II.12.3.question 3).)

Remarque II.3.8 On pourrait penser que les groupes abéliens (resp. A-modules,) libres de type fini ont tendance à se comporter comme des espaces vectoriels. Cependant même sous l'hypothèse *libre de type fini* un certains nombre de résultats ne se transposent pas du contexte des espaces vectoriels à celui des groupes abéliens (resp. A-modules :)

i) Une famille libre maximale n'et pas nécessairement une base (voir l'exercice II.12.3.question 1).)

ii) Un sous-groupe (resp. sous-A-module,) d'un groupe abélien (resp. A-module,) libre de type fini n'a pas nécessairement un supplémentaire (cf. II.12.3.question 2).)

iii) Une famille libre ne peut pas nécessairement se compléter en une base.

Les résultats positifs que nous pouvons cependant donner sont les suivants :

Proposition II.3.9 *Étant donné un groupe abélien (resp. A-module,) libre de type fini L, toute suite exacte*

$$0 \to Y \xrightarrow{i} X \xrightarrow{p} L \to 0$$

de groupes (resp. A-modules,) est scindée, (cf. I.9.11.i);) ce qui entraîne en particulier que Y possède un suplémentaire dans X isomorphe à L.

Preuve *: Soit $\lambda_{i\ ,1\leq i\leq r}$ une base de L. Le morphisme p étant surjectif, pour tout $1 \leq i \leq r$ il existe $\mu_i \in X$, tel que $p(\mu_i) = \lambda_i$. En vertu du lemme II.2.10, il existe un unique morphisme de groupes (resp. A-modules,)*

$$s : L \to X\ ,\ \lambda_i \mapsto \mu_{i\ ,1 \leq i \leq r}\ .$$

Comme,

$$\forall 1 \leq i \leq r,\ p(s(\lambda_i)) = p(\mu_i) = \lambda_i = \mathrm{Id}_L(\lambda_i),$$

l'énoncé d'unicité dans le lemme II.2.10 assure que

$$p \circ s = \mathrm{Id}_L\ .$$

On laisse alors le lecteur établir, à partir des résultats du paragraphe I.9 que l'on a un isomorphisme

$$X \cong i(Y) \oplus s(L)\ .$$

Proposition II.3.10 *Soient L_1 et L_2 des groupes abéliens (resp. A-modules,) libres de rangs respectifs r_1 et r_2.*

i) $L_1 \times L_2$ est libre de rang $r_1 + r_2$.

ii) Si

$$0 \to L_1 \longrightarrow L \longrightarrow L_2 \to 0$$

est une suite exacte courte de groupes (resp. A-modules,) L est un groupe abélien (resp. A-module,) libre de rang $r_1 + r_2$.

iii) Soit L un groupe abélien (resp. A-module,) tel que $L = L_1 \oplus L_2$. Alors L est libre de rang $r_1 + r_2$.

Preuve *: On laisse le soin au lecteur de vérifier que les arguments qu'il connaît bien dans le cas des espaces vectoriels pour établir les points i) et iii) s'adaptent sans presque de modification au cas des groupes abéliens (resp. A-modules.)*

On déduit ii) de i), dans la mesure où, dès qu'on a une suite exacte $0 \to L_1 \longrightarrow L \longrightarrow L_2 \to 0$, L_2 étant libre celle-ci sera scindée, en vertu de la proposition II.3.9. Dans ce cas, en appliquant la proposition I.9.13, on disposera d'un isomorphisme $L \cong L_1 \times L_2$ permettant de conclure graçe à i).

II.4 . −Sous-groupe (resp. sous-A-module,) d'un groupe abélien (resp. A-module,) libre de type fini

Si l'on veut, dans ce paragraphe (II.4,) tenir compte des généralisations des énoncés sur les groupes abéliens, aux A-modules, il faut nécessairement supposer que A est un anneau *principal* (cf. I.12.2.) On pourrait juste penser que c'est une hypothèse de confort et qu'on pourrait éventuellement l'affaiblir. La preuve du lemme II.4.1 montre déjà qu'on aurait du mal à s'en passer mais la remarque II.4.9 et surtout la proposition II.4.10 assurent définitivement qu'il n'en est pas question !

Lemme II.4.1 *Si L est un groupe abélien (resp. A-module,) libre de rang 1 (cf. II.3.6,) et M un sous-groupe (resp. sous- A-module,) de L, alors M est un groupe abélien (resp. A-module,) libre de rang plus petit que* 1.

Preuve *: On dispose, en vertu du corollaire II.3.5, d'un isomorphisme*

$$\phi \ : \ \mathbb{Z}(\text{resp. } A) \ \cong \ L \ .$$

Pour tout sous-groupe (resp. sous-A-module,) $M \ \subset \ L$, puisque ϕ est un morphisme, en particulier surjectif, $M \ = \ \phi[\phi^{-1}(M)]$.

En outre $\phi(M)$ est un sous-groupe de $\mathbb{Z}$ (cf. I.5.1.ii),) (resp. sous-A-module de A (cf. A.5.1.ii).))

Or un sous-groupe de $\mathbb{Z}$ est un idéal de $\mathbb{Z}$ (resp. un sous-A-module de A un idéal de A (cf. A.3.2.b).)) Il existe donc $a \ \in \ \mathbb{Z}(\text{resp. } A)$ tel que

$$\phi^{-1}(M) \ = \ a\mathbb{Z}(\text{resp. } aA \ .)$$

Il s'ensuit que $\phi(a)$ est une base de M si $a \ \neq \ 0$. Ainsi soit $M \ = \ \{0\}$ soit M est le sous-groupe (resp. sous- A-module,) de L de base $\phi(a)$ donc de rang 0 *ou* 1.

Remarque II.4.2 Une fois établi le lemme II.4.1 ci-dessus, on imagine qu'on pourra obtenir un résultat analogue pour des groupes abéliens (resp. A-modules,) libres de rang quelconque par un argument de récurrence sur le rang.

Rappelons cependant que, si L est un groupe abélien (resp. A-module,) libre de rang $r+1$, (r étant un entier), muni d'une base $\lambda_{i\ ,0\leq i\leq r}$, que D désigne le sous groupe (resp. sous-A-module,) de L engendré par $\{\lambda_0\}$, et H le sous-groupe (resp. sous-A-module,) engendré par $\{\lambda_1, \ldots, \lambda_r\}$,) D et H sont bien entendu supplémentaires dans L. Cependant, pour un sous-groupe (resp. sous-A-module,) $X \ \subset \ L$, il n'est pas du tout certain, et même faux en général, que X soit somme directe de $X \cap D$, et $X \cap H$. Ce résultat est déjà faux dans le cas des espaces vectoriels même si dans ce dernier cas, on peut adapter la situation en choisissant D convenablement, c'est-à-dire en choisissant une famille libre que l'on complètera convenablement. On ne dispose pas, dans le cas des groupes abéliens (resp. A-modules,) (même libres de type fini) d'un équivalent du théorème de la base incomplète et le mieux qu'on pourra espérer, dans le cas déjà très particulier des anneaux principaux, est exposé aux paragraphe II.11 et B.7.

Sans choix particulier de la base $\lambda_{i\ ,0\leq i\leq r}$ de L, le « découpage » $L \ = \ D \oplus H$, permet cependant d'obtenir un « découpage » de tout sous-groupe abélien (resp. A-module,) X qui nous permettra de metre en œuvre un argument de récurrence :

Notation II.4.3 Soit $r \ \in \ \mathbb{N}^*$, un entier et L un groupe abélien (resp. A-module,) libre de rang $r+1$ et de base $\lambda_{i\ ,0\leq i\leq r}$. Soit D le sous-groupe (resp. sous-A-module,) de L engendré par $\{\lambda_0\}$ et H par $\{\lambda_1 \ldots, \lambda_r\}$.

Lemme II.4.4 *Avec les notations ci-dessus on a deux suites exactes (cf. I.9.1,) de groupes (resp. A-modules,) scindées :*

$$0 \to D \xrightarrow{i} L \xrightarrow{p} H \to 0 \qquad \text{II.4.4.1}$$

et

$$0 \to H \xrightarrow{j} L \xrightarrow{q} D \to 0\,. \qquad \text{II.4.4.2}$$

Preuve *: Il suffit de remarquer que, par construction, $L = D \oplus H$, et d'appliquer le théorème I.9.15.*

Remarque II.4.5 On pourrait utiliser indifféremment l'une ou l'autre des suites exactes II.4.4.1 ou II.4.4.2 pour établir le théorème II.4.6 et l'on choisira de développer la construction à partir de II.4.4.1. Néanmoins une relecture attentive du paragraphe I.9 montrerait que ces deux suites exactes sont en fait deux formulations d'un même résultat, à savoir que $L = D \oplus H$ et peuvent se déduire l'une de l'autre.

Théorème II.4.6 *Étant donné un groupe abélien (resp. A-module,) L libre de rang $r \in \mathbb{N}$, tout sous-groupe (resp. sous-A-module,) M de L est libre de rang s avec $s \leq r$.*

Preuve *: On raisonne par récurrence sur l'entier r. Si $r = 0, L = \{0\}$ et $M = \{0\}$, si bien que la conclusion est immédiate.*

Pour $r \in \mathbb{N}$ si L est libre de rang $r+1$, il existe un isomorphisme

$$L \cong \mathbb{Z}^{r+1} (\text{resp. } A^{r+1})$$

ou, ce qui revient au même (cf. II.3.1,) une base $\lambda_{i\ ,0\leq i\leq r}$ de L. On reprend les notations II.4.3 et l'on considère la suite exacte II.4.4.1. Étant donné un sous-groupe abélien (resp. A-module,) M de L, $P := p(M)$ est un sous-groupe (resp. sous-A-module,) de H. Le groupe abélien (resp. A-module,) H étant libre de rang r, on peut, par hypothèse de récurrence, supposer que P est un groupe abélien (resp. A-module,) libre de rang s avec $s \leq r$. Soit donc $\rho_{i\ ,1\leq i\leq s}$ une base de P.

Choisissons des antécédents des $\rho_{i\ ,1\leq i\leq s}$ dans M i.e. $\sigma_{i\ ,1\leq i\leq s}$ des éléments de M tels que

$$\forall 1 \leq i \leq s,\ p(\sigma_i) = \rho_i$$

(on dit parfois des relèvements des ρ_i.) Puisque l'image par p de la famille $\sigma_{i\ ,1\leq i\leq s}$ est une base de P, donc une famille libre, la famille $\sigma_{i\ ,1\leq i\leq s}$ est une famille libre. Le sous-groupe (resp. sous-A-module,) S de M engendré par $\{\sigma_1 \ldots, \sigma_s\}$ est donc un sous-groupe (resp. sous-A-module,) libre de rang s de M et de L.

Le groupe abélien (resp. A-module,) $E := M \cap D$ est un sous-groupe (resp. A-module,) de D. Puisque D est un groupe abélien (resp. A-module,) de rang 1, il résulte du lemme II.4.1 que E est un groupe abélien (resp. A-module,) libre de rang ≤ 1.

Si donc on établit (ce qui va être fait dans le lemme II.4.6.1,) que

$$M = E \oplus S,$$

il résulte de la proposition II.3.10.iii), que M est un groupe abélien (resp. A-module,) libre de rang inférieur ou égale à $s+1 \leq r+1$.

Lemme II.4.6.1

$$M = E \oplus S\,.$$

Preuve : *Pour tout* $x \in M$, $p(x) \in P$ *si bien qu'il existe* a_i ,$1 \leq i \leq s$ *tel que* $p(x) = \sum_{i=1}^{s} a_i \rho_i$ *si bien que :*

$$\begin{aligned} & p(x) - \sum_{i=1}^{s} a_i \rho_i = 0 \\ \Leftrightarrow \quad & p(x) - \sum_{i=1}^{s} a_i p(\sigma_i) = 0 \\ \Leftrightarrow \quad & p\big(x - \sum_{i=1}^{s} a_i \sigma_i\big) = 0 \\ \Leftrightarrow \quad & x - \sum_{i=1}^{s} a_i \sigma_i \in \operatorname{Ker} p = D . \end{aligned}$$

Pour tout $x \in M$, *il existe donc* $y \in S$ *tel que* $z := x - y \in D$. *Or* $x \in M$, $y \in S \subset M$ *donc*

$$z \in M \cap D = E .$$

Il est immédiat de voir que

$$S \cap E \subset S \cap D = \{0\}$$

si bien que

$$M = S \oplus E .$$

Remarque II.4.7 Une lecture attentive de la preuve du théorème II.4.6 et plus particulièrement de la preuve du lemme II.4.6.1 permettra de se rendre compte, qu'un certain nombre d'arguments donnés ici semblent l'avoir déjà été, en particulier dans les preuves des propositions II.3.9 et I.9.13 ; ce qui pourrait laisser penser que l'on peut rédiger la preuve du théorème II.4.6 de manière plus concise en faisant appel à ces résultats antérieurs :

En effet, en reprenant les notations de la preuve, considérons la restrictions $q := p_{|M}$ de p à M à valeurs dans $P := p(M)$. Le noyau de q est $E = M \cap D$ et l'on a donc une suite exacte

$$0 \to E \longrightarrow M \xrightarrow{q} P \to 0 . \qquad \text{II.4.7.1}$$

Le lemme II.4.1 dont il est bien entendu inenvisageable de se passer, assure alors que E est un groupe abélien (resp. A-module,) libre de rang inférieur ou égal à 1. Le groupe abélien (resp. A-module,) H étant libre de rang r et P un sous-groupe abélien (resp. A-module,) de H, l'hypothèse de récurrence assure que P est libre de rang inférieur ou égal à r. Il suffit alors d'appliquer la proposition II.3.9 pour conclure.

Corollaire II.4.8 (du théorème II.4.6) *i) Tout sous-groupe (resp. sous-*A*-module,)* Y *d'un groupe abélien (resp.* A*-module,) de type fini* X *est de type fini.*

Preuve : *Si* X *est de type fini il existe (cf. II.3.3,) un groupe abélien (resp.* A*(-module,) libre de type fini* L *et un morphisme surjectif* $p : L \to X$. *Alors l'image inverse* $p^{-1}(Y)$ *de* Y *dans* L *est un sous-groupe (resp. sous-* A*-module,) de* L. *Ce dernier étant libre de type fini,* $p^{-1}(Y)$ *est encore libre de type fini en vertu du théorème II.4.6. Or la restriction*

$$p_{|p^{-1}(Y)} : p^{-1}(Y) \to N$$

est un morphisme surjectif ce qui entraîne, en vertu de la proposition II.1.9 que Y *est de type fini.*

ii) Étant donnée une suite exacte de groupes abéliens (resp. A-modules,)

$$0 \to N \longrightarrow X \longrightarrow Q \to 0,$$

X est de type fini si et seulement si N et Q le sont.

***Preuve** : Si X est de type fini, Q l'est ausssi en vertu de la proposition II.1.9 et N en vertu du point i). L'assertion réciproque a été montrée dans la proposition II.1.11.iii).*

Remarque II.4.9 On pourrait donner une réciproque au théorème II.4.6 dont nous n'aurons pas d'usage particulier dans ce cours. Cependant soit A un anneau tel que tout sous-A-module d'un A-module libre de rang r est un A-module libre de rang inférieur ou égal à r. L'anneau A lui-même étant un A-module libre de rang 1, tout idéal de A étant un sous-A-module de A il est libre de rang plus petit que 1 ce qui signifie exactement qu'il est principal.

On peut même donner un énoncé plus fort :

Proposition II.4.10 *Réciproquement, si A est un anneau intègre tel que tout sous-A-module d'un A-module libre de type fini est libre de type fini, alors A est principal.*

***Preuve** : Considérons en effet un idéal $\mathfrak{I} \subset A$ de A. En tant que sous-A-module de A lui-même il est donc libre de type fini c'est-à-dire qu'il possède une base ε_i ,$1 \leq i \leq d$. Si $d > 1$,*

$$\varepsilon_1 \varepsilon_2 - \varepsilon_2 \varepsilon_1 = 0$$

ce qui contredit le fait que $\{\varepsilon_1, \varepsilon_2\}$ soit libre et entraîne donc $d \leq 1$ c'est-à-dire $\mathfrak{I}$ principal.

II.5 . −Ordre d'un élément,, exposant d'un groupe (cf. IV.2, A.7)

Dans tout ce paragraphe (II.5,) $(A,+)$ **est un groupe abélien. On note toujours** $\cdot\ :\ \mathbb{Z}\times A\ \to\ A$ **la loi externe définie en I.6.6, et qui donne à** A **sa structure de** $\mathbb{Z}$**-module (cf. A.1.11.i).)**

Lemme II.5.1 ((cf. IV.2.1, A.7.1)) *Pour tout*

$$x\ \in\ A \text{ et } m\ \in\ \mathbb{Z},$$

il est équivalent que $nx\ =\ 0$, *ou que le morphisme de groupes*

$$\mathbb{Z}\ \to\ A\ ,\ m\ \mapsto\ mx \qquad \textit{II.5.1.1}$$

se factorise en un morphisme

$$\begin{array}{ccc} & & \mathbb{Z} \\ & & \downarrow \qquad \searrow_{m\mapsto mx} \\ \mathbb{Z}/n\mathbb{Z} & \to & A\ . \end{array} \qquad \textit{II.5.1.2}$$

Définition II.5.2 ((cf. IV.2.2, A.7.2)) i) (**Élément de torsion**)
Si x et n vérifient les conditions équivalentes du lemme II.5.1 ci-dessus, on dit que x est de n-*torsion*.
On dit que $x\ \in\ A$ est *de torsion* s'il existe $n\ \in\ \mathbb{Z}\ n\ \neq\ 0$, tel que x soit de n-torsion, *i.e.* tel que $nx\ =\ 0$.

ii) (**Partie de n-torsion**)
Pour tout $n\ \in\ \mathbb{N}^*$, on note

$$A[n]\ :=\ \{x\ \in\ A\ ;\ nx\ =\ 0\}$$

le sous-ensemble de A formé des éléments de n-torsion de A.
On appellera $A[n]$ la *partie de n-torsion* de A.
On dira que A est *de n-torsion* si $A\ =\ A[n]$.

iii) (**Ordre d'un élément**)
Pour tout $x\ \in\ A$, on dit que x est d'*ordre* n si le morphisme

$$\mathbb{Z}/n\mathbb{Z}\ \to\ A\ ,\ \overline{m}\ \mapsto\ mx \text{ (cf. II.5.1.2)}$$

est injectif ou, ce qui revient au même, si $n\mathbb{Z}$ est le noyau $\mathrm{Ann}_{\mathbb{Z}}(x)$ du morphisme II.5.1.1.
Si x est d'ordre $n\ \neq\ 0$, n est aussi le nombre d'éléments de l'image du morphisme IV.2.1.2 qui est encore l'image du morphisme II.5.1.1 ou bien encore le sous-groupe $<\ x\ >$ de A engendré par x.

iv) (**Exposant d'un groupe**)
L'ensemble

$$\mathrm{Ann}_{\mathbb{Z}}(A)\ :=\ \bigcap_{x\ \in\ A}\mathrm{Ann}_{\mathbb{Z}}(x)\ =\ \{n\ \in\ \mathbb{Z}\ ;\ \forall x\in A,\ n\cdot x\ =\ 0\}$$

est un sous-groupe, ou de manière équivalente un idéal de $\mathbb{Z}$ dont le générateur positif est usuellement appelé *exposant* du groupe A.

v) (**Partie de torsion**)
On note

$$\mathrm{Tor}_{\mathbb{Z}}(A) \text{ ou tout simplement } \mathrm{Tor}(A)\ :=\ \bigcup_{n\ \in\ \mathbb{N}^*}A[n]$$

l'ensemble des éléments de torsion de A qu'on appelle la *partie de torsion* de A.

vi) (**Groupe de torsion**)
On dit que A est *de torsion* si

$$A \;=\; \mathrm{Tor}(A)\,.$$

vii) (**Groupe sans torsion**)
On dit que A est *sans torsion* si

$$\mathrm{Tor}(A) \;=\; \{0\}\,.$$

Proposition II.5.3 (Ordre et exposant (cf. IV.2.3, A.7.3)) *i) L'exposant du groupe A est le **Ppcm** des ordres des éléments de A. Il s'ensuit, en vertu du théorème de* LAGRANGE*, que si A est de cardinal fini, ce dernier est un multiple de l'exposant de A.*

ii) Un entier m est l'exposant du groupe abélien A, si et seulement si $m\mathbb{Z}$ est le noyau du morphisme naturel

$$\mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)\ .\ \textit{(cf. I.6.8 .)}$$

iii) Pour A et B des groupes abéliens, si $A \subset B$, l'exposant de A divise celui de B.

iv) Pour tout morphisme de groupes $f : A \to B$ et tout $x \in A$, l'ordre de $f(x)$ dans B divise l'ordre de x dans A avec égalité si f est injectif.
Il s'ensuit que l'exposant de $f(A)$ divise l'exposant de A avec égalité si f est injectif.

Proposition II.5.4 (Propriétés de $A[n]$ (cf. IV.2.4, A.7.4)) *i) Pour tout $n \in \mathbb{N}$, $A[n]$ est un sous-groupe de A.*

***Preuve** : (cf. TD n° I, exercice A, question 1).)*

ii) Pour B un groupe abélien, $f : A \to B$ un morphisme de groupes, et tout $n \in \mathbb{N}$,

$$f(A[n]) \subset B[n] \text{ et } f[n] \;:=\; f_{|A[n]} : A[n] \to B[n]$$

est un morphisme de groupes, qui est un isomorphisme dès que f en est un.

***Preuve** : (cf. TD n° I, exercice A, question 2).)*

iii) Pour tout $(p,q) \in \mathbb{Z}\times\mathbb{Z}$ si p et q sont premiers entre eux

$$A[pq] \;=\; A[p] \,\oplus\, A[q]\,.$$

***Preuve** : (cf. TD n° I, exercice A, question 3).)*

iv) Si de plus A est d'exposant pq alors $A[p]$ (resp. $A[q]$,) est d'exposant p (resp. q.)

Proposition II.5.5 (Propriétés de la partie de torsion cf. A.7.5) *i) L'ensemble $\mathrm{Tor}(A)$ est un sous-groupe de A.*

***Preuve** : (cf. TD n° I, exercice A, question 1).)*

ii) Le quotient $A/\mathrm{Tor}(A)$ et sans torsion.

***Preuve** : (cf. TD n° I, exercice A, question 4).)*

iii) Pour tout groupe abélien B et tout morphisme $f : A \to B$,

$$f(\mathrm{Tor}(A)) \subset \mathrm{Tor}(B) \text{ et } f_{|\mathrm{Tor}(A)} : \mathrm{Tor}(A) \to \mathrm{Tor}(B)$$

est un morphisme de groupes qui est un isomorphisme dès que f en est un.

***Preuve** : (cf. TD n° I, exercice A, question 2).)*

iv) Si A est d'exposant strictement positif (i.e. $\mathrm{Ann}_{\mathbb{Z}}(a) \neq \{0\}$,) A est de torsion.

Remarque II.5.6 La réciproque du point II.5.5.iv) n'est en revanche pas vraie en général : Par exemple pour tout $\frac{a}{b} \in \mathbb{Q}/\mathbb{Z}$, $b\frac{a}{b} \in \mathbb{Z}$ c'est-à-dire que $b\frac{a}{b} = 0$ dans $\mathbb{Q}/\mathbb{Z}$. Cependant pour tout $n \in \mathbb{N}^*$, $a \in \mathrm{Ann}_{\mathbb{Z}}(\frac{1}{n})$ si et seulement si $a \in n\mathbb{Z}$, ce qui entraîne que

$$\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) \subset \bigcap_{n \in \mathbb{N}^*} n\mathbb{Z} = \{0\}\,.$$

En revanche si A est de type fini, on a la proposition suivante :

Proposition II.5.7 ((cf. IV.2.5, A.7.6)) *Si A est de type fini (cf. II.1.5,) A est de torsion si et seulement si A est d'exposant strictement positif.*

Proposition II.5.8 (cf. IV.2.6) *Un groupe abélien est de type fini et de torsion si et seulement s'il est fini.*

***Preuve** : (cf. TD n° III, exercice C.)*

II.6 . −Structure des groupes abéliens de type fini (cf. B.1)

Proposition II.6.1 ((cf. B.1.1)) *Un groupe abélien libre (cf. II.2.8,) est sans torsion (cf. II.5.2.vii).)*

Preuve *: Soit L un groupe abélien libre de base $\mathcal{B}$. Pour tout $x \in L, x \neq 0, a \in \mathrm{Ann}_{\mathbb{Z}}(x)$, (i.e. $a \cdot x = 0$.) Or il existe une partie finie $\mathcal{B}_x \subset \mathcal{B}$ et une application $\xi : \mathcal{B}_x \to \mathbb{Z}$ non identiquement nulle, tels que*

$$x = \sum_{\beta \in \mathcal{B}_x} \xi(\beta)\beta \, .$$

Il s'ensuit que $ax = 0$ entraîne

$$\sum_{\beta \in \mathcal{B}_x} a\xi(\beta)\beta = 0 \, .$$

Or $\mathcal{B}_x$ est une partie d'une famille libre donc est libre (cf. II.2.3.ii).) Il s'ensuit que

$$\forall \beta \in \mathcal{B}_x, \; a\xi(\beta) = 0 \, .$$

L'élément x n'étant pas nul il existe $\beta \in \mathcal{B}_x$ tel que $\xi(\beta) \neq_0$. Puisque $\mathbb{Z}$ est intègre, $a\xi(\beta) = 0$ entraîne $a = 0$ et finalement

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{0\}$$

ce qui assure que L est sans torsion.

On peut enfin donner la réciproque attendue, dans le cas des anneaux principaux à la proposition II.6.1 :

Théorème II.6.2 ((cf. B.1.2)) *Un groupe abélien A de type fini (cf. II.1.5,) est libre (cf. II.2.8,) si et seulement s'il est sans torsion (cf. II.5.2.vii).)*

Preuve *: Le fait qu'un groupe abélien libre est sans torsion découle de la proposition II.6.1.*

Réciproquement, soit A un groupe abélien de type fini et sans torsion. Il existe une partie génératrice finie $\alpha_{i\,,1\leq i\leq m}$ de A. Par ailleurs pour tout $a \in \mathbb{Z}$, $a\alpha_i = 0$ entraîne $a = 0$, puisque A est sans torsion. L'ensemble des parties libres de $\alpha_{i\,,1\leq i\leq m}$, est donc non vide puisque $\{\alpha_i\}$ est libre pour tout i. Il existe donc une partie libre maximale de $\alpha_{i\,,1\leq i\leq m}$ qu'on peut noter, quite à renuméroter $\alpha_{i\,,1\leq i\leq n}$ $n \leq m$.

Notons $B := \mathrm{Vect}\{\alpha_{i\,,1\leq i\leq n}\}$ le sous-groupe de A engendré par $\{\alpha_1, \ldots, \alpha_n\}$ qui est un groupe abélien libre de rang n.

Lemme II.6.2.1 *Pour tout $n < k \leq m$, il existe*

$$a_k \in \mathbb{Z} \setminus \{0\} \text{ tel que } a_k\alpha_k \in B \, .$$

Preuve *(**du lemme II.6.2.1**): Pour tout $n < k \leq m$, la famille $\{\alpha_{i\,,1\leq i\leq n}\} \cup \{\alpha_k\}$ est liée par maximalité de $\alpha_{i\,,1\leq i\leq n}$. Il existe donc $a_{i\,,1\leq i\leq n} \in A$ et $a_k \in A$ non tous nuls, tels que $\sum_{i=1}^{n} a_i\alpha_i + a_k\alpha_k = 0$. Or puisque $\alpha_{i\,,1\leq i\leq n}$ est libre, $a_k \neq 0$. De plus*

$$a_k\alpha_k = -\sum_{i=1}^{n} a_i\alpha_i \in B \, .$$

Soit

$$a := \prod_{i=n+1}^{m} a_i \text{ et} \lambda : A \to A\,,\ x \mapsto a \cdot x$$

(où les $a_{i\,,n+1\leq i\leq m}$ sont définis par le lemme II.6.2.1.) Notons que si $n = m$, la démonstration est déjà terminée puisque $A = B$, mais qu'on peut n'en pas tenir compte en posant dans ce cas $a = 1$ et poursuivre comme nous allons le faire.

Lemme II.6.2.2 *L'application λ définie ci-dessus est un morphisme injectif de groupes à valeurs dans B.*

***Preuve** (**du lemme II.6.2.2**): D'abord il est clair que λ est un morphisme.*

Ensuite $\lambda(x) = 0 \Leftrightarrow ax = 0$. Comme A est sans torsion et que $a \neq 0, \operatorname{Ker}\lambda = \{0\}$.

Enfin pour tout $x \in A$, il existe $x_{i\,,1\leq i\leq m} \in A$ tel que $x = \sum_{i=1}^{m} x_i\alpha_i$. Il s'ensuit que :

$$\begin{aligned}\lambda(x) &= ax\\ &= \sum_{i=1}^{m} ax_i\alpha_i\\ &= a\sum_{i=1}^{n} x_i\alpha_i + \sum_{i=n+1}^{m} x_i a\alpha_i\ .\end{aligned}$$

Or $a\sum_{i=1}^{n} x_i\alpha_i \in B$ par définition et $\sum_{i=n+1}^{m} x_i a\alpha_i \in B$ en vertu du lemme II.6.2.1. Il s'ensuit que $\lambda(x) \in B$.

D'après le lemme ci dessus, λ induit donc un isomorphisme de A sur $\operatorname{Im}\lambda \subset B$. Or B étant un groupe abélien libre de type fini, le théorème II.4.6, entraîne qu'il en est de même de $\operatorname{Im}\lambda$ et donc de A.

Proposition II.6.3 ((cf. B.1.3)) *Soit A un groupe abélien de type fini et $\operatorname{Tor}(A)$ son sous-groupe de torsion (cf. II.5.5.i),) et $p : A \to L := A/\operatorname{Tor}(A)$ la surjection canonique. Alors :*

i) Le sous-groupe $\operatorname{Tor}(A)$ de A est de type fini.

***Preuve** : (cf. II.4.8.i).)*

ii) Le groupe abélien L est libre de type fini.

***Preuve** : Le groupe L est de type fini en vertu de la proposition II.1.9, est sans torsion grâce à la proposition II.5.5.ii) et donc libre, de type fini, en vertu du théorème II.6.2.*

iii) La suite exacte

$$0 \to \operatorname{Tor}(A) \longrightarrow A \xrightarrow{p} L \to 0$$

est sindée (cf. I.9.11.i),) si bien que p définit un isomorphisme

$$A \cong \operatorname{Tor}(A) \oplus L\ .$$

***Preuve** : Puisque L est un groupe abélien libre en vertu de ii), la suite exacte*

$$0 \to \operatorname{Tor}_A(M) \longrightarrow M \xrightarrow{p} L \to 0$$

est sindée en vertu de la proposition II.3.9. L'isomorphisme $A \cong \operatorname{Tor}(A) \oplus L$ provient alors de la proposition I.9.13.

Théorème II.6.4 (Structure des groupes abéliens de type fini (cf. B.1.4)) *Soit A un groupe abélien de type fini (cf. II.1.5.)*

i) Il existe un groupe abélien T de type fini et de torsion (cf. II.5.2.vi),) (i.e. en vertu de II.5.8 un groupe abélien fini,) et un groupe abélien libre de type fini (cf. II.3.2,) L tels que

$$A \cong T \times L .$$

***Preuve** : (cf. II.6.3.iii).)*

ii) Le couple (T, L) est unique au sens où T est isomorphe au sous-groupe de torsion $\mathrm{Tor}(A)$ de A et s'il existe L_1 et L_2 tels que

$$A \cong T \times L_1 \cong T \times L_2$$

L_1 et L_2 sont isomorphe et ont donc en particulier même rang.

***Preuve** : Soit T un groupe abélien de type fini et de torsion, L un groupe abélien libre de type fini et*

$$f : T \times L \cong A \text{ un isomorphisme } .$$

$*$) (***Construction d'un morphisme** $g : L \to A/\mathrm{Tor}(A)$)*

Le sous-groupe $T \subset T \times L$ (cf. I.7.6,) est de torsion dans $T \times L$, son image $f(T)$ est donc un sous-groupe de $\mathrm{Tor}(A)$ en vertu du lemme II.5.5.iii). Si $p : A \to A/\mathrm{Tor}(A)$ désigne la surjection canonique $\mathrm{Ker}\, p = \mathrm{Tor}(A)$, si bien que $p \circ f$ se factorise en un morphisme

$$g : (T \times L)/T \to A/\mathrm{Tor}(A) .$$

Or le produit $T \times L$ donne lieu, en vertu de la proposition I.7.6 ou de sa reformulation dans le théorème I.9.15, à une suite exacte

$$0 \to T \longrightarrow T \times L \xrightarrow{q} \to 0L$$

rendant isomorphes L et $T \times L/T$. On peut donc considérer qu'on a un morphisme

$$g : L \to A/\mathrm{Tor}(A) \text{ tel que } g \circ q = p \circ f .$$

†) (***Un « morphisme de suites exactes »**)*

En notant $h := f_{|T}$, la restriction de f à T, nous pouvons récapituler les informations dont nous disposons dans le diagramme commutatif à lignes exactes suivant :

$$\begin{array}{ccccccccc} 0 \to & T & \xrightarrow{j} & T \times L & \xrightarrow{q} & L & \to 0 & & \\ & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & [2] & (1) \\ 0 \to & \mathrm{Tor}(A) & \xrightarrow{i} & A & \xrightarrow{p} & A/\mathrm{Tor}(A) & \to 0 . & & \end{array}$$

‡) (*g **est surjectif et** h **injectif**)*

Or $p \circ f$ étant surjectif et $g \circ q = p \circ f$, g est surjectif. De même $i \circ h = f \circ j$ et $f \circ j$ étant injectif, h est injectif.

2. Il est d'usage d'appeler un tel diagramme un *morphisme de suites exactes* mais il n'est vraiement pas nécessaire, dans l'immédiat tout du moins, de s'encombrer l'esprit avec une pareille terminologie.

§) (g **est injectif**)

Pour tout $x \in L$, il existe $y \in T \times L$ tel que $x = q(y)$. Il s'ensuit que $g(x) = 0$ entraîne $g[q(y)] = 0$ c'est-à-dire que $p[f(y)] = 0$ donc

$$f(y) \in \operatorname{Ker} p = \operatorname{Tor}(A) .$$

Il s'ensuit que (cf. II.5.5.iii),) $y = f^{-1}[f(y)]$ est de torsion dans $T \times L$. Il en résulte, toujours en vertu de loc. cit., que $x = q(y)$ est de torsion dans L. Or L étant libre il est sans torsion (cf. II.6.1,) si bien que $x = 0$. On en conclut que g est injectif.

¶) (h **est surjectif**)

Quiconque connaîtrait le lemme du serpent conclurait immédiatement du fait que g est injectif et f surjectif, que h est surjectif[3].

Soit donc $x \in \operatorname{Tor}(A)$, et $i(x)$ qu'on peut continuer à noter x son image dans A. Autrement dit, soit x un élément de torsion de A. Son image $f^{-1}(x)$ dans $T \times L$ est encore un élément de torsion ce qui entraîne que $q[f^{-1}(x)]$ est de torsion dans L qui est sans torsion. Il s'ensuit donc que $q[f^{-1}(x)] = 0$, c'est-à-dire que

$$f^{-1}(x) \in \operatorname{Ker} q = T$$

c'est-à-dire que $f^{-1}(x)$ est un antécédent pour x par h ce qui assure que h est surjectif.

‖) (**Conclusion**)

Il résulte de ce qui précède que g et h sont des isomorphismes ; ce qui prouve le résultat.

3. On ne supposera pas acquis ce résultat.

II.7 . −Rang d'un groupe abélien de type fini

On a défini le *rang* d'un groupe abélien (resp. A-module,) libre de type fini en II.3.6. On peut étendre cette définition au groupe abéliens de type fini en général. Les résultats du présent paragraphe (II.7,) s'appliqent également aux A-modules de type fini en prenant bien soint de faire l'hypothèse que A est un anneau principal. Ce qui suit s'appuyant essentiellement sur le théorème II.6.4, si on en veut l'analogue pour les A-modules de type fini, il faut utiliser le théorème B.1.4.

Définition II.7.1 (Rang d'un groupe abélien (resp. A-module,) de type fini) L'énoncé d'unicité II.6.4.ii) (resp. B.1.4.ii),) permet de définir le rang d'un groupe abélien (resp. A-module,) de type fini X comme le rang au sens de la définition II.3.6, de sa partie libre $\mathcal{L}(X) := X/\mathrm{Tor}(X)$ et l'on notra

$$\mathrm{rg}(X) := \mathrm{rg}(\mathcal{L}(X)) .$$

On déduit de ce qui précède, une nouvelle caractérisation des groupe abéliens (resp. A-modules,) de torsion (cf. II.5.2.vi) (resp. A.7.2.vi) :))

Corollaire II.7.2 (du théorème II.6.4 (resp. B.1.4)) *Un groupe abélien (resp. A-module,) X de type fini, est de torsion si et seulement si* $\mathrm{rg}(X) = 0$.

La définition II.7.1 ne prend tout son sens que si on dispose d'un énoncé similaire à la proposition II.3.10, or :

Proposition II.7.3 *Soient X_1 et X_2 deux groupes abéliens (resp. A-modules,) de type fini.*

*i) (**(cf. II.3.10.i),**)*
On a :

$$\mathrm{rg}(X_1 \times X_2) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2) .$$

***Preuve** : Écrivons*

$$X_1 = T_1 \times L_1 \text{ et } X_2 = T_2 \times L_2$$

grâce à II.6.4.i) (resp. B.1.4.i) avec T_i de type fini et de torsion et L_i libre de type fini (pour $i = 1$ ou 2.) On a alors

$$X_1 \times X_2 = (L_1 \times L_2) \times (T_1 \times T_2)$$

où $L_1 \times L_2$ est libre de rang

$$\mathrm{rg}(L_1) + \mathrm{rg}(L_2) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2)$$

d'après la proposition II.3.10.i), et $T_1 \times T_2$ est de torsion. Le résultat d'unicité II.6.4.ii) (resp. B.1.4.ii),) permet de conclure.

*ii) (**cf. II.3.10.iii)**)*
Si X_1 et X_2 sont des sous-groupes (resp. sous-A-modules,) d'un groupe abélien (resp. A-module,) X tels que

$$X = X_1 \oplus X_2,$$
$$\mathrm{rg}(X) = \mathrm{rg}(X_1) + \mathrm{rg}(X_2)\,.$$

***Preuve** : Il suffit d'utiliser l'isomorphisme*

$$X \cong X_1 \times X_2$$

donné par le théorème I.9.15, pour conclure grâce au point i).

On aimerait également avoir l'analogue du point II.3.10.ii), ce qui sera obtenu dans la proposition II.7.9. On introduit d'abord quelques notations (cf. II.7.4,) puis on énonce et on démontre les lemmes II.7.6 à II.7.8, qui sont des cas particuliers de la proposition qu'on veut obtenir mais entrent également comme ingrédients dans sa preuve.

Notation II.7.4 Pour un groupe abélien (resp. A-module,) X de type fini, on note toujours $\mathrm{Tor}(X)$ sa partie de torsion et l'on notera $\mathcal{L}(X) := X/\mathrm{Tor}(X)$ qui est un groupe abélien (resp. A-module,) libre de type fini. Le théorème II.6.4 (resp. B.1.4,) assure alors qu'on a toujours une suite exacte :

$$0 \to \mathrm{Tor}(X) \xrightarrow{j_X} X \xrightarrow{p_X} \mathcal{L}(X) \to 0 \qquad \text{II.7.4.1}$$

où $j_X = \mathrm{Id}_{X|\mathrm{Tor}(X)}$ est l'inclusion naturelle et p_X la surjection canonique.
Dans la suite on suppose que X est un groupe abélien (resp. A-module,) tel qu'il existe une suite exacte :

$$0 \to N \xrightarrow{i} X \xrightarrow{q} Q \to 0 \text{ avec } N \text{ et } Q \text{ de type fini.} \qquad \text{II.7.4.2}$$

Si N et Q sont de type fini X l'est aussi en vertu de la proposition II.1.11.iii).
Le lemme II.5.5.iii) (resp. A.7.5.iii),) donne le carré commutatif

$$\begin{array}{ccc} \mathrm{Tor}(N) & \xrightarrow{\mathrm{Tor}(i)} & \mathrm{Tor}(X) \\ {\scriptstyle j(N)}\downarrow & & \downarrow{\scriptstyle j(X)} \\ N & \xrightarrow{i} & X \end{array} \qquad \text{II.7.4.3}$$

qui donnent par factorisation un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Tor}(N) & \xrightarrow{j_N} & N & \xrightarrow{p_N} & \mathcal{L}(N) & \to & 0 \\ & & {\scriptstyle \mathrm{Tor}(i)}\downarrow & & {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \mathcal{L}(i)} & & \\ 0 & \to & \mathrm{Tor}(X) & \xrightarrow{j_X} & X & \xrightarrow{p_X} & \mathcal{L}(X) & \to & 0 \end{array} \qquad \text{II.7.4.4}$$

Lemme II.7.5 *Le morphisme $\mathcal{L}(i)$ dans le diagramme II.7.4.4 est injectif.*

Preuve : *Pour tout* $x \in \mathcal{L}(N)$ *il existe* $y \in N$ *tel que* $p_N(y) = x$. *Alors*

$$\mathcal{L}(i)[p_N(y)] = 0 \Leftrightarrow p_X[i(y)] = 0$$

i.e.

$$i(y) \in \operatorname{Ker} p_X = \operatorname{Im} j_X .$$

Il existe donc $z \in \operatorname{Tor}(X)$ *tel que* $i(y) = j_X(z)$. *Or* $z \in \operatorname{Tor}(X)$ *c'est-à-dire que* z *est de torsion i.e.*

$$\exists a \in \mathbb{Z} \setminus \{0\} (\textit{resp.}\ A \setminus \{0\}),\ az = 0 .$$

Il s'ensuit que

$$i(ay) = ai(y) = aj_X(z) = j_X(az) = 0 .$$

Puisque i *est injectif,* $ay = 0$ *i.e.* y *est de torsion i.e.*

$$\exists w \in \operatorname{Tor}(N),\ y = j_N(w) .$$

Finalement

$$x = p_N(y) = p_N[j_N(w)] = 0 .$$

Lemme II.7.6 *Sous les conditions II.7.4.2, si* N *et* X *sont libres et* Q *de torsion,*

$$\operatorname{rg}(X) = \operatorname{rg}(N) .$$

Preuve : *Puisque* X *est libre de type fini, choisissons une base* $x_i\,,1\leq i\leq r}$ *de* X. *Puisque* Q *est de torsion,*

$$\forall 1 \leq i \leq r,\ \exists a_i \in \mathbb{Z} \setminus \{0\} (\textit{resp.}\ A \setminus \{0\}),\ a_i q(xm_i) = 0 .$$

Il s'ensuit que $q(a_i x_i) = 0$, *i.e.*

$$\forall 1 \leq i \leq r,\ a_i x_i \in N .$$

Puisque $x_i\,,1\leq i\leq r}$ *est une partie libre de* X, $a_i x_i\,,1 \leq i \leq r}$ *est encore une partie libre de* X. *Le sous-module* P *qu'elle engendre est donc libre de rang* r. *Or*

$$P \subset N \subset X$$

ce qui entraîne, en vertu du théorème II.4.6, que

$$r = \operatorname{rg}(P) \leq \operatorname{rg}(N) \leq \operatorname{rg}(X) = r$$

d'où finalement

$$\operatorname{rg}(X) = \operatorname{rg}(N) .$$

Lemme II.7.7 *Sous les conditions de II.7.4.2, si Q est de torsion*

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N)\;.$$

Preuve : *D'après le lemme II.7.5, $\mathcal{L}(i) \;:\; \mathcal{L}(N) \;\to\; \mathcal{L}(X)$ est injectif ; notons donc*

$$R \;:=\; \mathcal{L}(X)/\mathcal{L}(N) \text{ et } r \;:\; \mathcal{L}(X) \;\to\; R \text{ la surjection canonique}$$

si bien qu'on a une suite exacte :

$$0 \;\to\; \mathcal{L}(N) \xrightarrow{\mathcal{L}(i)} \mathcal{L}(N) \xrightarrow{\;r\;} R \;\to\; 0\;. \qquad \textit{II.7.7.1}$$

Or

$$r \circ p_X \circ i \;=\; r \circ \mathcal{L}(i) \circ p_N \;=\; 0$$

si bien qu'il existe un morphisme

$$t \;:\; Q \;\to\; R \text{ tel que } t \circ q \;=\; r \circ p_X\;;$$

en d'autres termes qu'on a le diagramme commutatif suivant à lignes exactes :

$$\begin{array}{ccccccccc}
0 & \to & N & \xrightarrow{\;i\;} & X & \xrightarrow{\;q\;} & Q & \to & 0 \\
 & & {\scriptstyle p_N}\downarrow & & {\scriptstyle p_X}\downarrow & & \downarrow{\scriptstyle t} & & \\
0 & \to & \mathcal{L}(N) & \xrightarrow{\mathcal{L}(i)} & \mathcal{L}(X) & \xrightarrow{\;r\;} & R & \to & 0\;.
\end{array}$$

Cette dernière condition entraîne, puisque $r \circ p_X$ est surjectif, que r est surjectif. Ceci entraîne que R est de torsion.

On peut alors appliquer le lemme II.7.6 à la suite II.7.7.1 qui donne alors

$$\mathrm{rg}\big(\mathcal{L}(X)\big) \;=\; \mathrm{rg}\big(\mathcal{L}(N)\big)$$

c'est-à-dire

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N)\;.$$

Lemme II.7.8 *Sout les conditions de II.7.4.2, si Q est libre (de type fini,)*

$$\mathrm{rg}(X) \;=\; \mathrm{rg}(N) \;+\; \mathrm{rg}(Q)\;.$$

Preuve : *Si Q est libre, la suite exacte*

$$0 \;\to\; N \xrightarrow{\;i\;} X \xrightarrow{\;q\;} Q \;\to\; 0 \textit{ (cf. II.7.4.2 ,)}$$

est scindée (cf. II.3.9 ;) on a donc un isomorphisme

$$X \;\cong\; N \;\oplus\; Q$$

et le résulta découle alors du point II.7.3.ii).

Proposition II.7.9 *Soit X un groupe abélien (resp. A-module,) tel qu'on ait une suite exacte*

$$0 \to N \xrightarrow{i} X \xrightarrow{q} Q \to 0 \text{ (cf. II.7.4.2 ,)}$$

où N et Q sont des groupes abéliens (resp. A-moduless) de type fini, alors X est de type fini et

$$\mathrm{rg}(X) = \mathrm{rg}(N) + \mathrm{rg}(Q)\,.$$

Preuve *: Écrivons une décomposition de*

$$0 \to \mathrm{Tor}(Q) \xrightarrow{j_Q} Q \xrightarrow{p_Q} \mathcal{L}(Q) \to 0 \text{ (cf. II.7.4.1)}$$

où $\mathcal{L}(Q)$ est libre et $\mathrm{Tor}(Q)$ de torsion. Cette suite étant scindée on peut en fait écrire une suite exacte

$$0 \to \mathcal{L}(Q) \xrightarrow{\ell} Q \xrightarrow{t} \mathrm{Tor}(Q) \to 0 \text{ (cf. I.9.9 .)}$$

Notons alors $P := q^{-1}[\ell(\mathcal{L}(Q))]$ si bien que $q_{|P}$ donne un morphisme surjectif $p : P \to \mathcal{L}(Q)$ de noyau N (cf. I.8.16.)

On a donc un diagramme commutatif à lignes et colonnes exactes :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & N & \xrightarrow{j} & P & \xrightarrow{p} & \mathcal{L}(Q) & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_N}\downarrow & & {\scriptstyle \mathrm{Id}_{X\,|P}}\downarrow & & \downarrow{\scriptstyle \ell} & & \\
0 & \to & N & \xrightarrow{i} & X & \xrightarrow{q} & Q & \to & 0 \\
 & & {\scriptstyle 0}\downarrow & & {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle t} & & \\
 & & 0 & \to & R & \to & \mathrm{Tor}(Q) & \to & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array} \qquad \text{II.7.9.1}$$

où l'isomorphisme $R \cong \mathrm{Tor}(Q)$ n'est autre que celui du corollaire I.8.15.iii).

En appliquant le lemme II.7.7 à la suite exacte verticale centrale dans le diagramme II.7.9.1, puisque R est de torsion, on obtient

$$\mathrm{rg}(X) = \mathrm{rg}(P)\,.$$

En appliquant alors le lemme II.7.8 à la ligne horizontale du haut dans le diagramme II.7.9.1, puisque $\mathcal{L}(Q)$ est libre, on obtient

$$\mathrm{rg}(X) = \mathrm{rg}(P) = \mathrm{rg}(N) + \mathrm{rg}\big(\mathcal{L}(Q)\big) = \mathrm{rg}(N) + \mathrm{rg}(Q)\,.$$

II.8 . –Décomposition p-primaire (cf. IV.3, B.2)

Notation II.8.1 (cf. B.2.1) Pour un groupe abélien A, $p \in \mathbb{P}$ et $n \in \mathbb{N}$, on note

$$A[p^n] = \{x \in A\,;\, p^n x = 0\} \text{ sa partie de } p^n \text{ torsion (cf. II.5.2.v) ,)}$$

Définition II.8.2 (Composante p-primaire (cf. IV.3.1, B.2.2)) Pour A un groupe abélien et $p \in \mathbb{P}$, la *composante p-primaire* de A est

$$A[p^\infty] := \bigcup_{n \in \mathbb{N}} A[p^n]$$

qui est un sous-groupe de A en vertu de la proposition I.3.12.iii).

Théorème II.8.3 (de décomposition primaire (cf. IV.3.2, B.2.3)) *Étant donné un groupe abélien fini de cardinal n et d'exposant m (cf. II.5.2.iv),)*

$$\forall p \in \mathbb{P},\, A[p^\infty] = A[p^{v_p(m)}] = A[p^{v_p(n)}]\,; \qquad \textit{II.8.3.1}$$

de plus, on a des isomorphismes naturels (donnés par l'inclusion des sous-groupes :)

$$\bigoplus_{p \in \mathcal{S}(m)} A[p^\infty] \cong A\,; \qquad \textit{II.8.3.2}$$

$$\bigoplus_{p \in \mathcal{S}(n)} A[p^\infty] \cong A\,. \qquad \textit{II.8.3.3}$$

Preuve *: (cf. TD n° I, exercice A, question 10).)*

Corollaire II.8.4 (cf. B.2.5) *Étant donné un groupe abélien fini A d'exposant m, pour tout $p \in \mathcal{S}(m)$, il existe $x \in A$ d'ordre $p^{v_p(m)}$.*

Preuve *: Puisque $A[p^{v_p(m)}]$ s'injecte dans A, en vertu du théorème II.8.3, et que l'ordre se conserve par injection (cf. II.5.3.iv),) on peut supposer que $A = A[p^{v_p(m)}]$.*

On remarque alors que, pour tout $x \in A$ l'ordre de x est p^k avec $k \leq v_p(m)$. L'exposant de A étant le ***Ppcm*** *des ordres des éléments de A (cf. II.5.3.i),) il s'ensuit qu'il existe $x \in A$ d'ordre $p^{v_p(m)}$.*

II.9 . −Groupes cycliques (cf. IV.4, B.3)

Proposition II.9.1 (Groupes cycliques (cf. IV.4.1, B.3.1)) *Soit A un groupe abélien. Les assertions suivantes sont équivalentes :*

a) A est fini et $\#(A)$ est l'exposant de A (cf. II.5.2.iv).)

ii) A est fini et il existe $a \in A$ d'ordre $\#(A)$;

c) Le groupe A est monogène et fini.

d) Le groupe A est monogène (cf. II.1.7,) engendré par un élément d'ordre $d \in \mathbb{N}^*$ (cf. II.5.2.i).)

e) Il existe $d \in \mathbb{N}^*$ et un isomorphisme
$$\mathbb{Z}/d\mathbb{Z} \cong A\,.$$

f) Le groupe abéllien A est d'exposant $m \neq 0$ et isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

***Preuve** : Cet énoncé étant l'exact analogue de la proposition IV.4.1, certains arguments de preuve seront donnés ici tandis que d'autres seront donnés dans la preuve de IV.4.1 laissant le lecteur faire le parallèle entre ces deux preuves et les compléter.*

*i) (**a)** $\Rightarrow$ **ii)**)*
(cf. IV.4.1.)

*ii) (**ii)** $\Rightarrow$ **c)**)*
(cf. IV.4.1.)

*iii) (**c)** $\Rightarrow$ **d)**)*
Immédiat.

*iv) (**d)** $\Rightarrow$ **e)**)*
(cf. IV.4.1.)

*v) (**e)** $\Rightarrow$ **a)**)*
Découle du fait que $1_{\mathbb{Z}/d\mathbb{Z}}$ est précisément d'ordre d.

*vi) (**f)** $\Leftrightarrow$ **e)**)*
Est immédiat.

Définition II.9.2 (Groupes cycliques (cf. IV.4.2, B.3.2)) Un groupe vérifiant les assertions équivalentes de la proposition II.9.1 est un *groupe cyclique*. Un tel groupe est nécessairement abélien.

Proposition II.9.3 (Sous-groupe cyclique (cf. IV.4.5, B.3.5)) *Un groupe abélien A possède un sous-groupe cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$ si et seulement si A contient un élément d'ordre d.*

Proposition II.9.4 (Théorème chinois des restes (cf. IV.4.6, B.3.6)) *Si A est un groupe cyclique d'exposant m avec $m = pq$, p et q premier entre eux alors*

$$A \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} .$$

Remarque II.9.4.1 C'est exactement le théorème II.8.3 dans le cas cyclique.

Corollaire II.9.5 ((cf. IV.4.7, B.3.7)) *Soit A un groupe abélien $(x, y) \in A \times A$ d'ordres respectifs p et q avec p et q premiers entre eux, alors il existe $z \in A$ d'ordre pq.*

Preuve *:* *On a des morphismes injectifs*

$$\begin{array}{ccc} \mathbb{Z} & & \\ {\scriptstyle \pi_p}\downarrow & \searrow_{n\mapsto nx} & \\ \mathbb{Z}/p & \xrightarrow{\pi_p} & A \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{Z} & & \\ {\scriptstyle \pi_q}\downarrow & \searrow_{n\mapsto ny} & \\ \mathbb{Z}/q & \xrightarrow{\pi_q} & A \end{array} \qquad \textit{(cf. II.9.3 .)}$$

Le morphisme

$$\mathbb{Z} \times \mathbb{Z} \to A\ ,\ (m, n) \mapsto mx + ny$$

se factorise donc en un morphisme

$$\phi\ :\ \mathbb{Z}/p \times \mathbb{Z}/q \to A\ .$$

Or :

$$\begin{array}{lrcl} \forall (\alpha, \beta) = (\pi_p(m), \pi_q(n)) \in \mathbb{Z}/p \times \mathbb{Z}/q, & \phi(\alpha, \beta) & = & 0 \\ \Leftrightarrow & mx + ny & = & 0\ . \end{array}$$

Or

$$x \in A[p] \text{ et } y \in A[q]\ .$$

Comme $A[p]$ et $A[q]$ sont en somme directe (cf. II.5.4.iii),)

$$\begin{array}{rrcl} & mx + ny & = & 0 \\ \Leftrightarrow & mx = 0 & \text{et} & ny = 0 \\ \Leftrightarrow & p|m & \text{et} & q|n \\ \Leftrightarrow & \alpha = 0 & \text{et} & \beta = 0\ ; \end{array}$$

si bien que ϕ est injectif.

Enfin on dispose d'après le théorème chinois des restes, d'un isomorphisme

$$\gamma\ :\ \mathbb{Z}/(pq) \cong \mathbb{Z}/p \times \mathbb{Z}/q\ .$$

Le composé $\phi \circ \gamma$ est donc un morphisme injectif

$$\mathbb{Z}/(pq) \hookrightarrow A$$

ce qui donne, grâce encore à II.9.3 un élément d'ordre pq dans A.

II.10 . −Théorème de structure des groupes abéliens finis (cf. IV.11, B.6)

Notation II.10.0 ((cf. IV.11.0, B.6.0)) Dans tout ce paragraphe (II.10,) A est un groupe abélien fini d'exposant m. Rappelons (cf. II.5.8,) qu'il revient au même de demander que A soit de type fini (cf. II.1.5,) et de torsion (cf. II.5.2.vi).) En particulier A est d'exposant $m > 0$ (cf. II.5.7.)

Proposition II.10.1 (Existence d'un élément d'ordre maximal m (cf. IV.11.1, B.6.3)) *Il existe un élément*

$$a \in A \text{ d'ordre } m$$

i.e. un sous-groupe de A isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Preuve *: On a :*

$$A \cong \bigoplus_{p \in \mathcal{S}(m)} A[p^{v_p(m)}] \text{ (cf. II.8.3.2 .)}$$

On sait en outre, graçe au corollaire II.8.4, que, pour tout $p \in \mathcal{S}(m)$, il existe $x_p \in A$ d'ordre $p^{v_p(m)}$. Puisque $\mathcal{S}(m)$ est un ensemble fini, un argument de récurrence et le corollaire II.9.5 permettent de conclure.

Notation II.10.2 ((cf. IV.11.2, B.6.4)) Soit $C \subset A$ un sous-groupe cyclique de A isomorphe à $\mathbb{Z}/m\mathbb{Z}$ et construit grâce à la proposition II.10.1 ci-dessus. On note $Q := A/C$ si bien qu'on a une suite exacte :

$$0 \to C \xrightarrow{i} A \xrightarrow{q} Q \to 0 \,. \qquad \text{II.10.2.1}$$

Proposition II.10.3 (cf. IV.11.3) *Dans la suite exacte II.10.2.1, si Q et cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$, la surjection canonique q possède une section (cf. I.9.11.i),) i.e. il existe un morphisme de groupes*

$$s : Q \to A \text{ tel que } q \circ s = \mathrm{Id}_Q \,.$$

On déduit alors naturellement (cf. I.9.15,) de la suite exacte $0 \to C \xrightarrow{i} A \xrightarrow{q} Q \to 0$ un isomorphisme

$$A \cong C \times Q \,.$$

Preuve *: Soit y un générateur de Q (par example l'image de 1_A par la surjection canonique*

$$\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \,.)$$

Soit $x \in A$ tel que $q(x) = y$, si bien que $q(x)$ est d'ordre d. Notons n l'ordre de x. On a alors :

$$d|n|m \,. \qquad \text{II.10.3.1}$$

Par ailleurs, $q(dx) = dq(x) = 0$, c'est-à-dire que

$$dx \in \mathrm{Ker}\, q = i(C) \cong \mathbb{Z}/m\mathbb{Z} \,.$$

Soit donc z un générateur de $\mathrm{Ker}\, q$, il existe $a \in \mathbb{Z}$ tel que

$$dx = az \,.$$

Or $x \in M$, *si bien que* $mx = 0$. *Il résulte alors de II.10.3.1 qu'il existe*

$$k \in \mathbb{Z} \text{ tel que } m = dk .$$

Il s'ensuit que

$$0 = mx = kdx = kaz .$$

Comme z *est d'ordre* m,

$$kaz = 0 \Rightarrow m|ka,$$

c'est-à-dire que $dk|ka$, *d'où finalement*

$$d|a .$$

Il existe donc $b \in \mathbb{Z}$ *tel que* $a = db$.
Soit alors $w := x - bz$. *Il en résulte que*

$$dw = dx - dbz = dx - az = 0 \text{ et donc que}$$

l'ordre de w *divise* d.
Le morphisme $A \to M$, $1 \mapsto w$ *se factorise donc en un morphisme*

$$s : Q \to A , y \mapsto w .$$

Or

$$q(s(y)) = q(w)\, q(x - bz) = q(x) = y$$

d'où puisque y *est un générateur de* Q,

$$q \circ s = \mathrm{Id}_Q .$$

Proposition II.10.4 (cf. IV.11.4) *Dans la suite exacte II.10.2.1, si*

$$Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z}$$

est isomorphe à un produit de groupes cycliques alors la surrjection canonique $q : A \to Q$ *possède une section* s, *qui induit un isomorphisme*

$$A \cong C \times Q \cong \mathbb{Z}/m\mathbb{Z} \times \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} .$$

Preuve : *Supposons donc qu'il existe*

$$r \in \mathbb{N} \text{ et } d_k \,,1\leq k\leq r \ , \ \text{tels que } Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} .$$

Notons allors

$$\begin{array}{lrcl} \forall 1 \leq k \leq r, & & & \\ i_k : & \mathbb{Z}/d_k\mathbb{Z} & \longrightarrow & Q \\ & y & \longmapsto & (0, \ldots, 0, y, 0, \ldots, 0) \\ (\textit{resp. } \chi_k : & Q & \longrightarrow & \mathbb{Z}/d_k\mathbb{Z} \\ & (0, \ldots, 0, x, 0, \ldots 0) & \longmapsto & x \ ,) \end{array}$$

le morphisme injectif (resp. surjectif) défini par la structure de produit de Q comme en I.7.6. On constate alors presque immédiatement que

$$\sum_{k=1}^{r} i_k \circ \chi_k \;=\; \mathrm{Id}_Q\,. \qquad \textit{II.10.4.1}$$

Soit

$$A_k \;:=\; q^{-1}[i_k(\mathbb{Z}/d_k\mathbb{Z})],$$

d'où un diagramme commutatif :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C & \xrightarrow{j_k} & A_k & \xrightarrow{q_k} & \mathbb{Z}/d_k\mathbb{Z} & \to & 0 \\
 & & {\scriptstyle \mathrm{Id}_C}\downarrow & & {\scriptstyle \mathrm{Id}_{A\,|\,A_k}}\downarrow & & \downarrow{\scriptstyle i_k} & & \\
0 & \to & C & \xrightarrow{i} & A & \xrightarrow{q} & Q & \to & 0
\end{array}$$

Puisque

$$C \;\subset\; A_k \;\subset\; A,$$

l'exposant m de C divise l'exposant de A_k divisant lui-même l'exposant de A encore égal à m ; si bien que m est encore l'exposant de A_k.

On peut donc appliquer la proposition II.10.3 à la suite exacte

$$0 \;\to\; C \xrightarrow{j_k} A_k \xrightarrow{q_k} \mathbb{Z}/d_k\mathbb{Z} \;\to\; 0$$

du diagramme ci-dessus. Pour tout $1 \;\leq\; k \;\leq\; r$ il existe donc un morphisme

$$s_k \;:\; \mathbb{Z}/d_k\mathbb{Z} \;\to\; A_k \text{ tel que } q_k \;\circ\; s_k \;=\; \mathrm{Id}_{\,\mathbb{Z}/d_k\mathbb{Z}}\,.$$

On définit alors :

$$s \;:=\; \sum_{k=1}^{r} s_k \circ \chi_k \;:\; Q \;\to\; A\,.$$

Il s'ensuit que :

$$\begin{aligned}
q \circ s \;&=\; q \circ \big(\sum_{k=1}^{r} s_k \circ \chi_k\big) \\
&=\; \sum_{k=1}^{r} q \circ s_k \circ \chi_k \\
&=\; \sum_{k=1}^{r} i_k \circ q_k \circ s_k \circ \chi_k \\
&=\; \sum_{k=1}^{r} i_k \circ \chi_k \\
&=\; \mathrm{Id}_Q\,,
\end{aligned}$$

la dernière égalité étant II.10.4.1.

Théorème II.10.5 (de structure des groupes abéliens finis (cf. IV.11.5, B.6.13)) *Étant donné un groupe abélien fini A, il existe un unique entier $r \in \mathbb{N}$ et un unique r-uplet $d_{k\ ,1\leq k\leq r} \in \mathbb{N}$ tels que*

$$A \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z},\ d_1 > 1 \text{et } \forall 1 \leq k \leq r-1,\ d_k | d_{k+1}\ .$$

Remarque II.10.5.1 Il est immédiat de constater que si les conditions ci-dessus sont satisfaites, d_r est l'exposant de A.

Preuve *:*

i) ***(Existence)***
Si $A = \{0\}, r = 0$ convient.
Le groupe abélien A étant fini, on peut appliquer la proposition II.10.1 qui donne la suite exacte

$$0 \to C \xrightarrow{i} A \xrightarrow{q} Q \to 0 \text{ (cf. II.10.2.1 ,)}$$

où $C \cong \mathbb{Z}/m\mathbb{Z}$ est un groupe cyclique.
Bien entendu, si $Q = \{0\}, C \cong A$ et le résultat est établi.
Sinon, il résulte du téhorème I.9.19 que

$$\#(Q) < \#(A)\ .$$

On peut alors faire lh'ypothèse de récurrence qu'il existe

$$r \in \mathbb{N},\ d_{k\ ,1\leq k\leq r} \in \mathbb{N},\ d_1 > 1 \text{ tels que } Q \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} \text{ et } \forall 1 \leq k \leq r-1,\ d_k | d_{k+1}\ .$$

La proposition II.10.4 permet alors d'écrire

$$A \cong Q \times C \cong \prod_{k=1}^{r} \mathbb{Z}/d_k\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\ .$$

Le lemme II.5.3.iv) assure alors que $d_r | m$ ce qui achève la preuve.

ii) ***(Unicité)***
(cf. TD n° IV, exercice A, TD n° IV, exercice B)

Remarque II.10.5.3 Bien entendu le théorème II.10.5 peut être vu comme un corollaire du théorème B.6.13 puisque les arguments utilisés dans la preuve de ce dernier s'appliquent sans restriction aux groupes abéliens considérés comme $\mathbb{Z}$-modules.

On s'aperçoit néanmoins qu'ici, comme ce sera le cas en IV.11.5, un certain nombre d'argument est simplifié grâce notamment à des résultats come le théorème I.9.19.

Définition II.10.6 (Facteurs invariants (cf. IV.11.9, B.6.14)) Pour un groupe abélien fini A, les entiers

$$d_{k\ ,1\leq k\leq r} \text{ donnés par le théorème II.10.5}$$

ci-dessus sont appelés les *facteurs invariants* de A.

Il est d'usage de dire que lorsqu'on écrit alors

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

on a mis A sous sa *forme canonique*.

Corollaire II.10.7 ((cf. IV.11.10, B.6.15)) *i) Deux groupes abéliens finis sont isomorphes si et seulement si ils ont mêmes facteurs invariants.*

Preuve *: Soient A et B deux groupes abéliens finis. En vertu du théorème II.10.5.i), il existe*

$$r \in \mathbb{N} \text{ et } d_k\,,_{1\leq k\leq r} \text{ tels que } A \cong \mathbb{Z}/d_1\mathbb{Z}\times\ldots\times\mathbb{Z}/d_r\mathbb{Z} \text{ et } \forall 1\leq k\leq r-1,\ d_{k+1}|d_k\ .$$

Un isomorphisme $B \cong A$ donne par composition un isomorphisme

$$B \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}\ .$$

Les $d_k\,,_{1\leq k\leq r}$ sont alors les facteurs invariants de B grâce à l'énoncé d'unicité B.6.13.2).

Réciproquement si $r \in \mathbb{N}$, $d_k\,,_{1\leq k\leq r}$, sont simultanément les facteurs invariants de A et B, les isomorphismes

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \text{ et } B \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

donne un isomorphisme

$$B \cong A$$

grâce à la proposition I.4.9 par exemple.

ii) Deux groupes abéliens de type fini sont isomorphes si et seulement si ils ont même rang (cf. II.7.1) et mêmes facteurs invariants.

Preuve *: Écrivons, grâce au théorème II.6.4,*

$$A = \mathrm{Tor}(A) \oplus \mathcal{L}(A) \text{ et } B = \mathrm{Tor}(B) \oplus \mathcal{L}(B)$$

où $\mathrm{Tor}(A)$ et $\mathrm{Tor}(B)$ (resp. $\mathcal{L}(A)$ et $\mathcal{L}(B)$) sont de type fini et de torsion (resp. libres de type fini.)

Si $\phi : A \cong B$ est un isomorphisme

$$\mathrm{Tor}(\phi) : \mathrm{Tor}(A) \cong \mathrm{Tor}(B) \text{ (cf. II.5.4.ii) ,)}$$

est un isomorphisme, ce qui assure, d'après le point i) que A et B ont les mêmes facteurs invariants.

Les isomorphismes

$$A \cong B \text{ et } \mathrm{Tor}(A) \cong \mathrm{Tor}(B)$$

assurent, graçe au théorème B.1.4.ii) que $\mathcal{L}(A)$ et $\mathcal{L}(B)$ sont isomorphes, c'est-à-dire que A et B ont même rang.

Réciproquement si A et B ont les mêmes facteurs invariants il résulte de i) qu'il existe un isomorphisme $\psi : \mathrm{Tor}(A) \cong \mathrm{Tor}(B)$. Si $\mathcal{L}(A)$ et $\mathcal{L}(B)$ sont libres de type fini et ont même rang, n ils sont tous les deux isomorphes à $\mathbb{Z}^n$ ce qui done, par composition, un isomorphisme

$$\phi : \mathcal{L}(A) \cong \mathcal{L}(B)\ .$$

On vérifie facilement que le morphisme

$$\psi+\phi : A = \mathrm{Tor}(M) \oplus \mathcal{L}(A) \to B = \mathrm{Tor}(B) \oplus \mathcal{L}(B)\ ,\ (x+y) \mapsto \psi(x)+\phi(y)$$

est un isomorphisme.

Exemple II.10.8 a) Bien évidemment, étant donnés des entiers naturels $a \neq b$, $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$ ne sont pas isomorphes parce qu'il n'ont pas le même nombre d'éléments et c'est le plus élémentaire des invariant qui se conserve par isomorphisme.

b) Il n'est nul besoin des résultats donnés ci-dessus pour établir non plus que $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes, puisqu'il y a un élément d'ordre 4 dans le premier et qu'il n'y en a pas dans le second et que l'ordre se conserve par isomorphismes (cf. II.5.3.iv).) On pourrait aussi remarquer, ce qui revient un peu au même, que ces deux groupes n'ont pas même exposant.

c) Il commence à devenir délicat, en s'abstenant d'utiliser le corollaire II.10.7.i), de déterminer si $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ sont ou non isomorphes. Il n'est pas impossible qu'en analysant finement le nombre d'éléments d'ordre respectifs 2 et 4 dans chacun d'entre eux on arrive finalement à les discriminer. Se faisant, cela revient à analyser la 2^n-torsion dans chacun de ces groupes et du coup à redémontrer (partiellement peut-être) dans un cas particulier le théorème II.10.5.

Bien entendu, le premier groupe ayant pour facteurs invariants $(2, 2, 4)$ et le second $(4, 4)$ il ne sont pas isomorphes.

d) Il se peut qu'on ait affaire à des groupes qui ne sont pas donnés sous forme canonique : par exemple $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Le premier groupe n'est pas donné sous forme canonique alors que le second l'est. En appliquant itérativement le théorème chinois des restes on peut remettre ce groupe sous forme canonique ici : $\mathbb{Z}/12\mathbb{Z}$. Les facteurs invariants du premier groupe sont donc (12) tandis que ceux du second sont $(2, 6)$. Ces groupes ne sont donc pas isomorphes (à noter qu'ici en réalité l'argument de b) s'appliquait sans qu'on ait besoin d'avoir recours à des arguments sophistiqués.

e) (cf. TD n° IV, exercice C, II.12.5.)

II.11 . –Le théorème de la base adaptée et lalgorithme d'EUCLIDE–GAUSS (cf. B.7)

On donne dans ce paragraphe (II.11,) des énoncés relatifs aux groupes abéliens. Néanmoins lorsqu'un énoncé peut être donné sans difficulté pour des A-modules on le donnera. Néanmoins on prendra garde qu'il faut toujours supposer ici que A est un anneau principal. Il faudra même supposer, dans la construction que nous allons donner d'une base adaptée l'anneau A est euclidien (cf. I.13.6.1,) ce qui est bien entendu le cas de l'anneau $\mathbb{Z}$ et même de l'anneau $\mathbb{K}[X]$ (cf. III.4.2.) On pourra se reporter, pour des énoncés ne faisant pas intervenir cette hypothèse, c'est-à-dire valables pour des anneaux principaux quelconques aux paragraphes B.7.1 et B.7.2.

Définition II.11.1 (BAse adaptée) On dit qu'un couple $M \subset L$ de groupes abéliens (resp. A-modules,) libres de type fini (cf. II.3.2,) admet une *base adaptée*, s'il existe une base $\lambda_{i\ ,1\leq i\leq r}$ de L, un entier $s \leq r$, des éléments

$$d_{i\ ,1\leq i\leq s} \in \mathbb{Z}(\text{resp. } A) \text{ tel que } d_i\lambda_{i\ ,1\leq i\leq s} \text{ soit une base de } M$$

et

$$\forall 1 \leq i \leq s-1,\ d_{i+1}|d_i\ .$$

Remarque II.11.2 Si $\mathfrak{I} \subset A$ est un idéal, puisque A est principal, il existe $a \in A$ tel que $\mathfrak{I} = Aa$. Si $\mathfrak{I} \neq \{0\}$, $a \neq 0$ est une base de $\mathfrak{I}$. Comme 1 est une base de A, c'est une base adaptée pour $\mathfrak{I} \subset A$. On peut donc trouver une base adaptée dans cette situation.

Proposition II.11.3 *Si un couple $M \subset L$, possède une base adaptée*

$$\left(\lambda_{i\ ,1\leq i\leq r}\ , d_{i\ ,1\leq i\leq s}\right)_{,s\leq r} \forall 1 \leq i \leq s-1,\ d_{i+1}|d_i,$$

les éléments d_i non inversibles sont les facteurs invariants de L/M (cf. II.10.6, B.6.14.)

Preuve *: Soit $P := \mathbb{Z}^{-s}(\text{resp. } A^{r-s},)$ muni de sa base canonique (cf. II.1.4.c),) $\varepsilon_{i\ ,s+1\leq i\leq r}$. Soit*

$$Q := A/d_1 \times \ldots \times A/d_s \times P\ .$$

Il résulte du théorème II.6.4 (resp. B.1.4,) que

$$\mathrm{Tor}_A(Q) = A/d_1 \times \ldots \times A/d_s \text{ et } \mathrm{rg}(Q) = r-s\ .$$

Définissons un $\mathbb{Z}(\text{resp. } A)$-morphisme :

$$\begin{array}{rccl} \phi: & L & \longrightarrow & Q \\ & \lambda_i & \longmapsto & 1_{A/d_i}\ ,\ \forall 1 \leq i \leq s, \\ & \lambda_i & \longmapsto & \varepsilon_i\ ,\ \forall s+1 \leq i \leq r,\ . \end{array}$$

Alors :

Lemme II.11.3.1 *Le morphisme ϕ est surjectif et M est son noyau.*

Il découle alors du lemme II.11.3.1 ci-dessus et du théorème de factorisation des morphismes (cf. I.8.11,) qu'il existe un isomorphisme

$$\psi\ :\ L/M \cong Q \text{ tel que } \psi \circ \pi = \phi \text{ où } \pi\ :\ L \to L/M \text{ est la surjection canonique}\ .$$

Puisque

$$\forall 1 \leq i \leq s-1,\ d_{i+1} | d_i,$$

il existe un unique $1 \ \leq \ t \ \leq \ s$ *tel que*

$$d_i \ \in \ \mathbb{Z}^\times (\textit{resp. } A^\times) \ \Leftrightarrow \ i \geq t \ .$$

Comme pour $i \ \geq t$, $A/d_i \ = \ \{0\}$, *on en déduit que*

$$\mathrm{Tor}_A(Q) \ = \ A/d_1 \ \times \ \ldots \ \times \ A/d_t \ .$$

La condition $d_{i+1}|d_i$ *assure l'unicité de cette décomposition dans le théorème II.10.5.ii) (resp. B.6.13.2),) si bien que les* $d_{i\ ,1\leq i\leq t}$ *sont bien les facteurs invariant de* L/M.

***Preuve** (**du lemme II.11.3.1**):*

i) (***Surjectivité de*** ϕ)
Pour tout $\alpha \ \in \ Q$, *il existe un unique couple* (α_t, α_l),

$$\alpha_t \ \in \ \prod_{i=1}^{s} A/d_i \text{ et } \alpha_l \ \in \ P \textit{ tel que } \alpha \ = \ \alpha_t \ + \ \alpha_l \ .$$

Or

$$\exists a_{i\ ,1\leq i\leq s} \ \in \ A,\ \alpha_t \ = \ \big(a_1 1_{A/d_1}, \ldots, a_s 1_{A/d_s}\big) \text{ et } \exists a_{i\ ,s+1\leq i\leq r} \ \in \ A,\ \alpha_l \ = \ \sum_{i=s+1}^{r} a_i \varepsilon_i \ .$$

On vérifie alors que :

$$\begin{aligned} \phi\big(\sum_{i=1}^{r} a_i\lambda_i\big) \ &= \ \phi\big(\sum_{i=1}^{s} a_i\lambda_i\big) + \phi\big(\sum_{i=s+1}^{r} a_i\lambda_i\big) \\ &= \ \alpha_t + \alpha_l \\ &= \ \alpha \ . \end{aligned}$$

ii) (***Le noyau de*** ϕ)
Pour tout

$$x \ := \ \sum_{i=1}^{r} a_i\lambda_i \ \in \ M,$$

$\phi(x) \ = \ 0$ *entraîne que*

$$\phi\big(\sum_{i=1}^{s} a_i\lambda_i\big) \ = \ 0 \text{ et } \phi\big(\sum_{i=s+1}^{r} a_i\lambda_i\big) \ = \ 0$$

puisque $Q \ = \ \mathrm{Tor}_A(Q) \ \oplus \ P$.

La seconde égalité entraîne $\sum_{i=s+1}^{r} a_i\varepsilon_i \ = \ 0$ *qui entraîne*

$$\forall i \leq s+1 \leq r,\ a_i \ = \ 0$$

puisque $\varepsilon_{i\ ,1\ \leq\ s+1\ \leq\ i}$ *est une base de* P.

Par ailleurs $\phi(\sum_{i=1}^{s} a_i\lambda_i) \ = \ 0$, *équivaut à*

$$\forall 1 \leq i \leq s, \ a_i 1_{A/d_i} \ = \ 0$$

ce qui équivaut encore à

$$\forall 1 \leq i \leq s, \ d_i | a_i$$

qui équivaut finalement à

$$\forall i \leq 1 \leq s, \ a_i\lambda_i \ \in \ M \ .$$

Corollaire II.11.4 *Si* $M \ \subset \ L$ *possède une base adaptée*

$$\left(\lambda_i \ ,1\leq i\leq r \ , d_i \ ,1\leq i\leq s \ \right) \ ,s\leq r \ \forall 1 \leq i \leq s-1, \ d_{i+1}|d_i,$$

le s*-uplet* $d_i \ ,1\leq i\leq s$ *est unique (à association près.)*

Preuve *: C'est bien entendu une conséquence de l'identification faite entre les* $d_i \ ,1\leq i\leq s$ *et les facteurs invariants dans la proposition II.11.3 et l'énoncé d'unicité dans le théorème II.10.5.ii) (resp. B.6.13.2).)*

Notation II.11.5 Pour deux entiers naturels n et p, on note $\mathcal{M}_{n,p}(A)$ l'ensemble des matrices à n lignes et p colonnes à coefficients dans A et $\mathcal{M}_n(A) \ := \ \mathcal{M}_{n,p}(A)$ pour $p \ = \ n$ l'ensemble des matrices à n lignes et n collonnes à coefficients dans A.

Pour tous $(m,n,p) \ \in \ \mathbb{N}\times\mathbb{N}\times\mathbb{N}$, $(M,N) \ \in \ \mathcal{M}_{m,n}(A) \ \times \ \mathcal{M}_{n,p}(A)$, le produit $M \cdot N$ est défini de manière usuelle.

En particulier $(\mathcal{M}_n(A),+,\cdot)$ a une structure d'anneau (non commutatif en général) et on note $\mathrm{GL}_n(A)$ le groupe des élément inversibles de $\mathcal{M}_n(A)$ qu'on apelle ordinairement le *groupe linéaire*.

On notera

$$O_{1,n} \ \in \ \mathcal{M}_{1,n}(A) (\text{resp. } O_{n,1} \ \in \ \mathcal{M}_{n,1}(A) \ )$$

la matrice dont tous les coefficients sont nuls.

Lemme II.11.6 *Étant donné un* A*-module* L *libre de type fini et de rang* n*, muni d'une base* $\lambda_i \ ,1\leq i\leq n$ *l'application qui à tout endomorphisme*

$$f \ \in \ \mathrm{End}_A(L) \ = \ \mathrm{Hom}_A(L,L)$$

de L *associe la matrice* $M(f)$ *définie par*

$$\forall 1 \leq j \leq n, \ f(\lambda_j) \ = \ \sum_{i=1}^{n} M(f)_{i,j}\lambda_i$$

est un isomorphisme d'anneaux.

En particulier pour tout $f \ \in \ \mathrm{End}_A(L)$ f *est un automorphisme si et seulement si sa matrice* $M(f)$ *est inversible i.e.*

$$f \ \in \ \mathrm{Aut}_A(L) \ \Leftrightarrow \ M(f) \ \in \ \mathrm{GL}_n(A) \ .$$

Notation II.11.7 Soit $n \ \in \ \mathbb{N}^*$ un entier et L un A-module libre de rang n rapporté à une base $\lambda_i \ ,1\leq i\leq n$. On note $I_n \ \in \ \mathcal{M}_n(A)$ la matrice identité. Pour $M \ \in \ \mathcal{M}_{n,p}(A)$:

i) $((\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M)))$

l'opération sur les lignes de M symboliquement notée $(\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M))$ consistant à échanger la $i^{\text{ième}}$ et la $j^{\text{ième}}$ ligne, correspond à la multiplication à gauche par la matrice $P_{i,j}^{(n)}$ obtenue à partir de la matrice I_n en appliquant la permutation des lignes $\mathrm{Ligne}_i(I_n)$ et $\mathrm{Ligne}_j(I_n)$, qui correspond (par l'isomorphisme construit dans le lemme II.11.6,) à l'automorphisme de L défini par

$$\lambda_i \mapsto \lambda_j \ , \ \lambda_j \mapsto \lambda_i \ , \ \forall 1 \leq k \leq n, \ k \neq i \ , \ k \neq j \ , \ \lambda_k \mapsto \lambda_k \ ;$$

ii) $((\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M)))$

l'opération sur les lignes de m symboliquement notée $(\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M))$ consistant à remplacer la $i^{\text{ième}}$ ligne par une combinaison linéaire de cette dernière et d'une autre ligne, correspond à la multiplication à gauche par la matrice $T_{i,j}^{(n)}(a)$, *matrice de transvection* obtenue à partir de I_n par application de la transvection $(\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M))$, correspondant à l'automorphisme de L défini par

$$\lambda_j \mapsto \lambda_j + a\lambda_i \ , \ \forall 1 \leq k \leq n, \ k \neq j \ , \ \lambda_k \mapsto \lambda_k \ ;$$

iii) les opérations sur les colonnes correspondent, elles, à des multiplications à droite par les matrices $P_{i,j}^{(p)}$ et ${}^tT_{i,j}^{(p)}(a)$.

Remarque II.11.8 Les matrices $P_{i,j}^{(n)}$ et $T_{i,j}^{(n)}(a)$ introduites en II.11.7.i) et II.11.7.ii) correspondant à des automorphismes de L, sont donc inversibles.

II.11.9 . –[

Description de l'algorithme] L'algorithme consiste à transformer une matrice $M \in \mathcal{M}_{n,p}(A)$ par des opérations élémentaire sur les lignes et les colonnes. Seules les opérations suivantes sont autorisées :

—

$$\text{les permutations de lignes } (\mathrm{Ligne}_i(M) \leftrightarrow \mathrm{Ligne}_j(M))$$
$$\text{ou de colonnes } (\mathrm{Colonne}_i(M) \leftrightarrow \mathrm{Colonne}_j(M)),$$

—

$$\text{les transvections de lignes } (\mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) + a\mathrm{Ligne}_j(M) \ , \ i,j \in \{1,\dots,n\} \ , \ a \in A)$$
$$\text{ou de colonnes } (\mathrm{Colonne}_i(M) \leftarrow \mathrm{Colonne}_i(M) + a\mathrm{Colonne}_j(M) \ , \ i,j \in \{1,\dots,p\} \ , \ a \in A) \ .$$

—

$$\text{La multiplication d'une ligne et d'une colonne par } -1 \ .$$
$$(\mathrm{Ligne}_i(M) \leftarrow -\mathrm{Ligne}_i(M)) \text{ et } (\mathrm{Colonne}_j(M) \leftarrow -L\mathrm{Colonne}_j(M)) \ .$$

Comme dans l'algorithme de Gauss habituel, les opérations élémentaires correspondent à la multiplication par des matrices inversibles dans l'anneau $\mathcal{M}_n(A)$ (respectivement $\mathcal{M}_p(A)$). Une suite finie d'opérations élémentaires autorisées transforment donc la matrice M en une matrice de la forme PMQ où $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_p(A)$

Très précisément, il s'agit, par une suite finie d'opérations élémentaires autorisées, de transformer la matrice non nulle

$$M := (m_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathcal{M}_{n,p}(A) \qquad \text{II.11.9.1}$$

en une matrice de la forme (quasi-diagonale)

$$D \;=\; \begin{pmatrix} d_1 & 0 & & & 0 \\ 0 & d_2 & 0 & & \\ & & \ddots & & \\ & & & d_s & 0 \\ 0 & & & & 0 \end{pmatrix} \text{ où :} \qquad \text{II.11.9.2}$$

$$1 \;\leq\; s \;\leq\; \min(n,p)\,,$$
$$d_{i\,,1\leq i\leq s} \;\in\; A$$
$$d_1|d_2|\ldots|d_s\,.$$

Tous les autres coefficients de D sont nuls.

Notation II.11.9.3 L'anneau A étant euclidien on note

$$\mathbf{v} \;:\; A \;\setminus\; \{0\} \;\to\; \mathbb{N}$$

le *stathme euclidien* (cf. I.13.6.1.)

$$\text{si } A \;=\; \mathbb{Z}\,,\; \forall n \in \mathbb{Z} \;\setminus \{0\},\; \mathbf{v}(n) \;=\; |n|\,;$$

$$\text{si } A \;=\; \mathbb{K}[X]\,,\; \forall P \in \mathbb{K}[X] \;\setminus\; \{0\},\; \mathbf{v}(P) \;=\; \deg(P)\,.$$

Pour toute matrice

$$M \;:=\; (m_{i,j})_{\substack{1\,\leq\, i\,\leq\, n\\ 1\,\leq\, j\,\leq\, p}} \;\in\; \mathcal{M}_{n,p}(A),$$

on note

$$\mathbf{v}(M) \;:=\; \min_{\substack{1\,\leq\, i\,\leq\, n\\ 1\,\leq\, j\,\leq\, p}, m_{i,j}\,\neq\,0} \big(m_{i,j}\big)\,.$$

À chaque étape de l'algorithme, l'entier strictement positif $\mathbf{v}(M)$ décroît strictement, ce qui assure la finitude de l'algorithme.

Définition II.11.9.4 (Pivot) Un coefficient $m_{i,j}$ de M tel que $\mathbf{v}(m_{i,j}) \;=\; \mathbf{v}(M)$ s'appelle un *pivot*.

II.11.10 . –Les étapes de l'algorithme

i) (**Première étape**)

a) On choisit un pivot $m_{i,j}$ que l'on amène à la position $(1,1)$ grâce aux transpositions

$$\mathrm{Ligne}_1(M) \leftrightarrow \mathrm{Ligne}_i(M) \text{ et } \mathrm{Colonne}_1(M) \leftrightarrow \mathrm{Colonne}_j(M)\,.$$

b) Pour j de 2 à p et pour i de 2 à n on effectue les divisions euclidiennes

$$m_{1,j} \;=\; q_j m_{1,1} \;+\; r_j \text{ et } m_{i,1} \;=\; q'_i m_{1,1} \;+\; r'_i\,;$$

puis les transvections

$$\mathrm{Colonne}_j(M) \leftarrow \mathrm{Colonne}_j(M) - q_j \mathrm{Colonne}_1(M) \text{et } \mathrm{Ligne}_i(M) \leftarrow \mathrm{Ligne}_i(M) - a\mathrm{Ligne}_1(M)\,.$$

c) On a alors

$$\mathbf{v}(m_{1,j}) \ < \ \mathbf{v}(m_{1,1}) \text{ et } \mathbf{v}(m_{i,1}) \ < \ \mathbf{v}(m_{1,1}) \ \forall j > 1 \text{ et } i > 1 \ .$$

Si tous les $m_{1,j}$ et $m_{i,1}$ sont nuls, on passe à la deuxième étape ii).

Sinon on choisit l'un de ces coefficient non nul, on le place en position $(1,1)$ par une transposition, et on recommence b).

Puisque $\mathbf{v}(m_{1,1})$ diminue strictement à chaque étape le processus s'arrête, et on arrive à une matrice de la forme

$$\begin{pmatrix} m_{1,1} & O_{1,p-1} \\ O_{n-1,1} & M' \end{pmatrix} \text{ où } M' \ \in \ \mathcal{M}_{n-1,p-1}(A) \ . \qquad 1$$

ii) (**Deuxième étape**)

Si $m_{1,1}$ divise tous les coefficients de M', on passe à la troisième étape iii). Sinon, on choisit un coefficient $m_{i,j}$ qui n'est pas divisible par $m_{1,1}$ et on effectue l'opération $\mathrm{Ligne}_1(M) \leftarrow \mathrm{Ligne}_1(M) + \mathrm{Ligne}_j(M)$. (Notons que le coefficient $m_{1,1}$ n'est pas modifié). On recommence alors la première étape i) à partir de i).b) : divisions euclidiennes, transvections, transposition. On arrive à une matrice de la forme i).c).1 mais avec une nouvelle valeur de $\mathbf{v}(m_{1,1})$ strictement plus petite.

Comme à chaque fois la valeur de $\mathbf{v}(m_{1,1})$ diminue strictement, on arrive à une matrice de la forme

$$\begin{pmatrix} m_{1,1} & O_{1,p-1} \\ O_{n-1,1} & M' \end{pmatrix} \text{ où } M' \ \in \ \mathcal{M}_{n-1,p-1}(A) \qquad 1$$

et où $m_{1,1}$ divise tous les coefficients de M'.

iii) (**Troisième étape**)

On applique les étapes i) et ii) à la matrice M', ce qui ne modifie pas la première ligne et la première colonne. En répétant un nombre fini de fois le processus, on arrive à la forme quasi-diagonale II.11.9.2 souhaitée.

Proposition II.11.11 *Étant donnés deux entiers n et p la donnée d'une matrice M comme en II.11.9.1 équivaut à se donner les coordonnées de p vecteurs de A^n (ou d'un A-module libre de rang n, rapporté à une base.) Soit B le sous-A-module de A^n engendré par ces p vecteurs. Les multiplications autorisée à gauche de la matrice M correspondent à des changements de base dans A^n tandis que les multiplications autorisées à droite de M changent les générateurs de B en une autre famille de générateurs.*

Il s'ensuit, qu'au terme des transformations effectuées, le sous-A-module engendré par les colonnes de la matrice D (II.11.9.2) est encore B. Ces colonnes constituent alors manifestement une famille libre i.e. une base de B et cette base est évidemment adaptée à $B \ \subset \ A^n$ (cf. II.11.1.)

Si donc les étapes de l'algorithme ne sont pas uniques, si même les matrices P et Q telles que $D \ = \ PMQ$, ne le sont pas non plus le s-uplet $d_i \ ,1\leq i\leq s}$ constituant les éléments diagonaux de D, est quant à lui unique en vertu du théorème B.7.1.8.2). aux termes de la proposition II.11.3, ce sont mêmes des générateurs des facteurs invariants (cf. II.10.6,) du quotient A^n/B.

Théorème II.11.12 *Si $M \ \subset \ L$ sont des groupes abéliens, et L est libre de type fini (cf. II.3.2,) alors M est libre de type fini et le couple (L,M) possède une base adaptée $\left(\lambda_i \ ,1\leq i\leq r} \ , d_i \ ,1\leq i\leq s}\right) \ ,s\leq r} \ \forall 1 \leq i \leq s-1, \ d_{i+1}|d_i$, (ce qui contient en particulier le fait que $\mathrm{rg}(M) \ \leq \ \mathrm{rg}(L)$.) De plus le s-uplet $d_i \ ,1\leq i\leq s}$ est unique.*

Preuve *: D'abord le théorème II.4.6 assure que M est libre de type fini et $\mathrm{rg}(M) \ \leq \ \mathrm{rg}(L)$.*

Ensuite, l'existence d'une base adaptée est assurée par la proposition II.11.11.

L'unicité est finalement assurée par le corollaire II.11.4.

Exemple II.11.13 (Vecteur primitif) Soit $M := \begin{pmatrix} 6 & 10 & 30 \end{pmatrix}$ On effectue une suite d'opérations sur les colonnes :

$$\begin{array}{rcl} & & \begin{pmatrix} 6 & 10 & 30 \end{pmatrix} \\ \mathrm{Colonne}_3(M) \leftarrow \mathrm{Colonne}_3(M) - 5\mathrm{Colonne}_1(M), & & \\ \mathrm{Colonne}_2(M) \leftarrow \mathrm{Colonne}_2(M) - \mathrm{Colonne}_1(M) & \to & \begin{pmatrix} 6 & 4 & 0 \end{pmatrix} \\ \mathrm{Colonne}_1(M) \leftarrow \mathrm{Colonne}_1(M) - \mathrm{Colonne}_2(M) & \to & \begin{pmatrix} 2 & 4 & 0 \end{pmatrix} \\ \mathrm{Colonne}_2(M) \leftarrow \mathrm{Colonne}_2(M) - 2\mathrm{Colonne}_1(M) & \to & \begin{pmatrix} 2 & 0 & 0 \end{pmatrix} = D\,. \end{array}$$

On obtient la matrice Q en appliquant la suite d'opérations élémentaires à la matrice I_3 :

$$Q = \begin{pmatrix} 2 & -5 & -5 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On a donc

$$\begin{pmatrix} 2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 10 & 30 \end{pmatrix} \begin{pmatrix} 2 & -5 & -5 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}\,.$$

On a aussi

$$Q^{-1} = \begin{pmatrix} 3 & -5 & -15 \\ 1 & 2 & 5 \\ 0 & 0 & 1 \end{pmatrix}$$

et donc

$$\begin{pmatrix} 6 & 10 & 30 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & -5 & -15 \\ 1 & 2 & 5 \\ 0 & 0 & 1 \end{pmatrix}\,.$$

Remarque II.11.14 Comparer l'exemple ci-dessus au corollaire B.7.1.4.

Exemple II.11.15 Trouver une base de $\mathbb{Z}^3$ adaptée au sous-module F engendré par les vecteurs

$$y_1 := \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \text{ et } y_2 := \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}\,.$$

On a ici $Y = \begin{pmatrix} 1 & 2 \\ 1 & -1 \\ -1 & 0 \end{pmatrix}$ et en appliquant l'algorithme d'Euclide-Gauss on voit que la suite d'opérations élémentaires

$$\begin{array}{c} \mathrm{Colonne}_2(Y) \leftarrow \mathrm{Colonne}_2(Y) - 2\mathrm{Colonne}_1(Y)\,, \\ \mathrm{Ligne}_2(Y) \leftarrow \mathrm{Ligne}_2(Y) - \mathrm{Ligne}_1(Y)\,, \\ \mathrm{Ligne}_3(Y) \leftarrow \mathrm{Ligne}_3(Y) + \mathrm{Ligne}_1(Y)\,, \\ \mathrm{Ligne}_2(Y) \leftarrow \mathrm{Ligne}_2(Y) + \mathrm{Ligne}_3(Y)\,, \\ \mathrm{Ligne}_3(Y) \leftarrow \mathrm{Ligne}_3(Y) + 2\mathrm{Ligne}_1(Y) \end{array}$$

transforment la matrice Y en la matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{pmatrix}$. On en déduit que

$$Y = P^{-1}DQ \text{ avec } P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

On a alors $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & -1 \\ -1 & -2 & 1 \end{pmatrix}$. La base

$$\left\{ e_1 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \ e_2 = \begin{pmatrix} 0 \\ 3 \\ -2 \end{pmatrix}, \ e_3 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\}$$

est donc adaptée au sous espace F : c'est une base de $\mathbb{Z}^3$ et $(e_1, -e_2)$ est une base de F.

Exemple II.11.16 (Résolution d'un système $\mathbb{Z}$-linéaire) Soit

$$A := (a_{i,j}) \in \mathcal{M}_{n,p}(\mathbb{Z}) \text{ et } B := \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{Z}).$$

On cherche à résoudre le système linéaire $AX = B$, avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$.

i) (**Cas d'un système homogène**)

L'ensemble F de ses solutions est un sous-module de $\mathbb{Z}^p$. Il est libre, de rang $p - k$ où k est le rang de la matrice A. On écrit A sous la forme $A = PDQ^{-1}$ où D (cf. II.11.9.2.) Le système s'écrit alors $PDQ^{-1}X = 0$, c'est à dire $DY = 0$ où

$$Y = Q^{-1}X = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}.$$

L'ensemble des solutions du système $DY = 0$ est le sous $\mathbb{Z}$-module dont une base est $(Y_{k+1}, \ldots, Y_p)$ où Y_j est le vecteur colonne dont toutes les coordonnées sont nulles, sauf la coordonnée d'indice j qui vaut 1. Les vecteurs $X_j = QY_j$ $(k+1 \leq j \leq p)$ forment donc une $\mathbb{Z}$-base de F. Si l'on préfère une représentation paramétrique on peut écrire :

$$F = \left\{ \sum_{j=k+1}^{p} t_j X_j \ , \mid (t_{k+1}, \ldots t_p) \in \mathbb{Z}^{p-k} \right\}.$$

ii) (**Cas général**)

Le système s'écrit alors sous la forme

$$DY = C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

où $C = P^{-1}B$.

Pour que le système soit compatible il faut et il suffit que

$$\begin{cases} d_1|c_1, \ldots, d_k|c_k \\ c_{k+1} = \ldots = c_n = 0\,. \end{cases}$$

Les solutions du système $DY = C$ sont de la forme

$$\begin{pmatrix} c_1/d_1 \\ \vdots \\ c_k/d_k \\ t_{k+1} \\ \vdots \\ t_p \end{pmatrix}$$

où $t_{k+1,\ldots t_p}$ sont des entiers arbitraires. Les solutions du système $AX = B$ sont alors de la forme

$$(c_1/d_1)X_1 + \ldots + (c_k/d_k)X_k + t_{k+1}X_{k+1} + \ldots + t_pX_p$$

où $t_{k+1}, \ldots, t_p$ sont arbitraires dans $\mathbb{Z}$. On retrouve bien, comme dans le cas des espaces vectoriels" la structure de "sous-module affine" de l'ensemble des solutions. (On parle plus volontiers, dans ce cas, d'*espace principal homogène*).

iii) On peut traiter ici, à titre d'exemple, la résolution de l'équation $a_1x_1 + \ldots + a_px_p = b$. où a_1,..., a_p sont des entiers premiers entre eux.

II.12 . −Exercices

Exercice II.12.1 Démontrer les points II.1.11.i) et II.1.11.ii).

Exercice II.12.2 Soit M un A-module et $\mathcal{B}$ une base de M. Pour tout A-module N, définir une bijection entre l'ensemble des applications de $\mathcal{B}$ dans N et l'ensemble $\mathrm{Hom}_A(M,N)$ des morphismes de A-modules de M dans N.

Exercice II.12.3 Soit $n \in \mathbb{Z}$ un entier strictement plus grand que 1.

1) Montrer que $\{n\}$ est une partie libre maximale du $\mathbb{Z}$-module $\mathbb{Z}$ mais n'est pas une base.

2) Montrer que le sous-$\mathbb{Z}$-module $n\mathbb{Z}$ de $\mathbb{Z}$ n'a pas de supplémentaire dans $\mathbb{Z}$.

3) Montrer que $\mathbb{Z}$ et $n\mathbb{Z}$ sont des $\mathbb{Z}$-module libre de type fini et de rang 1.

Exercice II.12.4 [Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$]

1) Étant donnée une application $f : E \to F$, rappeler rapidement pourquoi, si f est surjective,

$$\forall A \subset F \; f(f^{-1}(A)) = A \, .$$

2) Soit G un groupe abélien, H un sous-groupe de G, et $\pi : G \to G/H$ la projection canonique. Notons $\mathcal{E}$ (resp. $\mathcal{F}$,) l'ensemble des sous-groupes de G contenant H, (resp. l'ensemble des sous-groupes de G/H.)

Montrer que les applications

$$\pi_* : \mathcal{E} \to \mathcal{F} \, , \; K \mapsto \pi(K) \text{ et } \pi^* : \mathcal{F} \to \mathcal{E} \, , \; L \mapsto \pi^{-1}(L)$$

sont bien définies et inverses l'une de l'autre.

3) Soit $n \in \mathbb{N}^*$,

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \, , \; x \mapsto x \, mod \, n$$

la projection canonique et L un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer qu'il existe un unique $d \in \mathbb{N}$, tel que

$$d|n \text{ et } L = \pi(d\mathbb{Z}) \, .$$

b) Construire un isomorphisme

$$\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/L \, .$$

On note $n = de$.

c) Construire un isomorphisme

$$\mathbb{Z}/e\mathbb{Z} \cong L \, .$$

Exercice II.12.5 [cf. IV.12.1]

1) Parmi les groupes suivants, lesquels sont isomorphes (justifier) :

$$G_1 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, G_2 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}, G_3 = (\mathbb{Z}/27\mathbb{Z})^\times \times \mathbb{Z}/25\mathbb{Z},$$
$$G_4 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

Lesquels sont cycliques ?

2) Déterminer les classes d'isomorphisme de groupes abéliens d'ordre 32, puis les classes d'isomorphisme de groupes abéliens d'ordre 18.

3) Un groupe abélien G a un élément d'ordre 11×2^4 et au moins 26 éléments d'ordre 11. Quel est le plus petit ordre possible du groupe ? Donner alors la structure (ou les structures possibles) pour cet ordre.

4) Déterminer à isomorphisme près les groupes abéliens de cardinal 300.

5) Les groupes abéliens

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \text{ et } \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$

sont-ils isomorphes ?

6) (**Groupes abéliens à** 144 **éléments**)
Donner les classes d'isomorphismes de groupes abéliens de cardinal 144.

7) Soit A **le groupe abélien** $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.
Trouver les entiers $k \geq 1$ et d_i ,$_{1 \leq i \leq k} \geq 2$ tels que :
— pour tout $1 \leq i < k$, $d_{i+1} | d_i$ et
—

$$A \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} .$$

8) Soit $G = \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/125\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Donner les invariants du groupe abélien fini G. Combien y a-t-il de sous-groupes d'exposant 5 dans G ?

9) On pose

$$A := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} , \; B := \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} , C := \mathbb{Z}/5\mathbb{Z} .$$

Trouver les entiers $k \geq 1$ et $d_i \geq 2$ pour $1 \leq i \leq k$ tels que d_{i+1} divise d_i pour tout $1 \leq i < k$ et tels que

$$A \times B \times C = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z} .$$

10) On admet que le groupe multiplicatif de l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ est cyclique quand p est un nombre premier impair. Trouver les entiers $k \geq 1$ et $d_i \geq 2$ pour $1 \leq i \leq k$ tels que d_{i+1} divise d_i pour tout $1 \leq i < k$ et tels que $(\mathbb{Z}/91\mathbb{Z})^\times \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_k\mathbb{Z}$.

11) a) On rappelle/admet que si p est un nombre premier impair et $n \geq 1$, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ des éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$ est cyclique. Donner son cardinal.

b) Soit $G = (\mathbb{Z}/6615\mathbb{Z})^\times$. Ecrire G sous la forme $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ avec s un entier positif et d_i des entiers positifs et $d_{i+1}|d_i$ pour $1 \leq i \leq s-1$.

12) Soient p, q, r trois nombres premiers distincts. Combien y a-t-il de classes d'isomorphismes de groupes abéliens d'ordre $p \times q^3 \times r^4$?

Donner la structure en termes d'entiers d_i avec $d_{i+1}|d_i$ de tous ceux possédant de plus un sous-groupe d'ordre r^3 et d'exposant r.

13) **a)** On rappelle/admet que si p est un nombre premier impair et $n \geq 1$, $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (groupe des éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$) est cyclique. Donner son cardinal.

b) Soit $G = (\mathbb{Z}/(49 \times 18 \times 17)\mathbb{Z})^\times$. Ecrire G sous la forme $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$ avec s un entier positif et d_i des entiers positifs tels que $d_{i+1}|d_i$ pour $1 \leq i \leq s-1$.