HAX501X – Groupes et anneaux 1

Clément Dupont
Université de Montpellier
2024-2025

Table des matières

Chapitre 1

Rappels d'arithmétique des entiers

1.1 Addition et multiplication des entiers relatifs

1.1.1 $\mathbb{Z}$ est un groupe abélien

L'ensemble $\mathbb{Z}$, muni de la loi $+$ de l'addition, est un **groupe**. Cela veut dire qu'on a les propriétés suivantes.

1) Associativité de $+$: $\forall a, b, c \in \mathbb{Z}\,,\ (a+b)+c = a+(b+c)$.

2) Élément neutre pour $+$: 0 est l'élément neutre, c'est-à-dire que $\forall a \in \mathbb{Z}\,,\ a+0 = a = 0+a$.

3) Inverse pour $+$: pour tout $a \in \mathbb{Z}$ il existe $b \in \mathbb{Z}$ tel que $a+b = 0 = b+a$. Il est appelé l'opposé de a et noté $-a$.

Comme la loi $+$ est commutative, on dit que $\mathbb{Z}$ est un **groupe abélien**[1].

4) Commutativité de $+$: $\forall a, b \in \mathbb{Z}\,,\ a+b = b+a$.

1.1.2 $\mathbb{Z}$ est un anneau commutatif

L'ensemble $\mathbb{Z}$, muni des lois $+$ et $\times$, est un **anneau**. Cela veut dire qu'on a les propriétés suivantes.

1) $(\mathbb{Z}, +)$ est un groupe abélien.

2) Associativité de $\times$: $\forall a, b, c \in \mathbb{Z}\,,\ (a \times b) \times c = a \times (b \times c)$.

3) Élément neutre pour $\times$: 1 est l'élément neutre, c'est-à-dire que $\forall a \in \mathbb{Z}\,,\ a \times 1 = a = 1 \times a$.

4) Distributivité de $\times$ par rapport à $+$: $\forall a, b, c \in \mathbb{Z}\,,\ a \times (b+c) = (a \times b) + (a \times c)$ et $(a+b) \times c = (a \times c) + (b \times c)$.

Comme la loi $\times$ est commutative, on dit que $\mathbb{Z}$ est un **anneau commutatif**[2].

5) Commutativité de $\times$: $\forall a, b \in \mathbb{Z}\,,\ a \times b = b \times a$.

[1] Ainsi nommés en l'honneur du mathématicien norvégien Niels Henrik Abel (1802-1829). Il est traditionnel d'utiliser l'adjectif "abélien" plutôt que "commutatif" pour les groupes.

[2] Pour les anneaux on utilise "commutatif"... c'est comme ça !

1.2 Divisibilité, division euclidienne, congruences

1.2.1 Divisibilité

Définition 1.2.1. *Soient $a, b \in \mathbb{Z}$. On dit que a* **divise** *b et on note*

$$a|b$$

s'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit aussi que a est un **diviseur** *de b, ou que b est* **divisible** *par a ou est un* **multiple** *de a.*

Exercice 1. Pour $n \in \mathbb{Z}$, quand a-t-on $1|n$? $n|1$? $0|n$? $n|0$?

On utilise tout le temps les propriétés suivantes de la divisibilité.

Proposition 1.2.2. *Pour $a, b, c \in \mathbb{Z}$ on a :*

1) Si $a|b$ et $b \neq 0$ alors $|a| \leqslant |b|$;

2) $a|a$;

3) si $a|b$ et $b|a$, alors $a = \pm b$;

4) transitivité de la divisibilité : si $a|b$ et $b|c$, alors $a|c$.

Démonstration. 1) Supposons que $a|b$ et $b \neq 0$. Alors on peut écrire $b = ak$ avec $k \in \mathbb{Z}$. De plus, comme $b \neq 0$, on a nécessairement $k \neq 0$, donc $|k| \geqslant 1$, et donc $|b| = |a| \times |k| \geqslant |a|$.

2) C'est clair car $a = a \times 1$.

3) Supposons que $a|b$ et $b|a$. On procède par disjonction de cas.

- Cas $a = 0$. Comme $a|b$ on peut écrire $b = an$ avec $n \in \mathbb{Z}$, et donc $b = 0 = a$.
- Cas $b = 0$. Le même raisonnement donne $a = 0 = b$.
- Cas $a \neq 0$ et $b \neq 0$. D'après 1) on a $|a| \leqslant |b|$ et $|b| \leqslant |a|$, d'où $|a| = |b|$, c'est-à-dire $a = \pm b$.

4) Supposons que $a|b$ et que $b|c$. Alors on peut écrire $b = am$ et $c = bn$ avec $m, n \in \mathbb{Z}$. On a donc $c = amn$, et comme $mn \in \mathbb{Z}$, a divise c.

□

Remarque 1.2.3. Par le point 1) de la proposition, un entier non nul a un nombre fini de diviseurs.

On utilise tout le temps la proposition suivante.

Proposition 1.2.4. *Si $n|a$ et $n|b$ alors pour tous $u, v \in \mathbb{Z}$, $n|(au + bv)$.*

Démonstration. Par hypothèse on peut écrire $a = nk$ et $b = nl$ avec $k, l \in \mathbb{Z}$. On a donc $au + bv = nku + nlv = n(ku + lv)$. Comme $ku + lv \in \mathbb{Z}$ on a donc que n divise $au + bv$. □

1.2.2 Nombres premiers

Définition 1.2.5. *Un* **nombre premier** *est un entier naturel p qui a exactement deux diviseurs positifs distincts : 1 et p. Un entier naturel $n \geqslant 2$ qui n'est pas premier est dit* **composé**.

Dit autrement, pour $n \in \mathbb{N}$:

▷ n est premier si et seulement si $n \neq 0, 1$ et pour tous $a, b \in \mathbb{N}$,

$$n = ab \quad \Longrightarrow \quad a = n \quad \text{ou} \quad b = n.$$

▷ n est composé si et seulement s'il existe une factorisation

$$n = ab \qquad \text{avec} \;\; 1 < a < n \;\; \text{et} \;\; 1 < b < n.$$

Clairement, 0 n'est pas premier puisqu'il a une infinité de diviseurs ; 1 n'est pas premier car il n'a qu'un seul diviseur positif, qui est lui-même. Le plus petit nombre premier est donc 2. C'est aussi le seul nombre premier pair.

Voici la liste des nombres premiers inférieurs à 100 :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Voici la liste des nombres premiers entre 9.999.900 et 10.000.000 :

$$9.999.901, 9.999.907, 9.999.929, 9.999.931, 9.999.937, 9.999.943, 9.999.971, 9.999.973, 9.999.991,$$

et entre 10.000.000 et 10.000.100 :

$$10.000.019, 10.000.079.$$

Proposition 1.2.6. *Soit $n \in \mathbb{Z}$ tel que $|n| \geqslant 2$. Alors le plus petit diviseur > 1 de n est un nombre premier. En particulier, n est divisible par un nombre premier.*

Démonstration. L'ensemble des diviseurs > 1 de n est une partie non vide de $\mathbb{N}$, car $|n|$ divise n et $|n| > 1$. Cet ensemble a donc un plus petit élément qu'on note a. Comme les diviseurs de a sont des diviseurs de n (par transitivité de la divisibilité), le plus petit diviseur > 1 de a est a lui-même. Conclusion : les seuls diviseurs positifs de a sont 1 et a, donc a est premier. □

Proposition 1.2.7. *Tout entier relatif non nul peut s'écrire, au signe près, comme un produit de nombres premiers. Dit autrement, pour tout $n \in \mathbb{Z} \setminus \{0\}$, il existe un entier $r \in \mathbb{N}$ et des nombres premiers $p_1, p_2, \ldots, p_r$ tels que*

$$n = \pm p_1 p_2 \cdots p_r.$$

Démonstration. Clairement, il suffit de traiter le cas où $n \in \mathbb{N}^*$. On procède par récurrence forte.

– Pour tout $n \in \mathbb{N}^*$ considérons l'assertion $P(n)$: "n peut s'écrire comme un produit de nombres premiers".

– Initialisation : $P(1)$ est vraie car 1 peut s'écrire comme un produit indexé par l'ensemble vide (c'est le cas où $r = 0$).

– Hérédité : soit $n \geqslant 2$ tel que $P(k)$ est vraie pour tout entier $k \in \{1, \dots, n-1\}$, et montrons que $P(n)$ est vraie. Par la proposition 1.2.6, il existe un nombre premier p qui divise n. On écrit $n = pk$, et comme $p > 1$ on a $1 \leqslant k < n$. Par $P(k)$ on peut écrire k comme produit de nombres premiers, et donc $n = pk$ peut s'écrire comme un produit de nombres premiers. Donc $P(n)$ est vraie.

– Conclusion : on a donc montré que $P(n)$ est vraie pour tout $n \in \mathbb{N}^*$.

□

▷ Il n'est **pas du tout évident** a priori que la décomposition d'un nombre en produit de nombre premiers est unique ! C'est pourtant vrai, mais on a besoin de développer un résultat intermédiaire (le lemme d'Euclide) pour le démontrer.

Le premier théorème de structure sur l'ensemble des nombres premiers est le résultat suivant dû à Euclide[3].

Théorème 1.2.8 (Théorème d'Euclide sur les nombres premiers). *L'ensemble des nombres premiers est infini.*

Démonstration. On procède par l'absurde. Supposons que l'ensemble des nombres premiers et fini et listons tous les nombres premiers : $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \dots, p_n$. Considérons l'entier naturel $N = p_1 p_2 \cdots p_n + 1$. Par la proposition 1.2.6, N est divisible par un nombre premier, donc il existe un indice $i \in \{1, \dots, n\}$ tel que $p_i | N$. Or, comme $p_i | p_1 p_2 \cdots p_n$, on a donc que $p_i | (N - p_1 p_2 \cdots p_n) = 1$ et donc $p_i = 1$, ce qui est absurde. On a donc montré que l'ensemble des nombres premiers est infini. □

Remarque 1.2.9. Une question naturelle, une fois qu'on sait qu'il y a une infinité de nombres premiers, est d'essayer de *quantifier* leur répartition parmi tous les entiers naturels. Pour cela, on veut estimer la **fonction de compte des nombres premiers**

$$\pi(n) = |\{\text{nombres premiers } p \leqslant n\}|,$$

et plus précisément comprendre comment la fonction $\pi(n)$ se comporte quand n est grand. En étudiant des tables de nombres premiers, le mathématicien allemand Carl Friedrich Gauss a conjecturé autour de 1793 (à l'âge de 16 ans !) l'équivalent suivant :

$$\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}.$$

(Dit autrement, le quotient $\pi(n)/n$ est équivalent à $1/\ln(n)$: si l'on choisit un nombre au hasard entre 1 et n avec n grand, on a environ 1 chance sur $\ln(n)$ qu'il soit premier.) L'équivalent conjecturé par Gauss fut prouvé indépendamment par le mathématicien français Jacques Hadamard et le mathématicien belge Charles Jean de la Vallée Poussin en 1896. On l'appelle aujourd'hui le **théorème des nombres premiers**. Sa preuve repose sur l'étude de la **fonction zêta**, introduite par le mathématicien allemand Bernhard

[3] Peu de choses précises sont connues de la vie d'Euclide, qui aurait vécu vers 300 avant notre ère.

Riemann en 1859 :

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \cdot$$

Il s'agit d'une fonction définie sur $\mathbb{C}$ et à valeurs dans $\mathbb{C}$, et son étude requiert les techniques de l'**analyse complexe**. Un des problèmes ouverts les plus connus des mathématiques, l'**hypothèse de Riemann**, est une conjecture sur la fonction zêta qui impliquerait une estimation très précise de la répartition des nombres premiers.

1.2.3 Division euclidienne

Théorème 1.2.10 (Division euclidienne). *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Il existe un unique couple (q, r) d'entiers relatifs avec $0 \leqslant r < |b|$ tels qu'on ait l'égalité*

$$a = bq + r.$$

On remarque que q détermine r (car $r = a - bq$) et que r détermine q (car $q = \frac{a-r}{b}$).

Démonstration. 1) On traite d'abord l'unicité. Supposons qu'il existe deux couples d'entiers relatifs (q, r) et (q', r') avec $0 \leqslant r < |b|$ et $0 \leqslant r' < |b|$, qui vérifient $a = bq + r$ et $a = bq' + r'$. Alors $bq + r = bq' + r'$ et donc $r - r' = b(q' - q)$.

Comme $0 \leqslant r < |b|$ et $0 \leqslant r' < |b|$ on a que $-|b| < r - r' < |b|$, d'où $|r - r'| < |b|$. Donc $|b(q' - q)| < |b|$, ce qui s'écrit $|b| \times |q' - q| < |b|$, et donc en multipliant par $\frac{1}{|b|}$: $|q' - q| < 1$. Or $q' - q$ est un entier, donc $q' - q = 0$ et $q = q'$. En remplaçant dans $bq + r = bq' + r'$, on obtient alors $r = r'$.

2) On traite maintenant l'existence.

– Traitons d'abord le cas où $b > 0$. Introduisons la partie

$$A = \{a - bk\,,\, k \in \mathbb{Z}\} \cap \mathbb{N}.$$

C'est une partie non vide de $\mathbb{N}$. En effet, si $a \geqslant 0$ alors $a = a - b0 \in A$; et si $a < 0$ alors $a - ba = a(1 - b) \in A$ car $a < 0$ et $1 - b \leqslant 0$. Donc A a un plus petit élément qu'on note r. Il existe donc $k \in \mathbb{Z}$ tel que $a - bk = r$, c'est-à-dire $a = bk + r$. On a évidemment $r \geqslant 0$, et il reste à montrer que $r < b$.
Procédons par l'absurde et supposons que $r \geqslant b$. Alors

$$a - b(k + 1) = a - bk - b = r - b \geqslant 0$$

et l'élément $r - b$ est donc dans A. Or, $r - b < r$ car $b > 0$, ce qui contredit le fait que r est le plus petit élément de A. On a donc montré par l'absurde que $r < b$.

– Dans le cas où $b < 0$, on applique ce qu'on vient de voir à $-b$, ce qui donne l'existence d'un couple (q, r) d'entiers relatifs avec $0 \leqslant r < |-b|$ et $a = (-b)q + r$. On a donc $a = b(-q) + r$ et $0 \leqslant r < |b|$.

□

Définition 1.2.11. *On appelle l'égalité $a = bq + r$ la* **division euclidienne** *de a par b, q le* **quotient** *et r le* **reste**.

Exercice 2. Calculer la division euclidienne de 1767 par 18.

Remarque 1.2.12. On a : $b|a \iff$ le reste dans la division euclidienne de a par b est 0.

1.2.4 Congruences

Définition 1.2.13. *Soit $n \in \mathbb{N}$. On dit que deux entiers relatifs $a, b \in \mathbb{Z}$ sont* **congrus modulo** *n et on note*

$$a \equiv b \pmod{n}$$

si n divise la différence $a - b$, c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Proposition 1.2.14. *La relation de congruence modulo n est une* **relation d'équivalence** *sur l'ensemble $\mathbb{Z}$, c'est-à-dire qu'on a les propriétés suivantes.*

1) Réflexivité : $\forall a \in \mathbb{Z}\,,\ a \equiv a \pmod{n}$.

2) Symétrie : $\forall a, b \in \mathbb{Z}\,,\ a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$.

3) Transitivité : $\forall a, b, c \in \mathbb{Z}\,,\ (a \equiv b \pmod{n} \text{ et } b \equiv c \pmod{n}) \implies a \equiv c \pmod{n}$.

Démonstration. 1) Réflexivité. Clairement, pour tout $a \in \mathbb{Z}$ on a $a \equiv a \pmod{n}$ puisque n divise $a - a = 0$.

2) Symétrie. Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$. Alors n divise $a - b$ et donc n divise $-(a - b) = b - a$, d'où $b \equiv a \pmod{n}$.

3) Transivité. Soient $a, b, c \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Alors n divise $a - b$ et $b - c$, donc n divise la somme $(a - b) + (b - c) = a - c$, d'où $a \equiv c \pmod{n}$. □

Remarque 1.2.15. La relation de congruence modulo 0 est un peu spéciale : $a \equiv b \pmod{0}$ si et seulement si $a = b$. La relation de congruence modulo 1 aussi : $a \equiv b \pmod{1}$ est vrai pour tous $a, b \in \mathbb{Z}$.

Dans toute la suite on fixe $n \in \mathbb{N}^*$.

Proposition 1.2.16. – *Pour tout $a \in \mathbb{Z}$, il existe un unique $r \in \{0, \dots, n-1\}$, qui est le reste dans la division euclidienne de a par n, tel que $a \equiv r \pmod{n}$.*

– *Par conséquent, pour $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans la division euclidienne par n.*

Démonstration. – C'est le théorème de division euclidienne (théorème 1.2.10).

– Pour $a, b \in \mathbb{Z}$, soient r et s les restes respectifs dans la division euclidienne de a et b par n. On a $a \equiv r \pmod{n}$ et $b \equiv s \pmod{n}$, et donc (en utilisant la symétrie et la transitivité de la relation de congruence), $a \equiv b \pmod{n} \iff r \equiv s \pmod{n}$, ce qui équivaut, par la première partie de la proposition, à $r = s$. □

La relation de congruence modulo n est compatible à la somme et au produit des entiers.

Proposition 1.2.17. *Soient $a, b \in \mathbb{Z}$. Si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$ alors on a :*

1) $a + a' \equiv b + b' \pmod{n}$;

2) $aa' \equiv bb' \pmod{n}$.

Démonstration. Par hypothèse, il existe $k, k' \in \mathbb{Z}$ tels que $a = b + kn$ et $a' = b' + k'n$.

1) On a donc $a + a' = b + kn + b' + k'n = b + b' + (k + k')n$, donc $a + a' \equiv b + b' \pmod{n}$.

2) On a aussi $aa' = (b+kn)(b'+k'n) = bb' + bk'n + b'kn + kk'n^2 = bb' + (bk' + b'k + kk'n)n$, donc $aa' \equiv bb' \pmod{n}$.

□

Remarque 1.2.18. De ces propriétés on en déduit facilement d'autres, par exemple :

- Si $a \equiv b \pmod{n}$, alors pour tout $c \in \mathbb{Z}$ on a $a+c \equiv b+c \pmod{n}$ et $ac \equiv bc \pmod{n}$. (En utilisant le fait qu'on a $c \equiv c \pmod{n}$).
- Si $a \equiv b \pmod{n}$, alors pour tout $k \in \mathbb{N}$ on a $a^k \equiv b^k \pmod{n}$. (Par récurrence sur k en utilisant la compatibilité de la relation de congruence au produit.)

Exercice 3. Pour quels entiers k a-t-on $k^2 \equiv 2 \pmod{6}$?

1.2.5 Inversion modulo un entier

Définition 1.2.19. *On dit qu'un $a \in \mathbb{Z}$ est* **inversible modulo** *n s'il existe $b \in \mathbb{Z}$ tel que*

$$ab \equiv 1 \pmod{n}.$$

On dit alors que b est **un inverse de** *a* **modulo** *n.*

▷ Clairement, on ne parle pas de **l'**inverse de a modulo n puisqu'il n'y a pas unicité : si b est un inverse de a modulo n, alors tout b' qui est congru à b modulo n l'est aussi. (Prouvez-le !) La proposition suivante montre que ce sont les seuls. Dit autrement, un inverse modulo n est unique... modulo n.

Proposition 1.2.20. *Si $b, b' \in \mathbb{Z}$ sont deux inverses de a modulo n alors $b \equiv b' \pmod{n}$.*

Démonstration. En multipliant des deux côtés la congruence $ab \equiv 1 \pmod{n}$ par b' on obtient $abb' \equiv b' \pmod{n}$. En multipliant des deux côtés la congruence $ab' \equiv 1 \pmod{n}$ par b on obtient $abb' \equiv b \pmod{n}$. Comme la relation de congruence modulo n est symétrique et transitive, on en conclut que $b \equiv b' \pmod{n}$. □

Proposition 1.2.21. *Soit $a \in \mathbb{Z}$ un entier inversible modulo n, et soit $b \in \mathbb{Z}$ un inverse de a. Alors on a, pour tous $x, y \in \mathbb{Z}$, l'équivalence :*

$$ax \equiv y \pmod{n} \iff x \equiv by \pmod{n}.$$

Démonstration. $\Longrightarrow$: En multipliant des deux côtés par b on obtient $abx \equiv by \pmod{n}$. D'autre part, comme $ab \equiv 1 \pmod{n}$ par hypothèse, on a en multipliant des deux côtés par x : $abx \equiv x \pmod{n}$. Comme la relation de congruence modulo n est symétrique et transitive, on en conclut que $x \equiv by \pmod{n}$.

$\Longleftarrow$: Même démonstration en multipliant des deux côtés par a.

□

1.3 PGCD et PPCM

1.3.1 Sous-groupes de $\mathbb{Z}$

Définition 1.3.1. *Un* **sous-groupe de** $\mathbb{Z}$ *est un sous-ensemble* $H \subset \mathbb{Z}$ *qui vérifie les conditions suivantes :*

1) $0 \in H$ *;*

2) H *est stable par somme :* $\forall a, b \in H,\ a + b \in H$ *;*

3) H *est stable par passage à l'opposé :* $\forall a \in H,\ -a \in H$*.*

Proposition 1.3.2. *Soit* H *un sous-groupe de* $\mathbb{Z}$*. Pour* $a \in H$ *et* $k \in \mathbb{Z}$*, on a :* $ka \in H$*.*

Démonstration. On traite d'abord le cas $k \in \mathbb{N}$, par récurrence.

– Pour tout $k \in \mathbb{N}$ considérons l'assertion $P(k)$: "$ka \in H$".

– Initialisation : $P(0)$ est vraie car par la condition 1), $0a = 0 \in H$.

– Hérédité : soit $k \in \mathbb{N}$ tel que $P(k)$ est vraie, et montrons que $P(k+1)$ est vraie. Par $P(k)$ on a que $ka \in H$. Or, $a \in H$, donc par la condition 2), $ka + a \in H$, c'est-à-dire $(k+1)a \in H$. Donc $P(k+1)$ est vraie.

– Conclusion : on a donc montré par récurrence que $P(k)$ est vraie pour tout $k \in \mathbb{N}$.

Maintenant, pour $k \in \mathbb{Z}$ avec $k < 0$, on peut écrire $ka = -(-k)a$. Par ce qu'on vient de voir, $(-k)a \in H$ puisque $-k \in \mathbb{N}$. Par la condition 3), on en conclut que $ka = -(-ka) \in H$. □

Proposition 1.3.3. *Pour tout entier naturel* n*, l'ensemble*

$$n\mathbb{Z} = \{nk\,,\ k \in \mathbb{Z}\}$$

est un sous-groupe de $\mathbb{Z}$*.*

▷ Dans la suite du cours on l'appellera le **sous-groupe de** $\mathbb{Z}$ **engendré par** n.

▷ Notons que $n\mathbb{Z}$ est l'ensemble des multiples de n : pour $a \in \mathbb{Z}$ on a :

$$a \in n\mathbb{Z} \quad \Longleftrightarrow \quad n|a.$$

Démonstration. On vérifie facilement les trois conditions :

1) $0 \in n\mathbb{Z}$ puisque $n|0$.

2) Soient $a, b \in n\mathbb{Z}$. Alors $n|a$ et $n|b$, donc $n|(a+b)$ et donc $a + b \in n\mathbb{Z}$.

3) Soit $a \in n\mathbb{Z}$. Alors $n|a$, donc $n| - a$ et donc $-a \in n\mathbb{Z}$.

□

Théorème 1.3.4. *Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration. – Commençons par l'unicité. Soient $m, n \in \mathbb{N}$ tels que $m\mathbb{Z} = n\mathbb{Z}$. Comme $m \in m\mathbb{Z}$, on a donc $m \in n\mathbb{Z}$ et donc $n|m$. De même, comme $n \in n\mathbb{Z}$ on a $n \in m\mathbb{Z}$ et donc $m|n$. Comme m et n sont $\geqslant 0$, on a donc $m = n$.

– Démontrons maintenant l'existence. Soit H un sous-groupe de $\mathbb{Z}$. D'après la condition 1) on a $0 \in H$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. On suppose donc maintenant que $H \neq \{0\}$, c'est-à-dire qu'il existe $a \in H$ tel que $a \neq 0$. Comme $-a \in H$ par la condition 3), on peut choisir un tel a qui soit > 0. Ainsi, $H \cap \mathbb{N}^*$ est non vide et on peut donc définir

$$n = \min(H \cap \mathbb{N}^*).$$

C'est le plus petit élément de H qui est $\geqslant 1$. On montre qu'on a $H = n\mathbb{Z}$.

▷ Comme $n \in H$, la proposition 1.3.2 implique que $n\mathbb{Z} \subset H$.

▷ Montrons que $H \subset n\mathbb{Z}$. Soit $a \in H$, et écrivons la division euclidienne de a par n sous la forme :

$$a = nq + r \qquad \text{avec } 0 \leqslant r < n.$$

Comme $n \in H$, la proposition 1.3.2 implique que $-nq \in H$. Comme $a \in H$, la condition 2) implique alors que $a - nq \in H$, d'où $r \in H$. On ne peut pas avoir $r \neq 0$ puisque on aurait alors $r \in H \cap \mathbb{N}^*$ et $r < n$, ce qui contredirait le fait que $n = \min(H \cap \mathbb{N}^*)$. Donc $r = 0$ et donc $a = nq \in n\mathbb{Z}$. On a donc bien montré que $H \subset n\mathbb{Z}$.

□

Définition 1.3.5. *On appelle n le* **générateur positif** *de $H = n\mathbb{Z}$.*

Exercice 4. Soient deux entiers naturels m, n. Montrer qu'on a l'équivalence :

$$m\mathbb{Z} \subset n\mathbb{Z} \iff n|m.$$

1.3.2 Le PGCD

Proposition 1.3.6. *Soient $a, b \in \mathbb{Z}$. L'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + bv\,,\ u, v \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.*

Démonstration. On vérifie facilement les trois conditions :

1) $0 \in a\mathbb{Z} + b\mathbb{Z}$ car $0 = a \times 0 + b \times 0$.

2) Soient $n, n' \in a\mathbb{Z}+b\mathbb{Z}$. Il existe alors $u, u', v, v' \in \mathbb{Z}$ tels que $n = au+bv$ et $n' = au'+bv'$. Alors $n + n' = au + bv + au' + bv' = a(u + u') + b(v + v')$ et donc $n + n' \in a\mathbb{Z} + b\mathbb{Z}$ car $u + u', v + v' \in \mathbb{Z}$.

3) Soient $n \in a\mathbb{Z}+b\mathbb{Z}$. Il existe alors $u, v \in \mathbb{Z}$ tels que $n = au+bv$. Alors $-n = -au-bv = a(-u) + b(-v)$ et donc $-n \in a\mathbb{Z} + b\mathbb{Z}$ car $-u, -v \in \mathbb{Z}$.

□

Définition 1.3.7. *Le générateur positif de $a\mathbb{Z}+b\mathbb{Z}$ est appelé le* **plus grand commun diviseur (PGCD)** *de a et b. On le note* $\mathrm{PGCD}(a,b)$ *ou* $a\wedge b$.

On a donc :

$$a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z}.$$

Proposition 1.3.8. *On a les propriétés suivantes, pour $a,b\in\mathbb{Z}$:*

1) $b\wedge a=a\wedge b$.

2) $(-a)\wedge b=a\wedge b$.

3) si $a\in\mathbb{N}$ *alors* $a\wedge a=a$.

4) Pour tout $k\in\mathbb{N}$ *alors* $(ka)\wedge(kb)=k(a\wedge b)$.

Démonstration. 1) C'est une conséquence du fait que $b\mathbb{Z}+a\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$. (Vérifiez-le !)

2) C'est une conséquence du fait que $(-a)\mathbb{Z}+b\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$. (Vérifiez-le !)

3) C'est une conséquence du fait que $a\mathbb{Z}+a\mathbb{Z}=a\mathbb{Z}$. (Vérifiez-le !)

4) On a $(ka)\mathbb{Z}+(kb)\mathbb{Z}=k(a\mathbb{Z}+b\mathbb{Z})=k(a\wedge b)\mathbb{Z}$. (Vérifiez chacune de ces deux égalités !) □

Remarque 1.3.9. Grâce au point 2) de la proposition ci-dessus, on se permettra d'énoncer certains résultats sur le PGCD seulement dans le cas des entiers naturels, pour simplifier.

La proposition suivante est un outil précieux pour le calcul du PGCD.

Proposition 1.3.10. *Pour $a,b,k\in\mathbb{Z}$ on a :* $(a+kb)\wedge b=a\wedge b$.

Démonstration. Cela revient à montrer l'égalité : $(a+kb)\mathbb{Z}+b\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$.

$\subset$: Soit $n\in(a+kb)\mathbb{Z}+b\mathbb{Z}$. Il existe $u,v\in\mathbb{Z}$ tels que $n=(a+kb)u+bv=au+b(ku+v)$. Comme $u,ku+v\in\mathbb{Z}$, on a donc $n\in a\mathbb{Z}+b\mathbb{Z}$.

$\supset$: Soit $n\in a\mathbb{Z}+b\mathbb{Z}$. Il existe $u,v\in\mathbb{Z}$ tels que $n=au+bv$. On force l'apparition de $a+kb$ en écrivant : $n=(a+kb-kb)u+bv=(a+kb)u+b(-ku+v)$. Comme $u,-ku+v\in\mathbb{Z}$, on a donc $n\in(a+kb)\mathbb{Z}+b\mathbb{Z}$.

□

▷ Dit autrement : le PGCD de a et b ne change pas si on remplace a par $a+kb$.

▷ C'est un analogue d'une **opération élémentaire** pour un système linéaire :

$$\begin{cases}A=0\\B=0\end{cases}\quad\Longleftrightarrow\quad\begin{cases}A+KB=0\\B=0\end{cases}$$

La terminologie de "plus grand commun diviseur" est expliquée par la proposition suivante.

Proposition 1.3.11. *Soient $a, b \in \mathbb{Z}$. Alors $a \wedge b$ est l'unique $d \in \mathbb{N}$ qui vérifie les deux conditions suivantes :*

1) $d|a$ et $d|b$;

2) pour tout $e \in \mathbb{N}$, $(e|a$ et $e|b) \Longrightarrow e|d$.

Démonstration. On montre d'abord que $a \wedge b$ vérifie les conditions 1) et 2).

1) Comme $a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, on a que $(a \wedge b)|a$. Par le même raisonnement, $(a \wedge b)|b$.

2) Soit $e \in \mathbb{N}$ tel que $e|a$ et $e|b$. Alors pour tous $u, v \in \mathbb{Z}$ on a $e|au + bv$, et donc e divise tous les éléments de $a\mathbb{Z} + b\mathbb{Z}$. Or, $a \wedge b \in (a \wedge b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, et donc $e|(a \wedge b)$.

Cela montre que $a \wedge b$ vérifie 1) et 2). Il nous reste à prouver l'unicité. Soient $d, d' \in \mathbb{N}$ qui vérifient 1) et 2). Alors $d'|a$, $d'|b$, et donc comme d vérifie 2), on a $d|d'$. En échangeant les rôles joués par d et d' on obtient aussi $d|d'$. Donc $d = d'$. □

Remarque 1.3.12. Il est vrai que le PGCD de a et b est le plus grand (au sens de l'ordre usuel $\leqslant$) entier naturel qui divise à la fois a et b. Mais c'est surtout, d'après la proposition précédente, le plus grand au sens de la divisibilité, ce qui est plus fort !

Exercice 5. Pour $a \in \mathbb{Z}$, que vaut $a \wedge 0$? $a \wedge 1$?

Remarque 1.3.13. Pour $a, b \in \mathbb{N}$, on montre facilement l'équivalence : $a \wedge b = a \iff a|b$.

Définition 1.3.14. *On dit que deux entiers $a, b \in \mathbb{Z}$ sont* **premiers entre eux** *si $a \wedge b = 1$.*

Proposition 1.3.15. *Deux entiers a et b sont premiers entre eux si et seulement si le seul diviseur positif commun à a et b est 1.*

Démonstration. D'après la proposition 1.3.11, $a \wedge b = 1$ si et seulement si pour tout $e \in \mathbb{N}$, $(e|a$ et $e|b) \Rightarrow e|1$. Cela revient à dire que le seul diviseur positif commun à a et b est 1. □

Un cas particulier utile est la proposition suivante

Proposition 1.3.16. *Soit p un nombre premier. Pour $a \in \mathbb{Z}$ on a l'équivalence :*

$$a \wedge p = 1 \quad \Longleftrightarrow \quad p \text{ ne divise pas } a.$$

Démonstration. Comme p est premier, ses seuls diviseurs positifs sont 1 et p. La proposition précédente implique donc que $a \wedge p = 1$ si et seulement si p n'est pas un diviseur de a. □

Exercice 6. Montrer que pour $a, b \in \mathbb{Z}$ on a :

$$a \wedge b = 1 \iff \text{il n'existe aucun nombre premier } p \text{ qui divise à la fois } a \text{ et } b.$$

Proposition 1.3.17. *Soient $a, b, a', b' \in \mathbb{Z}$ et $d \in \mathbb{N}^*$ tels que $a = da'$ et $b = db'$. On a :*

$$a \wedge b = d \iff a' \wedge b' = 1.$$

Démonstration. Cela découle du point 4) de la proposition 1.3.8 : $a \wedge b = d(a' \wedge b')$. □

Remarque 1.3.18. Application typique de cette proposition : faire des raisonnements sur le PGCD en se ramenant au cas d'entiers premiers entre eux. "Soient $a, b \in \mathbb{Z}$ et notons $d = a \wedge b$. On peut alors écrire $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$." Puis on raisonne sur a' et b'.

Remarque 1.3.19. On peut définir le PGCD d'une famille d'entiers $a_1, \ldots, a_r \in \mathbb{Z}$ de la manière suivante. On montre facilement (faites-le !) que l'ensemble

$$a_1\mathbb{Z} + \cdots + a_r\mathbb{Z} = \{a_1u_1 + \cdots + a_ru_r\,,\ u_1, \ldots, u_r \in \mathbb{Z}\}.$$

est un sous-groupe de $\mathbb{Z}$, et on définit $\mathrm{PGCD}(a_1, \ldots, a_r)$, aussi noté $a_1 \wedge \cdots \wedge a_r$, comme son générateur positif. Il est facile de démontrer (faites-le !) que ces opérations peuvent se calculer itérativement grâce au PGCD de deux nombres, par exemple :

$$a \wedge b \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

(Cela montre que la loi de composition interne $(a, b) \mapsto a \wedge b$ sur $\mathbb{N}$ est associative.)

1.3.3 L'algorithme d'Euclide

Théorème 1.3.20 (Algorithme d'Euclide). *Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On définit des entiers naturels $r_0, r_1, \ldots$ en posant*

$$r_0 = a,\ r_1 = b,$$

et pour tout $i \geqslant 1$, soit

$$r_{i-1} = r_iq_i + r_{i+1}$$

la division euclidienne de r_{i-1} par r_i (tant que $r_i \neq 0$). Soit $k \geqslant 0$ le plus petit entier tel que $r_{k+1} = 0$. Alors r_k est le PGCD de a et b.

Démonstration. La suite des restes est strictement décroissante après le premier terme $(r_1 > r_2 > r_3 > r_4 > \cdots)$, et donc atteint nécessairement 0, ce qui prouve l'existence de k. D'après la proposition 1.2.2 on a, pour tout $i \geqslant 1$, tant que $r_i \neq 0$, l'égalité :

$$r_{i-1} \wedge r_i = (r_{i-1} - r_iq_i) \wedge r_i = r_{i+1} \wedge r_i = r_i \wedge r_{i+1}.$$

On a donc : $a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_k \wedge r_{k+1} = r_k \wedge 0 = r_k$. □

Exercice 7. Utiliser l'algorithme d'Euclide pour calculer le PGCD de 1071 et 1029.

1.3.4 Le PPCM

Proposition 1.3.21. *Soient $a, b \in \mathbb{Z}$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

Démonstration. Laissé en exercice au lecteur (faites-le !). □

Définition 1.3.22. *Le générateur positif de $a\mathbb{Z} \cap b\mathbb{Z}$ est appelé le* **plus petit commun multiple (PPCM)** *de a et b. On le note* $\mathrm{PPCM}(a, b)$ *ou $a \vee b$.*

On a donc :

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

Proposition 1.3.23. *On a les propriétés suivantes, pour $a, b \in \mathbb{Z}$:*

1) $b \vee a = a \vee b$.

2) $(-a) \vee b = a \vee b$.

3) si $a \in \mathbb{N}$ *alors* $a \vee a = a$.

4) $(a \vee b) | ab$.

5) Pour tout $k \in \mathbb{N}$ *on a :* $(ka) \vee (kb) = k(a \vee b)$.

Démonstration. 1) C'est une conséquence du fait que $b\mathbb{Z} \cap a\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

2) C'est une conséquence du fait que $(-a)\mathbb{Z} \cap b\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ car $(-a)\mathbb{Z} = a\mathbb{Z}$.

3) C'est une conséquence du fait que $a\mathbb{Z} \cap a\mathbb{Z} = a\mathbb{Z}$.

4) On a $ab \in a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$, donc $(a \vee b) | ab$.

5) On a $(ka)\mathbb{Z} \cap (kb)\mathbb{Z} = k(a\mathbb{Z} \cap b\mathbb{Z}) = k(a \vee b)\mathbb{Z}$.

□

Remarque 1.3.24. Grâce au point 2) de la proposition ci-dessus, on se permettra d'énoncer certains résultats sur le PPCM seulement dans le cas des entiers naturels, pour simplifier.

La terminologie de "plus petit commun multiple" est expliquée par la proposition suivante.

Proposition 1.3.25. *Soient $a, b \in \mathbb{Z}$. Alors $a \vee b$ est l'unique $m \in \mathbb{N}$ qui vérifie les deux conditions suivantes :*

1) $a|m$ *et* $b|m$ *;*

2) pour tout $n \in \mathbb{N}$, $(a|n$ *et* $b|n) \Longrightarrow m|n$.

Démonstration. On montre d'abord que $a \vee b$ vérifie 1) et 2).

1) Comme $(a \vee b) \in (a \vee b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, on a que $(a \vee b) \in a\mathbb{Z}$ et $(a \vee b) \in b\mathbb{Z}$, donc $a|(a \vee b)$ et $b|(a \vee b)$.

2) Soit $n \in \mathbb{N}$ tel que $a|n$ et $b|n$. Alors $n \in a\mathbb{Z}$ et $n \in b\mathbb{Z}$, donc $n \in a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$, et donc $(a \vee b)|n$.

Cela montre que $a \vee b$ vérifie 1) et 2). Montrons maintenant l'unicité. Soient $m, m' \in \mathbb{N}$ qui vérifient 1) et 2). Comme $a|m'$ et $b|m'$ et que m vérifie 2), on a $m|m'$. En échangeant les rôles joués par m et m', on a aussi $m'|m$. Donc $m = m'$. □

Remarque 1.3.26. Il est vrai que le PPCM de a et b est le plus petit (au sens de l'ordre usuel $\leqslant$) entier naturel qui est un multiple de a et de b. Mais c'est surtout, d'après la proposition précédente, le plus petit au sens de la divisibilité, ce qui est plus fort !

Exercice 8. Pour $a \in \mathbb{Z}$, que vaut $a \vee 0$? $a \vee 1$?

Remarque 1.3.27. Pour $a, b \in \mathbb{N}$, on montre facilement l'équivalence : $a \vee b = a \iff b|a$.

Remarque 1.3.28. On peut définir le PPCM d'une famille d'entiers $a_1, \ldots, a_r \in \mathbb{Z}$ de la manière suivante. On montre facilement que l'ensemble

$$a_1\mathbb{Z} \cap \cdots \cap a_r\mathbb{Z}$$

est un sous-groupe de $\mathbb{Z}$, et on définit $\mathrm{PPCM}(a_1, \ldots, a_r)$, aussi noté $a_1 \vee \cdots \vee a_r$, comme son générateur positif. Il est facile de démontrer (faites-le !) que ces opérations peuvent se calculer itérativement grâce au PPCM de deux nombres, par exemple :

$$a \vee b \vee c = (a \vee b) \vee c = a \vee (b \vee c).$$

(Cela montre que la loi de composition interne $(a, b) \mapsto a \vee b$ sur $\mathbb{N}$ est associative.)

1.3.5 Une relation entre PGCD et PPCM

Proposition 1.3.29. *Soient $a, b \in \mathbb{N}$ et soit $d = a \wedge b$ et $m = a \vee b$. On a la relation :*

$$ab = dm.$$

Démonstration. Si $a = 0$ ou $b = 0$ alors $m = 0$ et la relation est vérifiée. On suppose donc maintenant que $a, b \neq 0$, ce qui implique que $d, m \neq 0$. On montre que $ab|dm$ et que $dm|ab$.

– Par le 4) de la proposition 1.3.23, le quotient $\frac{ab}{m}$ est un entier. Comme $a|m$, on a que $ab|mb$, et donc $\frac{ab}{m}|b$. De même, comme $b|m$, on a que $ab|ma$ et donc $\frac{ab}{m}|a$. Donc $\frac{ab}{m}$ est un diviseur commun à a et b, et donc par la caractérisation du PGCD, $\frac{ab}{m}|d$, d'où $ab|dm$.

– Comme $d|a$ on a $bd|ab$ et donc $b|\frac{ab}{d}$. (Noter que $\frac{ab}{d}$ est un entier puisque $d|a$.) De même, comme $d|b$ on a $ad|ab$ et donc $a|\frac{ab}{d}$. Donc $\frac{ab}{d}$ est un multiple commun de a et b, et donc par la caractérisation du PPCM, $m|\frac{ab}{d}$ et donc $dm|ab$.

□

Remarque 1.3.30. La relation $ab = dm$ peut être utilisée pour calculer m en ayant calculé d grâce à l'algorithme d'Euclide.

Proposition 1.3.31. *Soient $a, b \in \mathbb{N}^*$. Alors on a l'équivalence :*

$$a \wedge b = 1 \quad \Longleftrightarrow \quad a \vee b = ab.$$

Démonstration. C'est une conséquence de la proposition 1.3.29. □

1.4 Gauss, Euclide, et factorisation en produit de nombres premiers

1.4.1 Le lemme de Gauss

Théorème 1.4.1 (Lemme de Gauss). *Soient $a, b, c \in \mathbb{Z}$. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.*

Démonstration. On a d'une part $a|ac$, et par hypothèse on a d'autre part $a|bc$. Donc $a|(ac) \wedge (bc)$. Or $(ac) \wedge (bc) = (a \wedge b)|c| = |c|$ car $a \wedge b = 1$ par hypothèse. Donc $a|c$. □

On utilise souvent la variante suivante.

Théorème 1.4.2 (Variante du lemme de Gauss). *Soient $a, b, c \in \mathbb{Z}$. Si $a|c$, $b|c$, et $a \wedge b = 1$, alors $ab|c$.*

Démonstration. Comme $b|c$ on peut écrire $c = bk$ avec $k \in \mathbb{Z}$. On a donc $a|bk$ et $a \wedge b = 1$, donc par le lemme de Gauss, $a|k$. On en déduit que $ab|kb$, c'est-à-dire $ab|c$. □

Remarque 1.4.3. Application typique de ce théorème : pour montrer qu'un entier est divisible par 6, il suffit de montrer qu'il est divisible par 2 et 3, parce que $2 \wedge 3 = 1$.

Remarque 1.4.4. L'hypothèse "$a \wedge b = 1$" est évidemment importante dans le théorème ci-dessus. Par exemple, 4 et 6 divisent 12 mais $4 \times 6 = 24$ ne divise pas 12.

1.4.2 Le lemme d'Euclide

Théorème 1.4.5 (Lemme d'Euclide). *Soient $a, b \in \mathbb{Z}$, et soit p un nombre premier. Si $p|ab$, alors $p|a$ ou $p|b$.*

Démonstration. Il est équivalent de montrer que si $p|ab$ et p ne divise pas b, alors $p|a$. Or, si p ne divise pas b, comme p est premier, on a que $p \wedge b = 1$ (proposition 1.3.16). La conclusion résulte du lemme de Gauss. □

Remarque 1.4.6. L'hypothèse "p est premier" est évidemment importante dans le lemme d'Euclide. Par exemple, 6 divise $4 \times 9 = 36$, mais 6 ne divise ni 4 ni 9.

Exercice 9. Soient $u, a, b \in \mathbb{Z}$. Montrer qu'on a l'équivalence :

$$u \wedge (ab) = 1 \quad \Longleftrightarrow \quad (u \wedge a = 1 \ \text{ et } \ u \wedge b = 1).$$

1.4.3 Factorisation en produit de nombres premiers

Le théorème suivant est parfois appelé **théorème fondamental de l'arithmétique**.

Théorème 1.4.7 (Factorisation en produit de nombres premiers). *Tout entier $n \in \mathbb{N}^*$ peut s'écrire comme un produit de nombres premiers, de manière unique à l'ordre des facteurs près.*

Démonstration. L'existence a déjà été montrée (proposition 1.2.7) et il reste juste à démontrer l'unicité. On procède par récurrence.

– Pour tout $r \in \mathbb{N}$ considérons l'assertion $Q(r)$: "pour tous nombres premiers $p_1, \dots, p_r$, et pour tout $s \in \mathbb{N}$ et tous nombres premiers $q_1, \dots, q_s$, si $p_1 \cdots p_r = q_1 \cdots q_s$ alors on a $r = s$ et quitte à permuter les facteurs, on a $p_i = q_i$ pour tout $i = 1, \dots, r$."

– Initialisation : $Q(0)$ est vraie. En effet, pour tout $s \in \mathbb{N}$ et tous nombres premiers $q_1, \dots, q_s$, si $1 = q_1 \cdots q_s$ alors $s = 0$.

– Hérédité : soit $r \geqslant 1$ tel que $Q(r-1)$ est vraie et montrons que $Q(r)$ est vraie. Soient des nombres premiers $p_1, \dots, p_r$, soit $s \in \mathbb{N}$, et soit des nombres premiers $q_1, \dots, q_s$ tels qu'on ait $p_1 \cdots p_r = q_1 \cdots q_s$. On a donc $p_r | q_1 \cdots q_s$, et comme p_r est premier, le lemme d'Euclide implique qu'il existe $j \in \{1, \dots, s\}$ tel que $p_r | q_j$. Quitte à permuter les facteurs on peut supposer que $j = s$ et on a donc $p_r | q_s$. Or, puisque q_s est premier, cela implique que $p_r = q_s$. On peut donc simplifier par $p_r = q_s$ de chaque côté, et on obtient l'égalité : $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$. En appliquant $Q(r-1)$ on voit qu'on a $r - 1 = s - 1$, et quitte à permuter les facteurs qu'on a $p_i = q_i$ pour tout $i \in \{1, \dots, r-1\}$. On a donc montré que $Q(r)$ est vraie.

– Conclusion : on a montré que $Q(r)$ est vraie pour tout $r \in \mathbb{N}$.

□

▷ Il est courant d'écrire une décomposition en produit de nombres premiers sous la forme

$$n = 2^{a_2} \times 3^{a_3} \times 5^{a_5} \times 7^{a_7} \times 11^{a_{11}} \times 13^{a_{13}} \times \cdots = \prod_{p \text{ premier}} p^{a_p},$$

où le produit est indexé par l'ensemble des nombres premiers p, et où les a_p sont des entiers naturels qui sont presque tous nuls (c'est-à-dire tous nuls sauf un nombre fini). Par le théorème ci-dessus, les a_p sont uniquement déterminés par n.

Définition 1.4.8. *Dans une écriture comme ci-dessus, l'entier naturel a_p est appelé la* **valuation p-adique** *de n et noté $v_p(n)$.*

1.4.4 Application au calcul du PGCD et du PPCM

Proposition 1.4.9. *Soient deux entiers $n, n' \in \mathbb{N}^*$ écrits comme des produits de nombres premiers :*

$$n = \prod_{p \text{ premier}} p^{a_p} \quad \text{et} \quad n' = \prod_{p \text{ premier}} p^{a'_p}.$$

Alors on a :

$$n | n' \iff \forall p \text{ premier}, \ a_p \leqslant a'_p.$$

Démonstration. 1) $\Longleftarrow$. Si $a_p \leqslant a'_p$ pour tout nombre premier p, on peut définir l'entier

$$k = \prod_{p \text{ premier}} p^{a'_p - a_p}$$

et on a $n' = nk$, d'où $n | n'$.

2) $\Longrightarrow$. Si $n|n'$ alors il existe $k \in \mathbb{N}^*$ tel que $n' = nk$. Écrivons k comme produit de nombres premiers sous la forme

$$k = \prod_{p \text{ premier}} p^{b_p},$$

où les b_p sont des entiers naturels qui sont presque tous nuls. L'égalité $n' = nk$ s'écrit alors

$$\prod_{p \text{ premier}} p^{a'_p} = \prod_{p \text{ premier}} p^{a_p + b_p}.$$

Par unicité de la décomposition en produits de nombres premiers on a $a'_p = a_p + b_p$ pour tout nombre premier p, et donc $a'_p \geqslant a_p$.

□

Proposition 1.4.10. *Soient deux entiers $n, n' \in \mathbb{N}^*$ écrits comme des produits de nombres premiers :*

$$n = \prod_{p \text{ premier}} p^{a_p} \quad \text{et} \quad n' = \prod_{p \text{ premier}} p^{a'_p}.$$

Alors on a :

$$n \wedge n' = \prod_{p \text{ premier}} p^{\min(a_p, a'_p)} \quad \text{et} \quad n \vee n' = \prod_{p \text{ premier}} p^{\max(a_p, a'_p)}.$$

Démonstration. On traite le cas du PGCD, le cas du PPCM étant similaire. D'après la proposition 1.4.9, les diviseurs positifs communs à n et n' sont les entiers

$$\prod_{p \text{ premier}} p^{b_p}$$

avec $b_p \leqslant a_p$ et $b_p \leqslant a'_p$, c'est-à-dire $b_p \leqslant \min(a_p, a'_p)$. Il est alors clair que l'entier

$$\prod_{p \text{ premier}} p^{\min(a_p, a'_p)}$$

est un diviseur positif commun à n et n' qui est divisible par tous les diviseurs communs à n et n'. C'est donc le PGCD de n et n'. □

Exercice 10. Calculer les décompositions en produit de nombres premiers de 504 et 1540 et en déduire $504 \wedge 1540$ et $504 \vee 1540$.

1.5 Le théorème de Bézout et des applications

1.5.1 Le théorème de Bézout

Le théorème de Bézout[4] est l'énoncé suivant.

Théorème 1.5.1 (Théorème de Bézout). *Soient $a, b \in \mathbb{Z}$, et soit $d \in \mathbb{N}$. On a équivalence entre les deux assertions suivantes :*

(i) $d = a \wedge b$;

(ii) $d|a$, $d|b$, *et il existe* $u, v \in \mathbb{Z}$ *tels que* $au + bv = d$.

Démonstration. – $(i) \implies (ii)$. Supposons que $d = a \wedge b$. Par la proposition 1.3.11 on a $d|a$ et $d|b$. De plus on a par définition du PGCD, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Comme $d \in d\mathbb{Z}$, on a donc $d \in a\mathbb{Z} + b\mathbb{Z}$, et donc il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$.

– $(ii) \implies (i)$. Supposons que $d|a$, $d|b$, et qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$, et montrons que $d = a \wedge b$ en utilisant le critère de la proposition 1.3.11. Soit $e \in \mathbb{N}$ tel que $e|a$ et $e|b$. Alors $e|(au + bv)$, c'est-à-dire $e|d$. On en conclut que $d = a \wedge b$.

□

Définition 1.5.2. *Une égalité $au + bv = a \wedge b$ comme dans le théorème de Bézout est appelée une* **relation de Bézout** *pour a et b.*

Théorème 1.5.3 (Théorème de Bézout, cas particulier). *Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Démonstration. C'est une conséquence du théorème de Bézout puisque les conditions $1|a$ et $1|b$ sont automatiquement vérifiées. □

L'algorithme d'Euclide étendu

Théorème 1.5.4 (Algorithme d'Euclide d'étendu). *Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Reprenons les notations de l'algorithme d'Euclide (théorème 1.3.20) : on définit des entiers naturels $r_0, r_1, \ldots$ en posant*

$$r_0 = a,\ r_1 = b,$$

et pour tout $i \geqslant 1$, soit

$$r_{i-1} = r_i q_i + r_{i+1}$$

la division euclidienne de r_{i-1} par r_i (tant que $r_i \neq 0$). Soit $k \geqslant 0$ le plus petit entier tel que $r_{k+1} = 0$. On définit des nombres $u_0, u_1, \ldots, u_k$ et $v_0, v_1, \ldots, v_k$ en posant

$$\begin{cases} u_0 = 1 \\ u_1 = 0 \\ u_{i+1} = -q_i u_i + u_{i-1} \quad \text{pour } i \geqslant 1 \end{cases} \quad \text{et} \quad \begin{cases} v_0 = 0 \\ v_1 = 1 \\ v_{i+1} = -q_i v_i + v_{i-1} \quad \text{pour } i \geqslant 1 \end{cases}$$

[4] Nommé en l'honneur du mathématicien français Étienne Bézout (1730-1783). La contribution de Bézout aura surtout été d'étudier la généralisation du théorème au cas de polynômes.

Alors $a \wedge b = r_k$ et on a une relation de Bézout :

$$au_k + bv_k = r_k.$$

Démonstration. Le fait que $a \wedge b = r_k$ est le résultat du théorème 1.3.20. On montre par une récurrence double que pour tout $i \in \{0, 1, \ldots, k\}$ on a : $au_i + bv_i = r_i$. C'est clairement vrai pour $i = 0$ et $i = 1$. Pour l'hérédité, soit $i \geqslant 1$ tel qu'on ait $au_{i-1} + bv_{i-1} = r_{i-1}$ et $au_i + bv_i = r_i$. Alors on calcule :

$$au_{i+1} + bv_{i+1} = a(-q_i u_i + u_{i-1}) + b(-q_i v_i + v_{i-1}) = (au_{i-1} + bv_{i-1}) - (au_i + bv_i)q_i.$$

Grâce à l'hypothèse de récurrence on obtient $au_{i+1} + bv_{i+1} = r_{i-1} - r_i q_i = r_{i+1}$, et l'hérédité est montrée, ce qui conclut la récurrence. Pour $i = k$ on obtient la relation de Bézout. □

Remarque 1.5.5. En pratique on ne calcule pas les u_i et les v_i, mais on part de la dernière ligne de l'algorithme d'Euclide et on "remonte" le fil de l'algorithme pour obtenir la relation de Bézout.

Exercice 11. Utiliser l'algorithme d'Euclide étendu pour calculer le PGCD de 186 et 309 et trouver une relation de Bézout entre ces deux nombres.

1.5.2 Application à l'inversion modulo un entier

Proposition 1.5.6. *Soit $a \in \mathbb{Z}$. Alors a est inversible modulo n si et seulement si $a \wedge n = 1$. Dans ce cas-là, si $au + nv = 1$ est une relation de Bézout pour a et n, on a que u est un inverse de a modulo n.*

Démonstration. – Si a est inversible modulo n alors il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \pmod{n}$, et donc il existe $k \in \mathbb{Z}$ tel que $ab = 1 + kn$, ou encore $ab - kn = 1$. Par le théorème de Bézout, on a donc $a \wedge n = 1$.

– Si $a \wedge n = 1$ alors par le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$. On a donc $au \equiv 1 \pmod{n}$, donc a est inversible modulo n et u est un inverse de a modulo n. □

Exercice 12. Montrer que 14 est inversible modulo 31 et en calculer un inverse. Pour quels entiers x a-t-on $14\,x \equiv 2 \pmod{31}$?

1.6 Le théorème chinois des restes

1.6.1 Le théorème

Théorème 1.6.1 (Théorème chinois des restes). *Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. Soient $a, b \in \mathbb{Z}$. Alors le système*

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

a une solution $x_0 \in \mathbb{Z}$. De plus, l'ensemble des solutions est l'ensemble des entiers congrus à x_0 modulo mn.

Démonstration. – Comme $m \wedge n = 1$, par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$. On pose

$$x_0 = anv + bmu.$$

On a alors $x_0 = a(1 - mu) + bmu = a + mu(b - a)$ et donc $x_0 \equiv a \pmod{m}$. De même, on a $x_0 = anv + b(1 - nv) = b + nv(a - b)$ et donc $x_0 \equiv b \pmod{n}$.

– Soit $x \in \mathbb{Z}$ une solution du système. Alors $x \equiv x_0 \pmod{m}$ et $x \equiv x_0 \pmod{n}$, et donc $m|(x - x_0)$ et $n|(x - x_0)$. Comme $m \wedge n = 1$, le théorème 1.4.2 implique que $mn|(x - x_0)$ et donc que $x \equiv x_0 \pmod{mn}$. Réciproquement, tout entier x congru à x_0 modulo mn est congru à x_0 modulo m et n, et est donc une solution du système.

□

▷ On a donc :

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \iff x \equiv x_0 \pmod{mn}.$$

Remarque 1.6.2. Si m et n ne sont pas premiers entre eux, il se peut que le système n'ait même pas de solution. Par exemple, le système suivant n'a aucune solution $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 1 \pmod{4} \end{cases}$$

En effet, si $x \equiv 2 \pmod 6$ alors x est pair... et si $x \equiv 1 \pmod 4$ alors x est impair !

Remarque 1.6.3. Comment trouver une solution particulière x_0 ?

▷ On peut retenir la formule de la preuve ci-dessus.

▷ Ou, si m et n ne sont pas trop gros, trouver un élément commun dans les listes

$$a, a + m, a + 2m, a + 3m, \ldots \quad \text{et} \quad b, b + n, b + 2n, b + 3n, \ldots$$

(D'après le théorème, deux solutions consécutives sont séparées de mn et donc on n'a pas à chercher trop longtemps si m et n ne sont pas trop gros.)

1.6.2 Généralisation à plusieurs résidus

La version générale du théorème chinois des restes est la suivante. On la montre facilement en itérant le résultat pour deux équations.

Théorème 1.6.4. *Soient des entiers $n_1, \dots, n_r$ qui sont deux à deux premiers entre eux (pour tous $i \neq j$, $n_i \wedge n_j = 1$). Soient $a_1, \dots, a_r \in \mathbb{Z}$. Alors le système*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

a une solution $x_0 \in \mathbb{Z}$. De plus, l'ensemble des solutions est l'ensemble des entiers congrus à x_0 modulo $n_1 \cdots n_r$.

1.7 Le petit théorème de Fermat

1.7.1 Un résultat important sur les coefficients binomiaux

On commence par une proposition importante.

Proposition 1.7.1. *Soit p un nombre premier. Pour tout $k \in \{1, \dots, p-1\}$, p divise le coefficient binomial $\binom{p}{k}$.*

Démonstration. Rappelons qu'on a

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!},$$

et donc

$$p(p-1)(p-2)\cdots(p-k+1) = 1 \times 2 \times 3 \times \cdots \times k \times \binom{p}{k}.$$

Comme $k \geqslant 1$, p divise $p(p-1)(p-2)\cdots(p-k+1)$ et donc

$$p \text{ divise } 1 \times 2 \times 3 \times \cdots \times k \times \binom{p}{k}.$$

Comme $k \leqslant p-1$, aucun des entiers entre 1 et k n'est divisible par p. Par le lemme d'Euclide, p divise $\binom{p}{k}$. □

Exemple 1.7.2. Les coefficients binomiaux $\binom{7}{k}$, pour $0 \leqslant k \leqslant 7$ sont égaux à :

$$1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1.$$

Ils sont tous divisibles par 7, à part le premier $\binom{7}{0} = 1$ et le dernier $\binom{7}{7} = 1$.

Remarque 1.7.3. L'hypothèse "p est premier" est importante dans la proposition ci-dessus. Par exemple, 4 ne divise pas le coefficient binomial $\binom{4}{2} = 6$.

1.7.2 Le rêve de l'étudiant de première année ("freshman's dream")

Proposition 1.7.4. *Soit p un nombre premier. Alors pour tous $x, y \in \mathbb{Z}$ on a :*

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Démonstration. On a, d'après la formule du binôme de Newton :

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p.$$

Par la proposition 1.7.1, on a $p | \binom{p}{k}$ pour tout $k \in \{1, \dots, p-1\}$. Donc :

$$p \mid \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k.$$

On en déduit que

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

□

1.7.3 Le petit théorème de Fermat : première version

Le petit théorème de Fermat[5] est le résultat suivant.

Théorème 1.7.5 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ on a :*

$$a^p \equiv a \pmod{p}.$$

Démonstration. On démontre d'abord le théorème pour $a \in \mathbb{N}$, par récurrence.

- Pour tout $a \in \mathbb{N}$ considérons l'assertion $P(a)$: "$a^p \equiv a \pmod{p}$".
- Initialisation : $P(0)$ est vraie car $0^p = 0 \equiv 0 \pmod{p}$.
- Hérédité : soit $a \in \mathbb{N}$ tel que $P(a)$ est vraie. Alors $a^p \equiv a \pmod{p}$. Par la proposition précédente (rêve de l'étudiant de première année), on a :

  $$(a+1)^p \equiv a^p + 1^p \pmod{p}$$

  et comme $a^p \equiv a \pmod{p}$, on a donc

  $$(a+1)^p \equiv a + 1 \pmod{p},$$

  ce qui démontre $P(a+1)$.
- Conclusion : on a démontré que $P(a)$ est vraie pour tout $a \in \mathbb{N}$.

Maintenant, pour $a \in \mathbb{N}$, on a :

$$(-a)^p = (-1)^p a^p \equiv (-1)^p a \equiv -a \pmod{p}.$$

(La dernière congruence est claire pour p impair car alors $(-1)^p = -1$; pour $p = 2$, cela résulte du fait que $1 \equiv -1 \pmod{2}$.) Cela conclut la démonstration du petit théorème de Fermat. □

Remarque 1.7.6. L'hypothèse "p est premier" est importante dans le petit théorème de Fermat. Par exemple, $2^4 = 16$ n'est pas congru à 2 modulo 4.

1.7.4 Le petit théorème de Fermat : une seconde version

Théorème 1.7.7 (Petit théorème de Fermat, variante). *Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, si a n'est pas un multiple de p alors :*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Démonstration. D'après le théorème 1.7.5 on a, pour tout $a \in \mathbb{Z}$,

$$p \mid a^p - a = a(a^{p-1} - 1).$$

Or, si a n'est pas un multiple de p, on déduit du lemme d'Euclide que $p|(a^{p-1} - 1)$, et donc que $a^{p-1} \equiv 1 \pmod{p}$. □

[5] Nommé en l'honneur du mathématicien français Pierre de Fermat (160?-1665), qui l'énonça en 1640.

Chapitre 2

Étude de $\mathbb{Z}/n\mathbb{Z}$

2.1 Relations d'équivalence et quotient

2.1.1 Définitions

Rappelons qu'une relation binaire sur un ensemble E est un sous-ensemble $\mathcal{R} \subset E \times E$. On utilise la notation

$$x \,\mathcal{R}\, y$$

à la place de $(x, y) \in \mathcal{R}$, et on dit alors que x est en relation avec y pour la relation $\mathcal{R}$.

Définition 2.1.1. *Soit E un ensemble. Une* **relation d'équivalence** *sur E est une relation binaire $\sim$ sur E qui est réflexive, symétrique, et transitive, c'est-à-dire telles que les propriétés suivantes sont vérifiées.*

- *Réflexivité :* $\forall x \in E\,,\ x \sim x$;
- *Symétrie :* $\forall x, y \in E\,,\ x \sim y \implies y \sim x$;
- *Transitivité :* $\forall x, y, z \in E\,,\ (x \sim y \ \text{ et } \ y \sim z) \implies x \sim z$.

Exemple 2.1.2. Soit $n \in \mathbb{N}^*$. On a vu au chapitre 1 que la relation $\sim$ sur l'ensemble $E = \mathbb{Z}$ définie par

$$a \sim b \quad \iff \quad a \equiv b \ (\mathrm{mod}\ n)$$

est une relation d'équivalence.

Exercice 13. On définit une relation $\sim$ sur $\mathbb{R}^2$ par :

$$\vec{u} \sim \vec{v} \quad \iff \quad \exists \lambda > 0\ ,\ \vec{u} = \lambda \vec{v}.$$

Montrer que c'est une relation d'équivalence.

2.1.2 Classes d'équivalence

Soit une relation d'équivalence $\sim$ sur un ensemble E.

Définition 2.1.3. *La* **classe d'équivalence** *(ou juste la* **classe***) d'un élément $x \in E$ est l'ensemble*

$$\overline{x} = \{y \in E \mid y \sim x\}.$$

Exemple 2.1.4. Pour la relation de congruence modulo 7 on a

$$\overline{0} = \{\ldots, -7, 0, 7, 14, 21, 28, 35, \ldots\},$$

$$\overline{3} = \{\ldots, -4, 3, 10, 17, 24, 31, \ldots\},$$

et

$$\overline{24} = \overline{3}.$$

Proposition 2.1.5. *Pour $x_1, x_2 \in E$ on a :*

$$\overline{x_1} = \overline{x_2} \quad \Longleftrightarrow \quad x_1 \sim x_2.$$

Démonstration. – Supposons que $\overline{x_1} = \overline{x_2}$. Comme $\sim$ est réflexive on a $x_1 \sim x_1$ et donc $x_1 \in \overline{x_1}$, d'où $x_1 \in \overline{x_2}$, c'est-à-dire $x_1 \sim x_2$.

– Supposons que $x_1 \sim x_2$ et montrons que $\overline{x_1} = \overline{x_2}$.

On montre d'abord que $\overline{x_1} \subset \overline{x_2}$. Soit $x \in \overline{x_1}$, alors $x \sim x_1$. Comme $x_1 \sim x_2$ et que $\sim$ est transitive, on a donc $x \sim x_2$ et donc $x \in \overline{x_2}$. On a donc montré que $\overline{x_1} \subset \overline{x_2}$.

Comme $\sim$ est symétrique on a $x_2 \sim x_1$ et en échangeant les rôles joués par x_1 et x_2 l'argument précédent donne $\overline{x_2} \subset \overline{x_1}$. On a donc montré que $\overline{x_1} = \overline{x_2}$.

□

Proposition 2.1.6. *Les classes d'équivalence forment une partition de E, c'est-à-dire que tout élément de E est dans une et une seule classe d'équivalence.*

Démonstration. – Tout élément est dans sa propre classe d'équivalence : $\forall x \in E\,,\ x \in \overline{x}$, car $\sim$ est réflexive.

– Supposons qu'un élément $x \in E$ appartienne à deux classes d'équivalence $\overline{x_1}$ et $\overline{x_2}$. Alors $x \sim x_1$ et $x \sim x_2$. Comme $\sim$ est symétrique et transitive on a $x_1 \sim x_2$ et donc $\overline{x_1} = \overline{x_2}$ d'après la proposition 2.1.5.

□

Exemple 2.1.7. Pour la relation de congruence modulo 2, la partition en classes d'équivalence est :

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} = \{\text{entiers pairs}\} \sqcup \{\text{entiers impairs}\}.$$

Définition 2.1.8. *Soit $C \subset E$ une classe d'équivalence. Un élément $x \in C$ est appelé un* **représentant** *de la classe d'équivalence C.*

Exemple 2.1.9. Pour la relation de congruence modulo 7, 20 est un représentant de la classe d'équivalence $\overline{34}$.

Exercice 14. Dans le contexte de l'exercice 13, quelle est la classe d'équivalence de $(1,0)$? de $(1,2)$? de $(0,0)$? Décrire la partition de $\mathbb{R}^2$ en classes d'équivalence.

2.1.3 Quotient par une relation d'équivalence

Soit une relation d'équivalence $\sim$ sur un ensemble E.

Définition 2.1.10. *L'ensemble des classes d'équivalence est appelé* **quotient** *de E par la relation d'équivalence $\sim$ et noté $E/\sim$.*

▷ Les éléments de l'ensemble quotient $E/\sim$ sont les classes d'équivalence $\overline{x}$, pour $x \in E$, et on a égalité $\overline{x_1} = \overline{x_2}$ dans $E/\sim$ si et seulement $x_1 \sim x_2$ dans E (proposition 2.1.5).

Remarque 2.1.11. Le quotient est la manière mathématique d'*identifier* certains éléments de E entre eux. En effet, on décrète que des éléments qui sont équivalents (pour $\sim$) dans E sont maintenant *égaux* dans $E/\sim$.

Définition 2.1.12. *L'application*

$$\pi : E \longrightarrow E/\sim \, , \; x \mapsto \overline{x}$$

est appelée **application de quotient**.

▷ Il est clair que π est surjective, par définition.

2.1.4 Définir une application sur un quotient

Définition 2.1.13. *Soit une application*

$$f : E \longrightarrow F.$$

On dit que f **passe au quotient** *par $\sim$ si f prend la même valeur sur tous les éléments d'une même classe d'équivalence, c'est-à-dire si :*

$$\forall x, x' \in E \, , \; x \sim x' \implies f(x) = f(x').$$

Si f passe au quotient par $\sim$ alors on peut définir l'application

$$g : E/\sim \longrightarrow F \, , \; \overline{x} \mapsto f(x)$$

qui à une classe d'équivalence associe la valeur prise par f sur n'importe quel élément de cette classe d'équivalence. On dit que g est l'application **induite par** *f sur le quotient $E/\sim$.*

Exercice 15. Les applications suivantes passent-elles au quotient par la relation de congruence modulo 6 ?

$$f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto (-1)^n\ ;$$
$$f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto n^2 - 1\ .$$

Remarque 2.1.14. On considérera aussi des applications définies non pas sur E mais sur le produit cartésien de E avec lui-même :

$$f : E \times E \longrightarrow F.$$

Dans ce cas-là on dit que f passe au quotient si elle passe au quotient "en chaque variable", c'est-à-dire si le résultat de $f(x_1, x_2)$ ne dépend que des classes d'équivalence $\overline{x_1}$ et $\overline{x_2}$, ou plus formellement si

$$\forall x_1, x_2, x_1', x_2' \in E\ ,\ (x_1 \sim x_1' \ \text{ et } \ x_2 \sim x_2') \implies f(x_1, x_2) = f(x_1', x_2').$$

Dans ce cas-là on peut définir

$$g : (E/\sim) \times (E/\sim) \longrightarrow F\ ,\ (\overline{x_1}, \overline{x_2}) \mapsto f(x_1, x_2).$$

2.2 Étude de $\mathbb{Z}/n\mathbb{Z}$

On fixe dans cette partie un entier $n \in \mathbb{N}^*$.

2.2.1 Définition

On a vu au chapitre 1 que la relation de congruence modulo n,

$$a \sim b \iff a \equiv b \,(\mathrm{mod}\, n)\,,$$

est une relation d'équivalence sur l'ensemble $\mathbb{Z}$.

Définition 2.2.1. *On définit $\mathbb{Z}/n\mathbb{Z}$ comme le quotient de l'ensemble $\mathbb{Z}$ par la relation de congruence modulo n. Pour un entier $k \in \mathbb{Z}$, on note donc $\overline{k}$ sa classe d'équivalence dans $\mathbb{Z}/n\mathbb{Z}$.*

▷ On a donc, pour $a, b \in \mathbb{Z}$:

$$\overline{a} = \overline{b} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \iff \qquad a \equiv b \pmod{n}.$$

▷ Notamment, pour $a \in \mathbb{Z}$:

$$\overline{a} = \overline{0} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \iff \qquad n|a.$$

Proposition 2.2.2. *L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments : $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{n-1}$.*

Démonstration. Par division euclidienne (voir la proposition 1.2.16), pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, il existe un unique $r \in \{0, \ldots, n-1\}$ tel que $\overline{a} = \overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$. C'est exactement ce que dit la proposition. □

▷ On a

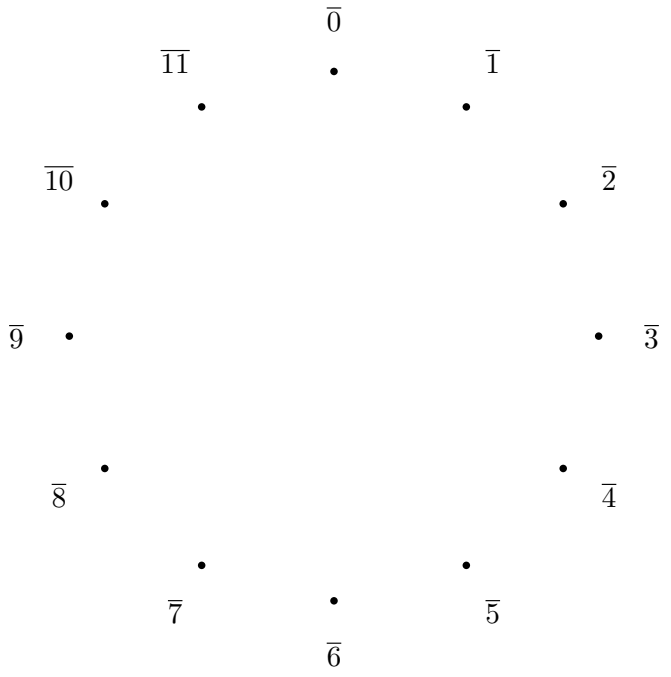
$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

▷ Dit autrement, la partition de $\mathbb{Z}$ en classes d'équivalence pour la relation de congruence modulo n est :

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} \sqcup \cdots \sqcup \overline{n-1}.$$

Exemple 2.2.3. Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3} = \overline{10} = \overline{73} = \overline{-4}$, qui est l'ensemble des entiers $a \equiv 3 \pmod 7$, c'est-à-dire l'ensemble des $a \in \mathbb{Z}$ dont le reste dans la division euclidienne par 7 est 3, ou encore l'ensemble $\{7k + 3\,,\, k \in \mathbb{Z}\}$.

2.2.2 $\mathbb{Z}/12\mathbb{Z}$ est une horloge



2.2.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.2.4. *L'addition dans $\mathbb{Z}$ passe au quotient et induit une loi $+$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par*

$$\overline{a} + \overline{b} = \overline{a+b}.$$

La multiplication dans $\mathbb{Z}$ passe au quotient et induit une loi $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par

$$\overline{a} \times \overline{b} = \overline{a \times b}.$$

Démonstration. C'est une traduction de la proposition 1.2.17. En effet, pour montrer que la somme $+$ dans $\mathbb{Z}/n\mathbb{Z}$ est bien définie, il faut montrer que le résultat $\overline{a+b}$ ne dépend pas du choix des représentants a et b. Dit autrement, on veut montrer que si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $\overline{a+b} = \overline{a'+b'}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire que $a+b \equiv a'+b' \pmod{n}$. C'est la proposition 1.2.17. Il en va de même pour le produit. □

Remarque 2.2.5. De manière plus formelle, on vient d'appliquer la remarque 2.1.14 à l'application

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}\ ,\ (a,b) \mapsto \overline{a+b}$$

(et de même pour le produit).

Exemple 2.2.6. Dans $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ on a

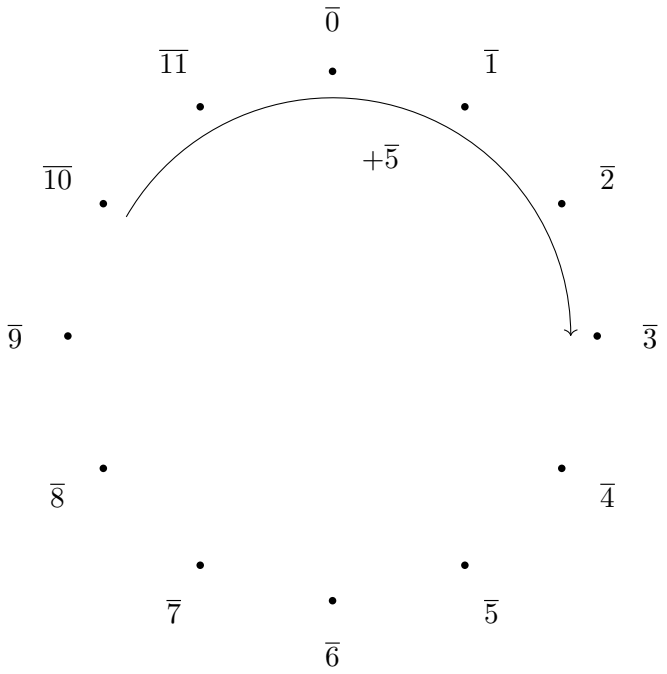
$$\overline{1} + \overline{1} = \overline{1+1} = \overline{2} = \overline{0}.$$

L'égalité "$\overline{1} + \overline{1} = \overline{0}$" veut dire : "la somme d'un nombre impair avec un nombre impair est un nombre pair".

Exemple 2.2.7. Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3}+\overline{6}=\overline{3+6}=\overline{9}=\overline{2}$.

Exercice 16. Écrire la table d'addition de $\mathbb{Z}/7\mathbb{Z}$.

▷ Voici une illustration de l'addition dans $\mathbb{Z}/12\mathbb{Z}$, vu comme une horloge.



Proposition 2.2.8. $(\mathbb{Z}/n\mathbb{Z},+)$ *est un* **groupe abélien**, *au sens où on a les propriétés suivantes.*

1) La loi $+$ *est associative : pour tous* $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}/n\mathbb{Z}$, $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$.

2) L'élément $\overline{0}$ *est élément neutre pour* $+$ *: pour tout* $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$, $\overline{a}+\overline{0}=\overline{a}=\overline{0}+\overline{a}$.

3) Tout élément $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ *a un inverse pour la loi* $+$*, qui est* $\overline{-a}$ *:* $\overline{a}+\overline{-a}=\overline{0}=\overline{-a}+\overline{a}$. *On note aussi* $-\overline{a}=\overline{-a}$.

4) La loi $+$ *est commutative : pour tous* $\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}$, $\overline{a}+\overline{b}=\overline{b}+\overline{a}$.

Démonstration. Toutes ces propriétés se démontrent en utilisant les mêmes propriétés de la loi $+$ dans $\mathbb{Z}$. Par exemple, pour l'associativité :

$$(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c}).$$

□

Exemple 2.2.9. Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3}\times\overline{6}=\overline{3\times6}=\overline{18}=\overline{11}=\overline{4}=\overline{-10}=\overline{74}$.

Exercice 17. Écrire la table de multiplication de $\mathbb{Z}/7\mathbb{Z}$.

Proposition 2.2.10. *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un* **anneau commutatif**, *au sens où on a les propriétés suivantes.*

1) $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

2) La loi $\times$ est associative : pour tous $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, $(\overline{a} \times \overline{b}) \times \overline{c} = \overline{a} \times (\overline{b} \times \overline{c})$.

3) L'élément $\overline{1}$ est élément neutre pour $\times$: pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times \overline{1} = \overline{a} = \overline{1} \times \overline{a}$.

4) La loi $\times$ est distributive par rapport à la loi $+$: pour tous $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times (\overline{b} + \overline{c}) = (\overline{a} \times \overline{b}) + (\overline{a} \times \overline{c})$ et $(\overline{a} + \overline{b}) \times \overline{c} = (\overline{a} \times \overline{c}) + (\overline{b} \times \overline{c})$.

5) La loi $\times$ est commutative : pour tous $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \times \overline{b} = \overline{b} \times \overline{a}$.

Démonstration. De même, ces propriétés se démontrent en utilisant les mêmes propriétés de la loi $\times$ dans $\mathbb{Z}$. □

2.2.4 Retour sur l'inversion modulo n

Définition 2.2.11. *On dit qu'un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est* **inversible dans** *$\mathbb{Z}/n\mathbb{Z}$ s'il existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a} \times \overline{b} = \overline{1}$. Dans ce cas, $\overline{b}$ est appelé* **l'inverse** *de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$ et noté*

$$\overline{b} = \overline{a}^{-1}.$$

▷ Vu que $\overline{a} \times \overline{b} = \overline{ab}$ par définition, c'est une manière de reformuler la définition 1.2.19 du chapitre précédent :

$$a \text{ est inversible modulo } n \iff \overline{a} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}.$$

▷ Ce qu'on gagne à travailler avec $\mathbb{Z}/n\mathbb{Z}$ est la possibilité de parler de **l**'inverse.

Proposition 2.2.12. *Si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il existe un unique $\overline{b}$ tel que $\overline{a} \times \overline{b} = \overline{1}$.*

Démonstration. C'est une reformulation de la proposition 1.2.20. On peut réécrire la preuve dans le langage de $\mathbb{Z}/n\mathbb{Z}$, comme suit. Soient $\overline{b}, \overline{b'} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\overline{a} \times \overline{b} = \overline{1}$ et $\overline{a} \times \overline{b'} = \overline{1}$. Alors en multipliant la première égalité par $\overline{b'}$ on obtient : $\overline{a} \times \overline{b} \times \overline{b'} = \overline{b'}$. En multipliant la deuxième égalité par $\overline{b}$ on obtient : $\overline{a} \times \overline{b} \times \overline{b'} = \overline{b}$. Donc $\overline{b} = \overline{b'}$. □

Reformulons la proposition 1.5.6 du chapitre précédent :

Proposition 2.2.13. *Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.*

▷ Rappelons que l'inverse de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$, quand il existe, se calcule en cherchant une relation de Bézout entre a et n : si $au + nv = 1$ alors on a $\overline{au + nv} = \overline{1}$ et donc $\overline{au} = \overline{1}$, d'où $\overline{a} \times \overline{u} = \overline{1}$ et donc

$$\overline{a}^{-1} = \overline{u}.$$

Exercice 18. Montrer que $\overline{13}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$ et calculer son inverse.

Théorème 2.2.14. *Soit p un nombre premier. Alors l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un* **corps**, *au sens où tout élément $\neq \overline{0}$ de $\mathbb{Z}/p\mathbb{Z}$ est inversible.*

Démonstration. Soit $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ avec $\overline{a} \neq \overline{0}$. Alors p ne divise pas a, et donc $p \wedge a = 1$ par la proposition 1.3.16, d'où par la proposition 2.2.13, $\overline{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. □

Exercice 19. Calculer les inverses de $\overline{1}, \ldots, \overline{12}$ dans $\mathbb{Z}/13\mathbb{Z}$.

Exercice 20. Soit p un nombre premier. Montrer qu'on a, pour tous $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$:

$$\overline{a} \times \overline{b} = \overline{0} \iff (\overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0}).$$

Montrer que cette propriété est fausse dans $\mathbb{Z}/n\mathbb{Z}$ si n est composé.

Exercice 21. Soit n un nombre composé. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps, c'est-à-dire qu'il existe un élément $\neq \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui n'est pas inversible.

2.2.5 Indicatrice d'Euler

Définition 2.2.15. *L'***indicatrice d'Euler** *est la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ définie par*

$$\varphi(n) = \textit{le nombre d'entiers } k \in \{1, \ldots, n\} \textit{ qui sont premiers avec } n.$$

▷ D'après la proposition 2.2.13, $\varphi(n)$ est le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 22. 1) Pour $n = 1, \ldots, 12$, lister les inversibles de $\mathbb{Z}/n\mathbb{Z}$ et calculer $\varphi(n)$.

2) Pour un nombre premier p, calculer $\varphi(p)$.

3) Pour un nombre premier p et un entier $r \geqslant 1$, calculer $\varphi(p^r)$.

2.2.6 Retour sur le théorème chinois des restes

Une manière plus abstraite d'exprimer le théorème chinois des restes est la suivante.

Théorème 2.2.16 (Théorème chinois des restes). *Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. L'application*

$$g : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie par

$$g(\overline{k}) = (\widetilde{k}, \widehat{k})$$

est une bijection. (Où l'on utilise les notations $\overline{k}$, $\widetilde{k}$ et $\widehat{k}$ pour désigner les classes d'équivalence dans $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ respectivement.)

Démonstration. – Il faut montrer que g est bien définie ! On considère d'abord l'application

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie par

$$f(k) = (\widetilde{k}\,, \widehat{k}\,).$$

On montre que f passe au quotient par la relation de congruence modulo mn. Soient $k, k' \in \mathbb{Z}$ tels que $k \equiv k' \pmod{mn}$, c'est-à-dire $mn|(k-k')$. Alors notamment m et n divisent $k-k'$, et donc $\widetilde{k} = \widetilde{k'}$ et $\widehat{k} = \widehat{k'}$, d'où $f(k) = f(k')$. On a donc montré que f passe au quotient par la relation de congruence modulo mn, et on note g l'application définie sur le quotient.

– Soit $(\widetilde{a}\,, \widehat{b}\,) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Un antécédent de $(\widetilde{a}\,, \widehat{b}\,)$ par g est un $\overline{k} \in \mathbb{Z}/mn\mathbb{Z}$ tel que

$$\begin{cases} \widetilde{k} = \widetilde{a} \\ \widehat{k} = \widehat{b} \end{cases}$$

ou dit autrement tel que

$$\begin{cases} k \equiv a \pmod{m} \\ k \equiv b \pmod{n} \end{cases}$$

Le théorème chinois des restes (théorème 1.6.1) affirme qu'un tel k existe et qu'il est unique modulo mn. Dit autrement, il existe un unique antécédent $\overline{k} \in \mathbb{Z}/mn\mathbb{Z}$ de $(\widetilde{a}\,, \widehat{b}\,)$ par g. On a donc montré que g est bijective.

□

Remarque 2.2.17. Voici une autre manière de montrer que g est bijective sans utiliser le théorème chinois des restes du chapitre 1.

▷ On montre que g est injective. Soient $k, k' \in \mathbb{Z}$ tels que $g(\overline{k}) = g(\overline{k'})$, c'est-à-dire :

$$\begin{cases} \widetilde{k} = \widetilde{k'} \\ \widehat{k} = \widehat{k'} \end{cases}$$

Cela revient à dire que

$$\begin{cases} k \equiv k' \pmod{m} \\ k \equiv k' \pmod{n} \end{cases}$$

Alors par définition, on a que $m|(k-k')$ et $n|(k-k')$. Comme par hypothèse $m \wedge n = 1$, la variante du lemme de Gauss (théorème 1.4.2) implique que $mn|(k-k')$, et donc $k \equiv k' \pmod{mn}$, d'où $\overline{k} = \overline{k'}$. On a donc bien montré que g est injective.

▷ Comme g est une application entre deux ensembles de même cardinal mn, elle est donc automatiquement bijective ! (Une application entre deux ensembles finis de même cardinal est injective ssi elle est surjective ssi elle est bijective.)

Exercice 23. Écrire explicitement l'application g dans le cas $m = 3$, $n = 4$, et vérifier qu'elle est bijective. Faire de même dans le cas $m = 2$, $n = 4$, et montrer que dans ce cas-là elle n'est pas bijective.

2.2.7 Multiplicativité de l'indicatrice d'Euler

Théorème 2.2.18. *Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Alors on a :*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Démonstration. Pour un entier $r \in \mathbb{N}^*$, notons I_r l'ensemble des inversibles de $\mathbb{Z}/r\mathbb{Z}$. On a $\varphi(r) = |I_r|$ et l'équivalence :

$$\overline{k} \in I_r \quad \Longleftrightarrow \quad k \wedge r = 1.$$

De plus, on a l'équivalence (exercice 9) :

$$k \wedge (mn) = 1 \quad \Longleftrightarrow \quad (k \wedge m = 1 \ \text{ et } \ k \wedge n = 1).$$

On en déduit l'équivalence :

$$\overline{k} \in I_{mn} \quad \Longleftrightarrow \quad (\widetilde{k}\,, \widehat{k}\,) \in I_m \times I_n.$$

On voit donc que la bijection g du théorème 2.2.16 induit une bijection

$$h : I_{mn} \longrightarrow I_m \times I_n \ , \ \overline{k} \mapsto (\widetilde{k}\,, \widehat{k}\,).$$

On en déduit que $|I_{mn}| = |I_m| \times |I_n|$, c'est-à-dire $\varphi(mn) = \varphi(m)\varphi(n)$. □

Exercice 24. Déduire du théorème précédent et de l'exercice 22 la formule suivante pour l'indicatrice d'Euler :

$$\varphi(n) = n \times \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \tfrac{1}{p}\right).$$

2.3 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

On fixe dans cette partie un entier $n \in \mathbb{N}^*$.

2.3.1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ engendrés par un élément

Définition 2.3.1. *Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Le* **sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{a}$** *est le sous-ensemble formé par les classes des multiples de a dans $\mathbb{Z}/n\mathbb{Z}$:*

$$\langle \overline{a} \rangle = \{\overline{ka}\,,\, k \in \mathbb{Z}\}.$$

Le cas d'un diviseur de n

On commence par étudier le cas où a est un diviseur positif de n.

Proposition 2.3.2. *Soit $d \in \mathbb{N}^*$ un diviseur de n et notons $e = \frac{n}{d}$ le "diviseur complémentaire".*

1) Le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{d}$ est un ensemble à e éléments :

$$\langle \overline{d} \rangle = \{\overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \dots, \overline{(e-1)d}\}.$$

(Remarquer que $\overline{ed} = \overline{n} = \overline{0}$.)

2) Plus précisément, on a une bijection :

$$\mathbb{Z}/e\mathbb{Z} \longrightarrow \langle \overline{d} \rangle \;\;,\;\; \widetilde{k} \mapsto \overline{kd}.$$

(Où l'on utilise la notation $\widetilde{k}$ pour les classes d'entiers dans $\mathbb{Z}/e\mathbb{Z}$ pour éviter la confusion avec la notation $\overline{k}$ qui correspond aux classes d'entiers dans $\mathbb{Z}/n\mathbb{Z}$.)

3) Pour $d, d' \in \mathbb{N}^*$ deux diviseurs de n, on a : $\langle \overline{d} \rangle = \langle \overline{d'} \rangle \iff d = d'$.

Démonstration. 1) Clairement, l'ensemble $\{\overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \dots, \overline{(e-1)d}\}$ a bien e éléments puisque les entiers 0, d, $2d$, $3d, \dots, (e-1)d$ sont entre 0 et $n-1$ et deux à deux distincts. Par définition on a l'inclusion $\{\overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \dots, \overline{(e-1)d}\} \subset \langle \overline{d} \rangle$. Pour l'inclusion réciproque, soit $k \in \mathbb{Z}$ et considérons l'élément $\overline{kd} \in \mathbb{Z}/n\mathbb{Z}$. On écrit la division euclidienne de k par e sous la forme : $k = ae + b$ avec $0 \leqslant b < e$. On a alors :

$$\overline{kd} = \overline{aed + bd} = \overline{an + bd} = \overline{bd}$$

qui est dans $\{\overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \dots, \overline{(e-1)d}\}$ car $b \in \{0, \dots, e-1\}$. Cela montre l'inclusion réciproque et donc l'égalité.

2) Soit l'application

$$f : \mathbb{Z} \to \langle \overline{d} \rangle \;,\; k \mapsto \overline{kd}.$$

On montre que f passe au quotient par la relation de congruence modulo e. Soient $k, k' \in \mathbb{Z}$ tels que $k \equiv k' \pmod{e}$. Il existe donc $l \in \mathbb{Z}$ tel que $k = k' + le$. Alors on a :

$$f(k) = \overline{kd} = \overline{(k' + le)d} = \overline{k'd + ln} = \overline{k'd} = f(k').$$

Donc f passe au quotient et induit l'application

$$g : \mathbb{Z}/e\mathbb{Z} \to \langle \overline{d} \rangle \;,\; \widetilde{k} \mapsto \overline{kd}.$$

Clairement, g est surjective par définition de $\langle \overline{d} \rangle$. Comme par la partie 1), $\langle \overline{d} \rangle$ est de cardinal e, comme $\mathbb{Z}/e\mathbb{Z}$, on en déduit que g est bijective. (Une application entre deux ensembles finis de même cardinal est injective ssi elle est surjective ssi elle est bijective.)

3) C'est évident d'après la partie 1) vu que le cardinal de $\langle \overline{d} \rangle$ est $\frac{n}{d}$.

□

Remarque 2.3.3. On notera les cas particuliers "extrêmes" $d = 1$ et $d = n$: $\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ et $\langle \overline{n} \rangle = \{\overline{0}\}$.

Remarque 2.3.4. On verra au chapitre suivant que la bijection

$$g : \mathbb{Z}/e\mathbb{Z} \longrightarrow \langle \overline{d} \rangle$$

est un **isomorphisme de groupes** au sens où il respecte les lois $+$. En effet, on a pour tous $\widetilde{k}, \widetilde{l} \in \mathbb{Z}/e\mathbb{Z}$:

$$g(\widetilde{k} + \widetilde{l}) = g(\widetilde{k + l}) = \overline{(k+l)d} = \overline{kd + ld} = \overline{kd} + \overline{ld} = g(\widetilde{k}) + g(\widetilde{l}).$$

Exemple 2.3.5. Soit $n = 12$ et $d = 2$.

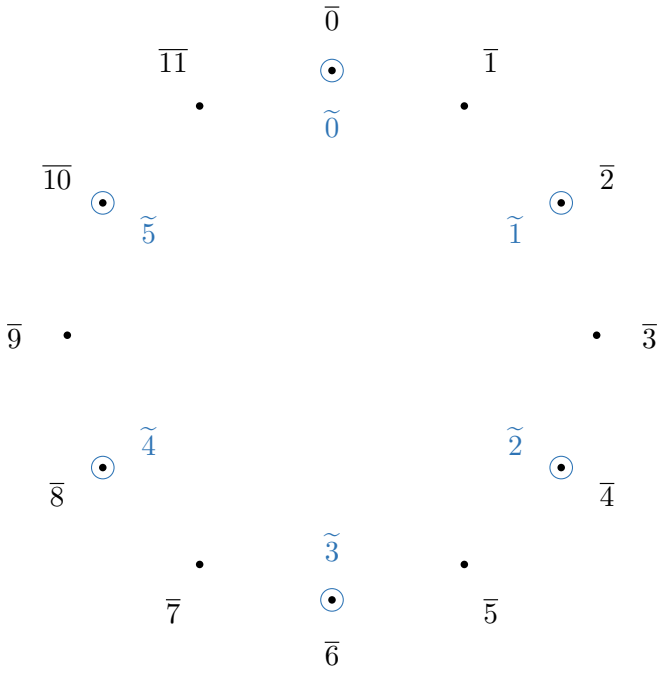
1) Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{2}$ est

$$\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}.$$

2) On a une bijection

$$\mathbb{Z}/6\mathbb{Z} \longrightarrow \langle \overline{2} \rangle \ , \ \widetilde{k} \mapsto \overline{2k}$$

donnée par $\widetilde{0} \mapsto \overline{0}$, $\widetilde{1} \mapsto \overline{2}$, $\widetilde{2} \mapsto \overline{4}$, $\widetilde{3} \mapsto \overline{6}$, $\widetilde{4} \mapsto \overline{8}$, $\widetilde{5} \mapsto \overline{10}$.



Exemple 2.3.6. Soit $n = 12$ et $d = 3$.

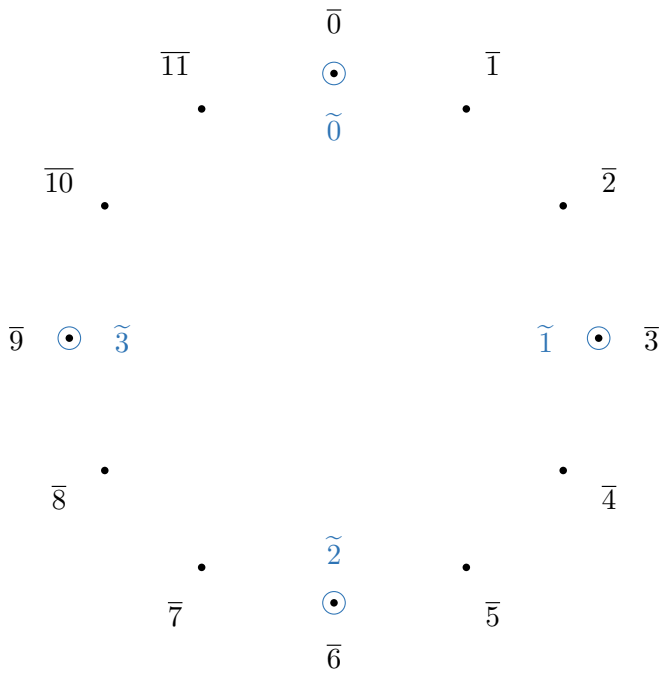
1) Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{3}$ est

$$\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}.$$

2) On a une bijection

$$\mathbb{Z}/4\mathbb{Z} \longrightarrow \langle \overline{3} \rangle \ , \ \widetilde{k} \mapsto \overline{3k}$$

donnée par $\widetilde{0} \mapsto \overline{0}$, $\widetilde{1} \mapsto \overline{3}$, $\widetilde{2} \mapsto \overline{6}$, $\widetilde{3} \mapsto \overline{9}$.



Le cas général

Passons maintenant au cas général.

Proposition 2.3.7. *1) Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et notons $d = a \wedge n$. Alors $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.*

2) Soient $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. Alors on a :

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

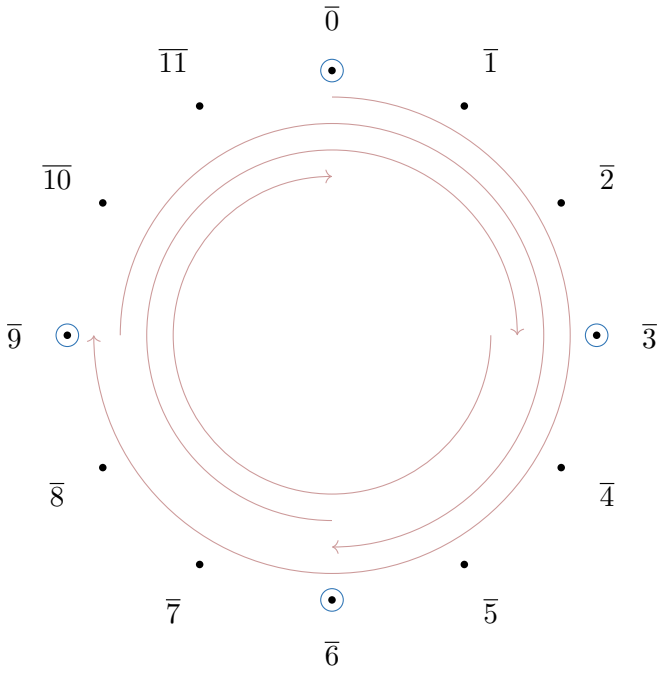
Démonstration. 1) – On montre que $\langle \overline{a} \rangle \subset \langle \overline{d} \rangle$. Comme $d = a \wedge n$, a est un multiple de d et on peut donc écrire $a = rd$ avec $r \in \mathbb{Z}$. Tout élément de $\langle \overline{a} \rangle$ s'écrit sous la forme $\overline{ka}$, qu'on peut donc réécrire $\overline{krd}$, et qui est donc dans $\langle \overline{d} \rangle$.

– On montre que $\langle \overline{d} \rangle \subset \langle \overline{a} \rangle$. D'après le théorème de Bézout, il existe des entiers u, v tels que $d = au + nv$. Tout élément de $\langle \overline{d} \rangle$ s'écrit sous la forme $\overline{kd} = \overline{k(au + nv)} = \overline{kau + nkv} = \overline{kua}$, et est donc dans $\langle \overline{a} \rangle$.

2) C'est une conséquence du 1) et de la partie 3) de la proposition 2.3.2.

□

Exemple 2.3.8. Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Un cas particulier de la proposition précédente est que pour $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ on a :

$$\langle \overline{a} \rangle = \mathbb{Z}/n\mathbb{Z} \quad \Longleftrightarrow \quad a \wedge n = 1.$$

Définition 2.3.9. *Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\langle \overline{a} \rangle = \mathbb{Z}/n\mathbb{Z}$ est appelé un* **générateur** *de $\mathbb{Z}/n\mathbb{Z}$.*

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont donc aussi, d'après la proposition 2.2.13, les inversibles de $\mathbb{Z}/n\mathbb{Z}$. Ils sont donc au nombre de $\varphi(n)$.

Exercice 25. Pour $n = 12$, quels sont les générateurs de $\mathbb{Z}/12\mathbb{Z}$? Pour chacun de ces générateurs, vérifiez que vous avez compris ce que cela veut dire en faisant tourner les aiguilles d'une horloge.

Exercice 26. Supposons que toutes les années ont 365 jours. Ma comète préférée passe à proximité de la Terre tous les 146 jours. Y aura-t-il une année où elle passera un 14 juillet ? Le résultat change-t-il si la comète passe à proximité de la Terre tous les 147 jours ?

2.3.2 Une vision axiomatique des sous-groupes

Dans le chapitre suivant on prendra un point de vue plus axiomatique sur les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (comparer la définition suivante avec la définition 1.3.1 du chapitre 1).

Définition 2.3.10. *Un* **sous-groupe de** $\mathbb{Z}/n\mathbb{Z}$ *est un sous-ensemble* $H \subset \mathbb{Z}/n\mathbb{Z}$ *qui vérifie les conditions suivantes :*

1) $\overline{0} \in H$ *;*

2) H *est stable par somme :* $\forall \overline{a}, \overline{b} \in H$, $\overline{a} + \overline{b} \in H$ *;*

3) H *est stable par passage à l'opposé :* $\forall \overline{a} \in H$, $-\overline{a} \in H$.

Proposition 2.3.11. *Pour tout* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\langle \overline{a} \rangle$ *est bien un sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Laissé au lecteur en exercice (faites-le !). □

La proposition suivante montre qu'on comprend déjà tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.3.12. *Soit* H *un sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$. *Alors il existe un unique diviseur positif* d *de* n *tel que* $H = \langle \overline{d} \rangle$.

Démonstration. L'unicité est une conséquence de la partie 3) de la proposition 2.3.2. Démontrons l'existence. On définit

$$H' = \{k \in \mathbb{Z} \mid \overline{k} \in H\} \quad \subset \mathbb{Z}.$$

On montre que H' est un sous-groupe de $\mathbb{Z}$:

1) $0 \in H'$ car $\overline{0} \in H$ puisque H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

2) H' est stable par somme : pour $a, b \in H'$, on a $\overline{a}, \overline{b} \in H$, et donc, comme H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ on a que $\overline{a} + \overline{b} \in H$, donc $\overline{a+b} \in H$ d'où $a + b \in H'$.

3) H' est stable par passage à l'opposé : pour $a \in H'$, on a $\overline{a} \in H$, et donc, comme H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, on a que $-\overline{a} \in H$, donc $\overline{-a} \in H$ d'où $-a \in H'$.

Le théorème 1.3.4 du chapitre 1 implique donc qu'il existe un entier $d \in \mathbb{N}$ tel que $H' = d\mathbb{Z}$. On en déduit que $H = \langle \overline{d} \rangle$. On prouve enfin que d divise n : comme $\overline{n} = \overline{0} \in H$, on a que $n \in H' = d\mathbb{Z}$, donc d divise n. □

Chapitre 3

Introduction à la théorie des groupes

3.1 Le langage des groupes

On rappelle qu'une **loi de composition interne** $*$ sur un ensemble E est une application

$$E \times E \to E\,,\ (x,y) \mapsto x * y.$$

3.1.1 Définition

Définition 3.1.1. *Un* **groupe** *est une paire $(G,*)$ où G est un ensemble et $*$ est une loi de composition interne sur G qui vérifie les axiomes suivants.*

(1) Associativité : $\forall x,y,z \in G\,,\ (x*y)*z = x*(y*z)$.

*(2) Élément neutre : il existe un élément $e \in G$ tel que $\forall x \in G\,,\ x*e = x = e*x$. On l'appelle l'***élément neutre** *du groupe.*

*(3) Inverse : pour tout $x \in G$ il existe un $y \in G$ tel que $x*y = e = y*x$. On l'appelle l'***inverse** *de x dans le groupe et on le note x^{-1}.*

On a donc :

$$x * x^{-1} = e = x^{-1} * x.$$

Remarque 3.1.2. Grâce à l'associativité de $*$ on n'est pas obligé de parenthéser quand on utilise plusieurs fois la loi $*$, et on peut écrire par exemple $x*y*z$ pour signifier $x*(y*z)$ ou $(x*y)*z$, qui sont égaux.

Proposition 3.1.3. *Soit $(G,*)$ un groupe. On a les propriétés suivantes :*

(a) L'élément neutre est unique. (Cela justifie le fait de l'appeler **l'***élément neutre.)*

(b) L'inverse d'un élément $x \in G$ est unique. (Cela justifie le fait de l'appeler **l'***inverse et de le noter x^{-1}.)*

(c) Pour tout $x \in G$ on a $(x^{-1})^{-1} = x$.

(d) Pour tous $x,y \in G$ on a $(x*y)^{-1} = y^{-1} * x^{-1}$.

Démonstration. (a) Supposons qu'il y ait deux éléments neutres $e, e' \in G$. Alors on a :

$$e' = e * e' = e$$

où dans la première égalité on a utilisé le fait que e est un élément neutre, et dans la deuxième égalité on a utilisé le fait que e' est un élément neutre. Donc $e = e'$ et on a prouvé que l'élément neutre est unique.

(b) Soit $x \in G$ et supposons qu'il existe $y, y' \in G$ qui vérifient

$$x * y = e = y * x \qquad \text{et} \qquad x * y' = e = y' * x.$$

Alors on a, en utilisant l'associativité de $*$:

$$y' = y' * e = y' * (x * y) = (y' * x) * y = e * y = y.$$

Donc $y = y'$ et on a prouvé que l'inverse est unique.

(c) C'est clair.

(d) Pour tous $x, y \in G$ on a, en utilisant l'associativité de $*$:

$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = y^{-1} * y = e$$

et de la même manière

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e.$$

Cela montre que $y^{-1} * x^{-1}$ est l'inverse de $x * y$, c'est-à-dire : $(x * y)^{-1} = y^{-1} * x^{-1}$. □

Définition 3.1.4. *Un dit qu'un groupe $(G, *)$ est* **abélien** *si la loi $*$ est commutative :*

$$\forall x, y \in G,\ x * y = y * x.$$

Exercice 27. Soit $(G, *)$ un groupe et soit $x \in G$. On suppose qu'il existe $y \in G$ tel que $x * y = e$. Montrer que $y = x^{-1}$.

Définition 3.1.5. *Un groupe $(G, *)$ est dit* **fini** *si l'ensemble G est fini. Son cardinal $|G|$ est alors appelé l'*__ordre__ *de G.*

Pour un groupe fini d'ordre $|G| = n$ pas trop grand, on peut écrire $G = \{x_1, \ldots, x_n\}$ et représenter la loi de composition interne $*$ sous la forme d'une **table de multiplication** (aussi appelée **table de Cayley**[1]), qui est un tableau à deux entrées qui contient le résultat de $x_i * x_j$ à l'intersection de la ligne i et de la colonne j.

[1] Nommée en l'honneur du mathématicien britannique Arthur Cayley (1821-1895).

3.1.2 Exemples

Exemples de groupes abéliens

▷ Un ensemble $G = \{e\}$ à un élément, muni de la loi $*$ définie par $e * e = e$, est un groupe abélien, qu'on appelle le **groupe trivial**.

(On remarque qu'un groupe ne peut pas être vide puisqu'il doit contenir un élément neutre.)

▷ $(\mathbb{Z}, +)$ est un groupe abélien. L'élément neutre est 0 et l'inverse de $n \in \mathbb{Z}$ est $-n$.

▷ $(\mathbb{R}, +)$, est un groupe abélien. Il en est de même pour $(\mathbb{K}, +)$ pour n'importe quel corps $\mathbb{K}$: par exemple, $(\mathbb{Q}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.

▷ Si V un $\mathbb{R}$-espace vectoriel, $(V, +)$ est un groupe abélien. Il en en de même pour les $\mathbb{K}$-espaces vectoriels, pour n'importe quel corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.

▷ $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien fini, d'ordre n. L'élément neutre est $\overline{0}$ et l'inverse de $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est $-\overline{a} = \overline{-a}$.

▷ $(\mathbb{R}^*, \times)$ est un groupe abélien. L'élément neutre est 1 et l'inverse d'un élément $x \in \mathbb{R}^*$ est $\frac{1}{x}$. Il en est de même pour $(\mathbb{K}^*, \times)$ pour n'importe quel corps $\mathbb{K}$: par exemple, $(\mathbb{Q}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.

Exercice 28. Écrire la table de multiplication du groupe $\mathbb{Z}/4\mathbb{Z}$.

Exemples de groupes non abéliens

▷ Pour tout $n \in \mathbb{N}$, on note $\mathrm{GL}_n(\mathbb{R})$ l'ensemble des matrices inversibles de taille n. Alors $(\mathrm{GL}_n(\mathbb{R}), \times)$ est un groupe qui n'est pas abélien si $n \geqslant 2$. On l'appelle le **groupe général linéaire** de degré n sur $\mathbb{R}$. L'élément neutre est la matrice identité I_n et l'inverse de $A \in \mathrm{GL}_n(\mathbb{R})$ est l'inverse usuel des matrices A^{-1}. Il en est de même pour $(\mathrm{GL}_n(\mathbb{K}), \times)$ pour n'importe quel corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.

▷ Soit V un $\mathbb{R}$-espace vectoriel et $\mathrm{Aut}(V)$ l'ensemble des automorphismes linéaires de V, c'est-à-dire des applications linéaires bijectives $f : V \to V$. Alors $(\mathrm{Aut}(V), \circ)$ est un groupe, qui n'est pas abélien si V est de dimension $\geqslant 2$. L'élément neutre est l'identité id_V et l'inverse de $f \in \mathrm{Aut}(V)$ est sa réciproque f^{-1}. Il en est de même si l'on part d'un espace vectoriel sur un corps $\mathbb{K}$, par exemple $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K} = \mathbb{C}$.

Exercice 29. Démontrer que $\mathrm{GL}_n(\mathbb{R})$ est abélien si $n \leqslant 1$ et ne l'est pas si $n \geqslant 2$. Pour V un $\mathbb{R}$-espace vectoriel, démontrer que $\mathrm{Aut}(V)$ est abélien si $\dim(V) \leqslant 1$ et non abélien si $\dim(V) \geqslant 2$.

▷ Pour tout $n \in \mathbb{N}$, notons $\mathfrak{S}_n$ l'ensemble des **permutations** de $\{1, \ldots, n\}$, c'est-à-dire des bijections $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Alors $(\mathfrak{S}_n, \circ)$ est un groupe, où l'élément neutre est l'identité $\mathrm{id}_{\{1,\ldots,n\}}$ et l'inverse de $\sigma \in \mathfrak{S}_n$ est sa réciproque σ^{-1}. On l'appelle le **groupe symétrique** sur n éléments. C'est un groupe fini d'ordre $n!$. Il n'est pas abélien si $n \geqslant 3$.

▷ Plus généralement, pour un ensemble E, fini ou infini, on définit l'ensemble $\mathrm{Bij}(E)$ des permutations de E, c'est-à-dire des bijections $\sigma : E \to E$. Alors $(\mathrm{Bij}(E), \circ)$ est un groupe qui n'est pas abélien si E a au moins 3 éléments.

Exercice 30. Lister les éléments de $\mathfrak{S}_2$, de $\mathfrak{S}_3$, de $\mathfrak{S}_4$. Écrire les tables de multiplication de $\mathfrak{S}_2$ et de $\mathfrak{S}_3$. Démontrer que $\mathfrak{S}_n$ est abélien si $n \leqslant 2$ et ne l'est pas si $n \geqslant 3$.

Non-exemples de groupes

- L'ensemble $\mathbb{Z}$ muni de la soustraction $-$ n'est pas un groupe car la loi $-$ n'est pas associative : on a $(7-2)-3=2$ et $7-(2-3)=8$.
- $(\mathbb{N},+)$ n'est pas un groupe car 7 n'a pas d'inverse pour $+$ dans $\mathbb{N}$.
- $(\mathbb{R},\times)$ n'est pas un groupe car 0 n'a pas d'inverse pour $\times$ dans $\mathbb{R}$.
- Pour $n \in \mathbb{N}^*$, notons $\mathrm{M}_n(\mathbb{R})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$. Alors $(\mathrm{M}_n(\mathbb{R}),\times)$ n'est pas un groupe car certaines matrices carrées n'ont pas d'inverse pour $\times$ dans $\mathrm{M}_n(\mathbb{R})$, par exemple la matrice nulle.
- Pour $n \in \mathbb{N}^*$, l'ensemble $\mathrm{GL}_n(\mathbb{R})$ muni de l'addition des matrices n'est pas un groupe... car l'addition des matrices n'est même pas une loi de composition interne sur $\mathrm{GL}_n(\mathbb{R})$. En effet, en général, la somme de deux matrices inversibles n'est pas inversible : par exemple, I_n et $-I_n$ sont inversibles mais leur somme est 0, qui n'est pas inversible.

3.1.3 Inversibles dans un monoïde

Définition 3.1.6. *Un* **monoïde** *est une paire $(M,*)$ où M est un ensemble et $*$ est une loi de composition interne sur M qui vérifie les axiomes suivants :*

(1) Associativité : $\forall x,y,z \in M$, $(x*y)*z = x*(y*z)$.

*(2) Élément neutre : il existe un élément $e \in M$ tel que $\forall x \in M$, $x*e = x = e*x$. On l'appelle l'***élément neutre** *du monoïde.*

Comme dans le cas d'un groupe, l'élément neutre est unique.

Définition 3.1.7. *Soit $(M,*)$ un monoïde. On dit qu'un élément $x \in M$ est* **inversible** *s'il existe $y \in M$ tel que $x*y = e = y*x$. On l'appelle l'***inverse** *de x dans M et on le note x^{-1}. On note*

$$M^\times \subset M$$

l'ensemble des éléments inversibles de M.

Comme dans le cas d'un groupe, l'inverse d'un élément est unique lorsqu'il existe.

Proposition 3.1.8. *Soit $(M,*)$ un monoïde. Alors $(M^\times,*)$ est un groupe.*

Démonstration. On montre facilement, comme dans la preuve du (d) de la proposition 3.1.3, que si $x,y \in M$ sont inversibles alors $x*y$ est inversible, d'inverse $y^{-1}*x^{-1}$. Donc $*$ est bien une loi de composition interne sur $M^\times$. Elle est associative car elle l'est sur M par définition. Elle a un élément neutre car l'élément neutre e de M est bien inversible : $e*e=e$. Enfin, chaque élément de $M^\times$ a un inverse pour $*$ par définition. □

Voici quelques exemples de cette construction.

- Si l'on part du monoïde $(\mathbb{R},\times)$, on obtient le groupe $(\mathbb{R}^*,\times)$. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$.

- Si l'on part du monoïde $(\mathrm{M}_n(\mathbb{R}), \times)$, on obtient le groupe $(\mathrm{GL}_n(\mathbb{R}), \times)$. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$.
- Pour tout $n \geqslant 1$, on peut considérer le monoïde $(\mathbb{Z}/n\mathbb{Z}, \times)$, on obtient alors le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$. C'est un groupe fini d'ordre $\varphi(n)$. Il est abélien puisque la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ est commutative.

Exercice 31. Écrire la table de multiplication du groupe $((\mathbb{Z}/8\mathbb{Z})^\times, \times)$.

Exercice 32. Vérifier que $(\mathbb{Z}, \times)$ est un monoïde. Quel est le groupe $(\mathbb{Z}^\times, \times)$?

3.1.4 Règles de calcul dans un groupe

Notation

On note souvent G à la place de $(G, *)$ quand la loi de composition interne est implicite. Par exemple : quand on écrit "le groupe $\mathbb{Z}$" on désigne implicitement le groupe $(\mathbb{Z}, +)$.

Quand on parle d'un groupe abstrait G on note souvent la loi de composition interne sous la forme **multiplicative**, en écrivant xy à la place de $x * y$. Dans ce cas on peut utiliser le symbole 1 pour l'élément neutre.

Dans le cadre d'un groupe abstrait qui est *abélien*, il est également commun d'utiliser plutôt la notation $+$ et de noter 0 l'élément neutre et $-x$ l'inverse de x (notation **additive**).

Puissances

Pour un élément $x \in G$ et un entier naturel $n \in \mathbb{N}$ on note x^n le produit n fois de x avec lui-même, défini par récurrence sur n par

$$x^0 = e \quad \text{et} \quad x^n = x^{n-1}x \quad \text{pour } n \geqslant 1.$$

On étend la notation x^n à tous les entiers relatifs $n \in \mathbb{Z}$ en posant, pour $n \in \mathbb{N}$:

$$x^{-n} = (x^{-1})^n.$$

On a les relations usuelles, valables pour tous $m, n \in \mathbb{Z}$:

$$x^{m+n} = x^m x^n \quad \text{et} \quad (x^m)^n = x^{mn}.$$

Remarque 3.1.9. Attention : on n'a pas en général $(xy)^n = x^n y^n$ pour $x, y \in G$ et $n \in \mathbb{N}$. Par exemple, $(xy)^2 = xyxy$ et $x^2y^2 = xxyy$. Si $xy = yx$ (par exemple si G est un groupe abélien) alors on a bien l'égalité.

Remarque 3.1.10. En notation additive, x^n s'écrit nx.

Simplification

On peut simplifier à gauche et à droite dans un groupe.

Proposition 3.1.11. *Soit G un groupe. Pour des éléments $x, y, z \in G$ on a les règles de simplification :*

$$xy = xz \iff y = z \qquad et \qquad xz = yz \iff x = y.$$

Démonstration. Dans les deux cas le sens $\Longleftarrow$ est évident. Pour le sens $\Longrightarrow$, il suffit de multiplier à gauche par x^{-1} dans le premier cas, à droite par z^{-1} dans le deuxième cas. □

Notamment, on a, pour G un groupe et $a, x, y \in G$:

$$ax = y \iff x = a^{-1}y.$$

Exercice 33. Montrer qu'en général la table de multiplication d'un groupe fini contient chaque élément du groupe dans chaque ligne et dans chaque colonne.

3.1.5 Produits de groupes

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit une loi de composition interne $*$ sur le produit cartésien $G_1 \times G_2$ par la formule :

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

Proposition 3.1.12. *Muni de cette loi de composition interne, $G_1 \times G_2$ est un groupe.*

Démonstration. Laissé au lecteur. On vérifie notamment que l'élément neutre de $G_1 \times G_2$ est (e_1, e_2), où e_1 est l'élément neutre de G_1 et e_2 l'élément neutre de G_2 ; et que l'inverse d'un élément $(x_1, x_2) \in G_1 \times G_2$ est (x_1^{-1}, x_2^{-1}). □

Définition 3.1.13. *On appelle $G_1 \times G_2$ le* **groupe produit** *(ou parfois* **produit direct***) de G_1 et G_2.*

Exercice 34. Écrire la table de multiplication du groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

▷ Plus généralement, pour une famille $(G_i)_{i \in I}$ de groupes indexée par un ensemble I, on peut former le produit

$$\prod_{i \in I} G_i,$$

qui est un groupe où la loi de groupe se calcule "coordonnée par coordonnée".

▷ Si tous les groupes G_i sont égaux au même groupe G, on note ce groupe G^I.

3.1.6 Fonctions à valeurs dans un groupe

Soit G un groupe et I un ensemble. Rappelons que G^I peut être vu comme l'ensemble des applications $f : I \to G$. Avec ce point de vue, la loi de groupe se calcule, pour $f_1, f_2 : I \to G$, par la formule

$$(f_1 f_2)(i) = f_1(i) f_2(i).$$

L'élément neutre est la fonction constante égale à e : $f(i) = e$ pour tout $i \in I$.

Exemple 3.1.14. Pour tout ensemble E, l'ensemble $\mathbb{Z}^E$ des applications $f : E \to \mathbb{Z}$ est un groupe pour l'addition des fonctions :

$$(f_1 + f_2)(x) = f_1(x) + f_2(x).$$

L'élément neutre est la fonction nulle.

3.2 Sous-groupes

3.2.1 Définition

Définition 3.2.1. *Soit G un groupe. Un* **sous-groupe** *de G est un sous-ensemble $H \subset G$ qui vérifie les conditions suivantes :*

1) $e \in H$;

2) H *est stable par produit :* $\forall x, y \in H$, $xy \in H$;

3) H *est stable par passage à l'inverse :* $\forall x \in H$, $x^{-1} \in H$.

Proposition 3.2.2. *Soit G un groupe, soit H un sous-groupe de G. Alors H, muni de la restriction de la loi de composition interne de G, est un groupe.*

Démonstration. Comme par l'hypothèse 2) H est stable par produit, la loi de composition interne de G induit bien une loi de composition interne sur H. Celle-ci est associative car elle l'est dans G. Elle a un élément neutre car par l'hypothèse 1) $e \in H$. Enfin, tout élément de H a un inverse dans H pour cette loi par l'hypothèse 3). □

Remarque 3.2.3. C'est une manière pratique de montrer que quelque chose est un groupe en montrant que c'est un sous-groupe d'un groupe déjà connu.

Exercice 35. Soit G un groupe et $H \subset G$ un sous-ensemble de G. Montrer que H est un sous-groupe de G si et seulement s'il vérifie les conditions suivantes :

1') $H \neq \varnothing$;

2') $\forall x, y \in H$, $xy^{-1} \in H$.

Remarque 3.2.4. Soit G un groupe et $H \subset G$ un sous-groupe. Alors pour tous $x, y \in H$ et pour tous $m, n \in \mathbb{Z}$, on a que $x^m y^n \in H$. (Savez-vous le prouver ?)

3.2.2 Exemples

▷ Pour tout groupe G on a les sous-groupes $\{e\}$ et G.

▷ On a déjà étudié les sous-groupes de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$ dans les chapitres précédents.

▷ Si V est un $\mathbb{R}$-espace vectoriel, tout sous-espace vectoriel $W \subset V$ est notamment un sous-groupe de V. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$. Il y a d'autres sous-groupes d'un espace vectoriel : par exemple $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ mais pas un sous-espace vectoriel (car $\mathbb{Z}$ n'est pas stable par multiplication par $\frac{1}{2}$, par exemple).

▷ On note

$$\mathbb{U} = \{z \in \mathbb{C}^* \,|\, |z| = 1\}$$

le cercle unité dans le plan complexe, et pour tout $n \in \mathbb{N}^*$,

$$\mathbb{U}_n = \{z \in \mathbb{C}^* \,|\, z^n = 1\}$$

l'ensemble des racines n-èmes de l'unité. On a des inclusions

$$\mathbb{U}_n \subset \mathbb{U} \subset \mathbb{C}^*$$

et $\mathbb{U}_n$ et $\mathbb{U}$ sont des sous-groupes de $\mathbb{C}^*$. On a le cas particulier important de $\mathbb{U}_2$, qui est le groupe $(\{-1, 1\}, \times)$.

▷ On rappelle la notation

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}.$$

C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, qu'on appelle le **groupe spécial linéaire** de degré n sur $\mathbb{R}$. De même en remplaçant $\mathbb{R}$ par un corps $\mathbb{K}$.

Exercice 36. Représenter dans le plan complexe les groupes $\mathbb{U}$, puis $\mathbb{U}_2$, $\mathbb{U}_3$, $\mathbb{U}_4$, $\mathbb{U}_5$, $\mathbb{U}_6$.

Exercice 37. Montrer que $\mathbb{U}_n$ et $\mathbb{U}$ sont des sous-groupes de $\mathbb{C}^*$. Montrer que $\mathrm{SL}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

Des non-exemples de sous-groupes :

▷ $H = \{\overline{0}, \overline{3}, \overline{4}\}$ n'est pas un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$ car $\overline{3} + \overline{4} = \overline{1} \notin H$.

▷ $\mathbb{N}$ n'est pas un sous-groupe de $\mathbb{Z}$ car il n'est pas stable par passage à l'opposé : $7 \in \mathbb{N}$ mais $-7 \notin \mathbb{N}$.

3.2.3 Sous-groupe engendré par une partie

Proposition 3.2.5. *Soit G un groupe, soit $(H_i)_{i\in I}$ une famille de sous-groupes de G indexée par un ensemble I. Alors l'intersection*

$$H = \bigcap_{i\in I} H_i$$

est un sous-groupe de G.

On rappelle la définition :

$$\bigcap_{i\in I} H_i = \{x \in G \mid \forall i \in I,\ x \in H_i\}.$$

▷ Notamment, si H et H' sont deux sous-groupes de G, alors l'intersection $H \cap H'$ est un sous-groupe de G.

Démonstration. 1) Pour tout $i \in I$, H_i est un sous-groupe de G, donc $e \in H_i$. On en déduit que $e \in H$.

2) Soit $x, y \in H$. Alors pour tout $i \in I$, $x \in H_i$ et $y \in H_i$, et donc $xy \in H_i$ car H_i est un sous-groupe de G. On en déduit que $xy \in H$.

3) Soit $x \in H$. Alors pour tout $i \in I$, $x \in H_i$ et donc $x^{-1} \in H_i$ car H_i est un sous-groupe de G. On en déduit que $x^{-1} \in H$.

□

Soit G un groupe et soit $S \subset G$ un sous-ensemble (pas nécessairement un sous-groupe).

Définition 3.2.6. *Le* **sous-groupe de** G **engendré par** S*, noté* $\langle S \rangle$*, est l'intersection de tous les sous-groupes de* G *qui contiennent* S*.*

C'est bien un sous-groupe de G par la proposition 3.2.5. On a clairement $S \subset \langle S \rangle$, et pour tout sous-groupe H de G on a l'équivalence :

$$S \subset H \quad \Longleftrightarrow \quad \langle S \rangle \subset H.$$

On dit donc que $\langle S \rangle$ est le plus petit (pour l'inclusion) sous-groupe de G qui contient S. Une image plus concrète de $\langle S \rangle$ est donnée par la proposition suivante.

Proposition 3.2.7. *Le sous-groupe* $\langle S \rangle$ *est l'ensemble des éléments de* G *qu'on peut obtenir en multipliant un certain nombre d'éléments de* S *et de leurs inverses, c'est-à-dire l'ensemble des produits*

$$x_1 x_2 \cdots x_n$$

avec $n \in \mathbb{N}$ *et pour tout* $i \in \{1, \ldots, n\}$*,* $x_i \in S \cup S^{-1}$*.*

On a noté S^{-1} l'ensemble des inverses des éléments de S. On prend aussi la convention qu'un produit indexé par l'ensemble vide dans un groupe est égal à l'élément neutre e.

Démonstration. Notons H_0 le sous-ensemble de G décrit par la proposition et montrons que $\langle S \rangle = H_0$. On montre d'abord que H_0 est un sous-groupe de G.

1) $e \in H_0$ (produit indexé par l'ensemble vide, c'est-à-dire avec $n = 0$).

2) H_0 est clairement stable par produit.

3) H_0 est stable par passage à l'inverse car l'inverse d'un produit $x_1 \cdots x_n$ est $x_n^{-1} \cdots x_1^{-1}$.

De plus, il est clair que $S \subset H_0$. Comme $\langle S \rangle$ est l'intersection de tous les sous-groupes de G qui contiennent S, on a donc l'inclusion $\langle S \rangle \subset H_0$.

Pour montrer l'inclusion réciproque $H_0 \subset \langle S \rangle$, il faut montrer que H_0 est inclus dans tous les sous-groupes de G qui contiennent S. Soit donc H un tel sous-groupe. Comme $S \subset H$ et que H contient e, est stable par produit et passage à l'opposé, tous les éléments $x_1 \cdots x_n$ avec $n \in \mathbb{N}$ et $x_i \in S \cup S^{-1}$ sont dans H. Donc $H_0 \subset H$. Comme cette inclusion est vraie pour tout sous-groupe H de G qui contient S, on en déduit que $H_0 \subset \langle S \rangle$. On a donc montré que $\langle S \rangle = H_0$. □

Définition 3.2.8. *On dit que* G *est* **engendré par** S *si* $\langle S \rangle = G$*. (On dit aussi que* S **engendre** G *ou que* S *est une* **partie génératrice** *de* G*.)*

▷ D'après la proposition 3.2.7, dire que G est engendré par S revient à dire que tout élément de G peut s'écrire comme un produit d'éléments de S et de leurs inverses.

▷ Lorsque $S = \{s_1, \ldots, s_k\}$ est finie, on note simplement.

$$\langle S \rangle = \langle s_1, \ldots, s_k \rangle.$$

Exercice 38. Montrer que le groupe symétrique $\mathfrak{S}_3$ est engendré par les transpositions $(1\ 2)$ et $(1\ 3)$:

$$\mathfrak{S}_3 = \langle\, (1\ 2), (1\ 3) \,\rangle.$$

Un cas important, qu'on étudiera en détail plus bas, est celui d'une partie à un élément s. Dans ce cas on a, d'après la proposition 3.2.7 :

$$\langle\, s \,\rangle = \{s^n,\ n \in \mathbb{Z}\}.$$

Remarque 3.2.9. En notation additive, cela s'écrit

$$\langle\, s \,\rangle = \{ns,\ n \in \mathbb{Z}\}.$$

Pour le groupe $\mathbb{Z}$, on retrouve donc les sous-groupes $\langle\, a \,\rangle = a\mathbb{Z}$. Pour le groupe $\mathbb{Z}/n\mathbb{Z}$, on retrouve les sous-groupes $\langle\, \overline{a} \,\rangle = \{\overline{ka},\ k \in \mathbb{Z}\}$.

Définition 3.2.10. *Un groupe G est* **cyclique** *(on dit aussi* **monogène***) s'il est engendré par un élément, c'est-à-dire s'il existe $s \in G$ tel que $G = \langle\, s \,\rangle$.*

▷ $\mathbb{Z} = \langle\, 1 \,\rangle$ est cyclique, et pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \langle\, \overline{1} \,\rangle$ est cyclique.

▷ On verra, quand on aura développé la notion d'isomorphisme de groupes, que ce sont les seuls groupes cycliques à isomorphisme près.

Exercice 39. Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un groupe cyclique.

Exercice 40. Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas un groupe cyclique. Montrer que $\mathfrak{S}_n$ n'est pas un groupe cyclique si $n \geqslant 3$.

Exercice 41. Montrer que $\mathbb{U}_n$ est un groupe cyclique, pour tout $n \in \mathbb{N}^*$.

▷ On verra, quand on aura développé la notion d'isomorphisme de groupes, que les groupes $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

Remarque 3.2.11. Dans certains ouvrages, la notion de groupe cyclique est réservée aux groupes finis, ce qui exclut $\mathbb{Z}$.

3.2.4 Rappel sur les sous-groupes de $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

On a déjà étudié les sous-groupes de $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ aux chapitres précédents.

Proposition 3.2.12. *Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique $n \in \mathbb{N}$ tel que*

$$H = \langle\, n \,\rangle = n\mathbb{Z}.$$

▷ Notons que l'unicité vient du fait qu'on a imposé que n soit dans $\mathbb{N}$: on a $\langle\, -n \,\rangle = \langle\, n \,\rangle$.

▷ Notamment, $\mathbb{Z} = \langle\, 1 \,\rangle = \langle\, -1 \,\rangle$.

Proposition 3.2.13. *Soit $n \in \mathbb{N}^*$. Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Il existe un unique diviseur positif d de n tel que*

$$H = \langle \overline{d} \rangle = \{\overline{kd},\ k \in \mathbb{Z}\}.$$

▷ Notons que l'unicité vient du fait qu'on a imposé que d soit un diviseur positif de n : on a $\langle \overline{a} \rangle = \langle \overline{d} \rangle$ pour tout $\overline{a}$ tel que $a \wedge n = d$.

▷ Notamment, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$ pour tout $\overline{a}$ tel que $a \wedge n = 1$.

3.3 Morphismes de groupes

3.3.1 Définitions

Définition 3.3.1. *Soient deux groupes $(G, *)$ et $(H, \#)$. Un* **morphisme de groupes** *de G dans H est une application $f : G \to H$ qui vérifie :*

$$\forall x, y \in G,\ f(x * y) = f(x) \# f(y).$$

Les morphismes de groupes sont parfois aussi appelés **homomorphismes de groupes**.

Remarque 3.3.2. En notation multiplicative, on écrit plutôt $f(xy) = f(x)f(y)$.

Proposition 3.3.3. *Soit $f : G \to H$ un morphisme de groupes.*

1) Si l'on note e_G et e_H les élément neutres respectifs de G et H, on a $f(e_G) = e_H$.

2) Pour tout $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Démonstration. 1) Comme f est un morphisme de groupes on a $f(e_G e_G) = f(e_G)f(e_G)$. Or $e_G e_G = e_G$, et on en déduit que $f(e_G) = f(e_G)f(e_G)$. En multipliant cette égalité par $f(e_G)^{-1}$, on obtient $e_H = f(e_G)$.

2) Soit $x \in G$. On calcule : $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$. Cela montre que l'inverse de $f(x)$ est $f(x^{-1})$, ou encore que $f(x^{-1}) = f(x)^{-1}$.

□

Proposition 3.3.4. *Soient $f : G \to H$ et $g : H \to K$ deux morphismes de groupes. Alors la composée $g \circ f : G \to K$ est un morphisme de groupes.*

Démonstration. Soient $x, y \in G$. On calcule :

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

□

Définition 3.3.5. *Un* **endomorphisme** *d'un groupe G est un morphisme de groupes de G dans G.*

Exercice 42. Soient G, H deux groupes et soit $f : G \to H$ un morphisme de groupes. Montrer que pour tout $x \in G$ et tout $n \in \mathbb{Z}$ on a $f(x^n) = (f(x))^n$.

3.3.2 Exemples

▷ L'application constante $f : G \to H$ définie par $f(x) = e_H$ pour tout $x \in G$, où e_H désigne l'élément neutre de H, est un morphisme de groupes. On l'appelle le **morphisme trivial**.

▷ L'identité d'un groupe G dans lui-même est un morphisme de groupes.

▷ Le déterminant des matrices est un morphisme de groupes

$$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^* \ , \ A \mapsto \det(A).$$

En effet, on a pour tous $A, B \in \mathrm{GL}_n(\mathbb{R})$ la formule

$$\det(AB) = \det(A)\det(B).$$

▷ La signature des permutations est un morphisme de groupes

$$\mathrm{sgn} : \mathfrak{S}_n \to \{-1, 1\} \ , \ \sigma \mapsto \mathrm{sgn}(\sigma),$$

c'est-à-dire qu'on a, pour deux permutations $\sigma, \sigma' \in \mathfrak{S}_n$:

$$\mathrm{sgn}(\sigma\sigma') = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\sigma').$$

▷ La fonction exponentielle induit un morphisme de groupes

$$\exp : \mathbb{R} \to \mathbb{R}^* \ , \ x \mapsto e^x.$$

(La loi de groupe dans $\mathbb{R}$ est $+$, la loi de groupe dans $\mathbb{R}^*$ est $\times$.) En effet, on a

$$\forall x, y \in \mathbb{R},\ \exp(x + y) = \exp(x)\exp(y).$$

▷ La fonction logarithme induit un morphisme de groupes

$$\ln : \mathbb{R}_+^* \to \mathbb{R} \ , \ x \mapsto \ln(x).$$

($\mathbb{R}_+^*$ est un groupe pour la multiplication parce que c'est un sous-groupe de $\mathbb{R}^*$... prouvez-le !) En effet on a

$$\forall x, y \in \mathbb{R}_+^*,\ \ln(xy) = \ln(x) + \ln(y).$$

▷ Soient V, W deux $\mathbb{R}$-espaces vectoriels. Toute application linéaire $f : V \to W$ est un morphisme de groupes (où l'on rappelle que la loi de groupe dans V et W est $+$).

Exercice 43. Lister tous les morphismes de groupes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$. Lister tous les endomorphismes de $\mathbb{Z}/3\mathbb{Z}$.

Exercice 44. Montrer que les endomorphismes de $\mathbb{Z}$ sont les applications $k \mapsto ak$ avec $a \in \mathbb{Z}$. Pour $n \in \mathbb{N}^*$, montrer que les endomorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\overline{k} \mapsto \overline{ak} = \overline{a} \times \overline{k}$, avec $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

3.3.3 Morphismes de groupes et sous-groupes

Proposition 3.3.6. *Soit $f : G \to H$ un morphisme de groupes.*

1) Soit H' un sous-groupe de H. Alors l'image réciproque $f^{-1}(H')$ est un sous-groupe de G.

2) Soit G' un sous-groupe de G. Alors l'image directe $f(G')$ est un sous-groupe de H.

Démonstration. 1) – Comme $f(e_G) = e_H$ et que $e_H \in H'$ car H' est un sous-groupe de H, on a que $e_G \in f^{-1}(H')$.

- On montre que $f^{-1}(H')$ est stable par produit. Soient $x_1, x_2 \in f^{-1}(H')$, alors $f(x_1) \in H'$ et $f(x_2) \in H'$. Comme H' est un sous-groupe de H, $f(x_1)f(x_2) \in H'$. Or, $f(x_1)f(x_2) = f(x_1x_2)$ et donc $f(x_1x_2) \in H'$, d'où $x_1x_2 \in f^{-1}(H')$.
- On montre que $f^{-1}(H')$ est stable par inverse. Soit $x \in f^{-1}(H')$, alors $f(x) \in H'$. Comme H' est un sous-groupe de H, $f(x)^{-1} \in H'$. Or $f(x)^{-1} = f(x^{-1})$ et donc $f(x^{-1}) \in H'$, d'où $x^{-1} \in f^{-1}(H')$.

2) – Comme G' est un sous-groupe de G, $e_G \in G'$. Or $f(e_G) = e_H$, donc $e_H \in f(G')$.

- On montre que $f(G')$ est stable par produit. Soient $y_1, y_2 \in f(G')$, il existe $x_1, x_2 \in G'$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$. On a donc $y_1y_2 = f(x_1)f(x_2) = f(x_1x_2)$, qui appartient à $f(G')$ car $x_1x_2 \in G'$ car G' est un sous-groupe de G.
- On montre que $f(G')$ est stable par inverse. Pour $y \in f(G')$, il existe $x \in G'$ tel que $y = f(x)$. Alors $y^{-1} = f(x)^{-1} = f(x^{-1})$, qui appartient à $f(G')$ car $x^{-1} \in G'$ car G' est un sous-groupe de G.

□

Définition 3.3.7. *Soit $f : G \to H$ un morphisme de groupes. On appelle* **noyau** *de f et on note* $\ker(f)$ *le sous-ensemble*

$$\ker(f) = \{x \in G \,|\, f(x) = e_H\},$$

où e_H désigne l'élément neutre de H.

On rappelle aussi la notation

$$\mathrm{Im}(f) = f(G) = \{f(x),\, x \in G\}.$$

Proposition 3.3.8. *Soit $f : G \to H$ un morphisme de groupes. Alors* $\ker(f)$ *est un sous-groupe de G et* $\mathrm{Im}(f)$ *est un sous-groupe de H.*

Démonstration. Pour le noyau, c'est un cas particulier de la proposition 3.3.6 1) avec $H' = \{e_H\}$. Pour l'image, c'est un cas particulier de la proposition 3.3.6 2) avec $G' = G$. □

Proposition 3.3.9. *Soit $f : G \to H$ un morphisme de groupes. Alors f est injectif si et seulement si* $\ker(f) = \{e_G\}$*, où e_G désigne l'élément neutre de G.*

Démonstration. Si f est injectif, alors comme $f(e_G) = e_H$, e_G doit être le seul antécédent de e_H par f, d'où $\ker(f) = \{e_G\}$. Réciproquement, supposons que $\ker(f) = \{e_G\}$ et montrons que f est injectif. Soient $x, y \in G$ tels que $f(x) = f(y)$, alors $f(x)f(y)^{-1} = e_H$, ou encore, en utilisant les propriétés déjà vues des morphismes de groupes : $f(xy^{-1}) = e_H$. Donc $xy^{-1} \in \ker(f)$, et donc par hypothèse $xy^{-1} = e_G$, d'où $x = y$. On a donc bien démontré que f est injectif. □

3.3.4 Isomorphismes de groupes

Définition 3.3.10. *Soient deux groupes G et H. Un* **isomorphisme de groupes** *de G dans H est un morphisme de groupes bijectif de G dans H. S'il existe un isomorphisme de groupes de G dans H on dit que G est* **isomorphe** *à H, ou que G et H sont isomorphes, et on note $G \simeq H$.*

Exemple 3.3.11. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n, et choisissons une base $\mathcal{B}$ de V. On a l'application

$$\mathrm{Mat}_{\mathcal{B}} : \mathrm{Aut}(V) \to \mathrm{GL}_n(\mathbb{R}) \ , \ f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$$

qui est bijective d'après le cours d'algèbre linéaire. (On rappelle que $\mathrm{Mat}_{\mathcal{B}}(f)$ désigne la matrice de f dans la base $\mathcal{B}$.) C'est un isomorphisme de groupes car on a, pour deux automorphismes linéaires $f, g : V \to V$:

$$\mathrm{Mat}_{\mathcal{B}}(f \circ g) = \mathrm{Mat}_{\mathcal{B}}(f) \times \mathrm{Mat}_{\mathcal{B}}(g).$$

On a donc un isomorphisme de groupes :

$$\mathrm{Aut}(V) \simeq \mathrm{GL}_n(\mathbb{R}).$$

La proposition suivante montre que si $G \simeq H$ alors $H \simeq G$.

Proposition 3.3.12. *Soit $f : G \to H$ un isomorphisme de groupes. Alors sa réciproque $f^{-1} : H \to G$ est aussi un isomorphisme de groupes.*

Démonstration. Il est clair que f^{-1} est bijectif et on doit juste montrer que c'est un morphisme de groupes. Soient $y_1, y_2 \in H$, on a :

$$f(f^{-1}(y_1)f^{-1}(y_2)) = f(f^{-1}(y_1))f(f^{-1}(y_2)) = y_1 y_2,$$

et donc $f^{-1}(y_1 y_2) = f^{-1}(y_1)f^{-1}(y_2)$. □

Exercice 45. Montrer que si $G \simeq H$ et $H \simeq K$ alors $G \simeq K$.

Exercice 46. Soit $n \in \mathbb{N}^*$. Montrer que les groupes $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont isomorphes.

Remarque 3.3.13. Si G et H sont deux groupes finis, dire que $G \simeq H$ revient à dire que G et H ont la même table de multiplication quitte à renommer certains éléments (c'est-à-dire à permuter certaines lignes et colonnes).

Remarque 3.3.14. Deux groupes G et H qui sont isomorphes ont **les mêmes propriétés** (les propriétés qui s'énoncent dans le langage de la théorie des groupes). Ainsi, pour montrer que deux groupes G et H ne sont pas isomorphes, il suffit de trouver une propriété (qui s'énonce dans le langage de la théorie des groupes) qui est vraie dans G et pas dans H, ou vice versa. À titre d'exemple, on conseille l'exercice suivant.

Exercice 47. Soient G et H deux groupes qui sont isomorphes.

1) Montrer que si G est abélien alors H est abélien.

2) Montrer que si G est cyclique alors H est cyclique.

3) Montrer que si l'équation $x^5 = e_G$ a 10 solutions $x \in G$ alors l'équation $y^5 = e_H$ a 10 solutions $y \in H$.

Le théorème chinois des restes refait son apparition :

Théorème 3.3.15. *Soient $m, n \in \mathbb{N}$ avec $m \wedge n = 1$. Alors on a un isomorphisme de groupes :*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Démonstration. Le théorème chinois des restes (théorème 2.2.16) affirme qu'on a une bijection

$$g : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\ ,\ \overline{k} \mapsto (\,\widetilde{k}\,,\,\widehat{k}\,).$$

C'est un morphisme de groupes. En effet, on a pour tous $\overline{k}, \overline{l} \in \mathbb{Z}/mn\mathbb{Z}$:

$$g(\overline{k}+\overline{l}) = g(\overline{k+l}) = (\widetilde{k+l}, \widehat{k+l}) = (\widetilde{k}+\widetilde{l}, \widehat{k}+\widehat{l}) = (\widetilde{k}, \widehat{k}) + (\widetilde{l}, \widehat{l}) = g(\overline{k}) + g(\overline{l}).$$

C'est donc un isomorphisme de groupes. □

Exercice 48. Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes (même s'il existe une bijection entre les ensembles sous-jacents à ces deux groupes).

Remarque 3.3.16. Soit $f : G \to H$ un morphisme de groupes qui est **injectif**. Alors f induit un isomorphisme de groupes $G \simeq f(G)$. (On rappelle que $f(G)$ est un sous-groupe de H.) Donc G est isomorphe à un sous-groupe de H.

Définition 3.3.17. *Soit G un groupe. Un* **automorphisme** *de G est un isomorphisme de G dans G. (Ou dit autrement, c'est un endomorphisme de G qui est bijectif.)*

3.4 Autour de la notion d'ordre

3.4.1 Ordre d'un élément dans un groupe

Définition 3.4.1. *Soit G un groupe et soit $x \in G$. L'***ordre** *de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $x^n = e$, avec la convention que x est d'***ordre infini** *si pour tout $n \in \mathbb{N}^*$, $x^n \neq e$.*

Remarque 3.4.2. En notation additive : l'ordre de x dans G est le plus petit $n \in \mathbb{N}^*$ tel que $nx = 0$, avec la convention que x est d'ordre infini si pour tout $n \in \mathbb{N}^*$, $nx \neq 0$.

Exemple 3.4.3. Le seul élément d'ordre 1 dans un groupe G est l'élément neutre e. Un élément x est d'ordre 2 si et seulement si $x \neq e$ et $x^2 = e$.

Pour un élément $x \in G$, considérons l'application

$$\varphi_x : \mathbb{Z} \to G \ , \ k \mapsto x^k.$$

C'est un morphisme de groupes : pour $k, k' \in \mathbb{Z}$ on a

$$\varphi_x(k + k') = x^{k+k'} = x^k x^{k'} = \varphi_x(k)\varphi_x(k').$$

Remarque 3.4.4. On montre facilement que φ_x est l'unique morphisme de groupes de $\mathbb{Z}$ dans G qui envoie 1 sur x.

Proposition 3.4.5. *Soit G un groupe, soit $x \in G$.*

▷ *Si x est d'ordre infini, φ_x induit un isomorphisme de groupes*

$$\mathbb{Z} \to \langle x \rangle \ , \ k \mapsto x^k.$$

▷ *Si x est d'ordre fini $n \in \mathbb{N}^*$, φ_x induit un isomorphisme de groupes*

$$\mathbb{Z}/n\mathbb{Z} \to \langle x \rangle \ , \ \overline{k} \mapsto x^k$$

et notamment

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

En particulier, l'ordre de x est égal à l'ordre du groupe $\langle x \rangle$.

Démonstration. Par définition, le sous-groupe de G engendré par x est l'image de φ_x :

$$\langle x \rangle = \mathrm{Im}(\varphi_x).$$

Comme φ_x est un morphisme de groupes, le noyau $\ker(\varphi_x)$ est un sous-groupe de $\mathbb{Z}$, et est donc de la forme

$$\ker(\varphi_x) = n\mathbb{Z}$$

avec $n \in \mathbb{N}$.

▷ Cas où $n = 0$. Donc $\ker(\varphi_x) = \{0\}$, et il n'existe aucun $k \in \mathbb{N}^*$ tel que $x^k = e$, d'où x est d'ordre infini. De plus, φ_x est injectif et induit donc un isomorphisme entre $\mathbb{Z}$ et $\langle\, x \,\rangle$.

▷ Cas où $n \geqslant 1$. Alors x est d'ordre n par définition. De plus, φ_x passe au quotient par la relation de congruence modulo n. En effet, pour $k \equiv k' \pmod{n}$, il existe $l \in \mathbb{Z}$ tel que $k = k' + ln$ et donc

$$\varphi_x(k) = x^k = x^{k'+ln} = x^{k'}(x^n)^l = x^{k'}e^l = x^{k'} = \varphi_x(k').$$

On obtient donc une application

$$\psi_x : \mathbb{Z}/n\mathbb{Z} \longrightarrow G\ ,\ \overline{k} \mapsto x^k.$$

On démontre facilement que ψ_x est un morphisme de groupes : pour $\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z}$ on a

$$\psi_x(\overline{k} + \overline{l}) = \psi_x(\overline{k+l}) = x^{k+l} = x^k x^l = \psi_x(\overline{k})\psi_x(\overline{l}).$$

Clairement, $\mathrm{Im}(\psi_x) = \mathrm{Im}(\varphi_x) = \langle\, x \,\rangle$. On démontre que ψ_x est injectif en démontrant que $\ker(\psi_x) = \{\overline{0}\}$. Soit $\overline{k} \in \ker(\psi_x)$, alors $x^k = e$ et donc $k \in \ker(\varphi_x) = n\mathbb{Z}$, donc $n|k$ et $\overline{k} = \overline{0}$. Conclusion : ψ_x est un morphisme de groupes injectif et d'image $\langle\, x \,\rangle$. Donc il induit un isomorphisme de groupes entre $\mathbb{Z}/n\mathbb{Z}$ et $\langle\, x \,\rangle$.

□

Exercice 49. Dans chaque cas, donner l'ordre de x dans le groupe G et décrire $\langle\, x \,\rangle$.

▷ $G = \mathbb{Z}$, $x = 1$.

▷ $G = \mathbb{Z}$, $x = -1$.

▷ $G = \mathbb{Z}$, $x = 2$.

▷ $G = \mathbb{R}^*$, $x = 1$.

▷ $G = \mathbb{R}^*$, $x = -1$.

▷ $G = \mathbb{R}^*$, $x = 2$.

▷ $G = \mathfrak{S}_4$, $x = (1\ 2\ 3)(3\ 4)$.

▷ $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

▷ $G = \mathrm{GL}_2(\mathbb{R})$, $x = \begin{pmatrix} 2 & -2 \\ 4 & -7 \end{pmatrix}$.

▷ $G = \mathbb{Z}/24\mathbb{Z}$, $x = \overline{14}$.

Exercice 50. Dans $\mathbb{Z}/n\mathbb{Z}$, quel est l'ordre d'un élément $\overline{k}$?

Exercice 51. Soit G un groupe, soit $x \in G$ un élément d'ordre fini n. Pour un élément $k \in \mathbb{Z}$, quel est l'ordre de x^k ?

Remarque 3.4.6. Dans un groupe **fini** G, tout élément $x \in G$ est d'ordre fini. En effet, si x était d'ordre infini alors le sous-groupe $\langle x \rangle \subset G$ serait infini (en bijection avec $\mathbb{Z}$), ce qui contredirait la finitude de G.

Proposition 3.4.7. *Soit G un groupe et soit $x \in G$ un élément d'ordre fini n. Alors pour tout $r \in \mathbb{Z}$ on a l'équivalence :*

$$x^r = e \quad \Longleftrightarrow \quad n|r.$$

Démonstration. Avec les notations ci-dessus, $x^r = e$ si et seulement si $r \in \ker(\varphi_x)$. Or $\ker(\varphi_x) = n\mathbb{Z}$ et donc c'est équivalent à $n|r$. □

Remarque 3.4.8. On a tendance à faire l'erreur de dire que si $x^r = e$ alors x est d'ordre r, ce qui est évidemment faux.

3.4.2 Retour sur les groupes cycliques

Proposition 3.4.9. *Soit G un groupe. Alors G est cyclique si et seulement s'il est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.*

Démonstration. Comme $\mathbb{Z}$ et tous les $\mathbb{Z}/n\mathbb{Z}$ sont des groupes cycliques, tout groupe isomorphe à un de ces groupes est cyclique (voir l'exercice 47). Réciproquement, si G est cyclique alors il existe $x \in G$ tel que $G = \langle x \rangle$, et la proposition 3.4.5 dit que G est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$. □

Proposition 3.4.10. *Soit G un groupe cyclique d'ordre fini $n \in \mathbb{N}^*$, et soit x un générateur de G. Pour chaque diviseur d de n, il existe exactement un sous-groupe de G d'ordre d, qui est le groupe cyclique engendré par $x^{n/d}$. Ce sont tous les sous-groupes de G.*

Démonstration. D'après la proposition 3.4.5, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq G$ qui envoie $\overline{k}$ sur x^k. Le résultat est alors une conséquence de la classification des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (proposition 3.2.13). □

Proposition 3.4.11. *Soit G un groupe cyclique d'ordre fini $n \in \mathbb{N}^*$, et soit x un générateur de G. Les générateurs de G sont les x^a avec $a \wedge n = 1$.*

Démonstration. D'après la proposition 3.4.5, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq G$ qui envoie $\overline{k}$ sur x^k. Le résultat est alors une conséquence de la classification des générateurs de $\mathbb{Z}/n\mathbb{Z}$. □

3.4.3 Le théorème de Lagrange

Théorème 3.4.12 (Théorème de Lagrange). *Soit G un groupe fini et soit H un sous-groupe de G. Alors $|H|$ divise $|G|$.*

Démonstration. On définit une relation $\sim$ sur G par :

$$x \sim y \iff \exists h \in H,\ xh = y.$$

On montre que c'est une relation d'équivalence.

1) Réflexivité. Soit $x \in G$, alors $xe = x$. Comme H est un sous-groupe de G, $e \in H$, et on en déduit que $x \sim x$.

2) Symétrie. Soient $x, y \in G$ tels que $x \sim y$. Alors il existe $h \in H$ tel que $xh = y$, et donc $x = yh^{-1}$. Comme H est un sous-groupe de G, $h^{-1} \in H$, et on en déduit que $y \sim x$.

3) Transitivité. Soient $x, y, z \in G$ tels que $x \sim y$ et $y \sim z$. Alors il existe $h, h' \in H$ tels que $xh = y$ et $yh' = z$. On a donc $xhh' = z$. Comme H est un sous-groupe de G, $hh' \in H$, et on en déduit que $x \sim z$.

On étudie maintenant les classes d'équivalence pour cette relation. Soit $x \in G$, on a une application

$$\mu : H \to \overline{x}\ ,\ h \mapsto xh.$$

Clairement, μ est surjectif par définition de $\overline{x}$. De plus, μ est injectif car $xh = xh'$ implique $h = h'$. Donc μ est bijectif, et donc la classe d'équivalence $\overline{x}$ a le même cardinal que H. Soit n le nombre de classes d'équivalences, c'est-à-dire le cardinal du quotient $G/\sim$. Comme les classes d'équivalence forment une partition de G, on a alors $|G| = n \times |H|$ et donc $|H|$ divise $|G|$. □

Définition 3.4.13. *Soit G un groupe fini et soit H un sous-groupe de G. Le quotient $\frac{|G|}{|H|}$ est appelé l'***indice** *de H dans G.*

Remarque 3.4.14. La classe d'équivalence $\overline{x}$ qui apparaît dans la preuve du théorème est aussi notée xH et appelée la **classe à gauche** de x suivant le sous-groupe H. L'ensemble des classes à gauche est noté G/H. On peut aussi considérer la **classe à droite** Hx, qui est la classe d'équivalence de x pour la relation d'équivalence où $x \sim y$ s'il existe $h \in H$ tel que $hx = y$. L'ensemble des classes à droite est noté $H\backslash G$. En général ces deux concepts sont différents : on peut avoir $xH \neq Hx$. (Mais clairement ces deux concepts coïncident si G est un groupe abélien.) Vous verrez au semestre prochain la notion de **sous-groupe distingué**, qui est un sous-groupe H de G tel que pour tout $x \in G$, $xH = Hx$. Cela permet de mettre une structure de groupe sur le quotient $G/H = H\backslash G$, qui s'appelle le **groupe quotient**. L'exercice suivant donne un exemple de sous-groupe qui n'est pas distingué.

Exercice 52. Soit $G = \mathfrak{S}_3$ et soit $H = \langle \tau \rangle = \{\mathrm{id}, \tau\}$ où τ est la transposition (1 2). Lister les classes à gauche des éléments de G suivant H, puis les classes à droite.

Théorème 3.4.15. *Soit G un groupe fini et soit $x \in G$. Alors l'ordre de x divise $|G|$.*

Démonstration. C'est une conséquence du théorème de Lagrange et du fait que l'ordre de x est égal à $|\langle x \rangle|$. □

Ce dernier théorème a la formulation équivalente suivante, par la proposition 3.4.7 :

Théorème 3.4.16. *Soit G un groupe fini. Pour tout $x \in G$ on a :*

$$x^{|G|} = e.$$

3.4.4 Application aux groupes d'ordre premier

Théorème 3.4.17. *Soit G un groupe d'ordre premier p. Alors G est cyclique, c'est-à-dire isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

▷ À isomorphisme près, $\mathbb{Z}/17\mathbb{Z}$ est donc le seul groupe d'ordre 17.

Démonstration. Comme $p \geqslant 2$, il existe un élément $x \in G$ avec $x \neq e$. On considère le sous-groupe $\langle x \rangle$ de G engendré par x. Comme $x \neq e$, ce n'est pas le groupe trivial. Par le théorème de Lagrange, l'ordre de $\langle x \rangle$ est un diviseur de p, et comme p est premier, on a donc $|\langle x \rangle| = p$. Comme $|G| = p$, on a donc $G = \langle x \rangle$, et donc G est cyclique. □

Remarque 3.4.18. Le théorème est évidemment faux en général sans l'hypothèse "p premier". Par exemple, on rappelle que le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique.

3.5 Étude du groupe symétrique

On fixe un entier $n \in \mathbb{N}$ et on se place dans le groupe symétrique $\mathfrak{S}_n$.

3.5.1 Décomposition en produit de cycles de supports disjoints

On rappelle les notions de cycle et de transposition.

Définition 3.5.1. *Pour un entier $k \geqslant 2$ et des éléments $i_1, i_2, \ldots, i_k$ deux à deux disjoints dans $\{1, \ldots, n\}$, le* **cycle** *(aussi appelé* **permutation circulaire***)*

$$\gamma = (i_1\ i_2\ \cdots\ i_k) \in \mathfrak{S}_n$$

est la permutation définie par

$$\begin{cases} \gamma(i_1) = i_2,\ \gamma(i_2) = i_3,\ \ldots,\ \gamma(i_{k-1}) = i_k,\ \gamma(i_k) = i_1 \\ \gamma(x) = x \quad \text{pour tout } x \in \{1, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}. \end{cases}$$

L'ensemble $\{i_1, i_2, \ldots, i_k\}$ est le **support** *de γ. L'entier k est la* **longueur** *de γ. (On dit aussi que γ est un k-***cycle***.)*

▷ Un k-cycle est d'ordre k dans $\mathfrak{S}_n$.

Exercice 53. Réciproquement, est-ce que tout élément de $\mathfrak{S}_n$ d'ordre k est un k-cycle ?

Définition 3.5.2. *Une* **transposition** *est un cycle de longueur 2, c'est-à-dire de la forme $(i\ j)$ pour deux éléments $i \neq j$ de $\{1, \ldots, n\}$.*

Proposition 3.5.3. *Soit $\sigma \in \mathfrak{S}_n$. Alors σ a une décomposition unique (à l'ordre des facteurs près) en produit de cycles de supports disjoints :*

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r$$

avec $r \in \mathbb{N}$ et les γ_i des cycles de $\mathfrak{S}_n$ dont les supports sont deux à deux disjoints.

Remarque 3.5.4. Deux cycles $\gamma, \gamma' \in \mathfrak{S}_n$ de supports disjoints commutent : $\gamma\gamma' = \gamma'\gamma$.

Exercice 54. Déterminer la décomposition en produit de cycles à supports disjoints de la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 9 & 6 & 7 & 4 & 5 & 3 & 1 \end{pmatrix}.$$

Exercice 55. Calculer l'inverse de la permutation $(1\ 3\ 7)(2\ 9\ 4\ 5)(6\ 8) \in \mathfrak{S}_9$.

Exercice 56. Avec les notations de la proposition 3.5.3, exprimer l'ordre de σ en fonction des longueurs des cycles γ_i. Quel est l'ordre maximal d'un élément du groupe symétrique $\mathfrak{S}_5$? de $\mathfrak{S}_6$? de $\mathfrak{S}_7$? de $\mathfrak{S}_8$?

3.5.2 Des systèmes de générateurs du groupe symétrique

Proposition 3.5.5. *Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions.*

Démonstration. Par la proposition 3.5.3, $\mathfrak{S}_n$ est engendré par les cycles. Il suffit donc de prouver que tout cycle peut s'écrire comme un produit de transpositions. C'est facile : on vérifie facilement que pour des éléments $i_1, \dots, i_k$ deux à deux distincts de $\{1, \dots, n\}$ on a

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k).$$

□

Remarque 3.5.6. Cette dernière formule ne tombe pas du ciel : si vous avez en face de vous des objets numérotés de 1 à k et que vous voulez opérer une permutation circulaire sur ces objets en ayant seulement le droit de permuter les objets deux par deux, comment vous y prendriez-vous ?

Exercice 57. Écrire la permutation de l'exercice 54 comme un produit de transpositions.

Proposition 3.5.7. *Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions adjacentes $(i\ i+1)$ pour $1 \leqslant i \leqslant n-1$.*

Démonstration. D'après la proposition 3.5.5, $\mathfrak{S}_n$ est engendré par les transpositions. Il suffit donc de prouver que toute transposition peut s'écrire comme un produit de transpositions adjacentes.

- ▷ On démontre par récurrence sur $k \geqslant 1$ qu'une transposition $(i\ j)$ avec $j - i = k$ peut s'écrire comme un produit de transpositions adjacentes.
- ▷ Initialisation : si $j - i = 1$, une transposition $(i\ i+1)$ est une transposition adjacente et il n'y a rien à prouver.
- ▷ Hérédité : on suppose l'hypothèse de récurrence prouvée pour un certain $k \geqslant 1$. Si $j - i = k + 1 \geqslant 2$ alors on a :

  $$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j).$$

  Puisque $(j-1) - i = k$, l'hypothèse de récurrence implique que la transposition $(i\ j-1)$ peut s'écrire comme un produit de transpositions adjacentes. Comme $(j-1\ j)$ est une transposition adjacente, on a donc montré que $(i\ j)$ peut s'écrire comme un produit de transpositions adjacentes.
- ▷ On a donc bien montré que toute transposition peut s'écrire comme un produit de transpositions adjacentes.

□

3.5.3 La signature et le groupe alterné

Théorème 3.5.8. *Il existe un unique morphisme de groupes*

$$\mathrm{sgn} : \mathfrak{S}_n \to \{-1, 1\}$$

qui est tel que $\mathrm{sgn}(\tau) = -1$ *pour* τ *une transposition.*

Définition 3.5.9. *On appelle* $\mathrm{sgn}(\sigma)$ *la* **signature** *de la permutation* $\sigma \in \mathfrak{S}_n$.

▷ On a donc, pour des transpositions $\tau_1, \ldots, \tau_k$:

$$\mathrm{sgn}(\tau_1 \cdots \tau_k) = (-1)^k.$$

▷ Le théorème 3.5.8 implique que si l'on écrit une permutation donnée comme un produit de transpositions, la parité du nombre de transpositions qui apparaissent dans ce produit ne dépend pas du choix d'écriture.

Proposition 3.5.10. *Pour tout* $k \geqslant 2$*, la signature d'un cycle de longueur* k *est* $(-1)^{k-1}$.

Démonstration. Cela provient du fait qu'un cycle de longueur k peut s'écrire comme un produit de $k-1$ transpositions, comme on l'a déjà vu :

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2)(i_2\ i_3)\cdots(i_{k-1}\ i_k).$$

□

▷ Cette proposition est utile pour calculer la signature d'une permutation qu'on a auparavant décomposée en produit de cycles : elle vaut $(-1)^r$ où r est le nombre de cycles de longueur paire qui interviennent dans la décomposition.

Définition 3.5.11. *Le* **groupe alterné** *sur* n *éléments, noté* $\mathfrak{A}_n$*, est le noyau de la signature, c'est-à-dire l'ensemble des permutations* $\sigma \in \mathfrak{S}_n$ *telles que* $\mathrm{sgn}(\sigma) = 1$.

▷ C'est un sous-groupe de $\mathfrak{S}_n$ car c'est le noyau d'un morphisme de groupes.

Exercice 58. Lister les éléments de $\mathfrak{A}_3$ et de $\mathfrak{A}_4$.

Proposition 3.5.12. *Pour* $n \geqslant 2$*, le groupe alterné* $\mathfrak{A}_n$ *est d'ordre* $\frac{n!}{2}$*. Dit autrement, c'est un sous-groupe de* $\mathfrak{S}_n$ *d'indice* 2.

Démonstration. Notons $\mathfrak{S}_n^- \subset \mathfrak{S}_n$ l'ensemble des permutations de signature -1. (Ce n'est pas un sous-groupe de $\mathfrak{S}_n$.... pourquoi ?) On a donc une partition $\mathfrak{S}_n = \mathfrak{A}_n \sqcup \mathfrak{S}_n^-$. Soit $\tau = (1\ 2)$. Pour $\sigma \in \mathfrak{A}_n$ on a $\tau\sigma \in \mathfrak{S}_n^-$ car $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\,\mathrm{sgn}(\sigma) = (-1) \times 1 = -1$. On a donc une application

$$\mathfrak{A}_n \to \mathfrak{S}_n^- \ ,\ \sigma \mapsto \tau\sigma,$$

dont on voit facilement qu'elle est bijective. (Montrez-le !) Cela implique que $|\mathfrak{A}_n| = |\mathfrak{S}_n^-|$ et donc que $|\mathfrak{S}_n| = |\mathfrak{A}_n| + |\mathfrak{S}_n^-| = 2|\mathfrak{A}_n|$, d'où le résultat. □

Remarque 3.5.13. C'est un fait général que si G est un groupe et $f : G \to H$ est un morphisme de groupes surjectif, alors $|H|$ divise $|G|$ et le noyau de f est un sous-groupe d'indice $|H|$ dans $|G|$. On retrouve la proposition précédente en appliquant ce fait au morphisme $\mathrm{sgn} : \mathfrak{S}_n \to \{-1, 1\}$, qui est surjectif si $n \geqslant 2$.

3.6 Étude du groupe orthogonal

3.6.1 Définition

Soit $n \in \mathbb{N}$. On se place dans $\mathbb{R}^n$ munie de sa base canonique et de son **produit scalaire** canonique, défini pour $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ par la formule :

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

La base canonique est donc orthonormée. On a aussi la **norme euclidienne** :

$$||x|| = \sqrt{\langle x, x \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

On retrouve le produit scalaire à partir de la norme grâce à la **formule de polarisation** :

$$\langle x, y \rangle = \frac{1}{2} \left(||x + y||^2 - ||x||^2 - ||y||^2 \right).$$

Proposition 3.6.1. *Soit $f \in \mathrm{Aut}(\mathbb{R}^n)$ un automorphisme linéaire de $\mathbb{R}^n$. Les assertions suivantes sont équivalentes.*

(i) f préserve la norme :

$$\forall x \in \mathbb{R}^n,\ ||f(x)|| = ||x||.$$

(ii) f préserve le produit scalaire :

$$\forall x, y \in \mathbb{R}^n,\ \langle f(x), f(y) \rangle = \langle x, y \rangle.$$

(iii) f envoie la base canonique de $\mathbb{R}^n$ sur une base orthonormée.

(iv) Si A désigne la matrice de f dans la base canonique,

$$^tA\, A = I_n = A\, {}^tA.$$

Démonstration. Si f préserve la norme alors elle préserve le produit scalaire grâce à la formule de polarisation. Donc $(i) \Rightarrow (ii)$.

Si f préserve le produit scalaire, alors on voit facilement que f envoie la base canonique de $\mathbb{R}^n$ sur une base orthonormée : si on note $e_1, \dots, e_n$ les vecteurs de la base canonique, on a pour $i, j \in \{1, \dots, n\}$,

$$\langle f(e_i), f(e_j) \rangle = \langle e_i, e_j \rangle = \begin{cases} 1 & \text{si } i = j; \\ 0 & \text{si } i \neq j \end{cases}$$

et donc $f(e_1), \dots, f(e_n)$ est une base orthonormée de $\mathbb{R}^n$. Donc $(ii) \Rightarrow (iii)$.

Si f satisfait (iii) alors les colonnes de A forment une base orthonormée de $\mathbb{R}^n$. On voit facilement que cela implique qu'on a $^tA\, A = I_n$ puisque le coefficient (i, j) du produit $^tA\, A$ est égal au produit scalaire $\langle f(e_i), f(e_j) \rangle$. On a donc $A^{-1} = {}^tA$ et donc $A\, {}^tA = I_n$. Donc $(iii) \Rightarrow (iv)$.

Supposons que f satisfait (iv). Pour un vecteur $x \in \mathbb{R}^n$ vu comme un vecteur colonne, on calcule la norme par la formule $||x||^2 = {}^t x\, x$. On a donc

$$||f(x)||^2 = {}^t(Ax)(Ax) = {}^t x\, {}^t A\, A\, x = {}^t x\, I_n\, x = {}^t x\, x = ||x||^2,$$

et donc f préserve la norme. Donc $(iv) \Rightarrow (i)$. □

Définition 3.6.2. *Un automorphisme linéaire $f \in \mathrm{Aut}(\mathbb{R}^n)$ est appelé* **automorphisme orthogonal** *s'il vérifie les assertions équivalentes (i), (ii), (iii), (iv) de la proposition précédente. On note*

$$\mathrm{O}_n(\mathbb{R}) \subset \mathrm{Aut}(\mathbb{R}^n)$$

l'ensemble des automorphismes orthogonaux de $\mathbb{R}^n$.

Les automorphismes orthogonaux sont parfois appelés **isométries linéaires**.

Proposition 3.6.3. *$\mathrm{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{Aut}(\mathbb{R}^n)$.*

Démonstration. 1) Clairement, l'identité est un automorphisme orthogonal.

2) Soient f, g deux automorphismes orthogonaux. Pour tout $x \in \mathbb{R}^n$ on a :

$$||f(g(x))|| = ||g(x)|| = ||x||$$

où la première égalité utilise le fait que f est un automorphisme orthogonal, et la deuxième égalité utilise le fait que g est un automorphisme orthogonal. Donc $f \circ g$ est un automorphisme orthogonal.

3) Soit f un automorphisme orthogonal. Pour tout $x \in \mathbb{R}^n$ on a :

$$||f(f^{-1}(x))|| = ||f^{-1}(x)||$$

et donc

$$||x|| = ||f^{-1}(x)||.$$

On en conclut que f^{-1} est un automorphisme orthogonal.

□

Définition 3.6.4. *On appelle $\mathrm{O}_n(\mathbb{R})$ le* **groupe orthogonal** *de degré n sur $\mathbb{R}$.*

Remarque 3.6.5. On rappelle l'isomorphisme de groupes (exemple 3.3.11)

$$\mathrm{Aut}(\mathbb{R}^n) \simeq \mathrm{GL}_n(\mathbb{R})$$

où l'on représente un automorphisme de $\mathbb{R}^n$ par sa matrice dans la base canonique. On se permet d'identifier ainsi les deux groupes $\mathrm{Aut}(\mathbb{R}^n)$ et $\mathrm{GL}_n(\mathbb{R})$, et on peut donc voir $\mathrm{O}_n(\mathbb{R})$ comme un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. D'après la proposition 3.6.1, c'est le sous-groupe formé des matrices carrées A de taille n qui vérifient ${}^t A\, A = I_n = A\, {}^t A$. (Avec ce point de vue, on parle de **matrices orthogonales**.)

3.6.2 Le groupe spécial orthogonal

Proposition 3.6.6. *Soit $f \in \mathrm{O}_n(\mathbb{R})$. Alors* $\det(f) \in \{-1, 1\}$.

Démonstration. Soit A la matrice de f dans la base canonique. D'après la proposition 3.6.1 on a ${}^tA\,A = I_n$, et donc en prenant les déterminants : $\det({}^tA)\det(A) = 1$. Or $\det({}^tA) = \det(A)$ et donc $\det(A)^2 = 1$, d'où $\det(A) \in \{-1, 1\}$. □

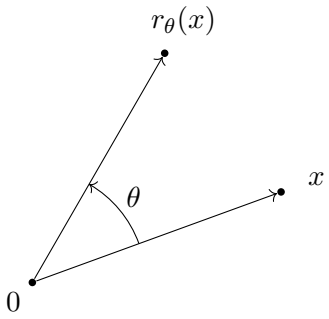
Définition 3.6.7. *L'ensemble des automorphismes orthogonaux de $\mathbb{R}^n$ dont le déterminant est égal à 1 est noté $\mathrm{SO}_n(\mathbb{R})$ est appelé le* **groupe spécial orthogonal** *de degré n sur $\mathbb{R}$.*

▷ C'est clairement un sous-groupe de $\mathrm{O}_n(\mathbb{R})$ car c'est le noyau du morphisme de groupes $\det : \mathrm{O}_n(\mathbb{R}) \to \{-1, 1\}$.

Remarque 3.6.8. Les éléments de $\mathrm{SO}_n(\mathbb{R})$ sont parfois appelés automorphismes orthogonaux **directs** car ils préservent l'orientation. Dit autrement, ils envoient la base canonique sur une base orthonormée directe. (En général, un automorphisme linéaire de $\mathbb{R}^n$ est dit direct si son déterminant est > 0, et indirect si son déterminant est < 0.)

3.6.3 Structure de $\mathrm{SO}_2(\mathbb{R})$

▷ Pour tout réel θ on a la **rotation** d'angle θ, notée $r_\theta \in \mathrm{SO}_2(\mathbb{R})$.



▷ Sa matrice dans la base canonique est

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

▷ On a

$$r_\theta = r_{\theta'} \quad \Longleftrightarrow \quad \theta - \theta' \in 2\pi\mathbb{Z}$$

et les identités évidentes :

$$r_0 = \mathrm{id} \quad , \quad r_\theta r_{\theta'} = r_{\theta+\theta'} \quad , \quad r_\theta^{-1} = r_{-\theta}.$$

Proposition 3.6.9. *Soit $f \in \mathrm{SO}_2(\mathbb{R})$. Alors f est une rotation, c'est-à-dire qu'il existe $\theta \in \mathbb{R}$, unique modulo $2\pi\mathbb{Z}$, tel que $f = r_\theta$.*

Démonstration. – Soit

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

la matrice de f dans la base canonique.

– L'égalité ${}^tA\,A = I_2$ se traduit par les égalités

$$a^2 + b^2 = c^2 + d^2 = 1\,, \quad ac + bd = 0.$$

Le fait que $\det(A) = 1$ se traduit par

$$ad - bc = 1.$$

– Comme $a^2 + b^2 = c^2 + d^2 = 1$, il existe $\theta, \theta' \in \mathbb{R}$ tels que

$$(a, b) = (\cos(\theta), \sin(\theta)) \quad \text{et} \quad (c, d) = (\cos(\theta'), \sin(\theta')).$$

Les identités $ac+bd = 0$ et $ad-bc = 1$ s'écrivent, en utilisant des formules de trigonométrie bien connues, sous la forme :

$$\cos(\theta' - \theta) = 0\,, \quad \sin(\theta' - \theta) = 1.$$

Donc il existe $k \in \mathbb{Z}$ tel que $\theta' - \theta = \frac{\pi}{2} + 2\pi k$, et donc $\theta' = \theta + \frac{\pi}{2} + 2\pi k$. On a donc $(c, d) = (\cos(\theta + \frac{\pi}{2}), \sin(\theta + \frac{\pi}{2})) = (-\sin(\theta), \cos(\theta))$, et donc $f = r_\theta$.

□

Remarque 3.6.10. On déduit de cette proposition que $\mathrm{SO}_2(\mathbb{R})$ est un groupe abélien, puisque les rotations commutent entre elles. De plus, ce groupe est isomorphe au groupe $\mathbb{U}$ (cercle unité dans $\mathbb{C}^*$), l'isomorphisme identifiant la rotation r_θ à $e^{i\theta}$.

Pour tout entier $n \in \mathbb{N}^*$ on note C_n le sous-groupe de $\mathrm{SO}_2(\mathbb{R})$ engendré par la rotation d'angle $2\pi/n$:

$$C_n = \langle\, r_{2\pi/n} \,\rangle \subset \mathrm{SO}_2(\mathbb{R}).$$

Comme $r_{2\pi/n}$ est d'ordre n, C_n est un groupe cyclique d'ordre n.

Proposition 3.6.11. *Les sous-groupes C_n, pour $n \in \mathbb{N}^*$, sont les seuls sous-groupes finis de $\mathrm{SO}_2(\mathbb{R})$.*

Démonstration. – Commençons par remarquer qu'un élément r_θ est d'ordre fini dans $\mathrm{SO}_2(\mathbb{R})$ si et seulement s'il existe $N \in \mathbb{N}^*$ tel que $r_\theta^N = \mathrm{id}$, c'est-à-dire $r_{N\theta} = \mathrm{id}$, ou encore $N\theta \in 2\pi\mathbb{Z}$. Donc les éléments d'ordre fini dans $\mathrm{SO}_2(\mathbb{R})$ sont les rotations r_θ avec $\theta \in 2\pi\mathbb{Q}$.

– Soit maintenant G un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Tous les éléments de G sont nécessairement d'ordre fini, et il existe donc un entier $N \in \mathbb{N}^*$ tel que les éléments de G soient tous de la forme $r_{2\pi k/N}$ avec $k \in \mathbb{Z}$. Donc G est un sous-groupe du groupe cyclique C_N. Par la classification des sous-groupes d'un groupe cyclique (proposition 3.4.10), G est donc un groupe cyclique C_n pour n un diviseur de N.

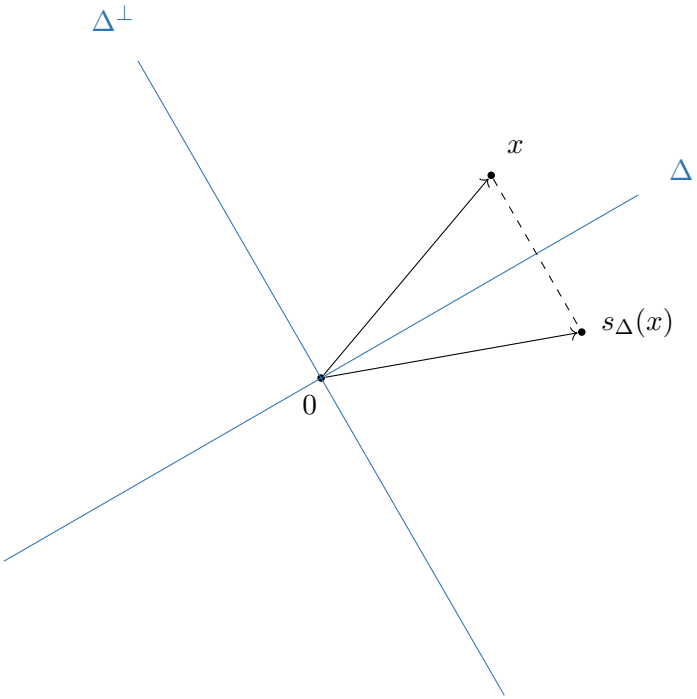
□

3.6.4 Structure de $\mathrm{O}_2(\mathbb{R})$

▷ Notons $\mathrm{O}_2^-(\mathbb{R}) \subset \mathrm{O}_2(\mathbb{R})$ l'ensemble des automorphismes orthogonaux de $\mathbb{R}^2$ dont le déterminant est -1. (Ce n'est pas un sous-groupe de $\mathrm{O}_2(\mathbb{R})$... pourquoi ?) On a donc une partition

$$\mathrm{O}_2(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R}) \sqcup \mathrm{O}_2^-(\mathbb{R}).$$

▷ Pour toute droite (linéaire) Δ de $\mathbb{R}^2$ on a la **réflexion** par rapport à Δ, notée $s_\Delta \in \mathrm{O}_2^-(\mathbb{R})$.



Remarque 3.6.12. La définition formelle de s_Δ est la suivante. Notons $\Delta^\perp$ la droite orthogonale à Δ, de sorte qu'on a la décomposition en somme directe orthogonale :

$$\mathbb{R}^2 = \Delta \oplus \Delta^\perp.$$

On définit s_Δ comme l'unique automorphisme linéaire de $\mathbb{R}^2$ qui agit comme id sur Δ et $-\mathrm{id}$ sur $\Delta^\perp$. Dit autrement, si e est un vecteur non nul de Δ et f un vecteur non nul de $\Delta^\perp$, la matrice de s_Δ dans la base (e, f) est :

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Cela permet notamment de se convaincre que $\det(s_\Delta) = -1$.

▷ En général, si l'on note θ l'angle orienté entre l'axe des abscisses et Δ, la matrice de s_Δ dans la base canonique est

$$\begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}.$$

▷ On note que s_Δ est d'ordre 2 : $s_\Delta \neq \mathrm{id}$ et $s_\Delta^2 = \mathrm{id}$.

Proposition 3.6.13. *Soit $f \in \mathrm{O}_2^-(\mathbb{R})$. Alors il existe une unique droite Δ telle que $f = s_\Delta$.*

Démonstration. L'unicité vient du fait que Δ est l'espace des points fixes de s_Δ. On traite maintenant l'existence. Soit $f \in \mathrm{O}_2^-(\mathbb{R})$.

– Son polynôme caractéristique est

$$\chi_f(X) = X^2 - \mathrm{tr}(f)X + \det(f) = X^2 - \mathrm{tr}(f)X - 1,$$

dont le discriminant est $(\mathrm{tr}(f))^2 + 4 > 0$. Donc $\chi_f(X)$ est scindé à racines réelles simples et f est donc diagonalisable, avec deux valeurs propres réelles distinctes.

– Pour une valeur propre réelle λ de f et un vecteur propre x correspondant, l'identité $||f(x)|| = ||x||$ s'écrit $||\lambda x|| = ||x||$, c'est-à-dire $|\lambda| \times ||x|| = ||x||$ et donc $|\lambda| = 1$, c'est-à-dire $\lambda = \pm 1$. Les deux valeurs propres de f sont donc 1 et -1.

– On a donc une décomposition $\mathbb{R}^2 = \Delta \oplus \Delta'$ où Δ est le sous-espace propre pour la valeur propre 1 et Δ' le sous-espace propre pour la valeur propre -1. Ce sont des droites. Pour $x \in \Delta$ et $x' \in \Delta'$, l'identité $\langle f(x), f(x')\rangle = \langle x, x'\rangle$ implique $-\langle x, x'\rangle = \langle x, x'\rangle$ et donc $\langle x, x'\rangle = 0$. Donc Δ et Δ' sont orthogonales, c'est-à-dire : $\Delta' = \Delta^\perp$.

– Conclusion : comme f agit comme id sur Δ et comme $-\mathrm{id}$ sur $\Delta^\perp$, on en déduit que $f = s_\Delta$.

□

On a donc obtenu une classification complète des éléments de $\mathrm{O}_2(\mathbb{R})$:

Théorème 3.6.14. *Soit $f \in \mathrm{O}_2(\mathbb{R})$. Alors f est soit une rotation r_θ, pour un $\theta \in \mathbb{R}$ unique modulo $2\pi\mathbb{Z}$, soit une réflexion s_Δ, pour une unique droite Δ.*

La proposition suivante explique comment multiplier ces éléments entre eux.

Proposition 3.6.15. *1) Soient Δ, Δ' deux droites de $\mathbb{R}^2$ et soit θ l'angle orienté entre Δ et Δ'. Alors on a :*

$$s_\Delta s_{\Delta'} = r_{-2\theta}.$$

2) Soit Δ une droite et $\theta \in \mathbb{R}$. Alors on a :

$$r_\theta s_\Delta = s_{r_{\theta/2}(\Delta)} \quad \text{et} \quad s_\Delta r_\theta = s_{r_{-\theta/2}(\Delta)}.$$

Notamment, on a :

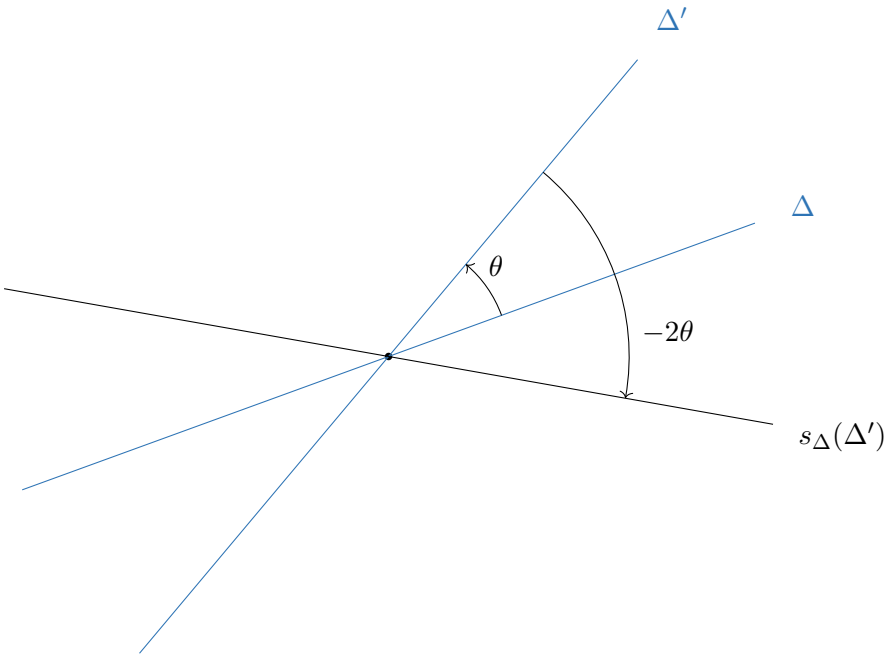
$$r_\theta s_\Delta = s_\Delta r_{-\theta}.$$

▷ Il découle de cette proposition que $\mathrm{O}_2(\mathbb{R})$ n'est pas un groupe abélien.

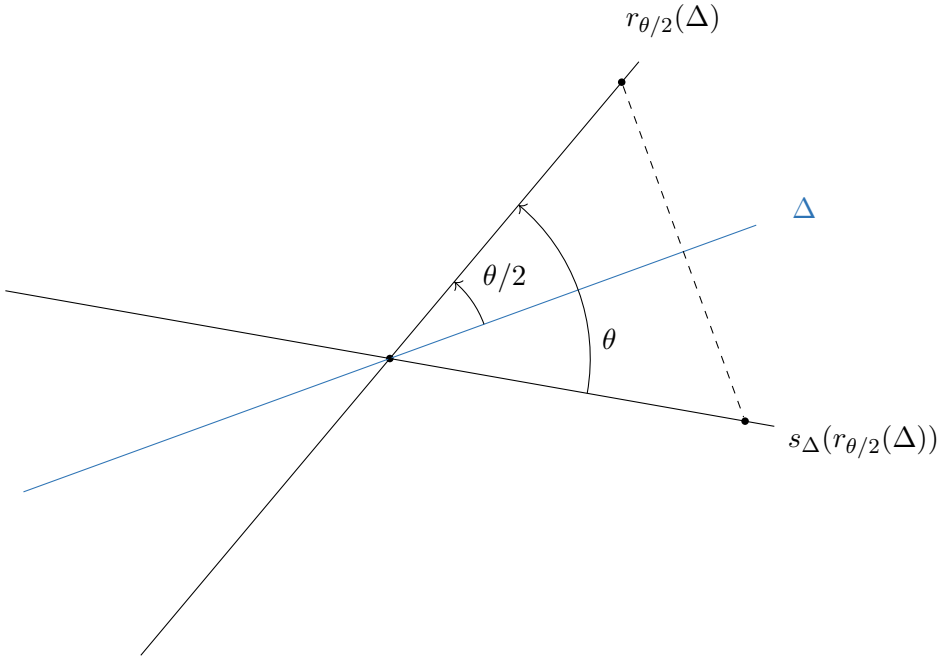
Démonstration. 1) On a $\det(s_\Delta s_{\Delta'}) = \det(s_\Delta)\det(s_{\Delta'}) = (-1) \times (-1) = 1$ et donc $s_\Delta s_{\Delta'} \in \mathrm{SO}_2(\mathbb{R})$. Par la proposition 3.6.9 on a donc $s_\Delta s_{\Delta'} = r_\varphi$ pour $\varphi \in \mathbb{R}$. Pour calculer φ il suffit de calculer l'angle orienté de D à $(s_\Delta s_{\Delta'})(D)$ pour n'importe quelle droite D de $\mathbb{R}^2$. On choisit de prendre $D = \Delta'$ car $s_{\Delta'}(\Delta') = \Delta'$. On a :

$$(s_\Delta s_{\Delta'})(\Delta') = s_\Delta(s_{\Delta'}(\Delta')) = s_\Delta(\Delta').$$

Or l'angle orienté de Δ' à $s_\Delta(\Delta')$ est -2θ (voir la figure suivante), et donc $\varphi = -2\theta$.



2) On a $\det(r_\theta s_\Delta) = \det(r_\theta)\det(s_\Delta) = 1 \times (-1) = -1$ et donc $r_\theta s_\Delta \in \mathrm{O}_2^-(\mathbb{R})$. Par la proposition 3.6.13, on a donc $r_\theta s_\Delta = s_{\Delta'}$ pour une droite Δ'. Cette droite Δ' est l'ensemble des points fixes de $s_{\Delta'}$, et il suffit donc de trouver une droite qui est fixée par $r_\theta s_\Delta$. On voit facilement que la droite $r_{\theta/2}(\Delta)$ est fixée par $r_\theta s_\Delta$ (voir la figure suivante), et donc $\Delta' = r_{\theta/2}(\Delta)$. La deuxième identité se montre de la même manière.



□

Remarque 3.6.16. On peut garder en tête les identités de conjugaison suivantes, conséquences de la proposition 3.6.15 : pour une rotation r et une réflexion s_Δ on a

$$s_\Delta \, r \, s_\Delta^{-1} = r^{-1}.$$

et

$$r \, s_\Delta \, r^{-1} = s_{r(\Delta)}.$$

Remarque 3.6.17. Si l'on choisit une droite Δ_0 de $\mathbb{R}^2$ et qu'on note $s = s_{\Delta_0}$, alors on peut représenter toutes les réflexions sous la forme $r_\theta s$ avec θ unique modulo $2\pi\mathbb{Z}$.

3.7 Étude du groupe diédral

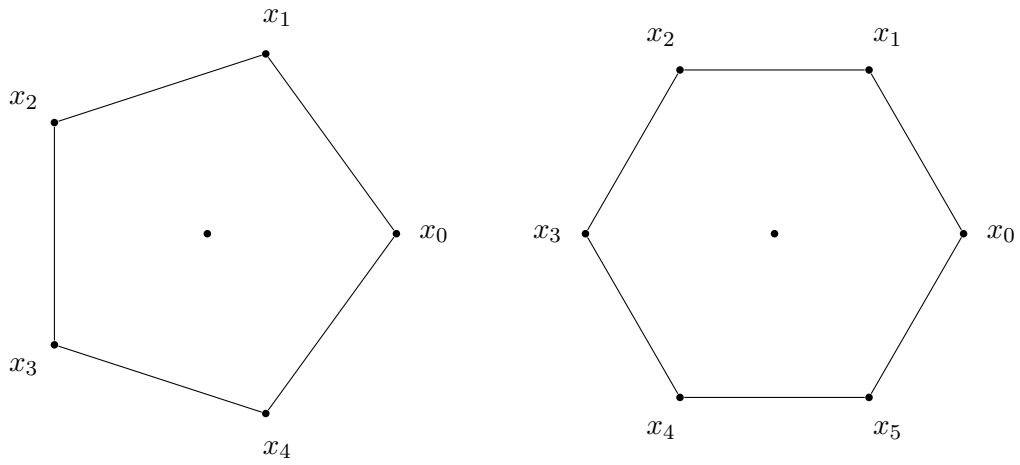
3.7.1 Définition

Soit un entier $n \in \mathbb{N}^*$. On note $P_n \subset \mathbb{R}^2$ l'ensemble formé des n points

$$x_k = (\cos(2\pi k/n), \sin(2\pi k/n))$$

pour $k \in \{0, \dots, n-1\}$. Ce sont les sommets d'un polygone régulier à n côtés.

Exemple 3.7.1. Voici P_5 et P_6.



Définition 3.7.2. *Le* **groupe diédral** D_n *est l'ensemble des* $f \in \mathrm{O}_2(\mathbb{R})$ *qui stabilisent* P_n*, c'est-à-dire tels que* $f(P_n) \subset P_n$*.*

Proposition 3.7.3. D_n *est un sous-groupe de* $\mathrm{O}_2(\mathbb{R})$*.*

Démonstration. 1) Clairement, $\mathrm{id} \in D_n$.

2) Soient $f, g \in D_n$. Alors $f(P_n) \subset P_n$ et $g(P_n) \subset P_n$ et donc $(fg)(P_n) = f(g(P_n)) \subset f(P_n) \subset P_n$, donc $fg \in D_n$.

3) Soit $f \in D_n$. Alors $f(P_n) \subset P_n$. Comme f est bijective, on a pour des raisons de cardinal $f(P_n) = P_n$ et donc $f^{-1}(f(P_n)) = f^{-1}(P_n)$, d'où $P_n = f^{-1}(P_n)$, et donc $f^{-1} \in D_n$.

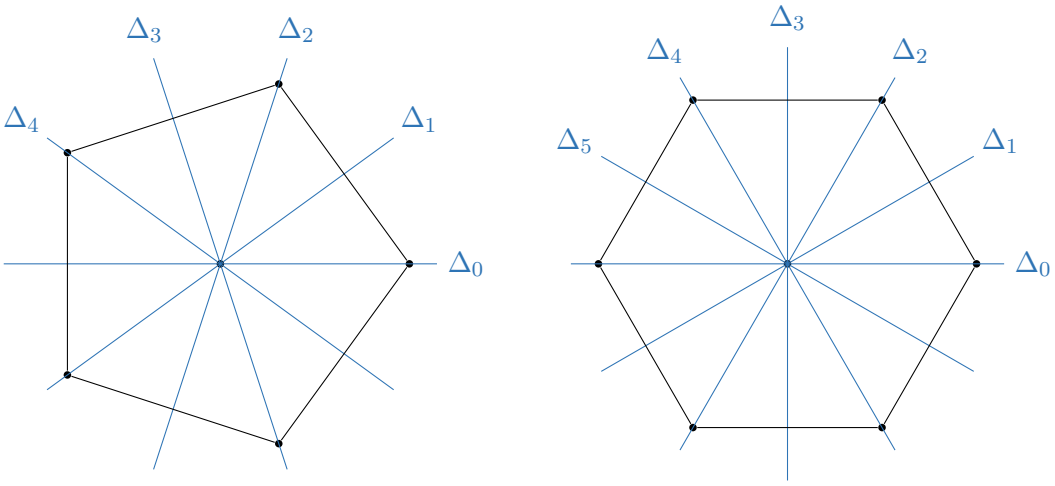
□

3.7.2 Structure de D_n

▷ Notons r la rotation d'angle $2\pi/n$. C'est clairement un élément de D_n, qui engendre le sous-groupe cyclique à n éléments $C_n = \langle r \rangle \subset D_n$.

▷ Pour $k \in \{0, \dots, n-1\}$, notons aussi Δ_k la droite qui fait un angle de $\pi k/n$ avec l'axe des abscisses, et s_k la réflexion par rapport à Δ_k. Ce sont aussi des éléments de D_n.

Exemple 3.7.4. Voici, dans les cas $n = 5$ et $n = 6$, les n droites Δ_k.



Proposition 3.7.5. *On a*

$$D_n \cap \mathrm{SO}_2(\mathbb{R}) = C_n = \{\mathrm{id}, r, r^2, \dots, r^{n-1}\}$$

et

$$D_n \cap \mathrm{O}_2^-(\mathbb{R}) = \{s_0, s_1, s_2, \dots, s_{n-1}\}.$$

Par conséquent, D_n est un groupe d'ordre $2n$ et

$$D_n = \{\mathrm{id}, r, r^2, \dots, r^{n-1}, s_0, s_1, s_2, \dots, s_{n-1}\}.$$

Démonstration. 1) Soit $f \in D_n \cap \mathrm{SO}_2(\mathbb{R})$. Alors f est une rotation et il existe $k \in \{0, \dots, n-1\}$ tel que $f(x_0) = x_k$. Donc $f = r^k$.

2) Soit $f \in D_n \cap \mathrm{O}_2^-(\mathbb{R})$. Alors f est une réflexion et il existe $k \in \{0, \dots, n-1\}$ tel que $f(x_0) = x_k$. Alors on a aussi $f(x_k) = x_0$ et donc $f(x_0 + x_k) = x_0 + x_k$. Donc f agit comme id sur la droite $\mathbb{R}(x_0 + x_k) = \Delta_k$, d'où $f = s_k$.

□

On calcule facilement dans le groupe D_n grâce à la proposition 3.6.15. Pour $0 \leqslant i, j \leqslant n-1$ on a

$$s_i s_j = r^{i-j}$$

et

$$r^i s_j = s_{j+i} \quad \text{et} \quad s_j r^i = s_{j-i}$$

où les indices sont entendus modulo n.

▷ On a $D_1 = \{\mathrm{id}, s_0\}$, qui est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

▷ On a $D_2 = \{\mathrm{id}, r, s_0, s_1\}$, où s_0 est la réflexion par rapport à l'axe des abscisses, s_1 est la réflexion par rapport à l'axe des ordonnées, et $s_0 s_1 = s_1 s_0 = r = -\mathrm{id}$. On voit facilement qu'on a $D_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

▷ Pour $n \geqslant 3$ le groupe diédral D_n n'est pas abélien, car par exemple $s_0 s_1 \neq s_1 s_0$.

Exercice 59. Écrire les tables de multiplication des groupes diédraux D_3 et D_4.

Exercice 60. Démontrer que les groupes D_3 et $\mathfrak{S}_3$ sont isomorphes.

On note maintenant $s = s_0$, la réflexion par rapport à l'axe des abscisses $\mathbb{R}(1,0)$. La proposition 3.6.15 implique que $s_k = r^k s$ pour tout $k \in \{0, \dots, n-1\}$, et on a donc la proposition suivante.

Proposition 3.7.6. *D_n est engendré par r et s, et plus précisément :*

$$D_n = \{\mathrm{id}, r, r^2, r^3, \dots, r^{n-1}, s, rs, r^2 s, r^3 s, \dots, r^{n-1} s\}.$$

Avec ces notations, on calcule facilement dans D_n en utilisant les relations

$$r^n = \mathrm{id}\ ,\ s^2 = \mathrm{id}\ ,\ sr^k = r^{-k} s.$$

Exemple 3.7.7. Dans D_5 on a

$$(r^2 s)(r^4 s) = r^2 (s r^4) s = r^2 (r^{-4} s) s = r^{-2} = r^3.$$

Chapitre 4

Introduction à la théorie des anneaux et des corps

4.1 Le langage des anneaux et des corps

4.1.1 Notation additive dans un groupe abélien

À partir de maintenant les groupes qui apparaîtront seront quasiment tous abéliens et en notation additive. On commence donc par faire quelques rappels/commentaires sur la notation additive dans les groupes abéliens.

Notation

Dans la suite on va rencontrer des groupes **abéliens** avec la **notation additive** $(G, +)$. L'élément neutre est noté 0_G et appelé le **zéro** de G, l'inverse d'un élément $x \in G$ est noté $-x$ et appelé l'**opposé** de x. On a les formules :

$$-(-x) = x \qquad \text{et} \qquad -(x+y) = (-x) + (-y).$$

(Noter que pour la dernière on utilise bien le fait que $+$ est commutative.)

On définit la **soustraction** de deux éléments $x, y \in G$ par la formule :

$$x - y = x + (-y).$$

Elle vérifie les règles de calcul habituelles :

$$x + y = z \iff x = z - y.$$

On peut notamment simplifier :

$$x + y = x' + y \iff x = x'.$$

Produit externe par $\mathbb{Z}$

Pour $x \in G$ et $n \in \mathbb{N}$ on note

$$nx = \underbrace{x + x + \cdots + x}_{n}$$

avec la convention que $0x = 0_G$. On étend cette opération aux entiers négatifs avec la formule $(-n)x = -(nx)$ pour $n \in \mathbb{N}$. On a donc donné un sens au **produit externe** nx avec $n \in \mathbb{Z}$ et $x \in G$. Cette opération vérifie les formules évidentes :

$$0x = 0_G\,,\ 1x = x\,,\ (m+n)x = mx + nx\,,\ m(nx) = (mn)x\,,\ n(x+y) = nx + ny.$$

(Noter que pour la dernière on utilise bien le fait que + est commutative.)

> **Remarque 4.1.1.** Tout $\mathbb{R}$-espace vectoriel est un groupe abélien. En fait, dans un $\mathbb{R}$-espace vectoriel E on peut plus généralement donner un sens au produit $ax \in E$ pour $a \in \mathbb{R}$ et $x \in E$, qui vérifie les mêmes axiomes que ci-dessus. On peut donc dire que $\mathbb{Z}$ joue pour les groupes abéliens le rôle que $\mathbb{R}$ joue pour les $\mathbb{R}$-espaces vectoriels. On pourrait dire qu'un groupe abélien est un $\mathbb{Z}$-espace vectoriel, mais on n'emploie pas cette terminologie car $\mathbb{Z}$ n'est pas un corps : on parle plutôt de $\mathbb{Z}$-**module**.

Morphismes

Dans la notation additive, un **morphisme de groupes** de G vers H est une application $f : G \to H$ qui vérifie

$$\forall x, y \in G,\ f(x+y) = f(x) + f(y).$$

Elle vérifie alors automatiquement $f(0_G) = 0_H$ et $f(-x) = -f(x)$ pour tout $x \in G$. On montre facilement que pour tous $x, y \in G$ et $m, n \in \mathbb{Z}$ on a :

$$f(mx + ny) = mf(x) + nf(y).$$

▷ On rappelle la notion de noyau d'un morphisme de groupes :

$$\ker(f) = \{x \in G \mid f(x) = 0_H\}.$$

Sous-groupes

Dans la notation additive, un **sous-groupe** d'un groupe G est un sous-ensemble $H \subset G$ qui vérifie les axiomes suivants :

(1) $0_G \in H$;

(2) H est stable par somme : $\forall x, y \in H,\ x + y \in H$;

(3) H est stable par passage à l'opposé : $\forall x \in H,\ -x \in H$.

▷ Soit G un groupe et soit H un sous-groupe de G. Alors pour tous $x, y \in H$ et pour tous $m, n \in \mathbb{Z}$ on a $mx + ny \in H$. Réciproquement, tout sous-ensemble $H \subset G$ non vide qui vérifie cette propriété est un sous-groupe de G.

Sous-groupe engendré par une partie

Soit G un groupe abélien et soient $x_1, \ldots, x_r \in G$. Le sous-groupe de G engendré par $x_1, \ldots, x_r$ peut être décrit comme l'ensemble des combinaisons $\mathbb{Z}$-linéaires de $x_1, \ldots, x_r$:

$$\langle x_1, \ldots, x_r \rangle = \{n_1x_1 + \cdots + n_rx_r,\ n_1, \ldots, n_r \in \mathbb{Z}\}.$$

Plus généralement, pour une partie $S \subset G$ quelconque, le sous-groupe de G engendré par S, noté $\langle S \rangle$, est l'ensemble des combinaisons linéaires **finies** $n_1x_1 + \cdots + n_rx_r$ avec $x_1, \ldots, x_r \in S$ et $n_1, \ldots, n_r \in \mathbb{Z}$.

4.1.2 Anneau

Définition 4.1.2. *Un* **anneau** *est un triplet $(A, +, \times)$ où A est un ensemble et $+$, $\times$ sont deux lois de composition internes sur A qui vérifient les axiomes suivants :*

(1) $(A, +)$ *est un groupe abélien.*

(2) Associativité de $\times$ *:* $\forall x, y, z \in A\,,\ (x \times y) \times z = x \times (y \times z)$ *(qu'on peut donc noter* $x \times y \times z$*).*

(3) Élément neutre pour $\times$ *: il existe un élément* $1_A \in A$ *tel que* $\forall x \in A\,,\ x \times 1_A = x = 1_A \times x$*. On l'appelle le* **un** *de l'anneau.*

(4) Distributivité de $\times$ *par rapport à* $+$ *:* $\forall x, y, z \in A,\ x \times (y + z) = x \times y + x \times z$ *et* $(x + y) \times z = x \times z + y \times z$*.*

Exercice 61. Montrer que l'élément neutre 1_A est unique.

Définition 4.1.3. *Un anneau* $(A, +, \times)$ *est* **commutatif** *si la multiplication est commutative, c'est-à-dire si :* $\forall x, y \in A\,,\ x \times y = y \times x$*.*

Remarque 4.1.4. Quand il n'y a pas d'ambiguïté on écrit simplement A pour $(A, +, \times)$, 0 pour 0_A et 1 pour 1_A, afin d'alléger les notations. On utilise aussi la notation habituelle $xy = x \times y$.

Exercice 62. Soit $(A, +, \times)$ un anneau.

- Montrer qu'on a $x \times 0_A = 0_A = 0_A \times x$ pour tout $x \in A$.
- Montrer qu'on a $(-x) \times y = -(x \times y) = x \times (-y)$ pour tous $x, y \in A$.
- Montrer qu'on a $(-1_A) \times x = -x = x \times (-1_A)$ pour tout $x \in A$.

Un exemple trivial d'anneau est l'**anneau nul** $A = \{0\}$. Les lois sont $0 + 0 = 0$, $0 \times 0 = 0$, et 0 est à la fois le neutre pour $+$ et le neutre pour $\times$.

Exercice 63. Soit $(A, +, \times)$ un anneau. Montrer que si $0_A = 1_A$ alors $A = \{0_A\}$ est l'anneau nul.

4.1.3 Exemples

Des exemples d'anneaux :

- ▷ Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ avec l'addition et la multiplication usuelles.
- ▷ Pour $n \in \mathbb{N}^*$, l'anneau $\mathbb{Z}/n\mathbb{Z}$, avec l'addition et la multiplication définies au chapitre 2. Le zéro est $\overline{0}$, le un est $\overline{1}$.
- ▷ L'anneau des polynômes à coefficients réels $\mathbb{R}[X]$, avec l'addition et la multiplication usuelles. Le zéro est le polynôme nul, le un est le polynôme constant 1.

- L'anneau des suites réelles $\mathbb{R}^{\mathbb{N}}$, muni de l'addition des suites $(u_n) + (v_n) = (u_n + v_n)$ et du produit des suites $(u_n)(v_n) = (u_n v_n)$. Le zéro est la suite nulle, le un est la suite constante égale à 1.
- L'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, noté $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$, muni de la somme $(f+g)(x) = f(x) + g(x)$ et du produit $(fg)(x) = f(x)g(x)$. Le zéro est la fonction nulle, le un est la fonction constante égale à 1.
- Les exemples précédents sont commutatifs. Les matrices carrées de taille n forment un anneau $(\mathrm{M}_n(\mathbb{R}), +, \times)$, qui n'est pas commutatif si $n \geqslant 2$. Le zéro est la matrice nulle, le un est la matrice identité I_n.
- Soit V un $\mathbb{R}$-espace vectoriel, et notons $\mathrm{End}(V)$ l'ensemble des endomorphismes $\mathbb{R}$-linéaires de V. Alors $(\mathrm{End}(V), +, \circ)$ est un anneau qui n'est pas commutatif si $\dim(V) \geqslant 2$. Le zéro est l'endomorphisme nul, le un est l'endomorphisme identité id_V.

4.1.4 Inversibles

Soit $(A, +, \times)$ un anneau. Alors $(A, \times)$ n'est pas un groupe en général, mais c'est un **monoïde** au sens du chapitre précédent (définition 3.1.6) : la multiplication est associative et a un élément neutre.

Pour un élément $x \in A$, on dit que x est **inversible** dans A s'il est inversible pour $\times$, c'est-à-dire s'il existe $y \in A$ tel que $x \times y = 1_A = y \times x$. Dans ce cas-là y est unique et est noté x^{-1}. On a les formules classiques :

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

L'ensemble des éléments inversibles de A est noté $A^\times$, et $(A^\times, \times)$ forme un groupe, qu'on appelle le **groupe des inversibles** de A.

Exercice 64. Pour les exemples d'anneaux A qu'on vient de voir, déterminer les groupes des inversibles $A^\times$.

Remarque 4.1.5. Si A n'est pas commutatif alors il est dangereux de noter x^{-1} sous la forme $\frac{1}{x}$. En effet, on serait alors tenté d'utiliser des fractions $\frac{x}{y}$ qui seraient alors ambiguës : on ne pourrait pas faire la différence entre $x \times \frac{1}{y}$ et $\frac{1}{y} \times x$. Dans le cas où A est commutatif, il n'y a pas de danger et on peut se permettre d'écrire des fractions – tant que le dénominateur est inversible évidemment.

Remarque 4.1.6. Si $A \neq \{0\}$ n'est pas l'anneau nul, c'est-à-dire si $0_A \neq 1_A$ (d'après l'exercice 63) alors 0_A n'est pas inversible. En effet, on a vu (dans l'exercice 62) que pour tout $x \in A$ on a $x \times 0_A = 0_A \neq 1_A$.

4.1.5 Corps

Définition 4.1.7. *Un* **corps** *est un anneau $K \neq \{0_K\}$ qui est commutatif et tel que tout élément $x \in K \setminus \{0_K\}$ est inversible.*

On rappelle (voir l'exercice 63) que la condition $K \neq \{0_K\}$ revient à dire que $0_K \neq 1_K$.

Remarque 4.1.8. Une définition équivalente : un corps est un anneau commutatif K qui est tel que $K^\times = K \setminus \{0_K\}$. (Noter que cette condition implique bien que $K \neq \{0_K\}$).

On notera $K^* = K \setminus \{0_K\}$ comme d'habitude.

Des exemples de corps :

▷ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

▷ Si p est un nombre premier alors $\mathbb{Z}/p\mathbb{Z}$ est un corps.

▷ L'ensemble $\mathbb{R}(X)$ des fractions rationnelles (quotients de polynômes) à coefficients réels est un corps.

Des non-exemples de corps :

▷ $\mathbb{Z}$ n'est pas un corps car il n'existe pas de $y \in \mathbb{Z}$ tel que $2 \times y = 1$.

▷ $\mathbb{R}[X]$ n'est pas un corps car il n'existe pas de $f \in \mathbb{R}[X]$ tel que $X \times f = 1$.

▷ Pour $n \geqslant 2$ un nombre composé, $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps. En effet, si l'on choisit un diviseur positif $d|n$ avec $d \neq 1$ et $d \neq n$, alors $\overline{d} \neq \overline{0}$ et $\overline{d}$ n'est pas inversible.

Remarque 4.1.9. On insiste sur le fait que dans un corps la multiplication est par définition commutative. La notion plus générale d'un anneau non nul dans lequel tout élément non nul a un inverse pour la multiplication s'appelle **anneau à division** ou **corps gauche**. On n'étudiera pas cette notion dans ce cours.

On rappelle la définition d'un espace vectoriel sur un corps.

Définition 4.1.10. *Soit K un corps. Un K-***espace vectoriel** *(ou* **espace vectoriel sur** *K) est un triplet $(E, +, .)$ où E est un ensemble, $+$ est une loi de composition interne sur E, et $.$ est une loi de composition externe $K \times E \to E$, $(a, x) \mapsto a.x$ telles que :*

(1) $(E, +)$ est un groupe abélien ;

(2) linéarité de la loi $.$: $\forall a \in K$, $\forall x, y \in E$, $a.(x + y) = a.x + a.y$;

(3) compatibilité à l'addition dans K : $\forall a, b \in K$, $\forall x \in E$, $(a + b).x = a.x + b.x$;

(4) compatibilité à la multiplication dans K : $\forall a, b \in K$, $\forall x \in E$, $(ab).x = a.(b.x)$;

(5) compatibilité à l'unité de K : $\forall x \in E$, $1_K.x = x$.

▷ Comme d'habitude, on note simplement ax au lieu de $a.x$.

Remarque 4.1.11. Les théorèmes classiques d'algèbre linéaire (pivot de Gauss, théorie des bases et de la dimension, existence de supplémentaires, théorème du rang, déterminant des matrices, etc.) sont vrais quel que soit le corps, même si on vous les a peut-être seulement énoncés pour $K = \mathbb{R}$ ou $\mathbb{C}$.

4.1.6 Règles de calcul dans un anneau

Puissances

Soit $(A, +, \times)$ un anneau. On peut définir, pour $x \in A$ et $n \in \mathbb{N}$, la puissance

$$x^n = \underbrace{x \times x \times \cdots \times x}_{n}$$

avec la convention $x^0 = 1_A$. Les propriétés usuelles sont satisfaites : $x^0 = 1_A$, $x^1 = x$, $x^{m+n} = x^m x^n$, $(x^m)^n = x^{mn}$.

> **Remarque 4.1.12.** Attention : on n'a pas en général $(xy)^n = x^n \times y^n$ pour $x, y \in A$ et $n \in \mathbb{N}$. Par exemple, $(xy)^2 = xyxy$ et $x^2y^2 = xxyy$. Si $xy = yx$ alors on a l'égalité.

Développement

Dans un anneau $(A, +, \times)$ on peut utiliser la compatibilité entre $+$ et $\times$ pour développer comme on a l'habitude, par exemple :

$$(x + y)(z + t) = xz + xt + yz + yt.$$

Cas particulier :

$$(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2.$$

> **Remarque 4.1.13.** Attention : si $xy \neq yx$ on a $(x + y)^2 \neq x^2 + 2xy + y^2$.

Identités remarquables

> **Proposition 4.1.14.** *Soit A un anneau et $x, y \in A$ tels que $xy = yx$. Alors on a les propriétés habituelles, pour $n \in \mathbb{N}$:*
>
> *(a)* $(xy)^n = x^n y^n$;
>
> *(b) (Formule du binôme de Newton)*
>
> $$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \ ;$$
>
> *(c)*
>
> $$x^n - y^n = (x - y) \left(\sum_{k=0}^{n-1} x^k y^{n-1-k} \right) .$$

Démonstration. (a) C'est évident.

(b) Par récurrence sur $n \in \mathbb{N}$ en utilisant la récurrence de Pascal : $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. On rappelle qu'on a $\binom{n}{k} = 0$ si $k < 0$ ou $k > n$.

▷ Initialisation. La formule est vraie pour $n = 0$: $(x + y)^0 = 1$ et $\binom{0}{0} x^0 y^0 = 1$.

▷ Soit $n \geqslant 1$, supposons qu'on a montré la formule pour $n-1$ et montrons-la pour n. On calcule :

$$\begin{aligned}
(x+y)^n &= (x+y)^{n-1}(x+y) \\
&= \left(\sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k}\right)(x+y) \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \left(\binom{n-1}{k-1} + \binom{n-1}{k}\right) x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \ .
\end{aligned}$$

▷ On a donc montré la formule du binôme de Newton par récurrence sur $n \in \mathbb{N}$.

(c) On développe le produit pour trouver une somme télescopique :

$$\begin{aligned}
(x-y)\left(\sum_{k=0}^{n-1} x^k y^{n-1-k}\right) &= \sum_{k=0}^{n-1} x^{k+1} y^{n-1-k} - \sum_{k=0}^{n-1} x^k y^{n-k} \\
&= \sum_{k=1}^{n} x^k y^{n-k} - \sum_{k=0}^{n-1} x^k y^{n-k} \\
&= x^n - y^n \ .
\end{aligned}$$

□

Exercice 65. Où utilise-t-on l'hypothèse $xy = yx$ dans les preuves ci-dessus ?

4.1.7 Anneaux intègres

Définition 4.1.15. *Un anneau commutatif A est dit* **intègre** *si $A \neq \{0\}$ et pour tous $x, y \in A$ on a*

$$xy = 0 \implies (x = 0 \ \text{ ou } \ y = 0) \ ,$$

ou par contraposée :

$$(x \neq 0 \ \text{ et } \ y \neq 0) \implies xy \neq 0 \ .$$

Exercice 66. Montrer que dans un anneau intègre on peut simplifier pour la multiplication, c'est-à-dire : si $ax = ay$ alors $a = 0$ ou $x = y$.

Proposition 4.1.16. *Si A est un corps alors A est intègre.*

Démonstration. Supposons que A est un corps, et soient $x, y \in A$ tels que $xy = 0$. Si $x \neq 0$ alors x est inversible et en multipliant par x^{-1} on obtient $y = 0$. □

Des exemples :

- ▷ $\mathbb{Z}$ est un anneau intègre qui n'est pas un corps. En effet, le produit de deux entiers non nuls est non nul, mais 2 n'est pas inversible dans $\mathbb{Z}$.
- ▷ $\mathbb{R}[X]$ est un anneau intègre qui n'est pas un corps. En effet, le produit de deux polynômes (à coefficients réels) non nuls est non nul, mais X n'est pas inversible dans $\mathbb{R}[X]$.
- ▷ L'anneau $\mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre. En effet, soit f la fonction indicatrice de l'intervalle $[0, 1]$ et g la fonction indicatrice de l'intervalle $[2, 3]$, on a $f \neq 0$, $g \neq 0$, mais $fg = 0$.
- ▷ Si $n \geqslant 2$ est un nombre composé, alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. En effet, écrivons $n = ab$ avec $1 < a, b < n$, on a alors $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, et $\overline{a} \times \overline{b} = \overline{ab} = \overline{n} = \overline{0}$.

4.1.8 Produit d'anneaux

Soient A et B deux anneaux. On munit le produit cartésien $A \times B$ de lois $+$ et $\times$:

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y)(x', y') = (xx', yy')$$

Proposition 4.1.17. *Muni de ces lois, $A \times B$ est un anneau.*

Démonstration. Laissé au lecteur. □

On vérifie que le zéro de $A \times B$ est $(0_A, 0_B)$ et que le un est $(1_A, 1_B)$. Si A et B sont commutatifs alors $A \times B$ l'est aussi.

Définition 4.1.18. *On appelle $A \times B$ l'***anneau produit** *de A et B.*

- ▷ Plus généralement, pour une famille $(A_i)_{i \in I}$ d'anneaux indexée par un ensemble I, on peut former le produit
$$\prod_{i \in I} A_i,$$
qui est un anneau où les lois se calculent "coordonnée par coordonnée".
- ▷ Si tous les anneaux A_i sont égaux au même anneau A, on note cet anneau A^I.

Remarque 4.1.19. Si $A \neq \{0_A\}$ et $B \neq \{0_B\}$ alors $A \times B$ n'est pas un anneau intègre. En effet on a $(1_A, 0_B)(0_A, 1_B) = (0_A, 0_B)$.

4.1.9 Fonctions à valeurs dans un anneau

Soit A un anneau et I un ensemble. Rappelons que A^I peut être vu comme l'ensemble des applications $f : I \to A$. Avec ce point de vue, les loi $+$ et $\times$ se calculent, pour $f_1, f_2 : I \to A$, par les formules

$$(f_1 + f_2)(i) = f_1(i) + f_2(i) \quad \text{et} \quad (f_1 \times f_2)(i) = f_1(i) \times f_2(i)$$

Le zéro est la fonction nulle ($f(i) = 0_A$ pour tout $i \in I$) et le un est la fonction constante égale à 1_A ($f(i) = 1_A$ pour tout $i \in I$).

Exemple 4.1.20.

1. Pour $I = \mathbb{R}$ et $A = \mathbb{R}$ on retrouve l'exemple déjà vu de l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$.
2. Pour $I = \mathbb{N}$ on obtient l'anneau $A^{\mathbb{N}}$ des suites d'éléments de A (où l'addition et la multiplication des suites se calcule terme à terme).

4.2 Sous-anneaux

4.2.1 Définition

Définition 4.2.1. *Soit $(A, +, \times)$ un anneau. Un* **sous-anneau** *de A est un sous-ensemble $B \subset A$ qui vérifie les conditions suivantes :*

(1) $(B, +)$ est un sous-groupe de $(A, +)$.

(2) $1_A \in B$.

(3) B est stable par $\times$: $\forall x, y \in B$, $x \times y \in B$.

Proposition 4.2.2. *Soit A un anneau et B un sous-anneau de A. Alors B, muni des restrictions des lois $+$ et $\times$, est un anneau, dont le zéro est $0_B = 0_A$ et le un est $1_B = 1_A$.*

Démonstration. Comme B est stable par $+$ et $\times$, ces deux opérations sont bien des lois de composition internes sur B. On vérifie alors facilement que les axiomes pour B sont une conséquence des axiomes pour A et du fait que $0_A \in B$ et $1_A \in B$. □

Remarque 4.2.3. C'est une manière pratique de montrer que quelque chose est un anneau en montrant que c'est un sous-anneau d'un anneau déjà connu.

Remarque 4.2.4. Si A est commutatif alors B l'est aussi. Si A est intègre alors B l'est aussi.

4.2.2 Exemples

Des exemples de sous-anneaux :

- A est toujours un sous-anneau de A.
- $\mathbb{Z}$ et $\mathbb{Q}$ sont des sous-anneaux de $\mathbb{R}$.
- L'ensemble des polynômes pairs $\mathbb{R}[X^2]$ est un sous-anneau de $\mathbb{R}[X]$.
- L'ensemble de suites convergentes est un sous-anneau de l'anneau $\mathbb{R}^{\mathbb{N}}$.
- L'ensemble des fonctions continues $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ est un sous-anneau de l'anneau $\mathbb{R}^{\mathbb{R}}$.

Des non-exemples de sous-anneaux :

- Pour un anneau $A \neq \{0_A\}$, le sous-groupe $\{0_A\}$ de A n'est pas un sous-anneau de A car il ne contient pas 1_A.
- Le sous-groupe $2\mathbb{Z} \subset \mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1.

Exercice 67. Montrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$.

4.2.3 Sous-corps

Définition 4.2.5. *Soit L un corps. Un* **sous-corps** *de L est un sous-anneau $K \subset L$ qui vérifie en plus :*

$$\forall x \in K \setminus \{0\},\ \frac{1}{x} \in K\ .$$

De manière équivalente, c'est un corps K qui est inclus dans L et dont les lois $+$ et $\times$ sont les restrictions de celles de L. On dit aussi que L est une **extension** *de K.*

Proposition 4.2.6. *Soit L un corps, soit K un sous-corps de L. Alors L acquiert une structure de K-espace vectoriel, où la somme est la somme dans L, et la multiplication externe $a.x$, avec $a \in K$ et $x \in L$, est simplement la multiplication ax dans le corps L.*

Démonstration. Laissé au lecteur. □

Exemple 4.2.7. $\mathbb{R}$ est un sous-corps de $\mathbb{C}$, ce qui fait de $\mathbb{C}$ un $\mathbb{R}$-espace vectoriel (de dimension 2). $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, ce qui fait de $\mathbb{R}$ un $\mathbb{Q}$-espace vectoriel (de dimension infinie).

4.3 Morphismes d'anneaux

4.3.1 Définition

Définition 4.3.1. *Soient A et B deux anneaux. Un* **morphisme d'anneaux** *de A vers B est une application $f : A \to B$ qui vérifie les axiomes suivants :*

(1) Compatibilité à la somme $+$: $\forall x, y \in A$, $f(x+y) = f(x) + f(y)$ (dit autrement, f est un morphisme de groupes) ;

(2) Compatibilité au produit $\times$: $\forall x, y \in A$, $f(x \times y) = f(x) \times f(y)$;

(3) Compatibilité aux unités : $f(1_A) = 1_B$.

La condition (1) implique que $f(0_A) = 0_B$, mais la condition (2) n'implique pas la condition (3). Par exemple le morphisme nul donné pour tout $x \in A$ par $f(x) = 0_B$ vérifie (1) et (2) mais pas (3).

Exercice 68. Montrer que la composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Proposition 4.3.2. *Pour un anneau A donné, il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$. Il est donné par la formule $f(n) = n1_A$ pour $n \in \mathbb{Z}$.*

Démonstration. Il est clair que la formule $f(n) = n1_A$ définit bien un morphisme d'anneaux, par les propriétés $(m+n)1_A = m1_A + n1_A$, $(mn)1_A = (m1_A)(n1_A)$, et $1\,1_A = 1_A$. Maintenant, si $g : \mathbb{Z} \to A$ est un morphisme d'anneaux quelconque, alors on doit avoir $g(1) = 1_A$ par la condition (3). La condition (1) implique, par une récurrence évidente sur $n \in \mathbb{N}$, qu'on a $g(n) = n1_A$ pour tout $n \in \mathbb{N}$. Comme on doit aussi avoir, toujours par la condition (1), $g(-n) = -g(n)$, on a $g(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On a donc $g = f$, ce qui montre l'unicité. □

Définition 4.3.3. *Un* **endomorphisme** *d'un anneau A est un morphisme d'anneaux de A dans A.*

4.3.2 Exemples

▷ Soit $n \in \mathbb{N}^*$. L'application $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $f(k) = \overline{k}$ est un morphisme d'anneaux. (C'est le seul, par la proposition 4.3.2.)

▷ La conjugaison $c : \mathbb{C} \to \mathbb{C}$ définie par $c(z) = \overline{z}$ est un morphisme d'anneaux.

4.3.3 Morphismes d'anneaux et inversibles

Proposition 4.3.4. *Soit $f : A \to B$ un morphisme d'anneaux et soit $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x)^{-1} = f(x^{-1})$. De plus, l'application induite $f : A^\times \to B^\times$ est un morphisme de groupes.*

Démonstration. On calcule : $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_A) = 1_B$, et de même $f(x^{-1})f(x) = 1_B$. Le fait que $f : A^\times \to B^\times$ est un morphisme de groupes est évident puisqu'on a $f(xy) = f(x)f(y)$ pour tous $x, y \in A$ et donc notamment pour tous $x, y \in A^\times$. □

4.3.4 Morphismes d'anneaux et sous-anneaux

Proposition 4.3.5. *Soit $f : A \to B$ un morphisme d'anneaux.*

1) Soit B' un sous-anneau de B. Alors $f^{-1}(B')$ est un sous-anneau de A.

2) Soit A' un sous-anneau de A. Alors $f(A')$ est un sous-anneau de B. Notamment, $\mathrm{Im}(f) = f(A)$ est un sous-anneau de B.

Démonstration. 1) ▷ $f^{-1}(B')$ est un sous-groupe de A car c'est l'image réciproque par un morphisme de groupes d'un sous-groupe de B (voir le chapitre précédent).

▷ Comme $f(1_A) = 1_B$ et que $1_B \in B'$, on a que $1_A \in f^{-1}(B')$.

▷ Stabilité par $\times$: pour $x, x' \in f^{-1}(B')$ on a $f(x), f(x') \in B'$, et donc $f(x)f(x') \in B'$ car B' est un sous-anneau de B. Or $f(x)f(x') = f(xx')$ et donc $xx' \in f^{-1}(B')$.

2) ▷ $f(A')$ est un sous-groupe de B car c'est l'image par un morphisme de groupes d'un sous-groupe de A (voir le chapitre précédent).

▷ $1_B = f(1_A) \in f(A')$ car $1_A \in A'$.

▷ Stabilité par $\times$: pour $y, y' \in f(A')$ on peut écrire $y = f(x)$ et $y' = f(x')$ avec $x, x' \in A'$, alors $yy' = f(x)f(x') = f(xx') \in f(A')$ car $xx' \in A'$.

□

Remarque 4.3.6. Attention : $\ker(f)$ n'est pas un sous-anneau de A puisqu'il ne contient pas l'unité 1_A (sauf si B est l'anneau nul, c'est-à-dire si $0_B = 1_B$). La bonne notion est ici celle d'**idéal**, qui sera introduite et étudiée plus loin.

4.3.5 Isomorphismes d'anneaux

Définition 4.3.7. *Un* **isomorphisme** *d'anneaux de A vers B est un morphisme d'anneaux $f : A \to B$ qui est bijectif. On dit alors que A et B sont* **isomorphes** *et on note parfois simplement $A \simeq B$.*

Exemple 4.3.8. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n, et choisissons une base $\mathcal{B}$ de V. On a l'application

$$\mathrm{Mat}_{\mathcal{B}} : \mathrm{End}(V) \to \mathrm{M}_n(\mathbb{R}) \ , \ f \mapsto \mathrm{Mat}_{\mathcal{B}}(f)$$

qui est bijective d'après le cours d'algèbre linéaire. (On rappelle que $\mathrm{Mat}_{\mathcal{B}}(f)$ désigne la matrice de f dans la base $\mathcal{B}$.) C'est un isomorphisme d'anneaux car on a, pour deux endomorphismes linéaires $f, g : V \to V$:

$$\mathrm{Mat}_{\mathcal{B}}(f + g) = \mathrm{Mat}_{\mathcal{B}}(f) + \mathrm{Mat}_{\mathcal{B}}(g),$$

$$\mathrm{Mat}_{\mathcal{B}}(f \circ g) = \mathrm{Mat}_{\mathcal{B}}(f) \times \mathrm{Mat}_{\mathcal{B}}(g),$$

$$\mathrm{Mat}_{\mathcal{B}}(\mathrm{id}_V) = I_n.$$

On a donc un isomorphisme d'anneaux :

$$\mathrm{End}(V) \simeq \mathrm{M}_n(\mathbb{R}).$$

Exemple 4.3.9. Soient $m, n \in \mathbb{N}$ avec $m \wedge n = 1$. Alors le théorème chinois des restes affirme qu'on a une bijection

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\ ,\ \overline{k} \mapsto (\widetilde{k}\ ,\ \widehat{k}\ ).$$

C'est un isomorphisme d'anneaux. En effet, on a pour tous $\overline{k}, \overline{l} \in \mathbb{Z}/mn\mathbb{Z}$:

$$f(\overline{k}+\overline{l}) = f(\overline{k+l}) = (\widetilde{k+l}, \widehat{k+l}) = (\widetilde{k}+\widetilde{l}, \widehat{k}+\widehat{l}) = (\widetilde{k}, \widehat{k}) + (\widetilde{l}, \widehat{l}) = f(\overline{k}) + f(\overline{l}),$$

$$f(\overline{k}\times\overline{l}) = f(\overline{k\times l}) = (\widetilde{k\times l}, \widehat{k\times l}) = (\widetilde{k}\times\widetilde{l}, \widehat{k}\times\widehat{l}) = (\widetilde{k}, \widehat{k}) \times (\widetilde{l}, \widehat{l}) = f(\overline{k}) \times f(\overline{l}),$$

et

$$f(\overline{1}) = (\widetilde{1}, \widehat{1}).$$

La proposition suivante montre que si $A \simeq B$ alors $B \simeq A$.

Proposition 4.3.10. *Soit $f : A \to B$ un isomorphisme d'anneaux. Alors sa réciproque $f^{-1} : B \to A$ est aussi un isomorphisme d'anneaux.*

Démonstration. On a déjà vu dans le chapitre précédent que f^{-1} est un isomorphisme de groupes, et il suffit de montrer que f^{-1} est compatible au produit et aux unités. Soient $y_1, y_2 \in B$, on a :

$$f(f^{-1}(y_1)f^{-1}(y_2)) = f(f^{-1}(y_1))f(f^{-1}(y_2)) = y_1y_2,$$

et donc $f^{-1}(y_1y_2) = f^{-1}(y_1)f^{-1}(y_2)$. De plus, comme $f(1_A) = 1_B$ on a $f^{-1}(1_B) = 1_A$. □

Exercice 69. Montrer que si $A \simeq B$ et $B \simeq C$ alors $A \simeq C$.

Remarque 4.3.11. Deux anneaux A et B qui sont isomorphes ont **les mêmes propriétés** (qui s'énoncent dans le langage de la théorie des anneaux). Ainsi, pour montrer que deux anneaux ne sont pas isomorphes, il suffit de trouver une propriété (qui s'énonce dans le langage de la théorie des anneaux) qui est vraie dans A et pas dans B, ou vice versa. À titre d'exemple, on conseille l'exercice suivant.

Exercice 70. Soient A et B deux anneaux qui sont isomorphes.

1) Montrer que si A est commutatif alors B est commutatif.

2) Montrer que si A est intègre alors B est intègre.

3) Montrer que si l'équation $x^2 = -1_A$ n'a pas de solution dans A alors l'équation $y^2 = -1_B$ n'a pas de solution dans B.

Définition 4.3.12. *Soit A un anneau. Un* **automorphisme** *de A est un isomorphisme de A dans A. (Ou dit autrement, c'est un endomorphisme de A qui est bijectif.)*

Exercice 71. Montrer que $\mathbb{C}$ et $\mathbb{R}^2$ sont isomorphes en tant que groupes mais pas en tant qu'anneaux.

4.3.6 Morphismes d'un corps vers un anneau non nul

Proposition 4.3.13. *Soient K un corps et $A \neq \{0\}$ un anneau non nul. Tout morphisme d'anneaux $f : K \to A$ est injectif.*

Démonstration. Soit $x \in K$ tel que $f(x) = 0_A$, et supposons que $x \neq 0_K$. Alors $0_A = f(\frac{1}{x})f(x) = f(\frac{1}{x} \times x) = f(1_K) = 1_A$, donc A est l'anneau nul, contradiction. □

▷ Notamment, un morphisme d'anneaux d'un corps K vers un corps L est injectif.

4.4 Caractéristique

4.4.1 Définition

Définition 4.4.1. *Soit A un anneau. La* **caractéristique** *de A est le plus petit entier $n \in \mathbb{N}^*$ tel que $n1_A = 0_A$, si ce nombre existe, et 0 sinon.*

Dit autrement, la caractéristique de A est l'ordre de 1_A dans le groupe $(A, +)$ si celui-ci est fini, et 0 si celui-ci est infini.

Exemple 4.4.2. $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n, et $\mathbb{Z}$ est de caractéristique 0.

Une autre manière de définir la caractéristique est la suivante : on considère le morphisme d'anneaux canonique

$$\varphi : \mathbb{Z} \to A \ , \ k \mapsto k1_A.$$

Alors φ est notamment un morphisme de groupes abéliens et donc $\ker(\varphi)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme

$$\ker(\varphi) = n\mathbb{Z}$$

pour un certain entier $n \in \mathbb{N}$. Cet entier n est la caractéristique de A. On a deux cas assez différents :

- Cas $n = 0$. Alors $\ker(\varphi) = \{0\}$ et donc φ est injectif, et donc induit un isomorphisme entre $\mathbb{Z}$ et le sous-anneau $\mathrm{Im}(\varphi) \subset A$. Conclusion : A contient un sous-anneau isomorphe à $\mathbb{Z}$.

- Cas $n > 0$. Alors φ passe au quotient par la relation de congruence modulo n (vérifiez-le). On a donc une application $\psi : \mathbb{Z}/n\mathbb{Z} \to A$ définie par $\psi(\overline{k}) = \varphi(k) = k1_A$. On vérifie facilement que ψ est un morphisme d'anneaux. On montre maintenant qu'il est injectif. Pour $k \in \{1, \dots, n-1\}$ on a $\psi(\overline{k}) = k1_A \neq 0_A$ puisque n est minimal. Donc $\ker(\psi) = \{\overline{0}\}$ et ψ est injectif. Il induit donc un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et le sous-anneau $\mathrm{Im}(\psi) \subset A$. Conclusion : A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

4.4.2 Caractéristique d'un anneau intègre

Proposition 4.4.3. *Un anneau intègre est soit de caractéristique 0 soit de caractéristique p premier.*

Démonstration. Soit A un anneau intègre. Comme $A \neq \{0\}$ on a $0_A \neq 1_A$ et A n'est pas de caractéristique 1. Supposons que A est de caractéristique $n \geqslant 2$ un nombre composé, c'est-à-dire tel qu'on peut écrire $n = ab$ avec $1 < a, b < n$. On peut réécrire $n1_A = 0_A$ comme $(a1_A)(b1_A) = 0_A$, et comme A est intègre cela implique qu'on a $a1_A = 0_A$ ou $b1_A = 0_A$. Comme $a, b < n$, c'est en contradiction avec le fait que n est minimal. □

La notion de caractéristique est particulièrement importante dans le cas des corps.

- Soit K un corps de caractéristique zéro. Alors on a un morphisme d'anneaux $\widetilde{\varphi} : \mathbb{Q} \to K$ donné par $\widetilde{\varphi}(\frac{a}{b}) = \frac{a1_K}{b1_K}$, qui est nécessairement injectif car $\mathbb{Q}$ est un corps. Donc K contient un sous-corps isomorphe à $\mathbb{Q}$. En particulier, c'est un $\mathbb{Q}$-espace vectoriel.

- Un corps de caractéristique p premier contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$. En particulier, c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

4.4.3 Corps finis

Une conséquence particulièrement frappante de la notion de caractéristique est le théorème suivant.

Théorème 4.4.4. *Soit K un corps* **fini**. *Alors il existe un nombre premier p et un entier $r \in \mathbb{N}^*$ tel que le cardinal de K est p^r.*

▷ En particulier, il n'existe pas de corps de cardinal $6 = 2 \times 3$ ou $20 = 4 \times 5$.

Démonstration. – Comme K est fini le morphisme d'anneaux $\varphi : \mathbb{Z} \to K$ ne peut pas être injectif, et K est de caractéristique p premier par la proposition 4.4.3.

– Alors K est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel, qui est nécessairement de dimension finie (il est engendré par l'ensemble de ses vecteurs, qui est un ensemble fini).

– Soit r la dimension de K en tant que $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et choisissons une base $e_1, \dots, e_r$ de K. On a alors un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-espaces vectoriels

$$(\mathbb{Z}/p\mathbb{Z})^r \to K \ , \ (x_1, \dots, x_r) \mapsto x_1 e_1 + \cdots + x_r e_r$$

(vérifier que c'est bien un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-espaces vectoriels !). En particulier on a une bijection entre K et $(\mathbb{Z}/p\mathbb{Z})^r$ et ces deux ensembles ont donc le même cardinal. Donc le cardinal de K est p^r.

□

Remarque 4.4.5. En fait, on peut prouver que pour tout nombre premier p et tout entier $r \in \mathbb{N}^*$ il **existe bien** un corps de cardinal p^r. Mieux, un tel corps est en fait unique à isomorphisme près. Un tel corps est généralement noté $\mathbb{F}_{p^r}$. Nous n'étudierons pas ces corps dans ce cours.

Remarque 4.4.6. Il y a évidemment des corps de caractéristique non nulle qui ne sont pas finis. Par exemple le corps des fractions rationnelles $(\mathbb{Z}/p\mathbb{Z})(X)$, pour p premier, est un corps infini de caractéristique p.

4.4.4 L'endomorphisme de Frobenius

Proposition 4.4.7. *Soit A un anneau commutatif de caractéristique p premier. Alors l'application*

$$F : A \to A \ , \ x \mapsto x^p$$

est un morphisme d'anneaux.

Définition 4.4.8. *On appelle F l'***endomorphisme de Frobenius** *de l'anneau A.*

Démonstration. Clairement on a $F(1) = 1$ et $F(xy) = F(x)F(y)$ pour tous $x, y \in A$ car A est commutatif. Le point subtil est de montrer qu'on a $F(x+y) = F(x) + F(y)$, c'est-à-dire $(x+y)^p = x^p + y^p$. Fixons $x, y \in A$, on a par la formule du binôme (qu'on a le droit d'utiliser car A est commutatif) :

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \ .$$

Pour $k \in \{1, \ldots, p-1\}$, on a vu dans le chapitre 1 (proposition 1.7.1) que p divise le coefficient binomial $\binom{p}{k}$, et donc le terme $\binom{p}{k} x^k y^{p-k}$ vaut 0 dans A. Il ne reste donc que les termes extrêmes : $(x+y)^p = x^p + y^p$. □

4.5 Polynômes à coefficients dans un anneau

On se contente ici de considérer des polynômes dont les coefficients sont pris dans un **anneau commutatif** R.

4.5.1 Définition

Définition 4.5.1. *Soit R un anneau commutatif. Un polynôme à une indéterminée à coefficients dans R est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de R qui est nulle à partir d'un certain rang (il existe un $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $a_n = 0$). On le note comme la combinaison linéaire*

$$f = \sum_{n=0}^{N} a_n X^n \ ,$$

où l'indéterminée X est un symbole formel.

La somme et le produit des polynômes est définie comme d'habitude : si f a pour coefficients a_n et g a pour coefficients b_n alors

$$f+g \text{ a pour coefficients } a_n + b_n$$

et

$$fg \text{ a pour coefficients } c_n = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0.$$

Cela donne à l'ensemble des polynômes une structure d'anneau commutatif (vérifiez-le !), dont le zéro est le polynôme nul (dont tous les coefficients sont 0) et dont le 1 est le polynôme 1 (dont les coefficients sont $1, 0, 0, \ldots$). On note cet anneau $R[X]$.

Définition 4.5.2. *Pour un polynôme non nul f de coefficients a_n, le* **degré** *de f est le plus grand entier $n \in \mathbb{N}$ tel que $a_n \neq 0$. Le coefficient a_n correspondant est appelé* **coefficient dominant** *de f. On dit que f est* **unitaire** *si son coefficient dominant est 1.*

▷ On adopte la convention que le polynôme nul 0 est de degré $-\infty$: $\deg(0) = -\infty$. On adopte la convention que le polynôme nul 0 est unitaire.

Exercice 72. Lister les polynômes de degré $\leqslant 3$ à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. Même chose pour $\mathbb{Z}/3\mathbb{Z}$.

Remarque 4.5.3. Vous avez une certaine familiarité des polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$. Mais attention, des choses non intuitives peuvent arriver si R est un anneau (commutatif) général : par exemple, dans $(\mathbb{Z}/4\mathbb{Z})[X]$ on a $(\overline{1} + \overline{2}X)^2 = \overline{1}$. Un produit de deux polynômes de degré 1 peut être de degré 0... Heureusement rien de tout cela ne se passe si l'anneau des coefficients est intègre !

4.5.2 Degré (cas des coefficients dans un anneau intègre)

Proposition 4.5.4. *Soit R un anneau intègre. Pour $f, g \in R[X]$ on a* $\deg(fg) = \deg(f) + \deg(g)$.

(On étend la somme à $\mathbb{N} \cup \{-\infty\}$ de manière évidente.)

Démonstration. L'égalité est toujours vraie si $f = 0$ ou $g = 0$ et on suppose donc que $f, g \neq 0$. Notons $m = \deg(f)$ et $n = \deg(g)$. Alors clairement tous les coefficients de degré $> m + n$ de fg sont nuls, d'où $\deg(fg) \leqslant m + n$. Si a désigne le coefficient de degré m de f et b le coefficient de degré n de g (coefficients dominants), alors le coefficient de degré $m+n$ de fg est le produit ab, qui est non nul car $a \neq 0$ et $b \neq 0$ et R est un anneau intègre. Donc $\deg(fg) = m + n$. □

Proposition 4.5.5. *Si R est un anneau intègre alors $R[X]$ est aussi un anneau intègre.*

Démonstration. Soient $f, g \in R[X]$ non nuls. Alors $\deg(f) \neq -\infty$ et $\deg(g) \neq -\infty$, et donc par la proposition précédente, $\deg(fg) \neq -\infty$ donc $fg \neq 0$. □

Proposition 4.5.6. *Soit R un anneau intègre. Les inversibles de $R[X]$ sont les polynômes constants inversibles dans R :*

$$R[X]^\times = R^\times.$$

Démonstration. Clairement, tous les polynômes constants inversibles dans R sont inversibles dans $R[X]$. Réciproquement, soit $f \in R[X]^\times$, alors il existe $g \in R[X]$ tel que $fg = 1$. On a donc $0 = \deg(fg) = \deg(f) + \deg(g)$ et donc $\deg(f) = \deg(g) = 0$. Donc f et g sont des polynômes constants, $f = a$ et $g = b$ avec $a, b \in R$. Comme $ab = 1$, on a $a \in R^\times$. □

4.5.3 Fonction polynomiale

À un polynôme $f \in R[X]$ on associe la **fonction polynomiale** correspondante, qu'on note par le même symbole

$$f : R \to R\ ,\ x \mapsto f(x).$$

Elle est définie, pour $f = \sum_{n=0}^{N} a_n X^n$, par $f(x) = \sum_{n=0}^{N} a_n x^n$. Noter que la première somme est une somme "formelle" qui est juste une notation pour les polynômes, alors que la deuxième somme est une vraie somme dans l'anneau R. (Évidemment, la notation pour les polynômes est choisie pour imiter la notation pour les fonctions polynomiales...)

Remarque 4.5.7. Soit p un nombre premier et considérons le polynôme $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$. Ce polynôme n'est pas nul (il est de degré p) mais la fonction polynomiale associée est nulle par le petit théorème de Fermat : pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $x^p - x = \overline{0}$. Il est donc important, en général, de faire la distinction entre polynôme et fonction polynomiale. On verra ci-dessous que si R est un corps infini alors il n'y a pas de risque à confondre polynôme et fonction polynomiale.

4.5.4 Variante : polynômes à plusieurs indéterminées

On peut aussi définir des anneaux de polynômes avec un nombre r d'indéterminées $X_1, \dots, X_r$ à coefficients dans un anneau commutatif R, notés $R[X_1, \dots, X_r]$. Un élément de cet anneau est une application $\mathbb{N}^r \to R$, $(n_1, \dots, n_r) \mapsto a_{n_1,\dots,n_r}$ telle que $a_{n_1,\dots,n_r} \neq 0$ seulement pour un nombre fini de multi-indices $(n_1, \dots, n_r)$. On le représente par la combinaison linéaire **finie** :

$$f = \sum_{(n_1,\dots,n_r)\in\mathbb{N}^r} a_{n_1,\dots,n_r} X_1^{n_1} \cdots X_r^{n_r} \ .$$

Les lois $+$ et $\times$ sont définies de manière évidente. On note que les indéterminées commutent deux à deux : $X_i X_j = X_j X_i$ et que l'anneau $R[X_1, \dots, X_r]$ est commutatif.

Exercice 73. Dans l'anneau $(\mathbb{Z}/3\mathbb{Z})[X, Y]$, développer $(X + \overline{2}Y)^3$.

Remarque 4.5.8. On a un isomorphisme d'anneaux naturel

$$R[X, Y] \simeq (R[X])[Y]$$

qui consiste à voir un polynôme en deux indéterminées X, Y comme un polynôme en une indéterminée Y dont les coefficients sont des polynômes en X. Plus généralement on a un isomorphisme d'anneaux naturel $R[X_1, \dots, X_r] \simeq (R[X_1, \dots, X_{r-1}])[X_r]$. Cette remarque permet parfois de prouver des propriétés des anneaux de polynomes à **plusieurs** indéterminées en se ramenant par récurrence au cas d'une seule indéterminée.

Remarque 4.5.9. On peut définir des anneaux de polynômes avec un ensemble quelconque (notamment infini) d'indéterminées ; dans ce cas, chaque polynôme donné ne fait intervenir qu'un nombre **fini** d'indéterminées.

4.6 Quelques notions supplémentaires

4.6.1 Algèbre sur un corps

Définition 4.6.1. *Soit K un corps. Une K-**algèbre** (ou **algèbre sur** K) est un quadruplet $(A, +, ., \times)$ où :*

(1) $(A, +, .)$ est un K-espace vectoriel ;

(2) $(A, +, \times)$ est un anneau ;

(3) les lois $.$ et $\times$ sont compatibles : $\forall a, b \in K$, $\forall x, y \in A$, $(a.x) \times (b.y) = (ab).(x \times y)$.

Des exemples de K-algèbres :

- ▷ Le corps K lui-même est une K-algèbre.
- ▷ On a l'algèbre $K^{\mathbb{N}}$ des suites d'éléments de K.
- ▷ L'anneau de polynômes $K[X]$ (qu'on redéfinira plus bas) est une K-algèbre.
- ▷ L'anneau des matrices $\mathrm{M}_n(K)$ est une K-algèbre (non commutative si $n \geqslant 2$).
- ▷ Pour V un K-espace vectoriel on a la K-algèbre des endomorphismes K-linéaires de V, notée $\mathrm{End}(V)$, non commutative si $\dim(V) \geqslant 2$.

4.6.2 Corps des fractions d'un anneau intègre

Soit A un anneau intègre. On veut se donner la possibilité de considérer des "fractions" d'éléments de A. On définit pour cela sur l'ensemble $A \times A\backslash\{0\}$ la relation :

$$(a, b) \sim (a', b') \;\Leftrightarrow\; ab' = a'b \; .$$

L'intuition qu'il faut avoir est que le couple (a, b) va jouer le rôle de la fraction $\frac{a}{b}$; de ce point de vue-là cette relation est naturelle puisqu'on a envie de considérer que $\frac{a}{b}$ et $\frac{a'}{b'}$ sont le même élément si $ab' = a'b$.

Proposition 4.6.2. *La relation $\sim$ sur $A \times A\backslash\{0\}$ est une relation d'équivalence.*

Démonstration. La relation $\sim$ est évidemment réflexive et symétrique. Le point subtil est la transitivité. Supposons qu'on a trois couples (a, b), (a', b'), (a'', b'') dans $A \times A\backslash\{0\}$ tels que $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'')$. Alors on a $ab' = a'b$ et $a'b'' = a''b'$. On calcule :

$$(ab'')b' = (ab')b'' = (a'b)b'' = (a'b'')b = (a''b')b = (a''b)b' \; .$$

On a donc $(ab'')b' = (a''b)b'$ et donc comme $b' \neq 0$ et comme A est intègre on peut simplifier et cela donne $ab'' = a''b$, donc $(a, b) \sim (a'', b'')$. La relation $\sim$ est donc bien transitive. □

- ▷ On note $\mathrm{Frac}(A)$ le quotient de $A \times A\backslash\{0\}$ par la relation d'équivalence $\sim$.
- ▷ On note $\frac{a}{b}$ la classe d'équivalence d'un couple (a, b) dans $\mathrm{Frac}(A)$.

Proposition 4.6.3. *Les formules*

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \qquad et \qquad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}$$

définissent des lois de composition internes sur $\mathrm{Frac}(A)$*, qui font de* $\mathrm{Frac}(A)$ *un corps.*

Définition 4.6.4. *On appelle* $\mathrm{Frac}(A)$ *le* **corps des fractions** *de l'anneau intègre* A*.*

Démonstration. Remarquons que les lois $+$ et $\times$ sont commutatives.

– Première étape : on montre que ces lois sont bien définies, c'est-à-dire passent au quotient. Soient (a,b) et (a',b') dans $A\times A\backslash\{0\}$ tels que $(a,b)\sim(a',b')$. On doit montrer que pour tout (c,d) on a $(a,b)+(c,d)\sim(a',b')+(c,d)$ et $(a,b)\times(c,d)\sim(a',b')\times(c,d)$. Pour la somme on calcule : $(ad+bc)b'd-(a'd+b'c)bd=(ab'-a'b)d^2=0$. Pour le produit on calcule : $(ac)(b'd)-(a'c)(bd)=(ab'-a'b)cd=0$.

– Deuxième étape : on montre que ces lois font bien de $\mathrm{Frac}(A)$ un corps.

(1) Associativité de $+$: on calcule $(\frac{a}{b}+\frac{c}{d})+\frac{e}{f}=\frac{(ad+bc)f+ebd}{bdf}$ et $\frac{a}{b}+(\frac{c}{d}+\frac{e}{f})=\frac{adf+b(cf+de)}{bdf}$, qui sont égaux.

(2) Neutre pour $+$: le neutre est $\frac{0}{1}$.

(3) Inverse pour $+$: on a $\frac{a}{b}+\frac{-a}{b}=\frac{0}{b^2}=\frac{0}{1}$ car $0\times 1=b^2\times 0$.

(4) Associativité de $\times$: on calcule $(\frac{a}{b}\times\frac{c}{d})\times\frac{e}{f}=\frac{ace}{bdf}$ et $\frac{a}{b}\times(\frac{c}{d}\times\frac{e}{f})=\frac{ace}{bdf}$.

(5) Neutre pour $\times$: le neutre est $\frac{1}{1}$.

(6) Compatibilité entre $+$ et $\times$: on calcule $\frac{a}{b}\times(\frac{c}{d}+\frac{e}{f})=\frac{a(cf+de)}{bdf}$ et $\frac{a}{b}\times\frac{c}{d}+\frac{a}{b}\times\frac{e}{f}=\frac{acbf+bdae}{bdbf}=\frac{a(cf+de)\times b}{bdf\times b}$, donc les deux résultats sont égaux.

(7) Inverse pour $\times$: pour $\frac{a}{b}\neq\frac{0}{1}$, c'est-à-dire tel que $a\neq 0$, on peut considérer l'élément $\frac{b}{a}\in\mathrm{Frac}(A)$ et on a $\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}$.

□

▷ Dans le cas $A=\mathbb{Z}$ on retrouve le corps $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$.

▷ Dans le cas $A=K[X]$, avec K un corps, on retrouve le corps $\mathrm{Frac}(K[X])=K(X)$, le corps des fractions rationnelles en une indéterminée à coefficients dans K.

▷ On a plus généralement le corps des fractions rationnelles en plusieurs indéterminées $K(X_1,\dots,X_r)=\mathrm{Frac}(K[X_1,\dots,X_r])$.

4.6.3 Sous-anneau engendré par une partie

Proposition 4.6.5. *Soit* A *un anneau, soit* $(B_i)_{i\in I}$ *une famille de sous-anneaux de* A *indexée par un ensemble* I*. Alors l'intersection*

$$B=\bigcap_{i\in I}B_i$$

est un sous-anneau de A*.*

On rappelle la définition :

$$\bigcap_{i\in I} B_i = \{x \in A \mid \forall i \in I,\, x \in B_i\}.$$

▷ Notamment, si B et B' sont deux sous-anneaux de A, alors l'intersection $B \cap B'$ est un sous-anneau de A.

Démonstration. (1) On a déjà vu au chapitre précédent que $(B, +)$ est un sous-groupe de $(A, +)$

(2) Comme chaque B_i est un sous-anneau de A, on a que $1_A \in B_i$ pour tout $i \in I$, et donc $1_A \in B$.

(3) Soient $x, y \in B$, alors pour tout $i \in I$, $x \in B_i$ et $y \in B_i$. Comme chaque B_i est un sous-anneau de A, on a que $xy \in B_i$ pour tout $i \in I$, et donc $xy \in B$.

□

Soit A un anneau et soit $S \subset A$ un sous-ensemble (pas nécessairement un sous-anneau).

Définition 4.6.6. *Le* **sous-anneau de** A **engendré par** S*, noté* $\langle S \rangle$*, est l'intersection de tous les sous-anneaux de* A *qui contiennent* S*.*

Remarque 4.6.7. La notation $\langle \cdots \rangle$ dépend donc du contexte : sous-groupe engendré par une partie, ou sous-anneau engendré par une partie.

C'est bien un sous-anneau de A par la proposition 4.6.5. On a clairement $S \subset \langle S \rangle$, et pour tout sous-anneau B de A on a l'équivalence :

$$S \subset B \quad \Longleftrightarrow \quad \langle S \rangle \subset B.$$

On dit donc que $\langle S \rangle$ est le plus petit (pour l'inclusion) sous-anneau de A qui contient S.

Proposition 4.6.8. *Le sous-anneau* $\langle S \rangle$ *est l'ensemble des éléments de* A *qu'on peut obtenir en faisant des combinaisons* $\mathbb{Z}$*-linéaires de produits d'éléments de* S*, c'est-à-dire l'ensemble des sommes*

$$\sum_{i=1}^{N} n_i\, x_{i,1} x_{i,2} \cdots x_{i,r_i}$$

avec $N \in \mathbb{N}$*, les* $n_i \in \mathbb{Z}$*, les* $r_i \in \mathbb{N}$ *et les* $x_{i,j} \in S$*.*

Ici on prend les conventions qu'une somme indexée par l'ensemble vide dans un anneau A est égale à 0_A, et qu'un produit indexé par l'ensemble vide dans un anneau A est égal à 1_A.

Démonstration. Notons B_0 le sous-ensemble de A décrit par la proposition et montrons que $\langle S \rangle = B_0$. On montre d'abord que B_0 est un sous-anneau de A.

1) On laisse au lecteur le soin de vérifier que $(B_0, +)$ est un sous-groupe de $(A, +)$.

2) On a que $1_A \in B_0$ (produit indexé par l'ensemble vide).

3) A est stable par produit car on peut développer :

$$\left(\sum_{i=1}^{N} n_i\, x_{i,1}\cdots x_{i,r_i}\right)\left(\sum_{j=1}^{M} m_j\, y_{j,1}\cdots y_{j,s_j}\right) = \sum_{\substack{1\leqslant i\leqslant N\\ 1\leqslant j\leqslant M}} n_i m_j\, x_{i,1}\cdots x_{i,r_i} y_{j,1}\cdots y_{j,s_j}.$$

De plus, il est clair que $S \subset B_0$. Comme $\langle\, S\,\rangle$ est l'intersection de tous les sous-anneaux de A qui contiennent S, on a donc l'inclusion $\langle\, S\,\rangle \subset B_0$.

Pour montrer l'inclusion réciproque $B_0 \subset \langle\, S\,\rangle$, il faut montrer que B_0 est inclus dans tous les sous-anneaux de A qui contiennent S. Soit donc B un tel sous-anneau. On a que $S \subset B$, que B contient 1_A et est stable par produit. Il contient tous les produits $x_{i,1}x_{i,2}\cdots x_{i,r_i}$ où les $x_{i,j} \in S$. Comme B est un sous-groupe de A, il est stable par combinaisons $\mathbb{Z}$-linéaires et contient donc tous les combinaisons linéaires de tels produits. Donc $B_0 \subset B$. Comme cette inclusion est vraie pour tout sous-anneau B de A qui contient S, on en déduit que $B_0 \subset \langle\, S\,\rangle$. On a donc montré que $\langle\, S\,\rangle = B_0$. □

Lorsque $S = \{s_1, \ldots, s_k\}$ est finie, on note simplement.

$$\langle\, S\,\rangle = \langle\, s_1, \ldots, s_k\,\rangle.$$

La description est particulièrement simple quand il y a un seul générateur.

Proposition 4.6.9. *Soit A un anneau, soit $s \in A$. Alors le sous-anneau de A engendré par s a la description concrète suivante :*

$$\langle\, s\,\rangle = \left\{\sum_{i=0}^{N} a_i s^i\,,\ N \in \mathbb{N},\ a_0, \ldots, a_N \in \mathbb{Z}\right\}.$$

Démonstration. C'est une conséquence de la proposition 4.6.8. □

4.7 Rappels d'arithmétique des polynômes (à coefficients dans un corps)

On se place dans $K[X]$, avec K un corps.

4.7.1 Divisibilité et division euclidienne

Définition 4.7.1. *Soient $f, g \in K[X]$. On dit que f* **divise** *g et on note*

$$f|g$$

s'il existe $h \in K[X]$ tel que $g = fh$. On dit aussi que f est un **diviseur** *de g, ou que g est* **divisible** *par f ou est un* **multiple** *de f.*

Parmi les propriétés importantes de la divisibilité on a, pour $f, g \in K[X]$:

▷ Si $f|g$ et $g \neq 0$ alors $\deg(f) \leqslant \deg(g)$.

▷ $(f|g \text{ et } g|f) \iff \exists\, a \in K^*,\ f = ag$.

Définition 4.7.2. *Un polynôme $f \in K[X]$ est dit* **irréductible** *s'il n'est pas constant et que ses seuls diviseurs sont tous de la forme $a \in K^*$ ou af avec $a \in K^*$.*

▷ Dit autrement, f est irréductible si f n'est pas constant et que pour tous $g, h \in K[X]$,

$$f = gh \quad \Longrightarrow \quad g \in K^* \ \text{ ou } \ h \in K^*.$$

▷ Tout polynôme f de degré 1 est irréductible. En effet, si on écrit $f = gh$ alors $\deg(g) + \deg(h) = 1$ et donc $\deg(g) = 0$ ou $\deg(h) = 0$.

Remarque 4.7.3. On rappelle la classification des polynômes irréductibles pour $K = \mathbb{C}$ et $K = \mathbb{R}$, conséquence du "théorème fondamental de l'algèbre" :

▷ Dans $\mathbb{C}[X]$, les seuls polynômes irréductibles sont les polynômes de degré 1.

▷ Dans $\mathbb{R}[X]$, les seuls polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant < 0 (c'est-à-dire de la forme $aX^2 + bX + c$ avec $b^2 - 4ac < 0$).

Dans $\mathbb{Q}[X]$ il existe des polynômes irréductibles de n'importe quel degré. Par exemple on peut montrer que le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \in \mathbb{N}^*$.

On rappelle le théorème de division euclidienne des polynômes.

Théorème 4.7.4. *Soit $f \in K[X]$ et $g \in K[X] \setminus \{0\}$. Alors il existe des polynômes $q, r \in K[X]$ avec $\deg(r) < \deg(g)$ tels que*

$$f = gq + r\ .$$

Le couple (q, r) est unique.

Exercice 74. Dans $\mathbb{R}[X]$, calculer la division euclidienne de $X^4 - X^2 + 7$ par $X^2 + X + 1$.

4.7.2 Racines

Proposition 4.7.5. *Soit $f \in K[X]$. On a l'équivalence :*

$$f(a) = 0 \quad \iff \quad (X - a) \mid f.$$

Démonstration. La direction $\Longleftarrow$ est évidente. Pour la direction $\Longrightarrow$, écrivons la division euclidienne de f par $X - a$ sous la forme $f = (X - a)g + \lambda$ avec $g \in K[X]$ et $\lambda \in K$. En évaluant cette égalité en a, on obtient $f(a) = \lambda$. Ainsi, si $f(a) = 0$ alors $\lambda = 0$ et donc $f = (X - a)g$, d'où $(X - a) \mid f$. □

Remarque 4.7.6. La proposition précédente est vraie même si l'on remplace K par n'importe quel anneau commutatif R (pouvez-vous le montrer ?). Ce n'est pas le cas de la proposition suivante.

Proposition 4.7.7. *Soit $f \in K[X]$, et soient $a_1, \dots, a_n$ des éléments deux à deux distincts de K. On a l'équivalence :*

$$f(a_1) = \cdots = f(a_n) = 0 \quad \iff \quad (X - a_1) \cdots (X - a_n) \mid f.$$

Démonstration. La direction $\Longleftarrow$ est évidente. On démontre la direction $\Longrightarrow$ par récurrence sur n.

- ▷ Hypothèse de récurrence : pour tout $n \in \mathbb{N}$ considérons l'hypothèse de récurrence $P(n)$: "pour tous $a_1, \dots, a_n \in K$ deux à deux distincts, pour tout $f \in K[X]$, si $f(a_1) = \cdots = f(a_n) = 0$ alors $(X - a_1) \cdots (X - a_n)$ divise f".
- ▷ Initialisation : pour $n = 0$ il n'y a rien à montrer et $P(0)$ est vraie.
- ▷ Hérédité : soit $n \geqslant 0$ tel que $P(n)$ est vraie, et montrons que $P(n+1)$ est vraie. Soient donc $a_1, \dots, a_{n+1} \in K$ deux à deux distincts, et soit $f \in K[X]$ un polynôme qui vérifie $f(a_1) = \cdots = f(a_{n+1}) = 0$. Comme $f(a_{n+1}) = 0$, la proposition précédente implique qu'on peut écrire
$$f = (X - a_{n+1})g$$
avec $g \in K[X]$. Si on évalue cette égalité en a_i, pour un certain $i \in \{1, \dots, n\}$, on obtient $0 = (a_i - a_{n+1})g(a_i)$. Or $a_i \neq a_{n+1}$ par hypothèse et donc, comme on travaille dans un corps K, on en conclut que $g(a_i) = 0$. On peut donc appliquer l'hypothèse de récurrence $P(n)$ à g, et il existe donc $h \in K[X]$ tel que $g = (X - a_1) \cdots (X - a_n)h$. On obtient donc
$$f = (X - a_1) \cdots (X - a_n)(X - a_{n+1})h$$
et donc $(X - a_1) \cdots (X - a_n)(X - a_{n+1})$ divise f. On a donc montré que $P(n+1)$ est vraie.
- ▷ Conclusion : on a donc bien montré que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

□

Définition 4.7.8. *Soit $f \in K[X]$. On dit que $a \in K$ est une* **racine** *de f si $f(a) = 0$.*

Proposition 4.7.9. *Un polynôme $f \in K[X]$ non nul de degré $\leqslant n$ a au plus n racines.*

Démonstration. Si f a $n+1$ racines $a_1, \ldots, a_{n+1}$ deux à deux distinctes, alors par la proposition précédente, $(X - a_1) \cdots (X - a_{n+1})$ divise f, et donc comme f est non nul, f est de degré $\geqslant n+1$. C'est impossible : contradiction. □

Remarque 4.7.10. La proposition précédente est fausse pour les polynômes à coefficients dans un anneau (commutatif) général. Par exemple, le polynôme $X^2 - X \in (\mathbb{Z}/6\mathbb{Z})[X]$ a 4 racines : $\overline{0}$, $\overline{1}$, $\overline{3}$, $\overline{4}$.

Exercice 75. Vérifier que dans $(\mathbb{Z}/6\mathbb{Z})[X]$ le polynôme $X^2 - X$ est divisible par X, par $X - \overline{1}$, par $X - \overline{3}$, et par $X - \overline{4}$, en accord avec la remarque 4.7.6.

Proposition 4.7.11. *Supposons que K est infini. Soient $f, g \in K[X]$ telles que les fonctions polynomiales associées à f et g sont égales. Alors les polynômes f et g sont égaux.*

Démonstration. Par hypothèse on a : $\forall x \in K$, $f(x) = g(x)$ et donc $(f-g)(x) = 0$. Donc le polynôme $f - g$ a tous les éléments de K pour racines. Comme K est infini, la proposition précédente implique que le polynôme $f - g$ est nul, et donc que les polynômes f et g sont égaux. □

▷ Cela justifie que pour $K = \mathbb{R}$ ou $K = \mathbb{C}$ on se permette de ne pas faire de différence entre polynômes et fonctions polynomiales.

Remarque 4.7.12. La proposition précédente est fausse sur un corps fini (remarque 4.5.7).

4.7.3 Idéaux de $K[X]$

Définition 4.7.13. *Un* **idéal** *de $K[X]$ est un sous-ensemble $I \subset K[X]$ qui vérifie*

1) I est un sous-groupe de $(K[X], +)$.

2) I est stable par multiplication par tout élément de $K[X]$: pour tout $f \in K[X]$, pour tout $g \in I$, $fg \in I$.

Proposition 4.7.14. *Soit $f \in K[X]$. Alors l'ensemble des multiples de f, noté*

$$(f) = \{fg,\ g \in K[X]\},$$

est un idéal de $K[X]$.

Démonstration. ▷ $0 \in (f)$ car $0 = f \times 0$.

▷ (f) est stable par somme : pour tous $g, h \in K[X]$ on a $fg + fh = f(g+h) \in (f)$.

▷ (f) est stable par passage à l'opposé : pour tout $g \in K[X]$ on a $-fg = f(-g) \in (f)$.

▷ (f) est stable par multiplication par tout élément de $K[X]$: pour $g \in K[X]$ et $h \in K[X]$ on a $fg \times h = f(gh) \in (f)$.

□

Proposition 4.7.15. *Soient $f_1, f_2 \in K[X]$.*

1) On a

$$(f_1) \subset (f_2) \iff f_2 | f_1.$$

2) On a

$$(f_1) = (f_2) \iff \exists\, a \in K^*,\ f_2 = a f_1.$$

Démonstration. 1) Supposons que $(f_1) \subset (f_2)$. Comme $f_1 = f_1 \times 1$, on a $f_1 \in (f_1)$ et donc $f_1 \in (f_2)$, d'où par définition $f_2 | f_1$. Réciproquement, supposons que $f_2 | f_1$, on peut donc écrire $f_1 = f_2 h$ avec $h \in K[X]$. Alors $(f_1) \subset (f_2)$ car pour tout $g \in K[X]$ on a $f_1 g = f_2(hg) \in (f_2)$.

2) Par 1), $(f_1) = (f_2)$ équivaut à : $f_1 | f_2$ et $f_2 | f_1$. C'est équivalent à : $\exists\, a \in K^*, f_2 = a f_1$.

□

Théorème 4.7.16. *Soit I un idéal de $K[X]$. Alors il existe un polynôme $f \in K[X]$ tel que $I = (f)$.*

▷ Par la proposition précédente, f n'est unique qu'à multiplication par un élément de K^* près.

▷ Si l'on demande que f soit unitaire, alors f devient unique.

Démonstration. Soit I un idéal de $K[X]$. Si $I = \{0\}$ alors $I = (0)$ et on a gagné. Sinon il existe un polynôme $f_0 \in I \setminus \{0\}$, et on en choisit un de degré minimal.

– On a $(f_0) \subset I$ car I est un idéal de $K[X]$.

– Montrons que $I \subset (f_0)$. Soit $f \in I$, on effectue la division euclidienne de f par f_0 : $f = f_0 q + r$ avec $q, r \in K[X]$, $\deg(r) < \deg(f_0)$. Comme I est un idéal et que f_0 et f sont dans I, $r = f - f_0 q \in I$. On ne peut pas avoir $r \neq 0$ puisque sinon on aurait $r \in I \setminus \{0\}$ de degré $< \deg(f_0)$, ce qui contredirait le fait que f_0 est de degré minimal parmi les polynômes dans $I \setminus \{0\}$. Donc $r = 0$ et $f = f_0 q \in (f_0)$. On a donc bien montré que $I \subset (f_0)$.

□

Définition 4.7.17. *Soit I un idéal de $K[X]$. L'unique polynôme f unitaire tel que $I = (f)$ est appelé le* **générateur unitaire** *de I.*

4.7.4 PGCD et PPCM

PGCD

Proposition 4.7.18. *Soient $f, g \in K[X]$. Alors l'ensemble*

$$(f, g) = \{fu + gv,\ u, v \in K[X]\}$$

est un idéal de $K[X]$.

▷ On l'appelle l'**idéal de $K[X]$ engendré par f et g.**

Démonstration. Laissé au lecteur. □

Définition 4.7.19. *Le générateur unitaire de (f, g) est appelé le* **plus grand commun diviseur (PGCD)** *de f et g. On le note* $\mathrm{PGCD}(f, g)$ *ou* $f \wedge g$.

On a donc :

$$(f, g) = (f \wedge g).$$

On laisse au lecteur le soin de démontrer que le PGCD des polynômes vérifie les mêmes propriétés que le PGCD des entiers. Notamment, on a la propriété importante, pour $f, g, h \in K[X]$:

$$(f + gh) \wedge g = f \wedge g.$$

Cette propriété permet d'expliquer qu'on peut calculer le PGCD des polynômes par l'**algorithme d'Euclide**.

On a aussi la proposition suivante qui explique la dénomination "plus grand commun diviseur".

Proposition 4.7.20. *Soient $f, g \in K[X]$. Alors $f \wedge g$ est l'unique $h \in K[X]$ unitaire qui vérifie les deux conditions suivantes.*

1) $h|f$ et $h|g$;

2) pour tout $k \in K[X]$, $(k|f \text{ et } k|g) \Longrightarrow k|h$.

Démonstration. Laissé au lecteur. □

Définition 4.7.21. *On dit que deux polynômes $f, g \in K[X]$ sont* **premiers entre eux** *si $f \wedge g = 1$.*

Cela revient à dire que les seuls diviseurs communs à f et g sont constants.

Exercice 76. Dans $\mathbb{R}[X]$, calculer le PGCD des polynômes $X^5 + 2X^4 - X^2 + 1$ et $X^4 - 1$.

PPCM

Proposition 4.7.22. *Soient $f, g \in K[X]$. L'ensemble $(f) \cap (g)$ est un idéal de $K[X]$.*

Démonstration. Laissé au lecteur. □

On note que $(f) \cap (g)$ est l'ensemble des polynômes qui sont à la fois des multiples de f et de g.

Définition 4.7.23. *Le générateur unitaire de $(f) \cap (g)$ est appelé le* **plus petit commun multiple (PPCM)** *de f et g. On le note* $\mathrm{PPCM}(f,g)$ *ou* $f \vee g$.

On a donc :

$$(f) \cap (g) = (f \vee g).$$

On laisse au lecteur le soin de démontrer que le PPCM des polynômes vérifie les mêmes propriétés que le PPCM des entiers. On a notamment la proposition suivante qui explique la dénomination "plus petit commun multiple".

Proposition 4.7.24. *Soient $f, g \in K[X]$. Alors $f \vee g$ est l'unique $h \in K[X]$ unitaire qui vérifie les deux conditions suivantes.*

1) $f|h$ et $g|h$;

2) pour tout $k \in K[X]$, $(f|k \text{ et } g|k) \Longrightarrow h|k$.

Démonstration. Laissé au lecteur. □

4.7.5 Gauss, Euclide, Bézout, et factorisation en polynômes irréductibles

On laisse au lecteur le soin d'énoncer et démontrer les analogues pour les polynômes des théorèmes classiques de l'arithmétique des entiers :

- ▷ le lemme de Gauss (et sa variante) ;
- ▷ le lemme d'Euclide ;
- ▷ le théorème de Bézout ;
- ▷ le théorème de factorisation en produit de polynômes irréductibles.

Exercice 77. Le faire en copiant les preuves du chapitre 1.

Exercice 78. Dans $\mathbb{R}[X]$, déterminer une relation de Bézout pour $X^5 + 2X^4 - X^2 + 1$ et $X^4 - 1$.

4.8 Idéaux

Dans toute cette section A est un anneau **commutatif**.

4.8.1 Définition

Définition 4.8.1. *Un* **idéal** *de A est un sous-ensemble $I \subset A$ qui vérifie :*

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

2) I est stable par multiplication par tout élément de A : pour tout $x \in I$, pour tout $a \in A$, $ax \in I$.

On a déjà rencontré cette notion dans deux cas :

- Pour $A = \mathbb{Z}$, tout sous-groupe I de $\mathbb{Z}$ est automatiquement un idéal de $\mathbb{Z}$: pour tout $x \in I$ et pour tout $k \in \mathbb{Z}$, $kx \in I$. La notion d'idéal se confond donc (dans ce cas particulier) avec la notion de sous-groupe.
- Pour $A = K[X]$ avec K un corps, on a vu la notion d'idéal dans la section précédente.

Exemple 4.8.2. Exemples triviaux : $\{0\}$ et A sont des idéaux de A.

Remarque 4.8.3. Ne surtout pas confondre la notion d'idéal et la notion de sous-anneau, qui sont différentes et qui jouent des rôles très différents dans la théorie des anneaux. En général, un idéal I ne contient pas 1_A.

Exercice 79. Soit I un idéal de A. Montrer que $1_A \in I$ si et seulement si $I = A$.

4.8.2 Idéal engendré par des éléments

La proposition suivante montre qu'il est facile de construire des idéaux.

Proposition 4.8.4. *Soient $x_1, \dots, x_r \in A$. Alors l'ensemble*

$$(x_1, \dots, x_r) = \{a_1 x_1 + \cdots + a_r x_r,\ a_1, \dots, a_r \in A\}$$

est un idéal de A. Pour tout idéal I de A on a

$$x_1, \dots, x_r \in I \iff (x_1, \dots, x_r) \subset I.$$

Définition 4.8.5. *On appelle $(x_1, \dots, x_r)$ l'***idéal de A engendré par** $x_1, \dots, x_r$.

Démonstration. On montre que $(x_1, \dots, x_r)$ est un idéal de A.

- $0 \in I$ car $0 = 0x_1 + \cdots + 0x_r$.
- I est stable par $+$: pour $a_1, \dots, a_r, a'_1, \dots, a'_r \in A$ on a

$$(a_1 x_1 + \cdots + a_r x_r) + (a'_1 x_1 + \cdots + a'_r x_r) = (a_1 + a'_1)x_1 + \cdots + (a_r + a'_r)x_r \in I\ .$$

▷ I est stable par $-$: pour $a_1, \dots, a_r \in A$ on a

$$-(a_1x_1 + \cdots + a_rx_r) = (-a_1)x_1 + \cdots + (-a_r)x_r \in I \ .$$

▷ I est stable par multiplication par tout élément de A : pour $a_1, \dots, a_r \in A$ et $a \in A$ on a

$$a(a_1x_1 + \cdots + a_rx_r) = (aa_1)x_1 + \cdots + (aa_r)x_r \ .$$

Cela montre que $(x_1, \dots, x_r)$ est un idéal de A. Clairement, $x_1, \dots, x_r \in (x_1, \dots, x_r)$, ce qui montre la direction $\Longleftarrow$ de l'équivalence. Pour la direction $\Longrightarrow$, soit I un idéal de A qui contient $x_1, \dots, x_r$, alors pour tout $a_1, \dots, a_r \in A$ on a, comme I est un idéal de A : $a_ix_i \in I$, et la somme $a_1x_1 + \cdots + a_rx_r$ doit donc aussi être dans I. Donc $(x_1, \dots, x_r) \subset I$. □

4.8.3 Idéaux et morphismes

Proposition 4.8.6. *Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors $\ker(f)$ est un idéal de A.*

Démonstration. On sait déjà que $\ker(f)$ est un sous-groupe abélien de A. Pour $x \in \ker(f)$ et $a \in A$ on a $f(ax) = f(a)f(x) = 0$ car $f(x) = 0$, et donc $ax \in \ker(f)$. □

La dernière proposition se généralise :

Proposition 4.8.7. *Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.*

▷ Pour $J = \{0\}$ on retrouve le fait que $f^{-1}(\{0\}) = \ker(f)$ est un idéal de A.

Démonstration. On sait déjà que $f^{-1}(J)$ est un sous-groupe de A. Pour $x \in f^{-1}(J)$ et $a \in A$ on a $f(ax) = f(a)f(x) \in J$ car $f(x) \in J$ et J est un idéal de B. Donc $ax \in f^{-1}(J)$. □

Exercice 80. Montrer qu'en général l'image **directe** d'un idéal par un morphisme d'anneaux n'est pas un idéal.

4.8.4 Idéaux principaux, anneaux principaux

Le cas particulier des idéaux engendrés par un seul élément $x \in A$ est important :

$$(x) = \{ax,\ a \in A\}.$$

Définition 4.8.8. *Un idéal (x) engendré par un seul élément est dit* **principal**.

On a rencontré les idéaux principaux dans deux cas :

▷ Pour $A = \mathbb{Z}$ et $n \in \mathbb{Z}$ on a $(n) = n\mathbb{Z}$.

▷ Pour $A = K[X]$ avec K un corps, on a rencontré les idéaux principaux (f) dans la section précédente.

Dans les deux cas les idéaux principaux nous ont aidé à développer les notions de PGCD et de PPCM, et donc toute l'arithmétique.

Définition 4.8.9. *Soit A un anneau. On dit que A est* **principal** *si A est intègre et que tout idéal de A est principal.*

▷ Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps, sont principaux.

▷ On verra en TD que les anneaux $\mathbb{Z}[X]$ et $K[X,Y]$, pour K un corps, ne sont pas principaux.

4.8.5 Anneaux euclidiens

Un anneau euclidien est un anneau intègre où il y a "une notion de division euclidienne".

Définition 4.8.10. *Soit A un anneau intègre. Une* **jauge euclidienne** *est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ qui vérifie : pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ avec*

$$a = bq + r \quad \text{et} \quad (r = 0 \ \text{ ou } \ \nu(r) < \nu(b)) \ .$$

On appelle une telle identité une **division euclidienne** *de a par b pour la jauge euclidienne ν. On dit que A est un* **anneau euclidien** *s'il possède une jauge euclidienne.*

▷ Notons qu'on ne demande pas d'avoir unicité de la division euclidienne.

Exemple 4.8.11. – L'anneau $\mathbb{Z}$ est euclidien, une jauge euclidienne est donnée par la valeur absolue : $\nu(m) = |m|$. (On pourra remarquer que pour cette jauge euclidienne, il n'y a pas unicité de la division euclidienne.)

– L'anneau $K[X]$ est euclidien si K est un corps, une jauge euclidienne est donnée par le degré : $\nu(f) = \deg(f)$.

La proposition suivante est la version "abstraite" de deux énoncés importants qu'on a vus dans ce cours :

▷ $\mathbb{Z}$ est un anneau principal : tous les idéaux de $\mathbb{Z}$ sont de la forme (n). (C'est-à-dire : tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.)

▷ Pour K un corps, $K[X]$ est principal : tous les idéaux de $K[X]$ sont de la forme (f).

C'est l'outil numéro un pour montrer qu'un anneau est principal.

Théorème 4.8.12. *Tout anneau euclidien est principal.*

Démonstration. Soit $I \subset A$ un idéal. Si $I = \{0\}$ alors $I = (0)$ est principal. Sinon I contient des éléments non nuls, et on choisit un élément $x \in I \setminus \{0\}$ tel que $\nu(x)$ est minimal, ce qui est possible car ν prend ses valeurs dans $\mathbb{N}$. On a donc : pour tout $y \in I \setminus \{0\}$, $\nu(y) \geqslant \nu(x)$. Comme $x \in I$, on a l'inclusion $(x) \subset I$ et on veut montrer l'inclusion réciproque. Soit $y \in I$, on a une division euclidienne $y = xq + r$, avec $r = 0$ ou $\nu(r) < \nu(x)$. Comme I est un idéal on a que $r = y - xq \in I$, et donc $r = 0$ par minimalité de $\nu(x)$. Ainsi, on a $y = xq \in (x)$. On a donc montré qu'on a $I = (x)$. Donc tout idéal de A est principal et A est un anneau principal. □

Remarque 4.8.13. Il existe des anneaux principaux qui ne sont pas euclidiens, mais ce n'est pas si facile à prouver en pratique. On n'en verra pas en exercice. Pour votre culture, un exemple d'un tel anneau est le sous-anneau de $\mathbb{C}$ donné par

$$A = \left\{ a + b\frac{1+i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\} .$$

(Vérifiez que c'est bien un sous-anneau de $\mathbb{C}$: il y a un petit calcul à faire.)

Remarque 4.8.14. Les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, ne sont pas principaux (voir TD). Ils ne sont donc pas euclidiens.

4.9 Arithmétique dans un anneau principal

4.9.1 Divisibilité dans un anneau intègre

Soit A un anneau intègre (et donc notamment commutatif).

Définition 4.9.1. *Soient $a, b \in A$. On dit que a* **divise** *b et on écrit*

$$a|b$$

s'il existe $c \in A$ tel que $b = ac$. On dit aussi que a est un **diviseur** *de b, ou que b est* **divisible** *par a ou est un* **multiple** *de a.*

Proposition 4.9.2. *On a :*

$$a|b \iff b \in (a) \iff (b) \subset (a) \ .$$

La relation de divisibilité est réflexive et transitive : on a pour tout $a \in A$, $a|a$, et pour tout $a, b, c \in A$, $a|b$ et $b|c$ impliquent $a|c$.

Démonstration. La première équivalence est évidente. Clairement, si $(b) \subset (a)$ alors $b \in (a)$. Si $b = ax$ avec $x \in A$ alors tout élément de (b) s'écrit $by = axy$ avec $y \in A$, donc est dans (a), et $(b) \subset (a)$. Comme $a|b$ équivaut à $(b) \subset (a)$, la relation de divisibilité est évidemment réflexive et transitive. □

Définition 4.9.3. *Soient $a, b \in A$. On dit que a et b sont* **associés** *s'il existe un inversible $u \in A^\times$ tel que $b = au$.*

Proposition 4.9.4. *Soient $a, b \in A$. On a :*

$$a \text{ et } b \text{ associés} \iff a|b \text{ et } b|a \iff (a) = (b) \ .$$

De plus, la relation d'association ("être associés") est une relation d'équivalence sur A.

Démonstration. Si a et b sont associés alors on peut écrire $b = au$ avec u inversible, et donc $a = u^{-1}b$, d'où $a|b$ et $b|a$. Réciproquement, si $a|b$ et $b|a$ alors on peut écrire $b = ax$ et $a = by$ et donc $a = axy$ d'où $a(1 - xy) = 0$. On a deux cas : si $a = 0$ alors $b = 0$ et donc a et b sont associés. Sinon, comme A est intègre on a $1 - xy = 0$ et donc $xy = 1$, donc x est inversible et donc a et b sont associés. Cela prouve la première équivalence. La deuxième est une conséquence de la proposition précédente. Enfin, comme "a et b associés" équivaut à $(a) = (b)$, il est clair que la relation d'association est une relation d'équivalence. □

Remarque 4.9.5. La relation de divisibilité n'est pas une relation d'ordre en général puisqu'elle n'est pas antisymétrique : $a|b$ et $b|a$ n'impliquent pas $a = b$ en général mais seulement a et b associés. Un meilleur point de vue est de considérer l'ensemble des idéaux de A ordonnés par l'inclusion (qui est une vraie relation d'ordre).

Définition 4.9.6. *On dit qu'un élément $x \in A$ non nul est* **irréductible** *si x n'est pas inversible et qu'on ne peut pas écrire $x = ab$ avec a et b non inversibles.*

Exemple 4.9.7. – Dans $A = \mathbb{Z}$ on retrouve la notion habituelle de divisibilité. Comme $\mathbb{Z}^\times = \{1, -1\}$, deux entiers m et n sont associés si et seulement si $m = \pm n$. Les éléments irréductibles sont les nombres premiers p et leurs opposés $-p$.

– Dans $A = K[X]$ pour K un corps, on retrouve la notion habituelle de divisibilité. Comme $K[X]^\times = K^\times$, deux polynômes f et g sont associés si et seulement si on peut écrire $f = \lambda g$ avec $\lambda \in K^\times$. Les éléments irréductibles sont les polynômes irréductibles.

Exercice 81. Dans un corps, quels éléments sont irréductibles ?

4.9.2 PGCD et PPCM dans un anneau principal

Dans le reste de cette section, A désigne un anneau **principal** (donc notamment intègre).

PGCD

Définition 4.9.8. *Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $d \in A$ est* **un PGCD** *de a et b si $(a, b) = (d)$.*

▷ Deux éléments a et b ont toujours un PGCD puisque A est principal.

▷ En général on ne peut pas dire **le** PGCD puisque $(d) = (d')$ si et seulement si d et d' sont associés.

▷ Dans les cas $A = \mathbb{Z}$ et $A = K[X]$, pour K un corps, on a fait des choix qui rendaient le PGCD unique : pour $A = \mathbb{Z}$ on demandait que $d \geqslant 0$, et pour $A = K[X]$ on demandait que d soit unitaire.

▷ Cela étant, on fait parfois un abus de langage et on dit quand même **le** PGCD, qu'on note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$, même si un tel élément est seulement défini **à association près**.

Proposition 4.9.9. *Soient $a, b \in A$. Alors $a \wedge b$ est l'unique (à association près) $d \in A$ qui vérifie les deux conditions suivantes.*

1) $d|a$ et $d|b$;

2) pour tout $e \in A$, $(e|a \text{ et } e|b) \Longrightarrow e|d$.

Démonstration. Laissé au lecteur. □

Proposition 4.9.10. *Soient $a, b, c \in A$. Alors à association près on a :*

$$(a + bc) \wedge b = a \wedge b.$$

Démonstration. Cela revient à montrer l'égalité des idéaux :

$$(a + bc, b) = (a, b).$$

▷ Soit $x \in (a + bc, b)$. Alors il existe $u, v \in A$ tels que $x = u(a + bc) + vb = ua + (uc + v)b$. Comme $u, uc + v \in A$, on a donc que $x \in (a, b)$.

▷ Soit $x \in (a, b)$. Alors il existe $u, v \in A$ tels que $x = ua + vb = u(a + bc - bc) + vb = u(a + bc) + (-uc + v)b$. Comme $u, -uc + v \in A$, on a donc que $x \in (a + bc, b)$.

□

▷ Dans le cas où A est un anneau euclidien, cette proposition implique qu'on peut calculer $a \wedge b$ grâce à l'**algorithme d'Euclide**.

PPCM

Proposition 4.9.11. *Soient $a, b \in A$. L'ensemble $(a) \cap (b)$ est un idéal de A.*

Démonstration. Laissé au lecteur. □

On note que $(a) \cap (b)$ est l'ensemble des éléments de A qui sont à la fois des multiples de a et de b.

Remarque 4.9.12. Plus généralement, on montre facilement que l'intersection de deux idéaux d'un anneau commutatif est un idéal.

Définition 4.9.13. *Soit A un anneau principal et soient $a, b \in A$. On dit qu'un élément $m \in A$ est* **un PPCM** *de a et b si $(a) \cap (b) = (m)$.*

▷ Deux éléments a et b ont toujours un PPCM puisque A est principal et que $(a) \cap (b)$ est un idéal de A.

▷ En général on ne peut pas dire **le PPCM** puisque $(m) = (m')$ si et seulement si m et m' sont associés.

▷ Dans les cas $A = \mathbb{Z}$ et $A = K[X]$, pour K un corps, on a fait des choix qui rendaient le PPCM unique.

▷ Cela étant, on fait parfois un abus de langage et on dit quand même **le PPCM**, qu'on note $\mathrm{PPCM}(a, b)$ ou $a \vee b$, même si un tel élément est seulement défini **à association près**.

Proposition 4.9.14. *Soient $a, b \in A$. Alors $a \vee b$ est l'unique (à association près) $m \in A$ qui vérifie les deux conditions suivantes.*

1) $a|m$ et $b|m$;

2) pour tout $n \in A$, $(a|n$ et $b|n) \Longrightarrow m|n$.

Démonstration. Laissé au lecteur. □

4.9.3 Gauss, Euclide, Bézout

On laisse au lecteur le soin de démontrer, en copiant les preuves du chapitre 1, que dans un anneau principal A ou a les théorèmes classiques suivants :

– le lemme de Gauss (et sa variante) ;

– le lemme d'Euclide ;

– le théorème de Bézout ;

Le théorème de factorisation en produit d'éléments irréductibles est aussi vrai, mais un peu plus subtil, comme on va le voir maintenant.

4.9.4 Factorisation en produit d'éléments irréductibles

Définition 4.9.15. *Soit A un anneau intègre. On dit que A est un anneau* **factoriel** *s'il y a existence et unicité de la décomposition en produit d'irréductibles dans A, c'est-à-dire plus précisément si :*

(1) pour tout $a \in A \setminus \{0\}$ il existe un nombre fini $x_1, \dots, x_r$ d'éléments irréductibles de A et un inversible $u \in A^\times$ tels que $a = u\, x_1 \cdots x_r$;

(2) si pour $a \in A \setminus \{0\}$ on a des écritures $a = u\, x_1 \cdots x_r$ et $a = v\, y_1 \cdots y_s$ avec les x_i, y_j irréductibles et u, v inversibles alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ et des éléments inversibles $u_i \in A^\times$ tels que $y_i = u_i x_{\sigma(i)}$ pour tout $i = 1, \dots, r$.

On veut montrer le théorème suivant.

Théorème 4.9.16. *Tout anneau principal est factoriel.*

On laisse le soin au lecteur de prouver la partie (2) de la définition en utilisant le lemme d'Euclide, comme dans le cas de $\mathbb{Z}$ et de $K[X]$. La partie subtile concerne la partie (1), c'est-à-dire l'**existence** de la factorisation en produit d'éléments irréductibles dans un anneau principal A. C'est le théorème 4.9.18, qui suit une proposition importante.

Proposition 4.9.17. *Soit A un anneau principal. Soit $(I_n)_{n\in\mathbb{N}}$ une suite d'idéaux de A tels que $I_n \subset I_{n+1}$ pour tout n. Alors cette suite est stationnaire : il existe un $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $I_n = I_N$.*

Démonstration. Posons $I = \bigcup_{n\geqslant 0} I_n$. On montre que I est un idéal de A.

▷ $0 \in I$ car $0 \in I_0$.

▷ I est stable par $+$: pour $x, y \in I$ il existe $m, n \in \mathbb{N}$ tels que $x \in I_m$ et $y \in I_n$, et on peut supposer $m \leqslant n$, et donc $x \in I_n$ car $I_m \subset I_n$. Comme I_n est stable par $+$ on a $x + y \in I_n$ donc $x + y \in I$.

▷ I est stable par $-$: pour $x \in I$ il existe $n \in \mathbb{N}$ tel que $x \in I_n$. Comme I_n est stable par $-$ on a $-x \in I_n$ et donc $-x \in I$.

▷ I est stable par multiplication par tout élément de A : soit $x \in I$ et $a \in A$. Alors il existe $n \in \mathbb{N}$ tel que $x \in I_n$. Comme I_n est stable par multiplication par a, on a $ax \in I_n$ donc $ax \in I$.

On a donc montré que I est un idéal de A (remarquez qu'on n'a pas utilisé le fait que A est principal). Comme A est principal on peut écrire $I = (x)$ avec un $x \in A$. Comme $x \in I$, il existe un $N \in \mathbb{N}$ tel que $x \in I_N$, donc $I = (x) \subset I_N$. Pour tout $n \geqslant N$ on a alors $I_N \subset I_n \subset I \subset I_N$ et donc $I_n = I_N = I$. □

▷ Cette condition dit qu'il ne peut pas y avoir de suite strictement croissante d'idéaux de A. Cette condition s'appelle la **condition de chaîne ascendante** et un anneau qui satisfait cette propriété est appelé **noethérien**[1]. On vient donc de montrer que tout anneau principal est noethérien. Un exemple d'un anneau non noethérien : un anneau de polynômes sur une infinité de variables $K[X_1, X_2, X_3, \ldots]$: la suite d'idéaux $I_n = (X_1, \ldots, X_n)$ est strictement croissante.

Théorème 4.9.18. *Soit A un anneau principal. Alors pour tout élément $a \in A \setminus \{0\}$ il existe un nombre fini $x_1, \ldots, x_r$ d'éléments irréductibles de A et un inversible $u \in A^\times$ tels que $a = u\, x_1 \cdots x_r$.*

Démonstration. Soit A un anneau principal. Soit $a \in A$, non nul et non inversible. On procède en deux étapes.

▷ On montre que a est divisible par un élément irréductible. Si a est irréductible alors on a gagné. Sinon on peut écrire $a = x_1 a_1$ avec x_1 et a_1 non inversibles. On a alors une inclusion stricte $(a) \subsetneq (a_1)$. On continue avec a_1 : s'il est irréductible alors on a gagné, sinon on peut écrire $a_1 = x_2 a_2$ avec x_2 et a_2 non inversibles. On a alors une inclusion stricte $(a_1) \subsetneq (a_2)$, et on continue avec a_2, etc. Par la proposition 4.9.17 ce processus ne peut pas continuer indéfiniment, et on arrive après un nombre fini d'étapes à un diviseur irréductible a_N de a.

▷ On montre que a est associé à un produit d'éléments irréductibles. Si a est irréductible alors on a gagné. Sinon, par l'étape précédente on peut écrire $a = x_1 a_1$ avec x_1 irréductible et a_1 non inversible. On a alors $(a) \subsetneq (a_1)$. Si a_1 est irréductible on a gagné, sinon on applique la première étape à a_1 qu'on écrit alors $a_1 = x_2 a_2$ avec x_2 irréductible et a_2 non inversible. On a alors $(a_1) \subsetneq (a_2)$ et on continue avec a_2, etc. Par la proposition 4.9.17, ce processus ne peut pas continuer indéfiniment, et on arrive après un nombre fini d'étapes à un a_N irréductible. On a alors $a = x_1 \cdots x_N a_N$ produit d'irréductibles.

□

Remarque 4.9.19. La réciproque du théorème 4.9.16 est fausse, comme on va le voir dans le prochain paragraphe. En effet, on verra que les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, sont factoriels, alors qu'il ne sont pas principaux (voir TD). Pour résumer, on a donc les implications suivantes, qui ne sont pas des équivalences :

$$\text{euclidien} \implies \text{principal} \implies \text{factoriel}.$$

[1] Nommé en l'honneur de la mathématicienne allemande Emmy Noether (1882-1935).

4.10 Arithmétique dans un anneau factoriel

Dans toute cette section A désigne un anneau **factoriel** (et donc notamment intègre).

4.10.1 PGCD et PPCM

Soit A un anneau factoriel. Dans ce paragraphe on fait un choix, pour simplifier les notations, d'un élément irréductible p_i dans chaque classe d'association, pour i dans un certain ensemble d'indices $\mathcal{I}$. Un élément $a \neq 0$ dans A a donc une écriture **unique** sous la forme

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i}$$

avec u inversible et les $m_i \in \mathbb{N}$ presque tous nuls (tous nuls sauf un nombre fini).

Proposition 4.10.1. *Soient deux éléments $a, a' \in A \setminus \{0\}$ écrits comme ci-dessus*

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i} \quad \text{et} \quad a' = u' \prod_{i \in \mathcal{I}} p_i^{m'_i}.$$

Alors on a :

$$a | a' \iff \forall i \in \mathcal{I},\ m_i \leqslant m'_i.$$

Démonstration. 1) $\Longleftarrow$. Si $m_i \leqslant m'_i$ pour tout $i \in \mathcal{I}$, on peut définir l'élément

$$b = u^{-1} u' \prod_{i \in \mathcal{I}} p_i^{m'_i - m_i} \in A$$

et on a $a' = ab$, d'où $a | a'$.

2) $\Longrightarrow$. Si $a | a'$ alors il existe $b \in A \setminus \{0\}$ tel que $a' = ab$. Écrivons b comme produit de nombres premiers sous la forme

$$b = v \prod_{i \in \mathcal{I}} p_i^{n_i},$$

où les n_i sont des entiers naturels presque tous nuls. L'égalité $a' = ab$ s'écrit alors

$$u' \prod_{i \in \mathcal{I}} p_i^{m'_i} = uv \prod_{i \in \mathcal{I}} p_i^{m_i + n_i}.$$

Par unicité de la décomposition en produits de nombres premiers on a $u' = uv$ et $m'_i = m_i + n_i$ pour tout $i \in \mathcal{I}$, et donc $m_i \leqslant m'_i$.

□

Soient $a, b \in A$ non nuls, écrits sous la forme ci-dessus,

$$a = u \prod_{i \in \mathcal{I}} p_i^{m_i} \quad \text{et} \quad b = v \prod_{i \in \mathcal{I}} p_i^{n_i}.$$

Définition 4.10.2. *On définit le* **PGCD** *de a et b, noté* $\mathrm{PGCD}(a, b)$ *ou $a \wedge b$, par la formule*

$$a \wedge b = \prod_{i \in \mathcal{I}} p_i^{\min(m_i, n_i)}.$$

On définit le **PPCM** *de a et b, noté* $\mathrm{PPCM}(a,b)$ *ou* $a \vee b$, *par la formule*

$$a \vee b = \prod_{i \in \mathcal{I}} p_i^{\max(m_i,n_i)} \ .$$

On a la propriété usuelle du PGCD :

Proposition 4.10.3. *Soient $a, b \in A \setminus \{0\}$. Alors $a \wedge b$ est l'unique (à association près) $x \in A$ qui vérifie les deux conditions suivantes.*

1) $x|a$ et $x|b$;

2) pour tout $y \in A$, $(y|a$ et $y|b) \Longrightarrow y|x$.

Démonstration. Par la proposition 4.10.1, un élément $x = w \prod_{i \in \mathcal{I}} p_i^{r_i}$ est un diviseur commun de a et b si et seulement si $r_i \leqslant m_i$ et $r_i \leqslant n_i$ pour tout $i \in \mathcal{I}$, c'est-dire : $r_i \leqslant \min(m_i, n_i)$. On voit donc que $a \wedge b$ vérifie les conditions (1) et (2). □

On a la propriété usuelle du PPCM :

Proposition 4.10.4. *Soient $a, b \in A \setminus \{0\}$. Alors $a \vee b$ est l'unique (à association près) $x \in A$ qui vérifie les deux conditions suivantes.*

1) $a|x$ et $b|x$;

2) pour tout $y \in A$, $(a|y$ et $b|y) \Longrightarrow x|y$.

Démonstration. Laissé au lecteur. □

On a aussi facilement le lien entre PGCD et PPCM :

Proposition 4.10.5. *Les produits*

$$ab \quad \text{et} \quad (a \wedge b)(a \vee b)$$

sont associés dans A.

Démonstration. On a :

$$(a \wedge b)(a \vee b) = uv \prod_{i \in \mathcal{I}} p_i^{\min(m_i,n_i)+\max(m_i,n_i)} = uv \prod_{i \in \mathcal{I}} p_i^{m_i+n_i} = uvab.$$

□

Définition 4.10.6. *On dit que a et b sont* **premiers entre eux** *si $a \wedge b = 1$.*

▷ Cela revient à dire qu'il n'y a aucun élément irréductible qui divise à la fois a et b. C'est aussi équivalent à dire que les seuls diviseurs communs à a et b sont les éléments inversibles de A.

Remarque 4.10.7. Il y a tout de même un résultat très utile en arithmétique qui est vrai dans un anneau principal mais pas dans tout anneau factoriel : le théorème de Bézout !

4.10.2 Hérédité de la factorialité

Le but de ce paragraphe est de démontrer le théorème suivant.

Théorème 4.10.8. *Soit A un anneau factoriel. Alors l'anneau $A[X]$ est factoriel.*

Corollaire 4.10.9. *Soit A un anneau factoriel (par exemple $A = \mathbb{Z}$ ou $A = K$ un corps). Alors pour tout entier n, l'anneau $A[X_1, \dots, X_n]$ est factoriel.*

Démonstration. Par récurrence sur n grâce à : $A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$. □

Remarque 4.10.10. Les anneaux $\mathbb{Z}[X]$ et $K[X, Y]$, pour K un corps, ne sont pas principaux (voir TD). Ce sont donc des exemples d'anneaux factoriels non principaux.

▷ Pour plus de clarté, on va seulement prouver le théorème dans le cas $A = \mathbb{Z}$, mais on conseille au lecteur de se convaincre que la même preuve fonctionne plus généralement pour n'importe quel anneau factoriel.

▷ On rappelle les inversibles de $\mathbb{Z}[X]$:

$$\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{-1, 1\}.$$

Définition 4.10.11. *Le* **contenu** *d'un polynôme $f = \sum_{n=0}^{N} a_n X^n \in \mathbb{Z}[X]$ est le PGCD des coefficients a_n. On le note $c(f)$. On dit que f est* **primitif** *si $c(f) = 1$, c'est-à-dire si les coefficients de f sont premiers entre eux dans leur ensemble.*

Exercice 82. 1) Montrer qu'on peut écrire $f = c(f)f_1$ avec $f_1 \in \mathbb{Z}[X]$ primitif.

2) Réciproquement, si on a $f = \lambda f_1$ avec $\lambda \in \mathbb{N}$ et $f_1 \in \mathbb{Z}[X]$ primitif, montrer que $c(f) = \lambda$.

Cette fois c'est l'existence de la décomposition en produit d'irréductibles qui est la plus facile :

Proposition 4.10.12. *Tout $f \in \mathbb{Z}[X] \setminus \{0\}$ peut s'écrire (au signe près) comme un produit d'irréductibles de $\mathbb{Z}[X]$.*

Démonstration. On commence par traiter le cas des polynômes primitifs, par récurrence sur le degré.

– Pour tout $n \in \mathbb{N}^*$ considérons l'assertion $P(n)$: "tout $f \in \mathbb{Z}[X]$ primitif de degré n peut s'écrire (au signe près) un produit d'irréductibles de $\mathbb{Z}[X]$".

– Initialisation. Si $\deg(f) = 0$ alors $f = \pm 1$ et il n'y a rien à prouver, donc $P(0)$ est vraie.

– Hérédité. Soit $n \in \mathbb{N}^*$ tel que $P(n)$ est vraie pour tout $k < n$, et montrons $P(n)$. Soit $f \in \mathbb{Z}[X]$ un polynôme primitif de degré n. Si f est irréductible alors on a gagné ; sinon par définition on peut écrire $f = gh$ avec g et h non inversibles dans $\mathbb{Z}[X]$. Comme f est primitif, g et h le sont aussi (En effet, si par exemple g ne l'était pas, alors le contenu

$c(g) \geqslant 2$ serait en facteur dans g et donc dans f). Si g ou h est constant alors il est égal à ± 1 donc inversible, ce qui est absurde ; donc g et h sont non constants, donc de degrés > 0. On en déduit que $\deg(g) < n$ et $\deg(h) < n$ et donc par l'hypothèse de récurrence, g et h peuvent être écrits (au signe près) comme produits d'irréductibles de $\mathbb{Z}[X]$. C'est donc aussi le cas pour f et on a gagné.

– Conclusion : on a montré que $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Pour un $f \in \mathbb{Z}[X] \setminus \{0\}$ général, on écrit $f = c(f)f_1$ avec f_1 primitif. Par ce qu'on vient de voir, on peut décomposer f_1 en produit d'irréductibles. Or, $c(f_1) \in \mathbb{N}^*$ peut être décomposé en produit de nombre premiers, qui sont des irréductibles de $\mathbb{Z}[X]$, et donc on a gagné. □

On passe maintenant à l'unicité de la décomposition en produit d'irréductibles dans $\mathbb{Z}[X]$.

▷ Avant de continuer, une remarque sera utile. Pour un polynôme

$$f = \sum_{n=0}^{N} a_n X^n \ \in \mathbb{Z}[X]$$

et pour un nombre premier fixé p, on peut réduire tous les coefficients de f modulo p et obtenir un polynôme

$$\overline{f} = \sum_{n=0}^{N} \overline{a_n} X^n \ \in (\mathbb{Z}/p\mathbb{Z})[X]$$

à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 83. Montrer que cette opération définit un morphisme d'anneaux

$$\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X] \ , \quad f \mapsto \overline{f} \ .$$

Montrer que ce morphisme est surjectif et décrire son noyau.

La proposition suivante s'appelle "lemme de Gauss", mais n'a pas vraiment de rapport avec l'autre lemme de Gauss de ce cours (théorème 1.4.1).

Proposition 4.10.13 (Lemme de Gauss). *Pour $f, g \in \mathbb{Z}[X]$ on a*

$$c(fg) = c(f)c(g) \ .$$

En particulier, le produit de deux polynômes primitifs est primitif.

Démonstration. On écrit $f = c(f)f_1$ et $g = c(g)g_1$ avec $f_1, g_1 \in \mathbb{Z}[X]$ primitifs. On a alors $fg = c(f)c(g)f_1g_1$ et il suffit de montrer que f_1g_1 est primitif. S'il ne l'est pas alors il existe un nombre premier $p \in \mathbb{Z}$ tel que p divise tous les coefficients de f_1g_1. En réduisant modulo p on obtient donc : $\overline{f_1}\,\overline{g_1} = \overline{f_1 g_1} = \overline{0}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Or, p étant premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre et donc $(\mathbb{Z}/p\mathbb{Z})[X]$ aussi. Ainsi on a $\overline{f_1} = 0$ ou $\overline{g_1} = \overline{0}$. Dans le premier cas, p divise tous les coefficients de f_1, et donc f_1 n'est pas primitif, ce qui est absurde. Dans le deuxième cas, c'est la même chose avec g_1. On a donc trouvé une contradiction, ce qui montre que f_1g_1 est primitif et que $c(fg) = c(f)c(g)$. □

Proposition 4.10.14. *Un polynôme non constant $f \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est primitif et irréductible dans $\mathbb{Q}[X]$.*

Remarque 4.10.15. Dans le cas d'un anneau factoriel A quelconque, le corps $\mathbb{Q}$ doit être remplacé par le corps des fractions $\mathrm{Frac}(A)$.

Démonstration. – Supposons que f est primitif et irréductible dans $\mathbb{Q}[X]$. Supposons $f = gh$ avec $g, h \in \mathbb{Z}[X]$. Comme f est irréductible dans $\mathbb{Q}[X]$ on a nécessairement que g ou h est inversible dans $\mathbb{Q}[X]$. On peut donc supposer que $g = \lambda \in \mathbb{Q}^\times$ et donc $\lambda \in \mathbb{Z} \setminus \{0\}$ puisque g a coefficients entiers. On a alors $f = \lambda h$ et comme f est primitif on a nécessairement $\lambda = \pm 1$. Résultat : g est inversible dans $\mathbb{Z}[X]$. On a donc montré que f est irréductible dans $\mathbb{Z}[X]$.

– Si f n'est pas primitif alors $c(f) \geqslant 2$ et on peut écrire $f = c(f) f_1$ avec f_1 primitif. Ainsi $c(f)$ n'est pas inversible dans $\mathbb{Z}[X]$, et f_1 non plus car f_1 est non constant. Donc f n'est pas irréductible.

Si f n'est pas irréductible dans $\mathbb{Q}[X]$ alors on peut écrire $f = gh$ avec $g, h \in \mathbb{Q}[X]$ non constants. On peut écrire $g = \frac{1}{u} g_1$ et $h = \frac{1}{v} h_1$ avec $g_1, h_1 \in \mathbb{Z}[X]$ non constants et $u, v \in \mathbb{N}^*$. On a donc l'égalité dans $\mathbb{Z}[X]$: $uv\, f = g_1 h_1$. En prenant les contenus et en utilisant le lemme de Gauss on obtient $uv\, c(f) = c(g_1)c(h_1)$. On a alors :

$$f = gh = \frac{1}{uv} g_1 h_1 = \frac{c(f)}{c(g_1)c(h_1)} g_1 h_1 = c(f) \frac{g_1}{c(g_1)} \frac{h_1}{c(h_1)} \cdot$$

Comme $\frac{g_1}{c(g_1)}$ et $\frac{h_1}{c(h_1)}$ sont dans $\mathbb{Z}[X]$ et non constants, f n'est pas irréductible dans $\mathbb{Z}[X]$.

□

Remarque 4.10.16. La partie "non triviale" de la proposition pécédente est l'implication (irréductible dans $\mathbb{Z}[X]$) $\Longrightarrow$ (irréductible dans $\mathbb{Q}[X]$). En pratique, c'est cette implication qui est utile. En effet, il est (de manière peut-être surprenante) plus facile de montrer qu'un polynôme à coefficients **entiers** est irréductible, notamment parce qu'on peut alors réduire les coefficients modulo un nombre premier p bien choisi.

Corollaire 4.10.17. *Les irréductibles de $\mathbb{Z}[X]$ sont les nombres premiers (et leurs opposés) et les polynômes primitifs qui sont irréductibles dans $\mathbb{Q}[X]$.*

Cette classification des irréductibles nous permet de montrer le lemme d'Euclide pour $\mathbb{Z}[X]$.

Proposition 4.10.18 (Lemme d'Euclide pour les polynômes à coefficients dans $\mathbb{Z}$). *Soient $f, g \in \mathbb{Z}[X]$, et soit $h \in \mathbb{Z}[X]$ un irréductible. Si $h | fg$ alors $h | f$ ou $h | g$.*

Démonstration. D'après le corollaire 4.10.17 il y a deux cas à considérer.

1) Soit $h = p$ un nombre premier et supposons que $p | fg$ dans $\mathbb{Z}[X]$. Alors p divise tous les coefficients de fg, donc p divise $c(fg) = c(f)c(g)$ par le lemme de Gauss, et donc (par le lemme d'Euclide pour $\mathbb{Z}$), $p | c(f)$ ou $p | c(g)$. Donc p divise f ou g.

2) Soit $h \in \mathbb{Z}[X]$ un polynôme primitif et irréductible dans $\mathbb{Q}[X]$, et soient $f, g \in \mathbb{Z}[X]$ tels que $h|fg$ dans $\mathbb{Z}[X]$. Alors $h|fg$ dans $\mathbb{Q}[X]$, et donc $h|f$ ou $h|g$ dans $\mathbb{Q}[X]$ par le lemme d'Euclide dans $\mathbb{Q}[X]$. On peut supposer que h divise f et écrire $f = hk$ avec $k \in \mathbb{Q}[X]$. On peut écrire $k = \frac{1}{u}k_1$ avec $u \in \mathbb{N}^*$ et $k_1 \in \mathbb{Z}[X]$. On a alors $uf = hk_1$ et en prenant les contenus et en utilisant le lemme de Gauss on obtient : $u\,c(f) = c(h)\,c(k_1) = c(k_1)$ car h est primitif. On a donc $\frac{1}{u} = \frac{c(f)}{c(k_1)}$ et on peut alors écrire $f = c(f)\,h\frac{k_1}{c(k_1)}$. Comme $\frac{k_1}{c(k_1)}$ a des coefficients entiers, on voit donc que h divise f dans $\mathbb{Z}[X]$.

□

On peut maintenant montrer l'unicité de la décomposition en produit d'irréductibles.

Proposition 4.10.19. *Dans $\mathbb{Z}[X]$ la décomposition en produit d'irréductibles est unique au signe près et à l'ordre des facteurs près.*

Démonstration. En utilisant le lemme d'Euclide (proposition 4.10.18) comme dans le cas de $\mathbb{Z}$ (voir la preuve du théorème 1.4.7). □

On a fini : on a montré que $\mathbb{Z}[X]$ est un anneau factoriel.