Algèbre 2

Andrei Teleman

Département de Mathématiques, Aix-Marseille Université

22 mars 2021

Table des matières

1 Divisibilité dans $\mathbb{Z}$. Équations diophantiennes affines

1.1 Le théorème de division euclidienne

Nous commençons par

Théorème 1.1.1 *(le théorème de division euclidienne) Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}$. Il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ telle que $n = mq + r$ et $0 \leq r < |m|$.*

Les entiers q, r donnés par ce théorème s'appellent le quotient, respectivement le reste de la division euclidienne de n par m. Si $r = 0$, alors on dit que n est divisible par m (soit que m divise n, m est un diviseur de n, ou n est un multiple de m) et on écrit $m|n$. En posant

$$m\mathbb{Z} := \{mk |\ k \in \mathbb{Z}\},$$

on constate que $m|n$ si et seulement si $n \in m\mathbb{Z}$.

Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Le plus grand commun diviseur (le pgcd) et le plus petit commun multiple (le ppcm) du couple (m,n) sont définis par

$$\text{pgcd}(m,n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},\ \text{ppcm}(m,n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}.$$

Exercice : Montrer que le sous-ensemble $\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\} \subset \mathbb{N}^*$ est non-vide et majoré et que le sous-ensemble $\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\} \subset \mathbb{N}^*$ est non-vide. En conclure que le pgcd et le ppcm d'un couple $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ existent.

Définition 1.1.2 *Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. On dit que m, n sont premiers entre eux si* $\text{pgcd}(m,n) = 1$.

Remarque 1.1.3 *Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$.*

1. *Soit $\mu \in \mathbb{Z}$ un multiple commun de (m,n). Alors* $\text{ppcm}(m,n)|\mu$.
2. *Soit $\delta \in \mathbb{Z}^*$ un diviseur commun de (m,n). Alors* $\delta|\text{pgcd}(m,n)$.

Démonstration: (1) Soient q, r le quotient respectivement le reste de la division euclidienne de μ par $\text{ppcm}(m,n)$. On a donc q, $r \in \mathbb{Z}$ et $0 \leq r < \text{ppcm}(m,n)$. Supposons par l'absurde que $\text{ppcm}(m,n)$ ne divise pas μ. Alors on aura $r \in \mathbb{N}^*$ et $r = \mu - q\,\text{ppcm}(m,n)$ sera un multiple commun de m et n strictement positif et strictement inférieur à $\text{ppcm}(m,n)$. Ceci contredit la définition de $\text{ppcm}(m,n)$.

(2) Remarquer que m, n sont des multiples communs de $d := \text{pgcd}(m,n)$ et δ donc, en utilisant (1), on obtient $\text{ppcm}(d,\delta)|m$ et $\text{ppcm}(d,\delta)|n$, donc $\text{ppcm}(d,\delta)$ est un diviseur commun strictement positif de m et n. Mais évidemment $\text{ppcm}(d,\delta) \geq d$ et $d := \text{pgcd}(m,n)$ est le diviseur commun *maximal* de m et n. Il en résulte $\text{ppcm}(d,\delta) = d$, donc δ divise $d = \text{pgcd}(m,n)$. ■

Remarque 1.1.4 *Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $d = \text{pgcd}(m,n)$. Posons $m' := m/d$, $n' := n/d$. Alors m', n' sont premiers entre eux.*

Démonstration: Exercice. ■

Rappelons qu'un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geq 2$ et les seuls diviseurs positifs de p sont 1 et p. On va noter par $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers. Rappelons que tout nombre naturel $n \in \mathbb{N}^*$ se décompose de manière unique comme produit de nombres premiers. Plus précisément, pour tout $p \in \mathcal{P}$ nous avons une application $v_p : \mathbb{N}^* \to \mathbb{N}$ telle que pour tout $n \in \mathbb{N}^*$ on a une décomposition

$$n = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \neq 0}} p^{v_p(n)}.$$

Donc $v_p(n) = 0$ si p ne divise pas n et est égale à la puissance de p dans la factorisation de n en nombres premiers, si p divise n. Plus précisément : $v_p(n) = \max\{k \in \mathbb{N} |\ p^k|n\}$.

Remarque 1.1.5 *Soient $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors $m|n$ si et seulement si pour tout $p \in \mathcal{P}$ on a $v_p(m) \leq v_p(n)$.*

Remarque 1.1.6 *Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors*

1.

$$\mathrm{pgcd}(m,n) = \prod_{\substack{p\in\mathcal{P} \\ v_p(m)\neq 0 \text{ et } v_p(n)\neq 0}} p^{\min(v_p(|m|),v_p(|n|))}, \quad \mathrm{ppcm}(m,n) = \prod_{\substack{p\in\mathcal{P} \\ v_p(m)\neq 0 \text{ ou } v_p(n)\neq 0}} p^{\max(v_p(|m|),v_p(|n|))}.$$

2. On a l'identité $|mn| = \mathrm{pgcd}(m,n)\,\mathrm{ppcm}(m,n)$.

Démonstration: Exercice. Pour la 2ème affirmation remarquer d'abord que

$$\mathrm{pgcd}(m,n) = \prod_{\substack{p\in\mathcal{P} \\ v_p(m)\neq 0 \text{ ou } v_p(n)\neq 0}} p^{\min(v_p(|m|),v_p(|n|))}.$$

Utiliser l'identité $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$. ■

1.2 L'égalité et le théorème de Bézout

On commence par

Théorème 1.2.1 *[L'égalité de Bézout] Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors il existe un couple $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que*

$$\mathrm{pgcd}(m,n) = um + vn.$$

En utilisant la notation $m\mathbb{Z} + n\mathbb{Z} := \{um + vn |\ (u,v) \in \mathbb{Z} \times \mathbb{Z}\}$, le théorème de Bézout dévient

$$\mathrm{pgcd}(m,n) \in m\mathbb{Z} + n\mathbb{Z}.$$

Démonstration: (de l'égalité de Bézout) Posons :

$$\mathcal{E} := \{k \in \mathbb{N}^* |\ \exists (u,v) \in \mathbb{Z} \times \mathbb{Z} \text{ tel que } k = um + vn\} = (m\mathbb{Z} + n\mathbb{Z}) \cap \mathbb{N}^*.$$

Remarquer que $\mathcal{E}$ est un sous-ensemble non-vide (pourquoi ?) de $\mathbb{N}^*$. Il en résulte que $\delta := \min(\mathcal{E})$ existe et $\delta \in \mathbb{N}^*$. Puisque $\delta \in \mathcal{E}$ on a

$$\delta = u_\delta m + v_\delta n$$

avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$. Nous allons montrer que $\delta = \mathrm{pgcd}(m,n)$. Il suffit de démontrer que

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

Pour démontrer (a) appliquons le théorème de division euclidienne aux couples (δ, m) et (δ, n). On obtient

$$m = q\delta + r, \ n = q'\delta + r',$$

où $(q,q') \in \mathbb{Z} \times \mathbb{Z}$, $0 \leq r < \delta$, $0 \leq r' < \delta$. Nous allons montrer (par l'absurde) que $r = r' = 0$. En effet, supposons par exemple $r > 0$. Alors

$$\mathbb{N}^* \ni r = m - q\delta = m - q(u_\delta m + v_\delta n) = (1 - qu_\delta)m + (-qv_\delta)n,$$

qui, évidemment, est un élément de $\mathcal{E}$. Mais on a $r < \delta$, ce qui contredit la définition de δ (le minimum de l'ensemble $\mathcal{E}$). Il en résulte $r = 0$. Un argument similaire donne $r' = 0$. Donc $r = r' = 0$, ce qui implique évidemment $\delta|m$ et $\delta|n$.

Pour démontrer (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d|u_\delta m$ et $d|v_\delta n$, donc $d|(u_\delta m + v_\delta n) = \delta$. ■

Il existe un algorithme simple qui permet de trouver à la fois $\mathrm{pgcd}(m,n)$ et un couple $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $\mathrm{pgcd}(m,n) = um + vn$. Il s'agit de l'algorithme d'Euclid. Les étapes de cet algorithme sont :

1. On fait la division euclidienne de n par m (donc on obtient une relation de la forme $n = q_1 m + r_1$ avec $q_1 \in \mathbb{Z}$ et $0 \leq r_1 < |m|$) et on pose la question : est-ce que le reste r_1 est nul? Si oui, on a $\text{pgcd}(m,n) = |m|$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.
2. On remarque $r_1 = n - q_1 m \in m\mathbb{Z} + n\mathbb{Z}$, on remplace le couple (m,n) par (r_1, m), on fait la division euclidienne de m par r_1 (donc on obtient une relation de la forme $m = q_2 r_1 + r_2$ avec $q_2 \in \mathbb{Z}$ et $0 \leq r_2 < r_1$) et on repose la question (1) pour le nouveau reste. Si oui, on a $\text{pgcd}(m,n) = r_1$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.
3. On remarque que $r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) \in m\mathbb{Z} + n\mathbb{Z}$, on remplace le couple (r_1, m) par (r_2, r_1) et on continue de la même manière.

Le nombre cherché $\text{pgcd}(m,n)$ coïncide soit avec $|m| = \text{sign}(m)m$ si m divise n, soit avec le dernier reste *non-nul* dans la suite finie de divisions euclidiennes obtenues de cette manière. Par récurrence on obtient facilement des relations de la forme $r_k = u_k m + v_k n$ pour tout k, en particulier on obtient une décomposition explicite de cette forme pour le dernier reste non-nul (qui coïncide avec $\text{pgcd}(m,n)$).

Exemple 1.2.2 En appliquant l'algorithme d'Euclid pour le calcul de $\text{pgcd}(8,135)$, on obtient successivement

$$135 = 16 \cdot 8 + 7\,,\ r_1 = 7 = (-16) \cdot 8 + 135\,,$$

$$8 = 1 \cdot 7 + 1\,,\ \ r_2 = 1 = 1 \cdot 8 - 1 \cdot 7 = 1 \cdot 8 - 1 \cdot ((-16) \cdot 8 + 135) = 17 \cdot 8 + (-1) \cdot 135\,,$$

et $r_3 = 0$. Donc $\text{pgcd}(8,135) = r_2 = 1 = 17 \cdot 8 + (-1) \cdot 135$.

Un corollaire important au théorème de Bézout concerne le cas d'un couple de nombres premiers entre eux.

Corollaire 1.2.3 *[Le théorème de Bézout] Soit $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors m, n sont premiers entre eux si et seulement s'il existe un couple $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$.*

L'implication

$$\Big(\exists (u,v) \in \mathbb{Z} \times \mathbb{Z},\ um + vn = 1\Big) \Rightarrow \text{pgcd}(m,n) = 1$$

est évidente, parce que tout diviseur commun de m et n est un diviseur de $um + vn$. L'implication dans le sens contraire est un cas spécial de l'égalité de Bézout.

Corollaire 1.2.4 *(Le théorème de Gauss dans $\mathbb{Z}$) Soient $(m,n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $x \in \mathbb{Z}$. Si n divise le produit mx et m, n sont premiers entre eux, alors n divise x.*

Démonstration: Soit $k \in \mathbb{Z}$ tel que $mx = kn$ et soit $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$. On obtient

$$x = 1 \cdot x = (um + vn)x = umx + vnx = ukn + vnx = n(uk + vx)$$

avec $(uk + vx) \in \mathbb{Z}$, donc n divise x. ■

On peut donner une démonstration alternative du corollaire 1.2.4 en utilisant les factorisations en nombres premiers de m, n et x. Puisque $n|(mx)$, tout nombre premier qui intervient dans la factorisation de n doit intervenir dans la factorisation de mx (donc aussi dans la factorisation de x) avec un exposant supérieur.

Corollaire 1.2.5 *Soient m, $n \in \mathbb{Z}^*$* `premiers entre eux`*. Pour un couple $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ les deux conditions suivantes sont équivalentes :*

1. *$mx = ny$.*
2. *Il existe $k \in \mathbb{Z}$ tel que $x = kn$ et $y = km$.*

Démonstration: L'implication 2.⇒1. est évidente. Pour l'implication 1.⇒2. remarquons que l'égalité $mx = ny$ implique $n|(mx)$, donc, d'après le théorème 1.2.4 (de Gauss) il en résulte $n|x$. Soit $k \in \mathbb{Z}$ tel que $x = kn$. On obtient $mkn = ny$, donc (puisque $n \neq 0$) $y = km$. ■

1.3 Équations diophantiennes de la forme $ax + by = c$.

Une équation diophantienne est une équation polynomiale à coefficients entiers (à une ou plusieurs inconnues), dont les inconnues sont aussi des entiers (donc dont les solutions sont cherchées dans $\mathbb{Z}$).

Soit $(a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$. Nous allons étudier l'équation diophantienne

$$ax + by = c, \tag{1}$$

donc nous allons déterminer l'ensemble des solutions entières

$$S_{a,b,c} := \{(x,y) \in \mathbb{Z} \times \mathbb{Z} |\ ax + by = c\}$$

de cette équation. Posons $d := \text{pgcd}(a,b)$ et soit $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $ua + vb = d$ (voir le théorème 1.2.1). On peut écrire $a = da'$, $b = db'$ avec a', $b' \in \mathbb{Z}^*$ premiers entres eux d'après la remarque 1.1.4.

Proposition 1.3.1 *Soit $(a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.*

1. *Si d ne divise pas c, alors $S_{a,b,c} = \emptyset$, donc l'équation diophantienne (1) n'admet aucune solution.*
2. *Supposons $d|c$ et soit $q := c/d$. Alors*
   (a) *$(qu, qv) \in S_{a,b,c}$, c'est à dire (qu, qv) est une solution particulière de l'équation diophantienne (1).*
   (b) *L'ensemble $S_{a,b,c}$ des solutions de l'équation diophantienne (1) s'écrit :*

$$S_{a,b,c} = \{(qu + kb', qv - ka') |\ k \in \mathbb{Z}\}.$$

Démonstration: 1. Si $S_{a,b,c} \neq \emptyset$ alors il existe une solution $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ de (1), donc

$$c = ax + by = d(a'x + b'y),$$

donc $d|c$.
2. En multipliant l'égalité connue $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$. Soit $(x,y) \in \mathbb{Z} \times \mathbb{Z}$. Nous avons

$$(x,y) \in S_{a,b,c} \Leftrightarrow ax + by = c \Leftrightarrow ax + by - (aqu + bqv) = 0 \Leftrightarrow a(x - qu) + b(y - qv) = 0 \Leftrightarrow a'(x - qu) + b'(y - qv) = 0$$

$$\Leftrightarrow a'(x - qu) = b'(qv - y).$$

D'après le corollaire 1.2.5 l'égalité $a'(x - qu) = b'(qv - y)$ est équivalente à la condition

$$\exists k \in \mathbb{Z},\ \Big((x - qu = kb') \wedge (qv - y = ka')\Big),$$

donc à la condition

$$\exists k \in \mathbb{Z},\ \Big((x = qu + kb') \wedge (y = qv - ka')\Big),$$

qui est évidemment équivalente à $(x,y) \in \{(qu + kb', qv - ka') |\ k \in \mathbb{Z}\}$.

■

2 Relations d'équivalence. Ensemble quotient. Le quotient $\mathbb{Z}/n\mathbb{Z}$

Définition 2.0.1 *Soit A un ensemble. Une relation sur A est un sous-ensemble $R \subset A \times A$. On convient d'écrire xRy au lieu de $(x,y) \in R$. Si xRy on dit que x est en relation R avec y. Une relation R sur A est dite relation d'équivalence si*

1. *R est réflexive, i.e.*
$$\forall x \in A,\ xRx.$$
2. *R est symétrique, i.e.*
$$\forall (x,y) \in A \times A\ (xRy \Rightarrow yRx).$$
3. *R est transitive, i.e.*
$$\forall (x,y,z) \in A \times A \times A\ ((xRy) \wedge (yRz) \Rightarrow xRz).$$

2.1 Classes d'équivalence par rapport à une relation d'équivalence. Ensemble quotient

On va commencer par la

Définition 2.1.1 *Deux ensembles C, D sont dits disjoints si $C \cap D = \emptyset$.*

Soit A un ensemble et soit $\mathcal{P}(A)$ l'ensemble des parties de A. Pour un *sous-ensemble* $\mathcal{Q} \subset \mathcal{P}(A)$ (donc pour un ensemble de parties de A) nous définissions

$$\bigcup_{C\in\mathcal{Q}} C := \{x \in A |\ \exists C \in \mathcal{Q},\ x \in C\},\ \bigcap_{C\in\mathcal{Q}} C := \{x \in A |\ \forall C \in \mathcal{Q},\ x \in C\}. \tag{2}$$

Définition 2.1.2 *Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :*

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$
2. $$\bigcup_{C\in\mathcal{Q}} C = A.$$
3. $$\forall C \in \mathcal{Q}\ \forall C' \in \mathcal{Q}\ \Big(C \neq C' \Rightarrow C \cap C' = \emptyset\Big).$$

Donc une partition de A est une décomposition de A en réunion de sous-ensembles *non-vides et disjoints deux à deux*.

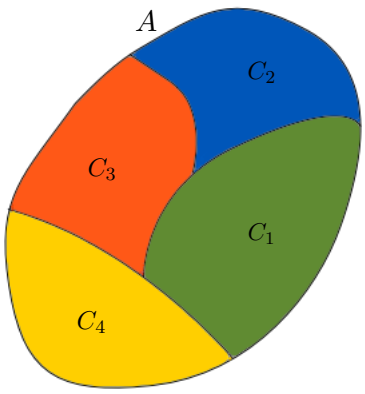


FIGURE 1 – Une partition $\{C_1, C_2, C_3, C_4\}$ d'un ensemble $A \subset \mathbb{R}^2$. Un puzzle à 4 pièces.

Exemples 2.1.3

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.
2. Soit A un ensemble et soit $\mathcal{S} := \{\{a\} |\ a \in A\} \subset \mathcal{P}(A)$ l'ensemble des singletons de A. $\mathcal{S}$ est une partition de A. Remarquer que $\mathcal{S}$ est vide si A est vide.
3. Soit $B \subset A$ un sous-ensemble de A tel que $B \neq \emptyset$ et $B \neq A$. Alors $\{B, {}^cB\}$ est une partition de A.
4. Soient
$$2\mathbb{Z} := \{2k |\ k \in \mathbb{Z}\},\ 2\mathbb{Z}+1 := \{2k+1 |\ k \in \mathbb{Z}\}$$
les ensembles des nombres entiers pairs, respectivement impairs. Alors $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ est une partition de $\mathbb{Z}$.

Définition 2.1.4 *Soit R une relation d'équivalence sur A et soit $a \in A$.*

1. *La classe d'équivalence de a par rapport à R est le sous-ensemble de A défini par*

$$[a]_R := \{b \in A |\ a\ R\ b\}.$$

Donc la classe d'équivalence $[a]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à a.

2. *Un sous-ensemble $C \subset A$ est dit classe d'équivalence par rapport à R s'il existe $a \in A$ tel que $C = [a]_R$.*
3. *L'ensemble quotient de A par R est l'ensemble A/R des classes d'équivalence par rapport à R :*

$$A/R := \{C \in \mathcal{P}(A) |\ \exists a \in A,\ C = [a]_R\}.$$

4. *La surjection canonique $p_R : A \to A/R$ est définie par*

$$p_R(a) := [a]_R,$$

donc p_R associe à un élément $a \in A$ sa classe d'équivalence $[a]_R$.

Exercice 2.1.5 Expliquer pourquoi p_R est bien surjective.

La proposition suivante montre que, dans la présence d'une relation d'équivalence, l'ensemble quotient A/R, regardé comme sous-ensemble de $\mathcal{P}(E)$, est une partition de A.

Proposition 2.1.6 *Soit A un ensemble et soit R une relation d'équivalence sur A. Alors*

1. *Pour tout $a \in A$ on a*

$$a \in [a]_R,$$

en particulier toute classe d'équivalence par rapport à R est non-vide.

2. *Soient $a, a' \in A$ et soient $C = [a]_R$, $C' = [a']_R \in A/R$ leurs classes d'équivalence. Les propriétés suivantes sont équivalentes :*
   (a) $C \cap C' \neq \emptyset$.
   (b) $a\ R\ a'$.
   (c) $C = C'$.

   En particulier deux classes d'équivalence $C = [a]_R$, $C' = [a']_R$ sont soit égales (quand $a\ R\ a'$), soit disjointes (quand $a \not R\ a'$).
3. *On a*

$$\bigcup_{C \in A/R} C = A.$$

4. *A/R est une partition de A.*

Démonstration: 1. Soit $a \in A$. Puisque R est réflexive on a $a\ R\ a$, donc $a \in [a]_R$ par la définition de $[a]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit donc $b \in C \cap C'$. Donc $b \in [a]_R$ et $b \in [a']_R$, i.e. $a\ R\ b$ et $a'\ R\ b$. En utilisant la symétrie et la transitivité de R on obtient $a\ R\ a'$.

$(b) \Rightarrow (c)$: En supposant $a\ R\ a'$ on va démontrer par double inclusion que $C = C'$. Soit $b \in C = [a]_R$. On a donc $a\ R\ b$. Puisque $a\ R\ a'$ on obtient (en utilisant la symétrie et la transitivité de R) $a'\ R\ b$ donc $b \in [a']_R = C'$. Argument similaire pour l'inclusion inverse.

$(c) \Rightarrow (a)$: Supposons $C = C'$. On a $C \cap C' = C$, qui est non-vide d'après 1.

3. L'inclusion $\bigcup_{C \in A/R} C \subset A$ est évidente parce toutes les classes d'équivalence C sont des sous-ensembles de A. Pour l'inclusion inverse, soit $a \in A$. D'après la première affirmation nous savons que $a \in [a]_R$, donc a appartient à sa propre classe d'équivalence (qui "participe" à la réunion $\bigcup_{C \in A/R} C$), donc $a \in \bigcup_{C \in A/R} C$.

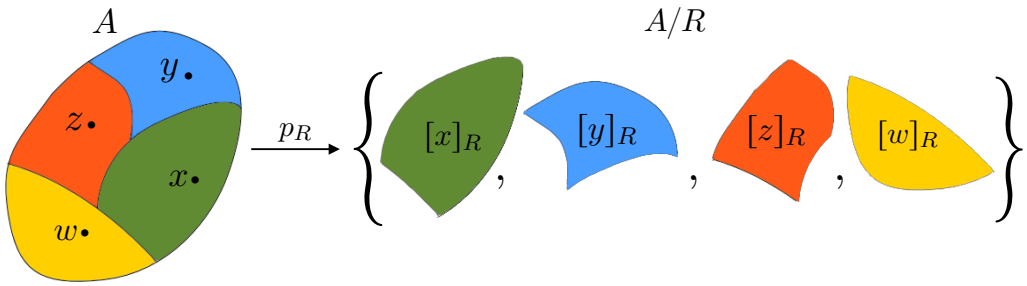


FIGURE 2 – Une relation d'équivalence R avec 4 classes d'équivalence. Chaque classe d'équivalence $C = [a]_R$ devient un élément de A/R. L'ensemble quotient A/R a 4 éléments.

4. En tenant compte de la définition 2.1.2, l'affirmation 4. est une conséquence directe de 1., 2. et 3. ■

En réalité la donnée d'une relation d'équivalence sur A est équivalente à la donnée d'une partition de A. La partition associée à une relation d'équivalence R est le quotient A/R regardé comme sous-ensemble de $\mathcal{P}(A)$. Le passage dans le sens contraire (d'une partition à une relation d'équivalence) est expliqué dans l'exercice suivant :

Exercice 2.1.7 Soit A un ensemble et soit $\mathcal{Q} \subset \mathcal{P}(A)$ une partition de A. Montrer que la relation R sur A définie par

$$a \, R \, b \text{ s'il existe } C \in \mathcal{Q} \text{ tel que } a \in C \text{ et } b \in C$$

est une relation d'équivalence sur A dont l'ensemble quotient A/R est $\mathcal{Q}$.

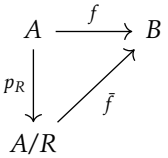
Définition 2.1.8 *Soit R une relation d'équivalence sur A. Une application $f : A \to B$ est dite compatible avec R si*

$$\forall x \in A \; \forall y \in A \left(x \, R \, y \Rightarrow f(x) = f(y) \right).$$

Exemples 2.1.9

1. Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par : $x \, R \, y$ si $y - x \in 2\mathbb{Z}$ (i.e. si x et y sont de même parité). L'application $f : \mathbb{Z} \to \{\pm 1\}$ définie par $f(k) = (-1)^k$ est compatible avec R.
2. Soit R la relation d'équivalence sur $\mathbb{R}$ définie par : $s \, R \, t$ si $t - s \in \mathbb{Z}$. L'application $f : \mathbb{R} \to \mathbb{C}$ définie par $f(t) := e^{2\pi i t}$ est compatible avec R.

Remarque 2.1.10 *Soient R une relation d'équivalence sur A et $f : A \to B$ une application compatible avec R. La formule $[x]_R \mapsto f(x)$ définit une application $\bar{f} : A/R \to B$ sur l'ensemble quotient A/R.*



Cette application a la propriété $\bar{f} \circ p_R = f$.

Démonstration: Exercice. ■

On peut reformuler cette remarque de la manière suivante : si f est compatible avec R, alors f "descend" au quotient A/R. On va dire aussi que $\bar{f}$ est *induite* par f.

2.2 Exemples élémentaires de relations d'équivalence

Voici quelques exemples élémentaires de relations d'équivalence. Dans chaque cas on va préciser les classes d'équivalence et l'ensemble quotient.

La relation "même année de naissance" sur l'ensemble des étudiants de ce groupe. Soit $\mathcal{G}$ ce groupe d'étudiants (ici présents). Considérons la relation R sur $\mathcal{G}$ définie par

$$x\ R\ y \text{ si } x,\ y \text{ sont nés la même année.}$$

C'est facile de voir que R est une relation d'équivalence sur $\mathcal{G}$. La classe d'équivalence $[x]_R$ de $x \in \mathcal{G}$ est l'ensemble formé par lui-même et tous ses collègues nés la même année. Combien de classes d'équivalence par rapport à R y a-t-il dans votre groupe ?

La relation d'égalité Δ sur A. Soit A un ensemble. Rappelons que la relation d'égalité sur A correspond à la diagonale $\Delta := \Delta_A \subset A \times A$ du produit cartésien $A \times A$. Par rapport à cette relation, un élément $a \in A$ est en relation avec lui-même et seulement avec lui même. Pour tout élément $a \in A$ la classe d'équivalence $[a]_\Delta$ par rapport à cette relation coïncide avec le singleton $\{a\}$. Dans ce cas

$$A/\Delta = \{\{a\} |\ a \in A\}$$

est l'ensemble des singletons associés aux éléments de A et la surjection canonique $p_\Delta : A \to A/R$ est la bijection définie par

$$p_\Delta(a) = \{a\}.$$

La relation totale $A \times A$ sur A. Soit A un ensemble. Le produit cartésien $\Pi := A \times A$ est une relation d'équivalence sur A. Pour tout élément $a \in A$ la classe d'équivalence $[a]_\Pi$ par rapport à cette relation coïncide avec A. L'ensemble quotient A/Π s'identifie au singleton $\{A\}$ et la surjection canonique est l'application constante $p_\Pi : A \to \{A\}$ donnée par $p_\Pi(a) = A$ pour tout $a \in A$.

La relation "de même parité" sur $\mathbb{Z}$. Soient $a,\ b \in \mathbb{Z}$. La condition "$a,\ b$ sont de même parité" définit une relation d'équivalence R_{par} sur $\mathbb{Z}$. Remarquons que $a\ R_{\text{par}}\ b$ si et seulement si $b - a$ est pair, donc R_{par} coïncide avec la relation de congruence mod 2.

La classe d'équivalence d'un nombre pair est $2\mathbb{Z} := \{2k |\ k \in \mathbb{Z}\}$ et la classe d'équivalence d'un nombre impair est $2\mathbb{Z}+1 := \{2k+1 |\ k \in \mathbb{Z}\}$. Le quotient $\mathbb{Z}/R_{\text{par}}$ est donc

$$\mathbb{Z}/R_{\text{par}} = \{2\mathbb{Z}, 2\mathbb{Z}+1\},$$

et la surjection canonique $p_{R_{\text{par}}} : \mathbb{Z} \to \mathbb{Z}/R_{\text{par}}$ est donnée par

$$p_{R_{\text{par}}}(x) = \begin{cases} 2\mathbb{Z} & \text{si} \quad x \text{ est pair} \\ 2\mathbb{Z}+1 & \text{si} \quad x \text{ est impair} \end{cases}.$$

Le relation "de même signe" sur $\mathbb{R}^*$. Soient $x,\ y \in \mathbb{R}^*$. La condition "$x,\ y$ sont de même signe" définit une relation d'équivalence R_{sign} sur $\mathbb{R}^*$. Remarquons que $x\ R_{\text{sign}}\ y$ si et seulement si $xy > 0$. La classe d'équivalence d'un nombre strictement positif est $\mathbb{R}^*_+$ et la classe d'équivalence d'un nombre strictement négatif est $\mathbb{R}^*_-$. Le quotient $\mathbb{R}^*/R_{\text{sign}}$ est donc

$$\mathbb{R}^*/R_{\text{sign}} = \{\mathbb{R}^*_-, \mathbb{R}^*_+\},$$

et la surjection canonique $p_{R_{\text{sign}}} : \mathbb{R}^* \to \mathbb{R}^*/R_{\text{sign}}$ est donnée par

$$p_{R_{\text{sign}}}(x) = \begin{cases} \mathbb{R}^*_+ & \text{si} \quad x > 0 \\ \mathbb{R}^*_- & \text{si} \quad x < 0. \end{cases}.$$

Le relation "même image par f" sur l'ensemble de définition de f. Soit $f : A \to B$ une application. La relation d'équivalence associée à f est la relation R_f sur A définie par

$$x\ R_f\ x' \text{ si } f(x) = f(x').$$

La classe d'équivalence d'un élément $a \in A$ est

$$[a]_{R_f} = \{x \in A |\ f(x) = f(a)\} = \{x \in A |\ f(x) \in \{f(a)\}\} = f^{-1}(\{f(a)\}).$$

Donc la classe d'équivalence de a par rapport à R_f est l'image réciproque $f^{-1}(\{f(a)\})$ du singleton $\{f(a)\}$. Cette image réciproque s'appelle *la fibre de f au-dessus de $f(a)$*, ou la fibre de f qui passe par a.

Remarque 2.2.1 *La formule*

$$\bar{f}([x]_{R_f}) = f(x) \tag{3}$$

définit une bijection

$$\bar{f} : A/R_f \to \mathrm{im}(f).$$

Démonstration: Il faut d'abord vérifier que $\bar{f}$ est bien définie, i.e. que le membre droit de (3) dépend seulement de la classe d'équivalence $[x]_{R_f}$. Il faut donc vérifier que si on choisit un autre "représentant" x' de la même classe, on aura $f(x) = f(x')$. Mais $x' \in [x]_{R_f}$ si et seulement si $x \; R_f \; x'$, si et seulement si $f(x) = f(x')$. Vérifier l'injectivité et la surjectivité de $\bar{f}$. ■

La signification de la remarque 2.2.1 est : l'ensemble quotient A/R_f "s'identifie" naturellement à l'image $\mathrm{im}(f)$ de f.

Exercice 2.2.2 Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \cos(x)$. Pour un élément $x \in \mathbb{R}$ écrire explicitement la classe d'équivalence $[x]_{R_f}$. La même question pour l'application $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sin(x)$.

Exercice 2.2.3 Soient A un ensemble et R une relation d'équivalence sur A. Quelle est la relation d'équivalence R_{p_R} associée à la surjection canonique $p_R : A \to A/R$? En déduire que *toute* relation d'équivalence sur A est associée à une application définie sur A.

2.3 Congruence mod n. Le quotient $\mathbb{Z}/n\mathbb{Z}$

2.3.1 Définition et premières propriétés

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk |\; k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Plus généralement, pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk |\; k \in \mathbb{Z}\}.$$

Rappelons que la relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y \,[n] \text{ si } n|(y - x), \tag{4}$$

et que cette relation est une relation d'équivalence sur $\mathbb{Z}$. Afin de pouvoir utiliser de manière homogène les notations introduites dans le chapitre 2.1, désignons par $\underset{n}{\equiv}$ cette relation d'équivalence. La définition (4) devient :

$$x \underset{n}{\equiv} y \text{ si } y - x \in \; n\mathbb{Z}. \tag{5}$$

La classe d'équivalence d'un élément $x \in \mathbb{Z}$ par rapport à $\underset{n}{\equiv}$ sera donc

$$[x]_n = \{y \in \mathbb{Z} |\; x \underset{n}{\equiv} y\} = \{y \in \mathbb{Z} |\; \exists k \in \mathbb{Z},\; y = x + nk\} = x + n\mathbb{Z},$$

en particulier la classe de 0 (la classe triviale mod n) est

$$[0]_n = n\mathbb{Z}.$$

Notre but est de comprendre en détail l'ensemble quotient $\mathbb{Z}/\underset{n}{\equiv}$. La notation standard pour cet ensemble quotient est $\mathbb{Z}/n\mathbb{Z}$ et cette notation est justifiée par la formule (5). Pour ce quotient on utilise aussi la notation simplifiée $\mathbb{Z}_n$.

Proposition 2.3.1 *Soit $n \in \mathbb{N}^*$.*

1. *L'application $\gamma : \{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\gamma(k) = [k]_n$ est bijective.*

2. *Les classes d'équivalence* $[0]_n, \ldots, [n-1]_n$ *sont distinctes deux à deux et l'ensemble quotient* $\mathbb{Z}/n\mathbb{Z}$ *s'écrit explicitement*

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}.$$

En particulier $\text{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Démonstration: On va utiliser le lemme 2.3.2 énoncé après la démonstration. On va donc construire une application

$$\rho : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$$

telle que

$$\gamma \circ \rho = \text{id}_{\mathbb{Z}/n\mathbb{Z}}, \ \rho \circ \gamma = \text{id}_{\{0,\ldots,n-1\}}.$$

L'application ρ est définie de la manière suivante : pour une classe $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$ posons

$$\rho(\xi) = \text{ le reste de la division euclidienne de } k \text{ par } n \tag{6}$$

(voir le théorème 1.1.1). Remarquons d'abord que ρ est bien définie. En effet, si on remplace k par un autre "représentant" k' de la classe ξ, on aura $k' - k \in n\mathbb{Z}$, donc le reste de la division euclidienne de k' par n coïncide avec le reste de la division euclidienne de k par n. Ceci montre que le membre droit de (6) dépend seulement de ξ.

L'égalité $\rho \circ \gamma = \text{id}_{\{0,\ldots,n-1\}}$ est évidente. Démontrons l'égalité $\gamma \circ \rho = \text{id}_{\mathbb{Z}/n\mathbb{Z}}$, i.e. $\gamma(\rho([k]_n) = [k]_n$ pour tout $k \in \mathbb{Z}$. Il suffit de remarquer que k et le reste de la division euclidienne de k par n sont congrus mod n, donc leurs classes mod n coïncident.

2. Est une conséquence directe de 1. Préciser les détails. ■

Lemme 2.3.2 *Soit* $f : A \to B$ *une application. Supposons qu'il existe une application* $g : B \to A$ *telle que* $g \circ f = \text{id}_A$ *et* $f \circ g = \text{id}_B$. *Alors* f *est bijective et* $g = f^{-1}$.

Démonstration: Exercice. ■

Exemple 2.3.3 Pour $n = 5$ on obtient $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. Montrer qu'on a aussi

$$\mathbb{Z}/5\mathbb{Z} = \{[33]_5, [56]_5, [27]_5, [15]_5, [29]_5\}.$$

2.3.2 Les opérations $+, \cdot$ sur $\mathbb{Z}/n\mathbb{Z}$.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est intéressant du point de vue de l'algèbre moderne parce qu'il peut être muni naturellement de deux opérations : l'addition et la multiplication des classes de congruence. Ces opérations sont "induites" par les opérations élémentaires sur $\mathbb{Z}$, mais ne sont pas des opérations avec des nombres. Ce sont des opérations algébriques nouvelles.

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x+y]_n.$$

Cette définition est cohérente, au sens que le membre droit $[x+y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes. En effet, si on choisit d'autres représentants x', y' de ces classes (c'est à dire $[x']_n = [x]_n$, $[y']_n = [y]_n$), alors il existe $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ tels que $x' - x = kn$, $y' - y = ln$, donc $(x'+y') - (x+y) = (k+l)n \in n\mathbb{Z}$, donc $[x'+y']_n = [x+y]_n$.

De manière similaire, la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n \cdot [y]_n := [xy]_n.$$

Exercice 2.3.4 Montrer que la définition de la multiplication est cohérente. Plus précisément, montrer que si $[x']_n = [x]$ et $[y']_n = [y]_n$, alors $[x'y']_n = [xy]_n$.

Exercice 2.3.5 Compléter les tables des deux opérations sur $\mathbb{Z}/7\mathbb{Z}$:

$+$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[0]_7$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$	$[0]_7$
$[2]_7$	$[2]_7$						
$[3]_7$	$[3]_7$						
$[4]_7$	$[4]_7$						
$[5]_7$	$[5]_7$						
$[6]_7$	$[6]_7$						

$\cdot$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$
$[1]_7$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[2]_7$	$[0]_7$						
$[3]_7$	$[0]_7$						
$[4]_7$	$[0]_7$						
$[5]_7$	$[0]_7$						
$[6]_7$	$[0]_7$						

.

En utilisant les propriétés élémentaires de l'addition et de la multiplication sur $\mathbb{Z}$ on obtient facilement :

Proposition 2.3.6 *Les opérations $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ satisfont les propriétés suivantes :*

1. *L'addition est associative :*
$$\forall(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ (\alpha+\beta)+\gamma = \alpha+(\beta+\gamma).$$
2. *La classe nulle $[0]_n$ est élément neutre pour l'addition :*
$$\forall \alpha \in \mathbb{Z}/n\mathbb{Z},\ \alpha + [0]_n = [0]_n + \alpha = \alpha.$$
3. *Pour toute classe $\alpha = [k]_n \in \mathbb{Z}/n\mathbb{Z}$ la classe $-\alpha := [-k]_n$ est un élément symétrique de α par rapport à l'addition :*
$$\alpha + (-\alpha) = [0]_n.$$
4. *L'addition est commutative :*
$$\forall(\alpha,\beta) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta = \beta+\alpha.$$
5. *La multiplication est associative :*
$$\forall(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ (\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma).$$
6. *La classe $[1]_n$ est élément neutre pour la multiplication :*
$$\forall \alpha \in \mathbb{Z}/n\mathbb{Z},\ \alpha\cdot[1]_n = [1]_n\cdot\alpha = \alpha.$$
7. *La multiplication est distributive par rapport à l'addition :*
$$\forall(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma.$$
8. *La multiplication est commutative :*
$$\forall(\alpha,\beta) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot\beta = \beta\cdot\alpha.$$

On va voir que, en utilisant la terminologie des anneaux, ces propriétés nous permettent de conclure que $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif. Cet anneau s'appelle l'anneau des entiers modulo n.

Remarque 2.3.7 *La multiplication des nombres (dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{C}$) a une propriété très importante : le produit de deux éléments non-nuls est toujours non-nul. Une difficulté importante : si $n \geq 2$ n'est pas un nombre premier, cette propriété n'est pas vraie dans $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 2.3.8 Dans $\mathbb{Z}/6\mathbb{Z}$ nous avons : $[2]_6 \neq [0]_6$, $[3]_6 \neq [0]_6$, mais $[2]_6 \cdot [3]_6 = [0]_6$.

Exercice 2.3.9
1. Donner la liste de tous les couples $(\lambda,\eta) \in (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$ tels que $\lambda\cdot\eta = [0]_{12}$.
2. Résoudre l'équation
$$x^2 - ([5]_{12})x + [6]_{12} = [0]_{12}$$
dans $\mathbb{Z}/12\mathbb{Z}$.

2.3.3 Éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$

Définition 2.3.10 *Un élément $\xi \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible, s'il est inversible par rapport à la multiplication, c'est à dire s'il existe $\eta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\xi\eta = [1]_n$. Le sous-ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sera noté $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proposition 2.3.11 *Une classe $\xi = [k]_n$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si* $\mathrm{pgcd}(k,n) = 1$. *En particulier, si p est un nombre premier on a $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]_p\}$, donc $\mathbb{Z}_p^\times = \left\{[1]_p, \ldots, [p-1]_p\right\}$.*

Démonstration: On a

$$[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow \exists \lambda \in \mathbb{Z}/n\mathbb{Z},\ [k]_n\lambda = [1]_n \Leftrightarrow \exists l \in \mathbb{Z},\ [k]_n[l]_n = [1]_n \Leftrightarrow \exists l \in \mathbb{Z},\ 1 - kl \in n\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow \exists (l,q) \in \mathbb{Z}\times\mathbb{Z},\ 1 - kl = nq \Leftrightarrow \exists (l,q) \in \mathbb{Z}\times\mathbb{Z},\ kl + nq = 1 \Leftrightarrow \mathrm{pgcd}(k,n) = 1.$$

Pour la dernière équivalence on a utilisé le théorème de Bézout. ■

Exemple 2.3.12 Pour $n = 30$ on obtient $(\mathbb{Z}/30\mathbb{Z})^\times = \left\{[1]_{30}, [7]_{30}, [11]_{30}, [13]_{30}, [17]_{30}, [19]_{30}, [23]_{30}, [29]_{30}\right\}$, donc $\mathrm{card}((\mathbb{Z}/30\mathbb{Z})^\times) = 8$.

Remarque 2.3.13 *$(\mathbb{Z}/n\mathbb{Z})^\times$ est stable par rapport à la multiplication, c'est à dire*

$$(\xi \in (\mathbb{Z}/n\mathbb{Z})^\times) \wedge (\eta \in (\mathbb{Z}/n\mathbb{Z})^\times) \Rightarrow \xi\eta \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Exercice 2.3.14 Préciser le sous-ensemble $(\mathbb{Z}/12\mathbb{Z})^\times \subset \mathbb{Z}/12\mathbb{Z}$ et faire la table de la multiplication sur ce sous-ensemble.

Notation simplifiée : On utilise souvent la notation $\mathbb{Z}_n$ pour le quotient $\mathbb{Z}/n\mathbb{Z}$ et la notation $\mathbb{Z}_n^\times$ pour le sous-ensemble des éléments inversibles.

2.4 Le théorème des restes chinois

Dans ce chapitre on va utiliser la notation simplifiée $\mathbb{Z}_n$ au lieu de $\mathbb{Z}/n\mathbb{Z}$. Soient $k \in \mathbb{N}^*$ et $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$. Posons $n := \prod_{i=1}^k n_i$ leur produit.

Remarque 2.4.1 *L'application*

$$F : \mathbb{Z} \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i},\ F(x) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

est compatible avec la relation d'équivalence $\underset{n}{\equiv}$ (voir la définition 2.1.8), donc d'après la remarque 2.1.10 , la formule

$$f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

définit de manière cohérente une application $f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}$.

Démonstration: Nos devons vérifier l'implication

$$x \underset{n}{\equiv} y \Rightarrow F(x) = F(y).$$

Mais $n = \prod_{i=1}^k n_i$, donc

$$x \underset{n}{\equiv} y \Rightarrow \Big(\prod_{i=1}^k n_i\Big) \,\Big|\, (y-x) \Rightarrow \forall i \in \{1,\ldots,k\},\ n_i | (y-x) \Rightarrow \forall i \in \{1,\ldots,k\},\ [x]_{n_i} = [y]_{n_i} \Rightarrow F(x) = F(y).$$

■

Remarque 2.4.2 *L'application f donnée par la remarque 2.4.1 est compatible avec les deux opérations $+$ et $\cdot$ sur $\mathbb{Z}_n$ et $\bigtimes_{i=1}^k \mathbb{Z}_{n_i}$. Plus précisément :*

$$f(\xi+\eta) = f(\xi) + f(\eta),\ f(\xi\eta) = f(\xi)f(\eta)$$

où a droite on a utilisé les opérations sur $\bigtimes_{i=1}^k \mathbb{Z}_{n_i}$ définies par

$$(\xi_1,\dots,\xi_k) + (\eta_1,\dots,\eta_k) := (\xi_1+\eta_1,\dots,\xi_k+\eta_k),$$
$$(\xi_1,\dots,\xi_k)(\eta_1,\dots,\eta_k) := (\xi_1\eta_1,\dots,\xi_k\eta_k).$$

Remarquons aussi que $f([1]_n) = ([1]_{n_1},\dots,[1]_{n_k})$.$+$ et $\cdot$ sur $\mathbb{Z}_n$ et $\bigtimes_{i=1}^k \mathbb{Z}_{n_i}$.

On va voir que, en utilisant la terminologie de la théorie des anneaux, ces propriétés nous permettent de conclure que $f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}$ est un homomorphisme d'anneaux.

Théorème 2.4.3 *(le théorème des restes chinois) Soient $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^k n_i$ et soit $f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}$ l'application définie par*

$$f([x]_n) := ([x]_{n_1},\dots,[x]_{n_k})$$

(voir la remarque 2.4.1). Si $n_1,\dots,n_k$ sont premiers entre eux deux à deux, alors f est bijective.

Démonstration: On va démontrer d'abord que f est injective. Soient $[x]_n$, $[y]_n \in \mathbb{Z}_n$. Nous avons

$$f([x]_n) = f([y]_n) \Leftrightarrow \left([x]_{n_i} = [y]_{n_i} \text{ pour } 1 \le i \le k\right) \Leftrightarrow (n_i | (y-x) \text{ pour } 1 \le i \le k).$$

En utilisant le lemme 2.4.4 expliqué après la démonstration, il en résulte

$$(n_i | (y-x) \text{ pour } 1 \le i \le k) \Leftrightarrow n | (y-x).$$

Donc

$$f([x]_n) = f([y]_n) \Leftrightarrow x \equiv y \mod n \Leftrightarrow [x]_n = [y]_n,$$

ce qui démontre l'injectivité de f. Pour justifier la bijectivité il suffit de remarquer que les ensembles $\mathbb{Z}_n$, $\bigtimes_{i=1}^k \mathbb{Z}_{n_i}$) sont finis et

$$\text{card}(\mathbb{Z}_n) = \text{card}(\bigtimes_{i=1}^k \mathbb{Z}_{n_i}) = n.$$

■

Lemme 2.4.4 *Soient $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et $x \in \mathbb{Z}$. Alors sont équivalentes :*

(i) n_i divise x pour $1 \le i \le k$.

(ii) $n = \prod_{i=1}^k n_i$ divise x.

Démonstration: L'implication

$$(n|x) \Rightarrow (n_i | x \text{ pour } 1 \le i \le k)$$

est toujours vraie (sans aucune conditions sur les n_i) et est évidente. Pour l'implication inverse, supposons que $n_i | x$ pour $1 \le i \le k$. On veut démontrer $n|x$. Le cas $x = 0$ est évident, donc on peut supposer $x \neq 0$ et on va comparer les factorisations en produit de nombres premiers de n et x. Soit p un nombre premier qui intervient dans la factorisation de $n = \prod_{i=1}^k n_i$ et soit s l'exposant de p dans cette factorisation. Puisque les n_i sont premiers entre eux deux à deux, il existe un unique $j \in \{1,\dots,k\}$ tel que le facteur p^s intervient aussi dans la factorisation de n_j. Puisque $n_j | x$ par hypothèse, il en résulte que p intervient aussi dans la factorisation de x et l'exposant de p dans cette factorisation est un nombre naturel $t \ge s$. D'après la remarque 1.1.5, il en résulte $n|x$.

On peut démontrer la remarque plus rapidement en utilisant une propriété élémentaire du ppcm : si les nombres n_i $(1 \le i \le k)$ sont premiers entre eux deux à deux, alors $\text{ppcm}(n_1,\dots,n_k) = \prod_{i=1}^k n_i$. ■

Remarque 2.4.5 *On va voir que, en utilisant la terminologie de la théorie des anneaux, la remarque 2.4.2 et le théorème 2.4.3 nous permettent de conclure que, si $n_1,\dots,n_k$ sont premiers entre eux deux à deux, alors l'application $f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}$ définie dans la remarque 2.4.1 est un isomorphisme d'anneaux.*

Soit $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$. En utilisant la remarque 2.4.2 on déduit facilement que $f(\mathbb{Z}_n^\times) \subset \bigtimes_{i=1}^k \mathbb{Z}_{n_i}^\times$. Si $n_1,\dots,n_k$ sont premiers entre eux, cette inclusion est une égalité et la restriction $f|_{\mathbb{Z}_n^\times}$ définit une bijection $h : \mathbb{Z}_n^\times \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}^\times$. Plus précisément :

Proposition 2.4.6 *(la version multiplicative du lemme chinois) Soit $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^k n_i$ leur produit. Alors la formule*

$$h([x]_n) := ([x]_{n_1},\dots,[x]_{n_k})$$

définit une bijection $h : \mathbb{Z}_n^\times \xrightarrow{\simeq} \bigtimes_{i=1}^k \mathbb{Z}_{n_i}^\times$.

On va voir que cette bijection est un isomorphisme de groupes.

On peut reformuler le théorème 2.4.3 de la manière suivante :

Corollaire 2.4.7 *Soit $(n_1,\dots,n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^k n_i$ leur produit. Soit $(y_1,\dots,y_k) \in \mathbb{Z}^k$ une famille arbitraire de k nombres entiers. Alors*

1. *Il existe $x \in \mathbb{Z}$ tel que*
$$[x]_{n_i} = [y_i]_{n_i} \text{ pour } 1 \le i \le k.$$
2. *La classe de congruence $[x]_n$ est déterminée uniquement par $([y_1]_{n_1},\dots,[y_k]_{n_k})$.*

Autrement dit

Remarque 2.4.8 *Dans les conditions et avec les notations du corollaire il existe $x \in \mathbb{Z}$ qui résout simultanément toutes les congruences $x \underset{n_i}{\equiv} y_i$ et la classe modulo n de cet entier x est déterminée uniquement.*

Nous avons un algorithme simple pour déterminer une solution x des congruences $x \underset{n_i}{\equiv} y_i$:

Posons $\hat{n}_j := \prod_{s\neq j} n_s$ et remarquons que, dans les hypothèses du corollaire, on a $\operatorname{pgcd}(n_j,\hat{n}_j) = 1$. D'après le théorème de Bézout il existe $(u_j,v_j) \in \mathbb{Z}\times\mathbb{Z}$ tels que

$$u_j n_j + v_j \hat{n}_j = 1\,.$$

On peut trouver explicitement un couple (u_j,v_j) avec cette propriété en utilisant l'algorithme de Euclid (voir la section 1.2). Posons $x_j := v_j\hat{n}_j$. Remarquons que

$$x_j \underset{n_j}{\equiv} 1,\ x_j \underset{n_i}{\equiv} 0 \text{ pour } i \neq j\,.$$

Expliquer ces congruences. Soit $x := \sum_{j=1}^k y_j x_j$. Pour $1 \le i \le k$ fixé on obtient

$$[x]_{n_i} = \Big[\sum_{j=1}^k y_j x_j\Big]_{n_i} = \sum_{j=1}^k [y_j]_{n_i}[x_j]_{n_i} = [y_i]_{n_i}\,,$$

parce que $[x_j]_{n_i} = 0$ pour $j \neq i$ et $[x_i]_{n_i} = 1$. Donc x est bien une solution des congruences $x \equiv y_i \bmod n_i$.

Exercice 2.4.9 Trouver $[m]$, $[n]$, $[p]$, $[q] \in \mathbb{Z}_{140}$ tels que :

1. $m \equiv 1 \bmod 4$, $m \equiv 0 \bmod 5$, $m \equiv 0 \bmod 7$.
2. $n \equiv 0 \bmod 4$, $n \equiv 1 \bmod 5$, $n \equiv 0 \bmod 7$.
3. $p \equiv 0 \bmod 4$, $p \equiv 0 \bmod 5$, $p \equiv 1 \bmod 7$.
4. $q \equiv 2 \bmod 4$, $q \equiv 3 \bmod 5$, $q \equiv 3 \bmod 7$.

3 Théorie des groupes

3.1 Définition. Exemples. Règles de calcul dans un groupe

Définition 3.1.1 *Soit M un ensemble. Une loi de composition interne sur M est une application*

$$l : M \times M \to M .$$

Notations possibles :

$$x \circ y := l(x,y),\ x * y := l(x,y),\ x \cdot y := l(x,y),\ x + y := l(x,y) \ldots$$

Sur un ensemble fini on peut définir une loi de composition interne à l'aide d'un tableau. Sur un ensemble à trois éléments $M = \{a,b,c\}$ une loi de composition interne $\circ$ sera définie par un tableau de la forme

$\circ$	a	b	c
a	$a \circ a$	$a \circ b$	$a \circ c$
b	$b \circ a$	$b \circ b$	$b \circ c$
c	$c \circ a$	$c \circ b$	$c \circ c$

.

Exemple 3.1.2 Par exemple la loi de composition interne définie par le tableau

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	b	c

, (7)

est l'application $l : \{a,b,c\} \times \{a,b,c\} \to \{a,b,c\}$ donnée par

$$l(a,a) = a,\ l(a,b) = b,\ l(a,c) = c,\ l(b,a) = b,\ l(b,b) = c,\ l(b,c) = a,\ l(c,a) = c,\ l(c,b) = b,\ l(c,c) = c.$$

Définition 3.1.3 *Une loi de composition interne $\circ : M \times M \to M$ est dite*

1. *commutative, si $x \circ y = y \circ x$ pour tous $x, y \in M$,*
2. *associative, si $x \circ (y \circ z) = (x \circ y) \circ z$ pour tous $x, y, z \in M$.*

Définition 3.1.4 *Soit $(M, \circ)$ un ensemble muni d'une loi de composition interne. Un élément $e \in M$ s'appelle élément neutre (pour $\circ$) si $e \circ m = m \circ e = m$ pour tout $m \in M$.*

Exercice 3.1.5 Est-ce que la loi de composition sur $\{a,b,c\}$ définie par le tableau (7) est commutative ? Est-ce qu'elle est associative ? Est-ce qu'elle admet un élément neutre ? Si oui, lequel ?

Remarque 3.1.6 *Si un élément neutre existe, il est unique.*

Démonstration: En effet, soient e, e_1 deux éléments neutres pour la loi de composition interne $\circ$. Alors

$$e \circ e_1 = e_1\ ,\ e \circ e_1 = e\ ,$$

où d'abord on a utilisé le fait que e est élément neutre, puis le fait que e_1 est élément neutre. Donc $e = e_1$. ■

Définition 3.1.7 *Soit $(M, \circ)$ un ensemble muni d'une loi de composition interne, soit $e \in M$ un élément neutre pour $\circ$ et soit $a \in M$. Un élément symétrique de a est un élément $a' \in M$ tel que*

$$a' \circ a = a \circ a' = e$$

Remarque 3.1.8 *Supposons que $\circ$ admet un elements neutre e et est associative. Soit $a \in M$. Si a admet un élément symétrique, alors il est unique.*

Démonstration: Soient a' et a'' éléments symétriques de $a \in M$. Alors

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''.$$

■

Définition 3.1.9 *Un groupe est un couple* $(G, \circ)$*, où* $\circ$ *est une loi de composition interne sur* G *telle que :*

1. $\circ$ *est associative.*
2. $\circ$ *admet un élément neutre* $e \in G$*.*
3. *Tout élément* $a \in G$ *admet un symétrique* $a' \in G$ *par rapport à* $\circ$*.*

Si G *est fini,* $\mathrm{card}(G)$ *s'appelle l'ordre du groupe et est noté* $|G|$*.*

Souvent, dans la définition d'un groupe, on remplace la formulation "un couple $(G, \circ)$" par "un ensemble G muni d'une loi de composition interne $\circ$".

Définition 3.1.10 *Un groupe* $(G, \circ)$ *est dit commutatif (ou abélien) si* $\circ$ *est commutative, donc si* $x \circ y = y \circ x$ *pour tous les* $x, y \in G$*.*

Exemple 3.1.11 Un singleton $\{e\}$ admet une seule loi de composition interne $\circ$ et $(\{e\}, \circ)$ est évidemment un groupe abélien. Un tel groupe s'appelle groupe trivial.

Exemple 3.1.12 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{R}^n, +)$ sont des groupes abéliens.

Exemple 3.1.13 $(\{\pm 1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ sont des groupes abéliens.

Exemple 3.1.14 Soit $n \in \mathbb{N}^*$. Le couple $(\mathbb{Z}_n, +)$ est un groupe abélien. Son élément neutre est la classe $[0]_n = n\mathbb{Z}$ et l'élément symétrique d'une classe $[k]_n \in \mathbb{Z}_n$ par rapport à l'addition est la classe $[-k]_n$.

Exemple 3.1.15 Soit $n \geq 2$. Le couple $(\mathbb{Z}_n, \cdot)$ admet un élément neutre, à savoir la classe $[1]_n = 1 + n\mathbb{Z}$, mais *n'est pas un groupe*, parce que la classe $[0]_n \in \mathbb{Z}_n$ n'est pas inversible par rapport à la multiplication. Par contre, d'après la remarque 2.3.14, la multiplication $\cdot$ définit une loi de composition interne sur le sous-ensemble $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ des éléments inversibles et $(\mathbb{Z}_n^\times, \cdot)$ est un groupe. L'élément symétrique d'une classe $\xi \in \mathbb{Z}_n^\times$ par rapport à la multiplication est la classe $\eta \in \mathbb{Z}_n^\times$ qui satisfait $\xi\eta = [1]_n$. Une telle classe existe d'après la définition 2.3.10.

Exemple 3.1.16 $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ où $\mathrm{GL}(n, \mathbb{R}) := \{A \in M_{n,n}(\mathbb{R}) |\ \det(A) \neq 0\}$ est l'ensemble des matrices carrées de taille n inversibles, ensemble muni de la multiplication matricielle est un groupe, qui pour $n \geq 2$ est *non-abélien*. L'élément neutre de $\mathrm{GL}(n, \mathbb{R})$ est la matrice unité I_n d'ordre n.

Exemple 3.1.17 (*Le groupe des permutations d'un ensemble*) Soit M un ensemble. On désigne par $\mathfrak{S}(M)$ l'ensemble des applications bijectives $f : M \to M$. Si on munit cet ensemble de la loi de composition interne définie par la composition des applications bijectives, on obtient un groupe $(\mathfrak{S}(M), \circ)$ qui s'appelle *le groupe symétrique* ou *le groupe des permutations de* M. L'élément neutre de ce groupe est l'application identique id_M et l'élément symétrique d'une application $f \in \mathfrak{S}(M)$ est l'application réciproque f^{-1}.

Si M est fini de cardinal n (c'est à dire avec n éléments), alors $|\mathfrak{S}(M)| = n!$, donc un ensemble avec n éléments a $n!$ permutations.

Par exemple pour $M = \{1, 2, \ldots, n\}$ on désigne par $\mathfrak{S}_n$ (ou S_n, ou $S(n)$) le groupe des permutations de $\{1, 2, \ldots, n\}$. $\mathfrak{S}_n$ s'appelle le groupe symétrique d'indice n et un élément de $\mathfrak{S}_n$ s'appelle permutation de degré n. On a donc $|\mathfrak{S}_n| = n!$. Une permutation $\sigma \in \mathfrak{S}_n$ s'écrit sous la forme

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

où $i_s \in \{1,\dots,n\}$ désigne l'image de $s \in \{1,2,\dots,n\}$ par l'application bijective $\{1,2,\dots,n\} \to \{1,2,\dots,n\}$ considérée. Puisqu'il s'agit d'une application injective on a $i_s \neq i_t$ pour $t \neq s$. Notons que

$$\mathfrak{S}_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} .$$

$$\mathfrak{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Notons que $\mathfrak{S}_2$ est abélien, tandis que $\mathfrak{S}_n$ est non-abélien pour $n \geq 3$. Démontrer cette affirmation pour $n = 3$ et puis pour $n \geq 3$. Notons que dans la liste des éléments de $\mathfrak{S}_3$ le 2ème, 3ème et 4ème élément sont des transpositions (ou 2-cycles), i.e. des permutations qui échangent deux éléments, laissant inchangés les autres. Le 5ème et le 6ème élément de la liste sont des 3-cycles et au même temps sont des permutations circulaires de l'ensemble $\{1,2,3\}$ (voir la section 3.6).

Exemple 3.1.18 Soit $(G_1, \circ)$, $(G_2, *)$ deux groupes. On définit leur produit direct par $(G_1 \times G_2, \cdot)$ où la loi de composition interne $\cdot$ sur le produit cartésien $G_1 \times G_2$ est donnée par la formule

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2) .$$

Exercice : Montrer que $(G_1 \times G_2, \cdot)$ défini de cette manière est bien un groupe.

De la même manière on définit la produit direct $\bigtimes_{i=1}^{k} G_i$ de k groupes $G_1, \dots, G_k$.

La théorie de groupes a été introduite en mathématiques par Évariste Galois, un mathématicien français génial, qui est mort en 1832 à 20 ans, suite à un duel. Galois a développé ce concept d'une manière non-formalisée dans le cadre de son travail sur la résolubilité des équations algébriques par les radicaux. L'importance cruciale de ce travail a été reconnue quelques décennies plus tard et actuellement ce travail est considéré comme le fondement de l'algèbre moderne.

Définition 3.1.19 *Pour un élément $x \in G$ et $n \in \mathbb{Z}$ on pose :*

$$x^n := \begin{cases} \underbrace{x \circ x \circ \dots \circ x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ (x')^{|n|} & \text{si} \quad n < 0 . \end{cases}$$

En particulier on a

$$x^{-1} = x' ,$$

donc on pourra utiliser la notation x^{-1} au lieu de x'. Pour une lci en notation multiplicative ($\cdot$, $*$, $\circ$, ou juxtaposition) , le symétrique $x' = x^{-1}$ de x s'appelle aussi l'inverse de x.

Proposition 3.1.20 *(Règles de calcul dans un groupe en notation multiplicative) Soit $(G, \circ)$ un groupe.*

1. *Pour tous $x, y \in G$ on a*
$$(x \circ y)' = y' \circ x' .$$
2. *Pour tous $x \in G$, $n \in \mathbb{Z}$ on a*
$$(x^n)' = (x')^n = x^{-n} .$$
3. *Pour tous $x \in G$, $m, n \in \mathbb{Z}$ on a*
$$x^n \circ x^m = x^{n+m} .$$
4. *Pour tous $x \in G$, $m, n \in \mathbb{Z}$ on a*
$$(x^m)^n = x^{mn} .$$

Démonstration: 1. Nous vérifions que $y' \circ x'$ satisfait aux propriétés qui caractérisent l'élément symétrique de $x \circ y$. En utilisant l'associativité et la définition de l'élément symétrique, on a

$$(x \circ y) \circ (y' \circ x') = x \circ (y \circ y') \circ x' = x \circ e \circ x' = x \circ x' = e\,,$$

$$(y' \circ x') \circ (x \circ y) = y' \circ (x' \circ x) \circ y = y' \circ y = e\,.$$

Donc $y' \circ x'$ est bien l'élément symétrique de $x \circ y$.

2. On traite d'abord le cas $n \in \mathbb{N}$, puis le cas $n \in \mathbb{Z}_-$. Dans chaque cas on utilise la récurrence.

3. Pour $n \in \mathbb{Z}$ fixé soit P_n la proposition : « Pout tout $m \in \mathbb{Z}$ on a $x^n \circ x^m = x^{n+m}$ ». On démontre par récurrence que P_n est vraie pour tout $n \in \mathbb{N}$, puis on démontre par récurrence que P_{-n} est vraie pour tout $n \in \mathbb{N}$. Compléter les détails.

4. Pour $n \in \mathbb{Z}$ fixé soit P_n la proposition : "Pout tout $m \in \mathbb{Z}$ on a $(x^m)^n = x^{mn}$." On applique la même méthode que celle utilisée pour démontrer 3. ■

Remarque 3.1.21 *Si la loi de composition interne d'un groupe est notée additivement (par +), alors on utilise la notation nx au lieu de x^n. On va poser alors*

$$nx := \begin{cases} \underbrace{x + x + \ldots + x}_{n \text{ fois}} & \text{si} \quad n > 0 \\ e & \text{si} \quad n = 0 \\ |n|x' & \text{si} \quad n < 0\,. \end{cases}$$

En particulier on aura $(-1)x = x'$ donc, pour une lci de groupe en notation additive, on pourra utiliser la notation $-x$ au lieu de x'.

Reformuler les règles de calcul dans un groupe $(G, +)$ en utilisant la notation additive nx. La notation additive + est réservée aux lois de composition internes commutatives.

3.2 Homomorphismes, monomorphismes, épimorphismes de groupes. Sous-groupes. Le noyau et l'image d'un morphisme

Définition 3.2.1 *Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes. Une application $f : G \to \tilde{G}$ est dite homomorphisme (morphisme) de groupes si*

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

Un morphisme f est dit monomorphisme s'il est injectif, est dit épimorphisme s'il est surjectif et est dit isomorphisme s'il est bijectif. Si f est un isomorphisme, l'application réciproque f^{-1} sera aussi un isomorphisme. Deux groupes $(G, \circ)$, $(\tilde{G}, *)$ sont dits isomorphes s'il existe un isomorphisme $f : G \to \tilde{G}$.

Deux groupes isomorphes ont les mêmes propriétés algébriques, donc ils sont algébriquement équivalents. Par exemple si l'un est abélien, l'autre sera aussi abélien.

Notons aussi que toute composition de deux morphismes (monomorphismes, épimorphismes, isomorphismes) est aussi un morphisme (respectivement monomorphisme, épimorphisme, isomorphisme). Démontrer ces affirmations.

Exemple 3.2.2 L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

Exemple 3.2.3 Soient $n_1, \ldots, n_k \in \mathbb{N}^*$ et soit $n := \prod_{i=1}^k n_i$. L'application

$$f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i},\ f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

(qui intervient dans le théorème des restes chinois) est un morphisme de groupes *additifs*, qui induit un morphisme de groupes *multiplicatifs* $h : \mathbb{Z}_n^\times \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}^\times$. Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors f et h sont des isomorphismes.

Remarque 3.2.4 *Soient $(G,\circ)$, $(\tilde{G},*)$ deux groupes et soient e, $\tilde{e}$ leurs éléments neutres respectivement. Soit $f : G \to \tilde{G}$ un homomorphisme de groupes. Alors*

1. $f(e) = \tilde{e}$,
2. *Pour tout $x \in G$ on a $f(x') = (f(x))'$.*
3. *Pour tout $x \in G$ et $k \in \mathbb{Z}$ on a $f(x^k) = f(x)^k$.*

Démonstration: En effet, f étant un morphisme de groupes on a $f(e) = f(e \circ e) = f(e) * f(e)$. En composant les deux membres par l'élément symétrique $f(e)'$ de $f(e)$ et en utilisant l'associativité de $*$ on obtient $f(e) = e'$. En plus $f(x') * f(x) = f(x \circ x') = f(e) = e'$, donc (en composant à droite les deux membres par $f(x)'$), on obtient bien $f(x') = (f(x))'$. Pour la 3ème affirmation, on considère deux cas :

(a) $k \in \mathbb{N}$,

(b) $-k \in \mathbb{N}^*$.

Dans chaque cas on utilise la récurrence. ■

Définition 3.2.5 *Soit $(G,\circ)$ un groupe. Un sous-ensemble $H \subset G$ s'appelle sous-groupe si les deux conditions suivantes sont vérifiées :*

1. $H \neq \emptyset$,
2. *pour tous les $x, y \in H$ on a $x \circ y' \in H$.*

Il existe une autre manière (équivalente) de définir la notion de sous-groupe :

Proposition 3.2.6 *$H \subset G$ est un sous-groupe si et seulement si les trois conditions suivantes sont vérifiées :*

1. $e \in H$,
2. *pour tous les $x, y \in H$ on a $x \circ y \in H$,*
3. *pour tout $x \in H$ on a $x' \in H$.*

Démonstration: Exercice. ■

En utilisant la proposition 3.2.6 et la définition 3.1.19 on obtient facilement :

Remarque 3.2.7 *Soit $H \subset G$ un sous-groupe et soit $x \in H$. Alors pour tout $k \in \mathbb{Z}$ on a $x^k \in H$.*

La proposition 3.2.6 montre aussi que, si H est un sous-groupe, alors la restriction

$$\circ|_{H \times H} : H \times H \to H$$

de $\circ$ à $H \times H$ définit une loi de composition *interne* sur H et, muni de cette loi de composition de interne, H devient lui-même un groupe (avec le même élément neutre e que celui de $(G,\circ)$). En plus, pour $x \in H$ l'élément symétrique de x dans le groupe $(H, \circ|_{H \times H})$ coïncide avec son élément symétrique dans le groupe de départ $(G,\circ)$.

Exemples : Soit $(G,*)$ un groupe. Alors $\{e\}$, G sont sous-groupes de $(G,*)$. $\{e\}$ s'appelle le sous-groupe trivial de $(G,*)$.
2. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \subset \mathbb{Z}$ est sous-groupe de $(\mathbb{Z},+)$. On peut montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.
3. Les inclusion $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes (par rapport à l'addition).
4. Les inclusion $\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des inclusions de sous-groupes (par rapport à la multiplication).
5. Soient $\mathrm{U} := \{z \in \mathbb{C} |\ |z| = 1\}$, $\mathrm{U}_n := \{z \in \mathbb{C} |\ z^n = 1\}$. Alors les inclusions $\mathrm{U}_n \subset \mathrm{U} \subset \mathbb{C}^*$ sont des inclusions de sous-groupe par rapport à la multiplication.

Définition 3.2.8 *Soit $(G,\circ)$ un groupe. Un sous-groupe $H \subset G$ est dit sous-groupe normal (ou distingué) si pour tout $x \in G$ et tout $h \in H$ on a $x \circ h \circ x' \in H$.*

La condition "pour tout $x \in G$ et tout $h \in H$ on a $x \circ h \circ x' \in H$" peut être reformulée de la manière suivante : pour tout $x \in G$ on a $x \circ H \circ x' \subset H$. Ici on a utilisé la notation

$$x \circ H \circ y := \{x \circ h \circ y |\ h \in H\}\ .$$

Remarque 3.2.9 *Si $H \subset G$ est un sous-groupe normal (distingué), alors pour tout $x \in G$ on a $x \circ H \circ x' = H$.*

Démonstration: Soit $x \in G$. Puisque H est normal on a $x \circ H \circ x' \subset H$, donc il suffit de montrer l'inclusion inverse $H \subset x \circ H \circ x'$. Mais cette inclusion est équivalente à $(x') \circ H \circ (x')' \subset H$ (qui est vraie, parce que H est normal et $x' \in G$). ■

Exemples : 1. $\{e\}$ est G sont sous-groupes normaux de $(G, *)$.
2. Si $(G, *)$ est un groupe abélien, alors tout sous-groupe de $(G, *)$ est normal (à justifier).
3. Le sous-ensemble

$$\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) |\ \det(A) = 1\}$$

est un sous-groupe normal de $(\mathrm{GL}(n, \mathbb{R}), \cdot)$. En effet, pour un couple $(B, A) \in \mathrm{GL}(n, \mathbb{R}) \times \mathrm{GL}(n, \mathbb{R})$ on a $\det(BAB^{-1}) = \det(A)$, donc $BAB^{-1} \in \mathrm{SL}(n, \mathbb{R})$ si $A \in \mathrm{SL}(n, \mathbb{R})$.
4. Soit $(\mathfrak{S}_n, \circ)$ le groupe symétrique de degré n et

$$\mathrm{A}_n := \{\sigma \in \mathfrak{S}_n |\ \varepsilon(\sigma) = 1\} \subset \mathfrak{S}_n$$

le sous-ensemble des permutations paires (de signature +1). A_n est un sous-groupe normal de $(\mathfrak{S}_n, \circ)$. En effet, pour un couple $(\sigma, \eta) \in \mathfrak{S}_n \times \mathfrak{S}_n$ on a $\varepsilon(\sigma \circ \eta \circ \sigma^{-1}) = \varepsilon(\eta)$, donc $\sigma \circ \eta \circ \sigma^{-1} \in \mathrm{A}_n$ si $\eta \in \mathrm{A}_n$.
5. Le sous-ensemble $H := \left\{\mathrm{id}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$ est un sous-groupe de $\mathfrak{S}_3$, mais ce sous-groupe n'est pas normal. En effet, en posant $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, on a $\sigma \circ \tau \circ \sigma^{-1} \notin H$.
6. Le centre d'un groupe $(G, \circ)$ est défini par

$$Z(G) := \{x \in G |\ \forall y \in G,\ x \circ y = y \circ x\}.$$

$Z(G)$ est un sous-groupe normal et abélien de G. Il coïncide avec G si $(G, \circ)$ est abélien. Quel est le centre de $\mathfrak{S}_3$?

Définition 3.2.10 *Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes avec éléments neutres $e \in G$, $\tilde{e} \in \tilde{G}$ et soit $f : G \to \tilde{G}$ un homomorphisme de groupes. On pose*

$$\ker(f) := \{x \in G |\ f(x) = \tilde{e}\} = f^{-1}(\{\tilde{e}\})\ ,\ \mathrm{im}(f) := \{y \in \tilde{G} |\ \exists x \in G, y = f(x)\}\ .$$

Remarque 3.2.11 *Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes avec éléments neutres $e \in G$, $\tilde{e} \in \tilde{G}$ et $f : G \to \tilde{G}$ un homomorphisme de groupes.*

1. $\mathrm{im}(f)$ *est un sous-groupe de $\tilde{G}$.*
2. $\ker(f)$ *est un sous-groupe normal de G.*
3. *Le sous-groupe* $\mathrm{im}(f) \subset \tilde{G}$ *est abélien si G est abélien.*
4. *f est un monomorphisme si et seulement si* $\ker(f) = \{e\}$.
5. *f est un épimorphisme si et seulement si* $\mathrm{im}(f) = \tilde{G}$.

Démonstration: Exercice. ■

Exercice 3.2.12 L'application exponentielle $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme de $(\mathbb{R}, +)$ à $(\mathbb{R}_+^*, \cdot)$. Remarquer que $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \cdot)$.

Exercice 3.2.13 Soient $f : G \to G'$, $g : G' \to G''$ homomorphismes de groupes. Montrer que

$$\ker(f) \subset \ker(g \circ f),\ \mathrm{im}(g \circ f) \subset \mathrm{im}(g).$$

Remarque 3.2.14 *Soient $(G, \circ)$, $(\tilde{G}, *)$ deux groupes et soit $f : G \to \tilde{G}$ un homomorphisme de groupes . Alors*

1. *Pour tout sous-groupe $H \subset G$ l'image $f(H) := \{f(x) |\ x \in H\}$ est un sous-groupe de $(\tilde{G}, *)$.*
2. *Pour tout sous-groupe $\tilde{H} \subset \tilde{G}$ l'image réciproque $f^{-1}(\tilde{H}) := \{x \in G |\ f(x) \in \tilde{H}\}$ est un sous-groupe de $(G, \circ)$. Ce sous-groupe est normal si $\tilde{H}$ est normal.*

En prenant $H = G$ (respectivement $\tilde{H} = \{\tilde{e}\}$) on obtient comme cas particuliers les sous-groupes $\mathrm{im}(f) \subset \tilde{G}$ (respectivement $\ker(f) \subset G$) définis ci-dessus.

Exercice 3.2.15 Soient $f : G \to \tilde{G}$ un morphisme et $H \subset G$ un sous-groupe. Si H est normal et f est surjective alors $f(H)$ est normal .

3.3 Le sous-groupe cyclique engendré par un élément. L'ordre d'un élément

Soit $(G, \circ)$ un groupe, e son élément neutre.

Définition 3.3.1 *Soit $x \in G$. On dit que x est un élément de torsion ou un élément d'ordre fini s'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$. Si c'est le cas, alors on définit l'ordre de x par*

$$\mathrm{ord}(x) := \min\{k \in \mathbb{N}^* |\ x^k = e\}\ .$$

Si l'ensemble $\{k \in \mathbb{N}^* |\ x^k = e\}$ est vide, on dira que x est un élément d'ordre infini.

Exemples 3.3.2

1. L'ordre de i dans le groupe $(\mathbb{C}^*, \cdot)$ est 4.
2. Le nombre complexe $2i$ est un élément d'ordre infini dans le groupe $(\mathbb{C}^*, \cdot)$.
3. La permutation $(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_3$ est un 3-cycle, donc un élément d'ordre 3 dans le groupe symétrique $(\mathfrak{S}_3, \circ)$.

Justifier ces affirmations.

Définition 3.3.3 *Soit $x \in G$. Le sous-groupe cyclique (monogène) engendré par x est défini par*

$$\langle x \rangle := \{x^k |\ k \in \mathbb{Z}\} = \{y \in G |\ \exists k \in \mathbb{Z},\ y = x^k\}.$$

Remarque 3.3.4 *Soit $x \in G$. Alors*

1. *$\langle x \rangle$ est bien un sous-groupe de $(G, \circ)$. Ce sous-groupe est abélien.*
2. *$\langle x \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) qui contient x. Plus précisément, pour tout sous-groupe $H \subset G$ tel que $x \in H$, on a $\langle x \rangle \subset H$.*

Démonstration: Exercice. Pour la première affirmation utiliser la proposition 3.1.20 et pour la deuxième utiliser la remarque 3.2.7. ■

On peut définir le sous-groupe cyclique engendré par x de la manière équivalente suivante. Soit $f_x : \mathbb{Z} \to G$ l'application définie par

$$F_x(k) := x^k\ .$$

Remarquer que (en munissant $\mathbb{Z}$ de la structure de groupe définie par l'addition) F_x est un homomorphisme de groupes. (Pourquoi ? Démontrer soigneusement cette affirmation). On a évidemment

$$\langle x \rangle = \mathrm{im}(F_x)\ , \tag{8}$$

ce qui (d'après la remarque 3.2.11) montre d'une nouvelle manière que $\langle x \rangle$ est un sous-groupe abélien de $(G, \circ)$.

Proposition 3.3.5 *Soit $x \in G$ un élément d'ordre fini n. Alors*

1. $\ker(F_x) = n\mathbb{Z}$.
2. *F_x est compatible avec la relation d'équivalence $\underset{n}{\equiv}$ sur $\mathbb{Z}$.*
   En particulier F_x induit une application $f_x : \mathbb{Z}_n \to G$ donnée par
   $$f_x([k]_n) = F_x(k) = x^k.$$
3. *f_x est un monomorphisme $(\mathbb{Z}_n, +) \to (G, +)$ et son image est $\langle x \rangle$, donc (par restriction au but) f_x induit un isomorphisme*
   $$g_x : \mathbb{Z}_n \xrightarrow{\simeq} \langle x \rangle.$$
4. *Les éléments $e, x, \ldots, x^{n-1}$ sont distincts deux à deux, $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ et $|\langle x \rangle| = n$.*

La proposition 3.3.5 nous précise explicitement le sous-ensemble $\langle x \rangle \subset G$ et affirme que le groupe $\langle x \rangle$ est isomorphe à $\mathbb{Z}_n$.

Démonstration: 1. : Soit $k \in \mathbb{Z}$. En appliquant le théorème de division euclidienne on obtient un couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que
$$k = qn + r,\ 0 \leq r \leq n-1,$$
d'où
$$x^k = x^{nq+r} = x^{nq} \circ x^r = (x^n)^q \circ x^r = e^q \circ x^r = e \circ x^r = x^r.$$
Il en résulte :
$$k \in \ker(f_x) \Leftrightarrow x^k = e \Leftrightarrow x^r = e \Leftrightarrow r = 0. \tag{9}$$

Nous devons justifier l'implication $x^r = e \Rightarrow r = 0$: Si, par l'absurde, $r > 0$, r sera un élément de $\mathbb{N}^*$ strictement inférieur à n tel que $x^r = e$, ce qui contredit la définition de $n = \mathrm{ord}(x)$.

L'équivalence (9) montre que
$$k \in \ker(F_x) \Leftrightarrow (r = 0) \Leftrightarrow k \in n\mathbb{Z},$$
donc $\ker(F_x) = n\mathbb{Z}$.

2. Montrons que F_x est compatible avec $\underset{n}{\equiv}$. Nous avons les équivalences :
$$u \underset{n}{\equiv} v \Leftrightarrow n|(v-u) \Leftrightarrow v - u \in n\mathbb{Z} = \ker(F_x) \Leftrightarrow F_x(v-u) = e \Leftrightarrow F_x(v) \circ F_x(u)' = e \Leftrightarrow F_x(u) = F_x(v), \tag{10}$$
en particulier $u \underset{n}{\equiv} v \Rightarrow F_x(u) = F_x(v)$, donc F_x est compatible avec $\underset{n}{\equiv}$.

3. Montrons que l'application $f_x : \mathbb{Z}_n \to G$ induite par F_x est injective. Soient $[u]_n, [v]_n \in \mathbb{Z}_n$. Nous avons
$$f_x([u]_n) = f_x([v]_n) \Leftrightarrow F_x(u) = F_x(v) \Leftrightarrow u \underset{n}{\equiv} v \Leftrightarrow [u]_n = [v]_n,$$
ce qui démontre l'injectivité de f_x. Montrons que f_x est morphisme de groupes :
$$f_x([u]_n + [v]_n) = f_x([u+v]_n) = F_x(u+v) = F_x(u) \circ F_x(v)$$
$$= f_x([u]_n) \circ f_x([v]_n).$$
Nous avons obtenu un monomorphisme $f_x : \mathbb{Z}_n \to G$ dont l'image est $\langle x \rangle$. Par restriction au but (corestriction), on obtient un isomorphisme $g_x : \mathbb{Z}_n \to \langle x \rangle$.

4. Conséquence directe de (3). ■

Remarque 3.3.6 *Soit $x \in G$ un élément d'ordre infini. Alors* $\ker(F_x) = \{0\}$, *donc $F_x : \mathbb{Z} \to G$ est un monomorphisme. Par restriction au but on obtient un isomorphisme $g_x : \mathbb{Z} \xrightarrow{\simeq} \langle x \rangle$.*

Conclusion: Le sous-groupe cyclique $\langle x \rangle$ engendré par x est isomorphe à $\mathbb{Z}_n$ si x est un élément d'ordre fini n et est isomorphe à $\mathbb{Z}$ si x est un élément d'ordre infini.

Définition 3.3.7 *Un groupe $(G,\circ)$ est dit groupe cyclique (ou monogène) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Si c'est le cas, on dira que x est un générateur de G ou que G est engendré par x.*

Définition équivalente : $(G,\circ)$ est un groupe cyclique (ou monogène) de générateur $x \in G$ si le morphisme $F_x : \mathbb{Z} \to G$ est un épimorphisme.

Exemple 3.3.8 Soit $n \in \mathbb{N}^*$. Le groupe $(\mathrm{U}_n,\cdot)$ est cyclique engendré par $e^{\frac{2\pi i}{n}}$.

Remarque 3.3.9 *Tout groupe cyclique fini d'ordre n est isomorphe à $\mathbb{Z}_n$. Tout groupe cyclique infini est isomorphe à $\mathbb{Z}$. En particulier tout groupe cyclique est abélien.*

Pour un groupe muni d'une lci en notation additive les notations utilisées dans les définitions introduites dans cette section changent :

Remarque 3.3.10 *Soit $(G,+)$ un groupe en notation additive et soit $x \in G$. Alors :*

1. *l'homomorphisme $F_x : \mathbb{Z} \to G$ associée à x s'écrit $F_x(k) = kx$.*
2. *x est d'ordre fini (de torsion) s'il existe $k \in \mathbb{N}^*$ tel que $kx = e$.*
3. *Si x est d'ordre fini, alors* $\mathrm{ord}(x) := \min\{k \in \mathbb{N}^* |\ kx = e\}$.
4. *Le sous-groupe cyclique engendré par x est $\langle x \rangle = \{kx |\ k \in \mathbb{Z}\} = \{y \in G |\ \exists k \in \mathbb{Z},\ y = kx\}$.*
5. *Si* $\mathrm{ord}(x) = n$, *alors* $\langle x \rangle = \{e, x, \ldots, (n-1)x\}$.

Exemples 3.3.11
1. $(\mathbb{Z}_n,+)$ est un groupe cyclique d'ordre n engendré par $[1]_n$.
2. $(\mathbb{Z},+)$ est un groupe cyclique infini engendré par 1.
3. Soit $n \in \mathbb{N}^*$. $(n\mathbb{Z},+)$ est un groupe cyclique infini engendré par n.

Exemple 3.3.12 Considérons le groupe $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},+)$ où $n_1, \ldots, n_k \in \mathbb{N}^*$. En général ce groupe produit n'est pas cyclique. Par exemple dans $\mathbb{Z}_2 \times \mathbb{Z}_2$ tout élément est d'ordre ≤ 2 donc n'engendre pas $\mathbb{Z}_2 \times \mathbb{Z}_2$. Par contre, si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, le théorème des restes chinois (le théorème 2.4.3 complété par l'exemple 3.2.2) fournit un isomorphisme $f : \mathbb{Z}_n \to \bigtimes_{i=1}^k \mathbb{Z}_{n_i}$ où $n = \prod_{i=1}^n n_i$. Puisque $(\mathbb{Z}_n,+)$ est cyclique engendré par $[1]_n$, il en résulte que $(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},+)$ engendré par $f([1]_n) = ([1]_{n_1}, \ldots, [1]_{n_k})$.

3.4 Relations d'équivalence suivant un sous-groupe. Le théorème de Lagrange. Groupe quotient par un sous-groupe distingué. Le premier théorème d'isomorphisme

Soit $(G,\circ)$ un groupe et $H \subset G$ un sous-groupe. On va écrire xy au lieu de $x \circ y$ pour simplifier les notations.

Définition 3.4.1 *Nous associons à H deux relations R_H, ${}_HR$ sur G définies par :*

1. *$x\ R_H\ y$ si $x'y \in H$*
2. *$x\ {}_HR\ y$ si $xy' \in H$*

La proposition suivante montre que R_H, ${}_HR$ sont des relations d'équivalence et précise les classes d'équivalence d'un élément $x \in G$ par rapport à ces relations.

Proposition 3.4.2
1. *R_H, ${}_HR$ sont des relations d'équivalence sur G.*
2. *La classe d'équivalence $[x]_H$ de x par rapport à R_H est*

$$[x]_H = xH := \{xh |\ h \in H\}\ .$$

3. *La classe d'équivalence ${}_H[x]$ de x par rapport à ${}_HR$ est*

$${}_H[x] = Hx := \{hx |\ h \in H\}\ .$$

Démonstration: La classe d'équivalence de x par rapport à R_H est par définition

$$[x]_H = \{y \in G |\ x\ R_H\ y\} = \{y \in G |\ x'y \in H\} = \{y \in G |\ \exists h \in H,\ x'y = h\} = \{y \in G |\ \exists h \in H,\ y = xh\} = xH.$$

Argument similaire pour ${}_H[x]$. Exercice. ■

Remarquer que la classe de l'élément neutre e (par rapport à R_H ou ${}_HR$) est H.

Définition 3.4.3 *R_H (respectivement ${}_HR$) s'appelle la relation d'équivalence (de congruence) à gauche (respectivement à droite) suivant H, ou modulo H. Les classes d'équivalence par rapport à R_H (respectivement ${}_HR$) s'appellent classes d'équivalence (ou de congruence) à gauche (respectivement à droite) suivant H.*

La terminologie "à gauche","à droite" est justifiée par la remarque suivante :

Remarque 3.4.4 *Soit $u \in G$. Alors*

1. *$x\ R_H\ y$ si et seulement si $(ux)\ R_H\ (uy)$. Cette propriété montre que la relation d'équivalence R_H est compatible à gauche avec la loi de composition interne de G.*
2. *$x\ {}_HR\ y$ si et seulement si $(xu)\ {}_HR\ (yu)$. Cette propriété montre que la relation d'équivalence ${}_HR$ est compatible à droite avec la loi de composition interne de G.*

Rappelons que, par définition, on dit que deux ensembles A, B *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 3.4.5 *Soient $H \subset G$ un sous-groupe et $x \in G$. Les applications $l_x : H \to xH$, $r_x : H \to Hx$ définies par*

$$l_x(h) = xh,\ r_x(h) = hx$$

sont bijectives. En particulier toutes les classes d'équivalence à gauche (ou à droite) suivant H ont le même cardinal.

Démonstration: Nous vérifions que l_x est injective, donc soient $h_1, h_2 \in H$ tels que $l_x(h_1) = l_x(h_2)$. On a donc $xh_1 = xh_2$ et en appliquant x^{-1} aux deux membres on obtient $h_1 = h_2$. Pour vérifier que l_x est surjective, soit $y \in xH$. Par la définition de xH, il existe $h \in H$ tel que $y = xh = l_x(h)$, ce qui montre que l_x est surjective. La bijectivité de r_x est proposée comme exercice ■

Les ensembles quotient G/R_H, $G/{}_HR$ sont notés dans la littérature mathématique :

$$G/H := G/R_H,\ H\backslash G := G/{}_HR.$$

En général ces ensembles quotient ne sont pas munis naturellement d'une structure de groupe. On va voir que, si H est un sous-groupe distingué, alors $R_H = {}_HR$ et $G/R_H = G/{}_HR$ aura une structure naturelle de groupe. Pour éviter toute confusion avec le groupe quotient associé à un sous-groupe distingué, on va utiliser les notations G/R_H, $G/{}_HR$ au lieu de G/H, $H\backslash G$.

Remarque 3.4.6 *Soit $H \subset G$ un sous-groupe et soient R_H, ${}_HR$ les relations de congruence à gauche, respectivement à droite suivant H. Alors les ensembles quotient G/R_H, $G/{}_HR$ ont le même cardinal.*

Démonstration: L'application $\iota : G \to G$ donnée par $x \mapsto x^{-1}$ est une bijection, qui induit une bijection $\bar{\iota} : G/R_H \to G/{}_HR$, donnée explicitement par $\bar{\iota}(xH) = Hx^{-1}$. Démontrer que $\bar{\iota}$ est bien définie et bijective. ■

Cette remarque est vraie en toute généralité, sans supposer que G, H, $|G/R_H|$, ou $|G/{}_HR|$ soit fini.

Définition 3.4.7 *Soit $H \subset G$ un sous-groupe et soient R_H, ${}_HR$ les relations de congruence à gauche, respectivement à droite suivant H. Supposons que l'ensemble G/R_H (ou, de manière équivalente, l'ensemble $G/{}_HR$) est fini. Le cardinal $|G/R_H| = |G/{}_HR|$ s'appelle l'indice de H dans G et est désigné par $|G : H|$.*

Théorème 3.4.8 (le théorème de Lagrange) *Soit $(G,\circ)$ un groupe fini et soit $H \subset G$ un sous-groupe. Alors*

$$|G| = |H| \cdot |G : H|.$$

On va utiliser un lemme élémentaire :

Lemme 3.4.9 (Lemme des bergers) — *Soient $k, l \in \mathbb{N}^*$ et soit M un ensemble qui possède une partition en k sous-ensembles, chacun de cardinal l. Alors $|M| = kl$.*

Démonstration: (du théorème de Lagrange) On va appliquer le lemme des bergers à la partition de G définie par les classes d'équivalence par rapport à R_H ($_HR$).

D'après la proposition 3.4.5 toutes ces classes ont le même cardinal $|H|$ et le nombre des classes d'équivalence par rapport à R_H ($_HR$) est $|G/R_H|$ (respectivement $|G/_HR|$). Il suffit de tenir compte que $|G/R_H| = |G/_HR| = |G : H|$. ■

Remarque 3.4.10 *Le théorème de Lagrange est vrai même en toute généralité, même si G est infini. Pour cette généralisation on a besoin de la généralisation du produit pour les nombres cardinaux infinis.*

Corollaire 3.4.11 *Soit $(G,\circ)$ un groupe fini, $H \subset G$ un sous-groupe. Alors $|H|$ est un diviseur de $|G|$.*

Corollaire 3.4.12 *Soit $(G,\circ)$ un groupe fini et soit $x \in G$. Alors*

1. $\mathrm{ord}(x)$ *est un diviseur de* $|G|$.
2. *Pour tout $x \in G$ on a $x^{|G|} = e$.*

Démonstration: 1. En effet, on a $\mathrm{ord}(x) = |\langle x\rangle|$, donc $\mathrm{ord}(x)$ est un diviseur de $|G|$ d'après le corollaire 3.4.11.

2. Soit $k := \mathrm{ord}(x)$. Puisque $k \| |G|$ il existe $l \in \mathbb{N}$ tel que $|G| = kl$. Alors $x^{|G|} = x^{kl} = (x^k)^l = e^l = e$. ■

Corollaire 3.4.13 *Soit $(G,\circ)$ un groupe fini dont l'ordre $|G|$ est un nombre premier p. Alors G est un groupe cyclique d'ordre p, en particulier il est isomorphe à $\mathbb{Z}_p$.*

Démonstration: Rappelons que, par définition, un nombre premier est un entier naturel $p \geq 2$ qui admet exactement deux diviseurs dans $\mathbb{N}^*$, à savoir 1 et p. Il en résulte $p = |G| \geq 2$. Soit $x \in G \setminus \{e\}$. Alors $\mathrm{ord}(x) \geq 2$. D'après le corollaire 3.4.12 $\mathrm{ord}(x)$ est un diviseur de p. Puisque ce diviseur est strictement supérieur à 1 et p est un nombre premier, il en résulte $\mathrm{ord}(x) = p$, donc $|\langle x\rangle| = p = |G|$. Puisque $\langle x\rangle$ est un sous-groupe de G, il en résulte $\langle x\rangle = G$. ■

Corollaire 3.4.14 (Le petit théorème de Fermat) *Si $p \geq 2$ est un nombre premier et $a \in \mathbb{Z}$ n'est pas divisible par p, alors*

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

Démonstration: D'après la proposition 2.3.11 on a $[a]_p \in \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]_p\}$ et l'ordre du groupe multiplicatif $\mathbb{Z}_p^\times$ est $p-1$. Il suffit d'appliquer le corollaire 3.4.12 au groupe $\mathbb{Z}_p^\times$ et à l'élément $[a]_p$ de ce groupe. ■

Corollaire 3.4.15 (le théorème de Euler) *Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premier avec n. Alors*

$$a^{\varphi(n)} \equiv 1 \ (mod)\ n$$

où $\varphi : \mathbb{N}^* \to \mathbb{N}$ désigne la fonction indicatrice d'Euler définie par

$$\varphi(n) := |\mathbb{Z}_n^\times| = \left|\left\{k \in \{1,\dots,n\},\ \mathrm{pgcd}(k,n) = 1\right\}\right|.$$

Démonstration: Exercice. Utiliser la même méthode que pour la démonstration du corollaire 3.4.14. Remarquer d'abord que $|\mathbb{Z}_n^\times| = \varphi(n)$. ■

Proposition 3.4.16 *Soit $(G,\circ)$ un groupe, $H \subset G$ un sous-groupe et soient R_H, ${}_HR$ les relations d'équivalence associées à H. Si H distingué, alors*

1. $R_H = {}_HR$,
2. *La formule $[x]_{R_H} \cdot [y]_{R_H} := [x \circ y]_{R_H}$ définit une structure de groupe sur $G/H := G/R_H = G/{}_HR$.*

Démonstration: 1. On va écrire xy au lieu de $x \circ y$ pour simplifier les notations. Soient $x, y \in G$. On a

$$x \, R_H \, y \Rightarrow x'y \in H \Rightarrow \exists h \in H \text{ tel que } x'y = h$$

Mais $x'y = h$ implique $y = xh$, donc $y' = h'x'$, d'où $xy' = xh'x'$. Mais $xh'x' \in H$ parce que $h' \in H$ et H est distingué. On a obtenu $xy' \in H$, donc $x \, {}_HR \, y$. L'implication $x \, {}_HR \, y \Rightarrow x \, R_H \, y$ est proposée comme exercice.

2. Nous devons démontrer que la définition de $\cdot$ est cohérente, donc que $[xy]_{R_H}$ dépend seulement des classes d'équivalence $[x]_{R_H}$, $[y]_{R_H}$. Soient donc $\tilde{x}$, $\tilde{y} \in G$ tels que $\tilde{x} \, R_H \, x$ et $\tilde{y} \, R_H \, y$. On a donc $\tilde{x}'x \in H$, $\tilde{y}'y \in H$. Soient donc h, $\chi \in H$ tels que $\tilde{x}'x = h$, $\tilde{y}'y = \chi$. Alors

$$(\tilde{x}\tilde{y})'(xy) = \tilde{y}'\tilde{x}'xy = (\chi y')(hx')(xy) = \chi(y'hy) \in H,$$

parce que $\chi \in H$ et (H étant distingué) $y'hy \in H$. Donc $(\tilde{x}\tilde{y}) \, R_H \, (xy)$, ce qui démontre que la classe d'équivalence $[x \circ y]_{R_H}$ dépend seulement des classes d'équivalence $[x]_{R_H}$, $[y]_{R_H}$, donc $\cdot$ est bien définie.

C'est très facile de démontrer que la loi de composition interne $\cdot$ sur G/R_H vérifie les axiomes du groupe. En effet, l'associativité de $\cdot$ résulte facilement de l'associativité de $\circ$. En plus on vérifie facilement que $[e]_{R_H} = H$ est élément neutre pour $\cdot$ et que $[x']_{R_H}$ est un élément symétrique de $[x]_{R_H}$. ■

Pour un sous-groupe distingué H la relation $R_H = {}_HR$ s'appelle relation d'équivalence (de congruence) suivant H. Aucune précision "à gauche" ou "à droite" n'est nécessaire dans ce cas. On va désigner par $[x]_H$ ou $[x]$ (si H est sous-entendu) la classe d'équivalence de x suivant H.

Définition 3.4.17 *Soit $(G,\circ)$ un groupe, $H \subset G$ un sous-groupe distingué. Le groupe quotient de G par H est le groupe $(G/H,\cdot)$, où $G/H := G/R_H$ et $\cdot$ est la loi de composition interne définie par*

$$[x] \cdot [y] := [x \circ y] \, .$$

L'épimorphisme canonique associé à H est l'épimorphisme $p_H : G \to G/H$ défini par $p(x) := [x]$.

Remarque 3.4.18 *L'application p_H est un épimorphisme avec* $\ker(p_H) = H$.

Démonstration: Exercice. ■

Exemple 3.4.19 Dans un groupe abélien tout sous-groupe est un sous-groupe distingué. En particulier $n\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$. Remarquer que le groupe $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ s'identifie au quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$ dans le sens de la théorie générale des groupe quotients. Donc construction d'un groupe quotient par un sous-groupe distingué généralise la construction des groupes $\mathbb{Z}/n/Z$.

Théorème 3.4.20 *[Propriété universelle du groupe quotient] Soient $(G,\cdot)$, $(\tilde{G},*)$ groupes, $H \subset G$ un sous-groupe distingué, $p_H : G \to G/H$ l'épimorphisme canonique associé à H et $f : G \to \tilde{G}$ un homomorphisme. Alors*

1. *Il existe un homomorphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$ si et seulement si $H \subset \ker(f)$.*
2. *Si cette condition est vérifiée, alors*
   (a) *$\bar{f}$ est unique,* $\ker(\bar{f}) = \ker(f)/H$ *et* $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$,
   (b) *$\bar{f}$ est un monomorphisme si et seulement si* $H = \ker(f)$,
   (c) *$\bar{f}$ est un épimorphisme si et seulement si f est un épimorphisme.*

$$\begin{array}{ccc} G & \xrightarrow{f} & \tilde{G} \\ {\scriptstyle p_H}\downarrow & \nearrow_{\bar{f}} & \\ G/H & & \end{array} \tag{11}$$

Démonstration:

1. Supposons qu'il existe un homomorphisme $\bar{f} : G/H \to \tilde{G}$ tel que $\bar{f} \circ p_H = f$. En utilisant la remarque 3.4.18 il en résulte $H = \ker(p_H) \subset \ker(\bar{f} \circ p_H) = \ker(f)$. Réciproquement, si $H \subset \ker(f)$ alors la formule $\bar{f}([x]) = f(x)$ définit (d'une manière cohérente !) un homomorphisme $\bar{f} : G/H \to \tilde{G}$. On aura alors

$$\forall x \in G\ (\bar{f} \circ p_H)(x) = \bar{f}(p_H(x)) = \bar{f}([x]) = f(x)\ ,$$

donc on a bien $\bar{f} \circ p_H = f$.

2.(a) La condition $\bar{f} \circ p_H = f$ est équivalente à

$$\forall x \in G\ \bar{f}([x]) = f(x)\ ,$$

donc pour $\bar{f}$ on a une seule possibilité. Pour la deuxième affirmation désignons par $\tilde{e}$ l'élément neutre de $\tilde{G}$ et remarquons que H est un sous-groupe distingué de $\ker(f)$, donc le groupe quotient $\ker(f)/H$ est défini. On a

$$\ker(\bar{f}) = \left\{[x] \in\ G/H |\ \bar{f}([x]) = \tilde{e}\right\} = \left\{[x] \in G/H |\ f(x) = \tilde{e}\right\} = \left\{[x] \in\ G/H |\ x \in \ker(f)\right\} = \ker(f)/H\ .$$

Pour démontrer la troisième affirmation remarquer que $\mathrm{im}(f) = \mathrm{im}(\bar{f} \circ p_H) = \mathrm{im}(\bar{f})$ où, pour la deuxième égalité on a utilisé la surjectivité de p_H.

2.(b) $\bar{f}$ est un monomorphisme si et seulement si $\ker(\bar{f})$ est trivial, donc si et seulement si le groupe quotient $\ker(f)/H$ est trivial, donc si et seulement si $\ker f$ contient une seule classe d'équivalence suivant H (i.e si et seulement si $\ker(f) = H$).

2.(c) Utiliser la troisième affirmation de 2(a). ■

Exemple 3.4.21 Soient $m, n \in \mathbb{N}^*$ et $p : \mathbb{Z} \to \mathbb{Z}_m$, $q : \mathbb{Z} \to \mathbb{Z}_n$ les épimorphismes canoniques. Dans le théorème 3.4.20 on va prendre $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $\tilde{G} = \mathbb{Z}_n$, $f = q$. On a $m\mathbb{Z} = \ker(p) \subset \ker(q) = n\mathbb{Z}$ et d'après théorème 3.4.20 il existe un unique homomorphisme $\bar{q} : \mathbb{Z}_m \to \mathbb{Z}_n$ tel que $\bar{q} \circ p = q$, i.e. tel que

$$\forall x \in \mathbb{Z},\ \bar{q}([x]_m) = [x]_n\ .$$

Le même théorème nous donne

$$\ker(\bar{q}) = \ker q/\ker p = n\mathbb{Z}/m\mathbb{Z}\ .$$

En plus $\bar{q}$ est un épimorphisme, parce que q est un épimorphisme.

Théorème 3.4.22 *(Le premier théorème d'isomorphisme) Soient $(G,\cdot)$, $(\tilde{G},*)$ groupes et $f : G \to \tilde{G}$ un homomorphisme. Alors la formule $\varphi([x]) := f(x)$ définit un isomorphisme*

$$\varphi : G/\ker(f) \xrightarrow{\simeq} \mathrm{im}(f)\ .$$

Démonstration: Dans la propriété universelle (le théorème 3.4.20) choisissons $H := \ker(f)$. D'après ce théorème f définit un monomorphisme $\bar{f} : G/\ker(f) \to \tilde{G}$ qui a la même image que f. Par restriction au but on obtient un isomorphisme $\varphi : G/\ker(f) \xrightarrow{\simeq} \mathrm{im}(f)$ avec la propriété requise. ■

Exemple 3.4.23 Considérons l'homomorphsime $f : (\mathbb{R},+) \to (\mathbb{C}^*,\cdot)$ défini par $f(t) = e^{2\pi i t}$. On a $\ker(f) = \mathbb{Z}$, $\mathrm{im}(f) = \mathrm{U} := \{z \in \mathbb{C}^* |\ |z| = 1\}$, donc, d'après le premier théorème d'isomorphisme, f induit un isomorphisme $\varphi : \mathbb{R}/\mathbb{Z} \xrightarrow{\simeq} \mathrm{U}$.

Exemple 3.4.24 Soit $f : (\mathbb{Z},+) \to (\mathbb{R}^*,\cdot)$ le morphisme défini par $f(k) = (-1)^k$. On a

$$\ker(f) = 2\mathbb{Z},\ \mathrm{im}(f) = \{\pm 1\},$$

donc f induit un isomorphisme $\varphi : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} \{\pm 1\}$ entre $(\mathbb{Z}/2\mathbb{Z},+)$ et $(\{\pm 1\},\cdot)$.

3.5 Le théorème de classification des groupes abéliens de type fini

Soit $(A,+)$ un groupe abélien et soit $(a_1,\dots,a_k)$ une famille de k éléments de A. Le sous-ensemble

$$\langle a_1,\dots,a_k\rangle := \left\{ \sum_{i=1}^{k} n_i a_i |\ n_i \in \mathbb{Z} \text{ pour } 1 \le i \le k \right\}$$

est un sous-groupe de A, qui s'appelle le sous-groupe engendré par la famille $(a_1,\dots,a_k)$. Dans la définition de $\langle a_1,\dots,a_k\rangle$ on a utilisé les notations introduites dans la remarque 3.1.21.

Définition 3.5.1 *Un groupe abélien $(A,+)$ est dit de type fini s'il existe une famille finie $(a_1,\dots,a_k)$ de A telle que $A = \langle a_1,\dots,a_k\rangle$. Si $A = \langle a_1,\dots,a_k\rangle$, on dit que $(a_1,\dots,a_k)$ est un système de générateurs de A.*

Exemple 3.5.2 Tout groupe cyclique est de type fini. En effet, par définition, un groupe cyclique est engendré par une famille à un seul élément.

Exemple 3.5.3 Le produit direct $\mathbb{Z}^k := \underbrace{\mathbb{Z}\times\dots\times\mathbb{Z}}_{k \text{ fois}}$ est un groupe abélien de type fini. En effet, soit $e_i \in \mathbb{Z}^k$ l'élément

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{ème place}\ .$$

Alors, pour un élément $x = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \in \mathbb{Z}^k$ on a $x = \sum_{i=1}^{k} x_i e_i \in \langle e_1,\dots,e_k\rangle$. On a démontré que $\mathbb{Z}^k = \langle e_1,\dots,e_k\rangle$, donc $\mathbb{Z}^k$ a une famille à k générateurs, en particulier il est de type fini.

Remarque 3.5.4 *Soit $(A,+)$ un groupe abélien. Les conditions suivantes sont équivalentes :*

1. *$(A,+)$ est de type fini,*
2. *il existe $k \in \mathbb{N}^*$ et un épimorphisme $f : \mathbb{Z}^k \to A$.*

Démonstration: En effet, si $A = \langle a_1,\dots,a_k\rangle$, alors l'application $f : \mathbb{Z}^k \to A$ définie par

$$f\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} := \sum_{i=1}^{k} x_i a_i$$

sera un épimorphisme. Pourquoi ?

Réciproquement, soit $f : \mathbb{Z}^k \to A$ est un épimorphisme. Posons $a_i := f(e_i)$. On va montrer que $A = \langle a_1,\dots,a_k\rangle$. En effet, soit $a \in A$. Puisque f est surjectif, il existe $x \in \mathbb{Z}^k$ tel que $f(x) = a$. Mais en utilisant l'exemple 3.5.3, on obtient $f(x) = f(\sum_{i=1}^{k} x_i e_i) = \sum_{i=1}^{k} x_i f(e_i) = \sum_{i=1}^{k} x_i a_i$. Ceci montre que $a \in \langle a_1,\dots,a_k\rangle$. ■

Théorème 3.5.5 (le théorème de structure des groupes abéliens de type fini) *Soit $(A,+)$ un groupe abélien de type fini.*

1. *(a) Il existe $r \in \mathbb{N}$ et une famille $(q_1,\dots,q_k)$ de puissances de nombres premiers tels qu'on a un isomorphisme de groupes*

$$A \simeq \left(\times_{i=1}^{k} \mathbb{Z}_{q_i}\right) \times \mathbb{Z}^r.$$

(b) *r est unique et la famille $(q_1,\dots,q_k)$ avec cette propriété est unique à ordre près.*

2. (a) *Il existe $r \in \mathbb{N}$ et une famille $(n_1,\dots,n_l)$ d'entiers > 1, tels que n_{i+1} est un diviseur de n_i (pour $1 \le i \le l-1$) et on a un isomorphisme de groupes*

$$A \simeq \left(\times_{i=1}^{l} \mathbb{Z}_{n_i}\right) \times \mathbb{Z}^r.$$

(b) *r et la famille $(n_1,\dots,n_l)$ avec ces propriétés sont uniques.*

Les nombres $q_1,\dots,q_k$ satisfaisant les conditions du théorème s'appellent *les diviseurs élémentaires* de $(A,+)$. Les entiers $n_1,\dots,n_l$ (qui sont des entiers > 1) s'appellent *les facteurs invariants* de $(A,+)$. Le nombre $r \in \mathbb{N}$ satisfaisant les conditions du théorème s'appelle *le rang* de $(A,+)$.

Remarquer que le rang d'un groupe abélien fini est nécessairement 0. Pourquoi ? Avec cette remarque on obtient :

Corollaire 3.5.6 *Soit $(A,+)$ un groupe abélien fini.*

1. *Il existe une famille $(q_1,\dots,q_k)$ de puissances de nombres premiers, unique à ordre près, telle que*

$$A \simeq \left(\times_{i=1}^{k} \mathbb{Z}_{q_i}\right).$$

2. *Il existe une famille $(n_1,\dots,n_l)$ d'entiers > 1, unique, telle que*
   (a) *$A \simeq \left(\times_{i=1}^{l} \mathbb{Z}_{n_i}\right)$.*
   (b) *n_{i+1} est un diviseur de n_i pour $1 \le i \le l-1$.*

Exemple 3.5.7 Considérons le groupe fini $A = \mathbb{Z}_{27} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$. Remarquer que 27, 9, 3, 16, 4, 2 sont des puissances des nombres premiers, donc les diviseurs élémentaires de A sont 27, 9, 3, 16, 16, 4, 2. En permutant les facteurs on obtient un isomorphisme

$$A \simeq (\mathbb{Z}_{27} \oplus \mathbb{Z}_{16}) \oplus (\mathbb{Z}_9 \oplus \mathbb{Z}_{16}) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_4) \oplus \mathbb{Z}_2\,.$$

D'après le lemme chinois on a des isomorphismes $\mathbb{Z}_{432} \simeq \mathbb{Z}_{27} \oplus \mathbb{Z}_{16}$, $\mathbb{Z}_{144} \simeq \mathbb{Z}_9 \oplus \mathbb{Z}_{16}$, $\mathbb{Z}_{12} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_4$. Donc

$$A \simeq \mathbb{Z}_{432} \oplus \mathbb{Z}_{144} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_2\,,$$

et $2|12$, $12|144$, $144|432$. Les facteurs invariants de A sont 432, 144, 12, 2.

3.6 Le groupe symétrique $\mathfrak{S}_n$

Soit M un ensemble fini et $n = |M|$ son cardinal. Rappelons qu'une permutation de M est une application bijective $M \to M$. L'ensemble des permutations de M est désigné par $\mathfrak{S}(M)$. Nous avons vu que $\mathfrak{S}(M)$, muni de la loi de composition interne donnée par la composition des bijections $M \to M$, est un groupe, qui est non-abélien pour $n \ge 3$. Remarquons que, en choisissant une bijection $b : \{1,\dots,n\} \to M$, on obtient un isomorphisme de groupes $\phi_b : \mathfrak{S}(M) \xrightarrow{\simeq} \mathfrak{S}_n$ donné par

$$\phi_b(\sigma) := b^{-1} \circ \sigma \circ b$$

Exercice : Montrer que ϕ_b est bien un isomorphisme de groupes.

Il en résulte que *le groupe $\mathfrak{S}(M)$ est isomorphe à $\mathfrak{S}_n$*, en particulier

1. $|\mathfrak{S}(M)| = |\mathfrak{S}_n| = n!$.
2. $\mathfrak{S}(M)$ est non-abélien si $n \ge 3$.

Dans cette section on va étudier le groupe symétrique $\mathfrak{S}(M)$ associé à un ensemble arbitraire M de cardinal n ; les résultats obtenus seront valables dans le cas particulier $\mathfrak{S}_n := \mathfrak{S}(\{1,\dots,n\})$.

Un arrangement de k éléments dans M est une famille $(m_1,\dots,m_k)$ d'éléments de M, distincts deux à deux. On va désigner par $\mathcal{A}^k(M)$ l'ensemble des arrangements de k éléments dans M. Rappelons que le cardinal de $\mathcal{A}^k(M)$ est

$$A_n^k := |\mathcal{A}^k(M)| = \frac{n!}{(n-k)!}\,.$$

Définition 3.6.1 *Soit $\sigma \in \mathfrak{S}(M)$.*

1. *Un élément $m \in M$ s'appelle point fixe de σ si $\sigma(m) = m$. L'ensemble des points fixes de σ sera noté M^σ.*
2. *Le support de σ est le sous-ensemble*

$$\mathrm{supp}(\sigma) := \{m \in M |\ \sigma(m) \neq m\} \subset M.$$

   Donc le support de σ est le complémentaire dans M du sous-ensemble M^σ des points fixes de σ.
3. *Un sous-ensemble $N \subset M$ est dit sous-ensemble invariant (partie invariante) par σ si $\sigma(N) = N$.*

Remarque 3.6.2 *Soit M un ensemble fini et $\sigma \in \mathfrak{S}(M)$.*

1. *Si $N \subset M$ est une partie invariante par σ, alors la restriction de σ à N définit une permutation de N.*
2. *M^σ et $\mathrm{supp}(\sigma)$ sont des parties invariantes par σ.*

Remarque 3.6.3 *Si $\alpha, \beta \in \mathfrak{S}(M)$ sont deux permutations à supports disjoints, alors $\alpha \circ \beta = \beta \circ \alpha$. Donc deux permutations à supports disjoints commutent.*

Démonstration: Il faut démontrer que

$$\forall x \in M \Rightarrow \alpha(\beta(x)) = \beta(\alpha(x)).$$

On va faire une discussion selon les cas. Si

$$x \in M \setminus \Big(\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)\Big)$$

alors $\alpha(\beta(x)) = \beta(\alpha(x)) = x$. Si $x \in \mathrm{supp}(\alpha)$ alors $\alpha(\beta(x)) = \beta(\alpha(x)) = \alpha(x)$. Pourquoi ? Si $x \in \mathrm{supp}(\beta)$ alors $\alpha(\beta(x)) = \beta(\alpha(x)) = \beta(x)$. Pourquoi ? ■

Définition 3.6.4 *Soit M un ensemble fini, $n = |M|$ son cardinal et $k \in \mathbb{N}^*$, $2 \leq k \leq n$. Une permutation $\alpha \in \mathfrak{S}(M)$ s'appelle cycle de longueur k, ou k-cycle, s'il existe un arrangement $(m_1, m_2 \ldots, m_{k-1}, m_k)$ de k éléments dans M tel que*

$$\alpha(m_1) = m_2,\ \alpha(m_2) = m_3,\ \ldots,\ \alpha(m_{k-1}) = m_k,\ \alpha(m_k) = m_1,\ \text{et } \alpha(m) = m \text{ pour } m \notin \{m_1, \ldots, m_k\}.$$

Si c'est le cas, on va écrire $\alpha = (m_1 m_2 \ldots m_k)$. Un 2-cycle s'appelle transposition. Un n-cycle s'appelle permutation circulaire de M.

Remarque 3.6.5

1. *L'élément inverse d'un k-cycle $\alpha = (m_1 m_2 \ldots m_{k-1} m_k)$ est le k-cycle $\alpha^{-1} = (m_k m_{k-1} \ldots m_2 m_1)$.*
2. *Si α est un k-cycle alors $\mathrm{ord}(\alpha) = k$.*
3. *La correspondance entre arrangements de k éléments et k-cycles de M (établie par la définition 3.6.4) n'est pas bijective. En effet, pour un arrangement $(m_1, m_2 \ldots, m_{k-1}, m_k)$ de k éléments dans M on a évidemment*

$$(m_1 m_2 \ldots m_{k-1} m_k) = (m_2 m_3 \ldots m_k m_1) = \cdots = (m_k m_1 \ldots m_{k-2} m_{k-1}),$$

   donc à chaque k-cycle correspondent k arrangements de k éléments dans M.
4. *Le nombre de k-cycles dans $\mathfrak{S}(M)$ est $\frac{1}{k} A_n^k = (k-1)! C_n^k$, en particulier dans $\mathfrak{S}(M)$ il y a $C_n^2 = \frac{n(n-1)}{2}$ transpositions et $(n-1)!$ permutations circulaires.*
5. *Un k-cycle (avec $k \geq 2$) s'écrit comme produit de $(k-1)$ transpositions. En effet on a*

$$(m_1 m_2 \ldots m_{k-1} m_k) = (m_1 m_k)(m_1 m_{k-1}) \ldots (m_1 m_3)(m_1 m_2).$$

6. *Si $n = 3$ alors $\mathfrak{S}(M)$ contient : id_M, trois transpositions et deux 3-cycles (qui seront des permutations circulaires de M). Si $n = 4$ alors $\mathfrak{S}(M)$ contient : id_M, six transpositions, huit 3-cycles et six 4-cycles (qui seront des permutations circulaires). Puisque $|\mathfrak{S}(M)| = 24$, dans ce cas on constate que $\mathfrak{S}(M) \setminus \{\mathrm{id}_M\}$ contient trois permutations qui ne sont pas des cycles.*

Remarque 3.6.6 *Le support d'un cycle $\alpha = (m_1 m_2 \dots m_k)$ est le sous-ensemble $\{m_1, m_2, \dots, m_k\}$. La restriction de α à ce sous-ensemble est une permutation circulaire. La donnée d'un k-cycle dans $\mathfrak{S}(M)$ est équivalente à la donnée d'un sous-ensemble $N \subset M$ de cardinal k et d'une permutation circulaire de N.*

Définition 3.6.7 *Soient $\alpha = (m_1 m_2 \dots m_{k-1} m_k)$, $\beta = (p_1 p_2 \dots p_{l-1} p_l) \in \mathfrak{S}(M)$ deux cycles. On dit que α, β sont des cycles disjoints si leur supports sont disjoints, donc si*

$$\{m_1, m_2, \dots, m_{k-1}, m_k\} \cap \{p_1, p_2, \dots p_{l-1}, p_l\} = \emptyset.$$

Proposition 3.6.8 *Soient α_1, α_2, ..., $\alpha_s \in \mathfrak{S}(M)$ des cycles disjoints deux à deux et soit $\sigma = \alpha_1 \alpha_2 \dots \alpha_s$ leur produit. Alors*

1. $\mathrm{supp}(\sigma) = \bigcup_{j=1}^{s} \mathrm{supp}(\alpha_i)$.
2. *Les sous-ensembles* $\mathrm{supp}(\alpha_i)$ *$(1 \le i \le s)$ donnent une partition de* $\mathrm{supp}(\sigma)$ *en parties invariantes par σ.*
3. *En désignant par k_i la longueur de α_i on a*

$$\mathrm{ord}(\sigma) = \mathrm{ppcm}(k_1, \dots, k_s).$$

Démonstration: 1., 2. Exercice.

3. Posons $M_i := \mathrm{supp}(\alpha_i)$ et soit a_i la permutation circulaire définie par la restriction de α_i à M_i (voir la remarque 3.6.6). En utilisant la remarque 3.6.3 on obtient pour tout $l \in \mathbb{N}$:

$$\sigma^l = \alpha_1^l \alpha_2^l \dots \alpha_s^l,$$

donc la permutation de M_i induite par σ^l est a_i^l. En tenant compte que σ^l coïncide avec id_M sur M^σ, il en résulte que $\sigma^l = \mathrm{id}_M$ si et seulement si $a_i^l = \mathrm{id}_{M_i}$ pour $1 \le i \le s$. Puisque $\mathrm{ord}(a_i) = k_i$, il en résulte que $\sigma^l = \mathrm{id}_M$ si et seulement si $k_i | l$ pour $1 \le i \le s$, donc si et seulement si $\mathrm{ppcm}(k_1, \dots, k_s) | l$.

Théorème 3.6.9 *[la décomposition d'une permutation en produit de cycles disjoints] Toute permutation $\sigma \in \mathfrak{S}(M) \setminus \{\mathrm{id}_M\}$ s'écrit comme produit de cycles disjoints deux à deux. Cette décomposition est unique à ordre près.*

Démonstration: On va utiliser la récurrence par rapport à $n = |M|$. Pour $n = 1$ l'affirmation du théorème est évidente. Supposons que l'affirmation du théorème est vraie pour tout ensemble de cardinal $n' < n$. Soit $\sigma \in \mathfrak{S}(M) \setminus \{\mathrm{id}_M\}$. Il existe $m_1 \in M$ tel que $\sigma(m_1) \neq m_1$. En posant $m_{j+1} := \sigma(m_j)$ on obtient par récurrence une suite $(m_j)_{j \in \mathbb{N}^*}$, où $m_j = \sigma^{j-1}(m_1)$. Soit k le plus petit élément $j \in \mathbb{N}^*$ avec la propriété $m_{j+1} \in \{m_1, \dots, m_j\}$. Remarquons que, avec ce choix $m_1, \dots, m_k$ seront distincts deux à deux (pourquoi) et que $m_{k+1} = m_1$. En effet, pour justifier la deuxième affirmation, notons que si (par l'absurde) on avait $m_{k+1} = m_j$ avec $2 \le j \le k$, alors on aurait

$$\sigma(m_{j-1}) = m_j = m_{k+1} = \sigma(m_k),$$

ce qui contredit l'injectivité de σ. On obtient donc un cycle

$$\alpha_1 = (m_1 m_2 \dots m_k).$$

Notons que le support $\{m_1, \dots, m_k\}$ de ce cycle est invariant par rapport à σ et que les restrictions

$$\sigma \Big| \{m_1, \dots, m_k\}, \ \alpha_1 \Big| \{m_1, \dots, m_k\}$$

de σ et α_1 à ce sous-ensemble coïncident. Posons

$$M' := M \setminus \{m_1, \dots, m_k\}$$

et soit $\sigma' \in \mathfrak{S}(M')$ la permutation définie par la restriction de σ à M'. Notons que σ coïncide avec α_1 sur $\{m_1, \dots, m_k\}$ et avec σ' sur M'. Si $\sigma' = \mathrm{id}_{M'}$, alors $\sigma = \alpha_1$ et l'affirmation est démontrée. Dans le cas contraire, par l'hypothèse de récurrence, on obtient une décomposition

$$\sigma' = \alpha_2' \alpha_3' \dots \alpha_s'$$

dans $\mathfrak{S}(M')$ en produit de cycles disjoints deux à deux. Pour $2 \leq j \leq s$ soit $\alpha_j \in \mathfrak{S}(M)$ la permutation qui coïncide avec α'_j sur M' et coïncide avec l'application identique sur $\{m_1, \ldots, m_k\}$. Alors α_j sera un cycle dans $\mathfrak{S}(M)$ de même longueur que α'_j. Avec ce choix on aura

$$\sigma = \alpha_1 \alpha_2 \ldots \alpha_s.$$

On obtient facilement cette égalité en utilisant une discussion selon les deux cas : $x \in \{m_1, \ldots, m_k\}$, $x \in M'$. Dans le premier cas on obtient $\sigma(x) = \alpha_1(x)$, dans le deuxième cas on obtient $\sigma(x) = \sigma'(x)$.

Pour démontrer l'unicité à ordre près, soient $\sigma = \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_s = \beta_1 \beta_2 \ldots \beta_t$ deux décompositions en produits de cycles disjoints deux à deux. Posons $\alpha_1 = (m_1 m_2 \ldots m_k)$. Puisque $m_1 \notin M^\sigma$, il appartient à l'un des supports $\mathrm{supp}(\beta_j)$. Après avoir réordonné ces cycles si nécessaire, on peut supposer que $m_1 \in \mathrm{supp}(\beta_1)$. Alors on aura $\alpha_1 = \beta_1$. Pourquoi ? Pour conclure on utilise de nouveau la récurrence par rapport à $|M|$. ■

Remarque 3.6.10 *La démonstration du théorème nous donne un algorithme explicite qui fournit une décomposition en cycles d'une permutation donnée.*

Exemple 3.6.11 Trouver une décomposition en produit de cycles disjoints de la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6 .$$

Corollaire 3.6.12 *Toute permutation $\sigma \in \mathfrak{S}(M)$ s'écrit comme produit de transpositions.*

Démonstration: D'après le théorème 3.6.9 σ admet une décomposition en produit de cycles. D'autre part, d'après la remarque 3.6.5.5., chaque cycle se décompose en produit de transpositions. ■

En général la décomposition d'une permutation en produit de transpositions n'est pas unique (même pas à ordre près). Par exemple dans $\mathfrak{S}_3$ on a $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (2\ 3)(1\ 3)$. Même le nombre des facteurs dans une décomposition d'une permutation en produit de transpositions n'est pas unique. Par exemple dans $\mathfrak{S}_n$ on a

$$(i\ j) = (1\ i)(1\ j)(1\ i) \text{ pour } i \neq j,\ i \geq 2,\ j \geq 2 .$$

Définition 3.6.13 *Soit $\sigma \in \mathfrak{S}_n$. Une inversion pour σ est un couple $(i, j) \in \{1, \ldots, n\}^2$ tel que*

$$i < j \text{ et } \sigma(i) > \sigma(j).$$

Le nombre d'inversions pour σ est désigné par $\iota(\sigma)$. La signature de σ est définie par

$$\varepsilon(\sigma) := (-1)^{\iota(\sigma)} \in \{-1, 1\}.$$

Exercice 3.6.14 Démontrer la formule suivante pour la signature d'une permutation $\sigma \in \mathfrak{S}_n$:

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma_j - \sigma_i}{j - i}.$$

Indication : Comparer le signe de $\prod_{1 \leq i < j \leq n} \frac{\sigma_j - \sigma_i}{j-i}$ avec $\varepsilon(\sigma)$ et montrer que sa valeur absolue est 1.

Lemme 3.6.15 *Soit τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.*

Démonstration: Exercice. Étudier le cas particulier $\tau = (1\ 2)$. ■

Il en résulte :

Proposition 3.6.16 *Soit $\sigma \in \mathfrak{S}_n$ et $\sigma = \tau_1 \ldots \tau_p$ une décomposition de σ en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^p$.*

En particulier, la parité du nombre de facteurs dans une décomposition de σ en produit de transpositions est invariante (dépend seulement de σ). Remarquer que la proposition 3.6.16 nous permet de donner une définition équivalente de la signature d'une permutation. Cette définition équivalente (qui tient compte de la parité du nombre de facteurs d'une décomposition en produit de transpositions) s'applique dans la cadre plus général des permutations d'un ensemble fini M.

Exemple 3.6.17 Soit $\alpha \in \mathfrak{S}_n$ un k-cycle. Alors $\varepsilon(\alpha) = (-1)^{k-1}$.

Proposition 3.6.18 *Munissons l'ensemble $\{-1, +1\}$ de la structure de groupe définie par la multiplication. L'application $\varepsilon : \mathfrak{S}_n \to \{-1, +1\}$ donnée par $\sigma \mapsto \varepsilon(\sigma)$ est un homomorphisme de groupes. Cet homomorphisme est un épimorphisme pour $n \geq 2$.*

Démonstration: Exercice. Utiliser la proposition 3.6.16. Pour démontrer la surjectivité de ε, il suffit de remarquer que $\varepsilon(\tau) = -1$ pour toute transposition $\tau \in \mathfrak{S}_n$. ■

Pour $n \geq 2$ le noyau $\ker(\varepsilon)$ est un sous-groupe distingué de $\mathfrak{S}_n$, qui s'appelle le groupe alterné de degré n et est noté A_n. L'ordre de ce groupe est $\frac{n!}{2}$. En effet, d'après le théorème de Lagrange on a

$$n! = |A_n|[\mathfrak{S}_n : A_n].$$

Puisque A_n est un sous-groupe normal, l'indice $[\mathfrak{S}_n : A_n]$ s'identifie à l'ordre $|\mathfrak{S}_n/A_n|$ du groupe quotient $\mathfrak{S}_n/A_n$. Mais d'après le 1-er théorème d'isomorphisme on a un isomorphisme $\mathfrak{S}_n/A_n \simeq \varepsilon(\mathfrak{S}_n) = \{-1, 1\}$. Donc $[\mathfrak{S}_n : A_n] = 2$.

4 Anneaux

4.1 Définition. Exemples. Règles de calcul dans un anneau

Définition 4.1.1 *1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+$, $\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que les conditions suivantes soient vérifiés :*

(A1) $(A,+)$ est un groupe abélien. Son élément neutre sera appelé l'élément nul de l'anneau et sera noté 0_A ou 0.

(A2) La lci $\cdot$ est associative et admet un élément neutre. Cet élément neutre sera appelé l'élément unité de l'anneau et sera noté 1_A ou 1.

(A3) La lci $\cdot$ est distributive à gauche et à droite par rapport à la lci $+$, i.e. pour tout $(x,y,z) \in A \times A \times A$ on a

$$x \cdot (y+z) = x \cdot y + x \cdot z,$$

$$(y+z) \cdot x = y \cdot x + z \cdot x.$$

2. Un anneau $(A,+,\cdot)$ est dit commutatif si $\cdot$ est commutative.

Soit $(A,+,\cdot)$ un anneau. Souvent on va omettre le symbole $\cdot$, donc, pour deux éléments x, $y \in A$ on va écrire xy au lieu de $x \cdot y$. Pour simplifier le texte on va utiliser désigner un anneau $(A,+,\cdot)$ par A, en sous-entendant qu'on a muni l'ensemble A de deux lci qui définissent une structure d'anneau.

Définition 4.1.2 *Deux éléments x, $y \in A$ sont dit commutables (permutables) si $xy = yx$.*

Donc un anneau $(A,+,\cdot)$ est commutatif si et seulement si tous deux éléments de A sont permutables.

Exemples 4.1.3 1. Soit A un singleton dont l'unique élément sera noté 0. Les lci $(0,0) \overset{+}{\mapsto} 0$, $(0,0) \overset{\cdot}{\mapsto} 0$ définissent une structure d'anneau sur $A = \{0\}$ avec $0_A = 1_A = 0$. Un tel anneau s'appelle anneau nul. Un anneau A nul si et seulement si $0_A = 1_A$. Pourquoi ? Un anneau $(A,+,\cdot)$ est non-nul si $\{0_A\} \subsetneq A$, c'est à dire si $0_A \neq 1_A$.

2. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des anneaux commutatifs.

3. Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}_n,+,\cdot)$ est un anneau commutatif.

4. Soit $n \in \mathbb{N}^*$. $(M_{n,n}(\mathbb{Z}),+,\cdot)$, $(M_{n,n}(\mathbb{Q}),+,\cdot)$, $(M_{n,n}(\mathbb{R}),+,\cdot)$, $(M_{n,n}(\mathbb{C}),+,\cdot)$ sont des anneaux. Pour $n \geq 2$ ces anneaux ne sont pas commutatifs.

5. Soit E un espace vectoriel réel ou complexe. $(\mathrm{End}(E),+,\circ)$ est un anneau. Pour $\dim(E) \geq 2$ cet anneau est non-commutatif.

6. Soit $(G,+)$ un groupe abélien dont l'élément neutre est noté 0_G. $(\mathrm{End}(G),+,\circ)$ est un anneau, en général non-commutatif. Son élément nul est l'endomorphisme trivial $x \mapsto 0_G$ et son élément unité est id_G.

7. Soient $(A,+,\cdot)$ un anneau, X un ensemble et soit $\mathcal{F}(X,A)$ l'ensemble des applications $X \to A$. Les lci $+$, $\cdot$ définies par
$$(f+g)(x) = f(x) + g(x),\ (f \cdot g)(x) = f(x) \cdot g(x)$$
définissent un structure d'anneau sur $\mathcal{F}(X,A)$. Cet anneau est commutatif si $(A,+,\cdot)$ est commutatif.

8. Soient A, B deux anneaux dont les lci sont notées par les mêmes symboles. Alors les lci
$$((x,y),(x',y')) \mapsto (x+x', y+y'),\ ((x,y),(x',y')) \mapsto (xx', yy')$$
définissent un structure d'anneau sur le produit cartésien $A \times B$. On peut généraliser cette construction pour une famille $(A_i)_{i \in I}$ d'anneaux.

4.1.1 L'anneau des polynômes à coefficients dans un anneau commutatif

A tout anneau commutatif A on peut associer un nouveau anneau commutatif : l'anneau $A[X]$ des polynômes à coefficients dans A.

Soit A un anneau commutatif. On va noter 0 son élément nul et 1 son élément unité.

Définition 4.1.4 *L'ensemble des polynômes à coefficients dans A est défini par*

$$A[X] := \{(a_k)_{k\geq 0} | \ \exists N \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k \geq N\}.$$

Le polynôme $(a, 0, 0\dots)$ s'appelle le polynôme constant associé à a.

Donc la donnée d'un polynôme à coefficients dans A est équivalente à la donnée d'une suite $(a_k)_{k\geq 0}$ de A dont tous les termes sont nuls à partir d'un certain indice. Cet ensemble a une structure naturelle de groupe abélien, l'addition étant donnée par

$$((a_k)_{k\geq 0}) + ((b_k)_{k\geq 0}) := (a_k + b_k)_{k\geq 0}.$$

Définition 4.1.5 *La multiplication dans $A[X]$ est la loi de composition interne donnée par la formule*

$$((a_k)_{k\geq 0})((b_l)_{l\geq 0}) = (c_n)_{n\geq 0} \text{ où } c_n := \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l \ .$$

C'est facile de vérifier que cette loi de composition est associative, admet un élément neutre, à savoir le polynôme constant $(1, 0, 0, \dots)$, est commutative, est distributive par rapport à l'addition dans $A[X]$. Il en résulte :

Proposition 4.1.6 *Les opérations $+, \cdot$ introduites ci-dessus munissent l'ensemble $A[X]$ d'une structure d'anneau commutatif.*

Comme dans la théorie élémentaire des polynômes on va identifier un élément $a \in A$ avec le polynôme constant $(a, 0, 0, \dots)$ qui lui correspond. En particulier on va utiliser la notation 1 pour l'élément unité $(1, 0, 0, \dots)$ de l'anneau $A[X]$.

On va noter par X la suite $(0, 1, 0, \dots) \in A[X]$. Notons que $X^2 = (0, 0, 1, 0, \dots)$, $X^3 = (0, 0, 0, 1, 0, \dots)$ et ainsi de suite. Avec la convention $X^0 := 1$ on obtient l'égalité suivante

$$(a_k)_{k\geq 0} = \sum_{k\geq 0} a_k X^k \ ,$$

(somme qui contient seulement un nombre fini de termes non-nuls). Cette égalité importante fait la liaison entre la définition moderne de la notion de polynôme (voir la définition 4.9.1) et la manière élémentaire d'introduire cette notion, à savoir comme une expression algébrique de la forme

$$a_0 + a_1 X + \cdots + a_N X^N \ .$$

La multiplication des polynômes donnée par la définition 4.9.2 correspond à la multiplication des expressions algébriques introduite au lycée.

En appliquant la construction $A \mapsto A[X]$ aux anneaux commutatifs connus, on obtient des nouveaux exemples d'anneaux commutatifs : $(\mathbb{Z}[X], +, \cdot)$, $(\mathbb{Q}[X], +, \cdot)$, $(\mathbb{R}[X], +, \cdot)$, $(\mathbb{C}[X], +, \cdot)$, $\mathbb{Z}_n[X]$.

4.1.2 Règles de calcul dans un anneau

Soit $(A, +, \cdot)$ un anneau. Puisque $(A, +)$ est un groupe abélien, on va utiliser la notation nx (pour un entier $n \in \mathbb{Z}$ et un élément $x \in A$) introduite dans la remarque 3.1.21. En particulier l'élément symétrique par rapport à l'addition (l'opposé) d'un élément $x \in A$ sera noté $-x$. On va aussi utiliser les règles de calcul connues dans un groupe en notation additive.

Proposition 4.1.7 *(Règles de calcul dans un anneau). Soit $(A,+,\cdot)$ un anneau. Alors*

1. *Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.*
2. *Pour tout $(x,y) \in A \times A$ on a $x(-y) = (-x)y = -(xy)$.*
3. *Pour tout $(x,y) \in A \times A$ on a $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$.*
4. *Pour tout élément $x \in A$ et $n \in \mathbb{N}$ on définit l'élément $x^n \in A$ en posant*

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ fois}} & \text{si} \quad n > 0, \\ 1 & \text{si} \quad n = 0. \end{cases}$$

   Alors on a l'identité $x^m \cdot x^n = x^{m+n}$

5. *Pour tout $x \in A$ et pour tout $n \in \mathbb{Z}$ on a $nx = (n\,1_A) \cdot x = x \cdot (n\,1_A)$.*

Démonstration: Exercice. ■

4.1.3 La formule du binôme pour deux éléments commutables dans un anneau.

Lemme 4.1.8 *Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables. Pour tous $k, l \in \mathbb{N}$ les éléments x^k, y^l sont aussi commutables.*

Démonstration: Démonstration en deux étapes :

1. En utilisant récurrence par rapport à k on démontre que x^k et y sont commutables pour tout $k \in \mathbb{N}$.
2. Fixons $k \in \mathbb{N}$. En utilisant la récurrence par rapport à l on démontre que x^k et y^l sont commutables.

■

Proposition 4.1.9 *Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables et $n \in \mathbb{N}$. Alors*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Démonstration: Exercice. Utiliser le lemme 4.1.8, la récurrence par rapport à n et l'identité

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

■

4.2 Diviseurs de zéro dans un anneau commutatifs. Anneaux commutatifs intègres

Définition 4.2.1 *Soit $(A,+,\cdot)$ un anneau commutatif non-nul. On dit qu'un élément $a \in A \setminus \{0_A\}$ est un diviseur de zéro si s'il existe $b \in A \setminus \{0_A\}$ tel que $ab = 0_A$. Un anneau commutatif est dit intègre, ou anneau d'intégrité, s'il est non-nul et ne possède aucun diviseur de zéro.*

Remarque 4.2.2 *Un anneau commutatif non-nul $(A,+,\cdot)$ est intègre si et seulement si*

$$\forall (x,y) \in A \times A \left(xy = 0 \Rightarrow (x = 0) \vee (y = 0) \right).$$

Exercice 4.2.3 Préciser les diviseurs de 0 de $(\mathbb{Z}_{12},+,\cdot)$.

Exemples 4.2.4

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.
2. Soit $n \in \mathbb{N}^*$. L'anneau $(\mathbb{Z}_n,+,\cdot)$ est intègre si et seulement si n est un nombre premier.

3. Soient $(A,+,\cdot)$, $(B,+,\cdot)$ deux anneaux commutatifs non-nuls. Alors $A\times B$ (muni de sa structure d'anneau produit) n'est pas intègre.
4. Soient $(A,+,\cdot)$ un anneau commutatif non-nul et X un ensemble. Si $\mathrm{card}(X)\geq 2$ alors $\mathcal{F}(X,A)$ (muni de sa structure naturelle d'anneau) n'est pas intègre. Pourquoi ?

On va montrer que, si A un anneau commutatif intègre, alors $A[X]$ est intègre. Cette proposition nous permet de construire des nouveaux anneaux intègres à partir des anneaux intègres connus.

Proposition 4.2.5 *Soit A un anneau commutatif intègre. Alors $A[X]$ est intègre.*

Démonstration: La démonstration utilise la notion de degré d'un polynôme :

Définition 4.2.6 *Soit $P(X)=\sum_{k\geq 0}a_kX^k\in A[X]$.*

$$\deg(P(X)):=\begin{cases}\max\{k\in\mathbb{N}|\ a_k\neq 0\} & \text{si} \quad P(X)\neq 0\\ -\infty & \text{si} \quad P(X)=0\end{cases}.$$

La formule connue $\deg(P(X)Q(X))=\deg(P(X))+\deg(Q(X))$. reste vraie pour les polynômes à coefficients *dans un anneau intègre* (Exercice). Cette formule montre : $P(X)Q(X)=0\Rightarrow(P(X)=0)\vee(Q(X)=0)$. ■

Exemple 4.2.7 Calculer $(\hat{2}X+\hat{4})(\hat{3}X+\hat{3})\in\mathbb{Z}_6[X]$.

Définition 4.2.8 *Soit $(A,+,\cdot)$ un anneau commutatif. Un élément $x\in A$ est dit inversible, s'il est inversible par rapport à la multiplication, i.e. s'il existe $y\in A$ tel que $xy=1$. On va désigner par $A^\times\subset A$ le sous-ensemble des éléments inversibles.*

Remarque 4.2.9 *Soit $(A,+,\cdot)$ un anneau commutatif. Alors $A^\times$ est stable par rapport à la multiplication et $(A^\times,\cdot)$ est un groupe commutatif.*

Exercice 4.2.10 Préciser les groupe des éléments inversibles dans les anneaux commutatifs suivants (munis de leurs opérations usuelles) : $\mathbb{Z}$, $\mathbb{Z}_{12}$, $\mathbb{Z}[X]$, $\mathbb{R}[X]$.

Définition 4.2.11 *Un anneau commutatif non-nul $(A,+,\cdot)$ s'appelle corps, si tout élément $x\in A\setminus\{0\}$ est inversible.*

Donc, un anneau commutatif non-nul $(A,+,\cdot)$ est un corps si et seulement si $A^\times=A\setminus\{0\}$.

Exemples 4.2.12 $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des corps.

Remarquons que, dans un anneau commutatif non-nul un élément inversible n'est jamais diviseur de 0. Pourquoi ? Il en résulte

Remarque 4.2.13 *Tout corps $(K,+,\cdot)$ est un anneau intègre.*

Proposition 4.2.14 *Soit $n\in\mathbb{N}^*$. Sont équivalentes*

1. *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.*
2. *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*
3. *n est un nombre premier.*

Démonstration: Exercice. Remarquer que $\mathbb{Z}/0\mathbb{Z}=\mathbb{Z}/\{0\}\simeq\mathbb{Z}$ est intègre, mais n'est pas un corps. ■

Exercice 4.2.15 Soit $(A,+,\cdot)$ un anneau commutatif intègre. Identifions A avec le sous ensemble de $A[X]$ formé par les polynômes constants. Montrer qu'un polynôme $P(X)\in A[X]$ est inversible si et seulement si $P(X)\in A^\times$. En déduire que $A[X]$ n'est jamais un corps.

Exemple 4.2.16 Le sous-ensemble

$$\mathbb{Q}[\sqrt{2}]:=\{a+b\sqrt{2}|\ a,\ b\in\mathbb{Q}\}\subset\mathbb{R}$$

muni de l'addition et de la multiplication ordinaires est un corps commutatif.

4.3 Sous-anneaux et idéaux dans un anneau commutatif. Anneaux quotients

Dans ce chapitre $(A,+,\cdot)$ désigne un anneau commutatif.

Définition 4.3.1 *Un sous-ensemble $B \subset A$ est dit sous-anneau de $(A,+,\cdot)$ si les conditions suivantes sont vérifiées :*

(i) *B est un sous-groupe du groupe abélien $(A,+)$.*

(ii) *$\forall (x,y) \in B \times B,\ x \cdot y \in B$.*

(iii) *$1_A \in B$.*

Remarque 4.3.2 *Si B est un sous-anneau de $(A,+,\cdot)$, alors B est stable par rapport aux lci $+$, $\cdot$ et les opérations induites sur B définissent une structure d'anneau sur B.*

Remarque 4.3.3 *Soient $(A,+,\cdot)$ un anneau commutatif et $B \subset A$ un sous-ensemble de A. Sont équivalentes*

(i) *B est un sous-anneau de $(A,+,\cdot)$.*

(ii) *$1_A \in B$ et $\forall (x,y) \in B \times B,\ \Big((x-y \in B) \wedge (x \cdot y \in B)\Big)$.*

Démonstration: Exercice. Utiliser la définition 3.2.5. ■

Remarque 4.3.4 *Tout sous-anneau d'un anneau intègre est un anneau intègre.*

Exemples 4.3.5

1. A est toujours un sous-anneau de $(A,+,\cdot)$ mais, si A est non-nul, $\{0_A\}$ ne sera pas un un sous-anneau de $(A,+,\cdot)$.
2. Les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-anneau.
3. Soit $(A,+,\cdot)$ un anneau commutatif. Identifions A avec le sous ensemble de $A[X]$ formé par les polynômes constants. Alors A devient un sous-anneau dans $(A[X],+,\cdot)$.

Définition 4.3.6 *Soit $I \subset A$. On dit que I est un idéal de A si*

(i) *I est un sous-groupe du groupe abélien $(A,+)$.*

(ii) *$\forall (a,x) \in A \times I,\ a \cdot x \in I$.*

Exemples 4.3.7 Soit $(A,+,\cdot)$ un anneau commutatif . A et $\{0_A\}$ sont des idéaux de $(A,+,\cdot)$. Tout idéal $I \subset A$ qui est différent de A et $\{0_A\}$ s'appelle *idéal propre* de $(A,+,\cdot)$

Une question naturelle : est-ce qu'un idéal $I \subset A$ peut être aussi un sous-anneau ? La réponse est donnée par la remarque suivante :

Remarque 4.3.8 *Soit $I \subset A$ un idéal de $(A,+,\cdot)$. Sont équivalentes*

(i) *$I = A$.*

(ii) *I est un sous-anneau.*

(iii) *$1_A \in I$.*

(iv) *I contient un élément inversible.*

Donc le seul idéal de A qui est sous-anneau de A est A lui même.

Exemple 4.3.9 Soit $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x |\ x \in A\} \subset A$$

est un idéal de $(A,+,\cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 4.3.10 *Un anneau commutatif $(A,+,\cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.*

Remarque 4.3.11 *L'ensemble des idéaux de* $(\mathbb{Z},+,\cdot)$ *est* $\{n\mathbb{Z}|\ n\in\mathbb{N}\}$. *En particulier* $(\mathbb{Z},+,\cdot)$ *est un anneau principal.*

Démonstration: Soit $I\subset\mathbb{Z}$ un idéal de $(\mathbb{Z},+,\cdot)$. Puisque I est in idéal, il est un sous-groupe du groupe abélien $(\mathbb{Z},+)$. Mais tout sous-groupe du groupe abélien $(\mathbb{Z},+)$ s'écrit sous la forme $n\mathbb{Z}$ avec $n\in\mathbb{N}$ (exercice). Réciproquement, tout sous-ensemble de la forme $n\mathbb{Z}$ est un idéal de $(\mathbb{Z},+,\cdot)$. ■

En utilisant le théorème division euclidienne pour les polynômes à coefficients dans un corps un va démontrer que pour tout corps K, l'anneau $K[X]$ est aussi principal.

Définition 4.3.12 *Un idéal* I *de* $(A,+,\cdot)$ *est dit maximal si* $I\neq A$ *et pour tout idéal* J *diffèrent de* I *qui contient* I *on a* $J=A$.

Exemple 4.3.13 L'idéal $n\mathbb{Z}$ de $(\mathbb{Z},+,\cdot)$ est maximal si et seulement si n est un nombre premier.

En effet, on peut supposer $n\geq 2$. Tout idéal de $\mathbb{Z}$ s'écrit sous la form $m\mathbb{Z}$ avec $m\in\mathbb{N}$. Nous avons les équivalences

$$n\mathbb{Z}\subset m\mathbb{Z}\Leftrightarrow m|n,\ n\mathbb{Z}=m\mathbb{Z}\Leftrightarrow m=n,\ m\mathbb{Z}=\mathbb{Z}\Leftrightarrow m=1.$$

En conclusion $n\mathbb{Z}$ n'est pas maximal si et seulement s'il existe un diviseur $m\in\mathbb{N}^*$ de n tel que $m\neq 1$ et $m\neq n$, donc si et seulement si n n'est pas un nombre premier.

Proposition 4.3.14 *Soit* $(I_s)_{s\in S}$ *une famille d'idéaux de* A. *Alors l'intersection* $\bigcap_{s\in S} I_s$ *est un idéal de* A.

Démonstration: Exercice. ■

Définition 4.3.15 *Soit* $S\subset A$ *un sous-ensemble. L'idéal engendré par* S *est l'intersection des tous les idéaux de* $(A,+,\cdot)$ *qui contiennent* S *:*

$$(S):=\bigcap_{\substack{I\text{ idéal de }A\\ S\subset I}} I$$

Donc l'idéal engendré par S *est le plus petit idéal (au sens de l'inclusion) de* A *qui contient* S.

Remarque 4.3.16 *Soit* $S\subset A$ *un sous-ensemble. Alors*

$$(S)=\Big\{\sum_{i=1}^{k} s_i\cdot x_i|\ k\in\mathbb{N},\ (s_1,\dots,s_k)\in S^k,\ (x_1,\dots,x_k)\in A^k\Big\}.$$

Démonstration: Démonstration en deux étapes :

1. Le sous-ensemble
$$I:=\Big\{\sum_{i=1}^{k} s_i\cdot x_i|\ k\in\mathbb{N},\ (a_1,\dots,a_k)\in S^k,\ (x_1,\dots,x_k)\in A^k\Big\}$$
est un idéal de $(A,+,\cdot)$ qui contient S. Ceci implique l'inclusion $(S)\subset I$.
2. Tout idéal de $(A,+,\cdot)$ qui contient S doit contenir I. Ceci implique $I\subset(S)$.

■

Définition 4.3.17 *Un idéal* I *de* A *est dit idéal de type fini s'il est engendré par un ensemble fini, donc s'il existe* $k\in\mathbb{N}$ *et* $s_1,\dots,s_k\in A$ *tels que*

$$I=\Big\{\sum_{i=1}^{k} s_i\cdot x_i|\ (x_1,\dots,x_k)\in A^k\Big\}.$$

Soient $I,J\subset A$ *deux idéaux de* A. *La somme* $I+J$ *est l'idéal défini par*

$$I+J:=(I\cup J)=\{x+y|\ x\in I,\ y\in J\}.$$

Plus généralement, pour une famille finie $(I_i)_{1\leq i\leq k}$ d'idéaux de $(A,+,\cdot)$ on pose

$$I_1+\ldots+I_k := (I_1\cup\ldots\cup I_k) = \Big\{\sum_{i=1}^{k} x_i |\ x_i\in I_i \text{ pour } 1\leq i\leq k\Big\}.$$

Exercice 4.3.18 Un idéal $I\subset A$ est maximal si et seulement si $I\neq A$ et pour tout $a\in A\setminus I$ on a $aA+I=A$.

Définition 4.3.19 *Un idéal I de A est dit premier si $I\neq A$ et l'implication suivante est vraie :*

$$(a\cdot b\in I)\Rightarrow(a\in I)\vee(b\in I).$$

Proposition 4.3.20 1. *L'idéal nul $\{0_A\}\subset A$ est premier si et seulement si A est intègre.*

2. *Tout idéal maximal $I\subset A$ de A est un idéal premier.*

Démonstration: 1. Évident.
2. En effet, soient I maximal et $a,\ b\in A$ tels que $ab\in I$. Si $a\notin I$, alors, d'après l'exercice 4.3.18 on a $aA+I=A$, donc il existe $x\in A$ et $z\in I$ tels que $ax+z=1$. En multipliant avec b on obtient $b=abx+bz\in I$ (parce que $ab\in I$ et $z\in I$). ■

Exemple 4.3.21 L'idéal principal engendré par le polynome X dans l'anneau $\mathbb{Z}[X]$ (muni des opérations usuelles) est premier, mais n'est pas maximal.

En effet, $X\mathbb{Z}[X]$ est contenu dans l'idéal $2\mathbb{Z}[X]+X\mathbb{Z}[X]$ et les deux inclusions

$$X\mathbb{Z}[X]\subset 2\mathbb{Z}[X]+X\mathbb{Z}[X],\ 2\mathbb{Z}[X]+X\mathbb{Z}[X]\subset\mathbb{Z}[X]$$

sont strictes.

4.3.1 Anneau quotient

Remarque 4.3.22 *Soient $(A,+,\cdot)$ un anneau commutatif, $I\subset A$ un idéal et $(A/I,+)$ le groupe quotient du groupe abélien $(A,+)$ par le sous-groupe I (voir la définition 3.4.17). La formule*

$$([x]_I,[y]_I)\mapsto[x\cdot y]_I$$

définit une lci sur A/I (notée par le même symbole $\cdot$) et le triplet $(A/I,+,\cdot)$ est un anneau commutatif dont l'élément unité est la classe $[1_A]_I$.

Démonstration: Exercice.

Définition 4.3.23 *L'anneau $(A/I,+,\cdot)$ défini dans la remarque 4.3.22 s'appelle l'anneau quotient de $(A,+,\cdot)$ par l'idéal I.*

Exemple 4.3.24 L'anneau quotient de $(\mathbb{Z},+,\cdot)$ par l'idéal $n\mathbb{Z}$ est précisément l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ des entiers modulo n.

Proposition 4.3.25 *Soient $(A,+,\cdot)$ un anneau commutatif et $I\subset A$ un idéal. Alors*

1. *I est un idéal maximal si et seulement si A/I est un corps.*
2. *I est un idéal premier si et seulement si A/I est intègre.*

Démonstration: Exercice. ■

4.4 Morphismes d'anneaux. Le premier théorème d'isomorphisme

Définition 4.4.1 *Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme ou un homomorphisme d'anneaux si les conditions suivantes sont vérifiées :*

(i) $f(1_A) = 1_B$.

(ii) Pour tout couple $(x, y) \in A \times A$ on a $f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Un morphisme $f : A \to B$ est dit monomorphisme (épimorphisme, isomorphisme) si l'application f est injective (respectivement surjective, bijective).

Un endomorphisme de A est un morphisme $A \to A$. Un automorphisme de A est un isomorphisme $A \to A$.

Le noyau d'un morphisme $f : A \to B$ est l'idéal de A défini par $\ker(f) := \{x \in A |\ f(x) = 0_B\}$.

Exemple 4.4.2 Soient A un anneau commutatif et $I \subset A$ un idéal. La surjection canonique $p : A \to A/I$ est un épimorphisme d'anneaux, qui s'appelle l'épimorphisme canonique.

Remarque 4.4.3 *Soient $f : A \to B$, $g : B \to C$ morphismes d'anneaux. Alors :*

(i) $g \circ f : A \to C$ *est un morphisme d'anneaux.*

(ii) Si f est un isomorphisme, alors l'application réciproque $f^{-1} : B \to A$ est un isomorphisme.

Démonstration: Exercice. ∎

Proposition 4.4.4 *Soit $f : A \to B$ un morphisme d'anneaux. Alors :*

(i) $f(0_A) = 0_B$.

(ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.

(iii) Soit $x \in A$ inversible. Alors $f(x)$ est inversible dans B et $f(x^{-1}) = (f(x))^{-1}$.

(iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.

(v) Soit $I \subset A$ un idéal de A. Si f est surjective, alors l'image $f(I)$ est un idéal de B.

(vi) Soit $B' \subset B$ est un sous-anneau de B. Alors l'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

(vii) Soit $I \subset B$ est un idéal de B. Alors $f^{-1}(I)$ est un idéal de A.

(viii) f est injectif si et seulement $\ker(f) = \{0_A\}$.

Démonstration: Exercice. ∎

Attention, en général l'image directe d'un idéal par un morphisme d'anneaux n'est pas nécessairement un idéal. Par exemple l'image de $\mathbb{Z}$ par le morphisme d'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ n'est pas un idéal de $\mathbb{Q}$.

L'anneau quotient est caractérisé par une propriété universelle. Sa démonstration utilise la méthode utilisée pour la propriété universelle du groupe quotient (voir le théorème 3.4.20).

Théorème 4.4.5 *(la propriété universelle de l'anneau quotient) Soient A, B deux anneaux commutatifs, $I \subset A$ un idéal de A, $p : A \to A/I$ l'épimorphisme canonique associé à I et $f : A \to B$ un morphisme d'anneaux. Alors*

1. *Il existe un homomorphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ p = f$ si et seulement si $I \subset \ker(f)$.*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle p}\downarrow & \nearrow_{\bar{f}} & \\ A/I & & \end{array} \tag{12}$$

2. *Si cette condition est vérifiée, alors*
   (a) $\bar{f}$ est unique, $\ker(\bar{f})$ s'identifie au quotient $\ker(f)/I$ et $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$,
   (b) $\bar{f}$ est un monomorphisme si et seulement si $I = \ker(f)$,
   (c) $\bar{f}$ est un épimorphisme si et seulement si f est un épimorphisme.

Comme dans la théorie des groupes (voir le théorème 3.4.22) en utilisant la propriété universelle on obtient facilement un théorème d'isomorphisme pour les morphismes d'anneaux :

Théorème 4.4.6 *(le premier théorème d'isomorphisme pour les anneaux) Soient A, B anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors la formule $\varphi([x]_I) := f(x)$ définit un isomorphisme*

$$\varphi : A/\ker(f) \xrightarrow{\simeq} \mathrm{im}(f)\,.$$

Exemple 4.4.7 Soit $K[X]$ l'anneau des polynômes a coefficients dans un corps K. Considérons le morphisme d'anneau $f : K[X] \to K$ défini par $f(P(X)) := P(0)$. La noyau $\ker(f)$ est l'idéal formé par les polynômes $\sum_{i=0}^{d} a_i X^i$ avec $a_0 = 0$, donc $\ker(f) = (X)$. Le 1er théorème d'isomorphisme nous donne un isomorphisme $\bar{f} : K[X]/(X) \to K$.

4.4.1 La caractéristique d'un anneau

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n1_A$$

est un morphisme d'anneaux. C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A. Son noyau est un idéal de $\mathbb{Z}$, donc s'écrit sous la forme $c_A\mathbb{Z}$ pour un nombre naturel $c_A \in \mathbb{N}$ qui dépend seulement de l'anneau A. On a donc

$$c_A = \begin{cases} 0 & \text{si} \quad \ker(\gamma_A) = \{0\}, \\ \min\{k \in \mathbb{N}^* |\ k1_A = 0_A\} = \mathrm{ord}(1_A) & \text{si} \quad \ker(\gamma_A) \neq \{0\}. \end{cases}$$

Définition 4.4.8 *Le nombre naturel c_A défini par l'égalité*

$$\ker(\gamma_A) = c_A\mathbb{Z}$$

s'appelle la caractéristique de l'anneau A.

Remarquer que $c_A = 1$ si et seulement si $1_A = 0_A$, c'est à dire si et seulement si $A = \{0_A\}$.
Le 1er théorème d'isomorphisme donne un isomorphisme

$$\bar{\gamma}_A : \mathbb{Z}/c_A\mathbb{Z} \to \mathrm{im}(\gamma_A) := \{k1_A |\ k \in \mathbb{Z}\}.$$

Remarque 4.4.9 *Si A est un anneau intègre (en particulier un corps) alors c_A est soit 0, soit un nombre premier.*

Démonstration: Exercice. Pour la 2ème affirmation utiliser la remarque 4.3.4 et la proposition 4.2.14.

Exemples 4.4.10
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux de caractéristique 0.
2. $\mathbb{Z}/n\mathbb{Z}$ et l'anneau des polynômes $(\mathbb{Z}/n\mathbb{Z})[X]$ sont des anneaux de caractéristique n.

4.5 Divisibilité dans un anneau commutatif intègre

4.5.1 Divisibilité et idéaux. Éléments associés

Définition 4.5.1 *Soit A un anneau commutatif intègre et soient $a, b \in A$. On dit que a divise b (ou que a est un diviseur de b, ou que b est un multiple de a) dans A, s'il existe $q \in A$ tel que $b = aq$.*

Remarque 4.5.2 *Un élément inversible $u \in A$ divise tout élément $b \in A$.*

Définition 4.5.3 *Soit $a, b \in A$. On dit que a et b sont associés s'il existe un élément inversible $u \in A$ tel que $b = au$.*

Exemple 4.5.4 Deux éléments $a, b \in \mathbb{Z}$ sont associés si et seulement si $b = \pm a$, donc si et seulement si $|a| = |b|$.

Remarque 4.5.5 *Soit A un anneau commutatif intègre.*

1. *Soient $a, b \in A$. Sont équivalentes*
   (a) *a et b sont associés,*
   (b) *$a|b$ et $b|a$.*
2. *La relation sur A définie par la condition " a et b sont associés" est une relation d'équivalence sur A.*

Démonstration: Exercice. Attention au cas ou $a = 0_A$ ou $b = 0_A$. ■

Rappelons que, pour un élément $a \in A$ on a noté par (a) l'idéal principal aA engendré par a.

Proposition 4.5.6 *Soient A un anneau commutatif intègre et $a, b \in A$.*

1. *$a|b$ si et seulement si $(b) \subset (a)$.*
2. *$(b) = (a)$ si et seulement si a sont associés.*

Démonstration: Exercice. ■

4.5.2 Éléments irréductibles, éléments premiers

Soit A un anneau commutatif intègre.

Définition 4.5.7 1. *Un élément $p \in A \setminus \{0\}$ est dit irréductible s'il n'est pas inversible et pour toute décomposition $p = bc$, on a soit $b \in A^\times$, soit $c \in A^\times$.*
Equivalent : $p \in A \setminus \{0\}$ est irréductible s'il n'est pas inversible et ses seuls diviseurs sont les éléments inversibles et les éléments qui lui sont associés.
2. *Un élément $p \in A \setminus \{0\}$ est dit premier s'il n'est pas inversible et l'implication suivante est vraie : $p|bc \Rightarrow p|b \vee p|c$.*

Remarque 4.5.8 *Soit A un anneau commutatif intègre.*

1. *Tout élément premier de A est irréductible.*
2. *Un élément $p \in A \setminus \{0\}$ est premier si et seulement si l'idéal principal $(p) = pA$ engendré par p est un idéal premier.*

Démonstration: 1. Soit $p \in A \setminus \{0\}$ premier et soit $p = bc$ une décomposition de p. Nous devons démontrer que $b \in A^\times$, ou $c \in A^\times$.

Puisque $p = bc$ on a $p|bc$, donc (p étant premier) $p|b$ ou $p|c$. Supposons $p|b$, i.e. il existe $q \in A$ tel que $b = pq$. On obtient :

$$p = pqc \Rightarrow p(1 - qc) = 0 \overset{A \text{ intègre}}{\Longrightarrow} 1 - qc = 0 \Rightarrow qc = 1 \Rightarrow c \in A^\times.$$

De manière similaire, en supposant $p|c$ on va obtenir $b \in A^\times$.

2. Exercice. ■

Exemples 4.5.9 1. Un entier $k \in \mathbb{Z}$ est irréductible si et seulement si k est premier, si et seulement si $|k|$ est un nombre premier au sens élémentaire.
2. Un polynôme $P(X) \in \mathbb{C}[X]$ est irréductible si et seulement si il est premier, si et seulement si $\deg(P(X)) = 1$.
3. Un polynôme $P(X) \in \mathbb{R}[X]$ est irréductible si et seulement si il est premier, si et seulement si soit $\deg(P(X)) = 1$, soit $\deg(P(X)) = 2$ et son discriminant est strictement négatif.

On va voir que l'équivalence (p est premier $\Leftrightarrow$ p est irréductible) reste vraie dans tout anneau factoriel, en particulier dans tout anneau principal. Mais, en général (dans un anneau intègre), un élément irréductible n'est pas nécessairement premier.

Proposition 4.5.10 *Considérons*

$$\mathbb{Z}[i\sqrt{5}] := \{a + ib\sqrt{5} |\ a,\ b \in \mathbb{Z}\}$$

muni de sa structure de sous-anneau de $\mathbb{C}$. *Dans cet anneau* 3 *est irréductible, mais n'est pas premier.*

Pour montrer que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: on va utiliser l'application $z \mapsto |z|^2$. Pour montrer que 3 n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$: $3|(2 + i\sqrt{5})(2 - i\sqrt{5})$, mais 3 ne divise aucun des deux facteurs. *Démonstration:* 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$: Soit

$$(a + ib\sqrt{5})(\alpha + i\beta\sqrt{5}) = 3 \tag{13}$$

une décomposition de 3 dans $\mathbb{Z}[i\sqrt{5}]$. On peut supposer $b \neq 0$, $\beta \neq 0$, sinon (13) sera décomposition dans $\mathbb{Z}$ et 3 est irréductible dans $\mathbb{Z}$. En comparant les modules au carré on obtient

$$(a^2 + 5b^2)(\alpha^2 + 5\beta^2) = 9$$

qui est impossible care $(a^2 + 5b^2) \geq 5$, $(\alpha^2 + 5\beta^2) \geq 5$.

3 n'est pas premier dans $\mathbb{Z}[i\sqrt{5}]$: Nous avons $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$, donc 3 divise ce produit. D'autre part 3 ne divise ni $2 + i\sqrt{5}$, ni $2 - i\sqrt{5}$. Il suffit de remarquer $\frac{2 \pm i\sqrt{5}}{3} \notin \mathbb{Z}[i\sqrt{5}]$. ■

4.6 Anneaux principaux

Rappel : Soient A un anneau commutatif et $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x |\ x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 4.6.1 *Un anneau commutatif* $(A, +, \cdot)$ *est dit anneau principal s'il est intègre et tout idéal de* A *est principal.*

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} |\ n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal. En utilisant le théorème division euclidienne pour les polynômes à coefficients dans un corps un va démontrer que pour tout corps K, l'anneau $K[X]$ est aussi principal.

4.6.1 Le pgcd dans un anneau principal

Soient A un anneau principal, $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in A$. Notre premier but est de comprendre en détail l'ensemble $\mathrm{Div}(a_1, \ldots, a_n) \subset A$ des diviseurs communs des éléments $a_1, \ldots, a_n$. Considérons l'idéal

$$(a_1, \ldots, a_n) = a_1 A + \ldots + a_n A \subset A$$

engendré par le sous-ensemble $\{a_1, \ldots, a_n\} \subset A$. Puisque A est un anneau principal, il existe $d \in A$ tel que

$$(a_1, \ldots, a_n) = (d)$$

et la proposition 4.5.6 montre que d est unique à la multiplication près par un élément inversible de A.

Proposition 4.6.2 *Soit* d *un générateur de l'idéal* $(a_1, \ldots, a_n)$. *Alors*

$$\mathrm{Div}(a_1, \ldots, a_n) = \mathrm{Div}(d),$$

donc d *est un diviseur commun des éléments* $a_1, \ldots, a_n$ *et l'ensemble des diviseurs communs des éléments* $a_1, \ldots, a_n$ *coïncide avec l'ensemble des diviseurs de* d.

Démonstration: Nous avons $(a_i) \subset (a_1,\dots,a_n) = (d)$. D'après la Proposition 4.5.6, il en résulte $d|a_i$ pour $1 \leq i \leq n$, donc d est un diviseur commun des éléments $a_1,\dots,a_n$. Ceci implique $\mathrm{Div}(d) \subset \mathrm{Div}(a_1,\dots,a_n)$. Réciproquement soit $\delta \in \mathrm{Div}(a_1,\dots,a_n)$. Puisque δ est un diviseur commun des éléments $a_1,\dots,a_n$, il en résulte que δ divise aussi tout élément de la forme $\sum_{i=1}^n a_i x_i$, donc tout élément de l'idéal $(a_1,\dots,a_n)$. Mais d appartient à cet idéal, donc $\delta|d$, c'est à dire $\delta \in \mathrm{Div}(d)$. ■

Définition 4.6.3 *Un générateur d de l'idéal $(a_1,\dots,a_n)$ s'appelle un* pgcd *des éléments $a_1,\dots,a_n$ et est noté* $\mathrm{pgcd}(a_1,\dots,a_n)$.

Remarquons que dans la théorie des anneaux principaux le pgcd d'un ensemble fini $\{a_1,\dots,a_n\}$ n'est pas nécessairement unique : il est unique à la multiplication près par un élément inversible de A, donc deux pgcd des éléments $\{a_1,\dots,a_n\}$ sont associés.

L'égalité $(a_1,\dots,a_n) = (d)$ écrite sous la forme

$$a_1A + \dots + a_nA = dA \tag{14}$$

s'appelle l'égalité ou l'identité de Bézout.

Définition 4.6.4 *Les éléments $a_1,\dots,a_n \in A$ sont dits premiers entre eux dans leur ensemble s'ils admettent 1 pour* pgcd. *Les éléments $a_1,\dots,a_n \in A$ sont dits premiers entre eux deux à deux si* $\mathrm{pgcd}(a_i,a_j) = 1$ *pour $i \neq j$.*

Exercice 4.6.5 Les entiers 9, 10, 5 sont premiers entre eux dans leur ensemble, mais ils ne sont pas premiers entre eux deux à deux.

Théorème 4.6.6 *(le théorème de Bézout pour les anneaux principaux) Soient A un anneau principal $a_1,\dots,a_n \in A$. Sont équivalentes :*

1. *$a_1,\dots,a_n$ sont premiers entre eux dans leur ensemble.*
2. *Il existe des éléments $u_1,\dots,u_n \in A$ tels que $\sum_{i=1}^n a_i u_i = 1_A$.*

Démonstration: Exercice. ■

Corollaire 4.6.7 *Soient $a, b, c \in A$. Si a est premier avec b et c, alors il est aussi premier avec bc.*

Démonstration: En utilisant l'égalité de Bézout on obtient des éléments u_1, u_2, v_1, $v_2 \in A$ tels que

$$au_1 + bu_2 = 1_A,\ av_1 + cv_2 = 1_A.$$

En multipliants les deux égalités on obtient une égalité de la forme $aU + bcV = 1_A$, donc a et bc sont premiers entre eux. ■

Corollaire 4.6.8 *(le théorème de Gauss pour les anneaux principaux) Soient $a, b, x \in A$ tels que $a|bx$. Si a est premier avec b, alors $a|x$*

Démonstration: Exercice. Utiliser la méthode de démonstration du théorème de Gauss dans $\mathbb{Z}$ (voir le Corollaire 1.2.4). ■

Corollaire 4.6.9 *Soit $a \in A$ et soient $b_1,\dots,b_n \in A$ premiers entre eux deux à deux. Si $b_i|a$ pour $1 \leq i \leq n$, alors $b_1 \dots b_n | a$.*

Démonstration: Supposons d'abord $n = 2$. Puisque $b_1|a$ il existe $q \in A$ tel que $a = b_1q$. Puisque $b_2|b_1q$ et b_1, b_2 sont premiers entre eux, il en résulte $b_2|q$, donc il existe $c \in A$ tel que $q = b_2c$. On obtient $a = b_1b_2c$, donc $b_1b_2|a$.

Pour le cas général se réduit au cas $n = 2$ en utilisant la récurrence par rapport à n. ■

Proposition 4.6.10 *Soit A un anneau principal et soit $p \in A$. Sont équivalentes :*

1. *p est irréductible.*
2. *p est premier.*

Démonstration: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$.

Puisque p irréductible il en résulte $\text{pgcd}(p,b) = p$ ou $\text{pgcd}(p,b) = 1$). Dans le premier cas il en résulte $p|b$ et dans le deuxième (en utilisant le théorème de Gauss) on obtient $p|c$. ■

Exercice 4.6.11 Énoncer et démontrer le théorème des restes chinois dans un anneau principal.

4.6.2 Le ppcm dans un anneau principal

Soit A un anneau principal et soient $a_1, \ldots, a_n \in A$. Notre but est de comprendre en détail l'ensemble $\text{Mult}(a_1, \ldots, a_n)$ des multiples communs des éléments $a_1, \ldots, a_n$. Remarquons que, pour i fixé, l'ensemble des multiples de a_i est précisément l'idéal principal (a_i), donc

$$\text{Mult}(a_1, \ldots, a_n) = (a_1) \cap \ldots \cap (a_n),$$

en particulier $\text{Mult}(a_1, \ldots, a_n)$ est un idéal de A. Puisque A est un anneau principal il existe $m \in A$ tel que $(a_1) \cap \ldots \cap (a_n) = (m)$ et m est unique à multiplication près par un élément inversible. Nous avons démontré.

Remarque 4.6.12 *Soient $a_1, \ldots, a_n \in A$ et soit m un générateur de l'intersection $(a_1) \cap \ldots \cap (a_n)$. Alors*

$$\text{Mult}(a_1, \ldots, a_n) = (m),$$

donc l'ensemble des multiples communs de a_i coïncide avec l'ideal principal engendré par m.

Définition 4.6.13 *Un générateur m de l'idéal $(a_1) \cap \ldots \cap (a_n)$ s'appelle un* ppcm *des éléments $a_1, \ldots, a_n \in A$ et est noté* $\text{ppcm}(a_1, \ldots, a_n)$.

Comme le pgcd, le ppcm est unique à multiplication près par un élément inversible.

Proposition 4.6.14 *Soient $a, b \in A$. Alors on a l'égalité*

$$\text{pgcd}(a,b)\text{ppcm}(a,b) = ab$$

à multiplication près par un élément inversible.

Démonstration: Soient $d := \text{pgcd}(a,b)$, $m := \text{ppcm}(a,b)$. On peut supposer $d \neq 0_A$, parce que si $d = 0$, alors $a = b = 0$ et l'égalité requise devient évidente. Soient $a', b' \in A$ tels que $a = a'd$, $b = b'd$. C'est facile de voir (en utilisant l'égalité et le théorème de Bézout) que a', b' sont premiers entre eux.

On va démontrer l'égalité d'idéaux $(a'b'd) = (m)$. En effet, pour démontrer l'inclusion $(a'b'd) \subset (m)$, remarquons que le produit $a'b'd = b'a = a'b$ est un multiple commun de a et b, donc appartient à l'idéal (m). On a donc $(a'b'd) \subset (m)$.

Pour l'inclusion inverse, soient $u, v \in A$ tels que $m = ua = vb$. On a donc $ua = vb$, donc $ua'd = vb'd$. A est intègre, donc l'égalité $ua'd = vb'd$ implique (puisque on a supposé $d \neq 0_A$) $ua' = vb'$. Puisque a', b' sont premiers entre eux, le théorème de Gauss donne $b'|u$, donc il existe $w \in A$ tel que $u = wb'$. On obtient $m = wb'a = wb'a'd$, donc $m \in (b'a'd)$, soit $(m) \subset (b'a'd)$.

L'égalité annoncée $(a'b'd) = (m)$ est donc démontrée. D'après la proposition 4.5.6 il existe un élément inversible $s \in A$ tel que $m = a'b'ds$, d'où $md = a'db'ds = abs$. ■

4.7 Anneaux euclidiens

Soit A un anneau commutatif intègre.

Définition 4.7.1 *Un stathme euclidien sur A est une application $\nu : A \setminus \{0_A\} \to \mathbb{N}$ vérifiant les deux propriétés*

1. $\forall (a,b) \in A \times (A \setminus \{0_A\})\ \exists (q,r) \in A \times A$ *tels que*
   (i) $a = bq + r$ *et*
   (ii) *soit* $r = 0_A$, *soit* $r \neq 0_A$ *et* $\nu(r) < \nu(b)$.
2. $\forall (a,b) \in (A \setminus \{0_A\}) \times (A \setminus \{0_A\}),\ \nu(a) \leq \nu(ab)$.

Attention, dans la défintion d'un stathme euclidien on ne requiert pas l'unicité du couple (q,r).

Définition 4.7.2 *Un anneau intègre A est dit euclidien s'il existe un stathme euclidien sur A.*

Exemples 4.7.3
1. $\mathbb{Z}$. En effet, l'application $\mathbb{Z} \setminus \{0\} \to \mathbb{N}$ donnée par $k \mapsto |k|$ est un stathme euclidien sur $\mathbb{Z}$.
2. L'anneau des polynômes $K[X]$, où K est un corps. En effet, l'application $K[X] \setminus \{0\} \to \mathbb{N}$ donnée par $P(X) \mapsto \deg(P(X))$ est un stathme euclidien sur $K[X]$.

Théorème 4.7.4 *(l'anneau des entiers de Gauss) Soit $\mathbb{Z}[i] := \{u + iv |\ u,\ v \in \mathbb{Z}\}$ muni de sa structure de sous-anneau de $\mathbb{C}$. L'application*

$$\nu : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N},\ \nu(u + iv) = u^2 + v^2$$

est un stathme euclidien sur $\mathbb{Z}[i]$. En particulier $\mathbb{Z}[i]$ est un anneau euclidien.

On va utiliser un lemme de géométrie élémentaire.

Lemme 4.7.5 *Soit $x \in \mathbb{R}^2$. Il existe $x' \in \mathbb{Z}^2$ tel que $d(x,x') < 1$.*

Démonstration: Exercice. ■

Démonstration: (du théorème) Nous avons l'identité $\nu(ab) = \nu(a)\nu(b)$, donc (puisque $\nu(b) \in \mathbb{N}^*$), ν vérifie la 2me condition dans la définition d'un stathme euclidien.

Pour la 1re condition : Soient $a = u + iv$, $b = s + it \in \mathbb{Z}[i]$ avec $b \neq 0$. À montrer l'existence d'un couple $(q,r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ t. q.

$$a = qb + r \text{ avec } r = 0 \text{ ou } (r \neq 0 \text{ et } \nu(r) < \nu(b)).$$

On applique le lemme 4.7.5 à $z := \frac{a}{b} \in \mathbb{C}$, en utilisant l'identification connue $\mathbb{C} = \mathbb{R}^2$. D'après ce lemme il existe $q \in \mathbb{Z}[i]$ tel que $d(z,q) < 1$, i.e. tel que $|z - q| < 1$. On obtient $|\frac{a}{b} - q|^2 < 1$, donc $|a - qb|^2 < |b|^2$. Posons $r := a - qb \in \mathbb{Z}[i]$. Avec ce choix on a bien $a = qb + r$. Si $r \neq 0$, l'inégalité $|a - qb|^2 < |b|^2$ devient $\nu(r) < \nu(b)$, donc le couple (q,r) trouvé satisfait les conditions requises. ■

Théorème 4.7.6 *Tout anneau eucliden est principal.*

Démonstration: Soient A un anneau euclidien et $\nu : A \setminus \{0_A\} \to \mathbb{N}$ un stathme euclidien sur A. Soit $I \subset A$ un idéal de A. On peut supposer $I \neq \{0_A\}$. Posons

$$m := \min\{\nu(x) |\ x \in I \setminus \{0_A\}\}.$$

et soit $a \in I \setminus \{0_A\}$ tel que $\nu(a) = m$. Nous allons montrer que $I = (a)$. Puisque $a \in I$ l'inclusion $(a) \subset I$ est évidente. Pour l'autre inclusion, soit $x \in I$. Puisque ν est un stathme euclidien sur A, il existe $(q,r) \in A \times A$ tel que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a) = m$. Dans l'égalité $x = aq + r$ nous avons $x \in I$ et $aq \in I$, donc $r \in I$. Nous affirmons que $r = 0_A$. En effet, dans le cas contraire on aurait $r \in I \setminus \{0_A\}$ et $\nu(r) < m$, ce qui contredit la définition de m. Donc $r = 0_A$, d'où $x = aq \in (a)$. ■

Corollaire 4.7.7 *Les anneaux*

1. $\mathbb{Z}$,
2. $K[X]$ *(où K est un corps)*,
3. $\mathbb{Z}[i]$

sont des anneaux euclidiens, donc principaux.

Exemple 4.7.8 L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal, mais n'est pas euclidien (voir TD).

4.8 Anneaux factoriels

4.8.1 Définitions. Propriétés. Exemples

Définition 4.8.1 *Soit A un anneau intègre. A est dit anneau factoriel si les deux propriétés suivantes sont vérifiées :*

1. *Pour tout élément $a \in A$, non nul et non inversible, il existe une suite finie $(p_1, \dots, p_m)$ d'éléments irréductibles de A telle que $a = \prod_{i=1}^{m} p_i$.*
2. *Soient $(p_1, \dots, p_m)$, $(q_1, \dots, q_n)$ deux suites finies d'éléments irréductibles de A telles que $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$. Alors $n = m$ et il existe une permutation σ de l'ensemble $\{1, \dots, m\}$ telle que pour tout i les éléments p_i, $q_{\sigma(i)}$ sont associés.*

Donc A est dit factoriel si tout élément $a \in A$, non nul et non inversible, se décompose en produit de facteurs irréductibles et la décomposition est unique à l'ordre des facteurs et à association près.

Remarque 4.8.2 *Soient A un anneau factoriel, $(p_1, \dots, p_m)$ une suite finie d'éléments irréductibles de A et p un élément irréductible de A tel que $p \mid \prod_{i=1}^{m} p_i$. Alors il existe $i \in \{1, \dots, m\}$ tel que p est associé avec p_i.*

Démonstration: Soit $b \in A$ tel que $a := \prod_{i=1}^{m} p_i = bp$. Si b est inversible, alors $m = 1$ et p est associé avec p_1. Si b n'est pas inversible, on le décompose en facteurs irréductibles et on introduit cette décomposition dans le produit bp. On obtient une nouvelle décomposition de a en facteurs irréductibles (dans laquelle p figure) et on utilise la propriété d'unicité (à l'ordre des facteurs et à association près) de la décomposition en facteurs premiers de a. ■

Proposition 4.8.3 *Soit A un anneau factoriel et soit $p \in A$. Sont équivalentes :*

1. *p est irréductible.*
2. *p est premier.*

Démonstration: Soit p irréductible et soient $b, c \in A$ tels que $p|bc$. Puisque A est factoriel, on peut décomposer b et c en produits de facteurs irréductibles :

$$b = \prod_{i=1}^{m} p_i, \; c = \prod_{j=1}^{n} q_j.$$

Alors $bc = (\prod_{i=1}^{m} p_i)(\prod_{j=1}^{n} q_j)$. D'après la remarque 4.8.2 p est associé avec l'un des facteurs p_i ou avec l'un des facteurs q_j. Donc $p|b$ ou $p|c$. ■

Corollaire 4.8.4 *Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :*

1. *A est factoriel.*
2. *Tout élément non nul et non inversible de A s'écrit comme produit d'éléments premiers.*

Démonstration: Exercice. ■

Soit A un anneau commutatif. Une suite $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est dite croissante si $I_n \subset I_{n+1}$ pour tout $n \in \mathbb{N}$. Une suite croissante d'idéaux est dite stationnaire s'il existe $k \in \mathbb{N}$ tel que pour tout $n \geq k$ on a $I_n = I_k$.

Remarque 4.8.5 *Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors la réunion $\bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.*

Remarque 4.8.6 *Soient A un anneau principal. Toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux de A est stationnaire.*

Démonstration: Puisque A est principal, la réunion $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal principal. Soit a un générateur de I. D'après la définition de la réunion d'une famille d'ensembles, il existe $k \in \mathbb{N}$ tel que $a \in I_k$, d'où $I = (a) \subset I_k$. D'autre part $I_k \subset \bigcup_{n\in\mathbb{N}} I_n = I$, donc $I = I_k$. Pour $n \geq k$ on a $I_k \subset I_n \subset I$, donc $I_n = I$. ■

Proposition 4.8.7 *Soit A un anneau intègre. Les propriétés suivantes sont équivalentes :*

1. *A est factoriel.*
2. *Les deux propriétés suivantes sont vérifiées :*
   (a) *Toute suite croissante d'idéaux principaux est stationnaire.*
   (b) *Tout élément irréductible est premier.*

Démonstration: L'implication 1. $\Rightarrow$ 2. est proposée comme exercice. On va démontrer l'implication plus difficile 2. $\Rightarrow$ 1., donc supposons que (a) et (b) sont vérifiées. D'après le corollaire 4.8.4 il suffit de démontrer que tout élément non-nul et non-inversible de A se décompose en produit d'éléments irréductibles.

Soit $a \in A$ non-nul et non-inversible. Supposons par l'absurde que a ne se décompose pas en produit de facteurs irréductibles. En particulier a n'est pas lui même irréductible, donc il se décompose sous la forme $a = bc$, avec b, c non-nuls et non-inversibles. Au moins l'un des deux facteurs, que nous notons a_1, ne se décompose pas en produit de facteurs irréductibles. Pourquoi ? Par récurrence on obtient une suite $(a_n)_{n\in\mathbb{N}}$ telle que

1. $a_0 = a$.
2. Pour tout $n \in \mathbb{N}$, a_n ne se décompose pas en produit de facteurs irréductibles.
3. Pour tout $n \in \mathbb{N}$, $a_{n+1} | a_n$.
4. Pour tout $n \in \mathbb{N}$, a_{n+1}, a_n ne sont pas associés.

Posons $I_n := (a_n)$. D'après la 3ème propriété la suite d'idéaux principaux $(I_n)_n$ est croissante et d'après la 4ème propriété cette suite n'est pas stationnaire. Ceci contredit l'hypothèse. ■

Théorème 4.8.8 *Tout anneau principal est factoriel.*

Démonstration: C'est une conséquence directe de la proposition 4.6.10, la remarque 4.8.6 et la proposition 4.8.7. ■

Le théorème suivant (dont la démonstration sera omise) fournit une classe importante d'anneaux factoriels.

Théorème 4.8.9 *Soit A un anneau factoriel. Alors l'anneau $A[X]$ des polynômes à coefficients dans A est factoriel.*

Exemple 4.8.10 L'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$ est factoriel, mais il n'est pas principal.

Corollaire 4.8.11 *Soient K un corps et $n \in \mathbb{N}^*$. Alors l'anneau $K[X_1, \ldots, X_n]$ des polynômes en n variables à coefficients dans K est un anneau factoriel.*

A remarquer que, pour $n \geq 2$ l'anneau $K[X_1, \ldots, X_n]$ n'est pas principal.

4.8.2 pgcd et ppcm dans un anneau factoriel

Soient A un anneau factoriel et $\mathcal{P}$ l'ensemble des éléments premiers de A. La relation $\text{Ass} \subset \mathcal{P} \times \mathcal{P}$ définie par

$$\text{Ass} := \{(p,q) \in \mathcal{P} \times \mathcal{P} |\ p,\ q \text{ sont associés}\}$$

est une relation d'équivalence sur $\mathcal{P}$. Dans chaque classe d'équivalence $C \in \mathcal{P}/\text{Ass}$ choisissons un représentant $p_C \in C$. Soit $P := \{p_C |\ C \in \mathcal{P}/\text{Ass}\}$ le sous-ensemble de $\mathcal{P}$ formé avec les représentants choisis.

Soit $p \in P$. La valuation associée à p est l'application $v_p : A \setminus \{0_A\} \to \mathbb{N}$ définie par

$$v_p(a) := \max\{k \in \mathbb{N} |\ p^k | a\}.$$

Remarque 4.8.12 *Soit A un anneau factoriel.*

1. *Soit $a \in A \setminus \{0\}$. Alors*
$$a = u \prod_{v_p(a) \neq 0} p^{v_p(a)},$$
où $u \in A$ est un élément inversible.
2. *Soient $a, b \in A \setminus \{0\}$. Alors $a|b$ si et seulement si pour tout $p \in P$ on a $v_p(a) \leq v_p(b)$.*

Dans la 1ère égalité on utilise la convention : le produit d'un sous-ensemble E d'éléments de A vaut 1_A si $E = \emptyset$.

Démonstration: 1. Si a est inversible alors l'affirmation est claire. Si a est non–inversible on obtient une décomposition de la forme $a = \prod_{i=1}^{n} q_i$ avec q_i premiers. Soit $p_i \in P$ associé avec q_i. On obtient $a = u \prod_{i=1}^{n} p_i$ avec u inversible. En regroupant les facteurs on arrive à une décomposition de la forme $a = u \prod_{s=1}^{l} p_{i_s}^{n_s}$, où $1 \leq l \leq n$, $n_s \in \mathbb{N}^*$ et $p_{i_s} \neq p_{i_t}$ pour $s \neq t$. C'est facile de voir que $n_s = v_{p_{i_s}}(a)$ et $v_p(a) = 0$ pour $p \notin \{p_{i_1}, \ldots, p_{i_l}\}$.

2. Exercice. ■

Soient $a_1, \ldots, a_n$ éléments non-nuls de A. Nous avons noté par $\text{Div}(a_1, \ldots, a_n)$, $\text{Mult}(a_1, \ldots, a_n)$ l'ensemble des diviseurs communs, respectivement l'ensemble des multiples communs des éléments $a_1, \ldots, a_n$.

Proposition 4.8.13 *Soient A un anneau factoriel et $a_1, \ldots, a_n$ éléments non-nuls de A. Alors*

1. *Il existe $d \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que* $\text{Div}(a_1, \ldots, a_n) = \text{Div}(d)$, *donc d est un diviseur commun des éléments $a_1, \ldots, a_n$ et l'ensemble des diviseurs communs des éléments $a_1, \ldots, a_n$ coïncide avec l'ensemble des diviseurs de d.*
2. *Il existe $m \in A \setminus \{0\}$, unique à multiplication près avec un élément inversible, tel que* $\text{Mult}(a_1, \ldots, a_n) = (m)$, *donc l'ensemble des multiples communs des éléments $a_1, \ldots, a_n$ coïncide avec l'idéal principal engendré par m.*

Démonstration: On va démontrer l'existence, l'unicité à multiplication près avec un élément inversible est proposée comme exercice. Pour $p \in P$ posons

$$k_p := \min\{v_p(a_i) |\ 1 \leq i \leq n\},\ l_p := \max\{v_p(a_i) |\ 1 \leq i \leq n\}.$$

C'est facile de voir (en utilisant la remarque 4.8.12) que

$$d := \prod_{k_p \neq 0} p^{k_p},\ m := \prod_{l_p \neq 0} p^{l_p}$$

satisfont les égalités requises

$$\text{Div}(a_1, \ldots, a_n) = \text{Div}(d),\ \text{Mult}(a_1, \ldots, a_n) = (m).$$

■

La proposition 4.8.13 nous permet de définir :

Définition 4.8.14 *Soient A un anneau factoriel et $a_1, \dots, a_n$ éléments non-nuls de A. Un élément $d \in A \setminus \{0\}$ qui vérifie l'égalité* $\mathrm{Div}(a_1, \dots, a_n) = \mathrm{Div}(d)$ *s'appelle* $\mathrm{pgcd}(a_1, \dots, a_n)$. *Un élément $m \in A \setminus \{0\}$ qui vérifie l'égalité* $\mathrm{Mult}(a_1, \dots, a_n) = (m)$ *s'appelle* $\mathrm{ppcm}(a_1, \dots, a_n)$.

D'après la proposition 4.8.13 le pgcd et le ppcm existent et sont uniques à multiplication près par un élément inversible.

Exercice 4.8.15 Soient a, b éléments non-nuls de l'anneau factoriel A. Alors $\mathrm{pgcd}(a,b)\mathrm{ppcm}(a,b) = ab$ à multiplication près par un élément inversible.

4.9 L'anneau des polynômes à coefficients dans un corps

Soit K un corps. On commence par la

Définition 4.9.1 *L'ensemble des polynômes à coefficients dans K est défini par*

$$K[X] := \{(a_k)_{k\geq 0} |\ \exists N \in \mathbb{N} \text{ tel que } a_k = 0 \text{ pour tout } k \geq N\}.$$

Donc la donnée d'un polynôme à coefficients dans K est équivalente à la donnée d'une suite $(a_k)_{k\geq 0}$ dont tous les termes sont nuls à partir d'un certain indice. Cet ensemble a une structure naturelle de K-espace vectoriel, l'addition dans cet espace vectoriel étant donnée par

$$((a_k)_{k\geq 0}) + ((b_k)_{k\geq 0}) := (a_k + b_k)_{k\geq 0}\ ,$$

et la multiplication par les scalaires dans cet espace vectoriel étant donnée par la formule

$$a((a_k)_{k\geq 0}) := (aa_k)_{k\geq 0}\ .$$

Pour tout $k \in \mathbb{N}$ notons par $e_k \in K[X]$ la suite définie par

$$(e_k)_i = \delta_{ik}\ ,$$

donc

$$e_0 = (1,0,0\dots)\ \ e_1 = (0,1,0,0,\dots)\ ,\ e_k = (0,\dots,0,1,0,0\dots) \text{ avec 1 sur la } k\text{ème place}\ .$$

C'est facile de vérifier que la famille $(e_k)_{k\in\mathbb{N}}$ est une base de $K[X]$, donc $K[X]$ est un K-espace vectoriel de dimension infinie. Un polynôme de la forme $ae_0 = (a,0,0\dots)$ sera appelé *polynôme constant*.

Définition 4.9.2 *La multiplication dans $K[X]$ est la loi de composition interne donnée par la formule*

$$((a_k)_{k\geq 0})((b_l)_{l\geq 0}) = (c_n)_{n\geq 0} \text{ où } c_n := \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l\ .$$

C'est facile de vérifier que cette loi de composition interne a les propriétés suivantes :

1. est associative,
2. admet un élément neutre, à savoir e_0,
3. est commutative,
4. est distributive par rapport à l'addition dans $K[X]$.

On va désigner l'élément $e_0 \in K[X]$ par 1 (en sous-entendant l'élément neutre de la multiplication définie dans $K[X]$) et le polynôme constant $ae_0 = (a,0,0\dots)$ sera noté simplement par a_0, donc chaque scalaire $a \in K$ sera identifié avec le polynôme constant $ae_0 = (a,0,0\dots)$ qui lui correspond.

En utilisant la définition de la multiplication c'est facile de vérifier que pour tout $k \in \mathbb{N}^*$ on a

$$(e_1)^k = e_k\ .$$

On va poser $X := e_1$. Avec la convention $X^0 := 1$ on obtient l'égalité suivante

$$(a_k)_{k\geq 0} = \sum_{k\geq 0} a_k X^k\ ,$$

(somme qui contient seulement un nombre fini de termes non-nuls). Cette égalité importante fait la liaison entre la définition moderne de la notion de polynôme (voir la définition 4.9.1) et la manière élémentaire d'introduire cette notion, à savoir comme une expression algébrique de la forme

$$a_0 + a_1 X + \cdots + a_N X^N \, .$$

La multiplication des polynômes donnée par la définition 4.9.2 correspond à la multiplication des expressions algébriques introduite au lycée.

On peut montrer facilement que $K[X]$, muni de l'addition et de la multiplication des polynômes, est *un anneau commutatif*.

Définition 4.9.3 *Le degré d'un polynôme $P(X) = \sum_{k\geq 0} a_k X^k$ est défini par*

$$\deg(P(X)) := \begin{cases} \max\{k \in \mathbb{N} |\, a_k \neq 0\} & \text{si} \quad P(X) \neq 0 \\ -\infty & \text{si} \quad P(X) = 0 \end{cases} .$$

Donc le degré d'un polynôme *non-nul* est (l'exposant de) la puissance maximale de X qui intervient effectivement dans l'expression de $P(X)$. Avec cette définition on obtient facilement la formule générale

$$\deg(P(X)Q(X)) = \deg(P(X)) + \deg(Q(X)) \tag{15}$$

En utilisant cette formule on obtient

Remarque 4.9.4 *1. L'anneau $K[X]$ est intègre, i.e. pour tous deux polynômes $P(X)$, $Q(X) \in K[X]$ nous avons l'implication*

$$P(X)Q(X) = 0 \Rightarrow \Big(P(X) = 0 \text{ ou } Q(X) = 0\Big) .$$

2. Les seuls polynômes inversibles dans l'anneau $K[X]$ sont les polynômes constants non-nuls.

Dans cette remarque la condition "inversible" signifie "inversible par rapport à la multiplication des polynômes", donc, par définition, un polynôme $P(X)$ est inversible si et seulement si il existe $Q(X) \in K[X]$ tel que $P(X)Q(X) = 1$. Si on multiplie un polynôme $P(X)$ par un élément inversible (donc par un polynôme constant non-nul) on va obtenir un polynôme qui a les mêmes propriétés de divisibilité (par exemple les mêmes diviseurs et les mêmes multiples) que $P(X)$. Cette remarque montre que, pour l'étude des problèmes de divisibilité dans $K[X]$ il suffit de se concentrer sur les *polynômes unitaires* au sens de la définition suivante :

Définition 4.9.5 *Un polynôme $P(X) \in K[X] \setminus \{0\}$ est dit unitaire si son coefficient du terme de plus haut degré (son coefficient dominant) est égal à 1.*

Par définition, un polynôme unitaire s'écrit donc sous la forme

$$X^d + \sum_{i=0}^{d-1} a_i X^i \text{ où } d = \deg(P(X)) \, .$$

Remarquons que tout polynôme $P(X) \in K[X] \setminus \{0\}$ s'écrit d'une manière unique comme un produit

$$P(X) = a\tilde{P}(X)$$

où $\tilde{P}(X)$ est un polynôme unitaire et $a \in K^*$ est le coefficient du terme de plus haut degré de $P(X)$.

Définition 4.9.6 *Soient $P(X)$, $S(X) \in K(X)$. On dit que $P(X)$ divise $S(X)$ (ou que $S(X)$ est divisible par $P(X)$) s'il existe $Q(X) \in K(X)$ tel que $S(X) = Q(X)P(X)$.*

Définition 4.9.7 *Un polynôme $P(X)$ avec $\deg(P(X)) > 0$ est dit irréductible s'il n'admet aucune factorisation de la forme $P(X) = Q_1(X)Q_2(X)$ avec $\deg(Q_i(X)) > 0$ pour $i \in \{1, 2\}$.*

Donc un polynôme $P(X)$ de degré strictement positif est irréductible si et seulement si l'un des deux facteurs de toute factorisation de $P(X)$ est un polynôme constant (qui sera nécessairement non-nul, donc inversible). En utilisant la définition et la formule (15) on obtient facilement

Remarque 4.9.8 *Tout polynôme de degré 1 est irréductible.*

Dans la section suivante on va donner la classification complète de tous les polynômes irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$. En particulier on va voir que, tandis que dans $\mathbb{C}[X]$ la réciproque de la remarque 4.9.8 est vraie (donc un polynôme $P(X) \in \mathbb{C}[X]$ est irréductible si et seulement si $\deg(P(X)) = 1$) dans $\mathbb{R}[X]$ la réciproque de cette remarque est fausse. En effet, il suffit de remarquer que le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$.

Définition 4.9.9 *Soit $P(X) = \sum_{k\geq 0} a_k X^k \in K(X)$. La fonction polynômiale associée à $P(X)$ est la fonction $p : K \to K$ définie par*

$$p(x) = P(x) = \sum_{k\geq 0} a_k x^k \ \forall x \in K \ .$$

L'équation algébrique associée à $P(X)$ est l'équation

$$P(x) = 0 \ .$$

Une solution $x_0 \in K$ de cette équation s'appelle racine de $P(X)$.

Notons que l'application

$$F : K[X] \to \mathcal{F}(K, K)$$

qui associe à tout polynôme sa fonction polynômiale est un morphisme d'anneaux, donc pour deux polynômes $P(X)$, $Q(X) \in K[X]$ on a les identités

$$(P + Q)(x) = P(x) + Q(x) \ , \ (PQ)(x) = P(x)Q(x) \ \forall x \in K \ .$$

Remarque 4.9.10 *Soit K un corps fini (par exemple $K = \mathbb{F}_p$ pour un nombre premier p). Alors l'application $F : K[X] \to \mathcal{F}(K, K)$ est surjective.*

Démonstration: Notons $n = \text{card}(K)$, $K = \{b_1, \ldots, b_n\}$ avec $b_i \neq b_j$ pour $i \neq j$. Pour $1 \leq i \leq n$ soit $P_i(X)$ le polynôme de degré $n-1$ défini par $P_i(X) = \prod_{j\neq i}(X - b_j)$. Remarquons que

$$P_i(b_i) = \prod_{j\neq i}(b_i - b_j) \neq 0, \ P_i(b_j) = 0 \text{ pour } j \neq i.$$

Soit $f \in \mathcal{F}(K, K)$. Posons $Q(X) := \sum_{i=1}^{n} \frac{f(b_i)}{P_i(b_i)} P_i(X) \in K[X]$. Pour $1 \leq j \leq n$ on a

$$Q(b_j) = \sum_{i=1}^{n} \frac{f(b_i)}{P_i(b_i)} P_i(b_j) = \frac{f(b_j)}{P_j(b_j)} P_j(b_j) = f(b_j),$$

donc la fonction polynomiale associée à $Q(X)$ est f. ∎

4.9.1 La division euclidienne dans l'anneau des polynômes

Théorème 4.9.11 *(le théorème de division euclidienne pour les polynômes) Soit $S(X)$, $P(X) \in K(X)$ avec $P(X) \neq 0$. Alors il existe une unique paire $(Q(X), R(X)) \in K[X] \times K[X]$ avec $\deg(R(X)) < \deg(P(X))$ telle que*

$$S(X) = Q(X)P(X) + R(X).$$

Le polynôme $Q(X)$ s'appelle le quotient et le polynôme $R(X)$ s'appelle le reste de la division euclidienne de $S(X)$ par $P(X)$.

Remarque 4.9.12 *Le théorème 4.9.11 montre que $(K[X], +, \cdot)$ est un anneau euclidien, donc principal.*

Le théorème 4.9.11 a quelques corollaires très importants :

Corollaire 4.9.13 *Soit $a \in K$. Un polynôme $P(X) \in K(X)$ est divisible par $X - a$ si et seulement si $P(a) = 0$, i.e. si et seulement si a est une racine de $P(X)$.*

Démonstration: En effet si $P(X)$ est divisible par $X-a$, alors on peut écrire $P(X)=(X-a)Q(X)$ pour un polynôme $Q(X)\in K[X]$. En remplaçant X par a on obtient $P(a)=0\cdot Q(a)=0$. Réciproquement, supposons que $P(a)=0$. En appliquant le théorème de division euclidienne aux polynômes $P(X)$, $X-a$ on obtient

$$P(X)=Q(X)(X-a)+R$$

où $\deg(R)\leq 0$, donc R est un polynôme constant. En remplaçant X par a on obtient $R=0$, donc $P(X)=Q(X)(X-a)$, ce qui montre que $P(X)$ est divisible par $X-a$. ■

Définition 4.9.14 *Soit $P(X)\in K(X)$ avec $\deg(P(X))>0$ et $a\in K$ une racine de $P(X)$. La multiplicité (ou l'ordre de multiplicité) de la racine a est définie par*

$$\mathrm{mult}_P(a):=\max\{k\in\mathbb{N}^*|\ (X-a)^k|P(X)\}\ .$$

Donc $\mathrm{mult}_P(a)$ est l'exposant de la puissance maximale de $X-a$ qui divise $P(X)$.

Définition 4.9.15 *Soient $P_1(X),\dots,P_k(X)\in K[X]$.*

1. *Un polynôme $P(X)\in K(X)\setminus\{0\}$ est dit diviseur commun des polynômes $P_i(X)$ si $P(X)|P_i(X)$ pour $1\leq i\leq k$.*
2. *Un polynôme $P(X)\in K(X)\setminus\{0\}$ s'appelle le plus grand commun diviseur (le pgcd) des polynômes $P_i(X)$ si les conditions suivantes sont vérifiées :*
   (a) *$P(X)$ est un diviseur commun des polynômes $P_i(X)$,*
   (b) *$P(X)$ est un diviseur commun de degré maximal de ces polynômes,*
   (c) *$P(X)$ est un polynôme unitaire.*

La condition 2c dans cette défintion est imposée par convention pour assurer l'unicité du plus grand commun diviseur. Si on n'impose pas cette condition, le pgcd sera seulement bien défini à multiplication par une constante non-nulle près.

Corollaire 4.9.16 *Soient $P_1(X),\dots,P_k(X)\in K[X]$ non tous nuls. Alors*

1. *Il existe un unique pgcd des polynômes $P_i(X)$, polynôme qui sera noté $\mathrm{pgcd}(P_1(X),\dots,P_k(X))$,*
2. *Il existe des polynômes $U_1(X),\dots,U_k(X)\in K[X]$ tels que*

$$\mathrm{pgcd}(P_1(X),\dots,P_k(X))=\sum_{i=1}^{k}U_i(X)P_i(X)\ . \tag{16}$$

Démonstration: L'unicité du pgcd est évidente (exercice). L'existence du pgcd et la formule (16) est une conséquence du théorème de division euclidienne. Commençons par le cas $k=2$.

Pour $k=2$ on obtient facilement une démonstration effective (qui donne un algorithme explicite de calcul du pgcd) par récurrence par rapport à $\deg(P_2(X))$. Plus précisément on va démontrer par récurrence par rapport à d que pour $d\in\{-\infty\}\cup\mathbb{N}=\{-\infty,0,1,2,\dots\}$ l'affirmation suivante est vraie :

($\mathcal{P}_d$)Toute paire de polynômes non tous nuls $(P_1(X),P_2(X))$ avec $\deg(P_2(X))=d$ admet un pgcd qui est donné par une expression de la forme

$$\mathrm{pgcd}(P_1(X),P_2(X))=U_1(X)P_1(X)+U_1(X)P_2(X)\ .$$

Pour $d=-\infty$ (initialisation) on a $P_2(X)=0$, donc (en tenant compte de l'hypothèse), on a nécessairement $P_1(X)\neq 0$. Remarquons que dans ce cas l'ensemble des diviseurs communs de $P_1(X)$ et $P_2(X)$ coïncide avec l'ensemble des diviseurs de $P_1(X)$, donc dans ce cas on a $\mathrm{pgcd}(P_1(X),P_2(X))=\tilde{P}_1(X)$, où $\tilde{P}_1(X)$ désigne le polynôme unitaire associé à $P_1(X)$. Si on désigne par a le coefficient du terme de plus haut degré de $P_1(X)$ on obtient dans ce cas $\mathrm{pgcd}(P_1(X),P_2(X))=a^{-1}P_1(X)$ et notre affirmation pour $d=-\infty$ est démontrée en choisissant $U_1(X)=a^{-1}$, $U_2(X)=0$.

Supposons maintenant que $d > -\infty$ et que la proposition $\mathcal{P}_{d'}$ est vraie pour tout $d' < d$ (l'hypothèse de récurrence). Puisque $d > -\infty$ on a $P_2(X) \neq 0$, donc on peut appliquer le théorème de division euclidienne à la paire $(P_1(X), P_2(X))$. On obtient

$$P_1(X) = Q(X)P_2(X) + R(X)\,, \tag{17}$$

avec $\deg(R(X)) < \deg(P_2(X))$. Par l'hypothèse de récurrence on sait que $\operatorname{pgcd}(P_2(X), R(X))$ existe et est donné par une expression de la forme

$$\operatorname{pgcd}(P_2(X), R(X)) = V_1(X)P_2(X) + V_2(X)R(X)\,. \tag{18}$$

Mais en utilisant (17) on constate que l'ensemble des diviseurs communs des polynômes $P_1(X)$, $P_2(X)$ coïncide avec l'ensemble des diviseurs communs des polynômes $P_2(X)$, $R(X)$. Donc $\operatorname{pgcd}(P_1(X), P_2(X))$ existe aussi et

$$\operatorname{pgcd}(P_1(X), P_2(X)) = \operatorname{pgcd}(P_2(X), R(X))\,.$$

En utilisant (18) puis (17) on obtient

$$\operatorname{pgcd}(P_1(X), P_2(X)) = V_1(X)P_2(X) + V_2(X)R(X) = V_1(X)P_2(X) + V_2(X)(P_1(X) - Q(X)P_2(X))$$

$$= V_2(X)P_1(X) + (V_1(X) - V_2(X)Q(X))P_2(X)\,,$$

et notre affirmation est démontrée pour d en choisissant $U_1(X) = V_2(X)$, $U_2(X) = (V_1(X) - V_2(X)Q(X))$.

Pour $k > 2$ le théorème est démontré par récurrence par rapport à k en utilisant la formule recursive (exercice)

$$\operatorname{pgcd}(P_1(X), \ldots, P_{k-1}(X), P_k(X)) = \operatorname{pgcd}(\operatorname{pgcd}(P_1(X), \ldots, P_{k-1}(X)), P_k(X))\,.$$

Par exemple, pour $k = 3$ on a

$$\operatorname{pgcd}(P_1(X), P_2(X), P_3(X)) = \operatorname{pgcd}(\operatorname{pgcd}(P_1(X), P_2(X)), P_3(X))\,,$$

donc il suffit d'appliquer deux fois la théorème d'existence pour le pgcd des deux polynômes. ■

Remarque 4.9.17 *La démonstration du corollaire 4.9.16 fournit un algorithme explicite pour le calcul du pgcd des deux polynômes, algorithme qui s'appelle l'algorithme d'Euclid :*

1. *Est-ce que $P_2(X) = 0$? Si $P_2(X) = 0$ on pose $\operatorname{pgcd}(P_1(X), P_2(X)) = \tilde{P}_1(X)$ et on arrête l'algorithme. Sinon on passe à l'étape suivante.*
2. *Si $P_2(X) \neq 0$ on fait la division euclidienne de $P_1(X)$ par $P_2(X)$, on remplace la paire initiale $(P_1(X), P_2(X))$ par la paire $(P_2(X), R(X))$ où $R(X)$ est le reste de cette division euclidienne et on revient à la question (1), posée pour la nouvelle paire.*

Donc le pgcd cherché coïncide avec `le polynôme unitaire associé au` *dernier reste non-nul obtenu dans cette suite finie de divisions euclidiennes.*
Pour le calcul du pgcd dans la cas général $k \geq 2$ on utilise la formule générale

$$\operatorname{pgcd}(P_1(X), \ldots, P_{k-1}(X), P_k(X)) = \operatorname{pgcd}(\operatorname{pgcd}(P_1(X), \ldots, P_{k-1}(X)), P_k(X))\,,$$

qui permet de réduire le problème au cas $k = 2$.

Définition 4.9.18 *On dit que k polynômes $P_1(X), \ldots, P_k(X) \in K[X]$, non tous nuls, sont premiers entre eux si $\operatorname{pgcd}(P_1(X), \ldots, P_k(X)) = 1$, i.e. si ces polynômes n'admettent aucun diviseur commun de degré strictement positif.*

Corollaire 4.9.19 *(Théorème de Bézout) Soient $P_1(X), \ldots, P_k(X) \in K[X]$ non tous nuls. Alors les conditions suivantes sont équivalentes :*

1. *$P_1(X), \ldots, P_k(X)$ sont premiers entre eux,*
2. *il existe $U_1(X), \ldots, U_k(X) \in K[X]$ tels que $\sum_{i=1}^{k} U_i(X)P_i(X) = 1$.*

4.9.2 Décomposition d'un polynôme en produit de polynômes irréductibles. Polynômes scindés

Le corollaire suivant sera énoncé sans démonstration. La démonstration est proposée comme exercice. Pour comprendre l'idée de démonstration commencer par le cas particulier d'un polynôme de degré 2, puis essayer de généraliser votre argument.

Corollaire 4.9.20 *Tout polynôme $P(X) \in K[X]$ avec $\deg(P(X)) > 0$ admet une factorisation de la forme*

$$P(X) = a(Q_1(X))^{m_1} \dots (Q_k(X))^{m_k} = a\prod_{i=1}^{k}(Q_i(X))^{m_i}\ ,$$

où a est le coefficient du terme de plus haut degré de $P(X)$, $m_i \in \mathbb{N}^*$ et $Q_i(X)$ sont des polynômes irréductibles unitaires distincts deux à deux. Cette factorisation est unique, à permutations des facteurs près.

Si tous les polynômes irréductibles unitaires $Q_i(X)$ dans cette factorisation sont des polynômes du premier degré, on va dire que $P(X)$ est *scindé dans K*. Remarquer qu'un polynôme *unitaire* du premier degré s'écrit sous la forme $X - a$ avec $a \in K$. Notre définition devient :

Définition 4.9.21 *Un polynôme $P(X) \in K[X]$ avec $\deg(P(X) > 0$ est dit scindé dans K s'il admet une factorisation de la forme*

$$P(X) = a(X - a_1)^{m_1} \dots (X - a_k)^{m_k} = a\prod_{i=1}^{k}(X - a_i)^{m_i}$$

où $m_i \in \mathbb{N}^*$ et $a_i \in K$ sont distincts deux à deux.

Remarquer que si $P(X)$ admet une telle factorisation, alors

1. a est le coefficient du terme de plus haut degré de $P(X)$,
2. $\deg(P(X)) = \sum_{i=1}^{k} m_i$,
3. l'ensemble des racines de $P(X)$ est $\{a_1, \dots, a_k\}$,
4. $\text{mult}_P(a_i) = m_i$ pour $1 \le i \le k$.

Définition 4.9.22 *Soient $n \in \mathbb{N}^*$, $k \in \mathbb{N}$ tel que $0 \le k \le n$. Le polynôme symétrique élémentaire $s_{n,k}(X_1, \dots, X_n)$ est un polynôme en n variables à coefficients entiers de degré k défini par*

$$s_{n,k}(X_1, \dots, X_n) := \begin{cases} 1 & \text{si} \quad k = 0 \\ \displaystyle\sum_{1 \le j_1 < \dots < j_k \le n} X_{j_1} \dots X_{j_k} & \text{si} \quad k > 0. \end{cases}$$

Par exemple :

$$s_{2,0}(X_1, X_2) = 1,\ s_{2,1}(X_1, X_2) = X_1 + X_2,\ s_{2,2}(X_1, X_2) = X_1X_2,\ s_{3,0}(X_1, X_2, X_3) = 1,$$
$$s_{3,1}(X_1, X_2, X_3) = X_1 + X_2 + X_3,\ s_{3,2}(X_1, X_2, X_3) = X_1X_2 + X_1X_3 + X_2X_3,\ s_{3,3}(X_1, X_2, X_3) = X_1X_2X_3.$$

Théorème 4.9.23 *(relations entre les racines et les coefficients d'un polynôme scindé) Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ un polynôme scindé de degré $n > 0$. Décomposons $P(X)$ sous la forme $P(X) = a_n \prod_{i=1}^{n}(X - r_i)$, donc chaque racine r de $P(X)$ intervient $\text{mult}_P(r)$ fois dans la famille $(r_1, \dots, r_n) \in K^n$. Alors on a les identités :*

$$\frac{a_{n-k}}{a_n} = (-1)^k s_{n,k}(r_1, \dots, r_n) \text{ pour } 0 \le k \le n.$$

En particulier

$$\frac{a_{n-1}}{a_n} = -\sum_{i=1}^{n} r_i\ ,\quad \frac{a_0}{a_n} = (-1)^n \prod_{i=1}^{r} r_i\,.$$

Démonstration: On développe $\prod_{i=1}^{d}(X - r_i)$ et on identifie les coefficients de X^k dans l'égalité

$$\sum_{i=0}^{n} a_i X^i = a_n \prod_{i=1}^{n}(X - r_i).$$

■

4.9.3 Le théorème de Gauss-d'Alembert

Le théorème de Gauss d'Alembert, où le théorème fondamental de l'algèbre, a beaucoup de conséquences importantes dans plusieurs domaines des mathématiques modernes. Nous allons utiliser ce résultat plus tard dans l'étude des endomorphismes d'un espace vectoriel de dimension finie. La démonstration de ce théorème dépasse le niveau et le but de ce cours, donc sera omise.

Théorème 4.9.24 *Tout polynôme $P(X) \in \mathbb{C}[X]$ avec $\deg(P(X)) > 0$ admet une racine complexe.*

En utilisant la terminologie de l'algèbre moderne, ce théorème affirme que $\mathbb{C}$ est un corps algébriquement clos. En général, un corps K est dit algébriquement clos si tout polynôme $P(X) \in K[X]$ avec $\deg(P(X)) > 0$ admet une racine dans K. Remarquer que $\mathbb{R}$ n'est pas algébriquement clos parce que, par exemple, le polynôme $X^2 + 1 \in \mathbb{R}[X]$ d'admet aucune racine réelle.

D'après le corollaire 4.9.13 l'existence d'une racine $a \in \mathbb{C}$ d'un polynôme $P(X) \in \mathbb{C}[X]$ implique la divisibilité de $P(X)$ par $X - a$. Si le quotient de $Q(X)$ de $P(X)$ par $X - a$ est encore un polynôme de degré strictement positif (i.e. si $\deg(P(X)) \geq 2$), on peut appliquer le théorème 4.9.24 à $Q(X)$ et on déduit que $Q(X)$ est aussi divisible par une polynôme de la forme $X - b$. Par récurrence on obtient donc

Corollaire 4.9.25 *Tout polynôme $P(X) \in \mathbb{C}[X]$ avec $\deg(P(X)) > 0$ est scindé dans $\mathbb{C}$ donc se factorise sous la forme*

$$P(X) = a(X - a_1)^{m_1} \dots (X - a_k)^{m_k} = a \prod_{i=1}^{k} (X - a_i)^{m_i} \tag{19}$$

où a est le coefficient du terme de plus haut degré de $P(X)$, $m_i \in \mathbb{N}^*$ et $a_i \in K$ sont distincts deux à deux.

Comme nous avons vu dans la section précédente, dans la factorisation (19) a est le coefficient du terme de plus haut degré de $P(X)$, on a $\deg(P(X)) = \sum_{i=1}^{k} m_i$, l'ensemble des racines de $P(X)$ est $\{a_1, \dots, a_k\}$ et $\text{mult}_P(a_i) = m_i$ pour $1 \leq i \leq k$.

Le dernier corollaire donne une classification complète des polynômes irréductibles dans $K[X]$ pour $K \in \{\mathbb{C}, \mathbb{R}\}$:

Corollaire 4.9.26 *1. L'ensemble des polynômes irréductibles unitaires de $\mathbb{C}[X]$ est*

$$\{X - a |\ a \in \mathbb{C}\}.$$

2. L'ensemble des polynômes irréductibles unitaires de $\mathbb{R}[X]$ est

$$\{X - a \mid a \in \mathbb{C}\} \cup \{X^2 + bX + c \mid a,\ b \in \mathbb{R},\ b^2 - 4c < 0\}\ .$$

La première partie du corollaire 4.9.26 est une conséquence directe de la remarque 4.9.8 et du corollaire 4.9.25. Pour la deuxième partie remarquons d'abord que tout polynôme du 2me degré à coefficients réels *à discriminant strictement négatif* est irréductible dans $\mathbb{R}[X]$. En effet, puisque un tel polynôme n'admet pas de racines réelles, il n'admet aucune factorisation (dans $\mathbb{R}[X]$!) en produit de polynômes du 1er degré. Pour démontrer que, réciproquement, tout polynôme irréductible dans $\mathbb{R}[X]$ est soit de la forme $X - a$, soit de la forme $X^2 + bX + c$ avec $b^2 - 4c < 0$, on utilise la proposition suivante concernant l'ensemble des racines *complexes* d'un polynômes à coefficients réels :

Proposition 4.9.27 *Soit $P(X) \in \mathbb{R}[X]$ avec $\deg(P(X)) > 0$ est soit $\mathcal{R}_P \subset \mathbb{C}$ l'ensemble des racines complexes de $P(X)$. Alors*

1. *$\mathcal{R}_P$ est stable par conjugaison, i.e on a l'implication $z \in \mathcal{R}_P \Rightarrow \bar{z} \in \mathcal{R}_P$.*
2. *Si $z \in \mathcal{R}_P$ on a*

$$\text{mult}_P(z) = \text{mult}_P(\bar{z})\ .$$

3. *En posant*

$$\mathcal{R}_P = \{a_1, \ldots, a_l, \alpha_1, \bar{\alpha}_1, \ldots, \alpha_m, \bar{\alpha}_m\}$$

avec $a_i \in \mathbb{R}$ *et* $\mathfrak{Im}(\alpha_i) > 0$ *et en désignant par a le coefficient du terme de plus haut degré de* $P(X)$ *on obtient la factorisation*

$$P(X) = a\prod_{i=1}^{l}(X-a_i)^{m_i}\prod_{j=1}^{m}(X-\alpha_j)^{\mu_j}(X-\bar{\alpha}_j)^{\mu_j} = a\prod_{i=1}^{l}(X-a_i)^{m_i}\prod_{j=1}^{m}(X^2-2\mathfrak{Re}(\alpha_j)X+|\alpha_j|^2)^{\mu_j}\ .$$

Remarquer que (puisque $\mathfrak{Im}(\alpha_i) > 0$) le discriminant du polynôme $X^2 - 2\mathfrak{Re}(\alpha_j)X + |\alpha_j|^2 \in \mathbb{R}[X]$ est bien strictement négatif. La proposition 4.9.27 montre en particulier qu'un polynôme $P(X) \in \mathbb{R}[X]$ de degré $d \geq 3$ ne peut pas être irréductible dans $\mathbb{R}[X]$, donc tout polynôme irréductible dans $\mathbb{R}[X]$ est de degré ≤ 2. Le corollaire 4.9.26 est une conséquence directe de cette remarque.