LES GROUPES

1. Rappels

Ce paragraphe contient des rappels sur les groupes et leurs morphismes.

Définition. Un *groupe* est un ensemble G muni d'une opération binaire (ou *loi*) $G \times G \to G$ avec trois propriétés :
(i) Associativité : on a $(xy)z = x(yz)$ pour tout $x, y, z \in G$.
(ii) Neutre : il existe un $e \in G$ avec $xe = x$ et $ex = x$ pour tout $x \in G$.
(iii) Inverses : pour tout $x \in G$ il existe un $y \in G$ avec $xy = e$ et $yx = e$.
Un groupe est *abélien* s'il vérifie en plus
(iv) Commutativité : on a $xy = yx$ pour tout $x, y \in G$.

L'élément neutre $e \in G$ est unique. Le y de la condition (iii) dépend uniquement de x aussi, et on l'écrit $y = x^{-1}$. C'est l'inverse de x. On a

$$(xy)^{-1} = y^{-1}x^{-1}, \qquad (x^{-1})^{-1} = x.$$

Notations. La notation $(G, \cdot, e)$ signifie "le groupe G avec loi notée $\cdot$ et le neutre noté e."

Un *groupe multiplicatif* est un groupe avec loi appelée la multiplication et neutre noté 1. Comme $(\mathbb{R}^\times, \cdot, 1)$.

Un *groupe additif* est un groupe avec loi notée $+$ et neutre noté 0. Les groupes additifs sont toujours abéliens. Comme $(\mathbb{Z}, +, 0)$.

Pour X un ensemble $(\mathrm{Bij}(X), \circ, \mathrm{Id}_X)$ est un groupe. Pour $X = \{1, 2, 3, \ldots, n\}$, on la note S_n (ou $\mathfrak{S}_n$). C'est le *groupe symétrique* sur n chiffres. [1]

On parlera assez souvent du groupe $\{1, -1\}$. Sa loi est la multiplication.

Simplification. Dans un groupe on a $xa = xb$ ssi on a $a = b$ car on peut multiplier les deux membres à gauche par x^{-1}. Similairement on a $ax = bx$ ssi on a $a = b$. Mais $ax = xb$ est différent de $a = b$ si le groupe n'est pas abélien.

Sous-groupes. Un sous-ensemble H d'un groupe $(G, \cdot, e)$ est un *sous-groupe* si $(H, \cdot, e)$ est un groupe.

Théorème 1.1. *Un sous-ensemble H d'un groupe $(G, \cdot, e)$ est un sous-groupe si et seulement si il vérifie les trois propriétés suivantes :*
(a) $e \in H$,
(b) Pour tout $x, y \in H$ on a $xy \in H$,
(c) Pour tout $x \in H$ on a $x^{-1} \in H$.

G et $\{e\}$ sont toujours des sous-groupes de G.

Puissances. Pour $n > 0$ on écrit $x^n = xxx \cdots x$ (n fois). On pose $x^0 = e$. Pour $n < 0$, on écrit $x^n = (x^{|n|})^{-1} = (x^{-1})^{|n|}$.

Dans un groupe additif on écrit $-x$ plutôt que x^{-1}, et nx plutôt que x^n.

1. Le groupe symétrique, et la signature et la décomposition en cycles d'une permutation étaient traités dans le cours de l'année précédente.

Morphismes de groupes.

Définition. Une application $\phi\colon G \to H$ entre deux groupes est un *morphisme de groupes* si on a $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ pour tout $g_1, g_2 \in G$. Un *isomorphisme* $\phi\colon G \xrightarrow{\cong} H$ est un morphisme bijectif. Un *automorphisme de* G est un isomorphisme de la forme $\phi\colon G \xrightarrow{\cong} G$.

Il faut faire attention que dans $\phi(g_1g_2)$ le produit g_1g_2 se fait avec la loi de G, mais dans $\phi(g_1)\phi(g_2)$ le produit se fait avec la loi de H. On remplace le produit g_1g_2 par la somme g_1+g_2 ou la composition $g_1 \circ g_2$ si la loi est $+$ ou $\circ$. Par exemple l'application $\exp : \mathbb{R} \to \mathbb{R}^\times$ est un morphisme du groupe additif $\mathbb{R}$ vers le groupe multiplicatif $\mathbb{R}^\times$ car il vérifie

$$\exp(x+y) = \exp(x)\exp(y)$$

pour tout $x, y \in \mathbb{R}$.

Quand on a un morphisme de groupes, on a aussi

$$\phi(e_G) = e_H, \qquad \phi(g^{-1}) = \phi(g)^{-1}.$$

Notons $\mathrm{Aut}(G) = \{\text{automorphismes de } G\}$. Alors $(\mathrm{Aut}(G), \circ, \mathrm{Id}_G)$ est un groupe.

L'*image* $\operatorname{im}\phi = \phi(G)$ d'un morphisme de groupes est un sous-groupe de H.

Le *noyau* $\ker\phi = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G.

Proposition 1.2. *Un morphisme de groupes* $\phi\colon G \to H$ *est injectif si et seulement si* $\ker\phi = \{e_G\}$.

Preuve. Exercice. □

Définition. Un sous-groupe $N \subset G$ est *distingué* ou *normal* si pour tout $g \in G$ et tout $n \in N$ on a $gng^{-1} \in N$.

On appelle gng^{-1} le *conjugué de* n *par* g. Donc un sous-groupe N est distingué s'il est stable sous conjugaison par tout élément g de G.

Tout sous-groupe d'un groupe abélien est distingué.

Les sous-groupes G et $\{e\}$ de G sont distingués.

Proposition 1.3. *Soit* $\phi\colon G \to H$ *un morphisme de groupes. Alors* $\ker\phi$ *est un sous-groupe distingué de* G.

Exemples. $H = \{I, (1\,2)\}$ est un sous-groupe non distingué de S_3 car le conjugué de $(1\,2) \in H$ par $(1\,3) \in S_3$ est

$$(1\,3) \circ (1\,2) \circ (1\,3)^{-1} = (1\,3) \circ (1\,2) \circ (1\,3) = (2\,3)$$

qui n'est pas dans H. La composition est déterminée soit par les calculs

$$1 \xrightarrow{(1\,3)} 3 \xrightarrow{(1\,2)} 3 \xrightarrow{(1\,3)} 1$$

$$2 \xrightarrow{(1\,3)} 2 \xrightarrow{(1\,2)} 1 \xrightarrow{(1\,3)} 3$$

$$3 \xrightarrow{(1\,3)} 1 \xrightarrow{(1\,2)} 2 \xrightarrow{(1\,3)} 2$$

soit par la formule

$$\sigma \circ (a_1\, a_2\, \ldots\, a_k) \circ \sigma^{-1} = (\sigma(a_1)\, \sigma(a_2)\, \ldots\, \sigma(a_k)).$$

La signature $\operatorname{sign}\colon S_n \to \{+1, -1\}$ est un morphisme de groupes (la loi de $\{+1, -1\}$ étant la multiplication). Donc son noyau $A_n = \{\sigma \in S_n \mid \text{la signature de } \sigma \text{ est } +1\}$ est un sous-groupe

distingué de S_n. Ces groupes s'appellent les *groupes alternés*. (Certains écrivent $\mathfrak{A}_n \subset \mathfrak{S}_n$ au lieu de $A_n \subset S_n$.) En particulier

$$A_3 = \{I, (1\,2\,3), (1\,3\,2)\}$$

est un sous-groupe distingué de S_3. [2]

Un fait intéressant mais un peu long à montrer est le suivant :

Théorème 1.4. *Pour $n \neq 4$ les seuls sous-groupes distingués de S_n sont $\{I\}$, A_n et S_n.*

Le groupe S_4 a un quatrième sous-groupe distingué $V = \{I, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

2. Les classes de H dans G

Ce paragraphe introduit les classes à gauche et les classes à droite d'un sous-groupe.

Pour $H \subset G$ un sous-groupe et $x \in G$, écrivons

$$xH = \{xh \mid h \in H\} \subset G, \qquad Hx = \{hx \mid h \in H\} \subset G.$$

Les xH pour les différents H sont les *classes à gauche* de H dans G. La classe à gauche d'un x spécifique est xH.

Les Hx sont les *classes à droite*. [3]

Lemme 2.1. *Soit H un sous-groupe de G, et $x, y \in G$.*

(a) On a des équivalences : $xH = yH \Leftrightarrow y \in xH \Leftrightarrow \exists h \in H$ avec $y = xh \Leftrightarrow x^{-1}y \in H$.

(b) On a soit $xH = yH$ soit $xH \cap yH = \varnothing$.

Donc les classes à gauche de x et y sont soit disjoints soit confondus. Et les membres de la classe xH sont exactement les y avec $xH = yH$, dont x lui-même.

Preuve. (a) (1ère $\Leftarrow$) Supposons qu'on a $y \in xH$. Alors il existe un $k \in H$ tel que $y = xk$. Montrons maintenant les deux inclusions $yH \subset xH$ et $xH \subset yH$.

Tout membre $yh \in yH$ se réécrit $yh = xkh \in xH$ car on a $kh \in H$ vu qu'on a $k, h \in H$ et H est un sous-groupe. Donc $yH \subset xH$.

Similairement tout membre $xh \in xH$ se réécrit $xh = yk^{-1}h \in xH$. Donc $xH \subset yH$. D'où $xH = yH$.

(1ère $\Rightarrow$) Si on a $xH = yH$ alors $y = ye \in yH = xH$.

(2ème et 3ème $\Leftrightarrow$) Evident.

(b) Supposons $xH \cap yH \neq \varnothing$ et montrons $xH = yH$. Mais si $xH \cap yH \neq \varnothing$, alors il existe $z \in xH \cap yH$. Par le (a) on a par conséquent $zH = xH$ et $zH = yH$. Par transitivité on a $xH = yH$. □

Lemme 2.2. *Pour tout x la classe à gauche xH est en bijection avec H sous l'application $H \to xH$ donnée par $h \mapsto xh$.*

Preuve. L'application est surjective par définition de xH, et elle est injective car $xh = xk$ entraîne $h = k$ par simplification. □

Les deux derniers lemmes ont des analogues pour les classes à droite.

---

2. La permutation $(1\,2\,3)$ fait $1 \to 2 \to 3 \to 1$, et $(1\,3)(2\,4)$ fait $1 \to 3 \to 1$ et $2 \to 4 \to 2$. A l'intérieur d'un couple de parenthèses $(\dots)$ chaque chiffre est envoyé sur le chiffre suivant. Le dernier chiffre avant un) est envoyé sur le premier chiffre après le (précédent. Les chiffres qui ne paraissent pas sont fixes.

3. En anglais on dit *left cosets* et *right cosets*.

Lemme 2.3. *Soit H un sous-groupe de G et $x, y \in G$.*
(a) On a des équivalences : $Hx = Hy \Leftrightarrow x \in Hy \Leftrightarrow \exists h \in H$ avec $x = hy \Leftrightarrow xy^{-1} \in H$.
(b) On a soit $Hx = Hy$ soit $Hx \cap Hy = \varnothing$.
(c) L'application $H \to Hx$ envoyant $h \mapsto hx$ est une bijection.

Définition. L'*indice* $[G : H]$ d'un sous-groupe $H \subset G$ est le nombre de classes à gauche distincts de H dans G.

L'*ordre* du groupe G, noté $|G|$, est son cardinal.

Théorème 2.4. *Pour un sous-groupe H dans G on a $|G| = [G : H]|H|$.*

Preuve. Par les lemmes, G est la réunion disjointe de $[G : H]$ sous-ensembles xH tous du même cardinal $|H|$. □

Corollaire 2.5. *Pour un sous-groupe $H \subset G$ d'un groupe fini, $|H|$ divise $|G|$.*

Exemple 2.6. (1) Pour $H = \{I, (1\,2)\} \subset S_3$ on a $[S_3 : H] = |S_3|/|H| = 6/2 = 3$. Les trois classes à gauche sont

$$\begin{aligned} IH = (1\,2)H = H &= \{I, (1\,2)\}, \\ (1\,3)H = (1\,2\,3)H &= \{(1\,3), (1\,2\,3)\}, \\ (2\,3)H = (1\,3\,2)H &= \{(2\,3), (1\,3\,2)\}. \end{aligned}$$

Les classes à droite sont

$$\begin{aligned} HI = H(1\,2) = H &= \{I, (1\,2)\}, \\ H(1\,3) = H(1\,3\,2) &= \{(1\,3), (1\,3\,2)\}, \\ H(2\,3) = H(1\,2\,3) &= \{(2\,3), (1\,2\,3)\}. \end{aligned}$$

Les classes à gauche et à droite ne coïncident pas.

(2) Considérons le sous-groupe $A_n \subset S_n$ de permutations de signature $+1$. Or pour $\sigma, \tau \in A_n$ on a $\sigma^{-1}\tau \in A_n$ ssi σ et τ sont de la même signature. Donc par le lemme 2.1(a) on a $\sigma A_n = \tau A_n$ si et seulement si $\mathrm{sign}(\sigma) = \mathrm{sign}(\tau)$. Pour tout $n \geq 2$ le sous-groupe $A_n \subset S_n$ a deux classes à gauche

$$\begin{array}{rcccl} IA_n & = & A_n & = & \{\text{permutations de signature } +1\}, \\ (1\,2)A_n & = & S_n \smallsetminus A_n & = & \{\text{permutations de signature } -1\}. \end{array}$$

On a $[S_n : A_n] = 2$ et $|A_n| = |S_n|/2 = n!/2$. Comme on a aussi $\sigma\tau^{-1} \in A_n$ ssi $\mathrm{sign}(\sigma) = \mathrm{sign}(\tau)$, ces deux classes à gauche sont aussi des classes à droite.

A noter : parmi les deux classes seulement A_n est un sous-groupe. L'autre classe $S_n \smallsetminus A_n$ est une classe à gauche (et à droite) du sous-groupe A_n.

(3) Le groupe multiplicatif $\mathbb{R}^\times$ contient un sous-groupe $\mathbb{R}^\times_{>0}$ de réels strictement positifs. Pour $x, y \in \mathbb{R}^\times$ on a $x^{-1}y = yx^{-1} \in \mathbb{R}^\times_{>0}$ ssi x et y sont du même signe. Donc on a exactement deux classes à gauche (et à droite), le sous-groupe $\mathbb{R}^\times_{>0}$ et la classe $\mathbb{R}^\times_{<0}$ de réels strictement négatifs. Noter que $[\mathbb{R}^\times : \mathbb{R}^\times_{>0}] = 2$ est fini malgré le fait que $\mathbb{R}^\times$ et $\mathbb{R}^\times_{>0}$ sont infinis.

Lemme 2.7. *Pour un sous-groupe $H \subset G$ et $x, y \in G$, on a $xH = yH$ ssi on a $Hx^{-1} = Hy^{-1}$.*

Preuve. Par les lemmes 2.1 et 2.3 on a

$$xH = yH \quad \Longleftrightarrow \quad x^{-1}y = x^{-1}(y^{-1})^{-1} \in H \quad \Longleftrightarrow \quad Hx^{-1} = Hy^{-1}. \qquad \square$$

Corollaire 2.8. *Les classes à gauche de H dans G sont en bijection avec les classes à droite sous les applications inverses*

$$\begin{array}{rcl} \{\textit{classes à gauche}\} & \leftrightarrows & \{\textit{classes à droite}\}, \\ xH & \mapsto & Hx^{-1}, \\ y^{-1}H & \leftarrow\!\shortmid & Hy \end{array}$$

Donc il y a $[G : H]$ classes à droite et $[G : H]$ classes à gauche. Mais pour un sous-groupe général, les classes à gauche et les classes à droite ne coïncident pas.

Preuve. Les deux applications sont bien définies par le lemme précédent. Si on compose les deux applications, on trouve $xH \mapsto Hx^{-1} \mapsto xH$ et $Hy \mapsto y^{-1}H \mapsto Hy$. Comme les deux compositions sont des applications identités, les deux applications sont des bijections inverses. □

Théorème 2.9. *Soit G un groupe et N un sous-groupe. Alors N est distingué si et seulement si pour tout $x \in G$ on a $Nx = xN$.*

Preuve. ($\Rightarrow$) Supposons que $N \subset G$ est un sous-groupe distingué, et montrons les deux inclusions. Les membres de Nx sont de la forme nx avec $n \in N$, et il se réécrivent $nx = x(x^{-1}nx)$. Comme N est distingué, on a $x^{-1}nx \in N$, d'où $nx = x(x^{-1}nx) \in xN$. On trouve $Nx \subset xN$. Similairement, un $xn \in xN$ se réécrit comme $xn = (xnx^{-1})x \in Nx$. Donc on a aussi $xN \subset Nx$. D'où $xN = Nx$.

($\Leftarrow$) Supposons qu'on a $Nx = xN$ pour tout $x \in G$. Or soit $n \in N$ et $x \in G$, et cherchons si on a bien $xnx^{-1} \in N$. Mais $xn \in xN = Nx$ doit se réécrire sous la forme $xn = n_1x$ avec $n_1 \in N$. On trouve donc $xnx^{-1} = n_1 \in N$. Donc N est un sous-groupe distingué de G. □

Le théorème 2.4 se généralise au théorème suivant.

Théorème 2.10. *Soit G un groupe et $H \subset K \subset G$ des sous-groupes. Alors on a $[G : H] = [G : K][K : H]$.*

Preuve. Le groupe $G = \bigsqcup_{i=1}^{[G:K]} x_iK$ est la réunion disjointe de $[G : K]$ classes à gauche de K. Le groupe $K = \bigsqcup_{j=1}^{[K:H]} y_jH$ est la réunion disjointe de $[K : H]$ classes à gauche de H. Chaque classe à gauche de K est alors aussi la réunion disjointe $x_iK = \bigsqcup_{j}^{[K:H]} x_iy_jH$ de $[K : H]$ classes à gauche de H. Donc $G = \bigsqcup_{i}^{[G:K]} \bigsqcup_{j=1}^{[K:H]} x_iy_jH$ est la réunion disjointe de $[G : K][K : H]$ classes à gauche de H. Donc on a $[G : H] = [G : K][K : H]$. □

3. Les ensembles quotient

Le but de ce paragraphe est de généraliser la construction de l'anneau quotient $\mathbb{Z}/6\mathbb{Z}$ (par exemple) de l'arithmétique modulaire que l'on construit à partir de l'anneau $\mathbb{Z}$ et la relation $\equiv$ de congruence modulo 6. Cet anneau arrive avec une surjection canonique notée

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \\ x & \longmapsto & \overline{x} \end{array} \qquad \text{avec} \qquad \overline{x} = \overline{y} \quad \Leftrightarrow \quad x \equiv y \pmod 6.$$

Les membres de $\mathbb{Z}/6\mathbb{Z}$ se notent avec presque les mêmes etiquettes que les membres de $\mathbb{Z}$ (on ajoute un bar pour distinguer $\overline{0} \in \mathbb{Z}/6\mathbb{Z}$ de $0 \in \mathbb{Z}$). Mais les deux ensembles sont bien différents parce qu'on a, par exemple $\overline{0} = \overline{6} = \overline{12}$ dans $\mathbb{Z}/6\mathbb{Z}$ mais $0 \neq 6 \neq 12$ dans $\mathbb{Z}$. Des etiquettes désignant des membres distincts de $\mathbb{Z}$ peuvent désigner un même membre de $\mathbb{Z}/6\mathbb{Z}$.

Le cadre général de cette construction s'appelle les "ensembles quotient". On a un ensemble X et une relation d'équivalence $\simeq$. On rappelle la définition.

Définition. Une *relation d'équivalence* sur un ensemble X est une relation[4] $\simeq$ sur X avec trois propriétés :
(1) Reflexivité : on a $x \simeq x$ pour tout x.
(2) Symétrie : si $x \simeq y$ alors $y \simeq x$.
(3) Transitivité : si $x \simeq y$ et $y \simeq z$, alors $x \simeq z$.

La *classe d'équivalence* d'un $x \in X$ par rapport à $\simeq$ est le sous-ensemble

$$\text{classe}(x) = \{z \in X \mid x \simeq z\} \subset X. \tag{1}$$

Cette classe d'équivalence se note aussi $\overline{x}$ ou $[x]$ ou $\text{cl}(x)$ ou ...

Proposition 3.1. *Soit $\simeq$ une relation d'équivalence sur un ensemble X. Alors :*
(a) Pour tout $x \in X$ on a $x \in \text{classe}(x)$.
(b) Pour tout $x, y \in X$ on a soit $\text{classe}(x) \cap \text{classe}(y) = \varnothing$ soit $\text{classe}(x) = \text{classe}(y)$.

La démonstration est laissée en exercice. Les classes d'équivalence sont donc soit disjointes soit confondues, et les membres d'une classe d'équivalence ξ sont exactement les x avec $\text{classe}(x) = \xi$. L'ensemble X est la réunion disjointe des classes d'équivalence distinctes.

Définition. Soit $\simeq$ une relation d'équivalence sur un ensemble X. Ecrivons les classes d'équivalences sous la forme $\overline{x} = \text{classe}(x)$. L'*ensemble quotient* est alors

$$\overline{X} \;=\; \{\overline{x} \mid x \in X\}. \tag{2}$$

On écrit aussi $X/\simeq$ au lieu de $\overline{X}$. La *surjection canonique* (appelée aussi la *projection* et l'*application quotient*) est l'application $\pi \colon X \to \overline{X}$ envoyant $x \mapsto \overline{x} = \text{classe}(x)$.

Ce qui est important est que le quotient de X par $\simeq$ est un ensemble dont les membres s'écrivent $\overline{x}$ avec $x \in X$ mais on ajoute le bar ou quelque chose similaire, et où on a

$$\overline{x} = \overline{y} \quad \Longleftrightarrow \quad x \simeq y \quad \Longleftrightarrow \quad \text{classe}(x) = \text{classe}(y). \tag{3}$$

Cela implique que l'on a une bijection

$$\begin{aligned} \overline{X} &\overset{\cong}{\longleftrightarrow} \{\text{classes d'équivalence de } \simeq \text{ dans } X\} \\ \overline{x} &\longleftrightarrow \text{classe}(x). \end{aligned} \tag{4}$$

Dans la définition "officielle" du quotient, cette bijection est une identité. Néanmoins si on a un "modèle" pour $\overline{X}$ où (4) est une bijection mais pas litéralement l'identité, cela marche aussi.

Par exemple, prenons encore $X = \mathbb{Z}$ avec la relation d'équivalence $\equiv$ de congruence modulo 6. Il y a 6 classes de congruence distinctes, donc le quotient a 6 membres

$$\overline{X} = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}. \tag{5}$$

On a deux types de "modèles" pour $\mathbb{Z}/6\mathbb{Z}$ et la surjection canonique.

Dans le modèle "classique", $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$ sont les nombres $0, 1, 2, 3, 4, 5$ avec seulement une écriture distinctive. La surjection canonique $\pi \colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/6\mathbb{Z}$ est $n \mapsto \text{RESTE}(n, 6)$ où $\text{RESTE}(n, 6)$ est le reste dans la division euclidienne de n par 6. Par exemple $\pi(323) = 5$.

4. C'est à dire une règle selon laquelle pour tout $x, y \in X$ on a soit $x \simeq y$ soit $x \not\simeq y$.

Dans le modéle “officiel”, les membres de $\mathbb{Z}/6\mathbb{Z}$ sont les sous-ensembles

$$\overline{m} = \text{classe}(m) = 6\mathbb{Z} + m = \{6k + m \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$$

avec $m \in \mathbb{Z}$. La surjection canonique $\pi\colon \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ est $\pi(n) = \overline{n} = \text{classe}(n)$. Par exemple $\pi(323) = \overline{323} = \text{classe}(323) = 6\mathbb{Z} + 323$.

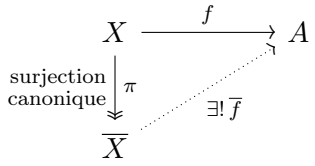
Chaque modèle a ses avantages et désavantages.

Théorème 3.2 (Propriété universelle d'un ensemble quotient)**.** *Soit $\simeq$ une relation d'équivalence sur X et $\pi\colon X \to \overline{X}$ la surjection canonique. Soit $f\colon X \to A$ une application. Alors il existe une unique application $\overline{f}\colon \overline{X} \to A$ avec $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in X$ si et seulement si pour $x, y \in X$ on a : $\overline{x} = \overline{y} \Rightarrow f(x) = f(y)$.*

L'application $\overline{f}$ est surjective ssi f est surjective.

L'application $\overline{f}$ est injective ssi on a en plus : $f(x) = f(y) \Rightarrow \overline{x} = \overline{y}$.

La condition $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in X$ est équivalent à $\overline{f} \circ \pi = f$. Ces applications forment un diagramme.



Preuve. ($\Rightarrow$) S'il existe $\overline{f}\colon \overline{X} \to A$ avec $\overline{f}(\overline{x}) = f(x)$ pour tout x, alors il est claire que quand $\overline{x} = \overline{y}$, alors $f(x) = \overline{f}(\overline{x}) = \overline{f}(\overline{y}) = f(y)$.

De plus, dans ce cas, toutes les valeurs de $\overline{f}$ sont déterminées par les équations $\overline{f}(\overline{x}) = f(x)$. Donc quand $\overline{f}$ existe, il est unique.

($\Leftarrow$) Supposons que $f\colon X \to A$ a la propriété que $\overline{x} = \overline{y}$ implique $f(x) = f(y)$. Alors comme $X \to \overline{X}$ est surjective, pour tout $\xi \in \overline{X}$ il existe un *représentant* $s_\xi \in X$ avec $\overline{s_\xi} = \xi$. Posons $\overline{f}(\xi) = f(s_\xi)$. Alors pour tout $x \in X$ on a $\overline{f}(\overline{x}) = f(s_{\overline{x}}) = f(x)$ car $\overline{s_{\overline{x}}} = \overline{x}$.

Surjectivité. De la formule $\overline{f}(\overline{x}) = f(x)$ on déduit que les deux ensembles image $\overline{f}(\overline{X}) \subset A$ et $f(X) \subset A$ sont les mêmes. Donc on a $\overline{f}(\overline{X}) = A$ ssi on a $f(X) = A$.

Injectivité. L'application $\overline{f}$ est injective ssi on a $\overline{f}(\overline{x}) = \overline{f}(\overline{y}) \Rightarrow \overline{x} = \overline{y}$. Mais vu qu'on a $\overline{f}(\overline{x}) = f(x)$ et $\overline{f}(\overline{y}) = f(y)$, ceci est équivalent à $f(x) = f(y) \Rightarrow \overline{x} = \overline{y}$. □

4. Les groupes, anneaux et espaces vectoriels quotients

Dans ce paragraphe on traite les structure algébriques quotients. La formule (7) est parmi les utiles du cours.

Groupes abéliens quotients. Soit $(G, +, 0)$ un groupe abélien et $H \subset G$ un sous-groupe. Pour $x, y \in G$ on écrit

$$x \equiv y \mod H \quad \overset{\text{déf}}{\iff} \quad x - y \in H \tag{6}$$

Le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ est la congruence modulo n des entiers. Une réécriture utile de cette définition est

$$\boxed{x \equiv y \mod H \quad \iff \quad \exists h \in H \text{ t.q. } x = y + h} \tag{7}$$

Lemme 4.1. *Pour H un sous-groupe du groupe abélien G, la relation (6)–(7) de congruence modulo H est une relation d'équivalence, et ses classes d'équivalence sont les classes (à gauche et à droite) de H dans G, c'est-à-dire* $\text{classe}(x) = H + x = x + H$.

Preuve. La congruence modulo H est une relation reflexive parce qu'on a $x = x + 0$ avec $0 \in H$. Elle est symétrique parce que s'il existe $h \in H$ avec $x = y + h$, alors $y = x + (-h)$ avec $-h \in H$. Elle est transitive parce que s'il existe $h, k \in H$ avec $x = y + h$ et $y = z + k$, alors $x = z + (k + h)$ avec $k + h \in H$. Donc la congruence modulo H est une relation d'équivalence.

Finalement on a

$$y \in \text{classe}(x) \iff x \equiv y \mod H \overset{(7)}{\iff} \exists h \in H \text{ avec } x = y + h \iff y \in x + H.$$

Donc on a bien $\text{classe}(x) = x + H = H + x$. □

On note G/H le quotient de l'ensemble G par la relation d'équivalence (6) de congruence modulo H. Ses membres s'écrivent $\overline{x}$ avec $x \in G$, mais on a

$$\overline{x} = \overline{y} \text{ dans } G/H \iff x \equiv y \mod H \iff x + H = y + H.$$

Surtout on a

$$\boxed{\overline{x} = \overline{y} \text{ dans } G/H \iff \exists h \in H \text{ avec } x = y + h} \tag{8}$$

En particulier on a

$$\boxed{\overline{x} = \overline{0} \iff x \in H.} \tag{9}$$

Théorème 4.2. *Soit H un sous-groupe d'un groupe abélien G, et soit G/H le quotient de G par la relation d'équivalence de congruence modulo H de (6). Alors la loi $G/H \times G/H \to G/H$ donnée par $\overline{x} + \overline{y} = \overline{x + y}$ est bien définie et est une loi de groupe abélien avec neutre $\overline{0}$ et opposés $-\overline{x} = \overline{-x}$.*

Preuve. Par le théorème 3.2, pour montrer que la loi donnée est bien définie, on suppose qu'on a $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$ et on doit en déduire $\overline{x + y} = \overline{x_1 + y_1}$. Mais $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$ signifie par (8) qu'il existe $h, k \in H$ avec $x = x_1 + h$ et $y = y_1 + k$. Alors on a

$$x + y = (x_1 + h) + (y_1 + k) = x_1 + y_1 + (h + k)$$

avec $h + k \in H$. Donc on a bien $\overline{x + y} = \overline{x_1 + y_1}$.

La loi de G/H est vérifie les axiomes d'un groupe abélien parce que la loi de G les vérifie. En effet on a

$$\begin{gathered} (\overline{x} + \overline{y}) + \overline{z} = \overline{(x + y) + z} = \overline{x + (y + z)} = \overline{x} + (\overline{y} + \overline{z}), \\ \overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}, \\ \overline{x} + \overline{0} = \overline{x + 0} = \overline{x}, \\ \overline{x} + \overline{-x} = \overline{x + (-x)} = \overline{0}. \end{gathered} \tag{10}$$

Donc G/H est bien un groupe abélien avec la loi $\overline{x} + \overline{y} = \overline{x + y}$, le neutre $\overline{0}$ et opposés $-\overline{x} = \overline{-x}$. □

Groupes quotients en général. Maintenant soit $(G, \cdot, e)$ un groupe et $H \subset G$ un sous-groupe. Au lieu d'avoir une relation de congruence modulo H, on en a deux :

$$x \equiv_r y \mod H \overset{\text{déf}}{\iff} xy^{-1} \in H \iff \exists h \in H \text{ avec } x = hy,$$

$$x \equiv_\ell y \mod H \overset{\text{déf}}{\iff} x^{-1}y \in H \iff \exists h \in H \text{ avec } x = yh.$$

Chacune est une relation d'équivalence selon un argument presque identique à la démonstration du lemme 4.1. On voit par les lemmes 2.1(a) et 2.3(a) qu'on a

$$x \equiv_r y \mod H \Leftrightarrow Hx = Hy, \qquad x \equiv_\ell y \mod H \Leftrightarrow xH = yH.$$

Donc les classes à droite et les classes à gauche de H dans G sont les classes d'équivalences pour ces deux congruences. Les deux ensembles quotients se notent

$$H\backslash G = \{Hx \mid x \in G\}, \qquad G/H = \{xH \mid x \in G\}.$$

Quand H est distingué dans G, les classes à gauche et à droite coïncident, et donc les deux relations de congruence modulo H coïncident aussi.

Ecrivons les membres de G/H comme $\overline{x} = xH$. On aimerait définir une multiplication sur G/H par la formule $\overline{x}\,\overline{y} = \overline{xy}$. Mais cela marche-t-il ? Selon le théorème 3.2, pour que ça marche il faut que $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$ implique $\overline{xy} = \overline{x_1 y_1}$. Mais si on a $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$, alors il existe $h, k \in H$ avec $x = x_1 h$ et $y = y_1 k$. On trouve

$$xy = x_1 h y_1 k = x_1 y_1 (y_1^{-1} h y_1) k$$

On a donc $\overline{xy} = \overline{x_1 y_1}$ si et seulement si on a $y_1^{-1} h y_1 \in H$. Ce dernier n'est vrai pour tout $h \in H$ et $y_1 \in G$ que si H est distingué dans G.

Conclusion : *La formule $\overline{x}\,\overline{y} = \overline{xy}$ donne une multiplication bien définie sur G/H si et seulement si H est distingué dans G.*

Théorème 4.3. *Soit N un sous-groupe distingué d'un groupe $(G, \cdot, e)$, et soit G/N le quotient de G par la relation d'équivalence où $x \equiv y$ si et seulement si $xN = yN$. Alors la loi $G/N \times G/N \to G/N$ donnée par $\overline{x}\,\overline{y} = \overline{xy}$ est bien définie et est une loi de groupe avec neutre $\overline{e}$ et inverses $\overline{x}^{-1} = \overline{x^{-1}}$.*

Preuve. On a déjà vu que la loi $\overline{x}\,\overline{y} = \overline{xy}$ est bien définie. Le calcul montrant que la loi de G/N vérifie les axiomes d'un groupe parce que la loi de G les vérifie est similaire à (10) ci-dessus et est laissé au lecteur. □

Remarque 4.4. On a $|G/N| = [G : N]$ car tous les deux sont le nombre de classes à gauche de N dans G.

On a $G/N = \{\overline{e}\}$ ssi on a $G = N$.

On a $\overline{x} = \overline{e}$ dans G/N ssi on a $x \in N$.

Le noyau de la surjection canonique $\pi\colon G \to G/N$ envoyant $x \mapsto \overline{x}$ est N.

Proposition 4.5. *Soit G un groupe et $N \subset H \subset G$ des sous-groupes avec N distingué dans G. Notons $\overline{x} = xN$ les membres de G/N.*

(a) Alors N est aussi un sous-groupe distingué de H, et $H/N \subset G/N$ est un sous-groupe. Pour $x \in G$ on a $\overline{x} \in H/N$ ssi on a $x \in H$. On a $[G/N : H/N] = [G : H]$.

(b) $H \subset G$ est un sous-groupe distingué ssi $H/N \subset G/N$ est un sous-groupe distingué.

Preuve. On note seulement que si on écrit $G = \bigsqcup_{i=1}^{[G:H]} y_i H$ comme la réunion disjointe de $[G : H]$ classes à gauche de H, alors $G/N = \bigsqcup_{i=1}^{[G:H]} \overline{y_i}\, H/N$ est la réunion disjointe de $[G : H]$ classes à gauche de H/N. Donc on a bien $[G/N : H/N] = [G : H]$. Le reste est facile et est laissé au lecteur. □

Proposition 4.6. *Soit $N \subset G$ un sous-groupe distingué, et $K \subset G/N$ un sous-groupe. Alors $\pi^{-1}(K) = \{x \in G \mid \overline{x} \in K\} \subset G$ est un sous-groupe contenant N, et on a $\pi^{-1}(K)/N = K$.*

Preuve. On utilise le critère de sous-groupe du théorème 1.1, en prenant compte des formules $\overline{x}\,\overline{y} = \overline{xy}$ et $\overline{x}^{-1} = \overline{x^{-1}}$ du théorème 4.3. Les détails sont laissés au lecteur. □

Théorème 4.7 (Propriété universelle du groupe quotient)**.** *Soit G un groupe et $N \subset G$ un sous-groupe distingué. Soit $\phi\colon G \to H$ un morphisme de groupes. Alors il existe un morphisme unique $\overline{\phi}\colon G/N \to H$ avec $\overline{\phi}(\overline{x}) = \phi(x)$ pour tout $x \in G$ si et seulement si on a $N \subset \ker\phi$.*

On a $\ker\overline{\phi} = (\ker\phi)/N$. En particulier le morphisme $\overline{\phi}$ est injectif ssi on a $N = \ker\phi$.

Le morphisme $\overline{\phi}$ est surjectif ssi ϕ est surjectif.

Preuve. Selon le théorème 3.2 il existe une unique application $\overline{\phi}\colon G/N \to H$ avec $\overline{\phi}(\overline{x}) = \phi(x)$ pour tout $x \in G$ ssi on a $\overline{x} = \overline{y} \;\Rightarrow\; \phi(x) = \phi(y)$. Mais la condition $\overline{x} = \overline{y}$ est équivalent à $x^{-1}y \in N$, tandis que la condition $\phi(x) = \phi(y)$ est équivalent à $x^{-1}y \in \ker\phi$. Donc il existe un $\overline{\phi}$ avec la propriété énoncée ssi on a $x^{-1}y \in N \Rightarrow x^{-1}y \in \ker\phi$, ce qui est équivalent à $N \subset \ker\phi$.

Quand l'application $\overline{\phi}$ existe, c'est un morphisme de groupes, parce qu'on a

$$\overline{\phi}(\overline{x}\,\overline{y}) = \overline{\phi}(\overline{xy}) = \phi(xy) = \phi(x)\phi(y) = \overline{\phi}(\overline{x})\,\overline{\phi}(\overline{y}).$$

De $\overline{\phi}(\overline{x}) = \phi(x)$, on déduit qu'on a $\overline{x} \in \ker\overline{\phi}$ ssi on a $x \in \ker\phi$. Ainsi $\ker\overline{\phi} = (\ker\phi)/N$. En particulier $\overline{\phi}$ est injectif ssi on a $\ker\overline{\phi} = (\ker\phi)/N = \{\overline{e}\}$ par la proposition 1.2, et ceci est équivalent à $\ker\phi = N$ par la remarque 4.4.

La condition de surjectivité suit directement du théorème 3.2. □

Corollaire 4.8. *Le morphisme de groupes $\phi\colon G \to H$ induit un isomorphisme $G/\ker\phi \xrightarrow{\cong} \operatorname{im}\phi$ donné par $\overline{x} \mapsto \phi(x)$.*

Proposition 4.9. *Soit G un groupe, et $N \subset H \subset G$ des sous-groupes distingués. Alors on a un isomorphisme naturel $\frac{G/N}{H/N} \cong G/H$ identifiant l'image de $x \in G$ sous la composition de surjections canoniques $G \twoheadrightarrow G/N \twoheadrightarrow \frac{G/N}{H/N}$ à son image sous la surjection canonique $G \twoheadrightarrow G/H$.*

Preuve. Soit $\pi\colon G \to G/H$ la surjection canonique. Comme on a $\ker\pi = H$ (remarque 4.4) et $N \subset H$, il existe $\overline{\pi}\colon G/N \to G/H$ avec $\overline{\pi}(\overline{x}) = \pi(x)$ par le théorème 4.7. De plus on a $\ker\overline{\pi} = (\ker\pi)/N = H/N$. Donc le corollaire 4.8 nous donne l'isomorphisme $\frac{G/N}{H/N} \cong G/H$. □

Soit $N \subset G$ un sous-groupe distingué et $H \subset G$ un sous-groupe. Considérons l'application

$$\begin{aligned} \psi_{H,N}\colon H &\longrightarrow G/N \\ h &\longmapsto \overline{h} = hN \end{aligned} \tag{11}$$

Ce $\psi_{H,N}$ est la composition de l'inclusion $H \hookrightarrow G$ avec la surjection canonique $\pi\colon G \twoheadrightarrow G/N$. On a $\ker\psi_{H,N} = H \cap N$ (exercice). L'image $\operatorname{im}\psi_{H,N}$ ne peut pas être H/N en général parce que cela n'a pas de sens quand on a $N \not\subset H$. Mais selon la proposition 4.6 on peut relever les sous-groupes $\{\overline{e}\} \subset \operatorname{im}\psi_{H,N} \subset G/N$ en les sous-groupes $N \subset \pi^{-1}(\operatorname{im}\psi_{H,N}) \subset G$, et on a $\operatorname{im}\psi_{H,N} = \pi^{-1}(\operatorname{im}\psi_{H,N})/N$. Or on a

$$\begin{aligned} \pi^{-1}(\operatorname{im}\psi_{H,N}) &= \{x \in G \mid \overline{x} \in \operatorname{im}\psi_{H,N}\} \\ &= \{x \in G \mid \exists h \in H \text{ avec } \overline{x} = \overline{h}\} \\ &= \{x \in G \mid \exists h \in H, \exists n \in N \text{ avec } x = hn\} \\ &= \{hn \mid h \in H, n \in N\} \\ &= HN. \end{aligned}$$

Donc HN est un sous-groupe de G avec $N \subset HN \subset G$, et on a $\operatorname{im}\psi_{H,N} = HN/N$. L'isomorphisme $H/\ker\psi_{H,N} \cong \operatorname{im}\psi_{H,N}$ du corollaire 4.8 est alors de la forme $H/(H \cap N) \cong HN/N$. En résumé :

Théorème 4.10. *Soit G un groupe, $N \subset G$ un sous-groupe distingué, $H \subset G$ un sous-groupe, et soit $\psi_{H,N} \colon H \to G/N$ le morphisme envoyant $h \mapsto \overline{h} = hN$.*

(a) Alors $HN = \{hn \mid h \in H, n \in N\}$ est un sous-groupe de G, et on a $\operatorname{im} \psi_{H,N} = HN/N$.

(b) On a $\ker \psi_{H,N} = H \cap N$.

(c) Il y a un isomorphisme naturel $H/(H \cap N) \cong HN/N$ envoyant la classe $\hat{h} = h(H \cap N) \in H/(H \cap N)$ en la classe $\overline{h} = hN \in HN/N$.

Espaces vectoriels quotients. Quand E est un espace vectoriel sur un corps commutatif K et $F \subset E$ est un sous-espace vectoriel, on peut utiliser la même notion de congruence que pour les groupes abéliens (7) :

$$x \equiv y \mod F \quad \overset{\text{déf}}{\iff} \quad \exists v \in F \text{ avec } x = y + v.$$

Les classes d'équivalence sont alors classes $\overline{x} = x + F$. On a $\overline{x} = \overline{0}$ ssi $x \in F$.

Théorème 4.11. *Soit F un sous-espace vectoriel d'un K-espace vectoriel E, et soit E/F le quotient de E par la relation d'équivalence de congruence modulo F. Alors l'addition $E/F \times E/F \to E/F$ donnée par $\overline{x} + \overline{y} = \overline{x+y}$ et la multiplication $K \times E/F \to E/F$ donnée par $r\overline{x} = \overline{rx}$ sont bien définies et font de E/F un K-espace vectoriel avec neutre $\overline{0}$ et opposés $-\overline{x} = \overline{-x}$.*

Preuve. L'addition est bien définie par le théorème 4.2. Pour montrer que la multiplication est bien définie, il faut montrer que pour $x, y \in E$ avec $\overline{x} = \overline{y}$, on a aussi $\overline{rx} = \overline{ry}$. Mais si $\overline{x} = \overline{y}$, alors il existe $v \in F$ avec $x = y + v$, et alors $rx = ry + rv$ avec $rv \in F$, et donc $\overline{rx} = \overline{ry}$.

Les lois de E/F vérifient les axiomes d'un espace vectoriel parce que les lois de E les vérifient, selon des calculs similaires à (10), qui sont laissés au lecteur. □

Théorème 4.12 (Propriété universelle de l'espace vectoriel quotient)**.** *Soit $F \subset E$ un sous-espace vectoriel d'un K-espace vectoriel. Soit $\phi \colon E \to V$ un morphisme de K-espaces vectoriels. Alors il existe un morphisme unique $\overline{\phi} \colon E/F \to V$ de K-espaces vectoriels avec $\overline{\phi}(\overline{x}) = \phi(x)$ pour tout $x \in E$ si et seulement si on a $F \subset \ker \phi$.*

On a $\ker \overline{\phi} = (\ker \phi)/F$. En particulier le morphisme $\overline{\phi}$ est injectif ssi on a $F = \ker \phi$.

Le morphisme $\overline{\phi}$ est surjectif ssi ϕ est surjectif.

Preuve. Tout est déjà démontré dans le théorème 4.7 sauf la K-linéarité de $\overline{\phi}$ qui se déduit de la K-linéarité de ϕ par

$$\overline{\phi}(r\overline{x}) = \overline{\phi}(\overline{rx}) = \phi(rx) = r\phi(x) = r\overline{\phi}(\overline{x}).$$ □

Théorème 4.13. *Soit $F \subset E$ un sous-espace d'un K-espace vectoriel. Alors on a*

$$\dim E = \dim F + \dim E/F.$$

Preuve. Exercice. □

Anneaux commutatifs quotients.

Définition. Un *idéal* I d'un anneau commutatif A est un sous-ensembles avec trois propriétés

(a) $0 \in I$.

(b) Si $x, y \in I$, alors $x + y \in I$.

(c) Si $x \in I$ et $a \in A$, alors $ax \in I$.

$\{0\}$ et A sous des ideáux de A.

$2\mathbb{Z}$, $6\mathbb{Z}$, et $n\mathbb{Z}$ sont des idéaux de l'anneau $(\mathbb{Z}, +, \cdot, 0, 1)$.

Théorème 4.14. *Soit I un idéal d'un anneau commutatif A, et soit A/I le quotient de A par la relation d'équivalence de congruence modulo I. Alors l'addition $A/I \times A/I \to A/I$ donnée par $\overline{x}+\overline{y} = \overline{x+y}$ et la multiplication $A/I \times A/I \to A/I$ donnée par $\overline{x}\,\overline{y} = \overline{xy}$ sont bien définies et font de A/I un anneau commutatif avec neutres $\overline{0}$ et $\overline{1}$ et opposés $-\overline{x} = \overline{-x}$.*

Preuve. On montre que la multiplication $A/I \times A/I \to A/I$ donnée par $\overline{x}\,\overline{y} = \overline{xy}$ est bien définie, et on laisse tout le reste au lecteur.

Supposons qu'on a $\overline{x} = \overline{x_1}$ et $\overline{y} = \overline{y_1}$. Cela signifie qu'il existe $r, s \in I$ avec $x = x_1 + r$ et $y = y_1 + s$. Alors on a

$$xy = (x_1 + r)(y_1 + s) = x_1y_1 + ry_1 + sx_1 + rs.$$

Comme on a $ry_1 + sx_1 + rs \in I$, on a bien $\overline{xy} = \overline{x_1y_1}$. □

Théorème 4.15 (Propriété universelle d'un anneau commutatif quotient)**.** *Soit $\phi\colon A \to B$ un morphismes d'anneaux commutatifs, et $I \subset A$ un idéal. Alors il existe un morphisme unique $\overline{\phi}\colon A/I \to B$ d'anneaux avec $\overline{\phi}(\overline{x}) = \phi(x)$ pour tout $x \in A$ si et seulement si on a $I \subset \ker\phi$.*

On a $\ker\overline{\phi} = (\ker\phi)/I$. En particulier le morphisme $\overline{\phi}$ est injectif ssi on a $I = \ker\phi$.

Le morphisme $\overline{\phi}$ est surjectif ssi ϕ est surjectif.

Le conoyau d'un morphisme.

Définition. Le *conoyau* d'un morphisme de groupes abéliens $\phi\colon G \to A$ est le groupe abélien quotient $\operatorname{coker}\phi = A/(\operatorname{im}\phi) = A/(\phi(G))$. Le *conoyau* d'un morphisme d'espaces vectoriel $\phi\colon V \to W$ est l'espace vectoriel quotient $\operatorname{coker}\phi = W/(\operatorname{im}\phi) = W/\phi(V)$.

Par exemple, le conoyau du morphisme $\mathbb{Z} \to \mathbb{Z}$ donné par $x \mapsto nx$ est $\mathbb{Z}/n\mathbb{Z}$.

Il y a 3 groupes ou espaces associés à un morphisme de groupes abéliens ou d'espaces vectoriels : le noyau, l'image et le conoyau.

5. Les groupes cycliques

Dans ce paragraphe, on fait des rappels sur les groupes $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ et ensuite les groupes cycliques en général.

Pour chaque entier $n \geq 0$, l'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe du groupe $(\mathbb{Z}, +, 0)$. On montre maintenant que ce sont les seuls sous-groupes de $\mathbb{Z}$.

Théorème 5.1. *Soit $H \subset \mathbb{Z}$ un sous-groupe additif. Alors soit $H = \{0\}$ soit $H = n\mathbb{Z}$ avec n le plus petit entier avec $n \geq 1$ et $n \in H$.*

Preuve. Supposons $H \neq \{0\}$. Alors H contient des membres non nuls, et comme H est stable sous opposés, il contient des membres strictement positifs. Soit n le plus petit entier avec $n \geq 1$ et $n \in H$. Comme H est stable sous sommes et opposés, on a $n\mathbb{Z} \subset H$.

Il reste à montrer $H \subset n\mathbb{Z}$. Donc soit $h \in H$. En faisant la division euclidienne de h par n on trouve des entiers q et r avec $h = qn + r$ et $0 \leq r \leq n - 1$. On a $r = h - qn \in H$. Mais on a $i \notin H$ pour $1 \leq i \leq n - 1$. On en déduit $r = 0$. Donc on a $h = qn \in n\mathbb{Z}$. On trouve donc $H = n\mathbb{Z}$. □

Les $n\mathbb{Z}$ (avec $n \geq 0$) sont aussi des idéaux de l'anneau commutatif $\mathbb{Z}$, et ce théorème démontre qu'ils sont les seuls idéaux de $\mathbb{Z}$.

Deux entiers a, b ont la même classe $\overline{a} = \overline{b}$ dans le groupe abélien (ou anneau) quotient $\mathbb{Z}/n\mathbb{Z}$ ssi ils ont le même reste quand on les divise par n. On en déduit que $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ sont les seuls membres de $\mathbb{Z}/n\mathbb{Z}$ et qu'ils sont distincts. Donc on a $|\mathbb{Z}/n\mathbb{Z}| = n$.

Proposition 5.2. *Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n. On a des isomorphismes naturels $\frac{\mathbb{Z}/n\mathbb{Z}}{d\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/d\mathbb{Z}$, et on a $|d\mathbb{Z}/n\mathbb{Z}| = \frac{n}{d}$.*

Preuve. Selon les propositions 4.5 et 4.6 les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $n\mathbb{Z} \subset d\mathbb{Z} \subset \mathbb{Z}$. On a

$$n\mathbb{Z} \subset d\mathbb{Z} \iff n \in d\mathbb{Z} \iff \exists k \in \mathbb{Z} \text{ avec } n = dk \iff d \text{ divise } n.$$

Cela démontre la première phrase de la proposition. Les isomorphismes naturels sont ceux de la proposition 4.9. Finalement par le théorème 2.10 et la remarque 4.4 on a

$$|d\mathbb{Z}/n\mathbb{Z}| = \frac{|\mathbb{Z}/n\mathbb{Z}|}{|\mathbb{Z}/d\mathbb{Z}|} = \frac{n}{d}. \qquad \square$$

Pour a, b entiers le théorème 5.1 s'applique aux sous-groupes $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.

Théorème 5.3. *Pour a, b entiers on a*

$$a\mathbb{Z} + b\mathbb{Z} = \operatorname{pgcd}(a,b)\mathbb{Z}, \qquad a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{ppcm}(a,b)\mathbb{Z}.$$

Preuve. Par le théorème 5.1 il existe $d \geq 1$ avec $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On a $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, et ainsi d divise a par la proposition 5.2. On a aussi $b\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, et par conséquent d divise b. Donc d est un diviseur commun de a et b.

Or soit e un diviseur commun de a et b. Alors on a $a\mathbb{Z} \subset e\mathbb{Z}$ et $b\mathbb{Z} \subset e\mathbb{Z}$. Comme $e\mathbb{Z}$ est stable sous l'addition, on a aussi $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \subset e\mathbb{Z}$. Donc e divise d. On trouve que d est un diviseur commun de a et b divisible par tous les diviseurs communs de a et b. On a donc $d = \operatorname{pgcd}(a,b)$ par la définition du pgcd.

La démonstration de $a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{ppcm}(a,b)\mathbb{Z}$ est similaire. $\square$

Le sous-groupe du groupe G *engendré* par le sous-ensemble $S \subset G$ et le plus petit sous-groupe de G contenant S. Il est noté $\langle S \rangle \subset G$. Ses membres sont e et les éléments de la forme $x_1 x_2 \dots x_r$ avec $x_i \in S \cup S^{-1}$ pour tout i. (Ici $S^{-1} = \{s^{-1} \mid s \in S\}$). En particulier le sous-groupe de G engendré par un élément g est

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}.$$

Quand la loi est $+$ on écrit souvent $\langle g \rangle = \mathbb{Z}g = \{n \cdot g \mid n \in \mathbb{Z}\} \subset G$.

Définition. Un groupe G est *cyclique* avec *générateur* g si on a $G = \langle g \rangle$. [5]

Définition. L'*ordre* d'un élément $g \in G$ (noté $\operatorname{ord}(g)$) est le plus petit $n \geq 1$ tel qu'on ait $g^n = e$ (ou $n \cdot g = 0$). S'il n'existe pas un tel n, on dit que g est d'ordre infini.

On a ainsi $\operatorname{ord}(g) = n$ ssi on a $g^n = e$ et aussi $g^i \neq e$ pour tout $1 \leq i \leq n-1$.

Pour chaque élément $g \in G$ on a un morphisme $\rho_g \colon \mathbb{Z} \to G$ envoyant $i \mapsto g^i$ (si la loi est $+$ c'est $i \mapsto i \cdot g$). L'image de ρ_g est le sous-groupe cyclique $\langle g \rangle \subset G$. En comparant la définition de l'ordre de g au théorème 5.1, on voit que $\ker \rho_g = n\mathbb{Z}$ avec $n = \operatorname{ord}(g)$ si ceci est fini, et $\ker \rho_g = \{0\}$ si $\operatorname{ord}(g) = \infty$. En appliquant l'isomorphisme $\mathbb{Z}/\ker \rho_g \cong \operatorname{im} \rho_g$ on trouve les résultats suivants.

Proposition 5.4. *Si $g \in G$ est d'ordre infini, alors il y a un isomorphisme $\mathbb{Z} \xrightarrow{\cong} \langle g \rangle$ envoyant $i \mapsto g^i$.*

5. Certains disent *monogène* plutôt que cyclique et réservent le mot *cyclique* pour les groupes cycliques finis.

Proposition 5.5. *Si* $\operatorname{ord}(g) = n$ *est fini, alors il y a un isomorphisme* $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \langle g \rangle$ *envoyant* $\overline{i} \mapsto g^i$. *Par conséquent*

(a) *On a* $g^m = e$ *si et seulement si* n *divise* m.

(b) *On a* $|\langle g \rangle| = \operatorname{ord}(g) = n$, *et* n *divise* $|G|$ *si* G *est fini.*

Donc tout groupe cyclique est isomorphe soit à $\mathbb{Z}$ soit à un $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 1$.

Corollaire 5.6. *Soit* G *un groupe d'ordre* n. *Alors* G *est cyclique ssi il existe* $g \in G$ *avec* $\operatorname{ord}(g) = n$.

Corollaire 5.7. *Si* $|G| = p$ *est un premier, alors* G *est cyclique.*

Proposition 5.8. *Soit* $g \in G$ *avec* $\operatorname{ord}(g) = n$. *Pour* $i \in \mathbb{Z}$ *on a* $\langle g^i \rangle = \langle g^{\operatorname{pgcd}(n,i)} \rangle$ *et* $\operatorname{ord}(g^i) = \frac{n}{\operatorname{pgcd}(n,i)}$. *En particulier* $\operatorname{ord}(g^i)$ *divise* $\operatorname{ord}(g)$, *et on a*

$$\operatorname{pgcd}(n,i) = 1 \quad \Longleftrightarrow \quad g^i \text{ engendre } \langle g \rangle \quad \Longleftrightarrow \quad \operatorname{ord}(g^i) = n$$

Preuve. D'abord il est clair de la définition que si d divise n, alors $\operatorname{ord}(g^d) = \frac{n}{d}$.

Maintenant soit i général. Comme i est un multiple de $\operatorname{pgcd}(n,i)$, on a $g^i \in \langle g^{\operatorname{pgcd}(n,i)} \rangle$ et par conséquent $\langle g^i \rangle \subset \langle g^{\operatorname{pgcd}(n,i)} \rangle$. Par le théorème 5.3 il existe $a, b \in \mathbb{Z}$ avec $\operatorname{pgcd}(n,i) = ai + bn$. On en déduit $g^{\operatorname{pgcd}(n,i)} = (g^i)^a (g^n)^b = (g^i)^a e^b = (g^i)^a$. D'où on a $g^{\operatorname{pgcd}(n,i)} \in \langle g^i \rangle$ et $\langle g^{\operatorname{pgcd}(n,i)} \rangle \subset \langle g^i \rangle$. On a montré $\langle g^i \rangle = \langle g^{\operatorname{pgcd}(n,i)} \rangle$.

Par la proposition 5.5(c) on a $\operatorname{ord}(g^i) = |\langle g^i \rangle| = |\langle g^{\operatorname{pgcd}(n,i)} \rangle| = \operatorname{ord}(g^{\operatorname{pgcd}(n,i)})$. Ce dernier ordre est $\frac{n}{\operatorname{pgcd}(n,i)}$ car $\operatorname{pgcd}(n,i)$ divise n. □

Finalement, on étudie le groupe d'automorphismes d'un groupe cyclique.

D'abord pour A un anneau commutatif, on note $A^\times = \{a \in A \mid \exists b \in A \text{ avec } ab = 1\}$ le sous-ensemble d'éléments inversibles de A. Alors $(A^\times, \cdot, 1)$ est un groupe abélien. Du lemme de Bezout on déduit que pour $n \geq 1$ on a

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{pgcd}(k,n) = 1\}.$$

Lemme 5.9. *Soit* G *un groupe abélien. Pour chaque* $a \in \mathbb{Z}$ *soit* $\rho_{a,G} \colon G \to G$ *l'application envoyant* $x \mapsto x^a$.

(a) *Chaque* $\rho_{a,G}$ *est un morphisme de groupes.*

(b) *Pour* $a, b \in \mathbb{Z}$ *on a* $\rho_{a,G} \circ \rho_{b,G} = \rho_{ab,G}$.

(c) *Si* $|G| = n$ *est fini, alors* $\rho_{a,G} = \rho_{a+nk,G}$ *pour tout* $k \in \mathbb{Z}$.

(d) *Si* $|G| = n$ *est fini, alors* $\rho_{a,G}$ *est un isomorphisme si* $\operatorname{pgcd}(a,n) = 1$.

Preuve. Les démonstrations de (a) et (b) sont laissées au lecteur.

(c) Pour tout $x \in G$, $\operatorname{ord}(x)$ divise $|G|$, et par conséquent $x^n = e$. On en déduit $\rho_{a+nk}(x) = x^a (x^n)^k = x^a e^k = x^a = \rho_a(x)$.

(d) Si $\operatorname{pgcd}(a,n) = 1$ alors il existe $b, m \in \mathbb{Z}$ avec $ab + mn = 1$. Par (b) et (c) on a

$$\rho_{a,G} \circ \rho_{b,G} = \rho_{b,G} \circ \rho_{a,G} = \rho_{ab,G} = \rho_{1-mn,G} = \rho_{1,G} = \mathrm{Id}_G \,.$$

Donc $\rho_{a,G}$ et $\rho_{b,G}$ sont des isomorphismes inverses. □

Théorème 5.10. *Si* G *est cyclique d'ordre* n, *on a un isomorphisme* $\iota \colon (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\cong} \operatorname{Aut}(G)$ *envoyant* $\overline{a} \mapsto \rho_{a,G}$.

Preuve. Par le lemme 5.9, le morphisme $\rho_{a,G}$ ne dépend que de la classe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, il est un automorphisme de G pour $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, et ι est un morphisme de groupes. Montrons que ι est bijectif.

Soit $\overline{a} \in \ker \iota$. Alors $\rho_{a,G} = \mathrm{Id}_G$. Soit $g \in G$ un générateur. On a $\rho_{a,G}(g) = g^a = \mathrm{Id}_G(G) = g$. Comme g est d'ordre n par la proposition 5.8, par la proposition 5.5 il y a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \langle g \rangle = G$ envoyant $\overline{i} \mapsto g^i$. De $g^a = g^1$ on déduit donc $\overline{a} = \overline{1}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Donc $\ker \iota = \{\overline{1}\}$, et ι est injectif par la proposition 1.2.

Maintenant soit $\sigma \in \mathrm{Aut}\, G$. Comme on a $\sigma(g) \in G = \langle g \rangle$, il existe $a \in \mathbb{Z}$ avec $\sigma(g) = g^a$. Les éléments de $G = \langle g \rangle$ s'écrivent tous sous la forme g^i, et on a $\sigma(g^i) = \sigma(g)^i = (g^a)^i = (g^i)^a = \rho_{a,G}(g^i)$. Donc on a $\sigma = \rho_{a,G}$. Comme σ est un isomorphisme, il préserve l'ordre de g. Donc on a $\mathrm{ord}(g^a) = \mathrm{ord}(\sigma(g)) = \mathrm{ord}(g) = n$. Par la proposition 5.8 on a $\mathrm{pgcd}(a, n) = 1$. Donc on a $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, et on a $\sigma = \iota(\overline{a})$. Donc ι est surjectif. □

6. Sur la structure des groupes abéliens fini

Dans ce paragraphe on démontre que tout groupe abélien fini est isomorphe à un produit de groupes cycliques.

Proposition 6.1. *Soit $g, h \in G$ avec $gh = hg$, et soit $\mathrm{ord}(g) = m$ et $\mathrm{ord}(h) = n$.*
(a) Alors $\mathrm{ord}(gh)$ divise $\mathrm{ppcm}(m, n)$.
(b) Alors $\frac{\mathrm{ppcm}(m,n)}{\mathrm{pgcd}(m,n)}$ divise $\mathrm{ord}(gh)$.
(c) Si m et n sont premiers entre eux, alors $\mathrm{ord}(gh) = mn$.

Preuve. (a) Comme m divise $\mathrm{ppcm}(m, n)$, on a $g^{\mathrm{ppcm}(m,n)} = e$. Comme n divise $\mathrm{ppcm}(m, n)$, on a $h^{\mathrm{ppcm}(m,n)} = e$. Comme g et h commutent, on a $(gh)^i = g^i h^i$ pour tout i. Donc on a $(gh)^{\mathrm{ppcm}(m,n)} = g^{\mathrm{ppcm}(m,n)} h^{\mathrm{ppcm}(m,n)} = e$. Par conséquent l'ordre de gh divise $\mathrm{ppcm}(m, n)$.

(b) Soit $r = \mathrm{ord}(gh)$. Alors on a $(gh)^r = g^r h^r = e$, et ainsi $g^r = h^{-r}$. Soit $d = \mathrm{ord}(g^r)$. D'une part $d = \mathrm{ord}(g^r)$ divise $m = \mathrm{ord}(g)$ par la proposition 5.8. Similairement $d = \mathrm{ord}(h^{-r})$ divise $n = \mathrm{ord}(h)$. Donc d divise $\mathrm{pgcd}(m, n)$. D'autre part on a $g^{rd} = e$. Donc $m = \mathrm{ord}(g)$ divise rd. Similairement on a $h^{-rd} = e$, et $n = \mathrm{ord}(h)$ divise rd. Donc $\mathrm{ppcm}(m, n)$ divise rd, et rd divise $r\,\mathrm{pgcd}(m, n)$. Par transitivité $\mathrm{ppcm}(m, n)$ divise $r\,\mathrm{pgcd}(m, n)$, et ainsi $\frac{\mathrm{ppcm}(m,n)}{\mathrm{pgcd}(m,n)}$ divise $r = \mathrm{ord}(gh)$.

(c) Immédiat de (a) et (b). □

Proposition 6.2. *Soit $g, h \in G$ avec $gh = hg$, et soit $\mathrm{ord}(g) = m$ et $\mathrm{ord}(h) = n$. Alors il existe r, s avec $\mathrm{ord}(g^r h^s) = \mathrm{ppcm}(m, n)$.*

Preuve. Factorisons $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ et $n = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$ avec les p_i des premiers distincts. Ecrivons

$$m_1 = \prod_{i \text{ avec } a_i \geq b_i} p_i^{a_i}, \qquad m_2 = \prod_{i \text{ avec } a_i < b_i} p_i^{a_i},$$
$$n_1 = \prod_{i \text{ avec } a_i \geq b_i} p_i^{b_i}, \qquad n_2 = \prod_{i \text{ avec } a_i < b_i} p_i^{b_i}.$$

Alors on a $m_1 m_2 = m$ et $\mathrm{ord}(g^{m_2}) = m_1$. On a $n_1 n_2 = n$ et $\mathrm{ord}(h^{n_1}) = n_2$. Les premiers divisant m_1 sont distincts des premiers divisant n_2, et par conséquent m_1 et n_2 sont premiers entre eux. Appliquant la proposition 6.1(c) à g^{m_2} et h^{n_1}, on trouve $\mathrm{ord}(g^{m_2} h^{n_1}) = m_1 n_2 = \mathrm{ppcm}(m, n)$. □

Corollaire 6.3. *Si $g_1, g_2, \ldots, g_r \in G$ commutent et si $\mathrm{ord}(g_i) = n_i < \infty$ pour tout i, alors il y a un élément $h \in \langle g_1, g_2, \ldots, g_r\rangle \subset G$ avec $\mathrm{ord}(h) = \mathrm{ppcm}(n_1, n_2, \ldots, n_r)$.*

Définition. L'*exposant* d'un groupe fini G, noté $\exp(G)$, est le plus petit $n \geq 1$ tel qu'on ait $x^n = e$ (ou $nx = 0$) pour tout $x \in G$. L'exposant de G est égal au ppcm des ordres de tous les éléments de G.

Un groupe nonabélien fini ne contient pas toujours un élément g avec $\mathrm{ord}(g) = \exp(G)$. Par exemple, les membres de S_3 sont d'ordres 1, 2 et 3. Le ppcm de ces ordres est 6, mais S_3 ne contient pas d'élément d'ordre 6. Les membres de S_5 sont d'ordres 1, 2, 3, 4, 5 et 6. Le ppcm de ces ordres est 60, mais S_5 ne contient pas d'élément d'ordre 60.

Mais dans un groupe abélien fini, on déduit du corollaire 6.3 le résultat suivant.

Corollaire 6.4. *Si G est un groupe abélien fini, alors il existe $g \in G$ avec $\mathrm{ord}(g) = \exp(G)$.*

On voudrait démontrer prochainement que tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques. C'est à dire, pour tout groupe abélien G il existe des entiers $d_1, d_2, \ldots, d_r$ et un isomorphisme

$$(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \cong G$$

Pour construire ces isomorphismes par récurrence, on aura besoin du lemme suivant.

Lemme 6.5. *Soit $H_1 \subset G_1$ et $H \subset G$ des sous-groupes de groupes abéliens. Soit $\phi\colon G_1 \to G$ un morphisme de groupes avec $\phi(H_1) \subset H$. Si ϕ induit des isomorphismes $\phi|_{H_1}\colon H_1 \xrightarrow{\cong} H$ et $\overline{\phi}\colon G_1/H_1 \xrightarrow{\cong} G/H$, alors ϕ est un isomorphisme.*

Preuve. Exercice. □

Pour chaque choix d'éléments $g_1, g_2, \ldots, g_r$ d'un groupe abélien G avec $g_i^{d_i} = e$ pour $i = 1, \ldots, r$ on a un morphisme de groupes

$$\begin{aligned} (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) &\longrightarrow G, \\ (\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_r) &\longmapsto g_1^{a_1} g_2^{a_2} \cdots g_r^{a_r} \end{aligned} \tag{12}$$

Ce morphisme est bien défini parce que si on a $a_i, b_i \in \mathbb{Z}$ avec $\overline{a}_i = \overline{b}_i$ dans $\mathbb{Z}/d_i\mathbb{Z}$, alors il existe un entier k avec $a_i = b_i + d_i k$, et on a $g_i^{a_i} = g_i^{b_i}(g_i^{d_i})^k = g_i^{b_i} e^k = g_i^{b_i}$.

Inversement, étant donné un morphisme $\phi\colon (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \to G$, en posant $g_1 = \phi(\overline{1}, \overline{0}, \overline{0}, \ldots, \overline{0})$ et $g_2 = \phi(\overline{0}, \overline{1}, \overline{0}, \ldots, \overline{0})$, etc., on voit que ϕ est de la forme (12) pour un certain choix de $g_1, g_2, \ldots, g_r$.

Maintenant démontrons le théorème.

Théorème 6.6. *Tout groupe abélien fini est isomorphe à un produit direct de groupe cycliques.*

C'est à dire, pour tout groupe abélien fini G il existe un isomorphisme de la forme

$$(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \cong G.$$

Preuve. On va par récurrence sur $|G|$. Pour $|G| = 1$ le groupe $G = \{e\}$ est cyclique.

Donc supposons $|G| > 1$. Soit $d_1 = \exp(G)$ le ppcm des ordres des éléments de G. On a $d_1 > 1$ parce que G contient des éléments non neutres. Pour tout $h \in G$, $\mathrm{ord}(h)$ divise d_1.

Par le corollaire 6.4 il existe $g_1 \in G$ avec $\mathrm{ord}(g_1) = d_1$. Le groupe quotient $G/\langle g_1\rangle$ est abélien avec $|G/\langle g_1\rangle| = \dfrac{|G|}{d_1} < |G|$. Par récurrence $G/\langle g_1\rangle$ est isomorphe à un produit de

groupes cycliques. Soit $\psi\colon (\mathbb{Z}/d_2\mathbb{Z})\times(\mathbb{Z}/d_3\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z}) \xrightarrow{\cong} G/\langle g_1\rangle$ un tel isomorphisme. Par la discussion autour de (12) il existe $\overline{h}_2,\overline{h}_3,\dots,\overline{h}_r \in G/\langle g_1\rangle$ tel que ψ soit le morphisme de la forme (12) pour ce choix d'éléments. De plus, comme ψ est un isomorphisme, et par exemple $\overline{h}_2$ correspond à $(\overline{1},\overline{0},\overline{0},\dots,\overline{0})$ sous l'isomorphisme ψ, on voit qu'on a $\operatorname{ord}(\overline{h}_2)=d_2$. Similairement $\operatorname{ord}(\overline{h}_i)=d_i$ pour tout $i=2,3,\dots,r$. Or $\operatorname{ord}(\overline{h}_i)$ dans $G/\langle g_1\rangle$ divise $\operatorname{ord}(h_i)$ dans G (exercice), et l'ordre de tout élément de G divise d_1. Donc $d_2,\dots,d_r$ divisent d_1.

Pour construire un (iso)morphisme $\phi\colon (\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})\to G$ il faut choisir des éléments $g_1,g_2,\dots,g_r\in G$ comme dans (12). On a déjà choisi $g_1\in G$, et il vérifie $g_1^{d_1}=e$. On veut maintenant choisir $g_2,\dots,g_r\in G$ de telle façon que chacun de ces g_i vérifie deux conditions :

$$\text{(i) } \overline{g}_i=\overline{h}_i \text{ dans } G/\langle g_1\rangle, \qquad\qquad \text{(ii) } g_i^{d_i}=e \text{ dans } G.$$

On procède dans la façon suivante. Pour chaque i on a $\overline{h}_i^{d_i}=\overline{e}$ dans $G/\langle g_1\rangle$. Donc il existe un entier a_i tel que $h_i^{d_i}=g_1^{a_i}$. Or d_i divise d_1, et $\operatorname{ord}(h_i)$ divise d_1. Donc on a

$$e=h_i^{d_1}=(h_i^{d_i})^{\frac{d_1}{d_i}}=(g_1^{a_i})^{\frac{d_1}{d_i}}.$$

On a $\operatorname{ord}(g_1)=d_1$. Donc d_1 divise $a_i\frac{d_1}{d_i}$, et par conséquent $\frac{a_i}{d_i}=k_i$ est entier. Posons $g_i=h_ig_1^{-k_i}$. Alors on a bien $\overline{g}_i=\overline{h}_i$ dans $G/\langle g_1\rangle$. Et on a $g_i^{d_i}=h_i^{d_i}g_1^{-k_id_i}=h_i^{d_i}g_1^{-a_i}=e$ dans G. Donc les conditions (i) et (ii) ci-dessus sont remplies pour $i=2,\dots,r$.

Les éléments $g_1,g_2,\dots,g_r\in G$ vérifient maintenant $g_i^{d_i}=e$ pour tout i à cause de la condition (ii). Donc ils déterminent un morphisme $\phi\colon(\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})\to G$ par (12). On veut montrer que ϕ est un isomorphisme en se servant du lemme 6.5. Le groupe G du lemme est notre G, et son sous-groupe est $H=\langle g_1\rangle\subset G$. L'autre groupe du lemme est $G_1=(\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})$, et son sous-groupe est $H_1=(\mathbb{Z}/d_1\mathbb{Z})\times\{\overline{0}\}\times\cdots\times\{\overline{0}\}\subset G_1$ qu'on peut identifier à $\mathbb{Z}/d_1\mathbb{Z}$. Or H_1 est le noyau de la projection de G_1 sur le produit direct de ses $r-1$ derniers facteurs :

$$\begin{array}{ccc}(\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})\\ (\overline{a}_1,\overline{a}_2,\dots,\overline{a}_r) & \longmapsto & (\overline{a}_2,\dots,\overline{a}_r)\end{array}$$

Donc on peut identifier $G_1/H_1\cong(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})$. La restriction $\phi|_{H_1}\colon\mathbb{Z}/d_1\mathbb{Z}\to\langle g_1\rangle$ est le morphisme $\overline{i}\mapsto g_1^i$. Il est un isomorphisme par la proposition 5.5 parce que $\operatorname{ord}(g_1)=d_1$. Le morphisme $\overline{\phi}\colon G_1/H_1\to G/H$ est

$$\begin{array}{rcl}\overline{\phi}\colon(\mathbb{Z}/d_2\mathbb{Z})\times(\mathbb{Z}/d_3\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z}) & \longrightarrow & G/\langle g_1\rangle\\ (\overline{a}_2,\overline{a}_3,\dots,\overline{a}_r) & \longmapsto & \overline{g}_2^{a_2}\overline{g}_3^{a_3}\cdots\overline{g}_r^{a_r}=\overline{h}_2^{a_2}\overline{h}_3^{a_3}\cdots\overline{h}_r^{a_r}\end{array}$$

L'égalité est à cause de la condition (i) ci-dessus. On a $\overline{\phi}=\psi$. Mais ψ est un isomorphisme par hypothèse. Donc ϕ est aussi un isomorphisme par le lemme 6.5. □

La démonstration du théorème 6.6 donne un peu plus. On construit un isomorphisme

$$(\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/d_r\mathbb{Z})\cong G.$$

avec $d_2,\dots,d_r$ divisant d_1. La construction est récursive. Donc on peut imposer que $d_3,\dots,d_r$ divisent d_2, que $d_4,\dots,d_r$ divisent d_3, etc. Donc les d_i ont la propriété que d_{i+1} divise d_i pour tout i. On reverra ces nombres dans le théorème 8.3 sous le nom des *facteurs invariants* de G.

7. Le théorème chinois

Le théorème chinois classique est :

Théorème 7.1. *Soit m et n des entiers qui sont premiers entre eux. Alors l'application*

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \\ \overline{a} & \longmapsto & (\hat{a}, \tilde{a}) \end{array}$$

est un isomorphisme d'anneaux.

On démontrera une version de ce théorème où le rôle de $\mathbb{Z}$ est pris par un anneau commutatif quelconque. On a besoin d'un peu de notation.

Le *produit* de deux idéaux I et J d'un anneau commutatif A est

$$IJ = \left\{ \sum_s i_s j_s \mid i_s \in I, j_s \in J \text{ pour tout } s \right\}.$$

C'est encore un idéal de A et on $IJ \subset I \cap J$. Parfois cette inclusion est stricte, et parfois il y a égalité.

Pour $A = \mathbb{Z}$, $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$, on a $IJ = mn\mathbb{Z}$ et $I \cap J = \text{ppcm}(m, n)\mathbb{Z}$. Dans ce cas on a $IJ = I \cap J$ ssi m et n sont premiers entre eux.

Théorème 7.2 (Le théorème chinois)**.** *Soit A un anneau commutatif et I, J des idéaux de A avec $I + J = A$. (On dit que I et J sont* étrangers.*) Alors on a $IJ = I \cap J$, et l'application*

$$\begin{array}{ccc} \overline{\phi}\colon A/IJ & \longrightarrow & (A/I) \times (A/J) \\ \overline{a} & \longmapsto & (\hat{a}, \tilde{a}) \end{array} \tag{13}$$

est un isomorphisme d'anneaux.

Ici $\overline{a}$, $\hat{a}$ et $\tilde{a}$ sont les classes de $a \in A$ dans les anneaux quotients différents.

Pour $A = \mathbb{Z}$ la condition $I + J = A$ devient $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, qui équivaut à $\text{pgcd}(m, n) = 1$.

Preuve. L'application $\phi\colon A \to (A/I) \times (A/J)$ envoyant $a \mapsto (\hat{a}, \tilde{a})$ est toujours un morphisme d'anneaux. On a toujours $IJ \subset I \cap J = \ker \phi$. Donc ϕ passe au quotient par le théorème 4.15, et le morphisme $\overline{\phi}$ de (13) est bien défini.

Supposons maintenant qu'on a $I + J = A$, et montrons qu'on a $IJ = I \cap J$ et que ϕ est bijectif. La démonstration repose sur le fait qu'on a $1 \in A = I + J$ et qu'on peut donc écrire $1 = e + f$ avec $e \in I$ et $f \in J$.

Démontrons $IJ = I \cap J$. On a toujours $IJ \subset I \cap J$. Pour l'autre inclusion, soit $a \in I \cap J$. Alors on a $e, a \in I$ et $a, f \in J$. Donc on a $a = a1 = a(e + f) = ea + af \in IJ$. Donc on a bien $I \cap J \subset IJ$ et par conséquent $IJ = I \cap J$.

Cela donne $IJ = I \cap J = \ker \phi$, et donc $\overline{\phi}$ est injectif.

Pour la surjectivité, notez que de $e \in I$ on déduit $\hat{e} = \hat{0}$ et $\hat{f} = \hat{1} - \hat{e} = \hat{1} - \hat{0} = \hat{1}$. Similairement de $f \in J$ on déduit $\tilde{f} = \tilde{0}$ et $\tilde{e} = \tilde{1}$. Donc pour $(\hat{a}, \tilde{b}) \in (A/I) \times (A/J)$ on a

$$\widehat{af + be} = \hat{a}\hat{f} + \hat{b}\hat{e} = \hat{a}\hat{1} + \hat{b}\hat{0} = \hat{a},$$
$$\widetilde{af + be} = \tilde{a}\tilde{f} + \tilde{b}\tilde{e} = \tilde{a}\tilde{0} + \tilde{b}\tilde{1} = \tilde{b}.$$

Donc on a on a $\phi(af + be) = (\hat{a}, \tilde{b})$. Donc ϕ et $\overline{\phi}$ sont surjectifs. □

8. Les classes d'isomorphisme de groupes abéliens finis

Dans ce paragraphe on classifie les groupes abéliens finis à isomorphisme près. On dit que deux groupes abéliens finis sont "dans la même classe d'isomorphisme" s'ils sont isomorphes. Ces classes d'isomorphisme sont les classes déquivalence pour la relation d'équivalence $\cong$ d'isomorphisme de groupes abéliens finis. On donnera une liste complète les classes d'isomorphisme de groupes abéliens finis d'ordre N pour chaque entier N.

Diviseurs élémentaires. Selon le théorème 6.6 tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques

$$(\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z}). \tag{14}$$

Si on supprime tous les facteurs de la forme $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$, le nouveau groupe est isomorphe à l'ancien (par exemple $\mathbb{Z}/2\mathbb{Z} \times \{\overline{0}\} \cong \mathbb{Z}/2\mathbb{Z}$). Donc tout groupe abélien fini est isomorphe à groupe de la forme (14) avec tous les $d_i \geq 2$. La seule exception est le groupe $\{0\}$ d'ordre 1.

Chaque d_i a une factorisation $d_i = q_1^{a_1} q_2^{a_2} \cdots q_t^{a_t}$ avec les q_j des premiers distincts et tous les $a_j \geq 1$. Le théorème chinois nous donne un isomorphisme

$$\mathbb{Z}/d_i\mathbb{Z} \cong (\mathbb{Z}/q_1^{a_1}\mathbb{Z}) \times (\mathbb{Z}/q_2^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_t^{a_t}\mathbb{Z}).$$

Donc dans (14) quand on remplace $\mathbb{Z}/d_i\mathbb{Z}$ par $(\mathbb{Z}/q_1^{a_1}\mathbb{Z}) \times (\mathbb{Z}/q_2^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/q_t^{a_t}\mathbb{Z})$, le nouveau groupe est isomorphe à l'ancien. Si on fait cela pour tout i, on trouve la partie *Existence* du théorème suivant.

Théorème 8.1. *Tout groupe abélien fini G d'ordre ≥ 2 est isomorphe à un groupe de la forme $(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{r_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})$ avec les p_i des premiers et les $r_i \geq 1$. De plus $p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}$ sont uniquement déterminés par G à ordre près.*

Définition. Les $p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}$ du théorème s'appellent les *diviseurs élémentaires* de G.

La partie *Unicité* du théorème est une conséquence du lemme 8.10 ci-dessous, qui donne une formule pour le nombre de diviseurs élémentaires $p_i^{r_i}$ qui sont égaux à un p^k donné.

Le produit des diviseurs élémentaires est égal à l'ordre du groupe :

$$\prod_{i=1}^{s} p_i^{r_i} = |G|. \tag{15}$$

Il peut être utile de fixer un ordre pour les diviseurs élémentaires. Nous utiliserons l'ordre où les premiers p_i sont en ordre croissant, et les puissances d'un même premier sont groupées ensemble et apparaissent en ordre **décroissant**. Par exemple : $2^3, 2^2, 2, 3, 3, 5^3, 5^3, 5$. Noter qu'on peut bien avoir des répétitions parmi les diviseurs élémentaires.

Utilisons le théorème 8.1 pour voir lesquels des groupes suivants d'ordre 216 sont isomorphes :

$$\begin{aligned} G_1 &= \mathbb{Z}/216\mathbb{Z}, & G_4 &= \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/108\mathbb{Z}, \\ G_2 &= \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}, & G_5 &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}, \\ G_3 &= \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}, & G_6 &= \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}. \end{aligned} \tag{16}$$

Pour G_1 on factorise $216 = 2^3 3^3$. Donc les diviseurs élémentaires de G_1 sont $2^3, 3^3$.
Pour G_2 on factorise $6 = 2 \cdot 3$ et $36 = 2^2 3^2$. Les diviseurs élémentaires de G_2 sont $2^2, 2, 3^2, 3$.
Pour G_3 on factorise $12 = 2^2 3$ et $18 = 2 \cdot 3^2$. Les diviseurs élémentaires de G_3 sont $2^2, 2, 3^2, 3$.
Pour G_4 on factorise $2 = 2$ et $108 = 2^2 3^3$. Les diviseurs élémentaires de G_3 sont $2^2, 2, 3^3$.
Pour G_5 on factorise $4 = 2^2$ et $54 = 2 \cdot 3^3$. Les diviseurs élémentaires de G_3 sont $2^2, 2, 3^3$.

Pour G_6 on factorise $9 = 3^2$ et $24 = 2^3 3$. Les diviseurs élémentaires de G_3 sont $2^3, 3^2, 3$.

On voit qu'on a $G_2 \cong G_3$ car leurs diviseurs élémentaires sont les mêmes. On a aussi $G_4 \cong G_5$. Il n'y a pas d'autres isomorphismes parmi ces groupes.

Partitions. Le théorème 8.1 nous permet de classifier les classes d'isomorphisme de groupes abéliens finis de chaque ordre N.

Prenons d'abord le cas où $N = p^n$ avec p un premier et $n \geq 1$. Alors selon la formule (15) et nos conventions d'ordre, les diviseurs élémentaires d'un groupe d'ordre p^n sont $p^{r_1}, p^{r_2}, \ldots, p^{r_s}$

$$n = r_1 + r_2 + \cdots + r_s \qquad \text{et} \qquad r_1 \geq r_2 \geq \cdots \geq r_s > 0 \tag{17}$$

Définition. Une *partition de n* est une suite finie d'entiers $(r_1, r_2, \ldots, r_s)$ vérifiant (17).

Donc les suites différentes de diviseurs élémentaires de groupes abéliens d'ordre p^n sont en bijection avec les partitions de n.

Il y a une seule partition de 1, à savoir (1). Donc il y a un seul groupe abélien d'ordre p à isomorphisme près : $\mathbb{Z}/p\mathbb{Z}$.

Il y a deux partitions de 2, à savoir (2) et (1, 1). Donc il y a deux groupes abéliens d'ordre p^2 à isomorphisme près : $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Il y a trois partitions de 3, à savoir (3), (2, 1) et (1, 1, 1). Donc il y a trois classes d'isomorphisme de groupes abéliens d'ordre p^3 : $\mathbb{Z}/p^3\mathbb{Z}$ et $(\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ et $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Il y a cinq partitions de 4, à savoir (4), (3, 1), (2, 2), (2, 1, 1) et (1, 1, 1, 1). Donc il y a cinq classes d'isomorphisme de groupes abéliens d'ordre p^4.

On écrit

$$\pi(n) = \text{le nombre de partitions de } n.$$

Il y a exactement $\pi(n)$ classes d'isomorphisme de groupes abéliens d'ordre p^n. Les premières valeurs de la fonction $\pi(n)$ sont [6]

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

Un logiciel traitant les séries de puissances calcule ces nombres facilement en utilisant la célèbre formule pour la série génératrice de $\pi(n)$:

$$\sum_{n \geq 0} \pi(n) T^n = \prod_{i \geq 1} \frac{1}{1 - T^i} \cdot \tag{18}$$

Maintenant classifions les classes d'isomorphisme de groupes abéliens d'ordre $N \geq 2$ en général. On peut écrire $N = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ avec les p_i des premiers avec $p_1 < p_2 < \cdots < p_t$ et les $n_i \geq 1$. Alors pour donner une suite de diviseurs élémentaires de groupes abéliens d'ordre N il faut donner une partition de chaque exposante n_i pour $i = 1, \ldots, t$. Plus précisément :

Théorème 8.2. *Soit $N = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ avec les p_i des premiers avec $p_1 < p_2 < \cdots < p_t$ et les $n_i \geq 1$. Alors diviseurs élémentaires de groupes abéliens d'ordre N sont les suites*

$$p_1^{r_{11}}, p_1^{r_{12}}, \ldots, p_1^{r_{1s_1}}, p_2^{r_{21}}, p_2^{r_{22}}, \ldots, p_2^{r_{2s_2}}, \ldots, p_t^{r_{t1}}, p_t^{r_{t2}}, \ldots, p_t^{r_{ts_t}}, \tag{19}$$

où pour chaque $i = 1, \ldots, t$ la suite $(r_{i1}, r_{i2}, \ldots, r_{is_i})$ est une partition de n_i.

Par conséquent il y a exactement $\prod_{i=1}^{t} \pi(n_i)$ classes d'isomorphisme de groupes abéliens d'ordre N.

6. Il y a une et une seule partition de 0, à savoir (). La somme de zéro nombres vaut 0.

Autrement dit, les classes d'isomorphisme de groupes abélien d'ordre $N = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ sont en bijection avec les uplets $\underline{\mathbf{\Pi}} = (\Pi_1, \Pi_2, \ldots, \Pi_t)$ avec chaque $\Pi_i = (r_{i1}, r_{i2}, \ldots, r_{is_i})$ une partition de n_i. Les diviseurs élémentaires correspondant à $\underline{\mathbf{\Pi}}$ sont ceux de (19).

Par exemple en factorisant $216 = 2^3 3^3$ on voit qu'il y a $\pi(3)\pi(3) = 3 \cdot 3 = 9$ classes d'isomorphisme de groupes abéliens d'ordre 216 correspondant aux diviseurs élémentaires suivants

$$\begin{array}{lll} 2^3, 3^3 & 2^3, 3^2, 3 & 2^3, 3, 3, 3 \\ 2^2, 2, 3^3 & 2^2, 2, 3^2, 3 & 2^2, 2, 3, 3, 3 \\ 2, 2, 2, 3^3 & 2, 2, 2, 3^2, 3 & 2, 2, 2, 3, 3, 3 \end{array} \tag{20}$$

Facteurs invariants. Les diviseurs élémentaires ne sont pas toujours les invariants les plus commodes d'une classe d'isomorphisme de groupes abéliens finis. Par exemple, que G est cyclique d'ordre 60 se voit plus aisément de l'isomorphisme $G \cong \mathbb{Z}/60\mathbb{Z}$ que de l'isomorphisme $G \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ associé aux diviseurs élémentaires. Heureusement il y a une deuxième façon de classifier les classes d'isomorphisme de groupes abéliens finis.

Théorème 8.3. *Soit G un groupe abélien fini d'ordre ≥ 2. Alors il existe une suite unique d'entiers naturels $e_1, e_2, \ldots, e_m$ avec (i) tous les $e_i \geq 2$ et (ii) e_i divisant e_{i+1} pour $i = 1, \ldots, m-1$ tel qu'il y ait un isomorphisme $G \cong (\mathbb{Z}/e_1\mathbb{Z}) \times (\mathbb{Z}/e_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_m\mathbb{Z})$.*

Définition. Les $e_1, e_2, \ldots, e_m$ du théorème s'appellent les *facteurs invariants* de G.

Pour calculer les facteurs invariants associés aux diviseurs élémentaires $2^3, 2^2, 3, 5^3, 5^3, 5$ on fait un petit tableau.

2^3	2^2	
3		
5^3	5^3	5
3000	500	5

Les trois premières lignes correspondent aux premiers 2, 3 et 5. Dans les cases de chaque ligne on écrit les diviseurs élémentaires qui sont les puissances du premier de la ligne en ordre **décroissant**. Dans la dernière ligne on écrit les produits des nombres dans chaque colonne. Les facteurs invariants sont ces produits arrangés dans l'ordre inverse : 5, 500, 3000. Notez que chaque facteur invariant non dernier divise le suivant.

Dans le cas général de (19) on fait un tableau avec une ligne pour chacun des premiers $p_1, p_2, \ldots, p_t$ plus une dernière ligne. Dans la ligne attribuée à p_i on écrit les diviseurs élémentaires qui sont des puissances de p_i en ordre **décroissant**. Pour (19) c'est $p_i^{r_{i1}}, p_i^{r_{i2}}, \ldots, p_i^{r_{is_i}}$. Puis on écrit dans la dernière ligne les produits des nombres dans chaque colonne. Les nombres dans la dernière ligne sont les facteurs invariants arrangés dans l'ordre inverse.

Les tableaux suivants correspondent aux diviseurs élémentaires dans la deuxième ligne de (20) :

2^2	2
3^3	
108	2

2^2	2
3^2	3
36	6

2^2	2	
3	3	3
12	6	3

Les facteurs invariants correspondant aux trois systèmes de diviseurs élémentaires sont $2, 108$ puis $6, 36$ et ensuite $3, 6, 12$. Notez que chaque facteur invariant non dernier divise le suivant.

Remarque 8.4. (a) On a $|G| = e_1 e_2 \cdots e_m$.

(b) G est cyclique d'ordre n ssi G a un seul facteur invariant n.

(c) Le plus grand facteur invariant e_m est égal à $\exp(G)$, l'exposant de G, le plus petit $n \geq 1$ avec $x^n = e$ (ou $nx = 0$) pour tout $x \in G$ (voir la définition avant le corollaire 6.4).

Théorème 8.5. *Soit G un groupe abélien fini avec la propriété que pour tout $d \geq 1$ il existe au plus d éléments $x \in G$ avec $x^d = e$. Alors G est cyclique.*

Preuve. Soit $e_1, e_2, \ldots, e_m$ les facteurs invariants de G. Par la remarque 8.4 G contient $|G| = e_1 e_2 \cdots e_m$ éléments vérifiant $x^{e_m} = 1$. Par l'hypothèse du théorème on doit alors avoir $e_1 e_2 \cdots e_m \leq e_m$. Mais comme tous les e_i sont ≥ 2, on ne peut avoir qu'un seul facteur invariant e_1, et $G \cong \mathbb{Z}/e_1\mathbb{Z}$ est cyclique. □

Corollaire 8.6. *Soit K un corps commutatif, et $G \subset K^\times$ un sous-groupe fini du groupe multiplicatif de K. Alors G est cyclique.*

En particulier si $\mathbb{F}_q$ est un corps fini avec q éléments, alors $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$.

Preuve. Comme conséquence de la factorisation unique dans $K[T]$, on sait que pour tout $d \geq 1$ le polynôme $T^d - 1 \in K[T]$ a au plus d racines dans K. Donc $G \subset K^\times$ contient au plus d éléments x avec $x^d = 1$. □

Les éléments de m-torsion. Pour $(G, +, 0)$ un groupe abélien fini et $m \geq 1$ un entier soit

$$\mathrm{Tors}_m(G) = \{x \in G \mid mx = 0\} \subset G.$$

C'est le sous-groupe des *éléments de m-torsion* de G. Les éléments de m-torsion sont ceux dont l'ordre divise m. On notera leur cardinal

$$\mathrm{tors}(m, G) = \mathrm{card}\{x \in G \mid mx = 0\}.$$

Ces nombres $\mathrm{tors}(m, G)$ ont les propriétés suivantes.

Lemme 8.7. *(a) Si G et H sont isomorphes, alors $\mathrm{tors}(m, G) = \mathrm{tors}(m, H)$ pour tout m.*
(b) On a $\mathrm{tors}(m, G \times H) = \mathrm{tors}(m, G)\,\mathrm{tors}(m, H)$ pour tout m.
(c) Si on a $\mathrm{pgcd}(m, |G|) = 1$, alors $\mathrm{tors}(m, G) = 1$.
(d) Pour p premier et k et r des entiers ≥ 1 on a

$$\mathrm{tors}(p^k, \mathbb{Z}/p^r\mathbb{Z}) = p^{\min(r,k)}. \tag{21}$$

Preuve. (a) Un isomorphisme $G \xrightarrow{\cong} H$ induit une bijection entre $\{x \in G \mid mx = 0\}$ et $\{y \in H \mid my = 0\}$.

(b) On a une égalité d'ensembles

$$\{(x, y) \in G \times H \mid m(x, y) = 0\} = \{x \in G \mid mx = 0\} \times \{y \in H \mid my = 0\}.$$

(c) Supposons qu'on a $\mathrm{pgcd}(m, |G|) = 1$. Si on a $x \in G$ avec $mx = 0$, alors $\mathrm{ord}(x)$ divise m et $|G|$, et donc $\mathrm{ord}(x)$ divise $\mathrm{pgcd}(m, |G|) = 1$. On en déduit qu'on a $x = 0$. Donc on a $\mathrm{tors}(m, G) = \mathrm{card}\{x \in G \mid mx = 0\} = \mathrm{card}\{0\} = 1$.

(d) On a

$$\mathrm{tors}(p^k, \mathbb{Z}/p^r\mathbb{Z}) = \mathrm{card}\{\overline{x} \in \mathbb{Z}/p^r\mathbb{Z} \mid p^k\overline{x} = \overline{0}\} = \left\{ \begin{array}{rll} |p^{r-k}\mathbb{Z}/p^r\mathbb{Z}| & = p^k & \text{si } k < r \\ |\mathbb{Z}/p^r\mathbb{Z}| & = p^r & \text{si } k \geq r \end{array} \right\} = p^{\min(r,k)}.$$

Cela donne la formule (21). □

On peut utiliser le lemme 8.7 pour compter le nombre d'éléments d'ordre p^s dans un groupe abélien fini.

Proposition 8.8. *Soit p un premier et $r_1 \geq r_2 \geq \cdots \geq r_s > 0$ des entiers. Alors le nombre d'éléments d'ordre p^s dans $H = (\mathbb{Z}/p^{r_1}\mathbb{Z}) \times (\mathbb{Z}/p^{r_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{r_s}\mathbb{Z})$ est*

$$\operatorname{tors}(p^s, H) - \operatorname{tors}(p^{s-1}, H) = p^{\sum_{i=1}^s \min(r_i, s)} - p^{\sum_{i=1}^s \min(r_i, s-1)}$$

Preuve. Pour un $x \in H$ on a $\operatorname{ord}(x) = p^s$ ssi on a $p^s \cdot x = 0$ mais $p^{s-1} \cdot x \neq 0$. Donc le nombre d'élément d'ordre p^s dans H est bien $\operatorname{tors}(p^s, H) - \operatorname{tors}(p^{s-1}, H)$. Les formules du lemme 8.7 donnent

$$\operatorname{tors}(p^k, H) = \prod_{i=1}^s \operatorname{tors}(p^k, \mathbb{Z}/p^{r_i}\mathbb{Z}) = \prod_{i=1}^s p^{\min(r_i, k)} = p^{\sum_{i=1}^s \min(r_i, k)}. \qquad \square$$

Pour $H_1 = (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ on a

p^s	1	2	4	8
$\operatorname{tors}(p^s, H_1)$	1	2^4	2^7	2^8
nb. d'éléments d'ordre p^s	1	$2^4 - 1 = 15$	$2^7 - 2^4 = 112$	$2^8 - 2^7 = 128$

Pour $H_2 = (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ on a

p^s	1	2	4	8	16
$\operatorname{tors}(p^s, H_2)$	1	2^3	2^6	2^7	2^8
nb. d'éléments d'ordre p^s	1	$2^3 - 1 = 7$	$2^6 - 2^3 = 56$	$2^7 - 2^6 = 64$	$2^8 - 2^7 = 128$

Les deux lemmes suivants donnent une formule pour le nombre de diviseurs élémentaires $p_i^{r_i}$ d'un groupe abélien fini G qui sont égaux à un p^k donné. Ils complètent la démonstration du théorème 8.1 en montrant que la liste des diviseurs élémentaires est uniquement déterminée par G à ordre près.

Lemme 8.9. *Pour p premier et k et r des entiers ≥ 1 on a*

$$\frac{\operatorname{tors}(p^k, \mathbb{Z}/p^r\mathbb{Z})^2}{\operatorname{tors}(p^{k-1}, \mathbb{Z}/p^r\mathbb{Z})\ \operatorname{tors}(p^{k+1}, \mathbb{Z}/p^r\mathbb{Z})} = \begin{cases} p & \text{si } k = r, \\ 1 & \text{si } k \neq r. \end{cases} \tag{22}$$

Preuve. Si on a $k < r$, alors $k-1, k, k+1$ sont tous $\leq r$. Si on a $k > r$, alors $k-1, k, k+1$ sont tous $\geq r$. En appliquant la formule (21), on trouve

$$\frac{\operatorname{tors}(p^k, \mathbb{Z}/p^r\mathbb{Z})^2}{\operatorname{tors}(p^{k-1}, \mathbb{Z}/p^r\mathbb{Z})\ \operatorname{tors}(p^{k+1}, \mathbb{Z}/p^r\mathbb{Z})} = \begin{cases} \dfrac{(p^k)^2}{p^{k-1}p^{k+1}} = 1 & \text{si } k < r, \\ \dfrac{(p^r)^2}{p^{r-1}p^r} = p & \text{si } k = r, \\ \dfrac{(p^r)^2}{p^r p^r} = 1 & \text{si } k > r. \end{cases}$$

Cela donne la formule (22). $\square$

Lemme 8.10. *Soit $p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}$ une suite finie de puissances de premiers, et soit $H = (\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{r_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})$. Soit G un groupe isomorphe à H. Alors pour toute puissance de premier p^k on a*

$$\operatorname{card}\{i \in \{1, 2, \ldots, s\} \mid p_i^{r_i} = p^k\} = \log_p \frac{\operatorname{tors}(p^k, G)^2}{\operatorname{tors}(p^{k-1}, G)\ \operatorname{tors}(p^{k+1}, G)}.$$

Ici $\log_p$ est le logarithme de base p. On a $\log_p x = t$ ssi on a $x = p^t$.

Preuve. Le lemme 8.7(c) et le lemme 8.9 montrent qu'on a

$$\frac{\mathrm{tors}(p^k, \mathbb{Z}/p_i^{r_i}\mathbb{Z})^2}{\mathrm{tors}(p^{k-1}, \mathbb{Z}/p_i^{r_i}\mathbb{Z})\ \mathrm{tors}(p^{k+1}, \mathbb{Z}/p_i^{r_i}\mathbb{Z})} = \begin{cases} 1 & \text{si } p^k \neq p_i^{r_i}, \\ p & \text{si } p^k = p_i^{r_i}. \end{cases}$$

(Le cas $p \neq p_i$ vient du lemme 8.7, et le cas $p = p_i$ vient du lemme 8.9.) Les parties (a)(b) du lemme 8.7 montrent alors

$$\begin{aligned} \frac{\mathrm{tors}(p^k, G)^2}{\mathrm{tors}(p^{k-1}, G)\ \mathrm{tors}(p^{k+1}, G)} &= \frac{\mathrm{tors}(p^k, H)^2}{\mathrm{tors}(p^{k-1}, H)\ \mathrm{tors}(p^{k+1}, H)} \\ &= \prod_{i=1}^{s} \frac{\mathrm{tors}(p^k, \mathbb{Z}/p_i^{r_i}\mathbb{Z})^2}{\mathrm{tors}(p^{k-1}, \mathbb{Z}/p_i^{r_i}\mathbb{Z})\ \mathrm{tors}(p^{k+1}, \mathbb{Z}/p_i^{r_i}\mathbb{Z})} = \prod_{\substack{i \text{ t.q.} \\ p_i^{r_i} = p^k}} p \times \prod_{\substack{i \text{ t.q.} \\ p_i^{r_i} \neq p^k}} 1 = p^{\mathrm{card}\{i | p_i^{r_i} = p^k\}}. \end{aligned}$$

En appliquant $\log_p$, on trouve la formule du lemme. □