Licence troisième année
Cours de Algèbre 1
2018–2019

Luis Paris

1 Groupes

1.1 Définitions et premières propriétés

Définition. Un *groupe* est un ensemble G muni d'une loi $* : G \times G \to G$, $(a, b) \mapsto a * b$ vérifiant les propriétés suivantes.

(a) La loi $*$ est *associative*, c'est-à-dire que $(a * b) * c = a * (b * c)$ pour tous $a, b, c \in G$.

(b) L'ensemble G possède un *élément neutre* pour la loi $*$, c'est à dire qu'il existe $e \in G$ tel que $a * e = e * a = a$ pour tout $a \in G$.

(c) Tout élément de G possède un *inverse*, c'est-à-dire que, pour tout $a \in G$ il existe $a' \in G$ tel que $a * a' = a' * a = e$.

Lemme 1.1. *Soit $(G, *)$ un groupe.*

(1) L'élément neutre e pour la loi $*$ est unique.

(2) Soit $a \in G$. Alors l'inverse de a est unique.

Démonstration. Supposons que G possède deux éléments neutres, e et e'. Alors $e = e * e' = e'$. Soit $a \in G$. Supposons que a possède deux inverses, a' et a''. Alors $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$. □

Remarque. Soient G un groupe et $a, b \in G$. Alors l'inverse de $a * b$ est $b^{-1} * a^{-1}$ (et non $a^{-1} * b^{-1}$). En effet $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$.

Définition. On dit qu'un groupe $(G, *)$ est *abélien* ou *commutatif* si la loi $*$ est *commutative*, c'est-à-dire $a * b = b * a$ pour tous $a, b \in G$.

Notations. L'élément neutre dans un groupe G se note normalement e ou 1 et la loi $\cdot$, $\times$ ou $*$ et l'inverse d'un élément a, a^{-1}. Par contre, si le groupe est abélien, alors l'élément neutre se note 0 et la loi $+$ et l'inverse d'un élément a, $-a$.

Exemples.

(1) $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes abéliens.

(2) Soient E un ensemble et $\mathrm{Bij}(E)$ l'ensemble des bijections de E dans E. Alors $(\mathrm{Bij}(E), \circ)$ est un groupe. L'élément neutre de $\mathrm{Bij}(E)$ est l'application identité, $\mathrm{id}_E : E \to E$. On n'a pas $f \circ g = g \circ f$ en général, donc $\mathrm{Bij}(E)$ n'est pas abélien (sauf si $\mathrm{card}(E) \leq 2$).

Définition. Soit $(G, *)$ un groupe et H une partie de G. On dit que H est un *sous-groupe* de G si :

(a) $e \in H$,

(b) $a * b \in H$ pour tout $a, b \in H$,

(c) $a^{-1} \in H$ pour tout $a \in H$.

Soient $(G, *)$ un groupe et H un sous-groupe de G. Comme on a $a * b \in H$, pour tout $a, b \in H$, on a une loi $* : H \times H \to H$, $(a, b) \mapsto a * b$. Cette loi s'appelle la *restriction* de $*$ à H. Le résultat suivant découle directement des définitions.

Lemme 1.2. *Soient $(G, *)$ un groupe, H un sous-groupe de G et $* : H \times H \to H$ la restriction de $*$ à H. Alors $(H, *)$ est un groupe.*

Proposition 1.3. *Soit H un sous-groupe de $\mathbb{Z}$. Alors $H = \{0\}$, ou bien il existe $m \in \mathbb{N}^*$ tel que $H = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$.*

Démonstration. Il est évident que $\{0\}$ est un sous-groupe de $\mathbb{Z}$. On prend donc un sous-groupe H de $\mathbb{Z}$ et on suppose que $H \neq \{0\}$. On commence par montrer que $H \cap \mathbb{N}^* \neq \emptyset$. Soit $x \in H \setminus \{0\}$. Si $x > 0$, alors $x \in H \cap \mathbb{N}^*$. Si $x < 0$, alors $-x \in H \cap \mathbb{N}^*$.

Notons m le plus petit élément de $H \cap \mathbb{N}^*$. On va montrer que $m\mathbb{Z} \subset H$. Montrons d'abord par récurrence que $mk \in H$ pour tout $k \in \mathbb{N}$. On a $m \times 0 = 0 \in H$ et $m \times 1 = m \in H$. Supposons que $mk \in H$. On a $mk, m \in H$, donc $m(k+1) = mk + m \in H$. Par le principe de récurrence on a donc $mk \in H$ pour tout $k \in \mathbb{N}$. Soit $k \in \mathbb{Z}$. Si $k \geq 0$ alors, par ce qui précède, $mk \in H$. Si $k \leq 0$ alors, par ce qui précède, $m(-k) \in H$, donc $-m(-k) = mk \in H$. On a donc $m\mathbb{Z} \subset H$.

Montrons que $H \subset m\mathbb{Z}$. Soit $x \in H$. Soit $x = mk + r$ la division de x par m. On a $r = x - mk \in H$ et $0 \leq r < m$. Comme m est le plus petit élément de $H \cap \mathbb{N}^*$, on a $r = 0$, donc $x = mk \in m\mathbb{Z}$. □

Proposition 1.4. *Soient G un groupe et $\{H_i \mid i \in I\}$ une collection de sous-groupes de G. Alors $\cap_{i \in I} H_i$ est un sous-groupe de G.*

Démonstration. Soit e l'élément neutre de G. On a $e \in H_i$ pour tout $i \in I$, donc $e \in \cap_{i \in I} H_i$. Soient $a, b \in \cap_{i \in I} H_i$. Pour tout $i \in I$ on a $a + b \in H_i$, car H_i est un sous-groupe, donc $a + b \in \cap_{i \in I} H_i$. Soit $a \in \cap_{i \in I} H_i$. Pour tout $i \in I$ on a $a^{-1} \in H_i$, donc $a^{-1} \in \cap_{i \in I} H_i$. □

Proposition 1.5. *Soient G et H deux groupes. Soit $*$ la loi sur $G \times H$ définie par*

$$(a_1, b_1) * (a_2, b_2) = (a_1 * a_2, b_1 * b_2)\,.$$

Alors $(G \times H, *)$ est un groupe.

Démonstration. Soient $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in (G \times H)$. Alors

$$\big((a_1, b_1) * (a_2, b_2)\big) * (a_3, b_3) = (a_1 * a_2, b_1 * b_2) * (a_3, b_3) = \big((a_1 * a_2) * a_3, (b_1 * b_2) * b_3\big) =$$
$$\big(a_1 * (a_2 * a_3), b_1 * (b_2 * b_3)\big) = (a_1, b_1) * (a_2 * a_3, b_2 * b_3) = (a_1 * b_1) * \big((a_2, b_2) * (a_3, b_3)\big)\,.$$

Soit $(a, b) \in (G \times H)$. Alors

$$(e_G, e_H) * (a, b) = (e_G * a, e_H * b) = (a, b)\,.$$

De même, on a $(a, b) * (e_G, e_H) = (a, b)$. Par ailleurs,

$$(a, b) * (a^{-1}, b^{-1}) = (a * a^{-1}, b * b^{-1}) = (e_G, e_H)\,.$$

De même, on a $(a^{-1}, b^{-1}) * (a, b) = (e_G, e_H)$. □

Définition. Soient G et H deux groupes. Une application $f : G \to H$ est un *homomorphisme* si $f(a * b) = f(a) * f(b)$ pour tous $a, b \in G$.

Lemme 1.6. *Soit $f : G \to H$ un homomorphisme de groupes.*

(1) On a $f(e_G) = e_H$.

(2) On a $f(a^{-1}) = f(a)^{-1}$ pour tout $a \in G$.

Démonstration. On a $f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$, donc

$$e_H = f(e_G) * f(e_G)^{-1} = \big(f(e_G) * f(e_G)\big) * f(e_G)^{-1} =$$
$$f(e_G) * \big(f(e_G) * f(e_G)^{-1}\big) = f(e_G) * e_H = f(e_G)\,.$$

Soit $a \in G$. Alors

$$e_H = f(e_G) = f(a * a^{-1}) = f(a) * f(a^{-1})\,.$$

De même, on a $f(a^{-1}) * f(a) = e_H$, donc $f(a^{-1}) = f(a)^{-1}$. □

Définition. Un homomorphisme $f : G \to G$ s'appelle un *endomorphisme*. Un homomorphisme bijectif $f : G \to H$ s'appelle un *isomorphisme*. Un isomorphisme $f : G \to G$ s'appelle un *automorphisme*.

Lemme 1.7. *Si $f : G \to H$ est un isomorphisme, alors la réciproque $f^{-1} : H \to G$ est un homomorphisme (et donc un isomorphisme).*

Démonstration. Soient $b_1, b_2 \in H$. On a $f(f^{-1}(b_1) * f^{-1}(b_2)) = (f \circ f^{-1})(b_1) * (f \circ f^{-1})(b_2) = b_1 * b_2$, donc $f^{-1}(b_1) * f^{-1}(b_2) = f^{-1}(b_1 * b_2)$. □

Définition. Soit $f : G \to H$ un homomorphisme. *L'image* de f, notée $\mathrm{Im}(f)$, est $f(G) = \{f(a) \mid a \in G\} \subset H$.

Lemme 1.8. *Soit $f : G \to H$ un homomorphisme de groupes.*

(1) $\mathrm{Im}(f)$ *est un sous-groupe de* H*.*

(2) f *est surjectif si et seulement si* $\mathrm{Im}(f) = H$*.*

Démonstration. La seconde partie du lemme est évidente. On démontre la première partie. $e_H = f(e_G)$, donc $e_H \in \mathrm{Im}(f)$. Soient $b_1, b_2 \in \mathrm{Im}(f)$. On prend $a_1, a_2 \in G$ tels que $b_1 = f(a_1)$ et $b_2 = f(a_2)$. Alors

$$b_1 * b_2 = f(a_1) * f(a_2) = f(a_1 * a_2)\,,$$

donc $b_1 * b_2 \in \mathrm{Im}(f)$. Soit $b \in \mathrm{Im}(f)$. On prend $a \in G$ tel que $b = f(a)$. Alors

$$b^{-1} = f(a)^{-1} = f(a^{-1})\,,$$

donc $b \in \mathrm{Im}(f)$. Ceci montre que $\mathrm{Im}(f)$ est un sous-groupe de F. □

Définition. Soit $f : G \to H$ un homomorphisme de groupes. Le *noyau* de f, noté $\mathrm{Ker}(f)$, est $f^{-1}(e_H) = \{x \in G \mid f(x) = e_H\} \subset G$.

Lemme 1.9. *Soit* $f : G \to H$ *un homomorphisme de groupes.*

(1) $\mathrm{Ker}(f)$ *est un sous-groupe de* G*.*

(2) f *est injectif si et seulement si* $\mathrm{Ker}(f) = \{e_G\}$*.*

Démonstration. On a $f(e_G) = e_H$, donc $e_G \in \mathrm{Ker}(f)$. Soient $a_1, a_2 \in \mathrm{Ker}(f)$. Alors

$$f(a_1 * a_2) = f(a_1) * f(a_2) = e_H * e_H = e_H\,,$$

donc $a_1 * a_2 \in \mathrm{Ker}(f)$. Soit $a \in \mathrm{Ker}(f)$. Alors

$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H\,,$$

donc $a^{-1} \in \mathrm{Ker}(f)$. Ceci montre que $\mathrm{Ker}(f)$ est un sous-groupe de G.

Supposons que f est injectif. Comme $f(e_G) = e_H$ on a forcément $e_G \in \mathrm{Ker}(f)$, donc $\{e_G\} \subset \mathrm{Ker}(f)$. Soit $a \in \mathrm{Ker}(f)$. On a $f(a) = e_H = f(e_G)$, donc $a = e_G$ car f est injectif. D'où $\mathrm{Ker}(f) \subset \{e_G\}$. Ceci montre que $\mathrm{Ker}(f) = \{e_G\}$.

Supposons que $\mathrm{Ker}(f) = \{e_G\}$. Soient $a_1, a_2 \in G$ tels que $f(a_1) = f(a_2)$. Alors

$$f(a_1 * a_2^{-1}) = f(a_1) * f(a_2^{-1}) = f(a_1) * f(a_2)^{-1} = e_H\,.$$

D'où $a_1 * a_2^{-1} \in \mathrm{Ker}(f)$, donc $a_1 * a_2^{-1} = e_G$, donc $a_1 = a_2$. Ceci montre que f est injectif. □

Définition. Soient G un groupe et X une partie de G. Le plus petit sous-groupe de G contenant X, noté $\langle X \rangle$, s'appelle le sous-groupe de G *engendré* par X. En d'autre termes, $\langle X \rangle$ est l'intersection de tous les sous-groupes de G contenant X. On dit que G

est *finiment engendré* ou de *type fini* s'il existe $X \subset G$ fini tel que $G = \langle X \rangle$. On dit que G est *monogène* s'il est engendré par un seul élément. On dit que G est *cyclique* s'il est monogène et fini.

Notation. Soient G un groupe et a un élément de G. Pour $n \in \mathbb{N}$ on définit a^n par récurrence sur n en posant $a^0 = e_G$ et , pour $n \geq 1$, $a^n = a * a^{n-1}$. Si $n \in \mathbb{Z}$ et $n < 0$, on pose $a^n = (a^{-n})^{-1}$.

Lemme 1.10. *Soient G un groupe et $a \in G$.*

(1) Soient $n, m \in \mathbb{Z}$. Alors $a^n * a^m = a^{n+m}$.

(2) Le sous-groupe de G engendré par a est $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Démonstration. Soient $n, m \in \mathbb{N}$. On montre par récurrence sur n que $a^n * a^m = a^{n+m}$. Supposons que $n = 0$. Alors $a^n * a^m = e * a^m = a^m = a^{m+0} = a^{n+m}$. Supposons que $a^n * a^m = a^{n+m}$. Alors $a^{n+1} * a^m = a * a^n * a^m = a * a^{n+m} = a^{n+1+m}$.

Soient $n, m \in \mathbb{N}$. Supposons que $m \geq n$. Alors, par ce qui précède, $a^n * a^{-n+m} = a^m$, donc $a^{-n+m} = (a^n)^{-1} * a^m = a^{-n} * a^m$. De même, on a $a^{-n+m} = a^m * a^{-n}$, donc $a^{n-m} = (a^{-n+m})^{-1} = (a^{-n})^{-1} * (a^m)^{-1} = a^n * a^{-m}$. Si $m \leq n$, on démontre de la même façon que $a^{n-m} = a^n * a^{-m}$ et $a^{-n+m} = a^{-n} * a^m$. Finalement, comme $a^{n+m} = a^m * a^n$, on a $a^{-n-m} = (a^{n+m})^{-1} = (a^n)^{-1} * (a^m)^{-1} = a^{-n} * a^{-m}$.

Soit $H = \{a^n \mid n \in \mathbb{Z}\}$. Par ce qui précède, on a un homomorphisme $\varphi_a : \mathbb{Z} \to G$, $n \mapsto a^n$. Il est clair que $H = \mathrm{Im}(\varphi_a)$, donc H est un sous-groupe de G. On a clairement $a \in H$, donc $\langle a \rangle \subset H$. On montre par récurrence sur n que $a^n \in \langle a \rangle$ pour tout $n \in \mathbb{N}$. Supposons que $n = 0$. Alors $a^0 = e \in \langle a \rangle$. Supposons que $a^n \in \langle a \rangle$. Alors $a^{n+1} = a * a^n \in \langle a \rangle$, car on a aussi $a \in \langle a \rangle$. Pour $n \in \mathbb{N}$ on a aussi $a^{-n} = (a^n)^{-1} \in \langle a \rangle$, car $\langle a \rangle$ est un sous-groupe et $a^n \in \langle a \rangle$. Donc $H \subset \langle a \rangle$, donc $H = \langle a \rangle$. □

Remarque. Si G est un groupe abélien, noté additivement, alors pour $a \in G$ le terme "a^n" se note $n\,a$. Donc, pour $n \in \mathbb{N}$, on définit $n\,a$ par récurrence sur n en posant $0\,a = 0$ et $(n+1)\,a = a + n\,a$. Pour $n \leq 0$ on pose $n\,a = -((-n)\,a)$.

Corollaire 1.11. *Soient G un groupe et $a \in G$. Il existe un homomorphisme surjectif $\varphi_a : \mathbb{Z} \to \langle a \rangle$, $n \mapsto a^n$.*

1.2 Groupes abéliens

Définition. Soient G un groupe abélien et H un sous-groupe de G. Soient $a, b \in G$. On dit que *a est congru à b modulo H* si $b - a \in H$. Cette relation se note $a \equiv b \pmod{H}$.

Lemme 1.12. *Soient G un groupe abélien et H un sous-groupe de G.*

(1) La relation "être congru modulo H" est une relation d'équivalence.

(2) *Si* $a \equiv b \pmod{H}$ *et* $c \equiv d \pmod{H}$, *alors* $(a+c) \equiv (b+d) \pmod{H}$, *pour tous* $a, b, c, d \in G$.

Démonstration. Soit $a \in G$. On a $a - a = 0 \in H$, donc $a \equiv a \pmod{H}$. Soient $a, b \in G$ tels que $a \equiv b \pmod{H}$. Alors $b - a \in H$, donc $a - b = -(b-a) \in H$, donc $b \equiv a \pmod{H}$. Soient $a, b, c \in G$ tels que $a \equiv b \pmod{H}$ et $b \equiv c \pmod{H}$. Alors $b - a, c - b \in H$, donc $c - a = (c-b) + (b-a) \in H$, donc $a \equiv c \pmod{H}$. Ceci montre que $\equiv \pmod{H}$ est une relation d'équivalence.

Soient $a, b, c, d \in G$ tels que $a \equiv b \pmod{H}$ et $c \equiv d \pmod{H}$. On a $b - a, c - d \in H$, donc $(b+d) - (a+c) = (b-a) + (d-c) \in H$, donc $(a+c) \equiv (b+d) \pmod{H}$. □

Définition. Soient G un groupe abélien et H un sous-groupe de G. L'ensemble des classes d'équivalence de $\equiv \pmod{H}$ s'appelle le *quotient de* G *par* H et se note G/H. Si $a \in G$, on note $[a]$ ou $[a]_H$ la classe d'équivalence de a. Grâce au lemme 1.12 on a une opération $(G/H) \times (G/H) \to (G/H)$, $(\alpha, \beta) \mapsto \alpha + \beta$ définie comme suit. Soient $\alpha, \beta \in G/H$. On choisit $a, b \in G$ tels que $\alpha = [a]$ et $\beta = [b]$ et on pose $\alpha + \beta = [a+b]$. Par le lemme 1.12 (2) cette définition ne dépend pas du choix de a et b.

Proposition 1.13. *Soient* G *un groupe abélien et* H *un sous-groupe de* G. *Alors* $(G/H, +)$ *est un groupe abélien.*

Démonstration. Soient $\alpha, \beta, \gamma \in G/H$. On choisit $a, b, c \in G$ tels que $\alpha = [a]$, $\beta = [b]$ et $\gamma = [c]$. Alors

$$\begin{aligned}(\alpha+\beta)+\gamma = ([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] \\ = [a]+[b+c] = [a]+([b]+[c]) = \alpha+(\beta+\gamma)\,.\end{aligned}$$

Soient $\alpha, \beta \in G/H$. On choisit $a, b \in G$ tels que $\alpha = [a]$ et $\beta = [b]$. Alors

$$\alpha + \beta = [a] + [b] = [a+b] = [b+a] = [b] + [a] = \beta + \alpha\,.$$

On pose $0_{G/H} = [0_G]$. Soit $\alpha \in G/H$. On choisit $a \in G$ tel que $\alpha = [a]$. Alors

$$\alpha + 0_{G/H} = [a] + [0_G] = [a + 0_G] = [a] = \alpha\,.$$

Soit $\alpha \in G/H$. On choisit $a \in G$ tel que $\alpha = [a]$ et on pose $-\alpha = [-a]$. Alors

$$\alpha + (-\alpha) = [a] + [-a] = [a-a] = [0_G] = 0_{G/H}\,.$$

□

Proposition 1.14. *Soit* $m \in \mathbb{N}$, $m \geq 2$. *Alors* $\mathbb{Z}/m\mathbb{Z}$ *est un groupe cyclique de cardinal* m. *Plus précisément,* $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots, [m-1]\}$.

Démonstration. Montrons d'abord que $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$. Soit $\alpha \in \mathbb{Z}/m\mathbb{Z}$. Soit $a \in \mathbb{Z}$ tel que $\alpha = [a]$. Soit $a = qm + r$ la division de a par m. On a $a - r = qm \in m\mathbb{Z}$, donc $a \equiv r \pmod{m}$, donc $[a] = [r] \in \{[0], [1], \ldots, [m-1]\}$.

Maintenant on montre que les éléments de $\{[0], [1], \ldots, [m-1]\}$ sont deux à deux distincts. Soient $a, b \in \{0, 1, \ldots, m-1\}$. On peut sans perte de généralité supposer que $b \geq a$. Si $[a] = [b]$, alors $a \equiv b \pmod{m}$, donc $b - a \in m\mathbb{Z}$, c'est-à-dire m divise $b - a$. Or on a $0 \leq b - a \leq m - 1$ et le seul élément de $\{0, 1, \ldots, m-1\}$ divisible par m est 0, donc $b - a = 0$, c'est-à-dire $a = b$.

Il est évident que l'on a $n\,[a] = [n\,a]$ pour tout $n, a \in \mathbb{Z}$, donc $\mathbb{Z}/m\mathbb{Z} = \langle [1] \rangle$. □

Lemme 1.15. *Soient G un groupe abélien et H un sous-groupe de G. Alors l'application $\pi : G \to (G/H)$, $a \mapsto [a]$, est un homomorphisme surjectif dont le noyau est H.*

Démonstration. Ce lemme est assez évident. Soient $a, b \in G$. Alors

$$\pi(a) + \pi(b) = [a] + [b] = [a + b] = \pi(a + b)\,.$$

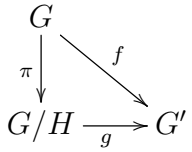
L'homomorphisme π est surjectif par définition. Finalement,

$$a \in \mathrm{Ker}(\pi) \;\Leftrightarrow\; \pi(a) = [a] = [0] \;\Leftrightarrow\; a = a - 0 \in H\,.$$

□

Définition. L'homomorphisme $\pi : G \to G/H$ du lemme 1.15 s'appelle la *projection canonique* de G sur G/H.

Proposition 1.16. *Soient $f : G \to G'$ un homomorphisme de groupes abéliens et H un sous-groupe de G tel que $H \subset \mathrm{Ker}(f)$. Alors il existe un unique homomorphisme $g : G/H \to G'$ qui fait commuter le diagramme suivant, où $\pi : G \to G/H$ est la projection canonique de G sur G/H.*



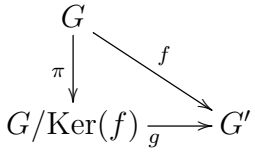
Démonstration. Soit $\alpha \in G/H$. On choisit $a \in G$ tel que $\alpha = [a]$ et on pose $g(\alpha) = f(a)$. Montrons que la définition de $g(\alpha)$ ne dépend pas du choix de a. Soit $a' \in G$ tel que $\alpha = [a'] = [a]$. On a $a \equiv a' \pmod{H}$, donc $a' - a \in H$, donc $a' - a \in \mathrm{Ker}(f)$, donc $f(a') - f(a) = f(a' - a) = 0$, donc $f(a') = f(a)$.

Montrons que g est un homomorphisme. Soient $\alpha, \beta \in G/H$. Soient $a, b \in G$ tels que $\alpha = [a]$ et $\beta = [b]$. Alors

$$g(\alpha) + g(\beta) = f(a) + f(b) = f(a + b) = g([a + b]) = g(\alpha + \beta)\,.$$

Pour $a \in G$ on a $(g \circ \pi)(a) = g(\pi(a)) = g([a]) = f(a)$, donc $g \circ \pi = f$. Soit $g' : G/H \to G'$ un (autre) homomorphisme tel que $g' \circ \pi = f$. On a $g \circ \pi = g' \circ \pi$ et π est surjectif, donc $g = g'$. □

Proposition 1.17. *Soient $f : G \to G'$ un homomorphisme surjectif de groupes abéliens. Alors il existe un isomorphisme $g : G/\mathrm{Ker}(f) \to G'$ qui fait commuter le diagramme suivant.*



Démonstration. On sait par la proposition 1.16 qu'il existe un homomorphisme $g : G/\mathrm{Ker}(f) \to G'$ tel que $g \circ \pi = f$. Comme f est surjectif, g doit forcément être surjectif. Reste à montrer que g est injectif. Soit $\alpha \in \mathrm{Ker}(g)$. Soit $a \in G$ tel que $\alpha = [a]$. On a $f(a) = g([a]) = g(\alpha)$, donc $a \in \mathrm{Ker}(f)$, donc $\alpha = [a] = 0$. Ceci montre que $\mathrm{Ker}(g) = \{0\}$ donc que g est injectif. □

Proposition 1.18. *Soit G un groupe abélien. Les deux conditions suivantes sont équivalentes.*

(i) G est engendré par n éléments.

(ii) Il existe un homomorphisme surjectif de $\mathbb{Z}^n$ sur G.

Démonstration. Supposons que G est engendré par n éléments $x_1, \ldots, x_n$. Soit $\varphi : \mathbb{Z}^n \to G$ l'application définie par

$$\varphi(\lambda_1, \ldots, \lambda_n) = \lambda_1 x_1 + \cdots + \lambda_n x_n \,.$$

Pour $(\lambda_1, \ldots, \lambda_n), (\mu_1, \ldots \mu_n) \in \mathbb{Z}^n$ on a

$$\begin{gathered}\varphi(\lambda_1, \ldots, \lambda_n) + \varphi(\mu_1, \ldots, \mu_n) = (\lambda_1 x_1 + \cdots + \lambda_n x_n) + (\mu_1 x_1 + \cdots + \mu_n x_n) = \\ (\lambda_1 + \mu_1)x_1 + \cdots + (\lambda_n + \mu_n)x_n = \varphi(\lambda_1 + \mu_1, \ldots \lambda_n + \mu_n) = \\ \varphi((\lambda_1, \ldots, \lambda_n) + (\mu_1, \ldots, \mu_n)) \,,\end{gathered}$$

donc φ est un homomorphisme de groupes. On a $x_1, \ldots, x_n \in \mathrm{Im}(\varphi)$, donc $\mathrm{Im}(\varphi) = G$, donc φ est surjectif.

Supposons qu'il existe un homomorphisme surjectif $\varphi : \mathbb{Z}^n \to G$. Posons $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (avec le 1 à la i-ème place) et $x_i = \varphi(e_i)$, pour tout $i \in \{1, \ldots, n\}$. On note H le sous-groupe de G engendré par $x_1, \ldots, x_n$. Comme $x_i \in H$, on a $\lambda_i x_i = \lambda_i \varphi(e_i) = \varphi(\lambda_i e_i) \in H$ pour tout $\lambda_i \in \mathbb{Z}$. Il s'en suit que, pour tout $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$, on a

$$\varphi(\lambda_1, \ldots, \lambda_n) = \varphi(\lambda_1 e_1 + \cdots + \lambda_n e_n) = \varphi(\lambda_1 e_1) + \cdots + \varphi(\lambda_n e_n) \in H \,,$$

donc $G = \mathrm{Im}(\varphi) \subset H$, donc $G = H$. Ceci montre que $x_1, \ldots, x_n$ engendrent G. □

Corollaire 1.19. *Soit G un groupe abélien engendré par n éléments. Alors il existe un sous-groupe H de $\mathbb{Z}^n$ tel que $G \simeq \mathbb{Z}^n/H$.*

Démonstration. Par la proposition 1.18 on a un homomorphisme surjectif $f : \mathbb{Z}^n \to G$. Posons $H = \mathrm{Ker}(f)$. Alors, par la proposition 1.17, $G \simeq \mathbb{Z}^n/H$. □

Définition. Soient G un groupe (non nécessairement abélien) et $x \in G$. On appelle *l'ordre* de x le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$ s'il existe. On dit que x est *d'ordre infini* sinon.

Exemple. Dans $\mathbb{Z}/m\mathbb{Z}$, $[1]$ est d'ordre m. Dans $\mathbb{Z}$, 1 est d'ordre infini.

Lemme 1.20. *Soient G un groupe et x un élément de G d'ordre n. Soit $k \in \mathbb{Z}$ tel que $x^k = e$. Alors n divise k.*

Démonstration. Soit $k = q\,n + r$ la division de k par n. Alors $x^r = x^{k-q\,n} = x^k\,(x^n)^q = e\,e^q = e$. Comme $0 \leq r < n$, la minimalité de n implique que $r = 0$, donc $k = qn$ est un multiple de n. □

Définition. Le cardinal d'un groupe fini G s'appelle aussi *l'ordre* de G.

Proposition 1.21. *Soit G un groupe monogène. Si G est infini, alors G est isomorphe à $\mathbb{Z}$. Si G est fini d'ordre n, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Soit G un groupe monogène. Soit $a \in G$ tel que $G = \langle a \rangle$. Par le lemme 1.10 tout élément de G est de la forme a^n avec $n \in \mathbb{Z}$. Comme $a^n * a^m = a^{n+m} = a^m * a^n$, il s'en suit que G est abélien. Par le corollaire 1.11 on a un homomorphisme surjectif $\varphi : \mathbb{Z} \to G$, $n \mapsto a^n$. Par la proposition 1.3 soit $\mathrm{Ker}(\varphi) = \{0\}$, soit il existe $n \in \mathbb{N}^*$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$. Si $\mathrm{Ker}(\varphi) = \{0\}$, alors $\varphi : \mathbb{Z} \to G$ est un isomorphisme. Supposons que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$. alors, par la proposition 1.17, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Comme $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n, G est obligatoirement d'ordre n dans ce cas. □

Proposition 1.22. *Soient $n \in \mathbb{N}^*$ et $[a] \in \mathbb{Z}/n\mathbb{Z}$. Alors l'ordre de $[a]$ est $\frac{n}{\mathrm{pgcd}(a,n)}$.*

Démonstration. Posons $d = \mathrm{pgcd}(a, n)$, $a = d\,a_1$ et $n = d\,n_1$. On veut montrer que $[a]$ est d'ordre n_1. D'abord, $n_1\,[a] = [n_1\,d\,a_1] = a_1\,[n] = a_1\,[0] = 0$. Soit $k \in \mathbb{Z}$ tel que $k\,[a] = 0$. On a $k[a] = [ka] = 0$, donc $n = n_1 d$ divise $ka = ka_1 d$, donc n_1 divise ka_1. Comme n_1 et a_1 sont premiers entre eux, il s'en suit que n_1 divise k. Donc, n_1 est le plus petit entier ≥ 1 vérifiant $n_1\,[a] = 0$. □

Définition. Soit G un groupe. Un élément $a \in G$ est dit de *torsion* s'il est d'ordre fini. Un *groupe de torsion* est un groupe dont tous les éléments sont d'ordre fini. On dit qu'un groupe G est *sans torsion* si le seul élément de G d'ordre fini est e.

Lemme 1.23. *Soient $n, m \in \mathbb{N}$. Si $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^m$, alors $n = m$.*

Démonstration. Soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$ un isomorphisme. Pour $i \in \{1, \dots, n\}$ on pose $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ et $u_i = \varphi(e_i)$. Soit $\phi : \mathbb{Q}^n \to \mathbb{Q}^m$ l'application linéaire qui envoie e_i sur u_i pour tout $i \in \{1, \dots, n\}$. Remarquer que φ est la restriction de ϕ à $\mathbb{Z}^n$. Soit $v \in \mathrm{Ker}(\phi)$. On écrit $v = \lambda_1 e_1 + \cdots + \lambda_n e_n$ avec $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$. Soit $\mu \in \mathbb{Z}^*$ tel que $\mu\lambda_i \in \mathbb{Z}$ pour tout $i \in \{1, \dots, n\}$. On a $\mu v \in \mathbb{Z}^n \cap \mathrm{Ker}(\phi) = \ker(\varphi) = \{0\}$, donc $\mu v = 0$, donc $v = 0$. Ceci montre que ϕ est injective, donc $\dim(\mathbb{Q}^n) = n \leq \dim(\mathbb{Q}^m) = m$. De même on a $m \leq n$, donc $n = m$. □

Lemme 1.24. *Soient $n \in \mathbb{N}$ et G un sous-groupe de $\mathbb{Z}^n$. Alors il existe $r \in \mathbb{N}$ tel que $r \leq n$ et $G \simeq \mathbb{Z}^r$. Cet r est unique (par le lemme 1.23).*

Démonstration. On raisonne par récurrence sur n. Supposons que $n = 1$. On sait par la proposition 1.3 que $G = \{0\}$ ou $G = m\mathbb{Z}$ avec $m \in \mathbb{N}^*$. Dans le second cas on a évidement $G \simeq \mathbb{Z}$.

On suppose que $n \geq 2$ plus l'hypothèse de récurrence. Soit $\pi : \mathbb{Z}^n \to \mathbb{Z}$ l'homomorphisme défini par

$$\pi(x_1, \dots, x_{n-1}, x_n) = x_n \,.$$

Remarquer que $\mathrm{Ker}(\pi) \simeq \mathbb{Z}^{n-1}$. Si $G \subset \mathrm{Ker}(\pi)$ alors, par hypothèse de récurrence, il existe $r \leq n-1$ tel que $G \simeq \mathbb{Z}^r$. On peut dont supposer que $G \not\subset \mathrm{Ker}(\pi)$. L'ensemble $\pi(G)$ est un sous-groupe de $\mathbb{Z}$ non trivial, donc il existe $m \in \mathbb{N}^*$ tel que $\pi(G) = m\mathbb{Z}$. Posons $G' = G \cap \mathrm{Ker}(\pi)$. Par hypothèse de récurrence il existe $r \leq n-1$ tel que $G' \simeq \mathbb{Z}^r$. On choisit $a \in G$ tel que $\pi(a) = m$ et on se fixe un isomorphisme $\varphi' : \mathbb{Z}^r \to G'$. On définit $\varphi : \mathbb{Z}^{r+1} = \mathbb{Z}^r \times \mathbb{Z} \to G$ par

$$\varphi(u, x) = \varphi'(u) + xa \,.$$

On va montrer que φ est un isomorphisme.

On montre facilement que φ est un homomorphisme de groupes. Soit $(u, x) \in \mathrm{Ker}(\varphi)$. On a

$$0 = \pi(\varphi(u, x)) = \pi(\varphi'(u)) + x\pi(a) = xm$$

donc $x = 0$ et $u \in \mathrm{Ker}(\varphi')$. Comme φ' est injectif, on a alors $u = 0$. Ceci montre que $\mathrm{Ker}(\varphi) = \{(0, 0)\}$, donc φ est injectif. Soit $y \in G$. On a $\pi(y) \in \pi(G) = m\mathbb{Z}$, donc il existe $x \in \mathbb{Z}$ tel que $\pi(y) = xm$. Posons $y' = y - xa$. Alors $\pi(y') = \pi(y) - x\pi(a) = xm - xm = 0$, donc $y' \in \mathrm{Ker}(\pi) \cap G = G'$. Soit $u \in \mathbb{Z}^r$ tel que $y' = \varphi'(u)$. Alors $y = y' + xa = \varphi'(u) + xa = \varphi(u, a)$. Ceci montre que φ est surjectif. □

Théorème 1.25. *Soit G un groupe abélien sans torsion de type fini. Il existe $n \in \mathbb{N}$ tel que G est isomorphe à $\mathbb{Z}^n$. Cet n est unique (par le lemme 1.23).*

Démonstration. On dit qu'une partie finie $\{x_1, \dots, x_n\}$ de L est *libre* si

$$\forall \lambda_1, \dots, \lambda_n \in \mathbb{Z},\ (\lambda_1 x_1 + \cdots + \lambda_n x_n = 0) \Rightarrow (\lambda_1 = \cdots = \lambda_n = 0).$$

L'assertion suivante est assez évidente.

Assertion 1. Si $\{x_1, \dots, x_n\}$ est une famille libre finie de G, alors $\langle x_1, \dots, x_n \rangle \simeq \mathbb{Z}^n$.

Par hypothèse, G est de type fini, donc on peut choisir m éléments $y_1, \dots, y_m \in G$, m fini, tels que G soit engendré par $\{y_1, \dots, y_m\}$.

Assertion 2. Si $\{x_1, \dots, x_n\}$ est une famille finie libre dans G, alors $n \leq m$.

Démonstration de l'assertion 2. Par la proposition 1.18 on a un homomorphisme surjectif $\varphi : \mathbb{Z}^m \to G$, $(\mu_1, \dots, \mu_m) \mapsto \mu_1 y_1 + \cdots + \mu_m y_m$. Pour tout $i \in \{1, \dots, n\}$ on choisit $\hat{x}_i \in \mathbb{Z}^m$ tel que $\varphi(\hat{x}_i) = x_i$ et on note $\hat{H}$ le sous-groupe de $\mathbb{Z}^m$ engendré par $\hat{x}_1, \dots, \hat{x}_n$. Soient $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$. Si $\lambda_1 \hat{x}_1 + \cdots + \lambda_n \hat{x}_n = 0$, alors

$$0 = \varphi(\lambda_1 \hat{x}_1 + \cdots + \lambda_n \hat{x}_n) = \lambda_1 \varphi(\hat{x}_1) + \cdots + \lambda_n \varphi(\hat{x}_n) = \lambda_1 x_1 + \cdots + \lambda_n x_n \,,$$

donc $\lambda_1 = \cdots = \lambda_n = 0$. D'où $\{\hat{x}_1, \dots, \hat{x}_n\}$ est une famille libre, donc $\mathbb{Z}^n \simeq \hat{H} \subset \mathbb{Z}^m$, donc, par le lemme 1.24, $n \leq m$. Ceci finit la démonstration de l'assertion 2.

On choisit une famille libre $\{x_1, \dots, x_n\} \subset G$ avec n maximal et on pose $H = \langle x_1, \dots, x_n \rangle$.

Assertion 3. Il existe $t \in \mathbb{Z}^*$ tel que $t\, y_j \in H$ pour tout $j \in \{1, \dots, m\}$.

Démonstration de l'assertion 3. Soit $j \in \{1, \dots, m\}$. Par la maximalité de n, la famille $\{x_1, \dots, x_n, y_j\}$ n'est pas libre. Il existe donc $\lambda_{1,j}, \dots, \lambda_{n,j}, \mu_j \in \mathbb{Z}$ non tous nuls tels que $\lambda_{1,j} x_1 + \cdots + \lambda_{n,j} x_n + \mu_j y_j = 0$. On a $\mu_j \neq 0$ sinon on aurait $\lambda_{1,j} x_1 + \cdots + \lambda_{n,j} x_n = 0$ et $\lambda_{1,j}, \dots, \lambda_{n,j}$ seraient non tous nuls. On pose $t = \mu_1 \mu_2 \cdots \mu_m$. Alors $t \neq 0$ et $t\, y_j \in H$ pour tout $j \in \{1, \dots, m\}$. Ceci montre l'assertion 3.

Assertion 4. On pose $tG = \{tz \mid z \in G\}$. Alors tG est un sous-groupe de G, inclus dans H et isomorphe à G.

Démonstration de l'assertion 4. On a $0 = t0 \in tG$. Soient $z_1, z_2 \in G$. Alors $tz_1 + tz_2 = t(z_1 + z_2) \in tG$. Soit $z \in G$. Alors $-(tz) = t(-z) \in tG$. Ceci montre que tG est un sous-groupe de G.

Soit $z \in G$. Comme $\{y_1, \dots, y_m\}$ engendre G, il existe $\mu_1, \dots, \mu_m \in \mathbb{Z}$ tel que $z = \mu_1 y_1 + \cdots + \mu_m y_m$ (cela provient de la surjectivité de $\varphi : \mathbb{Z}^m \to G$). Alors $tz = \mu_1(ty_1) + \cdots + \mu_m(ty_m) \in H$ car $ty_1, \dots, ty_m \in H$. Ceci montre que $tG \subset H$.

Soit $\kappa : G \to tG$, $z \mapsto tz$. Il est évident que κ est un homomorphisme et qu'il est surjectif. Si $z \in \mathrm{Ker}(\kappa)$, alors $tz = 0$, donc $z = 0$ car G est sans torsion. Donc $\mathrm{Ker}(\kappa) = \{0\}$ et κ est un isomorphisme. Ceci finit la démonstration de l'assertion 4.

Assertion 5. G est isomorphe à $\mathbb{Z}^n$.

Démonstration de l'assertion 5. Comme tG est un sous-groupe de $H \simeq \mathbb{Z}^n$, par le lemme 1.24 il existe $r \leq n$ tel que $tG \simeq \mathbb{Z}^r$. Comme G est isomorphe à tG, on a aussi $G \simeq \mathbb{Z}^r$. Comme H est un sous-groupe de $G \simeq \mathbb{Z}^r$, par le lemme 1.24 on a $n \leq r$, donc $r = n$. □

Lemme 1.26. *Soit G un groupe abélien. Notons G_T l'ensemble des éléments de G d'ordre fini. Alors G_T est un sous-groupe de G.*

Démonstration. Il est évident que $0 \in G_T$. Soient $a, b \in G_T$. Il existe $n, m \in \mathbb{N}^*$ tels que $na = mb = 0$. Alors $nm(a+b) = m(na) + n(mb) = m\,0 + n\,0 = 0$. Soit $a \in G_T$. Il existe $n \in \mathbb{N}^*$ tel que $na = 0$. Alors $n(-a) = -(na) = -0 = 0$. □

Lemme 1.27. *Soit G un groupe de torsion de type fini. Alors G est fini.*

Démonstration. Soient $y_1, \ldots, y_m \in G$ qui engendrent G. Pour $j \in \{1, \ldots, m\}$ on note n_j l'ordre de y_j. Alors l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z} & \to & G \\ & ([t_1], \ldots, [t_m]) & \mapsto & t_1 y_1 + \cdots + t_m y_m \end{array}$$

est bien définie et est un homomorphisme surjectif. En particulier, G est fini et son cardinal est inférieur ou égal à $n_1\, n_2 \cdots n_m$. □

Théorème 1.28. *Soit G un groupe abélien de type fini. Alors G_T est fini et il existe $n \in \mathbb{N}$ tel que $G \simeq G_T \times \mathbb{Z}^n$ et cet n est unique.*

Démonstration. On pose $H = G/G_T$.

Assertion 1. H est de type fini et sans torsion.

Démonstration de l'assertion 1. On note $\pi : G \to G/G_T = H$ la projection canonique. Si $\{y_1, \ldots, y_m\}$ engendre G, alors $\{\pi(y_1), \ldots, \pi(y_m)\}$ engendre $G/G_T = H$, donc H est de type fini. Soit $\alpha \in H$ un élément de torsion. Il existe $\lambda \in \mathbb{N}^*$ tel que $\lambda\alpha = 0$. Soit $a \in G$ tel que $\alpha = [a]$. Alors $0 = \lambda\,[a] = [\lambda a]$, donc $(\lambda a) \in G_T$, c'est-à-dire λa est un élément de torsion. Il existe $\mu \in \mathbb{N}^*$ tel que $\mu(\lambda a) = (\mu\lambda)a = 0$. Comme $\mu\lambda \neq 0$, on en déduit que a est un élément de torsion, c'est-à-dire $a \in G_T$, donc $\alpha = [a] = 0$. Ceci finit la démonstration de l'assertion 1.

Par le théorème 1.25 il existe $n \in \mathbb{N}$ tel que H est isomorphe à $\mathbb{Z}^n$. En d'autres termes, on peut trouver une famille libre $\{\beta_1, \ldots, \beta_n\}$ dans H qui engendre H. Pour tout $i \in \{1, \ldots, n\}$ on choisit $b_i \in G$ tel que $\pi(b_i) = \beta_i$. On définit $f : G_T \times \mathbb{Z}^n \to G$ par

$$f(a, \lambda_1, \ldots, \lambda_n) = a + \lambda_1 b_1 + \cdots + \lambda_n b_n\,.$$

On vérifie facilement que f est un homomorphisme. Montrons que f est injectif. Soit $(a, \lambda_1, \ldots, \lambda_n) \in \mathrm{Ker}(f)$. On a

$$0 = \pi(0) = \pi(f(a, \lambda_1, \ldots, \lambda_n)) = \pi(a + \lambda_1 b_1 + \cdots + \lambda_n b_n) = \\ \pi(a) + \lambda_1\pi(b_1) + \cdots + \lambda_n\pi(b_n) = \lambda_1\beta_1 + \cdots + \lambda_n\beta_n\,.$$

Cette dernière égalité implique que $\lambda_1 = \cdots = \lambda_n = 0$ car $\{\beta_1, \ldots, \beta_n\}$ est une famille libre. Finalement, on a aussi $a = f(a, 0, \ldots, 0) = 0$. Donc $\mathrm{Ker}(f) = \{(0, 0, \ldots, 0)\}$, donc f est injectif. Montrons que f est surjectif. Soit $c \in G$. Posons $\gamma = \pi(c)$. Il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{Z}$ tels que $\gamma = \lambda_1\beta_1 + \cdots + \lambda_n\beta_n$. Posons $a = c - \lambda_1 b_1 - \cdots - \lambda_n b_n$. On a

$$\pi(a) = \pi(c) - \lambda_1\pi(b_1) - \cdots - \lambda_n\pi(b_n) = \gamma - \lambda_1\beta_1 - \cdots - \lambda_n\beta_n = 0\,,$$

donc $a \in G_T$. D'où $c = a + \lambda_1 b_1 + \cdots + \lambda_n b_n = f(a, \lambda_1, \ldots, \lambda_n)$. Ceci montre que f est surjectif. En conclusion, $G \simeq G_T \times \mathbb{Z}^n$.

Le nombre n est unique car $H \simeq \mathbb{Z}^n$ (voir le lemme 1.23). G est de type fini, donc $G_T \times \mathbb{Z}^n$ est de type fini, donc $G_T \simeq (G_T \times \mathbb{Z}^n)/\mathbb{Z}^n$ est de type fini. On en conclue par le lemme 1.27 que G_T est fini. □

Définition. Soit G un groupe abélien de type fini et soit $n \in \mathbb{N}$ tel que $G \simeq G_T \times \mathbb{Z}^n$. Alors n s'appelle le *rang* de G est se note $n = \mathrm{rg}(G)$.

Il nous reste à comprendre les groupes abéliens finis. La démonstration du lemme suivant est laissée en exercice.

Lemme 1.29. *Soient G un groupe abélien fini et H un sous-groupe de G. Alors $|G| = |H| \times |G/H|$. En particulier $|H|$ divise $|G|$.*

Corollaire 1.30. *Soit G un groupe abélien fini et $a \in G$. Alors l'ordre de a divise $|G|$.*

Démonstration. L'ordre de a coïncide avec le cardinal de $\langle a \rangle$ qui, par le lemme 1.29, divise $|G|$. □

Définition. Soit G un groupe fini et p un nombre premier. Un élément $a \in G$ est un *élément de p-torsion* si son ordre est une puissance de p.

Lemme 1.31. *Soient G un groupe abélien fini et p un nombre premier. Alors l'ensemble G_p des éléments de p-torsion de G est un sous-groupe de G.*

Démonstration. 0 est d'ordre p^0, donc $0 \in G_p$. Soient $a, b \in G_p$. Il existe $n, m \in \mathbb{N}$ tel que $p^n\, a = 0$ et $p^m\, b = 0$. On a $p^{n+m}(a+b) = p^m(p^n\, a) + p^n(p^m\, b) = p^m\, 0 + p^n\, 0 = 0$, donc l'ordre de $a+b$ divise p^{n+m}, donc l'ordre de $a+b$ est une puissance de p, donc $(a+b) \in G_p$. Soit $a \in G_p$. Alors l'ordre de $-a$ est le même que celui de a qui est une puissance de p, donc $-a \in G_p$. □

Lemme 1.32. *Soient G un groupe abélien fini et p un nombre premier. Si $G_p \neq \{0\}$, alors p divise $|G|$ et G contient un élément d'ordre p.*

Démonstration. Supposons que $G_p \neq \{0\}$. Soit $a \in G_p \setminus \{0\}$. Il existe $n \geq 1$ tel que a est d'ordre p^n. Par le corollaire 1.30, p^n divise $|G|$, donc p divise $|G|$. De plus $p^{n-1}\, a$ est d'ordre p. □

Lemme 1.33. *Soient G un groupe abélien fini et p un nombre premier. Si p divise $|G|$, alors G contient un élément d'ordre p (et donc $G_p \neq \{0\}$).*

Démonstration. On raisonne par récurrence sur $|G|$. Supposons que $|G| = p$. Soit $a \in G \setminus \{0\}$. Alors l'ordre de a est non nul et divise p, donc l'ordre de a est p. On suppose que $|G| > p$ plus l'hypothèse de récurrence. Soit $a \in G \setminus \{0\}$ et t l'ordre de a. Si p divise t, alors $\frac{t}{p}\, a$ est d'ordre p. On peut donc supposer que p ne divise pas t. Soit $H = \langle a \rangle$. Par le lemme 1.29 on a $|G| = |H| \times |G/H|$. Le nombre p divise $|G|$ mais ne divise pas $|H| = t$, donc p divise $|G/H|$. Par hypothèse de récurrence, G/H contient un élément β d'ordre p. Soient $b \in G$ tel que $[b] = \beta$ et q l'ordre de b. On a $0 = [q\, b] = q\, [b] = q\, \beta$, donc p divise q et $\frac{q}{p}\, b$ est d'ordre p. □

Corollaire 1.34. *Soient G un groupe abélien fini et p un nombre premier. Alors le cardinal de G_p est une puissance de p.*

Démonstration. Soit q un nombre premier divisant $|G_p|$. Par le lemme 1.33, G_p contient un élément d'ordre q, donc $q = p$. D'où, le seul diviseur premier de $|G_p|$ est p, donc $|G_p|$ est une puissance de p. □

Théorème 1.35. *Soient G un groupe abélien fini et $p_1, \ldots, p_\ell$ les diviseurs premiers de $|G|$. Alors $G \simeq G_{p_1} \times \cdots \times G_{p_\ell}$.*

Démonstration. Soit $\varphi : G_{p_1} \times \cdots \times G_{p_\ell} \to G$ l'application définie par

$$\varphi(a_1, \ldots, a_\ell) = a_1 + \cdots + a_\ell\,.$$

On vérifie facilement que φ est un homomorphisme. Reste à montrer qu'il est injectif et surjectif.

Soit $(a_1, \ldots, a_\ell) \in \mathrm{Ker}(\varphi)$. Pour tout $i \in \{1, \ldots, \ell\}$ on note m_i l'ordre de a_i (qui est une puissance de p_i) et on pose $\hat{m}_i = \prod_{j \neq i} m_j$. Soit $i \in \{1, \ldots, \ell\}$. Remarquer que $\hat{m}_i a_j = 0$ pour tout $j \neq i$ donc

$$\hat{m}_i\, a_i = \hat{m}_i a_1 + \cdots + \hat{m}_i a_\ell = \hat{m}_i(a_1 + \cdots + a_\ell) = \hat{m}_i\, 0 = 0\,.$$

Comme m_i et $\hat{m}_i$ sont premiers entre eux, il existe $x, y \in \mathbb{Z}$ tels que $x m_i + y \hat{m}_i = 1$. Alors

$$a_i = (x m_i + y \hat{m}_i) a_i = x(m_i\, a_i) + y(\hat{m}_i\, a_i) = x\, 0 + y\, 0 = 0\,.$$

Donc $\mathrm{Ker}(\varphi) = \{(0, \ldots, 0)\}$, donc φ est injectif.

Soit $b \in G$. Soit m l'ordre de b. Comme m divise $|G|$, m s'écrit $m = m_1 m_2 \cdots m_\ell$ où m_i est une puissance de p_i pour tout $i \in \{1, \ldots, \ell\}$. Comme avant, on pose $\hat{m}_i = \prod_{j \neq i} m_j$. Les entiers $\hat{m}_1, \ldots, \hat{m}_\ell$ sont premiers entre eux, donc il existe $x_1, \ldots, x_\ell \in \mathbb{Z}$ tels que $x_1 \hat{m}_1 + \cdots + x_\ell \hat{m}_\ell = 1$. Pour $i \in \{1, \ldots, \ell\}$ on pose $b_i = (x_i \hat{m}_i)\, b$. On a $m_i b_i = x_i m_i \hat{m}_i\, b =$

$x_i m\, b = 0$, donc l'ordre de b_i divise m_i (qui est une puissance de p_i), donc l'ordre de b_i est une puissance de p_i, donc $b_i \in G_{p_i}$. De plus,

$$b = (x_1\hat{m}_1 + \cdots + x_\ell\hat{m}_\ell)b = (x_1\hat{m}_1)\, b + \cdots + (x_\ell\hat{m}_\ell)\, b = b_1 + \cdots + b_\ell = \varphi(b_1, \ldots, b_\ell)\,.$$

Ceci montre que φ est surjectif. □

Définition. Soit G un groupe abélien fini. La décomposition $G \simeq G_{p_1} \times \cdots \times G_{p_\ell}$ du théorème 1.35 s'appelle la *décomposition primaire* de G.

Corollaire 1.36. *Soient G un groupe abélien fini et $|G| = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ la décomposition de $|G|$ en facteurs premiers. Alors $|G_{p_i}| = p_i^{\alpha_i}$ pour tout $i \in \{1, \ldots, \ell\}$.*

Démonstration. Par le corollaire 1.34, il existe $\beta_i \in \mathbb{N}$ tel que $|G_{p_i}| = p_i^{\beta_i}$. Par le théorème 1.35 on a $|G| = \prod_{i=1}^{\ell} |G_{p_i}| = \prod_{i=1}^{\ell} p_i^{\beta_i}$. Par l'unicité de la décomposition de $|G|$ en facteurs premiers, on en conclue que $\alpha_i = \beta_i$ pour tout $i \in \{1, \ldots, \ell\}$. □

Le résultat suivant est une sorte de variante du théorème 1.35.

Proposition 1.37 (Lemme chinois). *Soient $u_1, u_2, \ldots, u_\ell$ des entiers positifs deux à deux premiers entre eux. Alors $\mathbb{Z}/(u_1u_2\cdots u_\ell)\mathbb{Z}$ est isomorphe à $\prod_{i=1}^{\ell} \mathbb{Z}/u_i\mathbb{Z}$.*

Démonstration. Posons $m = u_1u_2\cdots u_\ell$. Soit $\pi_i : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/u_i\mathbb{Z}$ l'application définie comme suit. Soit $\alpha \in \mathbb{Z}/m\mathbb{Z}$. Soit $a \in \mathbb{Z}$ tel que $\alpha = [a]_m$. Alors on pose $\pi_i(\alpha) = [a]_{u_i}$. Si $[a']_m = \alpha$, alors m divise $a - a'$, donc u_i divise $a - a'$, donc $[a']_{u_i} = [a]_{u_i}$. Ceci montre que π_i est bien défini, c'est-à-dire que la définition de $\pi_i(\alpha)$ ne dépend pas du choix de a. Il est clair aussi que π_i est un homomorphisme. Soit $\pi : \mathbb{Z}/m\mathbb{Z} \to \prod_{i=1}^{\ell} \mathbb{Z}/u_i\mathbb{Z}$ l'homomorphisme défini par

$$\pi(\alpha) = (\pi_1(\alpha), \pi_2(\alpha), \ldots, \pi_\ell(\alpha))\,.$$

Il est clair que π est un homomorphisme. Soit $\alpha = [a]_m \in \mathrm{Ker}(\pi)$. On a $\pi_i(\alpha) = [a]_{u_i} = 0$, donc u_i divise a pour tout $i \in \{1, \ldots, \ell\}$. Comme $u_1, u_2, \ldots, u_\ell$ sont deux à deux premiers entre eux, il s'en suit que $m = u_1u_2\cdots u_\ell$ divise a, donc $\alpha = [a]_m = 0$. Ceci montre que π est injectif. Comme $|\mathbb{Z}/m\mathbb{Z}| = |\prod_{i=1}^{\ell} \mathbb{Z}/u_i\mathbb{Z}| = m$, on en conclue que π est un isomorphisme. □

Le résultat suivant finit l'analyse (classification) des groupes abéliens de type fini.

Théorème 1.38. *Soient p un nombre premier et G un groupe abélien fini d'ordre une puissance de p. Alors il existe une suite croissante de nombres $1 \leq n_1 \leq n_2 \leq \cdots \leq n_\ell$ tel que G soit isomorphe à*

$$\mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_\ell}\mathbb{Z}\,.$$

La démonstration du théorème 1.38 repose sur les deux lemmes suivants.

Lemme 1.39. *Soient m un entier ≥ 2 et H un sous-groupe de $\mathbb{Z}/m\mathbb{Z}$. Alors H est cyclique engendré par un élément de la forme $[m']$, où m' divise m.*

Démonstration. Soit $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la projection canonique. Soit $\hat{H} = \pi^{-1}(H)$. Alors $\hat{H}$ est un sous-groupe de $\mathbb{Z}$ différent de $\{0\}$ (car $m \in \pi^{-1}(\{0\}) \subset \pi^{-1}(H) = \hat{H}$). Par la proposition 1.3 il existe $m' \in \mathbb{N}^*$ tel que $\hat{H} = m'\mathbb{Z}$. On a $H = \pi(\hat{H}) = \langle [m'] \rangle$, donc il reste juste à démontrer que m' divise m. Mais $m \in \hat{H} = m'\mathbb{Z}$, donc m' divise m. □

Lemme 1.40. *Soient G un groupe abélien fini, H un sous-groupe de G, m un entier positif, et $\varphi : H \to \mathbb{Z}/m\mathbb{Z}$ un homomorphisme. On suppose que l'ordre de tout élément de G divise m. Alors il existe un homomorphisme $\psi : G \to \mathbb{Z}/m\mathbb{Z}$ tel que $\psi|_H = \varphi : H \to \mathbb{Z}/m\mathbb{Z}$.*

Démonstration. On suppose d'abord que G est engendré par H et un élément x. Alors tout élément de G s'écrit sous la forme $b + \lambda x$ avec $b \in H$ et $\lambda \in \mathbb{Z}$ (mais pas de façon unique). Soit k l'ordre de x. Par hypothèse, k divise m. Par ailleurs, par le lemme 1.39, il existe un diviseur k' de k tel que $H \cap \langle x \rangle = \langle k'x \rangle$.

Posons $\beta = \varphi(k'x)$. Rappelons que k divise m et k' divise k. Soient $m_1, k_1 \in \mathbb{Z}$ tels que $m = k\, m_1$ et $k = k'\, k_1$, et soit $t \in \mathbb{Z}$ tel que $[t] = \beta = \varphi(k'x)$. On a $k_1(k'x) = kx = 0$, donc $[k_1 t] = k_1\, \beta = k_1 \varphi(k'x) = \varphi(kx) = \varphi(0) = 0$, donc $m = k_1 k' m_1$ divise $k_1 t$, donc $k' m_1$ divise t, donc k' divise t. On pose $t_1 = t/k'$ et $\beta_1 = [t_1]$. Remarquer que $k'\beta_1 = \beta = \varphi(k'x)$.

On définit une application $\psi : G \to \mathbb{Z}/m\mathbb{Z}$ comme suit. Soit $a \in G$. On choisit $b \in H$ et $\lambda \in \mathbb{Z}$ tels que $a = b + \lambda x$ et on pose $\psi(a) = \varphi(b) + \lambda\beta_1$. Montrons que ψ est bien définie, c'est-à-dire que la définition de $\psi(a)$ ne dépend pas du choix de b et λ. Soient $b' \in H$ et $\lambda' \in \mathbb{Z}$ tels que $a = b' + \lambda' x = b + \lambda x$. On a $b - b' = (\lambda' - \lambda)x \in H \cap \langle x \rangle$, donc k' divise $\lambda' - \lambda$. Soit $\mu \in \mathbb{Z}$ tel que $\lambda' - \lambda = \mu\, k'$. Alors

$$\varphi(b) + \lambda\beta_1 - \varphi(b') - \lambda'\beta_1 = \varphi(b - b') - (\lambda' - \lambda)\beta_1 = \varphi(\mu\, k'x) - (\lambda' - \lambda)\beta_1 = \\ \mu\varphi(k'x) - (\lambda' - \lambda)\beta_1 = \mu\beta - (\lambda' - \lambda)\beta_1 = \mu k'\beta_1 - (\lambda' - \lambda)\beta_1 = 0\,.$$

On montre facilement que ψ est un homomorphisme et on a $\psi|_H = \varphi$ par définition.

On suppose maintenant que G est engendré par H et un nombre fini d'éléments, $x_1, \ldots, x_\ell$. Notons H_i le sous-groupe de G engendré par H et $x_1, \ldots, x_i$. Ce qui précède montre par récurrence sur i qu'il existe un homomorphisme $\psi_i : H_i \to \mathbb{Z}/m\mathbb{Z}$ tel que $\psi_i|_H = \varphi : H \to \mathbb{Z}/m\mathbb{Z}$. On obtient alors le lemme avec $i = \ell$. □

Démonstration du théorème 1.38. On raisonne par récurrence sur $|G|$. Le cas $|G| = 1$ étant trivial, on peut supposer que $|G| \geq 2$ plus l'hypothèse de récurrence. L'ordre de G étant une puissance de p, on a forcément $G = G_p$, donc tout élément de G est d'ordre une puissance de p. Soit u le plus grand entier tel qu'il existe un élément de G d'ordre

p^u et soit $x \in G$ un élément d'ordre p^u. On pose $H = \langle x \rangle$ et on note $\varphi : H \to \mathbb{Z}/p^u\mathbb{Z}$ l'homomorphisme défini par $\varphi(\lambda x) = [\lambda]$. Soit $y \in G$. L'ordre de y est une puissance de p plus petite ou égale à p^u, donc cet ordre divise p^u. Par le lemme 1.40, on en déduit qu'il existe un homomorphisme $\psi : G \to \mathbb{Z}/p^u\mathbb{Z}$ tel que $\psi|_H = \varphi$.

Posons $G_1 = \mathrm{Ker}(\psi)$. Soit $f : G_1 \times \mathbb{Z}/p^u\mathbb{Z} \to G$ l'application définie par $f(a, [\lambda]) = a + \lambda x$. On vérifie facilement que f est bien définie et qu'elle est un homomorphisme. On va montrer qu'elle est bijective. Soit $(a, [\lambda]) \in \mathrm{Ker}(f)$. On a

$$0 = \psi(0) = \psi(a + \lambda x) = \psi(a) + \varphi(\lambda x) = [\lambda]\,,$$

puis $0 = f(a, 0) = a$, donc $(a, [\lambda]) = (0, 0)$. Ceci montre que f est injective. Soit $b \in G$. Soit $\lambda \in \mathbb{Z}$ tel que $\psi(b) = [\lambda]$. Posons $a = b - \lambda x$. Alors $a \in \mathrm{Ker}(\psi) = G_1$ et $b = a + \lambda x = f(a, [\lambda])$. Ceci montre que f est surjective.

Par hypothèse de récurrence, il existe une suite croissance $n_1 \leq \cdots \leq n_{\ell-1}$ telle que $G_1 \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_{\ell-1}}\mathbb{Z}$. Comme $G \simeq G_1 \times \mathbb{Z}/p^u\mathbb{Z}$, il s'en suit que $G \simeq Z/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_{\ell-1}}\mathbb{Z} \times \mathbb{Z}/p^u\mathbb{Z}$. On a $n_\ell \leq u$ car p^u est l'ordre maximal d'un élément de G. □

En combinant les théorèmes 1.35 et 1.38 et la proposition 1.37 on peut montrer (plus ou moins facilement) le résultat suivant.

Théorème 1.41. *Soit G un groupe abélien fini. Il existe une unique suite d'entiers $m_1, \ldots, m_\ell$ telle que $m_1 \geq 2$, m_i divise m_{i+1} pour tout $i \in \{1, \ldots, \ell-1\}$ et G est isomorphe à $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$.*

Définition. Soit G un groupe abélien fini. La décomposition $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$ du théorème 1.41 s'appelle la *décomposition en facteurs invariants* de G.

1.3 Groupe symétrique

Définition. Soit E un ensemble fini. Une bijection de E dans E s'appelle une *permutation* de E. Le groupe des permutations de E se note $\mathfrak{S}(E)$. Notons $[n]$ l'ensemble $\{1, \ldots, n\}$. Le groupe des permutations de $[n]$ s'appelle le *groupe symétrique* de l'ensemble à n éléments et se note $\mathfrak{S}_n$.

Proposition 1.42. *Soit E un ensemble fini à n éléments. Alors $\mathfrak{S}(E)$ est isomorphe à $\mathfrak{S}_n$.*

Démonstration. Soit $f : E \to [n]$ une bijection. Soit $\varphi : \mathfrak{S}(E) \to \mathfrak{S}_n$ l'application définie par $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. Pour $\sigma_1, \sigma_2 \in \mathfrak{S}(E)$ on a

$$\varphi(\sigma_1) \circ \varphi(\sigma_2) = (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1}) = f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1} = \varphi(\sigma_1 \circ \sigma_2)\,,$$

donc φ est un homomorphisme. Soit $\psi : \mathfrak{S}_n \to \mathfrak{S}(E)$ l'application définie par $\psi(\mu) = f^{-1} \circ \mu \circ f$. On vérifie comme pour φ que ψ est un homomorphisme. On a aussi de façon évidente $\varphi \circ \psi = \mathrm{id}_{\mathfrak{S}_n}$ et $\psi \circ \varphi = \mathrm{id}_{\mathfrak{S}(E)}$. On en conclue que φ est un isomorphisme. □

Définition. Un élément $\sigma \in \mathfrak{S}_n$ sera noté

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Soient $t_1, \ldots, t_\ell$ ℓ éléments deux à deux distincts de $[n]$. Soit $\sigma \in \mathfrak{S}_n$ la permutation définie par

$$\begin{array}{lcll} \sigma(t_i) & = & t_{i+1} & \text{pour } i = 1, \ldots, \ell - 1 \\ \sigma(t_\ell) & = & t_1 & \\ \sigma(t) & = & t & \text{si } t \notin \{t_1, \ldots, t_\ell\} \end{array}$$

Une telle transformation s'appelle un *cycle de longueur* ℓ et se note $\sigma = (t_1, t_2, \ldots, t_\ell)$. Un cycle de longueur 2 s'appelle une *transposition*. Nous utiliserons aussi la notation $\tau_{i,j}$ pour la transposition (i, j).

Exemples.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

est le cycle de longueur 3 (ou 3-cycle) $(1, 3, 5)$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

est la transposition $(2, 4) = \tau_{2,4}$.

Théorème 1.43. *Le groupe symétrique $\mathfrak{S}_n$ a $n!$ éléments.*

Démonstration. On raisonne par récurrence sur n. Supposons que $n = 1$. Alors $\mathfrak{S}_1 = \{\mathrm{id}\}$ et $\mathrm{card}(\mathfrak{S}_1) = 1 = 1!$. Supposons que $n \geq 2$ plus l'hypothèse de récurrence. Posons $H = \{\sigma \in \mathfrak{S}_n \mid \sigma(n) = n\}$. L'ensemble H est un sous-groupe de $\mathfrak{S}_n$ isomorphe à $\mathfrak{S}_{n-1}$, donc, par hypothèse de récurrence, $\mathrm{card}(H) = (n-1)!$. Soit $F : [n] \times H \to \mathfrak{S}_n$ l'application définie par

$$F(k, \mu) = \begin{cases} \tau_{k,n} \circ \mu & \text{si } k \neq n \\ \mu & \text{si } k = n \end{cases}$$

Si $\sigma \in \mathfrak{S}_n$ est tel que $\sigma(n) \neq n$, alors $(\tau_{n,\sigma(n)} \circ \sigma)(n) = n$, donc $\tau_{n,\sigma(n)} \circ \sigma \in H$. Ceci permet de définir l'application $G : \mathfrak{S}_n \to [n] \times H$ par

$$G(\sigma) = \begin{cases} (\sigma(n), \tau_{n,\sigma(n)} \circ \sigma) & \text{si } \sigma(n) \neq n \\ (n, \sigma) & \text{si } \sigma(n) = n \end{cases}$$

On vérifie facilement que $G \circ F = \mathrm{id}_{[n] \times H}$ et $F \circ G = \mathrm{id}_{\mathfrak{S}_n}$, donc F est une bijection, donc $\mathrm{card}(\mathfrak{S}_n) = \mathrm{card}([n] \times H) = n \times (n-1)! = n!$. □

Définition. Le *support* d'une permutation $\sigma \in \mathfrak{S}_n$ et $\mathrm{supp}(\sigma) = \{i \in [n] \mid \sigma(i) \neq i\}$.

Exemple. Le support de
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$$
est $\{1, 3, 4, 6\}$. Le support d'un cycle $(t_1, t_2, \ldots, t_\ell)$ est $\{t_1, t_2, \ldots, t_\ell\}$.

Lemme 1.44. *Soient $\sigma, \tau \in \mathfrak{S}_n$ tels que $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$. Alors $\sigma \circ \tau = \tau \circ \sigma$.*

Démonstration. Si $t \in \mathrm{supp}(\sigma)$, alors $\sigma(t) \in \mathrm{supp}(\sigma)$. Sinon, on aurait $\sigma(\sigma(t)) = \sigma^2(t) = \sigma(t)$, donc $\sigma(t) = t$, ce qui contredirait le fait que $t \in \mathrm{supp}(\sigma)$. Soit $t \in [n]$. Si $t \in \mathrm{supp}(\sigma)$, alors $t, \sigma(t) \notin \mathrm{supp}(\tau)$, donc $(\sigma \circ \tau)(t) = \sigma(t) = (\tau \circ \sigma)(t)$. De même, si $t \in \mathrm{supp}(\tau)$, alors $(\sigma \circ \tau)(t) = (\tau \circ \sigma)(t)$. Si $t \notin \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$, alors $(\sigma \circ \tau)(t) = \sigma(t) = t = \tau(t) = (\tau \circ \sigma)(t)$. D'où $\sigma \circ \tau = \tau \circ \sigma$. □

Théorème 1.45. *Soit $\sigma \in \mathfrak{S}_n$. Il existe une famille, unique à l'ordre près, de cycles c_i, $i = 1, \ldots, \ell$, telle que $\sigma = c_1 \circ c_2 \circ \cdots \circ c_\ell$ et $\mathrm{supp}(c_i) \cap \mathrm{supp}(c_j) = \emptyset$ pour tous $i, j \in \{1, \ldots, \ell\}$, $i \neq j$.*

Définition. Soit $\sigma \in \mathfrak{S}_n$. La décomposition de σ comme produit de cycles du théorème 1.45 s'appelle la *décomposition canonique en cycles* de σ.

Démonstration. *L'orbite* d'un élément $t \in [n]$ est l'ensemble $\mathcal{O}[t] = \{\sigma^k(t) \mid k \in \mathbb{Z}\}$.

Assertion 1. Soient $t, t' \in [n]$. Si $t' \in \mathcal{O}[t]$, alors $\mathcal{O}[t] = \mathcal{O}[t']$.

Démonstration de l'assertion 1. On suppose que $t' \in \mathcal{O}[t]$. Soit $k_0 \in \mathbb{Z}$ tel que $t' = \sigma^{k_0}(t)$. Soit $s \in \mathcal{O}[t]$. Il existe $k \in \mathbb{Z}$ tel que $s = \sigma^k(t)$. Alors $s = \sigma^{k-k_0}(\sigma^{k_0}(t)) = \sigma^{k-k_0}(t') \in \mathcal{O}[t']$. Ceci montre que $\mathcal{O}[t] \subset \mathcal{O}[t']$. Soit $s \in \mathcal{O}[t']$. Il existe $k \in \mathbb{Z}$ tel que $s = \sigma^k(t')$. Alors $s = \sigma^k(\sigma^{k_0}(t)) = \sigma^{k+k_0}(t) \in \mathcal{O}[t]$. Ceci montre que $\mathcal{O}[t'] \subset \mathcal{O}[t]$, donc $\mathcal{O}[t'] = \mathcal{O}[t]$.

Assertion 2. Soient $t \in [n]$ et $\ell = \mathrm{card}(\mathcal{O}[t])$. Alors $\sigma^\ell(t) = t$ et $\mathcal{O}[t] = \{t, \sigma(t), \ldots, \sigma^{\ell-1}(t)\}$.

Démonstration de l'assertion 2. Comme $\mathcal{O}[t]$ est fini, il existe $\ell > 0$ tel que $\sigma^\ell(t) \in \{t, \sigma(t), \ldots, \sigma^{\ell-1}(t)\}$. On prend le plus petit ℓ vérifiant cette propriété. Soit $k \in \{0, 1, \ldots, \ell - 1\}$ tel que $\sigma^\ell(t) = \sigma^k(t)$. On a $\sigma^{\ell-k}(t) = t \in \{t, \sigma(t), \ldots, \sigma^{\ell-k-1}(t)\}$, donc, par la minimalité de ℓ, $k = 0$, c'est-à-dire $\sigma^\ell(t) = t$. Soit $k \in \mathbb{Z}$. Soit $k = q\ell + r$ la division de k par ℓ. Alors
$$\sigma^k(t) = \big(\sigma^r \circ (\sigma^\ell)^q\big)(t) = \sigma^r(t) \in \{t, \sigma(t), \ldots, \sigma^{\ell-1}(t)\}\,.$$
Ceci montre que $\mathcal{O}[t] = \{t, \sigma(t), \ldots, \sigma^{\ell-1}(t)\}$. Reste à montrer que $\mathrm{card}(\mathcal{O}[t]) = \ell$. Supposons qu'il existe $a, b \in \{0, 1, \ldots, \ell - 1\}$ tels que $a < b$ et $\sigma^a(t) = \sigma^b(t)$. Alors $\sigma^b(t) \in \{t, \sigma(t), \ldots, \sigma^{b-1}(t)\}$. Ceci contredit la minimalité de ℓ, donc $t, \sigma(t), \ldots, \sigma^{\ell-1}(t)$ sont deux à deux distincts, donc $\mathrm{card}(\mathcal{O}[t]) = \ell$.

Notons $\mathcal{O}_1, \ldots, \mathcal{O}_\ell$ les orbites de σ de cardinal ≥ 2. Par l'assertion 1 on a $\mathrm{supp}(\sigma) = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_\ell$. Pour tout $i \in \{1, \ldots, \ell\}$ on choisit $t_i \in \mathcal{O}_i$ et on pose $c_i = (t, \sigma(t), \ldots, \sigma^{m_i-1}(t))$, où $m_i = \mathrm{card}(\mathcal{O}_i)$. Les assertions 1 et 2 impliquent que $\sigma = c_1 \circ c_2 \circ \cdots \circ c_\ell$. De plus, pour $i, j \in \{1, \ldots, \ell\}$, $i \neq j$, on a $\mathrm{supp}(c_i) \cap \mathrm{supp}(c_j) = \mathcal{O}_i \cap \mathcal{O}_j = \emptyset$. Ceci démontre l'existence de la décomposition.

Supposons que $\sigma = d_1 \circ d_2 \circ \cdots \circ d_{\ell'}$, où chaque d_i est un cycle et $\mathrm{supp}(d_i) \cap \mathrm{supp}(d_j) = \emptyset$ pour tous $i, j \in \{1, \ldots, \ell'\}$, $i \neq j$. Soit $i \in \{1, \ldots, \ell'\}$. Soit $t_i \in \mathrm{supp}(d_i)$. Alors $d_i = (t_i, \sigma(t_i), \cdots, \sigma^{m_i-1}(t_i))$, où m_i est la longueur du cycle d_i, et $\sigma^{m_i}(t_i) = t_i$. Comme les supports des d_i sont deux à deux disjoints, $\mathcal{O}_i = \{t_i, \sigma(t_i), \ldots, \sigma^{m_i-1}(t_i)\}$ est une orbite de σ. Il est clair que toutes les orbites de cardinal ≥ 2 sont de cette forme. On en conclue que $\ell' = \ell$ et, à permutation près, $c_i = d_i$ pour tout $i \in \{1, \ldots, \ell\}$. □