

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 $*$: $G \times G \rightarrow G$, $(a, b) \mapsto a * b$ 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 $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$. \square

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

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 $*$: $H \times H \rightarrow H$, $(a, b) \mapsto a * b$. 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 $*$: $H \times H \rightarrow H$ 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 $\bigcap_{i \in I} H_i$ 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 $e \in \bigcap_{i \in I} H_i$. Soient $a, b \in \bigcap_{i \in I} H_i$. Pour tout $i \in I$ on a $a + b \in H_i$, car H_i est un sous-groupe, donc $a + b \in \bigcap_{i \in I} H_i$. Soit $a \in \bigcap_{i \in I} H_i$. Pour tout $i \in I$ on a $a^{-1} \in H_i$, donc $a^{-1} \in \bigcap_{i \in I} H_i$. □

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

$$\begin{aligned} ((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) &= (a_1 * a_2, b_1 * b_2) * (a_3, b_3) = ((a_1 * a_2) * a_3, (b_1 * b_2) * b_3) = \\ &= (a_1 * (a_2 * a_3), b_1 * (b_2 * b_3)) = (a_1, b_1) * (a_2 * a_3, b_2 * b_3) = (a_1 * b_1) * ((a_2, b_2) * (a_3, b_3)). \end{aligned}$$

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 $f : G \rightarrow H$ est un *homomorphisme* si $f(a * b) = f(a) * f(b)$ pour tous $a, b \in G$.

Lemme 1.6. Soit $f : G \rightarrow H$ 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

$$\begin{aligned} e_H &= f(e_G) * f(e_G)^{-1} = (f(e_G) * f(e_G)) * f(e_G)^{-1} = \\ &= f(e_G) * (f(e_G) * f(e_G)^{-1}) = f(e_G) * e_H = f(e_G). \end{aligned}$$

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

Lemme 1.7. Si $f : G \rightarrow H$ est un isomorphisme, alors la réciproque $f^{-1} : H \rightarrow G$ 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 $f : G \rightarrow H$ un homomorphisme. L'image de f , notée $\text{Im}(f)$, est $f(G) = \{f(a) \mid a \in G\} \subset H$.

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

- (1) $\text{Im}(f)$ est un sous-groupe de H .
(2) f est surjectif si et seulement si $\text{Im}(f) = H$.

Démonstration. La seconde partie du lemme est évidente. On démontre la première partie. $e_H = f(e_G)$, donc $e_H \in \text{Im}(f)$. Soient $b_1, b_2 \in \text{Im}(f)$. 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 $b_1 * b_2 \in \text{Im}(f)$. Soit $b \in \text{Im}(f)$. On prend $a \in G$ tel que $b = f(a)$. Alors

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

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

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

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

- (1) $\text{Ker}(f)$ est un sous-groupe de G .
(2) f est injectif si et seulement si $\text{Ker}(f) = \{e_G\}$.

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

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

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

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

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

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

Supposons que $\text{Ker}(f) = \{e_G\}$. 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 $a_1 * a_2^{-1} \in \text{Ker}(f)$, 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'autres 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 $\varphi_a : \mathbb{Z} \rightarrow G, n \mapsto a^n$. Il est clair que $H = \text{Im}(\varphi_a)$, 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 $H = \langle a \rangle$. \square

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

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

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 $(a + c) \equiv (b + d) \pmod{H}$. \square

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 $(G/H) \times (G/H) \rightarrow (G/H)$, $(\alpha, \beta) \mapsto \alpha + \beta$ 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

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

\square

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, $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \dots, [m - 1]\}$.

Démonstration. Montrons d'abord que $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$. 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 $[a] = [r] \in \{[0], [1], \dots, [m-1]\}$.

Maintenant on montre que les éléments de $\{[0], [1], \dots, [m-1]\}$ sont deux à deux distincts. Soient $a, b \in \{0, 1, \dots, m-1\}$. 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 $\{0, 1, \dots, m-1\}$ divisible par m est 0, donc $b - a = 0$, c'est-à-dire $a = b$.

Il est évident que l'on a $n[a] = [na]$ 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 $\pi : G \rightarrow (G/H), a \mapsto [a]$, 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,

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

□

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

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

$$\begin{array}{ccc} G & & \\ \pi \downarrow & \searrow f & \\ G/H & \xrightarrow{g} & G' \end{array}$$

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 $a' - a \in \text{Ker}(f)$, 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 $g' : G/H \rightarrow G'$ un (autre) homomorphisme tel que $g' \circ \pi = f$. On a $g \circ \pi = g' \circ \pi$ et π est surjectif, donc $g = g'$. \square

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

$$\begin{array}{ccc} G & & \\ \pi \downarrow & \searrow f & \\ G/\text{Ker}(f) & \xrightarrow{g} & G' \end{array}$$

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

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, \dots, x_n . Soit $\varphi : \mathbb{Z}^n \rightarrow G$ l'application définie par

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

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

$$\begin{aligned} \varphi(\lambda_1, \dots, \lambda_n) + \varphi(\mu_1, \dots, \mu_n) &= (\lambda_1 x_1 + \dots + \lambda_n x_n) + (\mu_1 x_1 + \dots + \mu_n x_n) = \\ &= (\lambda_1 + \mu_1)x_1 + \dots + (\lambda_n + \mu_n)x_n = \varphi(\lambda_1 + \mu_1, \dots, \lambda_n + \mu_n) = \\ &= \varphi((\lambda_1, \dots, \lambda_n) + (\mu_1, \dots, \mu_n)), \end{aligned}$$

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

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

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

donc $G = \text{Im}(\varphi) \subset H$, donc $G = H$. Ceci montre que x_1, \dots, x_n engendrent G . \square

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 $f : \mathbb{Z}^n \rightarrow G$. Posons $H = \text{Ker}(f)$. Alors, par la proposition 1.17, $G \simeq \mathbb{Z}^n/H$. \square

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

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 $\varphi : \mathbb{Z} \rightarrow G$, $n \mapsto a^n$. Par la proposition 1.3 soit $\text{Ker}(\varphi) = \{0\}$, soit il existe $n \in \mathbb{N}^*$ tel que $\text{Ker}(\varphi) = n\mathbb{Z}$. Si $\text{Ker}(\varphi) = \{0\}$, alors $\varphi : \mathbb{Z} \rightarrow G$ est un isomorphisme. Supposons que $\text{Ker}(\varphi) = n\mathbb{Z}$. 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. \square

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

Démonstration. Posons $d = \text{pgcd}(a,n)$, $a = da_1$ et $n = dn_1$. On veut montrer que $[a]$ est d'ordre n_1 . D'abord, $n_1 [a] = [n_1 da_1] = a_1 [n] = a_1 [0] = 0$. 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 $n_1 [a] = 0$. \square

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 $\varphi : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ 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 $\phi : \mathbb{Q}^n \rightarrow \mathbb{Q}^m$ 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 $v \in \text{Ker}(\phi)$. On écrit $v = \lambda_1 e_1 + \dots + \lambda_n e_n$ 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 $\mu v \in \mathbb{Z}^n \cap \text{Ker}(\phi) = \text{ker}(\varphi) = \{0\}$, 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 $n = m$. \square

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 évidemment $G \simeq \mathbb{Z}$.

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

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

Remarquer que $\text{Ker}(\pi) \simeq \mathbb{Z}^{n-1}$. Si $G \subset \text{Ker}(\pi)$ alors, par hypothèse de récurrence, il existe $r \leq n - 1$ tel que $G \simeq \mathbb{Z}^r$. On peut donc supposer que $G \not\subset \text{Ker}(\pi)$. 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 $G' = G \cap \text{Ker}(\pi)$. 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 $\varphi' : \mathbb{Z}^r \rightarrow G'$. On définit $\varphi : \mathbb{Z}^{r+1} = \mathbb{Z}^r \times \mathbb{Z} \rightarrow G$ 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 $(u, x) \in \text{Ker}(\varphi)$. On a

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

donc $x = 0$ et $u \in \text{Ker}(\varphi')$. Comme φ' est injectif, on a alors $u = 0$. Ceci montre que $\text{Ker}(\varphi) = \{(0, 0)\}$, 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 $y' \in \text{Ker}(\pi) \cap G = G'$. 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. \square

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

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

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 $\varphi : \mathbb{Z}^m \rightarrow G$, $(\mu_1, \dots, \mu_m) \mapsto \mu_1 y_1 + \dots + \mu_m y_m$. 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 $\lambda_1 \hat{x}_1 + \dots + \lambda_n \hat{x}_n = 0$, alors

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

donc $\lambda_1 = \dots = \lambda_n = 0$. 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 $ty_j \in H$ 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 $\lambda_{1,j} x_1 + \dots + \lambda_{n,j} x_n + \mu_j y_j = 0$. On a $\mu_j \neq 0$ sinon on aurait $\lambda_{1,j} x_1 + \dots + \lambda_{n,j} x_n = 0$ et $\lambda_{1,j}, \dots, \lambda_{n,j}$ seraient non tous nuls. On pose $t = \mu_1 \mu_2 \dots \mu_m$. Alors $t \neq 0$ et $ty_j \in H$ 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 $\{y_1, \dots, y_m\}$ engendrent G , il existe $\mu_1, \dots, \mu_m \in \mathbb{Z}$ tel que $z = \mu_1 y_1 + \dots + \mu_m y_m$ (cela provient de la surjectivité de $\varphi : \mathbb{Z}^m \rightarrow G$). Alors $tz = \mu_1 (ty_1) + \dots + \mu_m (ty_m) \in H$ car $ty_1, \dots, ty_m \in H$. Ceci montre que $tG \subset H$.

Soit $\kappa : G \rightarrow tG$, $z \mapsto tz$. Il est évident que κ est un homomorphisme et qu'il est surjectif. Si $z \in \text{Ker}(\kappa)$, alors $tz = 0$, donc $z = 0$ car G est sans torsion. Donc $\text{Ker}(\kappa) = \{0\}$ 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 $r = n$. \square

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 $nm(a + b) = m(na) + n(mb) = m0 + n0 = 0$. Soit $a \in G_T$. Il existe $n \in \mathbb{N}^*$ tel que $na = 0$. Alors $n(-a) = -(na) = -0 = 0$. \square

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

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

$$\begin{aligned} \varphi : \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_m\mathbb{Z} &\rightarrow G \\ ([t_1], \dots, [t_m]) &\mapsto t_1y_1 + \dots + t_my_m \end{aligned}$$

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

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 $\pi : G \rightarrow G/G_T = H$ la projection canonique. Si $\{y_1, \dots, y_m\}$ engendrent G , alors $\{\pi(y_1), \dots, \pi(y_m)\}$ engendrent $G/G_T = H$, 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 $\{\beta_1, \dots, \beta_n\}$ dans H qui engendrent H . Pour tout $i \in \{1, \dots, n\}$ on choisit $b_i \in G$ tel que $\pi(b_i) = \beta_i$. On définit $f : G_T \times \mathbb{Z}^n \rightarrow G$ par

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

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

$$\begin{aligned} 0 = \pi(0) &= \pi(f(a, \lambda_1, \dots, \lambda_n)) = \pi(a + \lambda_1 b_1 + \dots + \lambda_n b_n) = \\ &= \pi(a) + \lambda_1 \pi(b_1) + \dots + \lambda_n \pi(b_n) = \lambda_1 \beta_1 + \dots + \lambda_n \beta_n. \end{aligned}$$

Cette dernière égalité implique que $\lambda_1 = \dots = \lambda_n = 0$ car $\{\beta_1, \dots, \beta_n\}$ est une famille libre. Finalement, on a aussi $a = f(a, 0, \dots, 0) = 0$. Donc $\text{Ker}(f) = \{(0, 0, \dots, 0)\}$, donc f est injectif. Montrons que f est surjectif. Soit $c \in G$. Posons $\gamma = \pi(c)$. Il existe $\lambda_1, \dots, \lambda_n \in \mathbb{Z}$ tels que $\gamma = \lambda_1\beta_1 + \dots + \lambda_n\beta_n$. Posons $a = c - \lambda_1b_1 - \dots - \lambda_nb_n$. On a

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

donc $a \in G_T$. D'où $c = a + \lambda_1b_1 + \dots + \lambda_nb_n = f(a, \lambda_1, \dots, \lambda_n)$. 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. \square

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 et se note $n = \text{rg}(G)$.

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 $|G|$. \square

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 $-a \in G_p$. \square

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 . \square

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 $0 = [qb] = q[b] = q\beta$, donc p divise q et $\frac{q}{p}b$ est d'ordre p . \square

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 . \square

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

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

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

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

Soit $(a_1, \dots, a_\ell) \in \text{Ker}(\varphi)$. Pour tout $i \in \{1, \dots, \ell\}$ 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 $i \in \{1, \dots, \ell\}$. Remarquer que $\hat{m}_i a_j = 0$ pour tout $j \neq i$ donc

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

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

$$a_i = (xm_i + y\hat{m}_i)a_i = x(m_i a_i) + y(\hat{m}_i a_i) = x0 + y0 = 0.$$

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

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

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

Ceci montre que φ est surjectif. \square

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 $i \in \{1, \dots, \ell\}$.

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 $i \in \{1, \dots, \ell\}$. \square

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

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

Démonstration. Posons $m = u_1 u_2 \cdots u_\ell$. Soit $\pi_i : \mathbb{Z}/m \mathbb{Z} \rightarrow \mathbb{Z}/u_i \mathbb{Z}$ 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 $\pi : \mathbb{Z}/m \mathbb{Z} \rightarrow \prod_{i=1}^{\ell} \mathbb{Z}/u_i \mathbb{Z}$ l'homomorphisme défini par

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

Il est clair que π est un homomorphisme. Soit $\alpha = [a]_m \in \text{Ker}(\pi)$. On a $\pi_i(\alpha) = [a]_{u_i} = 0$, donc u_i divise a pour tout $i \in \{1, \dots, \ell\}$. Comme u_1, u_2, \dots, u_ℓ sont deux à deux premiers entre eux, il s'en suit que $m = u_1 u_2 \cdots u_\ell$ 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. \square

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 $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ 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 . \square

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

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 $m = km_1$ 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 $[k_1t] = k_1\beta = k_1\varphi(k'x) = \varphi(kx) = \varphi(0) = 0$, donc $m = k_1k'm_1$ divise k_1t , 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 $\psi : G \rightarrow \mathbb{Z}/m\mathbb{Z}$ 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

$$\begin{aligned} \varphi(b) + \lambda\beta_1 - \varphi(b') - \lambda'\beta_1 &= \varphi(b - b') - (\lambda' - \lambda)\beta_1 = \varphi(\mu k'x) - (\lambda' - \lambda)\beta_1 = \\ &= \mu\varphi(k'x) - (\lambda' - \lambda)\beta_1 = \mu\beta - (\lambda' - \lambda)\beta_1 = \mu k'\beta_1 - (\lambda' - \lambda)\beta_1 = 0. \end{aligned}$$

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, \dots, x_ℓ . Notons H_i le sous-groupe de G engendré par H et x_1, \dots, x_i . Ce qui précède montre par récurrence sur i qu'il existe un homomorphisme $\psi_i : H_i \rightarrow \mathbb{Z}/m\mathbb{Z}$ tel que $\psi_i|_H = \varphi : H \rightarrow \mathbb{Z}/m\mathbb{Z}$. On obtient alors le lemme avec $i = \ell$. \square

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 $\varphi : H \rightarrow \mathbb{Z}/p^u\mathbb{Z}$ 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 $\psi : G \rightarrow \mathbb{Z}/p^u\mathbb{Z}$ tel que $\psi|_H = \varphi$.

Posons $G_1 = \text{Ker}(\psi)$. Soit $f : G_1 \times \mathbb{Z}/p^u\mathbb{Z} \rightarrow G$ 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 $(a, [\lambda]) \in \text{Ker}(f)$. 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 $a \in \text{Ker}(\psi) = G_1$ et $b = a + \lambda x = f(a, [\lambda])$. Ceci montre que f est surjective.

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

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, \dots, m_{ℓ} telle que $m_1 \geq 2$, m_i divise m_{i+1} pour tout $i \in \{1, \dots, \ell-1\}$ et G est isomorphe à $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_{\ell}\mathbb{Z}$.*

Définition. Soit G un groupe abélien fini. La décomposition $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_{\ell}\mathbb{Z}$ 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 $\{1, \dots, n\}$. 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 $f : E \rightarrow [n]$ une bijection. Soit $\varphi : \mathfrak{S}(E) \rightarrow \mathfrak{S}_n$ 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 $\psi : \mathfrak{S}_n \rightarrow \mathfrak{S}(E)$ 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 $\varphi \circ \psi = \text{id}_{\mathfrak{S}_n}$ et $\psi \circ \varphi = \text{id}_{\mathfrak{S}(E)}$. On en conclue que φ est un isomorphisme. \square

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

$$\left(\begin{array}{ccc} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{array} \right).$$

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

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

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

Exemples.

$$\left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{array} \right)$$

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

$$\left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{array} \right)$$

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 $\mathfrak{S}_1 = \{\text{id}\}$ et $\text{card}(\mathfrak{S}_1) = 1 = 1!$. 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, $\text{card}(H) = (n-1)!$. Soit $F : [n] \times H \rightarrow \mathfrak{S}_n$ 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 $G : \mathfrak{S}_n \rightarrow [n] \times H$ 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 $G \circ F = \text{id}_{[n] \times H}$ et $F \circ G = \text{id}_{\mathfrak{S}_n}$, donc F est une bijection, donc $\text{card}(\mathfrak{S}_n) = \text{card}([n] \times H) = n \times (n-1)! = n!$. \square

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

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 $(t_1, t_2, \dots, t_\ell)$ est $\{t_1, t_2, \dots, t_\ell\}$.

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

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

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

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 $\ell = \text{card}(\mathcal{O}[t])$. Alors $\sigma^\ell(t) = t$ et $\mathcal{O}[t] = \{t, \sigma(t), \dots, \sigma^{\ell-1}(t)\}$.

Démonstration de l'assertion 2. Comme $\mathcal{O}[t]$ est fini, il existe $\ell > 0$ tel que $\sigma^\ell(t) \in \{t, \sigma(t), \dots, \sigma^{\ell-1}(t)\}$. On prend le plus petit ℓ vérifiant cette propriété. Soit $k \in \{0, 1, \dots, \ell - 1\}$ tel que $\sigma^\ell(t) = \sigma^k(t)$. On a $\sigma^{\ell-k}(t) = t \in \{t, \sigma(t), \dots, \sigma^{\ell-k-1}(t)\}$, 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

$$\sigma^k(t) = (\sigma^r \circ (\sigma^\ell)^q)(t) = \sigma^r(t) \in \{t, \sigma(t), \dots, \sigma^{\ell-1}(t)\}.$$

Ceci montre que $\mathcal{O}[t] = \{t, \sigma(t), \dots, \sigma^{\ell-1}(t)\}$. Reste à montrer que $\text{card}(\mathcal{O}[t]) = \ell$. Supposons qu'il existe $a, b \in \{0, 1, \dots, \ell - 1\}$ tels que $a < b$ et $\sigma^a(t) = \sigma^b(t)$. Alors $\sigma^b(t) \in \{t, \sigma(t), \dots, \sigma^{b-1}(t)\}$. Ceci contredit la minimalité de ℓ , donc $t, \sigma(t), \dots, \sigma^{\ell-1}(t)$ sont deux à deux distincts, donc $\text{card}(\mathcal{O}[t]) = \ell$.

Notons $\mathcal{O}_1, \dots, \mathcal{O}_\ell$ les orbites de σ de cardinal ≥ 2 . Par l'assertion 1 on a $\text{supp}(\sigma) = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \dots \sqcup \mathcal{O}_\ell$. Pour tout $i \in \{1, \dots, \ell\}$ on choisit $t_i \in \mathcal{O}_i$ et on pose $c_i = (t_i, \sigma(t_i), \dots, \sigma^{m_i-1}(t_i))$, où $m_i = \text{card}(\mathcal{O}_i)$. Les assertions 1 et 2 impliquent que $\sigma = c_1 \circ c_2 \circ \dots \circ c_\ell$. De plus, pour $i, j \in \{1, \dots, \ell\}, i \neq j$, on a $\text{supp}(c_i) \cap \text{supp}(c_j) = \mathcal{O}_i \cap \mathcal{O}_j = \emptyset$. Ceci démontre l'existence de la décomposition.

Supposons que $\sigma = d_1 \circ d_2 \circ \dots \circ d_{\ell'}$, où chaque d_i est un cycle et $\text{supp}(d_i) \cap \text{supp}(d_j) = \emptyset$ pour tous $i, j \in \{1, \dots, \ell'\}, i \neq j$. Soit $i \in \{1, \dots, \ell'\}$. Soit $t_i \in \text{supp}(d_i)$. Alors $d_i = (t_i, \sigma(t_i), \dots, \sigma^{m_i-1}(t_i))$, 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, $\mathcal{O}_i = \{t_i, \sigma(t_i), \dots, \sigma^{m_i-1}(t_i)\}$ 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 $i \in \{1, \dots, \ell\}$. \square

Définition. Soit $\sigma \in \mathfrak{S}_n$. Soient $i, j \in [n], i < j$. On dit que σ présente une inversion en (i, j) si $\sigma(i) > \sigma(j)$. On appelle nombre d'inversions de σ et on note $\nu(\sigma)$ le nombre de couples (i, j) tels que $i < j$ et σ présente une inversion en (i, j) .

Définition. Soit $\sigma \in \mathfrak{S}_n$. On appelle signature de σ et on note $\varepsilon(\sigma)$ l'entier suivant.

$$\varepsilon(\sigma) = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Lemme 1.46. Soit $\sigma \in \mathfrak{S}_n$. Alors $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$. En particulier, $\varepsilon(\sigma) \in \{\pm 1\}$.

Démonstration. Soit $\sigma \in \mathfrak{S}_n$.

$$\begin{aligned} \prod_{i < j} \sigma(i) - \sigma(j) &= \left(\prod_{i < j, \sigma(i) < \sigma(j)} \sigma(i) - \sigma(j) \right) \left(\prod_{i < j, \sigma(i) > \sigma(j)} \sigma(i) - \sigma(j) \right) = \\ &= (-1)^{\nu(\sigma)} \left(\prod_{i < j, \sigma(i) < \sigma(j)} \sigma(i) - \sigma(j) \right) \left(\prod_{i < j, \sigma(i) > \sigma(j)} \sigma(j) - \sigma(i) \right) = \\ &= (-1)^{\nu(\sigma)} \left(\prod_{i \neq j, \sigma(i) < \sigma(j)} \sigma(i) - \sigma(j) \right) = (-1)^{\nu(\sigma)} \left(\prod_{i < j} i - j \right), \end{aligned}$$

donc

$$(-1)^{\nu(\sigma)} = \frac{\prod_{i < j} \sigma(i) - \sigma(j)}{\prod_{i < j} i - j} = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j} = \varepsilon(\sigma).$$

\square

Proposition 1.47. L'application signature $\varepsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$ est un homomorphisme de groupes, c'est-à-dire $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \varepsilon(\tau)$ pour tous $\sigma, \tau \in \mathfrak{S}_n$.

Démonstration. Soient $\sigma, \tau \in \mathfrak{S}_n$. Alors

$$\begin{aligned} & \prod_{i < j} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} = \\ & \left(\prod_{i < j, \tau(i) < \tau(j)} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} \right) \left(\prod_{i < j, \tau(i) > \tau(j)} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} \right) = \\ & \left(\prod_{i < j, \tau(i) < \tau(j)} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} \right) \left(\prod_{i < j, \tau(j) < \tau(i)} \frac{(\sigma \circ \tau)(j) - (\sigma \circ \tau)(i)}{\tau(j) - \tau(i)} \right) = \\ & \prod_{i \neq j, \tau(i) < \tau(j)} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} = \prod_{i < j} \frac{\sigma(i) - \sigma(j)}{i - j} = \varepsilon(\sigma) \end{aligned}$$

donc

$$\begin{aligned} \varepsilon(\sigma \circ \tau) &= \prod_{i < j} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{i - j} = \prod_{i < j} \left(\frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} \frac{\tau(i) - \tau(j)}{i - j} \right) = \\ & \left(\prod_{i < j} \frac{(\sigma \circ \tau)(i) - (\sigma \circ \tau)(j)}{\tau(i) - \tau(j)} \right) \left(\prod_{i < j} \frac{\tau(i) - \tau(j)}{i - j} \right) = \varepsilon(\sigma) \varepsilon(\tau). \end{aligned}$$

□

Lemme 1.48. La signature d'un ℓ -cycle est $(-1)^{\ell-1}$. En particulier, la signature d'une transposition est -1 .

Démonstration. Posons $\sigma = (1, 2)$. Alors

$$\{(i, j) \in [n]^2 \mid i < j \text{ et } \sigma(i) > \sigma(j)\} = \{(1, 2)\},$$

donc $\nu(\sigma) = 1$, donc $\varepsilon(\sigma) = (-1)^1 = -1$. Posons $\sigma = (i, j)$, où $i, j \in [n]$, $i \neq j$. On choisit $\tau \in \mathfrak{S}_n$ tel que $\tau(1) = i$ et $\tau(2) = j$ et on pose $\sigma' = \tau^{-1} \circ \sigma \circ \tau$. On a $\sigma'(1) = 2$, $\sigma'(2) = 1$ et $\sigma'(k) = k$ pour tout $k \in \{3, 4, \dots, n\}$, donc $\sigma' = (1, 2)$. Par ce qui précède il s'en suit que

$$-1 = \varepsilon(\sigma') = \varepsilon(\tau)^{-1} \varepsilon(\sigma) \varepsilon(\tau) = \varepsilon(\sigma).$$

Supposons que $\sigma = (t_1, t_2, \dots, t_\ell)$ est un cycle de longueur ℓ . On vérifie facilement que $\sigma = (t_1, t_2) \circ (t_2, t_3) \circ \dots \circ (t_{\ell-1}, t_\ell)$, donc

$$\varepsilon(\sigma) = \varepsilon((t_1, t_2)) \varepsilon((t_2, t_3)) \cdots \varepsilon((t_{\ell-1}, t_\ell)) = (-1)^{\ell-1}.$$

□

Définition. Le noyau de l'homomorphisme signature $\varepsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$ s'appelle le *groupe alterné* et se note \mathfrak{A}_n .

Le résultat suivant est une conséquence directe du théorème 1.45.

Lemme 1.49. *Les cycles engendrent le groupe symétrique \mathfrak{S}_n .*

Lemme 1.50. *Les transpositions engendrent le groupe symétrique \mathfrak{S}_n .*

Démonstration. On sait par le lemme 1.49 que \mathfrak{S}_n est engendré par les cycles, donc il suffit de montrer que tout cycle est un produit de transpositions. On vérifie facilement que, si $\sigma = (t_1, t_2, \dots, t_\ell)$, alors $\sigma = (t_1, t_2) \circ (t_2, t_3) \circ \dots \circ (t_{\ell-1}, t_\ell)$. \square

Proposition 1.51. *Pour $i \in \{1, \dots, n-1\}$ on pose $s_i = (i, i+1)$. Alors \mathfrak{S}_n est engendré par $\{s_1, s_2, \dots, s_{n-1}\}$.*

Démonstration. On sait par le lemme 1.50 que \mathfrak{S}_n est engendré par les transpositions donc il suffit de montrer que toute transposition est produit d'éléments de $\{s_1, s_2, \dots, s_{n-1}\}$. Soient $i, j \in \{1, \dots, n\}$, $i < j$. Alors

$$(i, j) = (i, i+1) \circ (i+1, i+2) \circ \dots \circ (j-2, j-1) \circ (j-1, j) \circ (j-2, j-1) \\ \circ \dots \circ (i+2, i+1) \circ (i, i+1) = s_i \circ s_{i+1} \circ \dots \circ s_{j-2} \circ s_{j-1} \circ s_{j-2} \circ \dots \circ s_{i+1} \circ s_i.$$

\square

Proposition 1.52. *Le groupe alterné \mathfrak{A}_n est engendré par les 3-cycles.*

Démonstration. Remarquons d'abord que, si $\sigma = (i, j, k)$ est un 3-cycle, alors $\varepsilon(\sigma) = (-1)^2 = 1$, donc $\sigma \in \text{Ker}(\varepsilon) = \mathfrak{A}_n$. Pour montrer la proposition 1.52 il suffit de montrer que tout élément de \mathfrak{A}_n est produit de 3-cycles. Soit $\sigma \in \mathfrak{S}_n$. Par le lemme 1.50 il existe des transpositions t_1, \dots, t_ℓ telles que $\sigma = t_1 \circ t_2 \circ \dots \circ t_\ell$. On a $1 = \varepsilon(\sigma) = (-1)^\ell$, donc ℓ est pair, disons $\ell = 2\ell'$. Pour montrer que σ est un produit de 3-cycles il suffit alors de montrer que $t_{2k-1} \circ t_{2k}$ est un produit de 3-cycles pour tout $k \in \{1, \dots, \ell'\}$. Si $t_{2k-1} = t_{2k}$, alors $t_{2k-1} \circ t_{2k} = \text{id}$ est un produit de 0 3-cycles. Supposons que $t_{2k-1} \neq t_{2k}$ et $\text{supp}(t_{2k-1}) \cap \text{supp}(t_{2k}) \neq \emptyset$. Dans ce cas il existe $a, b, c \in \{1, \dots, n\}$ deux à deux distincts tels que $t_{2k-1} = (a, b)$ et $t_{2k} = (b, c)$. Alors $t_{2k-1} \circ t_{2k} = (a, b) \circ (b, c) = (a, b, c)$ est le produit de 1 3-cycle. Supposons que $t_{2k-1} \neq t_{2k}$ et $\text{supp}(t_{2k-1}) \cap \text{supp}(t_{2k}) = \emptyset$. Dans ce cas il existe $a, b, c, d \in \{1, \dots, n\}$ deux à deux distincts tels que $t_{2k-1} = (a, b)$ et $t_{2k} = (c, d)$. Alors $t_{2k-1} \circ t_{2k} = (a, b) \circ (c, d) = (a, b) \circ (b, c) \circ (b, c) \circ (c, d) = (a, b, c) \circ (b, c, d)$ est le produit de 2 3-cycles. \square

2 Anneaux

2.1 Définitions et propriétés générales

Définition. Un *anneau* est un ensemble A muni de deux lois internes, $+$ et $*$, vérifiant :

- (a) $(A, +)$ est un groupe abélien ;

- (b) $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in A$;
- (c) il existe $1_A \in A \setminus \{0_A\}$ tel que $x * 1_A = 1_A * x = x$ pour tout $x \in A$;
- (d) $x * (y + z) = x * y + x * z$ et $(y + z) * x = y * x + z * x$ pour tous $x, y, z \in A$ (on dit que la multiplication est distributive par rapport à l'addition).

Exemples.

- (1) $(\mathbb{Z}, +, \times)$ est un anneau.
- (2) Soit V un espace vectoriel sur un corps \mathbb{K} . Alors $(\text{End}(V), +, \circ)$ est un anneau.

Lemme 2.1. Soit A un anneau. Pour tout $x \in A$ on a $0_A * x = x * 0_A = 0_A$.

Démonstration. Soit $x \in A$. Alors

$$x = 1_A * x = (1_A + 0_A) * x = 1_A * x + 0_A * x = x + 0_A * x.$$

En soustrayant x on en déduit que $0_A = 0_A * x$. Le même argument démontre l'autre égalité. \square

Définition. Un anneau A est dit *commutatif* si la multiplication est commutative, c'est-à-dire si $x * y = y * x$ pour tous $x, y \in A$.

Définition. Soit A un anneau. Un élément $x \in A \setminus \{0\}$ est dit *inversible* s'il existe $x' \in A$ tel que $x * x' = x' * x = 1_A$. Dans ce cas l'élément x' s'appelle un (le) *inverse* de x et se note x^{-1} . L'ensemble des éléments inversibles de A se note $\mathcal{U}(A)$.

Lemme 2.2. Soit A un anneau.

- (1) Tout élément inversible de A admet un unique inverse.
- (2) La multiplication détermine une loi interne sur $\mathcal{U}(A)$, et $(\mathcal{U}(A), *)$ est un groupe.

Démonstration. Soit x un élément inversible de A . Soient $x', x'' \in A$ deux inverses de x . Alors $x' = x' * 1_A = x' * x * x'' = 1_A * x'' = x''$.

Soient x, y deux éléments inversibles de A . Soient x', y' les inverses de x et y , respectivement. Posons $z = x * y$ et $z' = y' * x'$. Alors

$$z * z' = x * y * y' * x' = x * 1_A * x' = x * x' = 1_A.$$

De même, $z' * z = 1_A$, donc z est inversible. Ceci montre que la multiplication détermine une loi interne sur $\mathcal{U}(A)$. Le fait que $(\mathcal{U}(A), *)$ soit un groupe découle directement de la définition d'anneau. \square

Définition. Soit A un anneau commutatif. On dit que A est un *corps* si tout élément de $A \setminus \{0_A\}$ est inversible, c'est-à-dire si $\mathcal{U}(A) = A \setminus \{0_A\}$.

Exemple. \mathbb{Q}, \mathbb{R} et \mathbb{C} sont des corps.

Définition. Soit A un anneau. Un sous-ensemble B de A est un *sous-anneau* de A si :

- (a) B est un sous-groupe de $(A, +)$,
- (b) $1_A \in B$,
- (c) si $x, y \in B$, alors $x * y \in B$.

Exemple. \mathbb{Z} est un sous-anneau de \mathbb{Q} .

Lemme 2.3 (sans démonstration). *Soient $(A, +, *)$ un anneau et B un sous-anneau de A . Notons $+$ et $*$ les restrictions de $+$ et $*$ à $B \times B$. Alors $(B, +, *)$ est un anneau.*

Définition. On appelle *homomorphisme d'anneaux* une application $\varphi : A \rightarrow A'$ entre deux anneaux telle que

- (a) $\varphi(x + y) = \varphi(x) + \varphi(y)$ pour tous $x, y \in A$,
- (b) $\varphi(1_A) = 1_{A'}$,
- (c) $\varphi(x * y) = \varphi(x) * \varphi(y)$ pour tous $x, y \in A$.

Définition. L'image d'un homomorphisme d'anneaux $\varphi : A \rightarrow A'$, notée $\text{Im}(\varphi)$, est $\text{Im}(\varphi) = \{\varphi(x) \mid x \in A\}$.

Lemme 2.4. *L'image d'un homomorphisme d'anneaux $\varphi : A \rightarrow A'$ est un sous-anneau de A' .*

Démonstration. On sait déjà que $\text{Im}(\varphi)$ est un sous-groupe de A' . Soient $x', y' \in \text{Im}(\varphi)$. Soient $x, y \in A$ tels que $x' = \varphi(x)$ et $y' = \varphi(y)$. Alors

$$x' * y' = \varphi(x) * \varphi(y) = \varphi(x * y) \in \text{Im}(\varphi).$$

Finalement, $1_{A'} = \varphi(1_A) \in \text{Im}(\varphi)$. □

Définition. Soit A_1, \dots, A_n une collection finie d'anneaux. On définit un produit et une somme sur le produit cartésien $A_1 \times \dots \times A_n$ comme suit.

$$\begin{aligned} (a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 + b_1, \dots, a_n + b_n), \\ (a_1, \dots, a_n) * (b_1, \dots, b_n) &= (a_1 * b_1, \dots, a_n * b_n). \end{aligned}$$

Lemme 2.5 (sans démonstration). *Soit A_1, \dots, A_n une collection finie d'anneaux. Alors $(A_1 \times \dots \times A_n, +, *)$ est un anneau.*

Remarque. L'élément neutre pour l'addition dans $A_1 \times \dots \times A_n$ est $(0, 0, \dots, 0)$, et l'élément neutre pour la multiplication est $(1, 1, \dots, 1)$.

Définition. Un sous-ensemble I d'un anneau A est appelé un *idéal à gauche* (resp. *idéal à droite*) si :

- (a) I est un sous-groupe de $(A, +)$,

(b) pour tous $a \in A$ et $x \in I$ on a $ax \in I$ (resp. $xa \in I$).

Un sous-ensemble I qui est à la fois un idéal à gauche et un idéal à droite s'appelle un *idéal bilatère* de A .

Lemme 2.6. *Soit I un idéal de \mathbb{Z} . Alors $I = \{0\}$ ou il existe $m \in \mathbb{N}^*$ tel que $I = m\mathbb{Z}$.*

Démonstration. Comme I est un sous-groupe de \mathbb{Z} , on sait que $I = \{0\}$ ou $I = m\mathbb{Z}$ avec $m \in \mathbb{N}^*$. Il est clair aussi que $\{0\}$ est un idéal et, si $m \in \mathbb{N}^*$, alors $m\mathbb{Z}$ est un idéal. \square

Définition. Soit $\varphi : A \rightarrow A'$ un homomorphisme d'anneaux. Le *noyau* de φ est l'ensemble des éléments $x \in A$ tels que $\varphi(x) = 0_{A'}$. Il est noté $\text{Ker}(\varphi)$.

Proposition 2.7. *Le noyau d'un homomorphisme d'anneaux $\varphi : A \rightarrow A'$ est un idéal bilatère de A .*

Démonstration. On sait déjà que $\text{Ker}(\varphi)$ est un sous-groupe de A . Soient $x \in \text{Ker}(\varphi)$ et $a \in A$. On a

$$\varphi(a * x) = \varphi(a) * \varphi(x) = \varphi(a) * 0_{A'} = 0_{A'},$$

donc $a * x \in \text{Ker}(\varphi)$. De même, $x * a \in \text{Ker}(\varphi)$. Ceci montre que $\text{Ker}(\varphi)$ est un idéal bilatère de A . \square

Le lemme suivant est une conséquence directe du lemme 1.9.

Lemme 2.8. *Soit $\varphi : A \rightarrow A'$ un homomorphisme d'anneaux. Alors φ est injectif si et seulement si $\text{Ker}(\varphi) = \{0_A\}$.*

Lemme 2.9. *Soient A un anneau, et $\{I_i \mid i \in \Omega\}$ une collection non vide d'idéaux bilatères de A . Alors $\bigcap_{i \in \Omega} I_i$ est un idéal bilatère de A .*

Démonstration. On sait déjà que $\bigcap_{i \in \Omega} I_i$ est un sous-groupe de A . Soient $x \in \bigcap_{i \in \Omega} I_i$ et $a \in A$. On a $x \in I_i$ donc $a * x \in I_i$ pour tout $i \in \Omega$, donc $a * x \in \bigcap_{i \in \Omega} I_i$. De même, $x * a \in \bigcap_{i \in \Omega} I_i$. \square

Définition. On appelle idéal (bilatère) *engendré* par une partie S de A l'intersection de tous les idéaux bilatères contenant S . Autrement dit, c'est le plus petit idéal bilatère contenant S . Il se note (S) .

Lemme 2.10. *On suppose que A est un anneau commutatif. Soit $S = \{x_1, \dots, x_n\}$ une partie finie non vide de A . Alors l'idéal (x_1, \dots, x_n) engendré par S est égal à l'ensemble des éléments de A de la forme $a_1 * x_1 + \dots + a_n * x_n$, avec $a_1, \dots, a_n \in A$.*

Démonstration. Notons I l'ensemble des éléments de A de la forme $a_1 * x_1 + \dots + a_n * x_n$ avec $a_1, \dots, a_n \in A$. On a $0_A = 0_A * x_1 + \dots + 0_A * x_n \in I$. Soient $u, v \in I$. Il existe $a_1, \dots, a_n, b_1, \dots, b_n \in A$ tels que $u = a_1 * x_1 + \dots + a_n * x_n$ et $v = b_1 * x_1 + \dots + b_n * x_n$. Alors

$$u + v = (a_1 + b_1) * x_1 + \dots + (a_n + b_n) * x_n \in I.$$

Soit $u \in I$. Il existe $a_1, \dots, a_n \in A$ tels que $u = a_1 * x_1 + \dots + a_n * x_n$. Alors

$$-u = (-a_1) * x_1 + \dots + (-a_n) * x_n \in I.$$

Soient $u \in I$ et $b \in A$. Il existe $a_1, \dots, a_n \in A$ tels que $u = a_1 * x_1 + \dots + a_n * x_n$. Alors

$$b * u = (b * a_1) * x_1 + \dots + (b * a_n) * x_n \in I.$$

Ceci montre que I est un idéal de A .

Soit J un idéal de A contenant S . Soit $u \in I$. Il existe $a_1, \dots, a_n \in A$ tels que $u = a_1 * x_1 + \dots + a_n * x_n$. On a $a_i * x_i \in J$ pour tout $i \in \{1, \dots, n\}$, donc $u = a_1 * x_1 + \dots + a_n * x_n \in J$. Ceci montre que $I \subset J$. \square

Lemme 2.11. Soient A un anneau commutatif et $x \in A$. Alors $(x) = A$ si et seulement si x est inversible.

Démonstration. Supposons que $(x) = A$. On a $1_A \in (x)$, donc il existe $y \in A$ tel que $y * x = 1_A$, c'est-à-dire x est inversible et y est l'inverse de x . Supposons que x est inversible. Soit y l'inverse de x . On a $1_A = y * x \in (x)$. D'où, si $a \in A$, alors $a = a * 1_A \in (x)$. Ceci montre que $A = (x)$. \square

Définition. Soient A un anneau et I un idéal bilatère propre de A (i.e. $I \neq A$). Soient $a, b \in A$. On dit que a est congru à b modulo I si $b - a \in I$. Cette relation se note $a \equiv b \pmod{I}$. Rappelons que "être congru modulo I " est une relation d'équivalence, l'ensemble quotient se note A/I et la classe d'un élément $a \in A$ se note $[a] = [a]_I$.

Lemme 2.12. Soient A un anneau et I un idéal bilatère propre de A (i.e. $I \neq A$). Soient $a, b, c, d \in A$ tels que $a \equiv b \pmod{I}$ et $c \equiv d \pmod{I}$. Alors $a + c \equiv b + d \pmod{I}$ et $a * c \equiv b * d \pmod{I}$.

Démonstration. On sait déjà que $a + c \equiv b + d \pmod{I}$. Par ailleurs,

$$a * c - b * d = a * c - a * d + a * d - b * d = a * (c - d) + (a - b) * d \in I,$$

donc $a * c \equiv b * d \pmod{I}$. \square

Définition. Soient A un anneau et I un idéal bilatère propre de A . On définit des opérations $+$ et $*$ sur A/I comme suit. Soient $\alpha, \beta \in A/I$. On choisit $a, b \in A$ tels que $\alpha = [a]$ et $\beta = [b]$. On pose alors

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

Ces définitions ne dépendent pas du choix de a et b par le lemme 2.13.

Proposition 2.13. Soient A un anneau et I un idéal bilatère propre. Alors A/I muni des opérations $+$ et $*$ est un anneau.

Définition. L'anneau A/I de la proposition 2.13 s'appelle *l'anneau quotient* de A par I .

Démonstration. On sait que $(A/I, +)$ est un groupe abélien. On pose $1_{A/I} = [1_A]$. Si on avait $1_{A/I} = [1_A] = 0_{A/I} = [0_A]$, alors on aurait $1_A \in I$, donc $a = a * 1_A \in I$ pour tout $a \in A$, donc $A = I$. Ceci contredit le fait que I est propre, donc $1_{A/I} \neq 0_{A/I}$. Soient $a, b, c \in A$. Alors

$$\begin{aligned} ([a] * [b]) * [c] &= [a * b] * [c] = [(a * b) * c] = [a * (b * c)] = [a] * [b * c] = [a] * ([b] * [c]), \\ 1_{A/I} * [a] &= [1_A] * [a] = [1_A * a] = [a] \quad \text{et} \quad [a] * 1_{A/I} = [a] * [1_A] = [a * 1_A] = [a], \\ [a] * ([b] + [c]) &= [a] * [b + c] = [a * (b + c)] = [(a * b) + (a * c)] = \\ &= [a * b] + [a * c] = ([a] * [b]) + ([a] * [c]), \\ ([b] + [c]) * [a] &= [b + c] * [a] = [(b + c) * a] = [(b * a) + (c * a)] = \\ &= [b * a] + [c * a] = ([b] * [a]) + ([c] * [a]). \end{aligned}$$

Ceci montre que A/I est un anneau. □

Lemme 2.14. Soient A un anneau et I un idéal bilatère propre de A . L'application $\pi : A \rightarrow A/I, a \mapsto [a]$, est un homomorphisme d'anneaux surjectif dont le noyau est I .

Démonstration. Soient $a, b \in A$. Alors

$$\begin{aligned} \pi(a + b) &= [a + b] = [a] + [b] = \pi(a) + \pi(b), \\ \pi(a * b) &= [a * b] = [a] * [b] = \pi(a) * \pi(b). \end{aligned}$$

De plus, $\pi(1_A) = [1_A] = 1_{A/I}$. Ceci montre que π est un homomorphisme. Il est surjectif par construction. Finalement,

$$a \in \text{Ker}(\pi) \Leftrightarrow \pi(a) = [a] = [0] \Leftrightarrow a \in I,$$

donc $\text{Ker}(\pi) = I$. □

Proposition 2.15.

- (1) Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux et J un idéal bilatère de B . Alors $\varphi^{-1}(J)$ est un idéal de A .
- (2) Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux surjectif et I un idéal bilatère de A . Alors $\varphi(I)$ est un idéal bilatère de B .
- (3) Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux et I un idéal bilatère de A . Supposons que $I \subset \text{Ker}(\varphi)$. Alors il existe un unique homomorphisme $\psi : A/I \rightarrow B$ tel que $\varphi = \psi \circ \pi$, où $\pi : A \rightarrow A/I$ est la projection canonique. En d'autres termes, on a le diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \pi \downarrow & \nearrow \psi & \\ A/I & & \end{array}$$

Démonstration. Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux et J un idéal bilatère de B . On a $\varphi(0_A) = 0_B \in J$, donc $0_A \in \varphi^{-1}(J)$. Soient $a_1, a_2 \in \varphi^{-1}(J)$. Alors

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \in J,$$

donc $a_1 + a_2 \in \varphi^{-1}(J)$. Soit $a \in \varphi^{-1}(J)$. Alors

$$\varphi(-a) = -\varphi(a) \in J,$$

donc $-a \in \varphi^{-1}(J)$. Ceci montre que $\varphi^{-1}(J)$ est un sous-groupe de $(A, +)$. Soient $a \in \varphi^{-1}(J)$ et $x \in A$. Alors

$$\varphi(x * a) = \varphi(x) * \varphi(a) \in J,$$

donc $x * a \in \varphi^{-1}(J)$. De même, $a * x \in \varphi^{-1}(J)$. Ceci montre que $\varphi^{-1}(J)$ est un idéal bilatère de A .

Soient $\varphi : A \rightarrow B$ un homomorphisme surjectif et I un idéal bilatère de A . Comme $0_A \in I$, on a $0_B = \varphi(0_A) \in \varphi(I)$. Soient $b_1, b_2 \in \varphi(I)$. Il existe $a_1, a_2 \in I$ tels que $b_1 = \varphi(a_1)$ et $b_2 = \varphi(a_2)$. Alors

$$b_1 + b_2 = \varphi(a_1) + \varphi(a_2) = \varphi(a_1 + a_2) \in \varphi(I).$$

Soit $b \in \varphi(I)$. Il existe $a \in I$ tel que $b = \varphi(a)$. Alors

$$-b = -\varphi(a) = \varphi(-a) \in \varphi(I).$$

Ceci montre que $\varphi(I)$ est un sous-groupe de $(B, +)$. Soient $b \in \varphi(I)$ et $y \in B$. Il existe $a \in I$ tel que $b = \varphi(a)$. Par ailleurs, comme φ est surjectif, il existe $x \in A$ tel que $y = \varphi(x)$. Alors $x * a \in I$, donc

$$y * b = \varphi(x) * \varphi(a) = \varphi(x * a) \in \varphi(I).$$

De même, $b * y \in \varphi(I)$. Ceci montre que $\varphi(I)$ est un idéal bilatère de B .

Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux et I un idéal bilatère de A tel que $I \subset \text{Ker}(\varphi)$. Comme avant, pour $a \in A$, on note $[a]$ la classe de a dans A/I (i.e. $[a] = \pi(a)$). Pour $a \in A$ on pose

$$\psi([a]) = \varphi(a).$$

Montrons d'abord que ψ est bien définie. Soient $a, a' \in A$ tels que $[a] = [a']$. On a $a' - a \in I \subset \text{Ker}(\varphi)$, donc

$$\varphi(a') - \varphi(a) = \varphi(a' - a) = 0_B,$$

donc $\varphi(a') = \varphi(a)$.

Montrons que ψ est un homomorphisme. Soient $a_1, a_2 \in A$. Alors

$$\begin{aligned}\psi([a_1] + [a_2]) &= \psi([a_1 + a_2]) = \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) = \psi([a_1]) + \psi([a_2]), \\ \psi([a_1] * [a_2]) &= \psi([a_1 * a_2]) = \varphi(a_1 * a_2) = \varphi(a_1) * \varphi(a_2) = \psi([a_1]) * \psi([a_2]).\end{aligned}$$

Par ailleurs,

$$\psi(1_{A/I}) = \psi([1_A]) = \varphi(1_A) = 1_B.$$

Par définition on a

$$(\psi \circ \pi)(a) = \psi([a]) = \varphi(a)$$

pour tout $a \in A$, donc $\varphi = \psi \circ \pi$. De plus, si $\psi' : A/I \rightarrow B$ est un homomorphisme tel que $\varphi = \psi' \circ \pi$, alors

$$\psi'([a]) = (\psi' \circ \pi)(a) = \varphi(a) = \psi([a])$$

pour tout $a \in A$, donc $\psi' = \psi$. Ceci montre que ψ est unique. \square

Corollaire 2.16. Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux, $\pi : A \rightarrow A/\text{Ker}(\varphi)$ la projection canonique, et $\iota : \text{Im}(\varphi) \rightarrow B$ l'inclusion canonique. Il existe un unique isomorphisme $\varphi' : A/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi)$ tel que $\varphi = \iota \circ \varphi' \circ \pi$. En d'autres termes, on a le diagramme commutatif suivant :

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \pi \downarrow & & \uparrow \iota \\ A/\text{Ker}(\varphi) & \xrightarrow[\simeq]{\varphi'} & \text{Im}(\varphi) \end{array}$$

Démonstration. On considère l'application $\psi : A \rightarrow \text{Im}(\varphi)$ définie par

$$\psi(x) = \varphi(x)$$

pour $x \in A$. Il est clair que ψ est un homomorphisme, ψ est surjectif, $\text{Ker}(\psi) = \text{Ker}(\varphi)$, et $\iota \circ \psi = \varphi$. Par la proposition 2.15, il existe un unique homomorphisme $\varphi' : A/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi)$ tel que $\psi = \varphi' \circ \pi$. En composant par ι on obtient $\iota \circ \varphi' \circ \pi = \iota \circ \psi = \varphi$. L'homomorphisme φ' est surjectif car ψ est surjectif et $\psi = \varphi' \circ \pi$. Reste à montrer que φ' est injectif. Son unicité est laissée en exercice.

Soit $\alpha \in \text{Ker}(\varphi')$. Soit $a \in A$ tel que $\alpha = [a]$. On a

$$\varphi(a) = \varphi'([a]) = \varphi'(\alpha) = 0_B,$$

donc $a \in \text{Ker}(\varphi)$, ce qui signifie que $\alpha = [a] = [0_A] = 0$. Ceci montre que $\text{Ker}(\varphi') = \{0\}$, donc que φ' est injectif. \square

2.2 Anneaux commutatifs

A partir de maintenant nous supposons que les anneaux sont commutatifs.

Définition. Soient A un anneau et I et J deux idéaux de A . On note IJ l'idéal de A engendré par l'ensemble $\{x * y \mid x \in I \text{ et } y \in J\}$.

Exemple. On suppose que $A = \mathbb{Z}$, $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$. Alors $IJ = 6\mathbb{Z}$. De façon plus générale, si n et m sont deux entiers positifs, alors $(n\mathbb{Z})(m\mathbb{Z}) = (nm)\mathbb{Z}$.

Lemme 2.17. Soient A un anneau et I, J deux idéaux de A . Supposons que I soit engendré par $X = \{x_1, \dots, x_n\}$ et J soit engendré par $Y = \{y_1, \dots, y_m\}$. Alors IJ est engendré par $\{x_i * y_j \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq m\}$.

Démonstration. Notons K l'idéal engendré par $\{x_i * y_j \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq m\}$. Pour tous $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, m\}$ on a $x_i * y_j \in IJ$, donc $K \subset IJ$. Soient $x \in I$ et $y \in J$. Il existe $a_1, \dots, a_n \in A$ tels que $x = \sum_{i=1}^n a_i * x_i$. De même, il existe $b_1, \dots, b_m \in A$ tels que $y = \sum_{j=1}^m b_j * y_j$. Alors

$$x * y = \left(\sum_{i=1}^n a_i * x_i \right) * \left(\sum_{j=1}^m b_j * y_j \right) = \sum_{i=1}^n \sum_{j=1}^m (a_i * b_j) * (x_i * y_j) \in K.$$

Ceci montre que $IJ \subset K$, donc que $IJ = K$. □

Définition. Si I et J sont deux idéaux d'un anneau A , $I + J$ désigne l'ensemble

$$I + J = \{x + y \mid x \in I \text{ et } y \in J\}.$$

Lemme 2.18. Soient I et J deux idéaux d'un anneau A . Alors $I + J$ est un idéal de A .

Démonstration. On a $0_A \in I$ et $0_A \in J$, donc $0_A = 0_A + 0_A \in I + J$. Soient $z_1, z_2 \in I + J$. Il existe $x_1, x_2 \in I$ et $y_1, y_2 \in J$ tels que $z_1 = x_1 + y_1$ et $z_2 = x_2 + y_2$. Alors

$$z_1 + z_2 = (x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in I + J.$$

Soit $z \in I + J$. Il existe $x \in I$ et $y \in J$ tels que $z = x + y$. Alors

$$-z = (-x) + (-y) \in I + J.$$

Soient $z \in I + J$ et $a \in A$. Il existe $x \in I$ et $y \in J$ tels que $z = x + y$. Alors

$$a * z = (a * x) + (a * y) \in I + J.$$

□

Exemple. On a $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. On a $3\mathbb{Z} + 8\mathbb{Z} = \mathbb{Z}$. De façon générale, si n, m sont deux entiers positifs, $n\mathbb{Z} + m\mathbb{Z} = \text{pgcd}(n, m)\mathbb{Z}$.

Lemme 2.19. Soient I et J deux idéaux d'un anneau A . Si $I + J = A$, alors $IJ = I \cap J$.

Démonstration. Pour tous $x \in I$ et $y \in J$ on a $x * y = y * x \in I \cap J$, donc $IJ \subset I \cap J$. Soit $z \in I \cap J$. Comme $I + J = A$, il existe $x_0 \in I$ et $y_0 \in J$ tels que $1_A = x_0 + y_0$. Alors

$$z = z * 1_A = z * (x_0 + y_0) = (x_0 * z) + (z * y_0) \in IJ.$$

Ceci montre que $I \cap J \subset IJ$. □

Exemple. On a $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$ et $(4\mathbb{Z})(6\mathbb{Z}) = 24\mathbb{Z}$. Par contre $3\mathbb{Z} \cap 4\mathbb{Z} = (3\mathbb{Z})(4\mathbb{Z}) = 12\mathbb{Z}$.

Théorème 2.20. Soient I et J deux idéaux d'un anneau A . Si $I + J = A$, alors $A/(IJ) \simeq (A/I) \times (A/J)$.

Démonstration. Rappelons que, si K est un idéal de A et a est un élément de A , alors on note $[a]_K$ l'élément de A/K représenté par a . Soit $\varphi : A \rightarrow (A/I) \times (A/J)$ l'application définie par

$$\varphi(a) = ([a]_I, [a]_J).$$

On a

$$\varphi(1_A) = ([1_A]_I, [1_A]_J) = (1_{A/I}, 1_{A/J}).$$

Soient $a_1, a_2 \in A$. Alors

$$\begin{aligned} \varphi(a_1 + a_2) &= ([a_1 + a_2]_I, [a_1 + a_2]_J) = ([a_1]_I + [a_2]_I, [a_1]_J + [a_2]_J) \\ &= ([a_1]_I, [a_1]_J) + ([a_2]_I, [a_2]_J) = \varphi(a_1) + \varphi(a_2), \\ \varphi(a_1 * a_2) &= ([a_1 * a_2]_I, [a_1 * a_2]_J) = ([a_1]_I * [a_2]_I, [a_1]_J * [a_2]_J) = \\ &= ([a_1]_I, [a_1]_J) * ([a_2]_I, [a_2]_J) = \varphi(a_1) * \varphi(a_2). \end{aligned}$$

Ceci montre que φ est un homomorphisme.

Soit $\alpha \in (A/I) \times (A/J)$. Par définition, il existe $a, b \in A$ tels que $\alpha = ([a]_I, [b]_J)$. Comme $I + J = A$, il existe $x_0 \in I$ et $y_0 \in J$ tels que $x_0 + y_0 = 1$. Posons $c = a * y_0 + b * x_0$. On a

$$[c]_I = [a * y_0 + b * x_0]_I = [a * y_0]_I = [a * (1 - x_0)]_I = [a - a * x_0]_I = [a]_I.$$

De même, $[c]_J = [b]_J$. D'où

$$\varphi(c) = ([c]_I, [c]_J) = ([a]_I, [b]_J) = \alpha.$$

Ceci montre que φ est surjectif.

Soit $a \in A$. Alors

$$a \in \text{Ker}(\varphi) \Leftrightarrow \varphi(a) = ([a]_I, [a]_J) = ([0]_I, [0]_J) \Leftrightarrow a \in I \text{ et } a \in J \Leftrightarrow a \in I \cap J.$$

Autrement dit, $\text{Ker}(\varphi) = I \cap J = IJ$.

Par le corollaire 2.16, on en conclue que φ induit un isomorphisme $\psi : A/(IJ) \rightarrow (A/I) \times (A/J)$. \square

Remarque. Soient I, J deux idéaux de A tels que $I + J = A$. Soient $x_0 \in I$ et $y_0 \in J$ tels que $x_0 + y_0 = 1_A$. Alors l'isomorphisme $\psi : A/(IJ) \rightarrow (A/I) \times (A/J)$ du théorème 2.20 est défini par

$$\psi([c]_{IJ}) = ([c]_I, [c]_J),$$

et sa réciproque, $\psi^{-1} : (A/I) \times (A/J) \rightarrow A/(IJ)$, est définie par

$$\psi^{-1}([a]_I, [b]_J) = [ay_0 + bx_0]_{IJ}.$$

Corollaire 2.21. Soient m et n deux entiers positifs premiers entre eux. Alors $\mathbb{Z}/(mn)\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Définition. Un élément non nul x d'un anneau A est un *diviseur de zéro* s'il existe un élément non nul y de A tel que $xy = 0_A$. Un anneau (commutatif) est un *anneau intègre* s'il n'a pas de diviseur de zéro.

Exemples.

- (1) \mathbb{Z} est un anneau intègre.
- (2) Le produit de deux anneaux non triviaux n'est jamais intègre.

Théorème 2.22. Soit A un anneau intègre. Il existe un corps K tel que :

- (a) A s'identifie à un sous-anneau de K ,
- (b) pour tout $x \in K$ il existe $b \in A \setminus \{0_A\}$ tel que $x * b \in A$.

Démonstration. On pose $A^* = A \setminus \{0_A\}$. On note \sim la relation sur $A \times A^*$ définie par

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{si} \quad a_1 * b_2 = a_2 * b_1.$$

Montrons que \sim est une relation d'équivalence. Soit $(a, b) \in A \times A^*$. On a de façon évidente $a * b = a * b$, donc $(a, b) \sim (a, b)$. Ceci montre que \sim est réflexive. Soient $(a_1, b_1), (a_2, b_2) \in A \times A^*$ tels que $(a_1, b_1) \sim (a_2, b_2)$. On a $a_1 * b_2 = a_2 * b_1$, donc $a_2 * b_1 = a_1 * b_2$, donc $(a_2, b_2) \sim (a_1, b_1)$. Ceci montre que \sim est symétrique. Soient $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times A^*$ tels que $(a_1, b_1) \sim (a_2, b_2)$ et $(a_2, b_2) \sim (a_3, b_3)$. On a

$$a_1 * b_2 * b_3 = b_1 * a_2 * b_3 = a_3 * b_1 * b_2 \Rightarrow (a_1 * b_3 - a_3 * b_1) * b_2 = 0_A.$$

Comme A est intègre et $b_2 \neq 0$, il s'en suit que $a_1 * b_3 - a_3 * b_1 = 0_A$, donc $a_1 * b_3 = a_3 * b_1$, donc $(a_1, b_1) \sim (a_3, b_3)$. Ceci montre que \sim est transitive.

On note $K = (A \times A^*) / \sim$ l'ensemble des classes d'équivalence, et, pour $(a, b) \in A \times A^*$, on note $\frac{a}{b}$ la classe d'équivalence de (a, b) . On définit une somme et une multiplication dans K par

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 * b_2 + a_2 * b_1}{b_1 * b_2}, \quad \frac{a_1}{b_1} * \frac{a_2}{b_2} = \frac{a_1 * a_2}{b_1 * b_2}.$$

On doit montrer que ces opérations sont bien définies. Soient $(a_1, b_1), (a'_1, b'_1), (a_2, b_2), (a'_2, b'_2) \in A \times A^*$ tels que $(a_1, b_1) \sim (a'_1, b'_1)$ et $(a_2, b_2) \sim (a'_2, b'_2)$. Alors

$$(a_1 * b_2 + a_2 * b_1) * (b'_1 * b'_2) = a_1 * b'_1 * b_2 * b'_2 + a_2 * b'_2 * b_1 * b'_1 = a'_1 * b_1 * b_2 * b'_2 + a'_2 * b_2 * b_1 * b'_1 = (a'_1 * b'_2 + a'_2 * b'_1) * (b_1 * b_2)$$

donc

$$\frac{a_1 * b_2 + a_2 * b_1}{b_1 * b_2} = \frac{a'_1 * b'_2 + a'_2 * b'_1}{b'_1 * b'_2}.$$

Par ailleurs

$$(a_1 * a_2) * (b'_1 * b'_2) = (a_1 * b'_1) * (a_2 * b'_2) = (a'_1 * b_1) * (a'_2 * b_2) = (a'_1 * a'_2) * (b_1 * b_2)$$

donc

$$\frac{a_1 * a_2}{b_1 * b_2} = \frac{a'_1 * a'_2}{b'_1 * b'_2}.$$

Maintenant, on va montrer que K est un corps. On pose $0_K = \frac{0_A}{1_A}$ et $1_K = \frac{1_A}{1_A}$. Remarquez que $0_K = \frac{0_A}{b}$ et $1_K = \frac{b}{b}$ pour tout $b \in A^*$. Soient $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times A^*$.

$$\begin{aligned} \left(\frac{a_1}{b_1} + \frac{a_2}{b_2} \right) + \frac{a_3}{b_3} &= \frac{a_1 * b_2 + a_2 * b_1}{b_1 * b_2} + \frac{a_3}{b_3} = \frac{(a_1 * b_2 + a_2 * b_1) * b_3 + a_3 * b_1 * b_2}{b_1 * b_2 * b_3} = \\ &= \frac{a_1 * b_2 * b_3 + a_2 * b_1 * b_3 + a_3 * b_1 * b_2}{b_1 * b_2 * b_3} = \frac{a_1 * b_2 * b_3 + (a_2 * b_3 + a_3 * b_2) * b_1}{b_1 * b_2 * b_3} = \\ &= \frac{a_1}{b_1} + \frac{a_2 * b_3 + a_3 * b_2}{b_2 * b_3} = \frac{a_1}{b_1} + \left(\frac{a_2}{b_2} + \frac{a_3}{b_3} \right) \end{aligned}$$

donc $+$ est associative.

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 * b_2 + a_2 * b_1}{b_1 * b_2} = \frac{a_2 * b_1 + a_1 * b_2}{b_2 * b_1} = \frac{a_2}{b_2} + \frac{a_1}{b_1}$$

donc $+$ est commutative.

$$\frac{a_1}{b_1} + 0_K = \frac{a_1 * 1_A + 0_A * b_1}{b_1 * 1_A} = \frac{a_1}{b_1}$$

donc 0_K est élément neutre pour l'addition.

$$\frac{a_1}{b_1} + \frac{-a_1}{b_1} = \frac{a_1 * b_1 - a_1 * b_1}{b_1^2} = \frac{0_A}{b_1^2} = 0_K$$

donc $\frac{-a_1}{b_1}$ est l'opposé de $\frac{a_1}{b_1}$. Ceci montre que $(K, +)$ est un groupe abélien.

$$\left(\frac{a_1}{b_1} * \frac{a_2}{b_2} \right) * \frac{a_3}{b_3} = \frac{a_1 * a_2}{b_1 * b_2} * \frac{a_3}{b_3} = \frac{a_1 * a_2 * a_3}{b_1 * b_2 * b_3} = \frac{a_1}{b_1} * \frac{a_2 * a_3}{b_2 * b_3} = \frac{a_1}{b_1} * \left(\frac{a_2}{b_2} * \frac{a_3}{b_3} \right)$$

donc $*$ est associative.

$$\frac{a_1}{b_1} * \frac{a_2}{b_2} = \frac{a_1 * a_2}{b_1 * b_2} = \frac{a_2 * a_1}{b_2 * b_1} = \frac{a_2}{b_2} * \frac{a_1}{b_1}$$

donc $*$ est commutative.

$$\frac{a_1}{b_1} * 1_K = \frac{a_1 * 1_A}{b_1 * 1_A} = \frac{a_1}{b_1}$$

donc 1_K est élément neutre pour la multiplication.

$$\begin{aligned} \left(\frac{a_1}{b_1} * \frac{a_2}{b_2} \right) + \left(\frac{a_1}{b_1} * \frac{a_3}{b_3} \right) &= \frac{a_1 * a_2}{b_1 * b_2} + \frac{a_1 * a_3}{b_1 * b_3} = \frac{a_1 * a_2 * b_1 * b_3 + a_1 * a_3 * b_1 * b_2}{b_1 * b_2 * b_1 * b_3} = \\ &= \frac{a_1 * b_1 * (a_2 * b_3 + a_3 * b_2)}{b_1^2 * b_2 * b_3} = \frac{a_1 * (a_2 * b_3 + a_3 * b_2)}{b_1 * b_2 * b_3} = \frac{a_1}{b_1} * \frac{a_2 * b_3 + a_3 * b_2}{b_2 * b_3} = \\ &= \frac{a_1}{b_1} * \left(\frac{a_2}{b_2} + \frac{a_3}{b_3} \right) \end{aligned}$$

donc la multiplication est distributive par rapport à l'addition. Ceci montre que $(K, +, \cdot)$ est un anneau.

Supposons que $\frac{a_1}{b_1} \neq 0_K$. Alors $a_1 \neq 0_A$, donc

$$\frac{a_1}{b_1} * \frac{b_1}{a_1} = \frac{a_1 * b_1}{a_1 * b_1} = 1_K$$

donc $\frac{a_1}{b_1}$ admet un inverse. On en conclut que K est un corps.

On définit l'application $\varphi : A \rightarrow K$ par

$$\varphi(a) = \frac{a}{1_A}.$$

On va montrer que φ est un homomorphisme injectif.

Soient $a, b \in A$.

$$\varphi(a) + \varphi(b) = \frac{a}{1_A} + \frac{b}{1_A} = \frac{a * 1_A + b * 1_A}{1_A * 1_A} = \frac{a + b}{1_A} = \varphi(a + b).$$

$$\varphi(a) * \varphi(b) = \frac{a}{1_A} * \frac{b}{1_A} = \frac{a * b}{1_A} = \varphi(a * b).$$

$$\varphi(1_A) = \frac{1_A}{1_A} = 1_K.$$

Ceci montre que φ est un homomorphisme. Soit $a \in \text{Ker}(\varphi)$.

$$\varphi(a) = \frac{a}{1_A} = 0_K = \frac{0_A}{1_A} \Leftrightarrow a = a * 1_A = 0_A * 1_A = 0_A.$$

Ceci montre que φ est injectif.

Soit $x \in K$. Soient $a, b \in A, b \neq 0_A$, tels que $x = \frac{a}{b}$. Alors $b \neq 0_A$ et $b * x = a \in A$. Ceci montre la seconde condition sur K . \square

Définition. Le corps K du théorème 2.22 s'appelle le *corps des fractions* de A et se note $\mathbb{Q}(A)$.

Exemples. Si $A = \mathbb{Z}$, alors $\mathbb{Q}(A) = \mathbb{Q}$. Si $A = \mathbb{R}[x]$, alors $\mathbb{Q}(A) = \mathbb{Q}(x)$. Plus généralement, si $A = \mathbb{R}[x_1, \dots, x_n]$, alors $\mathbb{Q}(A) = \mathbb{R}(x_1, \dots, x_n)$.

Définition. Soient A un anneau et I un idéal de A . On dit que I est un *idéal premier* si, pour tous $x, y \in A$, la condition $x * y \in I$ implique $x \in I$ ou $y \in I$.

Proposition 2.23. *Un idéal I d'un anneau A est premier si et seulement si l'anneau quotient A/I est intègre.*

Démonstration. Supposons que l'anneau quotient A/I est intègre. Soient $x, y \in A$ tels que $x * y \in I$. On a $0 = [x * y] = [x] * [y]$. Comme A/I est intègre, cette égalité implique que $[x] = 0$ ou $[y] = 0$, c'est-à-dire $x \in I$ ou $y \in I$. Ceci montre que I est un idéal premier.

Supposons que I est un idéal premier. Soient $\alpha, \beta \in A/I$ tels que $\alpha * \beta = 0$. On choisit $a, b \in A$ tels que $\alpha = [a]$ et $\beta = [b]$. On a $[a * b] = [a] * [b] = \alpha * \beta = 0$, donc $a * b \in I$. Comme I est premier, il s'en suit que $a \in I$ ou $b \in I$, c'est-à-dire $\alpha = [a] = 0$ ou $\beta = [b] = 0$. Ceci montre que A/I est intègre. \square

Définition. Soient A un anneau et I un idéal de A . On dit que I est un *idéal maximal* s'il est différent de A et s'il n'existe pas d'idéal J différent de I et de A tel que $I \subsetneq J \subsetneq A$.

Proposition 2.24. *Un idéal I d'un anneau A est maximal si et seulement si A/I est un corps.*

Démonstration. Supposons que le quotient A/I est un corps. Soit J un idéal différent de I tel que $I \subsetneq J$. Soit $x \in J, x \notin I$. L'élément $[x]$ est non nul dans A/I , donc est inversible dans A/I . En d'autres termes, il existe $\beta \in A/I$ tel que $[x] * \beta = 1$. Soit $y \in A$ tel que $\beta = [y]$. On a

$$[0_A] = 1 - [x] * \beta = [1_A - x * y],$$

donc $1_A - x * y \in I \subset J$, donc $1_A \in J$ car $x \in J$. Il s'en suit que, pour tout $a \in A$, on a $a = a * 1_A \in J$, donc $J = A$. Ceci montre que I est un idéal maximal.

Supposons que I est un idéal maximal. Notons $\pi : A \rightarrow A/I$ l'homomorphisme quotient. Soit $\beta \in A/I, \beta \neq 0$. Par la proposition 2.15 (1), $J = \pi^{-1}(\langle \beta \rangle)$ est un idéal. Il contient $I = \pi^{-1}(0)$ et est différent de I car $\pi(I) = \{0\} \neq \langle \beta \rangle = \pi(J)$. Comme I est un idéal maximal, cela implique que $A = J$, donc $A/I = \pi(J) = \langle \beta \rangle$. En particulier, $1 \in J = \langle \beta \rangle$,

donc il existe $\beta' \in A/I$ tel que $\beta * \beta' = 1$, donc β est inversible. Ceci montre que A/I est un corps. \square

Théorème 2.25 (Krull - Sans démonstration). *Tout idéal propre d'un anneau A est inclus dans un idéal maximal.*

Corollaire 2.26. *Soient A un anneau et $x \in A$. Alors x est inversible si et seulement s'il n'est contenu dans aucun idéal maximal.*

Démonstration. Supposons que x n'est pas inversible. Par le lemme 2.11, on a $(x) \neq A$, donc, par le théorème 2.25, il existe un idéal maximal M tel que $x \in (x) \subset M$. Supposons que x est inclus dans un idéal maximal, M . Alors $(x) \subset M \neq A$, donc $(x) \neq A$, donc, par le lemme 2.11, x est non inversible. \square

2.3 Anneaux principaux

Définition. Un anneau commutatif A est un *anneau principal* si :

- (a) il est intègre,
- (b) tout idéal I de A est de la forme $I = (x) = \{a * x \mid a \in A\}$ pour un certain $x \in A$.

Lemme 2.27. *L'anneau \mathbb{Z} est principal.*

Démonstration. On sait que \mathbb{Z} est intègre. Par ailleurs, par le lemme 2.6, si I est un idéal de \mathbb{Z} , alors il existe $m \in \mathbb{N}$ tel que $I = m\mathbb{Z} = (m)$. \square

Lemme 2.28. *Soient x, y deux éléments non nuls d'un anneau intègre A . On a $(x) = (y)$ si et seulement s'il existe $u \in \mathcal{U}(A)$ tel que $y = u * x$.*

Démonstration. Supposons que $(x) = (y)$. Comme $y \in (x)$, il existe $u \in A$ tel que $y = u * x$. De même, il existe $v \in A$ tel que $x = v * y$. On a $x = v * y = v * u * x$, donc $(1_A - v * u) * x = 0_A$. Comme $x \neq 0_A$ et A est intègre, il s'en suit que $1_A - v * u = 0_A$, donc $v * u = 1_A$, c'est-à-dire u est inversible.

Supposons qu'il existe $u \in \mathcal{U}(A)$ tel que $y = u * x$. Soit $v \in \mathcal{U}(A)$ tel que $v * u = 1_A$. On a $y = u * x$, donc $y \in (x)$, donc $(y) \subset (x)$. Par ailleurs, $x = 1_A * x = v * u * x = v * y$, donc $x \in (y)$, donc $(x) \subset (y)$. Ceci montre que $(x) = (y)$. \square

Définition. Soit A un anneau. On dit qu'un élément $x \in A$ est *irréductible* si

- (a) x est non nul et n'est pas inversible,
- (b) si $x = u * v$ avec $u, v \in A$, alors u ou v est inversible.

Proposition 2.29. *Soient A un anneau principal et x un élément non nul de A . Les conditions suivantes sont équivalentes :*

- (i) l'élément x est irréductible,

- (ii) l'idéal (x) est premier,
- (iii) l'idéal (x) est maximal.

Démonstration. (iii) \Rightarrow (ii). Si (x) est maximal, alors $A/(x)$ est un corps, donc $A/(x)$ est intègre, donc (x) est premier.

(ii) \Rightarrow (i). On suppose que (x) est un idéal premier. On écrit $x = u * v$ avec $u, v \in A$. On a $x = u * v \in (x)$, donc $u \in (x)$ ou $v \in (x)$ (disons $u \in (x)$). Soit $a \in A$ tel que $u = a * x$. On a $x = u * v = a * x * v$, donc $(1_A - a * v) * x = 0_A$. Comme x est non nul et A est intègre, il s'en suit que $1_A - a * v = 0_A$, donc $a * v = 1_A$, donc v est inversible. Ceci montre que x est irréductible.

(i) \Rightarrow (iii). Supposons que x est irréductible. On va montrer que (x) est maximal. Pour ce faire, par la proposition 2.24, il suffit de montrer que $A/(x)$ est un corps. Soit $\beta \in A/(x)$, $\beta \neq 0$. On choisit $y \in A$ tel que $[y] = \beta$. Remarquez que $y \notin (x)$ car $[y] \neq 0$. Notons $I = (x, y)$ l'idéal engendré par x et y , et choisissons $z \in A$ tel que $I = (z)$. Comme $x, y \in I$, il existe $u, v \in A$ tels que $x = u * z$ et $y = v * z$. Comme x est irréductible, on a $u \in \mathcal{U}(A)$ ou $z \in \mathcal{U}(A)$. Si on avait $u \in \mathcal{U}(A)$, alors, par le lemme 2.28, on aurait $I = (z) = (x)$ et donc $y \in (x)$: contradiction. Donc $z \in \mathcal{U}(A)$. Par lemme 2.11, il s'en suit que $A = I$, donc $1_A \in I$, donc il existe $a, b \in A$ tels que $1_A = a * x + b * y$. Il s'en suit que $1 = [1_A] = [a * x + b * y] = [b] * [y] = [b] * \beta$, donc β est inversible. Ceci montre que $A/(x)$ est un corps. \square

Lemme 2.30. *Considérons une suite croissante d'idéaux dans un anneau principal A :*

$$I_1 \subset I_2 \subset \cdots \subset I_i \subset I_{i+1} \subset \cdots .$$

Il existe un entier N tel que $I_i = I_N$ pour tout $i \geq N$.

Démonstration. Posons $I = \cup_{i=1}^{\infty} I_i$. Montrons d'abord que I est un idéal de A . On a $0_A \in I_1$, donc $0_A \in I$. Soient $x, y \in I$. Il existe $i, j \in \mathbb{N}$ tels que $x \in I_i$ et $y \in I_j$. On peut supposer sans perte de généralité que $i \leq j$. Comme $I_i \subset I_j$, on a alors $x, y \in I_j$, donc $x + y \in I_j$, donc $x + y \in I$. Soit $x \in I$. Il existe $i \in \mathbb{N}$ tel que $x \in I_i$. Alors $-x \in I_i$, donc $-x \in I$. Soient $x \in I$ et $a \in A$. Il existe $i \in \mathbb{N}$ tel que $x \in I_i$. Alors $a * x \in I_i$, donc $a * x \in I$.

On choisit $x \in I$ tel que $I = (x)$. Soit $N \in \mathbb{N}$ tel que $x \in I_N$. Si $i \geq N$, alors $I = (x) \subset I_N \subset I_i \subset I$, donc $I_i = I_N$. \square

Définition. Soient A un anneau (commutatif) et $x, a \in A$. On dit que x *divise* a s'il existe $u \in A$ tel que $a = x * u$. On dit qu'un élément x de A est *premier* si :

- (a) x est non nul et n'est pas inversible,
- (b) si x divise un produit $a * b$, avec $a, b \in A$, alors x divise a ou b .

Lemme 2.31 (Lemme d'Euclide). *Soient A un anneau principal et x un élément de A . Alors x est irréductible si et seulement s'il est premier.*

Démonstration. Supposons que x est premier. Soient $a, b \in A$ tels que $x = a * b$. L'élément x divise le produit $a * b$ et est premier, donc x divise a ou b (disons x divise b). Il existe $u \in A$ tel que $b = x * u$. Alors $x = a * u * x$, donc $(1_A - a * u) * x = 0_A$, donc $1_A - a * u = 0_A$ (car A est intègre), donc $a * u = 1_A$, donc a est inversible. Ceci montre que x est irréductible.

Supposons que x est irréductible. On sait par la proposition 2.29 que (x) est un idéal premier. Soient $a, b \in A$ tels que x divise $a * b$. Alors $a * b \in (x)$, donc $a \in (x)$ ou $b \in (x)$, donc x divise a ou x divise b . Ceci montre que x est premier. \square

Définition. Soit A un anneau. Notons $\text{Irr}(A)$ l'ensemble des éléments irréductibles de A . On définit une relation d'équivalence \sim sur $\text{Irr}(A)$ par :

$$x \sim y \text{ s'il existe } u \in \mathcal{U}(A) \text{ tel que } y = u * x.$$

Un *système de représentants des éléments irréductibles* est une famille $\{x_i \mid i \in \Omega\}$ d'éléments irréductibles telle que pour tout $y \in \text{Irr}(A)$ il existe un unique $i \in \Omega$ tel que $y \sim x_i$.

Théorème 2.32. *Soient A un anneau principal et $\{x_i \mid i \in \Omega\}$ un système de représentants des éléments irréductibles de A . Tout élément non nul x de A s'écrit de façon unique sous la forme*

$$x = u * \prod_{i \in \Omega} x_i^{n_i},$$

avec $u \in \mathcal{U}(A)$, $n_i \in \mathbb{N}$ pour tout $i \in \Omega$, et seul un nombre fini d'entiers n_i sont non nuls. (Cette dernière condition garantit que ce produit est fini et donc est bien défini).

Démonstration. *Existence.* On pose

$$\text{Irr}^*(A) = \{y_1 * \cdots * y_\ell \mid y_i \in \text{Irr}(A) \text{ et } \ell \geq 1\} \cup \mathcal{U}(A) \cup \{0_A\}.$$

On a $\text{Irr}(A) \subset \text{Irr}^*(A)$. De plus, si $a, b \in \text{Irr}^*(A)$, alors $a * b \in \text{Irr}^*(A)$. On va montrer par l'absurde que $A = \text{Irr}^*(A)$.

Supposons que $A \neq \text{Irr}^*(A)$. On définit une suite d'éléments a_k dans $A \setminus \text{Irr}^*(A)$ comme suit. On choisit un élément $a_0 \in A \setminus \text{Irr}^*(A)$ quelconque. Supposons que a_k est défini. Comme a_k n'est ni irréductible ni inversible, il existe deux éléments $a_{k+1}, b_{k+1} \in A$ non inversibles tels que $a_k = a_{k+1} * b_{k+1}$. L'un d'entre eux, disons a_{k+1} , n'appartient pas à $\text{Irr}^*(A)$, sinon a_k lui-même appartiendrait à $\text{Irr}^*(A)$. Posons $I_k = (a_k)$ pour tout $k \in \mathbb{N}$. Comme a_{k+1} divise a_k , on a $I_k \subset I_{k+1}$. De plus, par le lemme 2.28, on a $I_k = (a_k) \neq (a_{k+1}) = I_{k+1}$, car b_{k+1} est non inversible. En d'autres termes, on a la suite croissante d'idéaux

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_k \subsetneq I_{k+1} \subsetneq \cdots.$$

Ceci contredit le lemme 2.30. On en conclue que $A = \text{Irr}^*(A)$.

Soit $x \in A$, $x \neq 0_A$. Si $x = u \in \mathcal{U}(A)$, alors

$$x = u * \prod_{i \in \Omega} x_i^0.$$

On peut donc supposer que x est non inversible. Par ce qui précède, il existe des éléments irréductibles y_1, \dots, y_ℓ tels que $x = y_1 * \dots * y_\ell$. Pour tout $k \in \{1, \dots, \ell\}$, il existe $i_k \in \Omega$ et $u_k \in \mathcal{U}(A)$ tels que $y_k = u_k * x_{i_k}$. On pose $u = u_1 * \dots * u_\ell$. Alors $x = u * x_{i_1} * \dots * x_{i_\ell}$. Pour tout $i \in \Omega$ on note n_i le nombre de $k \in \{1, \dots, \ell\}$ tels que $i = i_k$. Alors

$$x = u * \prod_{i \in \Omega} x_i^{n_i},$$

et les n_i sont presque tous nuls.

Unicité. On suppose que l'on a une égalité

$$u * \prod_{i \in \Omega} x_i^{n_i} = v * \prod_{i \in \Omega} x_i^{m_i},$$

avec $u, v \in \mathcal{U}(A)$. On pose $N = \sup\{\sum_{i \in \Omega} n_i, \sum_{i \in \Omega} m_i\}$ et on montre par récurrence sur N que $u = v$ et $n_i = m_i$ pour tout $i \in \Omega$. Le cas $N = 0$ étant trivial, on suppose que $N \geq 1$ plus l'hypothèse de récurrence. On peut sans perte de généralité supposer que $N = \sum_{i \in \Omega} n_i \geq \sum_{i \in \Omega} m_i$. En particulier, il existe $k \in \Omega$ tel que $n_k \geq 1$. L'élément x_k divise $v * \prod_{i \in \Omega} x_i^{m_i}$ donc, par le lemme 2.31, il existe $i \in \Omega$ tel que $m_i \geq 1$ et x_k divise x_i . Mais, x_k divise x_i que si $k = i$, donc $m_k \geq 1$. Posons

$$n'_i = \begin{cases} n_i & \text{si } i \neq k \\ n_k - 1 & \text{si } i = k \end{cases} \quad m'_i = \begin{cases} m_i & \text{si } i \neq k \\ m_k - 1 & \text{si } i = k \end{cases}$$

Alors

$$u * \prod_{i \in \Omega} x_i^{n'_i} = v * \prod_{i \in \Omega} x_i^{m'_i},$$

donc, par hypothèse de récurrence, $u = v$ et $n'_i = m'_i$, c'est-à-dire $n_i = m_i$, pour tout $i \in \Omega$. \square

Définition. Soient A un anneau principal et $a, b \in A$. Un *pgcd* de a et b est un générateur de (a, b) , et un *ppcm* de a et b est un générateur de $(a) \cap (b)$.

Lemme 2.33. Soient A un anneau principal et a, b deux éléments non nuls de A .

- (1) Soit m un pgcd de a et b . Alors m divise a et b . De plus, si un élément non nul d de A divise a et b , alors d divise m .
- (2) Soit M un ppcm de a et b . Alors a et b divisent M . De plus, si a et b divisent un élément d de A , alors M divise d .

Démonstration. Comme $a \in (a, b) = (m)$, m divise a . De même, m divise b . Supposons que d divise a et b . Alors $a, b \in (d)$, donc $(m) = (a, b) \subset (d)$, donc $m \in (d)$, donc d divise m .

On a $M \in (a)$, donc a divise M . De même, b divise M . Supposons que a et b divisent d . Alors $d \in (a) \cap (b) = (M)$, donc M divise d . \square

Lemme 2.34 (Identité de Bézout). *Soient A un anneau principal, a, b deux éléments non nuls de A , et m un pgcd de a et b . Il existe $x, y \in A$ tels que $m = x * a + y * b$.*

Démonstration. Comme $m \in (m) = (a, b)$, il existe $x, y \in A$ tels que $m = x * a + y * b$. \square

Lemme 2.35. *Soient A un anneau principal et $\{x_i \mid i \in \Omega\}$ un système de représentants des éléments irréductibles de A . Soient $a, b \in A$ que l'on écrit $a = u * \prod_{i \in \Omega} x_i^{n_i}$ et $b = v * \prod_{i \in \Omega} x_i^{m_i}$ avec $u, v \in \mathcal{U}(A)$. Alors a divise b si et seulement si $n_i \leq m_i$ pour tout $i \in \Omega$.*

Démonstration. Supposons que a divise b . Soit $c \in A$ tel que $b = a * c$. On écrit $c = w * \prod_{i \in \Omega} x_i^{k_i}$ avec $w \in \mathcal{U}(A)$. Alors $b = a * c = u * w * \prod_{i \in \Omega} x_i^{n_i + k_i}$. Par le théorème 2.32, il s'en suit que $m_i = n_i + k_i$, donc que $n_i \leq m_i$, pour tout $i \in \Omega$.

Supposons que $n_i \leq m_i$ pour tout $i \in \Omega$. Posons $k_i = m_i - n_i$ pour tout $i \in \Omega$, et $c = v * u^{-1} * \prod_{i \in \Omega} x_i^{k_i}$. Alors $a * c = u * v * u^{-1} * \prod_{i \in \Omega} x_i^{n_i + k_i} = v * \prod_{i \in \Omega} x_i^{m_i} = b$, donc a divise b . \square

Corollaire 2.36. *Soient A un anneau principal et $\{x_i \mid i \in \Omega\}$ un système de représentants des éléments irréductibles de A . Soient $a, b \in A$ que l'on écrit $a = u * \prod_{i \in \Omega} x_i^{n_i}$ et $b = v * \prod_{i \in \Omega} x_i^{m_i}$ avec $u, v \in \mathcal{U}(A)$.*

- (1) $\prod_{i \in \Omega} x_i^{\min(n_i, m_i)}$ est un pgcd de a et b .
- (2) $\prod_{i \in \Omega} x_i^{\max(n_i, m_i)}$ est un ppcm de a et b .

Démonstration. Exercice. \square

Définition. Un anneau commutatif intègre A est un *anneau euclidien* s'il existe une application $s : A \setminus \{0_A\} \rightarrow \mathbb{N}$ telle que :

pour tous $x, y \in A$, $y \neq 0$, il existe $q, r \in A$ tels que $x = q * y + r$ et $r = 0_A$ ou $s(r) < s(y)$.

L'élément r ci-dessus est appelé *reste de la division* de x par y .

Exemple.

- (1) \mathbb{Z} est euclidien en prenant $s(x) = |x|$.
- (2) $\mathbb{R}[X]$ est euclidien en prenant $s(P) = \deg(P)$.

Proposition 2.37. *Un anneau euclidien est principal.*

Démonstration. Soit I un idéal de A différent de $\{0_A\}$. On choisit un élément non nul y de I tel que $s(y)$ soit minimal. Comme $y \in I$, on a $(y) \subset I$. Soit $x \in I$. Il existe $q, r \in A$ tels que $x = q * y + r$ et $r = 0_A$ ou $s(r) < s(y)$. Comme $r = x - q * y \in I$ et $s(y)$ est minimal, on a $r = 0_A$, donc $x = q * y \in (y)$. Ceci montre que $I \subset (y)$. \square

Lemme 2.38. *Soient A un anneau euclidien et a, b deux éléments non nuls de A . Soient $q, r \in A$ tels que $a = q * b + r$ et $r = 0_A$ ou $s(r) < s(b)$. Si $r \neq 0_A$ et m est un pgcd de b et r , alors m est un pgcd de a et b .*

Démonstration. Supposons que $r \neq 0_A$. On a $r = a - q * b \in (a, b)$ et $b \in (a, b)$, donc $(r, b) \subset (a, b)$. Par ailleurs, $a = q * b + r \in (b, r)$ et $b \in (b, r)$, donc $(a, b) \subset (b, r)$. Soit m un pgcd de b et r . Alors $(m) = (b, r) = (a, b)$, donc m est un pgcd de a et b . \square