du sous-groupe $\ker \widetilde{\chi}$ divise nécessairement a. (L'exposant d'un sous-groupe divise toujours l'exposant du groupe.) □

3.2. Un exemple direct : les p-groupes abéliens élémentaires.

DÉFINITION 3.6. *Soit p un nombre premier. Un groupe abélien fini est dit* p-élémentaire *si on a $g^p = 1$ pour tout $g \in G$, soit encore en notation additive, si on a $px = 0$ pour tout $x \in G$.*

L'observation importante est qu'un tel groupe G est le groupe additif d'une unique structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En effet, pour $n \in \mathbb{Z}$ et $x \in G$, l'élément nx ne dépend que de $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$, et l'application $\mathbb{Z}/p\mathbb{Z} \times G \to G$, $(\overline{n}, x) \mapsto nx$ munit le groupe G d'une structure d'espace vectoriel sur le corps $\mathbb{Z}/p\mathbb{Z}$: on a $1x = x$, $m(nx) = (mn)x$, et $(m+n)x = mx + nx$ et $m(x+y) = mx + my$. Notons $G^\sharp$ ce $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. On constate que les sous-groupes de G coïncident avec les sous-espaces vectoriels de $G^\sharp$, que les familles génératrices du groupe G et coïncident avec celle de l'espace vectoriel $G^\sharp$, qu'un morphisme $G \to H$ est la même chose une application linéaire $G^\sharp \to H^\sharp$ etc...

PROPOSITION 3.7. *Soient p premier et G un groupe abélien fini. Alors G est p-élémentaire si, et seulement si, on a $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ pour un certain entier $n \geq 1$. De plus, le nombre minimal de générateurs de G est* $\dim_{\mathbb{Z}/p\mathbb{Z}} G^\sharp$.

DÉMONSTRATION — Pour la première assertion, il suffit de considérer une base de $G^\sharp$ comme $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Pour la seconde, c'est le fait qu'une famille d'éléments de G engendre G si, et seulement si, elle engendre le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $G^\sharp$. □

Cela redémontre (directement et facilement !) le Théorème 3.1 pour les groupes abéliens p-élémentaires : tous les facteurs invariants sont égaux à p, et il y en a exactement n où $|G| = p^n$.

3.3. Démonstration de l'unicité. Si G est un groupe, on note $\min(G)$ le nombre minimal de générateurs de G. Par définition, il est fini si, et seulement si, G est de type fini. Par la Proposition 3.7 par exemple $\min((\mathbb{Z}/p\mathbb{Z})^n) = n$ pour p premier et $n \geq 1$.

REMARQUE 3.8. Soient G et G' deux groupes et $n \geq 1$ un entier. Si $g_1, \ldots, g_n$ engendrent G, et si $f : G \to G'$ est un morphisme surjectif, alors $f(g_1), \ldots, f(g_n)$ engendrent G'. En particulier, on a $\min(G') \leq \min(G)$. En considérant la projection $G \times G' \to G, (g, g') \to g$, on en déduit par exemple $\min(G) \leq \min(G \times G')$.

Illustrons cette notion en montrant d'abord l'unicité du n dans le Théorème 3.1.

PROPOSITION 3.9. *Supposons $G = \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$ avec $n \geq 1$ et les a_i entiers tels que $a_1 \mid a_2 \mid \cdots \mid a_n$ et $a_1 > 1$. On a $n = \min(G)$.*

DÉMONSTRATION — Le groupe G est engendré par les n éléments par e_i avec $e_i = (0, \ldots, 0, \overline{1}, 0, \ldots, 0)$ (le $\overline{1}$ à la place i). On a donc $\min(G) \leq n$. D'autre part, pour p premier divisant a_1 on a $p \mid a_i$ pour tout i et on peut donc considérer un morphisme surjectif $f : G \to (\mathbb{Z}/p\mathbb{Z})^n$ en considérant coordonnée par coordonnée le morphisme évident $\mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, n \bmod a_i \mapsto n \bmod p$ (bien défini car $p \mid a_i$). D'après la Remarque 3.8, on a alors $\min(G) \geq \min((\mathbb{Z}/p\mathbb{Z})^n) = n$. □

Pour terminer la démonstration, nous allons considérer des sous-groupes naturels et judicieux des groupes abéliens finis.

DÉFINITION 3.10. *Soient G un groupe abélien et $n \geq 1$. Le sous-ensemble $G[n] = \{g \in G \mid g^n = 1\}$ est un sous-groupe de G appelée n-torsion de G.*

Ce groupe est le noyau du morphisme $G \to G,\ g \mapsto g^n$ (dont l'image, les puissance n-èmes, est intéressante aussi mais laissée de côté ici). Un élément de $G[n]$ est appelé aussi élément de n-torsion : c'est par définition un élément d'ordre fini divisant n. Si $n = p$ est premier, et si G est fini, alors $G[p]$ est abélien p-élémentaire.

LEMME 3.11. *Soient G et H deux groupes abéliens et $n \geq 1$.*

(i) On a $(G \times H)[n] = G[n] \times H[n]$.

(ii) Tout (iso-)morphisme $G \to H$ induit un (iso-)morphisme $G[n] \to H[n]$.

(iii) Supposons G cyclique d'ordre m et p premier. On a $G[p] = \{1\}$ sauf si $p|m$, auquel cas on a $G[p] \simeq \mathbb{Z}/p\mathbb{Z}$ et $G/G[p] \simeq \mathbb{Z}/(m/p)\mathbb{Z}$.

DÉMONSTRATION — Les (i) et (ii) sont évidents. Le (iii) est par exemple conséquence du Lemme 3.7 Chap. 2. De manière directe, écrivons $G = \langle g \rangle$ avec g d'ordre m. Pour $k \in \mathbb{Z}$ on a $(g^k)^p = 1$ si, et seulement si, $m \,|\, kp$. Si $p \nmid m$, cela équivaut à $k \equiv 0 \bmod m$, et donc $G[p] = \{1\}$. Si $p|m$, cela équivaut à $k \equiv 0 \bmod m/p$. On a donc $G[p] = \langle g^{m/p} \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, et le groupe $G/G[p]$, qui est engendré par l'image de g dans $G/G[p]$, est donc isomorphe à $\mathbb{Z}/(m/p)\mathbb{Z}$. □

DÉMONSTRATION — (de assertion d'unicité du Théorème 3.1) Soit $\mathscr{A}_n$ l'ensemble des suites finies $a = (a_1, \ldots, a_n)$ d'entiers ≥ 1 avec $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$ (il est plus simple dans l'argument qui suit de ne pas supposer $a_1 > 1$). Pour $a \in \mathscr{A}_n$ on pose $G_a = \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$. On suppose $a, b \in \mathscr{A}_n$ et $G_a \simeq G_b$, on veut montrer $a = b$.

On raisonne par récurrence sur $\sum_{i=1}^n (a_i + b_i)$. On conclut par récurrence si $a_1 = b_1 = 1$ car on a $\mathbb{Z}/\mathbb{Z} \simeq 1$ et $G \times 1 \simeq G$. Quitte à échanger a et b on peut supposer $a_1 > 1$. Soit p premier divisant a_1, et donc tous les a_i. Par le Lemme 3.11 (i) et (iii), on a donc $|G_a[p]| = p^n$, et $|G_b[p]| = p^r$ où r est le nombre d'entiers $1 \leq i \leq n$ tels que $p|b_i$. Mais on a aussi

$$G_a[p] \simeq G_b[p] \text{ et } G_a/G_a[p] \simeq G_b/G_b[p]$$

par le point (ii) du Lemme 3.11. De l'identité de gauche on déduit $r = n$ puis $p|b_i$ pour tout i. Mais toujours par le (iii) on constate que $G_a/G_a[p]$ et $G_b/G_b[p]$ sont respectivement isomorphes à [7] $G_{a'}$ et $G_{b'}$ avec $a'_i = a_i/p$ et $b'_i = b_i/p$ pour tout i (voir l'Exercice 2.31 Chap. 2). Par récurrence on en déduit $a' = b'$, puis $a = b$. □

7. On pourrait se passer de l'usage de quotients ici en disant que les sous-groupes des multiples de p dans G_a et G_b sont isomorphes, et respectivement isomorphes à $G_{a'}$ et $G_{b'}$.

3.4. Digression : sommes directes de groupes abéliens. Notre expérience des espaces vectoriels rend la notion de somme directe interne plus intuitive que celle de produit direct du point de vue additif. On fixe donc A un groupe abélien noté additivement. Si $A_1, A_2, \dots, A_n$ sont des sous-groupes de A, on pose

$$A_1 + A_2 + \cdots + A_n = \{\sum_{i=1}^{n} a_i \mid a_i \in A_i\}.$$

C'est manifestement un sous-groupe de A, appelé *somme* des A_i, encore noté $\sum_i A_i$. Par exemple, si $A_i = \mathbb{Z}a_i$ pour tout i, alors $A_1 + A_2 + \cdots + A_n$ coïncide avec le sous-groupe $\langle a_1, a_2, \dots, a_n\rangle$ de A engendré par les a_i. En général, l'application

$$\varphi : A_1 \times A_2 \times \cdots \times A_n \to A, (a_i) \mapsto \sum_i a_i, \tag{19}$$

est manifestement un morphisme de groupes d'image $\sum_i A_i$. Elle est surjective si, et seulement si, on a $A = \sum_i A_i$. Si φ est injectif (*i.e.* $\ker\varphi = \{0\}$), on dit que les A_i sont en *somme directe*, et on note alors aussi $\oplus_i A_i$ la somme des A_i.

Définition 3.12. *On dit que A est somme directe interne de ses sous-groupes A_i si l'application* (19) *est bijective, i.e. si on a $A = \oplus_i A_i$.*

Discutons enfin du point de vue *externe*. Maintenant $A_1, \dots, A_n$ sont des groupes abéliens quelconques et on pose $A = \prod_{i=1}^n A_i$. Pour tout i, le sous-groupe $A_i' = \{(a_j) \mid a_j = 0,\ \forall j \neq i\}$ de A est manifestement isomorphe à A_i, via l'inclusion $a \mapsto (0, \dots, a, \dots, 0)$, c'est pourquoi on le note souvent encore A_i. On a alors

$$\prod_{i=1}^{n} A_i = \bigoplus_{i=1}^{n} A_i', \text{ avec } A_i' \simeq A_i \text{ pour tout } i = 1, \dots, n.$$

C'est pourquoi lorsqu'on le voit ainsi, le groupe produit $\prod_{i=1}^n A_i$ est aussi noté $\bigoplus_{i=1}^n A_i$ et il est appelé *somme directe externe des A_i*. En particulier, on obtient la formulation suivante du Théorème 3.1.

Corollaire 3.13. *Pour tout groupe abélien fini G, de facteurs invariants a_1, a_2, $\cdots$, a_n, on a une décomposition $G = \oplus_{i=1}^n C_i$ avec C_i cyclique d'ordre a_i.*

⚠ Il faut bien noter que *la décomposition ci-dessus n'est pas unique*. En effet, considérons le cas $G = (\mathbb{Z}/p\mathbb{Z})^2$ avec p premier. Se donner une écriture $G = C_1 \oplus C_2$ avec $C_1 \simeq C_2 \simeq \mathbb{Z}/p\mathbb{Z}$ est la même chose que se donner une décomposition en somme directe de deux droites du plan $G^\sharp$: il y a exactement $p+1$ droites dans $G^\sharp$ (pourquoi ?) et donc $\frac{p(p+1)}{2}$ telles décompositions.

4. Groupes abéliens de type fini

Dans toute cette section G est un groupe abélien noté additivement.

Définition 4.1. *Soient $\mathscr{F} = \{g_1, \dots, g_n\}$ une famille d'éléments de G, et*

$$f : \mathbb{Z}^n \to G, (m_i) \mapsto \sum_{i=1}^{n} m_i g_i.$$

le morphisme de groupes associé. On dit que $\mathscr{F}$ est libre (ou $\mathbb{Z}$-libre) si f est injectif. On rappelle que $\mathscr{F}$ est génératrice (ou $\mathbb{Z}$-génératrice) si f est surjective. On dit enfin que $\mathscr{F}$ est une base (ou une $\mathbb{Z}$-base) si f est bijective.

Par exemple, la *base canonique* ϵ_i de $\mathbb{Z}^n$, définie par $(\epsilon_i)_j = \delta_{i,j}$, est clairement une $\mathbb{Z}$-base de $\mathbb{Z}^n$. L'anneau $\mathbb{Z}$ n'étant pas un corps, des différences substantielles apparaissent entre ces notions et les notions analogues dans les espaces vectoriels. Par exemple, la famille singleton $\{g\}$, avec $g \in G$, est libre si, et seulement si, g est d'ordre infini. Dans le groupe $G = \mathbb{Z}$, la famille $\{2, 3\}$ est génératrice, non libre car $2 \cdot 3 - 3 \cdot 2 = 0$, et on ne peut en extraire de base ! De même, la famille $\{2\}$ de $\mathbb{Z}$ est libre, mais elle ne se complète pas en une base : une famille $\{a, b\}$ a deux éléments non nuls de $\mathbb{Z}$ n'est jamais libre à cause de la relation $ba - ab = 0$.

Définition 4.2. *Un groupe abélien est dit* libre de rang n *s'il possède une $\mathbb{Z}$-base à n éléments, ou ce qui revient au même, s'il est isomorphe à $\mathbb{Z}^n$.*

Par conventions, $\{0\}$ est libre de rang 0. Le lemme suivant montre que l'entier n dans la définition ci-dessus est uniquement déterminé.

Lemme 4.3. *Pour tout entier $n \geq 0$ on a $\min(\mathbb{Z}^n) = n$. En particulier, on a $\mathbb{Z}^n \simeq \mathbb{Z}^m$ si, et seulement si, $n = m$.*

Démonstration — L'inégalité $\min(\mathbb{Z}^n) \leq n$ est évidente. En considérant le morphisme $\mathbb{Z}^n \to (\mathbb{Z}/2\mathbb{Z})^n$ de réduction modulo 2 sur chaque coordonnée, qui est surjectif, on a l'inégalité opposée $\min(\mathbb{Z}^n) \geq \min((\mathbb{Z}/2\mathbb{Z})^n) = n$. La seconde assertion s'en déduit car $G \simeq G'$ implique $\min(G) = \min(G')$ (Remarque 3.8 !). □

Parmi les exemples les plus importants de groupes abélien libres, on trouve les *réseaux* des espaces vectoriels réels de dimension finie.

Exemple 4.4. (*Réseaux*) Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n. Un *réseau* de V est un sous-groupe additif $\Lambda \subset V$ de la forme $\Lambda = \oplus_{i=1}^n \mathbb{Z} e_i$ avec $e_1, \ldots, e_n$ une $\mathbb{R}$-base de V. En particulier, un réseau est libre de rang n. Par exemple, $\mathbb{Z}^n$ est un réseau de $\mathbb{R}^n$. On peut démontrer la caractérisation topologique suivante : un sous-groupe H de V est un réseau si, et seulement si, (i) H et discret et (ii) H engendre V comme $\mathbb{R}$-espace vectoriel. Nous renvoyons au Complément 6 pour une démonstration de cet énoncé.

Le résulat principal suivant ramène la structure des groupes abéliens de type fini à celle des groupes abéliens finis, déjà élucidée. On pose

$$G_{\text{tor}} = \{g \in G \mid \exists n \geq 1,\ ng = 0\}$$

l'ensemble des éléments *de torsion* de G. C'est manifestement un sous-groupe de G, appelé *sous-groupe de torsion*, égal à la réunion des $G[n]$ pour $n \geq 1$.

Théorème 4.5. (Dirichlet) *Si G est un groupe abélien de type fini, son sous-groupe G_{tor} est fini et il existe un unique entier $n \geq 0$ tel que $G \simeq G_{\text{tor}} \times \mathbb{Z}^n$.*

L'entier n ci-dessus est appelé *rang* de G. On dit que G est *sans torsion* si $G_{\text{tor}} = \{0\}$.

Corollaire 4.6. *Un groupe abélien de type fini sans torsion est libre*

Pour démontrer le Théorème 4.5, nous aurons besoin du lemme suivant, qui dégage une propriété remarquable de $\mathbb{Z}$, appelée *projectivité*.

Lemme 4.7. *Soient G un groupe abélien et $f : G \to \mathbb{Z}$ un morphisme surjectif. Alors G est isomorphe à $\mathbb{Z} \times \ker f$.*

Démonstration — Par surjectivité de f, il existe $h \in G$ tel que $f(h) = 1$. L'élément h est d'ordre infini, car $nh = 0$ implique $0 = nf(h) = n \in \mathbb{Z}$. On a donc $H := \langle h \rangle \simeq \mathbb{Z}$. Vérifions que G est produit direct interne de H et de $\ker f$. On vient juste de montrer $H \cap \ker f = \{0\}$. Vérifions $G = H + \ker f$. Soit $g \in G$. Posons $n := f(g) \in \mathbb{Z}$, on a alors $f(g) = n = f(nh)$ et donc $g - nh \in \ker f$. □

Démonstration — (du Théorème) Soit G un groupe abélien de type fini. Montrons d'abord que s'il existe un élément d'ordre infini dans G, alors G est isomorphe à $G' \times \mathbb{Z}$ pour un certain groupe G'. Un tel G' est alors nécessairement abélien, et vérifie $\min(G') \leq \min(G) < \infty$ par la Remarque 3.8.

Supposons donc qu'il existe $g \in G$ d'ordre infini. Choisissons un isomorphisme $f : \langle g \rangle \xrightarrow{\sim} \mathbb{Z}$. D'après la Proposition 2.6, on peut étendre f en un morphisme $\widetilde{f} : G \to \mathbb{Q}$, car $\mathbb{Q}$ est divisible. Mais $\widetilde{f}(G)$ est un sous-groupe de type fini de $\mathbb{Q}$, donc de la forme $\mathbb{Z}\lambda$ pour un certain $\lambda \in \mathbb{Q}$ (Cor. 7.1 Chap. 1). On a $\lambda \neq 0$ car $\widetilde{f}(G)$ contient $f(G) = \mathbb{Z}$. Quitte à diviser $\widetilde{f}$ par λ, on a donc trouvé un morphisme surjectif $G \to \mathbb{Z}$. On conclut par le Lemme 4.7.

Posons $N = \min(G)$. Si on a $G \simeq G' \times \mathbb{Z}^n$ alors $N \leq n$ par le Lemme 4.3 et la Remarque 3.8. On en déduit que l'on peut itérer au plus N fois la première étape, *i.e.* qu'il existe $n \leq N$ tel que $G \simeq G' \times \mathbb{Z}^n$ et tel que tous les éléments de G' sont d'ordre fini. Mais alors on a aussi $\min(G') \leq \min(G) < \infty$, donc G' est de type fini, et comme ses él'ements sont d'ordre fini il est alors nécessairement fini (pourquoi ?). Le Lemme 4.8 montre alors $G' \simeq G_{\text{tor}}$ et $n = \min(G/G_{\text{tor}})$, d'où l'assertion d'unicité. □

Lemme 4.8. *Soient A et B deux groupes abéliens avec A fini et B libre de rang fini. Alors si on pose $G = A \times B$ on a $G_{\text{tors}} = A \times \{0\}$ et $G/G_{\text{tors}} \simeq B$.*

Démonstration — On a $G_{\text{tor}} = A_{\text{tor}} \times B_{\text{tor}}$ (Lemme 3.11) avec $A_{\text{tor}} = A$ et $B_{\text{tor}} = \{0\}$, donc $G_{\text{tors}} = A \times \{0\}$. On conclut car le morphisme de projection $G \to B, (a, b) \mapsto b$, est surjectif de noyau G_{tors}. □