Cours d'Algèbre de L3, M303, Licence MFA, Orsay, année 2016-2017

Nicolas Ratazzi [1]

1. nicolas.ratazzi@math.u-psud.fr

Table des matières

Chapitre 1

Arithmétique sur $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et groupes abéliens

1.1 Rappels ensemblistes, relation d'équivalence

Notation 1.1.1 : Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. Notons que

$$X \subset E \iff X \in \mathcal{P}(E).$$

Exemple 1.1.2 $\emptyset \in \mathcal{P}(E)\,;\ \ E \in \mathcal{P}(E)\,;\ \ x \in E \Rightarrow \{x\} \in \mathcal{P}(E).$

Définition 1.1.3 Soit E un ensemble. Une collection $\{X_i\}_{i\in I}$ de sous-ensembles de E est une *partition de E* si

1. $\forall i \neq j,\ X_i \cap X_j = \emptyset$.

2. $\bigcup_{i\in I} X_i = E$

3. $\forall i \in I,\ \ X_i \neq \emptyset$.

Définition 1.1.4 Soit E un ensemble non vide. Une relation binaire $\mathcal{R}$ est une *relation d'équivalence (sur E)* si

1. (symétrie) $\forall x, y \in E,\ \ x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

2. (réflexivité) $\forall x \in E,\ \ x\mathcal{R}x$.

3. (transitivité) $\forall x, y, z \in E,\ \ (x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z)$.

Exemples 1.1.5

1. La relation d'égalité est une relation d'équivalence.

2. Sur l'ensemble $\mathbb{Z}$, si $n \in \mathbb{N}$, la relation de congruence modulo n, notée "$x = y \bmod n$", définie par $(\exists k \in \mathbb{Z},\ \ x = y + kn)$ est d'équivalence.

Définition 1.1.6 Soit E un ensemble non vide, soit $\mathcal{R}$ une relation d'équivalence sur E et soit $x \in E$. On appelle *classe d'équivalence de* x et on note $C(x)$ le sous-ensemble de E, définie par

$$C(x) := \{y \in E \mid x\mathcal{R}y\}\,.$$

Remarque 1.1.7 Pour tout $x \in E$, l'élément x appartient à la classe d'équivalence x.

Définition 1.1.8 Avec les notations précédentes, on note $E/\mathcal{R}$ l'ensemble des classes d'équivalence de E pour $\mathcal{R}$. C'est un sous-ensemble de $\mathcal{P}(E)$ (autrement dit un élément de $\mathcal{P}(\mathcal{P}(E))$). On appelle cet ensemble, *l'ensemble quotient (de E pour $\mathcal{R}$).*

Notons que par construction même de $E/\mathcal{R}$, il existe une application surjective, appelée *projection canonique* (ou surjection canonique) définie par :

$$\pi \;:\; E \to E/\mathcal{R}, \quad x \mapsto \pi(x) := C(x).$$

Proposition 1.1.9 *Soit E un ensemble non vide. Une relation d'équivalence $\mathcal{R}$ étant donné, l'ensemble des classes d'équivalence pour $\mathcal{R}$ forme une partition de E. Réciproquement si on se donne une partition $(X_i)_{i\in I}$ de E, alors les X_i forment les classes d'équivalence de E pour la relation $\mathcal{R}$ définie par*

$$x\mathcal{R}y \text{ si } (\exists i \in I,\ x \in X_i \text{ et } y \in X_i)\,.$$

Démonstration : Évident □

Exemples 1.1.10

1. Soit $n \in \mathbb{N}$. Sur $E = \mathbb{Z}$, avec $x\mathcal{R}y \iff x = y \bmod n$, on a

   $$C(x) = \{y \in \mathbb{Z} \mid y = x \bmod n\} = \{y \in \mathbb{Z} \mid y \in x + n\mathbb{Z}\} = x + n\mathbb{Z}.$$

   On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. On parle de l'ensemble des *nombres entiers congrus modulo n*.

2. Deux cas particuliers au point précédent :

   (a) Si $n = 0$, alors pour tout entier $x \in \mathbb{Z}$, on a $C(x) = \{x\}$ et $\mathbb{Z}/0\mathbb{Z} = \{\{x\} \mid x \in \mathbb{Z}\}$ est naturellement en bijection avec $\mathbb{Z}$.

   (b) Si $n = 1$, alors $C(0) = \mathbb{Z}$ et donc $\mathbb{Z}/1\mathbb{Z} = \{C(0)\}$ est réduit à un élément.

   Si $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est la projection canonique, l'image d'un élément x sera notée, suivant le contexte, $x \bmod n$, $C(x)$, $\pi(x)$, voire $\bar{x}$.

3. Sur $E = \mathbb{Z} \times \mathbb{Z}^*$, avec $\mathcal{R}$ donnée par $(a,b)\mathcal{R}(c,d) \iff ad = bc$, on a

   $$C((a,b)) = \{(c,d) \mid ad = bc\}.$$

   On note $\mathbb{Q}$ l'ensemble quotient. On l'appelle l'ensemble des *nombres rationnels* et on a une injection $i \;:\; \mathbb{Z} \hookrightarrow \mathbb{Q}$ donnée par $a \mapsto C((a,1))$. Partant d'un anneau intègre commutatif A (cf. plus loin), cette construction permet de construire son corps des fractions $\mathrm{Frac}(A)$. On peut vérifier que les lois d'additions et de multiplications sur $\mathbb{Z}$ (ou A) s'étendent à $\mathbb{Q}$ (ou $\mathrm{Frac}(A)$) de sorte que l'injection i est un morphisme d'anneaux (cf. plus loin).

4. Sur $E = \{\text{suites de Cauchy } (u_n) \text{ à valeurs dans } \mathbb{Q}\}$, on définit la relation $u\mathcal{R}v$ par $\lim u_n - v_n = 0$. C'est une relation d'équivalence. On a

$$C(u) = \{u + \varepsilon \mid \varepsilon \text{ suite de rationnels tels que } \lim \varepsilon_n = 0\}.$$

On note $\mathbb{R}$ l'ensemble quotient et on peut prouver qu'il s'agit bien de l'ensemble des réels vérifiant les propriétés que l'on lui connait. Là encore on a une injection de $\mathbb{Q}$ dans $\mathbb{R}$ fournie par $r \mapsto C((r_n))$ où (r_n) est la suite constante égale à r.

5. Soit $n \geq 1$. Sur $E = \mathbb{R}^n - \{0\}$ on pose $x\mathcal{R}y \iff \exists \lambda \in \mathbb{R}^*,\ x = \lambda y$. Cette fois on voit que

$$C(x) = \text{droite vectorielle de } \mathbb{R}^n, \text{ passant par } x, \text{ privée de } 0.$$

L'ensemble quotient est noté $\mathbb{P}^{n-1}(\mathbb{R})$ et s'appelle *l'espace projectif de dimension* $n-1$. Par exemple on a $\mathbb{P}^0(\mathbb{R}) = \{1\}$ et $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ (la direction infinie étant donnée par la droite verticale, axe des ordonnées).

6. Soit $n \geq 1$, sur $E = \mathcal{M}_n(\mathbb{R})$ on peut considérer la relation d'équivalence $A\mathcal{R}B \iff \exists P \in \mathrm{GL}_n(\mathbb{R}),\ A = P^{-1}BP$. Si $A\mathcal{R}B$ on dit que A *est semblable à* B.

1.2 Le quadruplet $(\mathbb{N}, +, \times, \leq)$

Définition 1.2.1 Soit E un ensemble non vide. Une relation binaire $\mathcal{R}$ est une *relation d'ordre (sur E)* si

1. (anti-symétrie) $\forall x, y \in E,\ \ x\mathcal{R}y$ et $y\mathcal{R}x \Rightarrow x = y$.
2. (réflexivité) $\forall x \in E,\ \ x\mathcal{R}x$.
3. (transitivité) $\forall x, y, z \in E,\ \ (x\mathcal{R}y$ et $y\mathcal{R}z \Rightarrow x\mathcal{R}z)$.

Exemple 1.2.2 la relation $\leq$ est une relation d'ordre sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mais la relation $<$ n'en n'est pas une (pourquoi ?).

Définition 1.2.3 Un *ensemble ordonné* est la donnée d'un couple $(E, \leq)$ constitué d'un ensemble non vide et d'une relation d'ordre. On dit que la relation $\leq$ est *totale* (et que E est *totalement ordonné*) si

$$\forall x, y \in E,\ \ x \leq y \text{ ou } \ y \leq x.$$

Exemple 1.2.4

1. La relation $\leq$ est une relation d'ordre totale sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
2. La relation de divisibilité $a|b$ sur $\mathbb{N}$, définie par $\exists k \in \mathbb{N},\ b = ka$ est une relation d'ordre qui n'est pas totale (par exemple 2 ne divise pas 5 et 5 ne divise pas 2).
3. Attention, la relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{Z}$ (car par exemple $-1|1$ et $1|-1$ mais $1 \neq -1$).

1.2.1 Une construction axiomatique de $\mathbb{N}$

Définition 1.2.5 Soit $(E, \leq)$ un ensemble ordonné et F un sous-ensemble non vide de E. On dit que m est un *plus petit élément de* F si

$$\forall x \in F,\ m \leq x \ \text{ et } \ m \in F.$$

On définit de même la notion de *plus grand élément*. De tels éléments sont nécessairement uniques (exercice).

Pour pouvoir faire de l'arithmétique il est nécessaire de présupposer existant un ensemble ordonné $(\mathbb{N}, \leq)$ vérifiant les 3 axiomes suivants :

1. Toute partie non vide admet un plus petit élément.

2. L'ensemble $\mathbb{N}$ n'est pas majoré.

3. Toute partie majorée non vide de $\mathbb{N}$ admet un plus grand élément.

Proposition 1.2.6 *L'ensemble* $\mathbb{N}$ *est totalement ordonné.*

Démonstration : Soient $x, y \in \mathbb{N}$. L'ensemble $\{x, y\}$ étant non vide, il admet un plus petit élément donc soit $x \leq y$ soit $y \leq x$. □

Notation 1.2.7 On note 0 le plus petit élément de $\mathbb{N}$. L'ensemble $\mathbb{N}$ n'étant pas majoré on voit en particulier que $\mathbb{N} - \{0\}$ est non vide, donc admet un plus petit élément : on note 1 cet élément. Plus généralement, pour tout entier $n \in \mathbb{N}$, l'ensemble

$$S_n := \{k \in \mathbb{N} \mid n \leq k \text{ et } k \neq n\}$$

est non vide (sinon $\mathbb{N}$ serait majoré par n) donc admet un plus petit élément, strictement plus grand que n : on le note $s(n)$ et on l'appelle le *successeur de* n.

1.2.2 Principe de Récurrence

Théorème 1.2.8 *Soit* $E \subset \mathbb{N}$ *tel que* $0 \in E$ *et tel que*

$$\forall n \in \mathbb{N},\ (n \in E \Rightarrow s(n) \in E)\,.$$

Alors $E = \mathbb{N}$.

Démonstration : Par l'absurde, supposons que $E \neq \mathbb{N}$ et posons F l'ensemble non vide $\mathbb{N} - E$. Cet ensemble F admet un plus petit élément : n_0. Posons

$$P_{n_0} := \{k \in \mathbb{N} \mid k \leq n_0 \text{ et } k \neq n_0\}.$$

Comme $0 \in E$, on a $n_0 \geq 1$, donc $0 \in P_{n_0}$ et de plus P_{n_0} est visiblement majoré par n_0, donc il admet un plus grand élément : notons le $p(n_0)$ (prédécesseur de n_0). Par construction $p(n_0) < n_0$ donc $p(n_0) \notin F$, donc $p(n_0) \in E$, donc $s(p(n_0)) \in E$. On vérifie que $s(p(n_0)) = n_0$ [En effet, par définition du successeur, $s(p(n_0))$ est strictement plus grand que $p(n_0)$ donc par définition de $p(n_0)$, on a $s(p(n_0)) \geq n_0$. De plus $n_0 > p(n_0)$ et $s(p(n_0))$ est le plus petit élément k tel que $k > p(n_0)$, donc $n \geq s(p(n_0))$.] et ceci permet de conclure par l'absurde. □

Remarque 1.2.9 On a prouvé en cours de route que $s \circ p = \mathrm{Id}_{\mathbb{N}^*}$. On vérifie de même que $p \circ s = \mathrm{Id}_{\mathbb{N}}$.

1.2.3 Addition, multiplication et unicité de $\mathbb{N}$

On définit l'addition + par récurrence par la formule :

$$\forall n \in \mathbb{N},\ n+0 := n \quad n+1 := s(n) \text{ et } \quad \forall m \in \mathbb{N}^*, n+m := (n+p(m))+1.$$

Nous pouvons réinterpréter le principe de récurrence sous la forme suivante : si $\mathcal{P}(n)$ est une propriété des entiers $n \in \mathbb{N}$ telle que $\mathcal{P}(0)$ est vraie et telle que $\forall n \in \mathbb{N}$, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, alors pour tout entier $n \in \mathbb{N}$ la propriété $\mathcal{P}(n)$ est vérifiée [il suffit de poser $E = \{n \in \mathbb{N} \mid \mathcal{P}(n)\}$ et d'appliquer le principe de récurrence prouver précédemment].

Théorème 1.2.10 *Il existe, à bijection croissante près, un unique ensemble ordonné vérifiant les axiomes 1,2 et 3 donnés pour* $\mathbb{N}$.

Démonstration : Notons $\mathbb{N}'$ un ensemble ordonné vérifiant les mêmes axiomes. On définit par récurrence l'application suivante

$$\varphi : \mathbb{N} \to \mathbb{N}', \text{ par la formule } \varphi(0) = 0' \text{ et } \forall n \in \mathbb{N},\ \varphi(n+1) = \varphi(n) +' 1',$$

øù $0', 1', +'$ désigne les analogues dans $\mathbb{N}'$ de $0, 1, +$ dans $\mathbb{N}$. Il est aisé de vérifier que φ est une bijection croisante. □

On définit la multiplication de la même façon que l'addition, par récurrence :

$$\forall n \in \mathbb{N},\ 0 \times n = 0, \text{ et } \forall m \in \mathbb{N},\ (m+1) \times n = m \times n + n.$$

Il est à partir de là possible de prouver par récurrence toutes les propriétés usuelles de + et $\times$ sur les entiers. Notamment la commutativité de + et de $\times$, la compatibilité de $\leq$ avec +, la propriété de *régularité pour* + : $x + n = y + n \Rightarrow x = y$, la même propriété pour la loi $\times$, l'associativité de + et de $\times$ et enfin la distributivité de $\times$ sur +. Nous laissons ceci en exercices au lecteur motivé.

1.2.4 Division euclidienne sur $\mathbb{N}$

Théorème 1.2.11 *Soit* $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. *Il existe un unique couple* $(q, r) \in \mathbb{N}^2$ *tel que*

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

Démonstration : Commençons par prouver l'existence. On effectue pour cela une récurrence sur a : si $a = 0$ ou plus généralement si $a < b$ alors le couple $(q, r) = (0, a)$ convient. Si la propriété est vraie au rang $a - 1 \geq 0$: soit b un élément quelconque de $\mathbb{N}^*$. Si $a < b$ il n'y a rien à prouver par ce qui précède. Sinon $a - b \geq 0$ et de plus $a - b \leq a - 1$ donc on peut appliquer l'hypothèse de récurrence à $a - b$. On obtient l'existence d'un couple (q, r) tel que :

$$a - b = bq + r \text{ et } 0 \leq r < b, \text{ donc } a = b(q+1) + r.$$

le couple $(q + 1, r)$ permet donc de conclure la récurrence.

Prouvons maintenant l'unicité. Supposons pour cela donné deux couples (q, r) et (q', r') tels que

$$bq + r = a = bq' + r' \text{ et } 0 \leq r, r' < b.$$

quitte à échanger les roles de (q, r) et de (q', r'), on peut supposer (et on le fait !) que $r' \geq r$. On a donc dans $\mathbb{N}$ l'égalité suivante :

$$b(q - q') = r' - r.$$

Si $r = r'$ ceci permet d'en déduire que $q = q'$. Sinon $r' > r$, donc l'égalité précédente donne visiblement $q > q'$ et la même égalité implique alors que $r' - r \geq b$ donc que $r' \geq b$ ce qui est impossible. Finalement par l'absurde ceci prouve que $r = r'$ et permet de conclure. □

Corollaire 1.2.12 ***(Écriture en base** g**)*** *Soit $g \geq 2$ un entier. On a :*

$$\forall a \in \mathbb{N}\ \exists r \in \mathbb{N}\ \exists a_0, \ldots, a_r \in \{0, \ldots, g-1\},\ \text{tels que } a = a_0 + \cdots + a_r g^r.$$

Démonstration : On effectue une récurrence sur a : si $a = 0$ c'est évident. Si la propriété est vraie jusqu'au rang $a - 1 \geq 0$, montrons la au rang a. On effectue la division euclidienne de a par g : $\exists (q, r)$ tels que $a = gq + r$ et $0 \leq r < g$. Si q était au moins égal à a, on aurait $gq \geq 2a$ donc $a = gq + r \geq 2a + r \geq 2a > a$ ce qui est impossible. Donc $q < a$ et on peut lui appliquer l'hypothèse de récurrence : $q = q_0 + \cdots + q_n g^n$ donc $a = r + q_0 g + \cdots + q_n g^{n+1}$. □

Remarque 1.2.13 Si les derniers a_i dans l'écriture en base g sont nuls, on peut les supprimer de l'écriture. De même on peut ajouter des a_i nuls à droite dans l'écriture. L'énoncé suivant indique qu'à part ces deux cas, il y a unicité de l'écriture en base g.

Proposition 1.2.14 *Soit $a \in \mathbb{N}$ et soit $g \geq 2$ un entier. S'il existe $a_0, \ldots, a_r, b_0, \ldots, b_s \in \{0, \ldots, g-1\}$ avec $s \geq r$, alors*

$$a_0 = b_0\ ;\ \ldots\ ;\ a_r = b_r \text{ et } b_{r+1} = \cdots = b_s = 0.$$

Démonstration : Exercice □

1.2.5 Nombres premiers

Définition 1.2.15 Un entier n est dit *composé* s'il est de la forme $n = ab$ avec $a, b \geq 2$ deux entiers. Un entier n est dit *premier* si $n \geq 2$ et si n n'est pas composé.

Remarque 1.2.16 On voit sur la définition qu'un entier composé vérifie toujours $n \geq 4$. De même on voit aisément sur la définition qu'un nombre premier pair est nécessairement égal à 2.

Théorème 1.2.17 ***(Existence et unicité de la décomposition en facteurs premiers)*** *Soit $n \geq 2$ un entier.*

1. *L'entier n peut s'écrire comme un produit $\prod_{i=1}^{r} p_i$ de facteurs premiers (les p_i pouvant se répéter).*
2. *S'il existe deux décompositions $\prod_{i=1}^{r} p_i = n = \prod_{i=1}^{s} q_i$ (avec p_i, q_i des nombres premiers et $r, s \geq 1$), alors $r = s$ et il existe une bijection σ de $\{1, \ldots, r\}$ sur lui même, telle que*

$$\forall i \leq r,\ q_i = p_{\sigma(i)}.$$

Démonstration : Le point 1 se prouve par récurrence sur n : si n est premier (notamment si $n = 2$) l'existence d'une décomposition en facteurs premiers est évidente. Si $n \geq 4$ est composé. Supposons la propriété vraie jusquàu rang $n-1$. Par définition d'être composé, $n = ab$ avec $a, b \geq 2$ donc également $a, b < n$. L'hypothèse de récurrence appliquée à a et à b permet de conclure.

Pour ce qui est de l'unicité : quitte à réindexer les divers facteurs premiers, on peut supposer qu'ils sont ordonnés de la façon suivante :

$$p_1 \leq \ldots \leq p_r \text{ et } q_1 \leq \ldots \leq q_s.$$

De plus quitte à échanger les rôles de (p_i) et (q_i), on peut supposer que $p_1 \leq q_1$. Nous allons maintenant montrer le point 2 par récurrence sur n.

Si $p_1 = q_1$ alors $m := p_2 \ldots p_r = q_2 \ldots q_s < n$ donc l'hypothèse de récurrence appppliquée à m entraîne que $r - 1 = s - 1$ et que les $(q_i)_{i\geq 2}$ sont obtenus par permutation des $(p_i)_{i\geq 2}$. La même chose est *a fortiori* vraie pour les $(q_i)_{i\geq 1}$ et les $(p_i)_{i\geq 1}$.

Si par l'absurde on a $p_1 < q_1$, alors posons $m := n - p_1 q_2 \ldots q_s$. Il y a deux façons d'écrire ce nombre :

$$m = p_1 \left(\prod_{i=2}^{r} p_i - \prod_{i=2}^{s} q_i \right) = (q_1 - p_1) \prod_{i=2}^{s} q_i.$$

Par construction $m < n$ et de plus $m > 1$ (sinon on voit sur l'écriture $1 = m = (q_1 - p_1) \prod_{i=2}^{s} q_i$ que ceci impliquerait que $s = 1$ et $1 = q_1 - p_1$ donc $q_1 = 1 + p_1$ ou p_1 serait pair mais la remarque précédant l'énoncé du théorème nous indique que dans ce cas p_1 ou q_1 vaudrait 2, donc $p_1 = 2$ et $q_1 = 3$ et $3 = q_1 = n = \prod p_i$ serait donc pair : impossible !). On peut décomposer en facteurs premiers les nombres $q_1 - p_1$ ainsi que $\prod_{i=2}^{s} p_i - \prod_{i=2}^{s} q_i$ et l'hypothèe de récurrence (concernant l'unicité de l'écriture) appliquée à m donne que p_1 est l'un des facteurs premiers de $q_1 - p_1$ (en effet, p_1 est strictement plus petit que tout les q_i et p_1 est l'un des facteurs premiers de $m = (q_1 - p_1) \prod_{i=2}^{s} q_i$). Finalement p_1 divise $q_1 - p_1$ donc $p_1 \geq 2$ divise q_1 et est strictement plus petit que ce dernier. Ceci contredit le fait que q_1 est premier et conclut la preuve. □

Remarque 1.2.18 Lorsque l'on disposera d'un peu plus d'outils, nous verrons ultérieurement dans le cours une preuve plus simple de ce résultat.

1.3 Entiers relatifs, groupes et anneaux

1.3.1 Groupes, définitions

Définition 1.3.1 Un *groupe* est la donnée d'un couple $(G, \cdot)$ où G est un ensemble non vide et où $\cdot$ est une application de $G \times G$ dans G, appelée *loi de composition interne* vérifiant :

1. (Associativité) $\forall x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. (Existence d'un élément neutre) $\exists e \in G$, $\forall z \in G$ on a $g \cdot e = e \cdot g$.
3. (Existence d'un inverse) $\forall x \in G$, $\exists y \in G$ tel que $x \cdot y = y \cdot x = e$.

Lemme 1.3.2 ***(Unicité du neutre et de l'inverse)*** *Si e et e' sont deux éléments neutres pour la loi $\cdot$ alors $e = e'$. De même si $x \in G$ et si y et y' sont deux inverses pour x alors $y = y'$.*

Démonstration : Pour la première assertion, on a $e \cdot e' = e$ par définition de l'élément neutre e'. De même par définition de l'élément neutre e, on a $e \cdot e' = e'$. Donc $e = e'$. Concernant la seconde assertion, on voit que $x \cdot y = e$. Multipliant cette égalité par y' on obtient $y' \cdot (x \cdot y) = y' \cdot e = y'$ et par associativité de la loi $\cdot$ on en déduit que $(y' \cdot x) \cdot y = y'$. Or $y' \cdot x = e$ donc $y = y'$. □

Remarque 1.3.3 Quelques commentaires sur la définition :

1. Le plus souvent, la notation $\cdot$ pour la loi de composition sera sous-entendue : on écrira xy au lieu de $x \cdot y$. On parlera dans ce cas de *notation multiplicative* (par opposition à la *notation additive* consistant à écrire $x + y$).
2. On fera le plus souvent l'abus de langage consistant à parler du groupe G plutôt que du groupe $(G, \cdot)$.
3. Le neutre pour la notation multiplicative est noté traditionnellement 1 (au lieu de e) et le neutre en notation additive se note traditionnellement 0.
4. L'inverse d'un élément x pour la notation multiplicative est noté traditionnellement x^{-1} et l'inverse en notation additive se note traditionnellement $-x$ et est appelé l'opposé.

Proposition 1.3.4 *Soit G un groupe et $x, y \in G$. On a $(xy)^{-1} = y^{-1}x^{-1}$.*

Démonstration : On calcule $z = (xy)y^{-1}x^{-1}$ et on voit en utilisant l'associativité que $z = 1$. De même on vérifie que $y^{-1}x^{-1}(xy) = 1$. □

Définition 1.3.5 Un groupe G est dit *commutatif* (ou *abélien*) si

$$\forall x, y \in G, \quad xy = yx.$$

Exemple 1.3.6

1. $(\mathbb{Z}, +)$ est un groupe (mais $(\mathbb{Z}, \cdot)$ ou $(\mathbb{Z}^*, \cdot)$ ou $(\mathbb{N}, +)$ n'en sont pas). Il est commutatif.
2. L'ensemble des matrices inversibles $\mathrm{GL}_n(\mathbb{R})$ est un groupe pour la multiplcation matricielle, de neutre I_n. Il n'est pas commutatif (exercice).
3. L'ensemble des matrices carrées de taille $n \times n$, noté $\mathcal{M}_n(\mathbb{R})$ est un groupe pour l'addition.
4. L'ensemble des bijections d'un ensemble X sur lui même est un groupe pour la composition. On le note $(S(X), \circ)$.

1.3.2 Anneaux

Définition 1.3.7 Un *anneau* est un triplet $(A, +, \times)$ tel que $(A, +)$ est un groupe commutatif et vérifiant de plus les propriétés suivantes :

1. La multiplication admet un neutre (que l'on note 1).
2. La loi $\times$ est associative.
3. (distributivité) $\forall a, b, c \in A$, $(a + b)c = ac + bc$ et $a(b + c) = ab + ac$.

Proposition 1.3.8 *Si A est un anneau et $a \in A$, on a $0 \cdot a = 0$. On dit que 0 est absorbant.*

Démonstration : On a $0 \cdot a = (0+0) \cdot a = (0 \cdot a) + (0 \cdot a)$. En additionnant l'opposé de $0 \cdot a$ dans cette égalité on obtient le résultat. □

Remarque 1.3.9 Étant donné un anneau $(A, +, \cdot)$ on munit naturellement A^n d'une structure d'anneau pour tout $n \geq 1$ en définissant l'addition et la multiplication dans A^n composante par composante.

Définition 1.3.10 Un anneau est *commutatif* si la loi $\times$ est commutative. Un anneau est dit *intègre* si

$$\forall x, y \in A, \quad xy = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Exemple 1.3.11

1. $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif intègre.
2. si $n \geq 2$, $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ est un anneau non commutatif, non intègre (exercice).
3. Si A est un anneau (intègre ou non), alors A^n n'est jamais intègre si $n \geq 2$ (exercice).

Définition 1.3.12 Soit A un anneau et $x \in A$. L'élément x est dit *inversible* s'il existe $y \in A$ tel que $xy = yx = 1$. On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 1.3.13 *L'ensemble $A^\times$ est un groupe pour la multiplication de A.*

Démonstration : L'élément neutre $1 \in A$ pour la loi $\cdot$ sur A est évidemment inversible donc $A^\times$ est non vide. De plus la loi $\cdot$ est associative sur A donc *a fortiori* sur $A^\times$ qui est un sous-ensemble de A. Si $x, y \in A^\times$ alors la proposition 1.3.4 nous assure que $xy \in A^\times$ d'inverse $y^{-1}x^{-1}$. Notamment la loi $\cdot$ est bien définie sur $A^\times \times A^\times$ à valeurs dans $A^\times$. Les autres propriétés sont immédiatement vérifiées. □

1.3.3 Corps

Définition 1.3.14 Un *corps* est un anneau commutatif A tel que $A^\times = A - \{0\}$.

Exemple 1.3.15 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, le corps des fractions rationnelles $K(X)$ d'un corps K sont des corps. Par contre $\mathbb{Z}$, $\mathcal{M}_n(\mathbb{R})$ avec $n \geq 2$, K^n si K est un corps et $n \geq 2$, ne sont pas des corps.

1.3.4 Division euclidienne sur $\mathbb{Z}$

Proposition 1.3.16 *Pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{Z}^\times$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$a = bq + r \quad \text{avec} \quad 0 \leq r < |b|.$$

Démonstration : Nous laissons l'unicité en exercice. Pour l'existence : si a et b sont tout deux positifs, le résultat est déjà connu. Si $b > 0$ et $a < 0$ alors $-a > 0$ et on peut appliquer le résultat au couple $(-a, b)$. Si $b < 0$ alors $-b > 0$ et on peut reprendre l'argument qui précède. □

1.3.5 Premières applications à la théorie des groupes

Soit G un groupe et $g \in G$. On définit la puissance g^n, pour $n \geq 0$ par réccurrence (sur n) en posant

$$g^0 := 1, \quad \text{et} \quad \forall n \geq 0,\ g^{n+1} = g^n \cdot g.$$

Proposition 1.3.17 *Soit $g \in G$. Pour tout entier $n, m \geq 0$ on a*

$$g^{n+m} = g^n g^m \text{ et } (g^n)^m = g^{nm}.$$

Démonstration : C'est une simple récurrence. □

Définition 1.3.18 Soient $(G, \cdot)$ et $(H, \star)$ deux groupes et soit $\varphi : G \to H$ une application. On dit que φ est un *morphisme* de groupes si

$$\forall x, y \in G \quad \varphi(x \cdot y) = \varphi(x) \star \varphi(y).$$

Exemple 1.3.19 Nous donnons trois exemples avec des lois diverses de morphismes de groupes :

1. Soit $a \in \mathbb{Z}$, $\varphi_a : \mathbb{Z} \to \mathbb{Z}$ donné $x \mapsto ax$.
2. L'application exponentielle de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \cdot)$.
3. L'application logarithme de $(\mathbb{R}_+^*, \cdot)$ vers $(\mathbb{R}, +)$.

Proposition 1.3.20 *Si $\varphi : G \to H$ est un morphisme de groupes, on a $\varphi(1_G) = 1_H$. Et si $x \in G$ on a $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Démonstration : On a $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \star \varphi(1_G)$. En multipliant cette égalité par l'inverse de $\varphi(1_G)$ on en déduit que $1_H = \varphi(1_G)$. concernant la seconde assertion, notons que l'on a $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$. En multipliant par l'inverse de $\varphi(x)$ on peut conclure. □

Proposition 1.3.21 *Soit G un groupe. Les morphismes de groupes $\varphi : \mathbb{Z} \to G$ sont exactement les $\varphi_g : n \mapsto g^n$ quand g décrit G.*

Démonstration : Tout d'abord on vérifie aisément que si $g \in G$, l'application φ_g est un morphisme de groupes : en effet soit $a, b \in \mathbb{Z}$ on a $\varphi_g(a+b) = g^{a+b} = g^a g^b = \varphi_g(a)\varphi_g(b)$. Soit maintenant φ un morphisme quelconque de $\mathbb{Z}$ dans G. Par la proposition précédente, on sait que $\varphi(0) = 1_G$ (le neutre de $\mathbb{Z}$ étant 0). De plus, si $n \in \mathbb{N}$ on a $\varphi(n+1) = \varphi(n)\varphi(1)$ et par récurrence on voit donc que $\varphi(n+1) = g^n g = g^{n+1}$ en posant $g := \varphi(1)$. Enfin, si $n < 0$ on a $-n > 0$et $\varphi(n) = \varphi(-n)^{-1} = (g^{-n})^{-1} = g^n$. Ceci prouve que $\varphi = \varphi_g$. □

Définition 1.3.22 Soit $(G, \cdot)$ un groupe et H un sous ensemble de G. On dit que H est un *sous-groupe* de G si H muni de la loi $\cdot$ est un groupe.

Proposition 1.3.23 *Soient $(G, \cdot)$ un groupe et $H \subset G$. On a*

$$H \text{ est un sous-groupe de } G \iff \forall x, y \in H, \quad xy^{-1} \in H \text{ et } H \neq \emptyset.$$

Démonstration : L'implication de gauche à droite découle facilement des définitions. Réciproquement

1. L'élément neutre 1 est dans H : en effet on sait que H est non vide, donc admet un élément h_0 ; de plus par hypothèse $1 = h_0 h_0^{-1}$ est également dans H.
2. pour tout $x \in H$, on a $x^{-1} = 1 \cdot x^{-1} \in H$.
3. Pour tout $x, y \in H$ on a y^{-1} dans H par ce qui précède et donc $x \cdot y = x \cdot (y^{-1})^{-1} \in H$.

La loi $\cdot$ étant associative sur G l'est *a fortiori* sur H. Ceci prouve que H est un sous-groupe de G. □

Définition 1.3.24 Soit $\varphi : G \to H$ un morphisme de groupes. On note

$$\mathrm{Im}(\varphi) := \{h \in H \mid \exists x \in G,\ \varphi(x) = h\} \ \textit{l'image de } \varphi,$$

et

$$\mathrm{Ker}(\varphi) := \{g \in G \mid \varphi(g) = 1\} \ \textit{le noyau de } \varphi.$$

Proposition 1.3.25 *Les sous-ensembles* $\mathrm{Im}(\varphi)$ *et* $\mathrm{Ker}(\varphi)$ *sont des sous-groupes de* G *et de* H *respectivement.*

Démonstration : Faisons la preuve pour l'image et laissons en exercice la preuve pour le noyau. Le groupe G n'étant pas vide, il contient l'élément neutre 1_G, donc l'image contient l'élément $1_H = \varphi(1_G)$. De plus si $x, y \in \mathrm{Im}(\varphi)$ alors $\exists a, b \in G$ tels que $\varphi(a) = x$ et $\varphi(b) = y$. Donc on a

$$xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \mathrm{Im}(\varphi).$$

Par la proposition précédente nous pouvons conclure. □

Proposition 1.3.26 *Si* $\varphi : G \to H$ *est un morphisme de groupes, on a*

$$\varphi \text{ injectif} \iff \mathrm{Ker}(\varphi) = \{1\}.$$

Démonstration : Supposons que φ est injectif et soit $g \in \mathrm{Ker}(\varphi)$. On a $\varphi(g) = 1 = \varphi(1)$. Par injectivité ceci implique que $g = 1$ donc que $\mathrm{Ker}(\varphi) \subset \{1\}$. L'élément 1 étant visiblement dans le noyau on conclut que $\mathrm{Ker}(\varphi) = \{1\}$. Réciproquement supposons que $\mathrm{Ker}(\varphi) = \{1\}$. Soient $x, y \in G$ tels que $\varphi(x) = \varphi(y)$. En multipliant à droite par l'inverse de $\varphi(y)$ on obtient :

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

Par hypothèse on en déduit que $xy^{-1} = 1$ donc que $x = y$ en multipliant à droite par y. □

Proposition 1.3.27 *Les sous-groupes de* $\mathbb{Z}$ *sont les* $n\mathbb{Z}$ *quand* n *décrit l'ensemble des entiers naturels.*

Démonstration : Notons tout d'abord que si $n \in \mathbb{N}$ alors l'ensemble $n\mathbb{Z}$ est visiblement un sous-groupe de $\mathbb{Z}$ (exercice). Réciproquement : soit $G \subset \mathbb{Z}$ un sous-groupe de $\mathbb{Z}$. Si $G = \{0\}$ alors G est de la forme $n\mathbb{Z}$ avec $n = 0$. Sinon, en prenant un élément non nul dans G et quitte à considérer son opposé,on voit qu'il existe un élément dans $G \cap \mathbb{N}^*$. Cette partie $G \cap \mathbb{N}^*$ est donc une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément : notons le g_0. Les multiples de g_0 sont donc tous dans G (pour tout entier n, l'élément $ng_0 = g_0 + \cdots + g_0 \in G$

car G est stable par addition) donc $g_0\mathbb{Z} \subset G$. Soit maintenant $g \in G$ un élément quelconque. La division euclidienne de g par g_0 nous donne : il existe $(q, r) \in \mathbb{Z}^2$ tels que $g = g_0 q + r$ et $0 \leq r < g_0$. Donc $r = g - qg_0$ est dans G comme différence de deux éléments du groupe G. Or $r \in G \cap \mathbb{N}$ est strictement plus petit que le plus petit élément de $G \cap \mathbb{N}^*$, donc $r = 0$. Ainsi $g = qg_0$ est dans $g_0\mathbb{Z}$ donc $G \subset g_0\mathbb{Z} \subset G$. Autrement dit $G = g_0\mathbb{Z}$, ce que l'on voulait prouver. □

Définition 1.3.28 Soit φ un morphisme de groupes. On dit que φ est un *isomorphisme* si φ est bijectif.

Proposition 1.3.29 *Un isomorphisme est tel que sa bijection réciproque est automatiquement un morphisme de groupes.*

Démonstration : Notons $\varphi : G \to H$ l'isomorphisme dont on part et posons $\psi : H \to G$ sa bijection réciproque. On veut montrer que ψ est un morphisme de groupes. Soit donc $a, b \in H$, on a

$$\psi(ab) = \psi(a)\psi(b) \iff \varphi\left(\psi(ab)\right) = \varphi\left(\psi(a)\psi(b)\right) \iff ab = \varphi\left(\psi(a)\psi(b)\right).$$

Par ailleurs φ est un morphisme de groupes donc

$$ab = \varphi\left(\psi(a)\psi(b)\right) \iff ab = \varphi(\psi(a))\varphi(\psi(b)) \iff ab = ab.$$

La dernière assertion dans la série d'équivalences étant vraie, la première l'est également, autrement dit, ψ est un morphisme de groupes. □

1.3.6 Ordre d'un élément dans un groupe

Soient G un groupe et $g \in G$. Notons $\varphi_g : \mathbb{Z} \to G$ le morphisme $n \mapsto g^n$. Le noyau de φ_g est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour un certain entier $d \geq 0$.

1. Si $d = 0$: les g^n sont deux à deux distincts lorsque n est variable. On dit que g est *d'ordre infini.*
2. Si $d > 0$: on dit que g est *d'ordre* d.

Proposition 1.3.30 *Si g est d'ordre $d > 0$, alors $\exists k \geq 1$ tel que $g^k = 1$ et d est le plus petit tel entier k. De plus : $g^n = 1 \iff d|n$ et $\mathrm{Im}(\varphi_g) = \{1, g, \ldots, g^{d-1}\}$.*

Démonstration : Par définition de l'ordre, le nombre $k := d$ assure l'existence d'un k comme voulu. Si $g^k = 1$ et si $k \geq 1$, alors $k \in d\mathbb{Z}$ donc en particulier $k \geq d$. Par ailleurs, $g^k = 1 \iff k \in \mathrm{Ker}\varphi_g \iff k \in d\mathbb{Z} \iff d|k$. □

Définition 1.3.31 Soit G un groupe et $g \in G$. On appelle *sous-groupe engendré par g* le groupe $\mathrm{Im}\varphi_g$. On le note $\langle g \rangle$.

1. Si $d = 0$, l'ordre de g est infini et le cardinal du groupe $\langle g \rangle$ est infini.
2. Si $d > 0$, l'ordre de g est d et le cardinal du groupe $\langle g \rangle$ est d.

Remarque 1.3.32 Si le cardinal de G est fini, alors tout les éléments de G sont d'ordre fini (en effet sinon φ_g aurait une image infini tout en étant inclus dans G, ce qui est impossible).

Théorème 1.3.33 ***(Lagrange)*** *Soit G un groupe fini et H un sous-groupe de G. Alors*

$$\mathrm{Card}(G) = \mathrm{Card}(G/H) \times \mathrm{Card}(H).$$

En particulier, le cardinal de H divise celui de G.

Pour prouver le théorème nous introduisons la relation déquivalence suivante, appelée *relation de congruence modulo H*, sur G en posant :

$$x \equiv y \bmod H \text{ si par définition } \exists h \in H \ x = yh.$$

Vérifions tout d'abord que cette relation est bien une relation d'équivalence :

1. réflexivité : on a $x = x \cdot 1$ et $1 \in H$ donc $x \equiv x \bmod H$.
2. symétrie : si $x = y \bmod H$, il existe $h \in H$ tel que $x = yh$, donc $y = xh^{-1}$. En posant $k = h^{-1}$ on voit qu'il existe $k \in H$ tel que $y = xk$, donc $y \equiv x \bmod H$.
3. transitivité : si $x \equiv y \bmod H$ et $y \equiv z \bmod H$, alors il existe $h_1, h_2 \in H$ tels que $x = yh_1$ et $y = zh_2$. Donc $x = yh_1 = (zh_2)h_1 = z(h_2h_1)$. Donc $x \equiv z \bmod H$.

Définition 1.3.34 les classes d'équivalences pour cette relation sont appelées les *classes à gauche* et l'ensemble quotient se note G/H. On a

$$\mathrm{Cl}(x) = \{y \in G \mid \exists h \in H \ y = xh\} = xH.$$

Remarque 1.3.35 Notons que l'on aurait pu également introduire une relation très similaire donnée par

$$x \equiv y \bmod H \text{ si par définition } \exists h \in H \ x = hy.$$

Il s'agit également d'une relation d'équivalence et les classes d'équivalences sont appelées les classes à droite et l'ensemble quotient se note $H\backslash G$. On a $\mathrm{Cl}(x) = Hx$. Sauf mention contraire, nous travaillerons toujours avec les classes à gauche plutôt qu'avec les classes à droite.

Notons que si le groupe G est fini, toutes les classes à gauche on le même cardinal : celui de H. En effet on a pour tout $x \in G$, une bijection de H vers $\mathrm{Cl}(x) = xH$ donnée par $h \mapsto xh$.

Preuve du théorème 1.3.33 : On considère la relation de congruence d'ensemble quotient G/H. Les classes déquivalences forment une partition de G, elles ont toutes le même cardinal ($\mathrm{Card}(H)$) et il y en a $\mathrm{Card}(G/H)$ (rappelons que par définition, l'ensemble quotient G/H est l'ensemble des classes d'équivalences). On obtient ainsi la formule suivante :

$$\mathrm{Card}(G) = \mathrm{Card}(G/H) \times \mathrm{Card}(H).$$

Ceci prouve le théorème. □

Corollaire 1.3.36 *Si $\mathrm{Card}(G) = n \in \mathbb{N}^*$, alors tout élément de G est d'ordre $d|n$.*

Démonstration : Soit $g \in G$. On sait que l'ordre d de g est fini car G est fini. Or $d = \mathrm{Card}(\langle g \rangle)$. Donc le théorème de Lagrange assure que d divise n. □

Corollaire 1.3.37 *Soit $\varphi : G \to F$ un morphisme de groupes avec G fini. Alors $\mathrm{Im}(\varphi)$ est un groupe fini et*

$$\mathrm{Card}(\mathrm{Im}(\varphi)) \times \mathrm{Card}(\mathrm{Ker}(\varphi)) = \mathrm{Card}(G).$$

Démonstration : Posons $H = \mathrm{Ker}(\varphi)$. c'est un sous-groupe de G donc le théorème de Lagrange nous assure que $\mathrm{Card}(G/H) \times \mathrm{Card}(\mathrm{Ker}(\varphi)) = \mathrm{Card}(G)$. Il reste pour conclure à prouver que $\mathrm{Im}(\varphi)$ est en bijection avec l'ensemble quotient $G/\mathrm{Ker}(\varphi)$. condiérons pour cela l'application suivante :

$$\bar{\varphi} : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi) \subset F,\ g\mathrm{Ker}(\varphi) \mapsto \varphi(g).$$

Notons tout d'abord que cette application est bien définie (autrement dit ce que l'on écrit à un sens et la valeur $\varphi(g)$ ne dépend par du choix d'un réprésentant de la classe déquivalence $g\mathrm{Ker}(\varphi)$). Soit donc $x, y \in G$ tels que $x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi)$. Nous voulons montrer que $\varphi(x) = \varphi(y)$. Or on a

$$\varphi(x) = \varphi(y) \iff \varphi(y^{-1})\varphi(x) = 1 \iff y^{-1}x \in \mathrm{Ker}\varphi \iff x \in y\mathrm{Ker}(\varphi) \iff x\mathrm{Ker}(\varphi) \subset y\mathrm{Ker}(\varphi).$$

Par symétrie des rôles de x et de y, ceci est également équivalent à $y\mathrm{Ker}(\varphi) \subset x\mathrm{Ker}(\varphi)$. Donc finalement nous voyons que $\varphi(x) = \varphi(y)$ si et seulement si $x\mathrm{Ker}(\varphi) = y\mathrm{Ker}(\varphi)$. Ceci prouve non seulement que l'application $\bar{\varphi}$ est bien définie mais également qu'elle est injective. La surjectivité est immédiate par défintion de l'ensemble image. □

1.4 Congruences

1.4.1 Définition et premiers résultats

Définition 1.4.1 Soit $n \geq 0$ un entier et soient $a, b \in \mathbb{Z}$. On dit que *a est congru à b modulo n*, et on note $a = b \bmod n$ si par définition n divise $a - b$.

Remarque 1.4.2 $a = b \bmod n \iff \exists k \in \mathbb{Z}\ a = b + kn \iff a \in b + n\mathbb{Z}$. Notons $\mathrm{Cl}(x)$ la classe d'équivalence d'un élément x pour cette relation de congruence modulo n. C'est un cas particulier de la relation de congruence modulo un sous groupe comme on le voit en posant $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ et en travaillant en notations additives. On note donc naturellement $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. On voudrait munir cet ensemble d'une structure d'anneau, qui soit de plus raisonnablement compatible avec celle provenant de $\mathbb{Z}$. C'est ce que nous allons nous attacher ` faire dans la suite de ce paragraphe.

Proposition 1.4.3 *Soient $a, b, x, y \in \mathbb{Z}$ tels que $a = x \bmod n$ et $b = y \bmod n$. Alors on a :*

$$a + b = x + y \bmod n \text{ et } ab = xy \bmod n.$$

Démonstration : Nous faisons la preuve pour l'addition eet laissons au lecteur le soin de faire la preuve pour la multiplication. Dire que $a+b = x+y \bmod n$ équivaut à dire $\exists \lambda \in \mathbb{Z},\ a+b = x + y + n\lambda$. Or par hypothèses, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $a = x + n\alpha$ et $b = y + n\beta$. Donc $a + b = x + y + n(\alpha + \beta)$. □

Corollaire 1.4.4 *Soit $r \geq 1$ et soient $\{a_i\}_{1\leq i\leq r}, \{x_i\}_{1\leq i\leq r} \in \mathbb{Z}^r$ tels que pour tout i, on a $a_i = x_i \bmod n$. Alors on a*

$$\sum_{i=1}^{r} x_i = \sum_{i=1}^{r} a_i \bmod n \text{ et } \prod_{i=1}^{r} a_i = \prod_{i=1}^{r} x_i \bmod n.$$

Démonstration : Immédiat à partir de la proposition, par récurrence sur le nombre r de termes. □

Corollaire 1.4.5 *Si $a = b \bmod n$ alors pour tout entier $k \in \mathbb{N}$ on a $a^k = b^k \bmod n$.*

Démonstration : Il suffit d'appliquer le corollaire précédent avec $r := k$, $a_i := a$ et $x_i := b$. □

Exemple 1.4.6 On a $10 = 1 \bmod 9$ donc $10^k = 1 \bmod 9$ pour tout entier $k \geq 0$. Si $x = a_r a_{r-1} \dots a_0$ est l'écriture de x en base 10 on voit donc que $x = a_0 + \cdots + a_r \bmod 9$. Ce résultat est ce que l'on appelle *la preuve par* 9.

1.4.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$, $n \geq 0$

Notation 1.4.7 Dans $\mathbb{Z}/n\mathbb{Z}$, la classe d'un élément $a \in \mathbb{Z}$ est notée $a \bmod n$ (ou $\bar{a}$ ou $\pi(a)$, l'appication $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ étant la surjection canonique).

Proposition 1.4.8 *Soient $a, b \in \mathbb{Z}$. On a*

$$a \bmod n = b \bmod n \iff a = b \bmod n.$$

Démonstration : Supposons tout d'abord que $a \bmod n = b \bmod n$. L'élément a appartient à la classe $a \bmod n$ donc à la classe $b \bmod n = \{b + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$. Notamment il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ ce qui équivaut à dire que $a = b \bmod n$. Réciproquement Si $a = b \bmod n$, il existe $k \in \mathbb{Z}$ tel que $a = b + kn$ donc $a \in b \bmod n$ et donc visiblement l'ensemble $a \bmod n$ est inclus dans $b \bmod n$. De même par symétrie des rôles de a et b, on a $b \bmod n \subset a \bmod n$, donc $a \bmod n = b \bmod n$. □

Remarque 1.4.9 En fait l'énoncé précédent vaut en fait pour toute relation d'équivalence $\mathcal{R}$ sur un ensemble E. Précisément on a dans ce cas :

$$x \mathcal{R} y \iff C(x) = C(y).$$

Par division euclidienne on voit que $\mathbb{Z}/n\mathbb{Z}$ est de cardinal n (pour $n \geq 1$) et que les classes $\bar{1}, \dots, \overline{n-1}$ sont deux à deux distinctes et forment donc l'ensemble $\mathbb{Z}/n\mathbb{Z}$. On munit cet ensemble d'une structure d'anneau commutatif en posant :

$$\forall a, b \in \mathbb{Z}, \quad (a \bmod n) + (b \bmod n) := (a + b) \bmod n \quad \text{et} \quad (a \bmod n) \cdot (b \bmod n) := ab \bmod n.$$

Ceci est bien défini par ce qui précède (cf la proposition 1.4.3). On vérifie que ces opérations définissent sur $\mathbb{Z}/n\mathbb{Z}$ un structure d'anneau commutatif, de neutre $0 \bmod n$ pour l'addition, de neutre $1 \bmod n$ pour la multiplication, tels que $-a \bmod n$ est l'opposé de $a \bmod n$. De plus, la projection canonique est un *morphisme d'anneaux*, *ie* vérifie les propriétés suivantes :

1. C'est un morphisme de groupes, *ie* $\forall x, y \in \mathbb{Z}$ on a $\pi(x + y) = \pi(x) + \pi(y)$.
2. Il est compatible à la multiplication : $\forall x, y \in \mathbb{Z}$ on a $\pi(xy) = \pi(x) \cdot \pi(y)$.
3. $\pi(1) = 1 \bmod n$.

Ceci est évident sur la définition des lois $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$.

Remarque 1.4.10 Notons que si un morphisme de groupes envoie automatiquement le neutre sur le neutre, la condition 3. précédente n'est pourtant pas impliquée par les deux précédentes. Par exemple l'application nulle vérifie trivialement les points 1 et 2 mais pas 3. Donnons deux exemples un peu moins naifs :

1. Considérons l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}^2$ donnée par $(x, y) \mapsto (x, 0)$. Elle vérifie les points 1. et 2. mais $\varphi(1, 1) = (1, 0) \neq (1, 1)$.
2. Considérons l'application $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ qui envoie 0 sur 0 et 1 sur $3 \bmod 6$. Elle est bien définie, stable par addition et multiplication mais $3 \bmod 6 \neq 1 \bmod 6$.

En fait si l'on considère un morphisme non nul $\varphi : A \to B$ entre deux anneaux, on a

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = \varphi(1)^2.$$

Donc l'élément $\varphi(1)$ est solution dans B de l'équation $X(X - 1) = 0$ et est non nul (sinon $\varphi(a) = \varphi(a \cdot 1) = \varphi(a) \cdot \varphi(1) = 0$ pour tout $a \in A$ et φ serait le morphisme nul). Notamment si l'anneau B est intègre on voit que dans ce cas $\varphi(1)$ doit bien être égal à 1.

Exemple 1.4.11 Déterminons les inversibles de $\mathbb{Z}/4\mathbb{Z}$. On a $(\mathbb{Z}/4\mathbb{Z})^\times = \{1 \bmod 4 \ ; \ 3 \bmod 4\}$ (nous mettrons ceci dans un contexte plus global un peu plus loin dans ce cours). Par ailleurs on a $(2 \bmod 4) \cdot (2 \bmod 4) = 4 \bmod 4 = 0 \bmod 4$. Or $2 \neq 0 \bmod 4$, donc l'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre. Plus généralement si $n = n_1 n_2 \geq 2$ est composé dans $\mathbb{Z}$ alors l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre comme on le voit en considérant le produit $(n_1 \bmod n) \cdot (n_2 \bmod n) = 0 \bmod n$.

Lemme 1.4.12 *Soit A un anneau commutatif intègre fini. Alors A est un corps.*

Démonstration : Il s'agit de prouver que tout élément $a \in A$ non nul est inversible. Soit a un tel élément. L'application $\varphi_a : A \to A$, $x \mapsto ax$ est injective (car A est intègre : $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x = y$). L'ensemble A étant de plus fini, elle est donc automatiquement surjective par cardinalité. Notamment il existe $b \in A$ tel que $\varphi_a(b) = 1$, donc $ab = 1$ et par commutativité ceci prouve que b est l'inverse de a. □

Théorème 1.4.13 *Soit $p \geq 2$ un entier on a*

$$p \text{ est premier } \iff \mathbb{Z}/p\mathbb{Z} \text{ est un corps } \iff \mathbb{Z}/p\mathbb{Z} \text{ est intègre.}$$

Démonstration : Si $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est en particulier un anneau intègre (si $ab = 0$ et $a \neq 0$ on multiplie par a^{-1} pour obtenir $b = 0$). Si $p \geq 2$ n'est par premier, il est composé donc par l'exemple précédent, on en déduit que $\mathbb{Z}/p\mathbb{Z}$ n'est pas intègre, ce qui prouve par la contraposée que si $\mathbb{Z}/p\mathbb{Z}$ est intègre alors p est premier. Il nous suffit donc de prouver que si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps pour conclure. En fait le lemme 1.4.12 précédent nous indique qu'il suffit de prouver que $\mathbb{Z}/p\mathbb{Z}$ est intègre pour conclure. Considérons donc $p \geq 2$ un nombre premier et $a, b \in \mathbb{Z}$ tels que $ab \bmod p = 0 \bmod p$. On a $ab = 0 \bmod p$ donc p divise ab. l'unicité de la décomposition en facteurs premiers implique que p est un facteur premier de a ou de b. On a donc $a = 0 \bmod p$ ou $b = 0 \bmod p$. □

1.4.3 Sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $n \geq 2$ un entier. On sait par le théorème de Lagrange que si H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ alors son cardinal divise n.

Définition 1.4.14 Soit G un groupe. On dit que G est *monogène* s'il existe $g \in G$ tel que $G = \{g^k \mid k \in \mathbb{Z}\}$. Si de plus G est fini, on dit qu'il est *cyclique*. Un élément g comme précédemment est appelé un *générateur* de G. On note $\langle g \rangle$ le groupe engendré par g.

Lemme 1.4.15 *Soit G un groupe cyclique et H un sous-groupe de G. Alors H est cyclique.*

Démonstration : Le sous-groupe H est inclus dans G donc est fini. Montrons qu'il est monogène. Notons n le cardinal de G et k le cardinal de H. On introduit par ailleurs un générateur g_0 de G. On a ainsi $G = \{1 = g_0^0, g_0, \ldots, g_0^{n-1}\}$. Considérons k le plus petit élément non nul tel que $g_0^k \in H$. On va montrer que H est le groupe engendré par $x = g_0^k$. Tout d'abord notons que x étant dans H, toutes les puissances de x sont dans H, donc le groupe $\langle x \rangle \subset H$. Réciproquement, soit $h \in H$. L'élément h est dans G donc il existe $d \geq 0$ tel que $h = g_0^d$. On peut effectuer la division euclidienne de d par k : il existe (q, r) tels que $d = kq + r$ et $0 \leq r < k$. On a $g_0^d = (g_0^k)^q \cdot g_0^r$ donc en divisant par x^q on obtient

$$g_0^r = g_0^d (x^q)^{-1} = h(x^q)^{-1} \in H.$$

Par définition du plus petit élément k, ceci implique que $r = 0$ donc que h est un multiple de x *ie* que $H \subset \langle x \rangle$. □

Exemple 1.4.16 Soit $n \geq 2$, l'élément $1 \bmod n$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$. Donc les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont tous cycliques.

Théorème 1.4.17 *Pour tout diviseur d de $n \geq 2$, il existe un et un seul sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$: l'ensemble $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$ des multiples de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration : Soit d un entier divisant n. Notons tout d'abord que l'ensemble $H := \{k\frac{n}{d} \mid k \in \{0, \ldots, d-1\}\}$ est visiblement un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d. Si E est un sous-groupe de cardinal d. Il est cyclique par le lemme précédent, engendré par un élément x_0 (d'ordre d). On a en particulier $dx_0 = 0 \bmod n$ donc il existe $k \in \mathbb{N}$ tel que $dx_0 = kn$. En divisant par k on constate que x_0 est dans H. Donc E est inclus dans H et par cardinalité on conclut que $E = H$, d'où l'unicité. □

1.5 Divisibilité dans $\mathbb{Z}$

1.5.1 Valuation p-adique et nombres premiers

Soit $n \in \mathbb{N}^*$. Nous noterons désormais toujours $\mathcal{P}$ l'ensemble des nombres premiers.

Proposition 1.5.1 *L'ensemble $\mathcal{P}$ est infini.*

Démonstration : Par l'absurde sinon on aurait $\mathcal{P} = \{p_1, \ldots, p_r\}$ pour un certain entier $r \geq 1$. Dans ce cas on pourrait considérer l'entier $N = 1 + \prod_{i=1}^{r} p_i$.C'est un entier plus grand que 2 donc on peut le décomposer en facteurs premiers. Soit p divisant N un tel facteur premier. Par définition $p \in \mathcal{P}$, donc on doit avoir $p|1$ ce qui est impossible. □

Définition 1.5.2 Soit $n \geq 2$ un entier. Décomposons n en facteurs premiers :

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

Par l'unicité de la décomposition en facteurs premiers le nombre $v_p(n)$ est bien défini et n étant fixé, la suite $(v_p(n))_{p \in \mathcal{P}}$ est nulle pour tout nombre premier sauf un nombre fini d'entre eux. On dit que $v_p(n)$ est la *valuation p-adique de n*. On pose $v_p(1) = 1$ pour tout $p \in \mathcal{P}$.

Lemme 1.5.3 *Soit $a, b \geq 1$ on a pour tout $p \in \mathcal{P}$, $v_p(ab) = v_p(a) + v_p(b)$.*

Démonstration : Cela résulte immédiatement de l'existence et de l'unicité de la décomposition en facteurs premiers pour a, b et ab. □

1.5.2 Pgcd

Lemme 1.5.4 *Soient $a, b \in \mathbb{Z}$. Alors $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.*

Démonstration : On a $a|b$ si et seulement si $\exists n \in \mathbb{Z}$ tel que $b = an$ ce qui implique que $\forall \lambda \in \mathbb{Z}$, $b\lambda = an\lambda$. Donc $b\mathbb{Z} \subset a\mathbb{Z}$. Réciproqument, si $b\mathbb{Z} \subset a\mathbb{Z}$, alors $b \times 1$ est dans $a\mathbb{Z}$ donc $\exists n \in \mathbb{Z}$ tel que $b = an$ autrement dit $a|b$. □

Corollaire 1.5.5 *Soient $a, b \in \mathbb{Z}$. On a ($a|b$ et $b|a$) si et seulement si $a\mathbb{Z} = b\mathbb{Z}$ ssi $a = \pm b$.*

Démonstration : Immédiat. □

Définition 1.5.6 Soit $n \in \mathbb{N}^*$ et soient $a_1, \ldots, a_n$ des entiers relatifs non tous nuls. On appelle $\text{pgcd}(a_1, \ldots, a_n)$ *le plus grand diviseur commun positif* des a_i. On le note aussi $a_1 \wedge \ldots \wedge a_n$.

Remarque 1.5.7 Pour tout $i \geq r$ l'entier 1 divise a_i. De plus les a_i étant non tous nuls, on peut supposer que $a_1 \neq 0$ quitte à renuméroter. On voit alors que l'ensemble $D := \{d \in \mathbb{N}^* \mid \forall i \leq r,\ d|a_i\}$ est inclus dans $\{d \in \mathbb{N}^* \mid d|a_1\}$ donc dans $\{1, \ldots, |a_1|\}$. En particulier l'ensemble D est une partie majorée non-vide de $\mathbb{N}$, donc admet un plus grand élément. Ceci justifie l'existence du pgcd.

Notation 1.5.8 Par convention nous poserons $\text{pgcd}(0, \ldots, 0) := 0$.

Proposition 1.5.9 *Soit $n \in \mathbb{N}^*$ et soient $a_1, \ldots, a_n$ des entiers relatifs. On a*

$$\text{pgcd}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_1, \ldots, v_p(a_n)\}}.$$

Démonstration : Notons $\delta := \text{pgcd}(a_1, \ldots, a_n)$. On a

$$\forall i,\ \delta|a_i \Rightarrow \forall i,\ \forall p \in \mathcal{P},\ v_p(\delta) \leq v_p(a_i) \Rightarrow \forall p \in \mathcal{P},\ v_p(\delta) \leq \min\{v_p(a_i) \mid 1 \leq i \leq n\}.$$

De plus on voit que $p^\alpha | p^\beta \iff \alpha \leq \beta$ donc l'inégalité précédente entraîne :

$$\delta | \prod_{p \in \mathcal{P}} p^{\min\{v_p(a_1), \ldots, v_p(a_n)\}} =: d.$$

Réciproquement pour tout i, on a $\min\{v_p(a_1), \ldots, v_p(a_n)\} \leq v_p(a_i)$ ce qui implique que $d|a_i$ pour tout i. De plus $d \geq 0$, donc $d \leq \delta$ et $\delta|d$ ce qui conclut. □.

Proposition 1.5.10 *Soit $r \in \mathbb{N}^*$ et soient $n, a_1, \ldots, a_r$ des entiers relatifs. On a*

1. $\text{pgcd}(na_1, \ldots, na_r) = |n|\text{pgcd}(a_1, \ldots, a_r)$.
2. *si $\delta := \text{pgcd}(a_1, \ldots, a_r) \neq 0$, alors pour tout i on a, $\frac{a_i}{\delta} \in \mathbb{Z}$ et $\text{pgcd}(\frac{a_i}{\delta} \mid 1 \leq i \leq r) = 1$.*

Démonstration : Donnons une preuve de la première assertion. Quitte à supprimer tous les indices i tels que $a_i = 0$, on peut supposer (et on le fait) que les a_i sont tous non nuls. Si $n = 0$ le résultat est évident. On peut donc supposer $n \neq 0$ et, quitte à remplacer n par son opposé, on peut même supposer que $n \geq 1$. On a par la proposition précédente :

$$\text{pgcd}(na_1, \ldots, na_r) = \prod_{p \in \mathcal{P}} p^{\min\{v_p(na_1, \ldots, v_p(na_r)\}}.$$

Par le lemme 1.5.3 on obtient donc

$$\begin{aligned}\mathrm{pgcd}(na_1,\dots,na_r) &= \prod_{p\in\mathcal{P}} p^{\min(v_p(n)+v_p(a_i)\ |\ 1\le i\le r)}\\ &= \prod_{p\in\mathcal{P}} p^{v_p(n)} \prod_{p\in\mathcal{P}} p^{\min(v_p(a_i)\ |\ 1\le i\le r)}\\ &= |n|\mathrm{pgcd}(a_1,\dots,a_r).\end{aligned}$$

Nous laissons le second point en exercice. □

1.5.3 Algorithme d'Euclide

Étant donnés deux entiers relatifs $a, b \in \mathbb{Z}$ on donne ici un algorithme permettant de calculer leur pgcd $a \wedge b$.

On a $a \wedge b = |a| \wedge |b|$, donc on peut dans la suite supposer que a et b sont positifs.

On a $a \wedge b = b \wedge a$, donc on peut supposer que $a \geq b \geq 0$.

Si $b = 0$ alors par définition $a \wedge b = a$.

Sinon : on pose $(A_0, U_0, V_0) := (a, 1, 0)$ de sorte que $A_0 = aU_0 + bV_0$ et $(A_1, U_1, V_1) = (b, 0, 1)$ de sorte que $A_1 = aU_1 + bV_1$.

Supposons écrit (A_n, U_n, V_n) de sorte que $A_n = aU_n + bV_n$. Alors deux possibilités : si $A_n = 0$ alors $a \wedge b = A_{n-1} = aU_{n-1} + bV_{n-1}$; sinon on effectue la division euclidienne de A_{n-1} par A_n pour obtenir :

$$A_{n-1} = A_n Q_n + A_{n+1} \text{ avec } 0 \leq A_{n+1} < A_n.$$

Posons $U_{n+1} = U_{n-1} - U_n Q_n$ et $V_{n+1} = V_{n-1} - V_n Q_n$. On a alors

$$A_{n+1} = aU_{n+1} + bV_{n+1}.$$

Il reste pour conclure à vérifier deux choses :

1. Tout d'abord que l'algorithme ci-dessus termine au bout d'un nombre fini d'étapes. Or la suite A_i est une suite d'entiers positifs qui est visiblement strictement décroissante.
2. Ensuite que si $A_n = 0$ on a bien $a \wedge b = A_{n-1}$. Montrons pour se faire par récurrence sur n que $d(:= a \wedge b) = A_n \wedge A_{n-1}$ si n est tel que $A_n \neq 0$.
   (a) Si $n = 0$ on a $A_0 = a$ et $A_1 = b$ d'où le résultat.
   (b) Si la propriété est vraie au rang $n-1$ et si n est tel que $A_n \neq 0$. On a dans ce cas $A_{n+1} = A_{n-1} - A_n Q_n$ donc les diviseurs de A_n et de A_{n-1} sont les mêmes que ceux de A_n et A_{n+1}. Donc le pgcd d de a et b est le même par hypothèse de récurrence que celui de A_n et de A_{n-1} donc que celui de A_n et A_{n+1}.

Remarque 1.5.11 Cet algorithme permet d'une part de calculer le pgcd de a et b, mais il donne par ailleurs une relation (dite *de Bézout*) : $d = au + bv$.

Proposition 1.5.12 ***(Bézout)*** *Soient $a, b \in \mathbb{Z}$. On a*

$$d = \mathrm{pgcd}(a, b) \Rightarrow \exists u, v \in \mathbb{Z} \quad d = au + bv.$$

Démonstration : C'est l'algorithme ci-dessus. □

Définition 1.5.13 Deux éléments $a, b \in \mathbb{Z}$ sont dits *premiers entre eux* si $a \wedge b = 1$.

Théorème 1.5.14 ***(Bézout)*** *On a*

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z} \quad au + bv = 1.$$

Démonstration : Le sens $\Rightarrow$ est donné par l'implication précédente. Réciproquement, si $d = a \wedge b$ alors d divise a et b donc d divise $au + bv = 1$. Or d est positif, donc $d = 1$. □

1.5.4 Applications

Résolution de $ax + by = c$, $a, b, c \in \mathbb{Z}$ en les inconnues $x, y \in \mathbb{Z}$

Lemme 1.5.15 ***(Gauss)*** *Soit $a, b \in \mathbb{Z}$ tels que $a \wedge b = 1$ et tels que a divise bc. Alors a divise c.*

Démonstration : Les nombres a et b étant premiers entre eux, on a une relation de Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. De plus il existe $k \in \mathbb{Z}$ tel que $ak = bc$ donc on obtient :

$$c = (au + bv)c = auc + bvc = auc + akv = a(uc + kv).$$

Autrement dit, a divise c. □

Nous pouvons utiliser ce lemme pour résoudre les équations diophantiennes du type donné dans le titre de ce paragraphe :

Théorème 1.5.16 *Soient $a, b, c \in \mathbb{Z}$. Si $a \wedge b$ ne divise pas c, l'équation $ax + by = c$ n'a pas de solution dans $\mathbb{Z}^2$. Sinon l'ensemble des solutions de cette équation est l'ensemble*

$$\left\{(x, y) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}, \quad x = c'u_0 - b'k, \ y = c'v_0 + a'k\right\},$$

où a', b' et c' sont définis par $a = (a \wedge b)a'$, $b = (a \wedge b)b'$, $c = (a \wedge b)c'$, et où u_0, v_0 sont tels que $au_0 + bv_0 = a \wedge b$.

Démonstration : Si le $\mathrm{pgcd}(a, b)$ ne divise pas c, il n'y a visiblement pas de solution (évident par l'absurde). Sinon

$$\exists u_0, v_0 \text{ tels que } au_0 + bv_0 = d \ \text{ et } \ \exists a', b', c' \text{ tels que } c'd = c,\ a'd = d,\ b'd = b \ \text{ et } \ \mathrm{pgcd}(a', b') = 1.$$

Notons (x, y) un couple solution. On a donc $ac'u_0 + bc'v_0 = ax + by$, donc $a(c'u_0 - x) = b(y - c'v_0)$ soit encore

$$a'(c'u_0 - x) = b'(y - c'v_0).$$

En appliquant le lemme de Gauss à cette dernière identité on voit que a' divise $y - c'v_0$, donc il existe $k \in \mathbb{Z}$ tel que $y = c'v_0 + a'k$. En remplaçant dans l'équation on en tire $x = c'u_0 - b'k$. Réciproquement on vérifie que tout les couples de cette forme sont solution de l'équation. □

Inversibles et générateurs dans $\mathbb{Z}/n\mathbb{Z}$

Proposition 1.5.17 *Soient $n \geq 2$ et $x \in \mathbb{Z}$. On a équivalence entre les trois propriétés suivantes :*

1. *Le groupe engendré par $x \bmod n$ est $(\mathbb{Z}/n\mathbb{Z}, +)$.*
2. *$x \bmod n$ est inversible (pour la multiplication).*
3. $\mathrm{pgcd}(x, n) = 1$.

Démonstration : Prouvons tout d'abord que (2) équivaut à (3) :

$$\begin{aligned} \bar{x} \text{ est inversible} &\iff \exists y \in \mathbb{Z},\ \bar{x} \cdot \bar{y} = \bar{1} \\ &\iff \exists y \in \mathbb{Z},\ n | xy - 1 \\ &\iff \exists y \in \mathbb{Z},\ \exists a \in \mathbb{Z},\ an = xy - 1 \\ &\iff \exists y \in \mathbb{Z},\ \exists a \in \mathbb{Z},\ xy - an = 1 \\ &\iff \mathrm{pgcd}(x, n) = 1. \end{aligned}$$

Soit maintenant $x \in \mathbb{Z}$ tel que $x \bmod n$ est inversible. Soit $y \in \mathbb{Z}$ tel que $y \bmod n$ est l'inverse de $x \bmod n$. On a pour tout entier $k \in \mathbb{Z}$

$$\begin{aligned} k \bmod n &= k \times (1 \bmod n) \\ &= k \times (yx \bmod n) \\ &= ky \times (x \bmod n). \end{aligned}$$

On voit sur cette dernière écriture que cet élément apartient au groupe engendré par $x \bmod n$, autrement dit que $\mathbb{Z}/n\mathbb{Z} = \langle x \bmod n \rangle$. Réciproquement si $\mathbb{Z}/n\mathbb{Z} = \langle x \bmod n \rangle$, alors il existe un entier k tel que $k \times (x \bmod n) = 1 \bmod n$. Donc $kx \bmod n = 1 \bmod n$ autrement dit $k \bmod n$ est l'inverse de $x \bmod n$. □

Définition 1.5.18 Étant donnés deux éléments $a, b \in \mathbb{Z}$, on définit le $\mathrm{ppcm}(a, b)$ comme étant le plus petit entier positif, multiple commun de a et b. On définit de même le ppcm d'une famille finie d'éléments.

Proposition 1.5.19 *On a* $\mathrm{ppcm}(a_1, \ldots, a_r) = \prod_{p \in \mathcal{P}} p^{\sup\{v_p(a_1), \ldots, v_p(a_r)\}}$.

Démonstration : Même preuve que pour le pgcd. □

Remarque 1.5.20 Si $n \in \mathbb{Z}$ et $a, b \in \mathbb{Z}$ on a $\mathrm{ppcm}(na, nb) = |n| \mathrm{ppcm}(a, b)$.

Proposition 1.5.21 *Si $n \in \mathbb{Z}$ et $a, b \in \mathbb{Z}$ on a* $\mathrm{pgcd}(a, b) \times \mathrm{ppcm}(a, b) = |ab|$.

Démonstration : On peut par exemple le prouver en utilisant les interprétations des pgcd et ppcm en terme de valuations. □

1.5.5 Lemme Chinois

Lemme 1.5.22 *Si A, B sont deux anneaux, alors $A \times B$ est un anneau (pour les lois définies coordonnées par coordonnées) et $(A \times B)^\times = A^\times \times B^\times$.*

Démonstration : Évident. □

Lemme 1.5.23 *Soit $d, n \in \mathbb{N} - \{0\}$ tels que d divise n. Alors la fonction $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ définie par $\varphi(x \bmod n) := x \bmod d$ est bien définie et est un morphisme d'anneaux.*

Démonstration : Le seul point non trivial est de vérifier que l'application φ est bien définie. Soient donc $x, y \in \mathbb{Z}$ tels que $x \bmod n = y \bmod n$. Il existe $k \in \mathbb{Z}$ tel que $x = y + kn$. Or d divise n donc il existe $\lambda \in \mathbb{Z}$ tel que $n = \lambda d$, donc en particulier $x = y + (k\lambda)d$ donc $x = y \bmod d$, autrement dit, φ ne dépend pas du choix d'un représentant modulo n donc est bien définie.□

Théorème 1.5.24 ***(Restes Chinois)*** *Soient $a, b \in \mathbb{N} - \{0, 1\}$. L'application $\varphi : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ définie par $\varphi(x \bmod ab) = (x \bmod a, x \bmod b)$ est un morphisme d'anneaux. De plus, si a et b sont premiers entre eux alors φ est un isomorphisme de bijection réciproque :*

$$\psi(x \bmod a, y \bmod b) = bvx + auy \bmod ab \quad \text{où} \quad au + bv = 1 \ \text{ est une relation de Bézout.}$$

Si a et b ne sont pas premiers entre eux, alors les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ne sont pas isomorphes.

Démonstration : Par le lemme 1.5.23 l'application φ est bien définie et est clairement un morphisme d'anneaux. En terme de cardinalité, on a $ab = \mathrm{Card}(\mathbb{Z}/ab\mathbb{Z}) = \mathrm{Card}(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{Card}(\mathbb{Z}/b\mathbb{Z})$ et la relation $|\mathrm{Ker}(\varphi)| \times |\mathrm{Im}(\varphi)| = ab$ implique donc que φ et un isomorphisme si et seulement si φ est injective. Or ceci se vérifie aisément : si $x = 0 \bmod a$ et $x = 0 \bmod b$ alors a et b divisent x et étant premiers entre eux, on en déduit que ab divise x autrement dit que $x = 0 \bmod ab$. On pourrait également vérifier à la main que $\varphi \circ \psi = \mathrm{Id}$ et que $\psi \circ \varphi = \mathrm{Id}$. Concernant le dernier point notons $d = \mathrm{pgcd}(a, b) \geq 2$ et supposons par l'absurde qu'il existe un morphisme d'anneaux f de $\mathbb{Z}/ab\mathbb{Z}$ vers le produit $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Alors il existe a_1, b_1 tels que $a_1 d = a$ et $b_1 d = b$ et $\mathrm{pgcd}(a_1, b_1) = 1$. De plus $f(1) = (1, 1)$ et

$$f(a_1 b_1 d \bmod ab) = (a_1 d b_1 \bmod a, a_1 b_1 d \bmod b) = (ab_1 \bmod a, a_1 b \bmod b) = (0, 0).$$

Or $1 \leq a_1 b_1 d < ab$ car $d \geq 2$ donc $a_1 b_1 d \neq 0 \bmod ab$ ce qui donne une contradiction avec l'injectivité de f. □

Remarque 1.5.25 En modifiant légèrement l'argument donné pour la preuve du second point du théorème précédent, on pourrait même montrer que : "Si a et b ne sont pas premiers entre eux, alors les groupes $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ne sont pas isomorphes." Nous laissons ceci en exercice.

Corollaire 1.5.26 *Soient a, b deux entiers premiers entre eux. Alors l'isomorphisme φ précédent induit un isomorphisme de groupes entre les inversibles*

$$\varphi : (\mathbb{Z}/ab\mathbb{Z})^\times \to (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times .$$

1.5.6 Fonction indicatrice d'Euler

Théorème 1.5.27 ***(Petit théorème de Fermat)*** *Soit p un premier et soit $a \in \mathbb{Z}$. On a $a^p = a \bmod p$. De plus, si $\mathrm{pgcd}(a,p) = 1$ alors $a^{p-1} = 1 \bmod p$.*

Démonstration : Soit $a \in \mathbb{Z}$. Si $\mathrm{pgcd}(a,p) \neq 1$ alors $p|a$ donc $a \bmod p = a^p \bmod p = 0 \bmod p$. Sinon $a \bmod p \neq 0$ donc $\bar{a}$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$ donc son ordre divise $p-1$ donc $a^{p-1} = 1 \bmod p$. □

Exemple 1.5.28 Calculons le reste de la division euclidienne de 666^{999} par 13 : $666 = 55 \times 13 + 3 = 3 \bmod 13$ donc $666^{999} = 3^{999} \bmod 13$. Or le petit théorème de Fermat nous dit que $3^{12} = 1 \bmod 13$ car 13 est premier. On effectue donc la division euclidienne de 999 par 12 : $999 = 83 \times 12 + 3$ pour en déduire que $666^{999} = 3^{999} = 3^3 = 1 \bmod 13$. □

Définition 1.5.29 On appelle *fonction indicatrice d'Euler* la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ donnée par $n \mapsto \mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^\times$.

Remarque 1.5.30 On a

$$\varphi(n) = \mathrm{Card}\{x \bmod n \mid x \text{ engendre } \mathbb{Z}/n\mathbb{Z}\} = \{x \in \mathbb{Z} \mid 1 \leq x \leq n \text{ et } \mathrm{pgcd}(x,n) = 1\}.$$

La formule suivante nous permet de calculer la valeur de $\varphi(n)$:

$$\text{Si } n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \text{ alors } \varphi(n) = \prod_{p \in \mathcal{P}} p^{v_p(n)-1}(p-1).$$

Démonstration : Ceci se prouve par récurrence sur le nombre de facteurs permiers intervenant dans la décomposition en facteurs premiers de l'entier n.

1. Si $n = p^d$ alors

$$\begin{aligned} \varphi(n) &= \mathrm{Card}\{x \in \{1, \ldots, p^d\} \mid \mathrm{pgcd}(x, p^d) = 1\} \\ &= p^d - \mathrm{Card}\{p, 2p, \ldots, p^{d-1}p\} = p^d - p^{d-1} \\ &= p^{d-1}(p-1). \end{aligned}$$

2. Si $n = \prod_{i=1}^{d+1} p_i^{a_i}$. On a $n = \alpha\beta$ avec $\mathrm{pgcd}(\alpha, \beta) = 1$ et $\alpha := \prod_{i=1}^{d} p_i^{a_i}$ et $\beta := p_{d+1}^{a_{d+1}}$. Le corollaire 1.5.26 précédent nous donne l'égalité de cardinaux

$$\mathrm{Card}\left(\mathbb{Z}/ab\mathbb{Z}\right)^\times = \mathrm{Card}\left(\mathbb{Z}/a\mathbb{Z}\right)^\times \times \mathrm{Card}\left(\mathbb{Z}/b\mathbb{Z}\right)^\times.$$

Donc $\varphi(n) = \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. L'hypothèse de récurrence et l'initialisation de la récurrence nous permettent alors de conclure. □

Lemme 1.5.31 ***(Euclide)*** *Soient $a, b \in \mathbb{Z}$ et soit p premier.*

$$p|ab \Rightarrow p|a \quad \text{ou} \quad p|b.$$

Démonstration : On peut donner trois preuves de ce résultat :

1. Un calcul de valuation p-adique.
2. On sait que $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $ab = 0 \bmod p$ implique que a ou b est nul modulo p.

3. Si p ne divise pas a alors, comme $p|ab$ et que $\text{pgcd}(p,a) = 1$ le lemme de Gauss implique que $p|b$. □

Remarque 1.5.32 On déduit immédiatement de ce résultat l'unicité de la décomposition en facteurs premiers d'un entier.

Application : le système de cryptographie RSA.

Corollaire 1.5.33 *Soit $n \geq 2$. Il y a exactement $\varphi(d)$ éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$ pour tout les diviseurs d de n.*

Démonstration : Soit d un diviseur de n et soit $x \in \mathbb{Z}/n\mathbb{Z}$ d'ordre d. On sait que le groupe H engendré par x est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d (par le théorème 1.4.17). Il est cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Dans $\mathbb{Z}/d\mathbb{Z}$ il y a exactement $\varphi(d)$ éléments d'ordre d et l'ordre est conservé par isomorphisme. Ceci conclut. □

1.6 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 1.6.1 *Soit p premier. Alors*

1. *Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*
2. *(Admis) Le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ est cyclique si p est premier impair et $r \geq 1$.*

Démonstration : Nous allons utiliser le résultat suivant (qui se prouve par récurrence et en utilisant de la division euclidienne) : si k est un corps et $P \in k[X]$ un polynôme de degré $d \geq 1$ alors P admet au plus d racines. Notamment le polynôme $X^d - 1$ admet au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$ si $d \geq 1$.

Posons G le groupe des inversibles de $\mathbb{Z}p\mathbb{Z}$, de cardinal $p-1$ et pour tout entier $d|p-1$, notons $G_d = \{x \in G \mid x \text{ est d'ordre } d\}$. On a : G est la réunion disjointe des G_d donc

$$p - 1 = |G| = \sum_{d|p-1} |G_d|.$$

Nous voulons prouver que $|G_{p-1}| \geq 1$. Fixons un entier d divisant $p-1$. Soit G_d est vide, soit il existe $x_0 \in G_d$. Dans ce second cas, le groupe H_d engendré par x_0 ; étant isomorphe à $\mathbb{Z}/d\mathbb{Z}$, possède exactement $\varphi(d)$ éléments d'ordre d. Donc

$$|G_d| = 0 \quad \text{ou} \quad |G_d| \geq \varphi(d).$$

Par ailleurs, $\mathbb{Z}/(p-1)\mathbb{Z}$ est la réunion disjointe des $A_d := \{x \in \mathbb{Z}/(p-1)\mathbb{Z} \mid x \text{ est d'ordre d}\}$. Par le corollaire 1.5.33 on sait que A_d est de cardinal exactement $\varphi(d)$, d'où la formule :

$$p - 1 = \sum_{d|p-1} \varphi(d). \tag{1.1}$$

Enfin on sait que $|H_d| = d$ et donc que pour tout $y \in H_d$, on a $y^d = 1$. Si $z \in G_d$ est d'ordre d alors $z^d = 1$. Or les racines du polynôme $X^d - 1$ sont toutes dans H_d, donc $z \in H_d$. Donc $|G_d| \leq \varphi(d)$ et par ce qui précède on en déduit que

$$|G_d| = 0 \quad \text{ou} \quad |G_d| = \varphi(d).$$

Autrement dit, $G_d = \varepsilon(d)\varphi(d)$ où $\varepsilon(d) \in \{0, 1\}$. Finalement on tire de ceci que

$$\sum_{d|p-1} \varphi(d) = p - 1 = |G| = \sum_{d|p-1} |G_d| = \sum_{d|p-1} \varepsilon(d)\varphi(d).$$

On en conclut que pour tout d (et notamment pour $d = p - 1$) on a $\varepsilon(d) = 1$. □

Remarque 1.6.2 Attention le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ n'est pas cyclique : il est composé de 4 éléments, tous d'ordre divisant 2, donc ne peut être isomorphe à $\mathbb{Z}/4\mathbb{Z}$ (il est en fait isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$).

Théorème 1.6.3 *Soit $n \geq 1$ un entier. On a*

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times .$$

Démonstration : Cf. TD. □

Corollaire 1.6.4 *Le groupe des automorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ est abélien de cardinal $\varphi(n)$.*

Démonstration : Immédiat. □

1.7 Quotients de groupes abéliens, d'anneaux et d'espaces vectoriels

1.7.1 Quotient de groupes abéliens

Dans ce paragraphe on se donne un groupe abélien A (fini ou non) et un sous-groupe B de A. On reprend la notion de *classe de congruences* introduite dans le preuve du théorème de Lagrange et on dit que x *est congru à* y *modulo* B si par définition $x - y \in B$, ce que l'on écrit :

$$\forall x, y \in A, \quad x = y \bmod B \iff x - y \in B.$$

Notons que travaillant avec des groupes commutatifs, les notions de classes à droite et de classes à gauche coincident. Cette relation est une relation d'équivalence sur A. On note A/B l'ensemble quotient formé des classes d'équivalence $\mathrm{Cl}(x) = x + B := x \bmod B$. Enfin on note $\pi_B : A \to A/B$ la surjection canonique. On souhaite mettre sur A/B une structure de groupe telle que la projection canonique soit un morphisme de groupes. Autrement dit, nous souhaitons définir une loi $+$ sur A/B telle que

$$\forall x, y \in A, \quad \pi_B(x + y) = \pi_B(x) + \pi_B(y).$$

Sur cette identité on constate que la seule solution est donc de poser comme addition sur A/B la définition suivante :

$$\forall x, y \in A, \quad (x \bmod B) + (y \bmod B) := (x + y) \bmod B.$$

Théorème 1.7.1 *La loi ci-dessus est bien définie et munie l'ensemble A/B d'une structure de groupe, de neutre $0 \bmod B$, telle que π_B est un morphisme de groupes et telle que l'opposé d'un élément $a \bmod B$ est l'élément $-a \bmod B$.*

Démonstration : Le point essentiel est de vérifier que cette application + est bien définie sur $A/B \times A/B$, les axiomes de groupes étant ensuite facilement vérifiés et le fait que π_B estun morphisme découlant de la définition même de l'aplication +. Soient donc $x, y, u, v \in A$ tels que $x = u \bmod B$ et $y = v \bmod B$. On veut montrer que $(x + y) = (u + v) \bmod B$. Or on a $(x+y)-(u+v) = (x-u)+(y-v)$ qui est donc une somme de deux éléments de B donc est dans B, autrement dit $x + y = u + v \bmod B$. □

Remarque 1.7.2 Noter que toute cette construction est une généralisation de la construction du groupe $\mathbb{Z}/n\mathbb{Z}$ comme on le voit en prenant $A = \mathbb{Z}$ et $B = n\mathbb{Z}$.

Proposition 1.7.3 *Soient A, B, C trois groupes abéliens et soit $\psi : A \to C$ un morphisme de groupes. On suppose que B est un sous-groupe de A tel que $B \subset \mathrm{Ker}(\psi)$. Il existe alors un unique morphisme $\bar{\psi} : A/B \to C$ tel que $\psi = \bar{\psi} \circ \pi_B$.*

Démonstration : Soient $f, g : A/B \to C$ deux morphismes de groupes tels que $g \circ \pi_B = \psi = f \circ \pi_B$. Vérifions que $g = f$: on va voir que f et g coincident point par point. Soit donc X un élément quelconque de A/B. Par définition (et surjectivité de π_B) il existe $x \in A$ tel que $X = (x \bmod B) = \pi_B(x)$. Donc on a

$$g(X) = g(x \bmod B) = g(\pi_B(x)) = \psi(x) = f(\pi_B(x)) = f(x \bmod B) = f(X).$$

Ceci prouve que $f = g$ et donc l'unicité de l'aplication $\bar{\psi}$. Reste à prouver qu'il existe un tel morphisme de groupes $\bar{\psi}$ satisfaisant $\psi = \bar{\psi} \circ \pi_B$. Supposons pour l'instant qu'il existe une telle application $\bar{\psi}$ et vérifions que c'est un morphisme de groupes. Soient $X, Y \in A/B$. Il existe $x, y \in A$ tels que $X = (x \bmod B)$ et $Y = (y \bmod B)$. On a de plus :

$$\begin{aligned}
\bar{\psi}(X+Y) &= \bar{\psi}(x \bmod B + y \bmod B) \\
&= \bar{\psi}(\pi_B(x) + \pi_B(y)) \text{ d'où en utilisant que } \pi_B \text{ est un morphisme,} \\
&= \bar{\psi}(\pi_B(x+y)) \text{ d'où par définition de } \bar{\psi}, \\
&= \psi(x+y) \text{ et } \psi \text{ étant un morphisme,} \\
&= \psi(x) + \psi(y) \\
&= \bar{\psi}(X) + \bar{\psi}(Y).
\end{aligned}$$

Finalement si la fonction $\bar{\psi}$ existe, c'est automatiquement un morphisme de groupes. Reste à prouver l'existence de la fonction $\bar{\psi}$. Soit $X = \pi_B(x) = x \bmod B \in A/B$, on pose pour cela : $\bar{\psi}(X) := \psi(x)$. La seule chose à vérifier est que cette application est bien définie : on se donne donc $y \in A$ tel que $x = y \bmod B$ et il reste à voir que $\psi(x) = \psi(y)$. Or

$$\psi(x) = \psi(y) \iff \psi(x-y) = 0 \iff x - y \in \mathrm{Ker}(\psi).$$

Par hypothèse B est inclus dans $\mathrm{Ker}(\psi)$ donc $x = y \bmod B$ entraîne que $x - y \in B \subset \mathrm{Ker}(\psi)$ et l'identité précédente implique que $\bar{\psi}$ est bien définie. □

Corollaire 1.7.4 ***(Factorisation Canonique)*** *Soit $\psi : A \to C$ un morphisme de groupes abéliens. Alors ψ se factorise de la façon suivante :*

$$\psi : A \xrightarrow{\pi} A/\mathrm{Ker}(\psi) \xrightarrow{\bar{\psi}} \mathrm{Im}(\psi) \xhookrightarrow{i} C,$$

où π est la projection canonique sur $A/\mathrm{Ker}(\psi)$ et où $i(x) = x$ est l'inclusion naturelle de $\mathrm{Im}(\psi)$ dans C.

De plus le morphisme $\bar{\psi}$ est un isomorphisme de groupes entre $A/\mathrm{Ker}(\psi)$ et $\mathrm{Im}(\psi)$.

Démonstration : On applique la proposition précédente avec $B = \mathrm{Ker}(\psi)$. La seule chose restant à vérfier est l'injectivité de $\bar{\psi}$: soit donc $a \bmod \mathrm{Ker}(\psi)$ dans le noyau de $\bar{\psi}$. On a

$$0 = \bar{\psi}(a \bmod \mathrm{Ker}(\psi)) = \psi(a).$$

Donc a est dans le noyau de ψ. En particulier $a = 0 \bmod \mathrm{Ker}\psi$ d'où l'injectivité de $\bar{\psi}$. □

Corollaire 1.7.5 *Soient $\psi : A \to B$ un morphisme de groupes abéliens. Si A est fini alors on a*

$$\mathrm{Card}(A) = \mathrm{Card}(\mathrm{Im}(\psi)) \cdot \mathrm{Card}(\mathrm{Ker}(\psi)).$$

1.7.2 Quotient d'un anneau par un idéal

Définition 1.7.6 Soit A un anneau commutatif et I un sous-ensemble de A. On dit que I *est un idéal de A* si

1. I est un sous-groupe du groupe commutatif $(A, +)$, et
2. $\forall x \in I$, $\forall a \in A$, on a $ax \in I$.

Exemple 1.7.7 Soit A un anneau commutatif.

1. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ quand n parcourt les entiers positifs ou nul (un idéal est un sous-groupe donc les idéaux de $\mathbb{Z}$ sont parmi les $n\mathbb{Z}$. De plus les $n\mathbb{Z}$ sont visiblement des idéaux).
2. $\{0\}$ et A sont des idéaux de A.
3. Si $\varphi : A \to B$ est un morphisme d'anneaux, alors $\mathrm{Ker}(\varphi)$ est un idéal de A (mais $\mathrm{Im}(\varphi)$ est un sous-anneau de B qui n'est pas un idéal en général).

L'idéal I étant en particulier un sous-groupe de $(A, +)$ on peut en particulier considérer la relation de congruence précédemment introduite :

$$\forall x, y \in A,\ x = y \bmod I \overset{\text{définition}}{\iff} x - y \in I.$$

On note A/I l'ensemble quotient constitué des classes d'équivalence $x + I$ pour cette relation. On sait déjà que l'on peut munir A/I d'une (unique) loi de groupe (abélien) telle que π_I est un morphisme de groupes. La loi est donnée par

$$\forall X = \pi_I(x), Y = \pi_I(y) \in A/I, \quad X + Y := \pi_I(x + y).$$

Autrement dit on a $(x \bmod I) + (y \bmod I) = (x + y) \bmod I$ pour tout $x, y \in A$. On peut en fait faire mieux, utilisant que I est un idéal :

Proposition 1.7.8 *Le groupe abélien $(A/I, +)$ est muni d'une seconde loi $\cdot$ telle que le triplet $(A/I, +, \cdot)$ est un anneau commutatif et telle que π_I est un morphisme d'anneaux. La loi est donnée par*

$$\forall x, y \in A, \quad (x \bmod I) \cdot (y \bmod I) := (xy) \bmod I.$$

L'élément neutre est $1 \bmod I$.

Démonstration : Par définition on voit que $\forall x, y \in A$ on a $\pi_I(xy) = \pi_I(x) \cdot \pi_I(y)$ et $\pi_I(1) = 1$. Donc si la loi est bien définie et A/I est un anneau, alors π_I est visiblement un morphisme d'anneaux. Prouvons que la loi $\cdot$ est bien définie sur A/I. Soit $x, a, y, b \in A$ tels que $x = a \bmod I$ et $y = b \bmod I$. On veut montrer que $xy = ab \bmod I$ autrement dit que la différence $xy - ab$ est dans I. Or on a

$$\exists \lambda, \mu \in I, \quad x = a + \ \lambda \text{ et } \ y = b + \mu.$$

Donc $xy = ab + \lambda y + a\mu$. Comme I est un idéal, on voit que $a\mu + \lambda y \in I$ ce que l'on voulait montrer. Il reste à prouver que munis de cette seconde loi $\cdot$, A/I est un anneau. Pour cela il suffit vérifier que $\cdot$ est associative et distributive sur $+$. Ceci découle des propriétés analogues sur A. □

Tout comme dans le cas des groupes nous pouvons utiliser cette notion de quotient pour obtenir la *factorisation canonique d'un morphisme d'anneaux* :

Théorème 1.7.9 ***(Factorisation Canonique)*** *Soit $\psi : A \to B$ un morphisme d'anneaux commutatifs. Alors ψ se factorise de la façon suivante :*

$$\psi : A \xrightarrow{\pi} A/\mathrm{Ker}(\psi) \xrightarrow{\bar{\psi}} \mathrm{Im}(\psi) \xhookrightarrow{i} B,$$

où π est la projection canonique sur $A/\mathrm{Ker}(\psi)$ et où $i(x) = x$ est l'inclusion naturelle de $\mathrm{Im}(\psi)$ dans B.

De plus le morphisme $\bar{\psi}$ est un isomorphisme d'anneaux entre $A/\mathrm{Ker}(\psi)$ et $\mathrm{Im}(\psi)$.

Démonstration : Notons $I := \mathrm{Ker}(\psi)$. Par la factorisation canonique pour les groupes abéliens, il suffit de vérifier que $\bar{\psi}$ est un morphisme d'anneaux pour conclure. On sait déjà que c'est un morphisme de groupes. Par ailleurs, on a $\bar{\psi}(1 \bmod I) = \bar{\psi}(\pi_I(1)) = \psi(1) = 1$. La dernière égalité provenant de ce que ψ est un morphisme d'anneaux. De même, on a

$$\begin{aligned} \forall X = \pi_I(x), Y = \pi_I(y), \quad \bar{\psi}(X \cdot Y) &= \bar{\psi}(\pi_I(x)\pi_I(y)) = \bar{\psi}(\pi_I(xy)) \\ &= \psi(xy) = \psi(x)\psi(y) = \bar{\psi}(X)\bar{\psi}(Y). \end{aligned}$$

Ceci achève la preuve. □

Avec cette notion d'anneau quotient nous allons maintenant pouvoir définir la caractéristique d'un corps et construire explicitement le corps à quatre éléments.

Définition 1.7.10 Soit $\mathbb{K}$ un corps. Considérons le morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{K}$ défini par $n \mapsto n \cdot 1$. Soit $n \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$. On dit que l'entier n est *la caractéristique du corps* $\mathbb{K}$. Par la factorisation canonique, on en déduit un morphisme d'anneaux injectif $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{K}$. En particulier, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre, donc $n = 0$ (on dit que $\mathbb{K}$ est de caractéristique nulle) ou $n = p$ est un nombre premier (on dit que $\mathbb{K}$ est de caractéristique p).

1.7.3 Quotient d'espaces vectoriels

Dans ce paragraphe, après avoir rappelé la définition d'un espace-vectoriel sur un corps $\mathbb{K}$ ainsi que la notion d'application linéaire, nous supposerons que le lecteur a déjà une connaissance des notions de base liées aux espaces vectoriels : notamment la notion de (somme de) sous-espaces vectoriels, de dimension, de supplémentaires, de famille libre et/ou génératrice. Nous

utilisons ces notions pour construire les espaces vectoriels quotients et obtenir dans ce contexte la factorisation canonique d'une application linéaire.

Dans toute la suite de ce paragraphe $\mathbb{K}$ est un corps fixé une fois pour toute (cela peut par exemple être $\mathbb{R}, \mathbb{C}$ mais aussi $\mathbb{Q}$, ou $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier).

Définition 1.7.11 Soit E un ensemble. On dit que E est *un $\mathbb{K}$-espace vectoriel* si

1. E est muni d'une loi $+$ (dite *interne*) telle que $(E, +)$ est un groupe abélien,
2. E est muni d'une loi $\cdot$ (dite *externe*) telle que $\forall x, y \in E$ et $\forall \lambda, \mu \in \mathbb{K}$, on a
   (a) $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
   (b) $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$
   (c) $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$
   (d) $1 \cdot x = x$.

Définition 1.7.12 Soit $(E, +, \cdot)$ un $\mathbb{K}$-e.v et soit $F \subset E$. On dit que F est un *sous-espace vectoriel* de E (s.e.v en abrégé) si $(F, +, \cdot)$ est un $\mathbb{K}$-e.v.

Proposition 1.7.13 *Soit $(E, +, \cdot)$ un $\mathbb{K}$-e.v et soit $F \subset E$. Alors F est un sous $\mathbb{K}$-e.v. si et seulement si*

$$F \neq \emptyset, \quad \text{et} \quad \forall x, y \in F,\ \forall \lambda, \mu \in \mathbb{K},\ \lambda x + \mu y \in F.$$

Démonstration : Classique. □

Définition 1.7.14 Soit $f : E \to F$ une application entre deux $\mathbb{K}$-e.v. On dit que f est *linéaire* si

$$\forall x, y \in E,\ \forall \lambda, \mu \in \mathbb{K},\ f(\lambda x + \mu y) = \lambda f(x) + \mu f(y).$$

Remarque 1.7.15 Notons qu'une application linéaire est en particulier un morphisme de groupes (il suffit de prendre $\lambda = \mu = 1$ pour s'en convaincre).

Exemple 1.7.16 Si $f : E \to F$ est une application linéaire, alors $\mathrm{Ker}(f)$ est un sous-e.v de E et $\mathrm{Im}(f)$ est un sous-e.v de F.

Soit E un espace vectoriel et F un sous-e.v de E. On peut considérer l'ensemble quotient pour la relation de congruence modulo F donnée comme toujours par

$$\forall x, y \in E, \quad x = y \bmod F \quad \overset{\text{définition}}{\iff} \quad x - y \in F.$$

L'ensemble E/F des classes d'équivalences $x + F$ est muni d'une structure de groupe abélien telle que la projection canonique π_F est un morphisme de groupes. Utilisant que E et F sont des espaces vectoriels, nous allons munir cet ensemble quotient d'une structure de K-espace vectoriel tel que π_F est une application linéaire. On définit pour cela la loi externe $\cdot$ sur E/F de la façon suivante :

$$\forall X = \pi_F(x) \in E/F,\ \forall \lambda \in \mathbb{K}, \quad \lambda \cdot X := \pi_F(\lambda x).$$

Proposition 1.7.17 *Muni de la loi externe précédente, $(E/F, +, \cdot)$ est un $\mathbb{K}$-e.v tel que $\pi_F : E \to E/F$ est une application linéaire.*

Démonstration : Par le travail fait sur les groupes abéliens, on sait que $(E/F, +)$ est un groupe abélien et on vérifie aisément que muni de $\cdot$ c'est un $\mathbb{K}$-e.v. Par ailleurs on sait aussi que π_F est un morphisme de groupes et on vérifie que c'est une application linéaire : soit $x, y \in E$ et soit $\lambda, \mu \in \mathbb{K}$; on a

$$\begin{aligned} \pi_F(\lambda x + \mu y) &= \pi_F(\lambda x) + \pi_F(\mu y) \text{ car } \pi_F \text{ est un morphisme de groupes} \\ &= \lambda \pi_F(x) + \mu \pi_F(y) \text{ par définition de } \cdot. \end{aligned}$$

Ceci conclut la preuve. □

Définition 1.7.18 Soient E un $\mathbb{K}$-ev et soit F un s.e.v de E. Si E/F est de dimension finie, on dit que F est de *codimension finie* dans E. On appelle *codimension* de F dans E l'entier $\mathrm{codim}_E F := \dim(E/F)$. Si $\mathrm{codim}_F(E) = 1$ on dit que F est *un hyperplan de* E.

Proposition 1.7.19 *Soit E un $\mathbb{K}$-ev. Un s.e.v F de E est de codimension finie dans E si et seulement si F admet un supplémentaire S dans E de dimension finie. On a alors* $\dim S = \mathrm{codim}_E F$.

Démonstration : Supposons tout d'abord que E/F est de dimension finie. Soit $x \in E$. Notons $\bar{x} := \pi_F(x)$, l'image de x modulo F. On introduit une base $(\bar{e}_1, \ldots, \bar{e}_n)$ de E/F et notons $S := \mathrm{Vect}(e_1, \ldots, e_n)$.

On a $F \cap S = \{0\}$: en effet, si $x = \sum_i \lambda_i e_i \in F \cap S$, alors modulo F on a $0 = \bar{x} = \sum_i \lambda_i \bar{e}_i$ donc pour tout i ceci implique que $\lambda_i = 0$ donc que $x = 0$.

On a $E = F + S$: en effet, si $x \in E$, il existe $\lambda_1, \ldots, \lambda_n$ tels que $\bar{x} = \sum_i \lambda_i \bar{e}_i$. Posons $y := \sum_i \lambda_i e_i \in S$. On a $\bar{y} = \bar{x}$ donc $x - y$ est dans F donc x est la somme d'un élément $y \in S$ et d'un élément $x - y \in F$. Ceci prouve la première implication.

Notons que dans ce cas, on a $\dim S = n = \dim(E/F)$ ce qui prouve la seconde assertion de la proposition.

Supposons maintenant réciproquement qu'il existe S de dimension finie, notée n, tel que $E = F \oplus S$. Soit $(e_1, \ldots, e_n)$ une base de S.Vérifions que $(\bar{e}_1, \ldots, \bar{e}_n)$ est une base de E/F où l'on a noté $\bar{x} := \pi_F(x)$ l'image dans E/F d'un élément de E par la projection canonique.

La famille est est génératrice : en effet, si $X \in E/F$, il existe $x \in E$ tel que $X = \pi_F(x) = \bar{x}$. Donc il existe $s \in S$ et $y \in F$ tels que $x = s + y$ donc tels que $X = \bar{s} + \bar{y}$. Mais $y \in F$ donc $\bar{y} = \pi_F(y) = 0$ dans E/F. Donc $X = \bar{x} = \bar{s} \in \mathrm{Vect}(\bar{e}_1, \ldots, \bar{e}_n)$.

La famille est libre : en effet si on a $\sum_i \lambda_i \bar{e}_i = 0$ dans E/F alors par définition de la relation de congruence, on a $\sum_i \lambda_i e_i \in F$. Or les e_i sont tous dans S sonc la somme également et comme $F \cap S = \{0\}$ on en déduit que $\sum_i \lambda_i e_i = 0$. Mais la famille $(e_1, \ldots, e_n)$ est libre donc les λ_i sont tous nuls. Ceci conclut la preuve. □

Corollaire 1.7.20 *Soit E un $\mathbb{K}$-e.v de dimension finie et F un s.e.v de E. Alors F est de codimension finie dans E et*

$$\mathrm{codim}_E F = \dim E - \dim F.$$

Nous pouvons maintenant utiliser ces résultats pour prouver dans le contexte des espaces vectoriels un théorème de factorisation canonique des applications linéaires et en déduire le théorème du rang.

Théorème 1.7.21 *Soit $f : E \to F$ une application linéaire entre deux $\mathbb{K}$-e.v. Alors f se factorise par passage au quotient en une application linéaire $\bar{f} : E/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ qui est un isomorphisme de $\mathbb{K}$-e.v.*

Démonstration : On sait par la factorisation canonique pour les groupes abéliens que f se factorise par passage au quotient en un morphisme de groupes $\bar{f} : E/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ qui est un isomorphisme. Il suffit donc pour conclure de vérifier que $\bar{f}$ est linéaire ce qui est facile sur les définitions. □

Corollaire 1.7.22 ***(Théorème du rang)*** *Soient E un $\mathbb{K}$-e.v de dimension finie, F un $\mathbb{K}$-e.v et $f : E \to F$ une application linéaire. Alors*

$$\dim E = \dim \mathrm{Im}(f) + \dim \mathrm{Ker}(f).$$

Démonstration : Posons $F := \mathrm{Ker}(f)$. Le corollaire préédent 1.7.20 nous assure que E/F est de dimension finie et que l'on a $\dim(E/F) = \mathrm{codim}_E F = \dim E - \dim F$ Or on sait par le théorème précédent que E/F est isomorphe à $\mathrm{Im}(f)$. Notamment ces deux e.v sont de même dimension ce qui permet de conclure. □

1.7.4 Construction du corps à 4 éléments

Soit $\mathbb{F}_4 = \{x, y, a, b\}$ un ensemble à quatre éléments. On voudrait munir cet ensemble d'une structure de corps et voir que cette structure est unique à isomorphisme près. Posons

$$0 := x \quad \text{et} \quad 1 := y.$$

On cherche donc à construire une loi $+$ telle que $(\mathbb{F}_4, +)$ est groupe abélien et une loi $\cdot$ telle que $(\mathbb{F}_4, +, \cdot)$ est un corps. Introduisons le morphisme $\varphi : \mathbb{Z} \to \mathbb{F}_4$ donné par $n \mapsto n \cdot 1$. Notons $d\mathbb{Z}$ son noyau. Par factorisation canonique, on voit que $\mathbb{Z}/d\mathbb{Z}$ s'injècte dans $\mathbb{F}_4$, donc est intègre et de cardinal divisant 4, donc $d = 2$: le corps $\mathbb{F}_4$ est de caractéristique 2 et est muni d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Notamment, en tant que groupe il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Ceci impose complètement la loi de groupe $+$ sur $\mathbb{F}_4$ qui est donc unique. Notamment pour tout $x \in \mathbb{F}_4$ on a $x + x = 2x = 0$. On pose ensuite :

$a+1 := b$ (sinon on aurait $a + 1 = 1$ qui implique $a = 0$ ou $a + 1 = 0$ qui implique $a = -1 = 1$).

$a + b := 1$ (un raisonnement similaire au précédent exclut les autres possibilités).

Ceci définit complètement la loi de groupe commutatif sur $\mathbb{F}_4$. On vérifie aisément les axiomes de groupe commutatif à partir de là.

Il reste à définir la multiplication $\cdot$: pour tout $x \in \mathbb{F}_4$ on pose $0 \cdot x := 0$ car 0 est absorbant dans un anneau et $1 \cdot x := x$ car 1 doit être le neutre pour $\cdot$. Le groupe des inversible du corps $\mathbb{F}_4$ est de cardinal 3 (composé de tous les éléments non nuls). Le nombre 3 étant premier on en déduit l'isomorphisme de groupes $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Ceci impose la loi de multiplication : les éléments a et b sont nécessairement d'ordre 3 donc

$a^2 := b$ (sinon $a^2 = 1$ implique a d'ordre divisant 2 et $a^2 = a$ implique $a = 1$).

$b^2 := a$ (par symétrie), et

$ab := 1$ (car a et b sont inversibles donc ab aussi et $ab = a$ implique $b = 1$ et $ab = b$ implique $a = 1$).

On vérifie alors aisément que muni de ces lois $+$ et $\cdot$, l'ensemble $(\mathbb{F}_4, +, \cdot)$ est un corps.

Chapitre 2

Dualité

2.1 Dual

Dans tout ce chapitre, E est un espace vectoriel sur un corps $\mathbb{K}$. Les en-têtes de paragraphe indiqueront si on suppose E de dimension finie ou non.

Définition 2.1.1 On appelle *forme linéaire* sur E toute application linéaire de E dans $\mathbb{K}$. On note E^* l'ensemble des formes linéaires de E dans $\mathbb{K}$ et on l'appelle le *dual de* E.

Proposition 2.1.2 *l'ensemble E^* est un $\mathbb{K}$-ev.*

Démonstration : Immédiat. □

Définition 2.1.3 On appelle *bidual de* E, le dual E^{**} de E^*.

2.1.1 En dimension finie

On suppose ici que $\dim E = n < +\infty$.

Définition 2.1.4 Soit $(e_1, \ldots, e_n)$ une base de E. On définit pour $i \in \{1, \ldots, n\}$, les *formes linéaires coordonnées* $e_i^* : E \to \mathbb{K}$ par la formule

$$\forall \lambda_i \in \mathbb{K}, \quad e_i^* \left(\sum_{j=1}^{n} \lambda_j e_j \right) := \lambda_j, \quad \text{ie} \quad e_i^*(e_j) = \delta_{ij}$$

où δ_{ij} est le symbole de Kronecker valant 1 si $i = j$ et 0 sinon.

Remarque 2.1.5 Deux remarques :

1. Cette définition reste valable en dimension quelconque, partant d'une base $(e_i)_{i \in I}$ de E.
2. Attention : la définition de chaque e_i^* dépend du choix de toute la base $(e_1, \ldots, e_n)$. Par exemple si $E = \mathbb{R}^2$, posons $e_1 = (1, 0)$ et $v_1 = (0, 1)$ et $v_2 = (1, 1)$. Alors $\mathcal{B} := (e_1, v_1)$ et $\mathcal{B}_2 = (e_1, v_2)$ sont deux bases de $\mathbb{R}^2$. De plus

   $$\text{dans la base } \mathcal{B}_1, \text{ on a } e_1^*(v_2) = e_1^*(e_1 + v_1) = e_1^*(e_1) = 1;$$

   Mais

   $$\text{dans la base } \mathcal{B}_2, \text{ on a } e_1^*(v_2) = 0.$$

Théorème 2.1.6 *Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. Alors $\mathcal{B}^* := (e_1^*, \dots, e_n^*)$ est une base de E^*, appelée base duale de $\mathcal{B}$. Notamment on a $\dim E = \dim E^*$ et*

$$\forall \varphi \in E^*, \quad \varphi = \sum_{i=1}^{n} \varphi(e_i) e_i^*.$$

Démonstration : Supposons donnée une relation $\sum_{i=1}^n \lambda_i e_i^* = 0$. En évaluant cette identité en e_k pour tout $k \leq n$ on voit que $\lambda_k = 0$ pour tout k, d'où la liberté de la famille. Montrons maintenant que cette famille est génératrice : soit $\varphi \in E^*$ et soit $x = \sum_{i=1}^n \lambda_i e_i$ un élément quelconque de E. On a

$$\varphi(x) = \sum_{i=1}^{n} \lambda_i \varphi(e_i) = \sum_{i=1}^{n} e_i^*(x) \varphi(e_i).$$

Ceci prouve que les e_i^* forment une famille génératrice ainsi que la formule annoncée dans le théorème. □

Remarque 2.1.7 En dimension infinie, la famille $(e_i^*)_{i \in I}$ est toujours libre mais n'est plus génératrice.

2.1.2 Matrices et bases duales en dimension finie

On suppose ici que $\dim E = n < +\infty$.

Soient $\mathcal{B}_1, \mathcal{B}_2$ deux bases de E, de bases duales respectives $\mathcal{B}_1^*, \mathcal{B}_2^*$. Notons $\mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2)$ la matrice de passage de la base $\mathcal{B}_1$ à la base $\mathcal{B}_2$, ie telle que si $x \in E$ est un vecteur représenté par la matrice (colonne) X dans la base $\mathcal{B}_1$ et par la matrice (colonne) Y dans la base $\mathcal{B}_2$, on a

$$X = \mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2) Y.$$

Proposition 2.1.8 *On a $\mathrm{Pass}(\mathcal{B}_1^*, \mathcal{B}_2^*) = \left({}^t\mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2)\right)^{-1}$.*

Démonstration : Soit $f \in E^*$ de matrice (ligne) $(\alpha_1, \dots, \alpha_n)$ dans la base $\mathcal{B}_1^*$ et de matrice (ligne) $(\beta_1, \dots, \beta_n)$ dans la base $\mathcal{B}_2$. Soit $x \in E$ est un vecteur représenté par la matrice (colonne) X dans la base $\mathcal{B}_1$ et par la matrice (colonne) Y dans la base $\mathcal{B}_2$. On a

$$X = \mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2) Y \quad \text{et} \quad f(x) = (\alpha_1, \dots, \alpha_n) X = (\beta_1, \dots, \beta_n) Y.$$

Donc

$$(\alpha_1, \dots, \alpha_n) \mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2) Y = (\beta_1, \dots, \beta_n) Y.$$

Ceci est vrai pour tout Y donc on obtient ainsi

$$(\alpha_1, \dots, \alpha_n) \mathrm{Pass}(\mathcal{B}_1, \mathcal{B}_2) = (\beta_1, \dots, \beta_n),$$

Soit le résultat voulu en transposant cette égalité. □

2.1.3 Bidual en dimension finie

On suppose ici que $\dim E = n < +\infty$.

Théorème 2.1.9 *Soit $x \in E$. On note $\widehat{x} : E^* \to \mathbb{K}$ l'élément de E^{**} donné par la formule*

$$\forall \varphi \in E^*, \quad \widehat{x}(\varphi) := \varphi(x).$$

L'application $J : E \to E^{**}$, $x \mapsto \widehat{x}$ est un isomorphisme de $\mathbb{K}$-ev.

Démonstration : On vérifie aisément que $\widehat{x}$ est une forme linéaire sur E^* et que J est une application linéaire. On sait, étant en dimension finie, que $\dim E = \dim E^* = \dim E^{**}$. Il suffit donc de vérifier que J est injective pour conclure. Soit $x \in \mathrm{Ker}(J)$. Si $x \neq 0$ alors on peut compléter x en une base $(x, e_2, \ldots, e_n)$ de E et on a notamment $x^*(x) = 1$. En particulier on voit que $\widehat{x}(x^*) = 1 \neq 0$ ce qui contredit le fait que x est dans le noyau de J. D'où le résultat. □

2.1.4 Base antéduale en dimension finie

On suppose ici que $\dim E = n < +\infty$.

Proposition 2.1.10 *Soit $(f_1, \ldots, f_n)$ une base de E^*. Il existe une unique base $(e_1, \ldots, e_n)$ de E telle que*

$$\forall i \leq n, \quad e_i^* = f_i.$$

Démonstration : Par le théorème 2.1.9, on sait que pour tout $i \in \{1, \ldots, n\}$, il existe $e_i \in E$ tel que $f_i^* = \widehat{e_i}$. Donc on a

$$\forall i \neq j, \quad f_i^*(f_j) = 0 = \widehat{e_i}(f_j) = f_j(e_i) \quad \text{et} \quad f_i^*(f_i) = 1 = \widehat{e_i}(f_i) = f_i(e_i).$$

Ceci prouve que $f_i = e_i^*$ pour tout i. D'où l'existence. Montrons maintenant l'unicité : soit $(e_1, \ldots, e_n)$ une base de E telle que $e_i^* = f_i$ pour tout i. Si $i \neq j$ alors $e_i^*(e_j) = f_i(e_j) = 0 = \widehat{e_j}(f_i)$ et par ailleurs, pour tout i, $e_i^*(e_i) = f_i(e_i) = 1 = \widehat{e_i}(f_i)$. Ceci prouve que $\widehat{e_i} = f_i^*$ pour tout i. Or par injectivité de l'application J dans le théorème 2.1.9, on sait qu'il existe au plus un vecteur e_i tel que $\widehat{e_i} = f_i$, d'où l'unicité. □

Définition 2.1.11 Une base comme obtenue dans la proposition ci-dessus est dite *base antéduale* de $(f_1, \ldots, f_n)$.

2.1.5 Crochet de dualité en dimension finie

On suppose ici que $\dim E = n < +\infty$.

L'isomorphisme entre E et E^{**} nous donne la formule

$$\forall x \in E, \ \forall \varphi \in E^*, \quad \varphi(x) = \widehat{x}(\varphi).$$

On introduit le *crochet de dualité*

$$\langle x, \varphi \rangle := \varphi(x) = \widehat{x}(\varphi).$$

L'isomorphisme J se réécrit alors : $\forall x \in E$, $J(x) = \langle x, \cdot \rangle$.

2.1.6 Bidual et base antéduale en dimension finie

On suppose ici que $\dim E = n < +\infty$.

Proposition 2.1.12 *Soit $\mathcal{B}$ une base de E. Alors $J(\mathcal{B})$ est la base duale de $\mathcal{B}^*$.*

Démonstration : Posons $\mathcal{B} = (e_1, \ldots, e_n)$. On a

$$J(e_k)(e_i^*) = \langle e_k, e_i^* \rangle = e_i^*(e_k) = \delta_{ki}.$$

Par ailleurs par définition, $(e_k^*)^*(e_i^*) = \delta_{ki}$. □

Corollaire 2.1.13 ***(Expression de la base antéduale)*** *Soit $\mathcal{C}$ une base de E^*. Alors la base antéduale, $\mathcal{B}$ de $\mathcal{C}$, est donnée par la formule*

$$\mathcal{B} = J^{-1}(\mathcal{C}^*).$$

Démonstration : Par la proposition 2.1.10 précédente, il existe une base antéduale $\mathcal{B}$ de $\mathcal{C}$. On a $\mathcal{B}^* = \mathcal{C}$. Donc par la proposition 2.1.12 précédente on obtient $J(\mathcal{B}) = (\mathcal{B}^*)^* = \mathcal{C}^*$. □

2.2 Orthogonalité

2.2.1 Définition et premières propriétés

La dimension de E est ici a priori quelconque (finie ou infinie).

Définition 2.2.1 Soit A un sous-ensemble de E et B un sous-ensemble de E^*. On appelle *orthogonal de A* le s.e.v, noté $A^\perp$, de E^* défini par

$$A^\perp := \{\varphi \in E^* \mid \forall a \in A \ \langle a, \varphi \rangle = 0\}.$$

On appelle *orthogonal de B* le s.e.v B° de E défini par

$$B^\circ := \{x \in E \mid \forall \varphi \in B \ \langle x, \varphi \rangle = 0\}.$$

Remarque 2.2.2 En utilisant l'identification entre E et E^{**} donnée par J on voit qu'en dimension finie, on a

$$B^\perp = J(B^\circ)$$

ce qui justifie l'appelation orthogonal dans les deux cas. De plus, tout résultat prouvé, en dimension finie, pour $A^\perp$ entraîne, via J le même résultat pour B°. Donnons une preuve de l'identité ci-dessus :

$$\begin{aligned} B^\perp &= \{y \in E^{**} \mid \forall \varphi \in B \ \langle \varphi, y \rangle = 0\} \\ &= \{J(x) \in E^{**} \mid x \in E, \ \forall \varphi \in B \ \langle \varphi, J(x) \rangle = 0\} \\ &\quad \{J(x) \in E^{**} \mid x \in E, \ \forall \varphi \in B \ \langle x, \varphi \rangle = 0\} \\ &= J(B^\circ). \end{aligned}$$

Remarque 2.2.3 Si φ est une forme linéaire (ie un élément de E^*), on a $\{\varphi\}^\circ = \mathrm{Ker}(\varphi)$.

Proposition 2.2.4 *Si E est un $\mathbb{K}$-ev de dimension quelconque, on a les 4 propriétés suivantes :*

1. *Si $A_1 \subset A_2 \subset E$, alors $A_2^\perp \subset A_1^\perp$.*
2. *Si $B_1 \subset B_2 \subset E^*$, alors $B_2^\circ \subset B_1^\circ$.*
3. *Si $A \subset E$, alors $A^\perp = \mathrm{Vect}(A)^\perp$.*
4. *Si $B \subset E^*$, alors $B^\circ = \mathrm{Vect}(B)^\circ$.*

Démonstration : Nous donnons une preuve pour les points 1. et 3. et laissons le lecteur vérifier es propriétés analogues 2 et 4. Commençons par le point 1 : Soit $\varphi \in A_2^\perp$, on a $\varphi(x) = 0$ pour tout $x \in A_2$. En particulier ceci est vrai pour tout $x \in A_1$, donc φ est dans $A_1^\perp$. Concernant le point 3 : on a $A \subset \mathrm{Vect}(A)$ donc par ce que l'on vient de prouver on voit que $\mathrm{Vect}(A)^\perp \subset A^\perp$. Réciproquement, soit $\varphi \in A^\perp$, alors pour tout $x \in A$, on a $\varphi(x) = 0$, par linéarité de φ, on voit donc que φ s'annule sur toute combinaison linéaire d'éléments de A, autrement dit φ est dans $\mathrm{Vect}(A)^\perp$. □

2.2.2 Orthogonaux en dimension finie

On suppose ici que $\dim E = n < +\infty$. On se donne par ailleurs F un s.e.v de E de dimension $p \leq n$.

Pour obtenir $F^\perp$:

1. On se donne une base $(e_1, \ldots, e_p)$ de F.
2. On la complète en une base $(e_1, \ldots, e_n)$ de E.
3. On dualise cette seconde base obtenant ainsi une base $(e_1^*, \ldots, e_n^*)$ de E^*.

Proposition 2.2.5 *On a $F^\perp = \mathrm{Vect}(e_{p+1}^*, \ldots, e_n^*)$.*

Démonstration : On raisonne par équivalences :

$$\begin{aligned}
\varphi \in F^\perp &\iff \forall x \in F,\ \langle x, \varphi \rangle = 0 \\
&\iff \forall i \leq p,\ \langle e_i, \varphi \rangle = 0 \\
&\iff \forall i \leq p,\ \langle \varphi, e_i^{**} \rangle = 0 \text{ on a ici utilisé la proposition 2.1.12} \\
&\iff \varphi \in \mathrm{Vect}(e_{p+1}^*, \ldots, e_n^*).
\end{aligned}$$

□

De même si l'on part de G un s.e.v de E^* de dimension $p \leq n$, pour obtenir V° :

1. On se donne une base $(\varphi_1, \ldots, \varphi_p)$ de G.
2. On la complète en une base $(\varphi_1, \ldots, \varphi_n)$ de E^*.
3. On antédualise cette base, obtenant ainsi une base $(e_1, \ldots, e_n)$ de E telle que $e_i^* = \varphi_i$ pour tout i.

Proposition 2.2.6 $G^0 = \mathrm{Vect}(e_{p+1}, \ldots, e_n)$.

Démonstration : Comme précédemment, ou en utilisant l'isomorphisme J. □

Théorème 2.2.7 *Soit E un $\mathbb{K}$-ev de dimension finie. Soit F un s.e.v de E et G un s.e.v de E^*. On a*

1. $\dim F + \dim F^\perp = \dim E$ *et* $F^{\perp\circ} = F$.
2. $\dim G + \dim F^\circ = \dim E$ *et* $G^{\circ\perp} = G$.

Démonstration : C'est une conséquence immédiate de ce qui précède. □

Corollaire 2.2.8 *Si E est de dimension finie et F est un s.e.v de E alors*

$$F = E \iff F^\perp = \{0\}.$$

Remarque 2.2.9 L'égalité $F^{\perp\circ} = F$ reste vraie en dimension quelconque et on a de même $V \subset V^{\circ\perp}$. Mais cette inclusion n'est pas une égalité en général. Cette dernière assertion se voit par exemple en considérant $E = \mathbb{R}[X]$ et pour s.e.v V de E^*, le s.e.v engendré par les $\varphi_n : P \mapsto P^{(n)}(0)$ pour $n \in \mathbb{N}$ (**Exercice**).

2.2.3 Équations d'un sous-espace vectoriel en dimension finie

On peut traduire le théorème 2.2.7 précédent en termes d'équations :

Proposition 2.2.10 *Soit E un $\mathbb{K}$-e.v de dimension finie n.*

1. *Soit $\varphi_1, \dots, \varphi_p$ des éléments de E^* tels que $\mathrm{rg}(\varphi_1, \dots, \varphi_p) = r$. Alors le s.e.v $F = \{x \in E \mid \forall i \leq p,\ \varphi(x) = 0\}$ est de codimension r dans E.*
2. *Réciproquement, si F est un s.e.v de codimension r dans E, il existe r formes linéaires linéairement indépendantes $\varphi_1, \dots, \varphi_r$ tel que $F = \{x \in E \mid \forall i \leq r,\ \varphi(x) = 0\}$.*

Démonstration : On a en effet

$$\begin{aligned}\{x \in E \mid \forall i \leq p,\ \varphi_i(x) = 0\} &= \{x \in E \mid \forall i \leq p,\ \langle x, \varphi_i\rangle = 0\} \\ &= \{x \in E \mid \forall i \leq p,\ \langle x, \mathrm{Vect}(\varphi_1, \dots, \varphi_p)\rangle = 0\} \\ &= \mathrm{Vect}(\varphi_1, \dots, \varphi_p)^\circ.\end{aligned}$$

En posant $F = \{x \in E \mid \forall i \leq p,\ \varphi_i(x) = 0\}$, on en déduit :

$$\begin{aligned}F &= \dim \mathrm{Vect}(\varphi_1, \dots, \varphi_p)^\circ \\ &= \dim E - \dim \mathrm{Vect}(\varphi_1, \dots, \varphi_p) \\ &= \dim E - \mathrm{rg}(\varphi_1, \dots, \varphi_p).\end{aligned}$$

Pour le sens réciproque, introduisons une base $(\varphi_1, \dots, \varphi_r)$ de $F^\perp$. On vérifie immédiatement que $x \in F \iff \varphi_i(x) = 0$ pour tout $i \leq r$. □

Proposition 2.2.11 *Soient E de dimension finie, A_1, A_2 deux s.e.v de E et B_1, B_2 deux s.e.v de E^*. On a*

1. $(A_1 + A_2)^\perp = A_1^\perp \cap A_2^\perp$.
2. $(A_1 \cap A_2)^\perp = A_1^\perp + A_2^\perp$.
3. $(B_1 + B_2)^\circ = B_1^\circ \cap B_2^\circ$.

4. $(B_1 \cap B_2)^\circ = B_1^\circ + B_2^\circ$.

Démonstration : En utilisant l'isomorphisme J on voit qu'il suffit de prouver les points 1 et 2. On a $A_i \subset A_1 + A_2$ donc $(A_1 + A_2)^\perp \subset A_i^\perp$. Par ailleurs

$$\begin{aligned} \varphi \in A_1^\perp \cap A_2^\perp &\Rightarrow \langle A_1, \varphi\rangle = \langle A_2, \varphi\rangle = \{0\} \\ &\Rightarrow \langle A_1 + A_2, \varphi\rangle \subset \{0\} + \{0\} = \{0\} \\ &\Rightarrow \varphi \in (A_1 + A_2)^\perp. \end{aligned}$$

Ceci prouve le point 1. Pour le second point, on a

$$\begin{aligned} \varphi \in A_1^\perp + A_2^\perp &\Rightarrow \exists \varphi_i \in A_i^\perp,\ \varphi = \varphi_1 + \varphi_2 \\ &\Rightarrow \exists \langle A_1 \cap A_2, \varphi\rangle \subset \langle A_1 \cap A_2, \varphi_1\rangle + \langle A_1 \cap A_2, \varphi_2\rangle \\ &\Rightarrow \langle A_1 \cap A_2, \varphi\rangle \subset \langle A_1, \varphi_1\rangle + \langle A_2, \varphi_2\rangle \\ &\Rightarrow \langle A_1 \cap A_2, \varphi\rangle \subset \{0\} + \{0\} = \{0\} \\ &\Rightarrow \varphi \in (A_1 \cap A_2)^\perp \end{aligned}$$

On conclut en utilisant l'identité de dimension (valable pour tout s.e.v F, G)

$$\dim(F + G) + \dim(F \cap G) = \dim F + \dim G.$$

□

2.2.4 Orthogonalité et hyperplans

On part d'un $\mathbb{K}$ e.v E de dimension quelconque (finie ou infinie).

Proposition 2.2.12 *Soit $\varphi \in E^*$ une forme linéaire non nulle. Alors son noyau,* $\mathrm{Ker}(\varphi)$ *est un hyperplan de E. Réciproquement, tout hyperplan est le noyau d'une forme linéaire non nulle.*

Démonstration : Soit $0 \neq \varphi \in E^*$. On sait que $E/\mathrm{Ker}(\varphi)$ est isomorphe à $\mathrm{Im}(\varphi)$. Comme φ est non nulle, elle est surjective sur $\mathbb{K}$, donc $\mathrm{Ker}(\varphi)$ est de codimension 1, autrement dit est un hyperplan. Réciproquement, soit H un hyperplan de E. D'après la proposition 1.7.19 il existe un supplémentaire S à H dans E, de dimension 1. Autrement dit, il existe $x_0 \in E$ tel que $E = \mathbb{K}x_0 \oplus H$. On définit φ en posant $\varphi(x_0) = 1$ et $\varphi(x) = 0$ pour tout $x \in H$. Ceci donne le résultat. □

2.3 Applications transposées

2.3.1 Généralités

Les espaces vectoriels sont ici a priori de dimension quelconque.

Définition 2.3.1 Soient E et F deux $\mathbb{K}$-ev de dimension quelconque. Soit $u \in \mathrm{End}(E, F)$ une application linéaire de E dans F. L'application de F^* à valeurs dans E^* définie par $f \mapsto f \circ u$ est linéaire. Cette application s'appelle *la transposée de u* et se note ${}^t u$.

Proposition 2.3.2 *Soient E et F deux $\mathbb{K}$-ev. On a*

$$\mathrm{Ker}({}^t u) = (\mathrm{Im}\, u)^\perp.$$

De plus, si E et F sont de dimension finie, on a

$$\mathrm{rg}(u) = \mathrm{rg}({}^t u) \quad \text{et} \quad \mathrm{Im}({}^t u) = (\mathrm{Ker}\, u)^\perp.$$

Démonstration : Pour le premier point on raisonne par équivalences :

$$\varphi \in \mathrm{Ker}({}^t u) \iff \varphi \circ u = 0 \iff \mathrm{Im}u \subset \mathrm{Ker}\varphi \iff \varphi \in (\mathrm{Im}u)^\perp.$$

En dimension finie on a $\dim F = \mathrm{rg}(u) + \dim(\mathrm{Im}u)^\perp = \dim F^*$. Donc allié au point 1, ceci montre que

$$\mathrm{rg}(u) = \dim F^* - \dim(\mathrm{Im}u)^\perp = \dim F^* - \dim(\mathrm{Ker}{}^t u) = \mathrm{rg}({}^t u).$$

Pour le dernier point, soit $g \in \mathrm{Im}({}^t u)$. Il existe $f \in F^*$ telle que $g = f \circ u$, donc pour tout $x \in \mathrm{Ker}(u)$ on a $g(x) = 0$ et donc g apartient à $\mathrm{Ker}(u)^\perp$. Par ailleurs on a :

$$\mathrm{rg}({}^t u) = \mathrm{rg}(u) = \dim E - \dim \mathrm{Ker}(u) = \dim(\mathrm{Ker}u)^\perp.$$

On conclut donc par un argument de dimension. □

Remarque 2.3.3 Nous donnons plus loin, en dimension finie, une interprétation matricielle de ${}^t u$ qui permet de retrouver l'égalité de rang.

Proposition 2.3.4 *Soient E, F, G trois $\mathbb{K}$-ev. Soient $u \in \mathrm{End}(E, F)$ et $v \in \mathrm{End}(F, G)$. On a*

$${}^t(v \circ u) = {}^t u \circ {}^t v.$$

Démonstration : C'est un simple jeu d'écriture : soit $g \in G^*$, on a,

$$g \circ (v \circ u) = (g \circ v) \circ u = {}^t u(g \circ v) = {}^t u \circ [{}^t v(g)].$$

□

Proposition 2.3.5 *Soit E de dimension finie et $u \in \mathrm{End}(E)$. Un s.e.v F de E est stable par u si et seulement si $F^\perp$ est stable par ${}^t u$.*

Démonstration : Supposons que F est stable par u et soit $\varphi \in F^\perp$. On a $\varphi(F) = \{0\}$, donc $\varphi(u(F) \subset \varphi(F) = \{0\}$. Ceci montre que si $\varphi \in F^\perp$ alors ${}^t u(\varphi) \in F^\perp$ donc que $F^\perp$ est stable par ${}^t u$. Réciproquement d'après le point 2. de la proposition 2.2.10, en notant r la codimension de F dans E, on sait qu'il existe r formes linéaires $\varphi_1, \ldots, \varphi_r$ telles que $F = \bigcap_{i=1}^r \mathrm{Ker}\varphi_i$. En particulier on voit que pour tout i, on a $F \subset \mathrm{Ker}(\varphi_i)$ ie que $\varphi_i \in F^\perp$. Mais $F^\perp$ est stable par ${}^t u$ donc ${}^t u\varphi_i = \varphi_i \circ u \in F^\perp$ pour tout i, donc $\varphi_i(u(F)) = \varphi_i[u(F)] = 0$ pour tout i. Autrement dit pour tout i, on a $u(F) \subset \mathrm{Ker}\varphi_i$ donc $u(F) \subset F$. □

Remarque 2.3.6 Cet énoncé reste vrai en dimension quelconque. Par ailleurs il s'agit d'un énoncé très utile pour des raisonnements par récurrence sur la dimension (cf. par exemple plus tard une démonstration du théorème de trigonalisation).

2.3.2 Lien avec l'interprétation matricielle

Soient E, F deux $\mathbb{K}$-ev de dimension finie (notées respectivement m et n). Soit $u \in \mathrm{End}(E, F)$, soit $\mathcal{B}$ une base de E (de base duale $\mathcal{B}^*$) et soit $\mathcal{B}'$ une base de F (de base duale $\mathcal{B}'^*$).

Proposition 2.3.7 *Avec les notations précédentes on a*

$$\left[{}^t u\right]_{\mathcal{B}^*}^{\mathcal{B}'^*} = {}^t\left([u]_{\mathcal{B}}^{\mathcal{B}'}\right).$$

Démonstration : Soient $f \in F^*$. Notons $(\alpha_1, \ldots, \alpha_m)$ sa matrice (ligne) dans la base $\mathcal{B}'$. Posons $g := f \circ u \in E^*$ et notons $(\beta_1, \ldots, \beta_n)$ sa matrice (ligne) dans la base $\mathcal{B}$. On a

$$(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_m)[u]_{\mathcal{B}}^{\mathcal{B}'}.$$

En transposant on obtient ainsi (en notant Y le vecteur colonne formé des β_i et X le vecteur colonne formé des α_i)

$$Y = {}^t\left([u]_{\mathcal{B}}^{\mathcal{B}'}\right) X.$$

Ceci donne le résultat. □

Chapitre 3

Formes bilinéaires et sesquilinéaires

Dans toute la suite $\mathbb{K}$ est un corps quelconque (qui peut notamment être le corps des complexes $\mathbb{C}$). Sur le corps des complexes, nous noterons $\bar{\cdot}$ la conjuguaison complexe.

3.1 Définitions et généralités

Définition 3.1.1 Soit E un $\mathbb{K}$-e.v et $\varphi : E \times E \to \mathbb{K}$ une application. On dit que φ est *bilinéaire* sur E si

1. Pour tout $y \in E$, l'application $\varphi(x, \cdot) : y \mapsto \varphi(x, y)$ est linéaire, et si
2. Pour tout $x \in E$, l'application $\varphi(\cdot, y) : x \mapsto \varphi(x, y)$ est linéaire.

Définition 3.1.2 Soit E un $\mathbb{C}$-e.v et $\varphi : E \times E \to \mathbb{C}$ une application. On dit que φ est *sesquilinéaire* sur E si

1. Pour tout $y \in E$, l'application $\varphi(x, \cdot) : y \mapsto \varphi(x, y)$ est linéaire, et si
2. Pour tout $x \in E$, l'application $\varphi(\cdot, y) : x \mapsto \varphi(x, y)$ vérifie :

$$\forall u, v \in E, \forall \lambda \in \mathbb{C}, \quad \varphi(u + \lambda v, y) = \varphi(u, y) + \bar{\lambda}\varphi(v, y).$$

La propriété 2. s'appelle l'*anti-linéarité*.

Remarque 3.1.3 Sur le corps $\mathbb{C}$ on peut donc considérer deux types d'objets :

1. Les formes bilinéaires (puis, cf. plus loin, les formes bilinéaires symétriques et les formes quadratiques associées).
2. Les formes sesquilinéaires (puis, cf. plus loin, les formes sesquilinéaires à symétrie hermitienne et les formes hermitiennes associées).

Exemple 3.1.4

1. Soit E le $\mathbb{C}$-ev (de dimension infinie) des fonctions continues de $[0, 1]$ dans $\mathbb{C}$. L'application
$$\varphi : E^2 \to \mathbb{C}, \quad (f, g) \mapsto \int_0^1 \overline{f(t)} g(t) dt$$
est une forme sesquilinéaire sur E.
2. L'application $\varphi : \mathbb{K}^2 \to \mathbb{K}$, $(x, y) \mapsto xy$ est bilinéaire.

Convention et notation : Un certain nombre de résultats sur les formes bilinéaires (sur un corps $\mathbb{K}$ quelconque) et sur les formes sesquilinéaires (sur $\mathbb{C}$) peuvent s'énoncer et se démontrer de façon assez parallèle. Afin de ne pas tout écrire en double nous introduisons la fonction $\sigma : \mathbb{K} \to \mathbb{K}$ qui sera

1. $\sigma = \mathrm{Id}_{\mathbb{K}}$ sur un corps quelconque ;
2. $\sigma = \mathrm{Id}_{\mathbb{C}}$ ou $\sigma = \bar{\cdot}$ sur le corps $\mathbb{C}$.

Nous parlerons alors désormais de forme σ-sesquilinéaire pour désigner :

1. sur un corps $\mathbb{K}$ quelconque, une forme bilinéaire ($\sigma = \mathrm{Id}_{\mathbb{K}}$) ;
2. sur $\mathbb{C}$, une forme bilinéaire si $\sigma = \mathrm{Id}_{\mathbb{C}}$ et une forme sesquilinéaire si $\sigma = \bar{\cdot}$.

Par convention, un énoncé de la forme "Soit $\mathbb{K}$ un corps et φ une forme σ-sesquilinéaire..." signifiera donc pour nous que l'on peut choisir $\mathbb{K}$ quelconque (éventuellement $\mathbb{K} = \mathbb{C}$) et φ bilinéaire, ou bien $\mathbb{K} = \mathbb{C}$ et φ sesquilinéaire.

De plus nous utiliserons dans ce qui suit la notation exponentielle λ^σ pour désigner respectivement : λ si $\sigma = \mathrm{Id}_{\mathbb{K}}$ et $\bar{\lambda}$ si $\sigma = \bar{\cdot}$. Si M est une matrice composée d'éléments m_{ij} dans $\mathbb{K}$ on notera de même M^σ la matrice (m_{ij}^σ) et on notera M^* sa matrice transposée : $M^* = {}^tM^\sigma$.

Supposons E un $\mathbb{K}$-ev de dimension finie n et φ une forme σ-sesquilinéaire. Notons $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Soient $x, y \in E$ il existe une unique décomposition des vecteurs x et y dans la base $\mathcal{B}$:

$$x = \sum_{i=1}^{n} x_i e_i \quad \text{et} \quad y = \sum_{i=1}^{n} y_i e_i.$$

On a donc par linéarité (ou anti-linéarité si $\mathbb{K} = \mathbb{C}$ et si φ est sesquilinéaire avec $\sigma = \bar{\cdot}$)

$$\varphi(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i^\sigma y_j \varphi(e_i, e_j).$$

Autrement dit la forme φ est déterminée par les n^2 valeurs $\varphi_{ij} := \varphi(e_i, e_j)$. Notons A la matrice carrée de taille n, $(\varphi_{ij})_{i,j}$.

Définition 3.1.5 On dit que A est *la matrice associée à la forme* φ.

Proposition 3.1.6 *Avec les notations précédentes, en notant X (respectivement Y) le vecteur colonne correspondant à x (respectivement à y), on a*

$$\varphi(x, y) = X^* A Y.$$

Démonstration : Il suffit d'écrire le produit matriciel $X^*(AY)$. □

On suppose toujours E de dimension finie et on se donne $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E ainsi que la matrice de passage, P de $\mathcal{B}$ à $\mathcal{B}'$. Soit φ une forme σ-sesquilinéaire de matrice A dans la base $\mathcal{B}$ et de matrice A' dans la base $\mathcal{B}'$. On a la formule

$$A' = P^* A P.$$

Définition 3.1.7 Soit $\mathbb{K}$ un corps quelconque et soit φ une forme *bilinéaire*. On dit que φ est *symétrique* (respectivement *anti-symétrique*) si pour tout $x, y \in E$ on a

$$\varphi(x, y) = \varphi(y, x) \quad \text{(respectivement} \quad \varphi(x, y) = -\varphi(y, x)).$$

Remarque 3.1.8 Si E est de dimension finie, φ est symétrique (resp. anti-symétrique) si et seulement si sa matrice associée dans une base est symétrique (resp. anti-symétrique).

Proposition 3.1.9 *Soit K un corps de caractéristique différente de 2. Notons $\mathcal{S}_n$ (resp. $\mathcal{A}_n$) le s.e.v des matrices symétriques (resp. anti-symétriques) de $\mathcal{M}_n(\mathbb{K})$. On a*

$$\mathcal{M}_n(\mathbb{K}) = \mathcal{S}_n \oplus \mathcal{A}_n.$$

De plus $\mathcal{S}_n$ est un $\mathbb{K}$-e.v de dimension $n(n+1)/2$ et $\mathcal{A}_n$ est un $\mathbb{K}$-ev de dimension $n(n-1)/2$.

Démonstration : Si M est à la fois symétrique et anti-symétrique on a $-M = {}^tM = M$, donc $2M = 0$ et comme la caractéristique est différente de 2, ceci entraîne que $M = 0$. De plus si M est une matrice quelconque de $\mathcal{M}_n(\mathbb{K})$ alors on voit que ($2 \neq 0$ étant inversible dans $\mathbb{K}$)

$$M = \frac{M + {}^tM}{2} + \frac{M - {}^tM}{2}.$$

Ceci nous donne une décomposition de M comme somme d'un élément de $\mathcal{S}_n$ et d'un élément de $\mathcal{A}_n$. Montrons maintenant la seconde partie de l'énoncé : notons E_{ij} la matrice dont tous les coefficients sont nuls sauf celui situé en ligne i, colonne j, auquel on attribue la valeur 1. On voit aisément que la famille $((E_{ii})_{1\leq i\leq n}, (E_{ij} + E_{ji})_{1\leq i<j\leq n})$ est une base de $\mathcal{S}_n$ et que la famille $(E_{ji} - E_{ij})_{1\leq i<j\leq n}$ est une base de $\mathcal{A}_n$. □

Définition 3.1.10 Soit $\mathbb{K} = \mathbb{C}$ et soit φ est une forme sesquilinéaire, on dit que φ est *à symétrie hermitienne* (ou simplement hermitienne) si pour tout $x, y \in E$, on a

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

Remarque 3.1.11 Si E est de dimension finie, φ est hermitienne si et seulement si sa matrice M associée dans une base est hermitienne, ie vérifie $M^* = M$.

Attention : Si l'on considère l'ensemble des matrices hermitiennes sur le corps $\mathbb{C}$, cet ensemble n'est pas un $\mathbb{C}$-e.v ! (**Exercice**).

3.2 Formes quadratiques, formes hermitiennes

Soit E un $\mathbb{K}$-ev quelconque sur un corps $\mathbb{K}$ de caractéristique différente de 2 (respectivement $\mathbb{K} = \mathbb{C}$).

Définition 3.2.1 On appelle *forme quadratique* (resp. *forme hermitienne*) sur E toute application q de la forme

$$q \ : \ E \to \mathbb{K}, \quad x \mapsto \varphi(x, x)$$

où φ est une forme bilinéaire symétrique (resp. une forme sesquilinéaire à symétrie hermitienne).

Remarque 3.2.2 Bien noter que si $\mathbb{K} = \mathbb{C}$ deux types d'objets existent : les formes quadratiques sur $\mathbb{C}$ d'une part, les formes hermitiennes sur $\mathbb{C}$ d'autre part.

Remarque 3.2.3 Dans le cas hermitien, notons que q est en fait à valeurs dans le sous-corps des réels $\mathbb{R}$ de $\mathbb{C}$. (**Exercice**).

Proposition 3.2.4 *Soit q une forme quadratique (resp. une forme hermitienne) sur E. Il existe une unique forme bilinéaire symétrique (resp. sesquilinéaire à symétrie hermitienne) φ telle que*

$$\forall x \in E, \ q(x) = \varphi(x, x).$$

De plus dans le cas d'une forme quadratique, on a

$$\varphi(x,y) = \frac{1}{2}\left[q(x+y) - q(x) - q(y)\right] = \frac{1}{4}\left[q(x+y) - q(x-y)\right],$$

et dans le cas hermitien, on a,

$$\varphi(x,y) = \frac{1}{4}\left[q(x+y) - q(x-y)\right] + \frac{1}{4i}\left[q(x+iy) - q(x-iy)\right].$$

Démonstration : Dans le cas bilinéaire symétrique : soit f l'application définie par la formule :

$$\forall x, y \in E,\ f(x,y) := \frac{1}{2}\left[q(x+y) - q(x) - q(y)\right].$$

On vérifie immédiatement qu'elle est bilinéaire symétrique et de plus que $f(x,x) = q(x)$. Soit maintenant f une forme bilinéaire symétrique telle que $f(u,u) = q(u)$ pour tout $u \in E$. Alors les formules

$$q(x+y) = f(x+y, x+y) = q(x) + 2f(x,y) + q(y)$$

et

$$q(x-y) = f(x-y, x-y) = q(x) - 2f(x,y) + q(y)$$

nous permettent d'en déduire que

$$f(x,y) = \frac{1}{2}\left[q(x+y) - q(x) - q(y)\right] = \frac{1}{4}\left[q(x+y) - q(x-y)\right],$$

ce qui prouve également l'unicité. La preuve dans le cas hermitien se fait de même. □

Définition 3.2.5 L'application φ obtenue dans la proposition précédente s'appelle la *forme polaire de q*.

Exemple 3.2.6 Soit φ une forme bilinéaire symétrique sur un $\mathbb{K}$-e.v E de dimension finie n, avec $\mathbb{K}$ de caractéristique différente de 2. On suppose donnée une base $(e_1, \ldots, e_n)$ de E. Dans cette base φ est donnée par

$$\varphi(x,y) = \sum_{i,j=1}^{n} a_{ij} x_i y_j \quad \text{avec} \quad a_{ij} := \varphi(e_i, e_j).$$

La forme quadratique q associée à φ est

$$q(x) = \sum_{i=1}^{n} a_{ii} x_i^2 + \sum_{1 \le i < j \le n} (a_{ij} + a_{ji}) x_i x_j.$$

Réciproquement, si $q(x) = \sum_{i=1}^{n} a_{ii} x_i^2 + \sum_{1 \le i < j \le n} a_{ij} x_i x_j$, alors q est une forme quadratique et sa forme polaire est

$$\varphi(x,y) = \sum_{i=1}^{n} a_{ii} x_i y_i + \frac{1}{2} \sum_{1 \le i < j \le n} a_{ij}(x_i y_j + x_j y_i).$$

Dans le cas hermitien sur un $\mathbb{C}$-ev E de dimension n avec la donnée d'une forme sesquilinéaire φ à symétrie hermitienne, on obtient :

$$\varphi(x,y) = \sum_{i,j=1}^{n} a_{ij} \bar{x}_i y_j \quad \text{avec} \quad a_{ij} := \varphi(e_i, e_j) \leftrightarrow q(x) = \sum_{i=1}^{n} a_{ii} |x_i|^2 + \sum_{1 \le i < j \le n} (a_{ij} + a_{ji}) \bar{x}_i x_j.$$

Définition 3.2.7 Soit q une forme quadratique (resp. hermitienne) sur un $\mathbb{K}$ e.v (respectivement un $\mathbb{C}$-e.v) E de dimension finie et soit $\mathcal{B}$ une base de E. On appelle *matrice de* q dans la base $\mathcal{B}$ la matrice de la forme polaire associée à q. De même le *rang de* q est le rang de sa matrice.

Exemple 3.2.8 On se place dans $\mathbb{R}^3$ et on définit la forme quadratique q par

$$\forall u = (x, y, z) \in \mathbb{R}^3, \quad q(u) := 3x^2 + y^2 + 2xy - 3xz.$$

Sa matrice dans la base canonique est $A = \begin{pmatrix} 3 & 1 & -\frac{3}{2} \\ 1 & 1 & 0 \\ -\frac{3}{2} & 0 & 0 \end{pmatrix}$.

Exemple 3.2.9 On se place sur $\mathbb{C}^2$ et on définit

$$\forall u = (x, y) \in \mathbb{C}^2, \quad q(u) = \bar{x}x - 2\bar{y}y + \frac{3}{2}\bar{y}x + \frac{3}{2}y\bar{x}.$$

Alors q est une forme hermitienne de forme polaire

$$\forall (u_1, u_2) = ((x_1, y_1), (x_2, y_2)) \in (\mathbb{C}^2)^2, \quad \varphi(u_1, u_2) = \bar{x}_1 x_1 - 2\bar{y}_1 y_2 + \frac{3}{2}\bar{y}_1 x_2 + \frac{3}{2} y_2 \bar{x}_1,$$

et de matrice $A = \begin{pmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & -2 \end{pmatrix}$. Son rang est 2.

3.3 Orthogonalité

Soit E un $\mathbb{K}$-ev quelconque sur un corps $\mathbb{K}$ de caractéristique différente de 2 (respectivement $\mathbb{K} = \mathbb{C}$ dans le cas hermitien). Soit $x \in E$ un vecteur fixé et soit φ une forme bilinéaire symétrique (respectivement sesquilinéaire à symétrie hermitienne). L'application $\varphi(x, \cdot)$ est une forme linéaire sur E, donc un élément du dual E^*.

On introduit l'application linéaire (respectivement anti-linéaire)

$$\widetilde{\varphi} : E \to E^*, \quad x \mapsto \varphi(x, \cdot).$$

Définition 3.3.1 On dit que φ est *non dégénérée* si l'application $\widetilde{\varphi}$ est injective (en dimension fini, il revient au même de dire que $\widetilde{\varphi}$ est bijective). Le noyau $\operatorname{Ker} \widetilde{\varphi} := \{x \in E \mid \widetilde{\varphi}(x) = 0\}$ de $\widetilde{\varphi}$ s'appelle le *noyau de* φ et le *rang de* φ est par définition celui de $\widetilde{\varphi}$.

Notations : Notons Φ la forme polaire de φ. On notera également par abus dans la suite $\operatorname{Ker}\Phi := \operatorname{Ker}\varphi$.

Définition 3.3.2 On appelle *cône isotrope* de Φ l'ensemble

$$C_\Phi := \{x \in E \mid \Phi(x) = 0\}.$$

On dit que Φ *est définie* si $C_\Phi = \{0\}$. Un vecteur $x \in E$ est dit *isotrope* si $\Phi(x) = 0$ ie si $x \in C_\Phi$.

Remarque 3.3.3 On a $\operatorname{Ker}(\Phi) \subset C_\Phi$, ie si Φ est définie alors φ est non dégénérée. La réciproque est fausse en générale comme le montre facilement l'exemple $\Phi(x, y) = x^2 - y^2$.

Définition 3.3.4 Soient $x, y \in E$. On dit que x *et* y *sont orthogonaux* (pour φ) on note $x \perp y$ si $\varphi(x, y) = 0$. Soit $A \subset E$ un ensemble. On appelle *orthogonal de* A le sev de E, noté $A^\perp$ défini par

$$A^\perp := \{y \in E \mid \forall x \in A,\ \varphi(x, y) = 0\}.$$

Deux sous-ensembles A et B de E sont *orthogonaux* si $\forall (a, b) \in A \times B$, on a $a \perp b$. On note $A \perp B$.

Remarque 3.3.5

1. Notons que A est toujours orthogonal à $A^\perp$ et que dire que x est isotrope équivaut à dire que $x \perp x$.
2. $E^\perp = \mathrm{Ker}(\varphi)$.
3. Si $B = \{\varphi(x, \cdot)\ | x \in A\} \subset E^*$ alors $A^\perp$ est l'orthogonal au sens du dual de B, ie $A^\perp = B^\circ$.

Le dernier point de la remarque précédente nous indique qu'il est naturel de retrouver des propriétés d'orthogonalité djà vues :

Proposition 3.3.6 *Si* $A \subset E$ *alors,*

1. $A^\perp = (\mathrm{Vect}(A))^\perp$.
2. $A \subset A^{\perp\perp}$
3. $A \subset B \subset E \Rightarrow B^\perp \subset A^\perp$.

Démonstration : Les points 1. et 3. ont déjà été prouvé. Montrons le point 2 : soit $x \in A$, on a

$$A^{\perp\perp} = \{z \in E \mid \forall y \in A^\perp,\ \varphi(y, z) = 0\}.$$

Soit $y \in A^\perp$: on a $\varphi(x, y) = 0$, donc $\varphi(y, x)^\sigma = 0$. Or σ est un automorphisme donc $\varphi(y, x) = 0$. □

Proposition 3.3.7 *Supposons que* E *est de dimension finie et notons* A *la matrice de* φ *dans une base* $\mathcal{B}$ *de* E. *On a* $\mathrm{Ker}(\Phi) = \mathrm{Ker}(A)$ *en identifiant* $x \in E$ *avec son vecteur colonne* X *qui le représente dans la base* $\mathcal{B}$.

Démonstration : $x \in \mathrm{Ker}(\varphi)$ ssi $\forall y \in E$ on a $\varphi(x, y) = 0$ ssi $\forall Y,\ X^* A Y = 0$ ssi $X * A = 0$ ssi $(X^* A)^* = 0$ ssi $A^* X = 0$. Or $A = A^*$ d'où la résultat. □

Proposition 3.3.8 *On suppose que* Φ *est non dégénérée et* E *est de dimension finie. Soit* F *un sev de* E. *On a*

$$\dim F + \dim F^\perp = \dim E, \quad \text{et} \quad F = F^{\perp\perp}.$$

Démonstration : L'application $\bar{\varphi}_F : y \in F \mapsto \varphi(\cdot, y)$ est linéaire donc on a $\mathrm{rang}(\bar{\varphi}_F) + \dim \mathrm{Ker}(\bar{\varphi}_F) = \dim F$. Or

$$\mathrm{Ker}\bar{\varphi}_F := \{y \in F \mid \forall x \in E,\ \varphi(x, y) = 0\} = F \cap E^\perp = F \cap \mathrm{Ker}(\varphi).$$

De plus on a vu que

$$(\mathrm{Im}(\bar{\varphi}_F)^\circ = \{y \in E \mid \forall x \in F,\ \varphi(x, y) = 0\} = F^\perp.$$

Or $\dim(\mathrm{Im}\bar{\varphi}_F)^\circ = \dim E - \dim \mathrm{Ker}(\bar{\varphi}_F)$. Donc

$$\dim F^\perp = \dim E - \dim F + \dim(F \cap \mathrm{Ker}(\varphi)). \tag{3.1}$$

Comme φ est non dégénérée on a $\mathrm{Ker}\varphi = 0$ ce qui conclut le premier point de la proposition. Concernant le second point, on sait que $F \subset F^{\perp\perp}$. Raisonnons par dimension : on applique le premier point de la proposition avec F et avec $F^\perp$. Ceci permet de conclure. □

Remarque 3.3.9 L'identité (3.1) reste vraie sans supposer que φ est non dégénérée.

Proposition 3.3.10 *Si E est dimension finie, que Φ est définie et que F est un sev de E alors*

$$F \oplus F^\perp = E.$$

Démonstration : Par dimension il suffit de vérifier que la somme est directe : soit $x \in F \cap F^\perp$, alors $\varphi(x,x) = 0$ donc $x = 0$ car φ est définie. □

3.3.1 Bases orthogonales

Définition 3.3.11 Une base $\mathcal{B}$ de E est dite *orthogonale* (pour φ) si $\forall e, e' \in \mathcal{B}$, on a $\varphi(e,e') = 0$. Une base est dite *orthonormale* si de plus $\forall e \in \mathcal{B}$ on a $\varphi(e,e) = 1$.

Remarque 3.3.12 En dimension finie n une base $\mathcal{B} = (e_1, \ldots, e_n)$ est orthogonale si et seulement si

$$\begin{aligned} & \forall \lambda_i \in \mathbb{K}, \quad \Phi\left(\sum_{i=1}^n \lambda_i e_i\right) = \sum_{i=1}^n \lambda_i \lambda_i^\sigma \Phi(e_i) \\ \iff \quad & [\mathrm{Mat}(\Phi)]_{\mathcal{B}} = \mathrm{diag}(\Phi(e_1, \ldots, \Phi(e_n)) \\ \iff \quad & [\mathrm{Mat}(\Phi)]_{\mathcal{B}} \text{ est diagonale.} \end{aligned}$$

On se place désormais dans toute la suite de ce paragraphe en dimension finie : $\dim E = n < +\infty$

Théorème 3.3.13 *Si E est de dimension finie alors il existe une base Φ-orthogonale pour E.*

Démonstration : Par récurrence sur la dimension n de E : le rsultat est évident en dimension 1, supposons le vrai en dimension $n-1$. Soit E de dimension n. Si φ est la forme nulle alors toute base est orthogonale. Sinon il existe $x \in E$ tel que $\Phi(x) \neq 0$. Posons $f : E \to \mathbb{K}$ la forme linéaire définie par $f(v) := \varphi(x,v)$. Ce n'est pas la forme linéaire nulle car $f(x) = \Phi(x) \neq 0$. Son noyau est donc un hyperplan H de supplémentaire dans E la droite engendrée par x. Par hypothèse de récurrence (sur l'espace H), il existe une base $(e_2, \ldots, e_n)$ Φ-orthogonale de H. De plus par construction on a $f(x, e_i) = 0$ pour $i \geq 2$. En posant $e_1 := x$ on conclute. □

Corollaire 3.3.14 *Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que $A = A^*$. Il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que P^*AP est diagonale.*

Démonstration : L'application $\Phi : \mathbb{K}^n \to \mathbb{K}$, $X \mapsto X^*AX$ est une forme quadratique (respectivement hermitienne) de forme polaire $\varphi :\ (X,Y) \mapsto X^*AY$. Par le théorème il existe une base Φ-orthogonale : $\mathcal{B}$. En notant P la matrice de changement de la base canonique à la base $\mathcal{B}$ on obtient que P^*AP est diagonale. □

1. Soit q une forme quadratique sur E de dimension n. Dans une base orthogonale, on a (en posant $x = \sum_{i=1}^n s_i e_i$ la décomposition dans cette base) :

$$q(x) = \sum_{i=1}^n a_i x_i^2 \quad \text{où} \quad a_i := q(e_i) \in \mathbb{K}.$$

2. Soit h une forme hermitienne sur un $\mathbb{C}$-ev E de dimension n. Dans une base orthogonale, on a (en posant $x = \sum_{i=1}^n s_i e_i$ la décomposition dans cette base) :

$$h(x) = \sum_{i=1}^n a_i x_i \bar{x}_i \quad \text{où} \quad a_i := h(e_i) \in \mathbb{R}.$$

On voit donc que si λ_i est un scalaire non nul, en remplaçant e_i par $\frac{e_i}{\lambda_i}$ dans la base $\mathcal{B}$ on obtient une nouvelle base $\mathcal{B}'$ orthogonale et telle que

$$x = \sum_{i=1}^n x_i \frac{e_i}{\lambda_i}, \text{ donc } \quad q(x) = \sum_{i=1}^n \frac{a_i}{\lambda_i^2} x_i^2 \text{ dans le cas quadratique}$$

et

$$x = \sum_{i=1}^n x_i \frac{e_i}{\lambda_i}, \text{ donc } \quad h(x) = \sum_{i=1}^n \frac{a_i}{|\lambda_i|^2} |x_i|^2 \text{ dans le cas hermitien.}$$

Conclusion : Dans la base orthogonale $\mathcal{B}$, remplacer e_i par $\frac{e_i}{\lambda_i}$ change le coefficient a_i en $\frac{a_i}{\lambda_i^2}$ dans le cas quadratique et en $\frac{a_i}{|\lambda_i|^2}$ dans le cas hermitien.

Corollaire 3.3.15 *Si $\mathbb{K} = \mathbb{C}$ et $\varphi : E \times E \to \mathbb{C}$ est bilinéaire symétrique avec E de dimension n. Alors il existe une base $\mathcal{B}$ telle que dans cette base la matrice de φ est $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ et dans cette base la forme quadratique correspondante q s'écrit $q(x) = \sum_{i=1}^r x_i^2$.*

Démonstration : On prend la base $\mathcal{B}$ donnée par le théorème 3.3.13. Quitte à permuter les coordonnées on peut supposer que les r premières valeurs $q(e_i)$ sont non nulles et les suivantes sont nulles (pour un certain entier r). Quand $q(e_i) \neq 0$ on remplace e_i par $\frac{e_i}{\lambda_i}$ où $\lambda_i \in \mathbb{C}$ est tel que $\lambda_i^2 = q(e_i)$. Un tel λ_i existe toujours dans $\mathbb{C}$. La nouvelle base donne la résultat. □

Corollaire 3.3.16 *Si $\mathbb{K} = \mathbb{R}$ et $\varphi : E \times E \to \mathbb{R}$ est bilinéaire symétrique avec $\dim E = n$. Il existe une base $\mathcal{B}$ de E telle que la matrice de φ dans cette base est $\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et dans cette base la forme quadratique correspondante q s'écrit $q(x) = \sum_{i=1}^p x_i^2 - \sum_{i=p+1}^{p+q} x_i^2$.*

Démonstration : C'est la même preuve que pour le corollaire précédent à ceci prêt que sur $\mathcal{R}$ on ne peut pas toujours résoudre l'équation $\lambda_i^2 = q(e_i)$. Si $q(e_i) > 0$ on fait comme avant, et si $q(e_i) < 0$ on trouve λ_i tel que $\lambda_i^2 = -q(e_i)$. On ordonne ensuite les e_i de sote que pour les p première valeurs $q(e_i) > 0$, que pour les q suivantes $q(e_i) < 0$ et les $n - (p + q)$ dernières sont telles que $q(e_i) = 0$. Dans la nouvelle base on a alors l'écriture attendue. □

Corollaire 3.3.17 *L'énoncé précédent reste valable sur $\mathbb{K} = \mathbb{C}$ en partant cette fois d'une matrice hermitienne. La forme associée h sécrit alors, dans une base convenable,*

$$h(x) = \sum_{i=1}^{p} |x_i|^2 - \sum_{i=p+1}^{p+q} |x_i|^2.$$

Démonstration : Même preuve que précdemment en résolvant cette fois sur $\mathbb{C}$ l'équation $|\lambda_i|^2 = \pm h(e_i)$. □

Définition 3.3.18 Les corollaires 3.3.16 et 3.3.17 s'appelle *la loi d'inertie de Sylvester* et le couple (p, q) obtenu s'appelle *la signature* (de φ).

Proposition 3.3.19 *Dans les deux corollaires précédents, le couple (p, q) ne dépend pas du choix d'une base de E dans laquelle on a l'écriture annoncée. De plus $p + q = \mathrm{rg}(\varphi)$.*

Démonstration : Le second point est clair sur l'expression matricielle dans la base donnée par les corollaires 3.3.16 et 3.3.17. Pour le premier point : soient $(e_1, \ldots, e_n)$ une base telle que la matrice de φ dans cette base est $(I_p, -I_q, 0_{n-(p+q)})$ et soit $(f_1, \ldots, f_n)$ une base dans laquelle la matrice de φ est $(I_{p'}, I_{q'}, 0_{n-(p'+q')})$. Comme $p+q = \mathrm{rg}(\varphi) = p'+q'$ il nous suffit de prouver que $p = p'$ pour conclure. De plus par symétrie des rôles, il suffit en fait de montrer que $p \leq p'$ (le même raisonnement en échangeant les rôles de p et de p' prouverat l'inégalité réciproque). Soit donc $x \in \mathrm{Vect}(e_1, \ldots, e_p) - \{0\}$, on a $\varphi(x, x) = \sum_{i=1}^{p} |x_i|^2 > 0$. De même si $x \in \mathrm{Vect}(f_{p'+1}, \ldots, f_n)$, on a $\varphi(x, x) = -\sum_{i=p'+1}^{n} |x_i|^2 \leq 0$. Notamment on en déduit que $\mathrm{Vect}(e_1, \ldots, e_p) \cap \mathrm{Vect}(f_{p'+1}, \ldots, f_n) = \{0\}$. Ainsi la somme des dimension de ces deux espaces est inférieures à n, donc $p + (n - p') \leq n$ ie $p \leq p'$. □

3.3.2 Réduction de Gauss des formes quadratiques et des formes hermitiennes

Soit K un corps de caractéristique différente de 2. On travaille sur l'espace $E = \mathbb{K}^n$ avec une forme quadratique

$$q(x) = q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{ii} x_i^2 + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j.$$

On sait qu'il existe une base $(e_1, \ldots, e_n)$ orthogonale pour q. Posons $\alpha_i := q(e_i)$. On a

$$\forall x \in E,\ q(x) = q\left(\sum_{i=1}^{n} e_i^*(x) e_i\right) = \sum_{i=1}^{n} \alpha_i (e_i^*(x))^2.$$

On a ainsi écrit q comme une combinaison linéaire de carrés de formes linéaires, linéairement indépendantes. La méthode de Gauss permet d'obtenir une telle base e_i explicite. Deux cas se présentent :

1. si $\exists i$ tel que $a_{ii} \neq 0$. Quitte à renuméroter on peut supposer que $a := a_{11} \neq 0$. Dans ce cas, on écrit :

$$q(x_1, \ldots, x_n) = a x_1^2 + x_1 B(x_2, \ldots, x_n) + C(x_2, \ldots, x_n),$$

où B est une forme linéaire en $(x_2, \ldots, x_n)$ et C est quadratique en $(x_2, \ldots, x_n)$. Ceci nous permet de réécrire

$$q(x) = a\left(x_1 + \frac{B}{2a}\right)^2 + \left(C - \frac{B^2}{4a^2}\right).$$

Le terme $\left(x_1 + \frac{B}{2a}\right)^2$ est le carré d'une forme linéaire et le second terme est une forme quadratique en $(x_2, \ldots, x_n)$. Par récurrence, ce second terme se décompose en somme de carrés de formes linéaires en $(x_2, \ldots, x_n)$ linéairement indépendantes. Comme x_1 n'intervient pas dans ces formes linéaires, la famille obtenue en ajoutant $\left(x_1 + \frac{B}{2a}\right)$ reste linéairement inépendante.

2. Si $\forall i$, $a_{ii} = 0$ soit q est la forme nulle auquel cas le résultat est trivial, soit $\exists i < j$ tel que $a_{ij} \neq 0$. Quitte à renuméroter on peut supposer que $a := a_{12} \neq 0$. Dans ce cas, on écrit
$$q(x) = ax_1x_2 + x_1B(x_3, \ldots, x_n) + x_2C(x_3, \ldots, x_n) + D(x_3, \ldots, x_n)$$
où B et C sont des formes linéaires et D est quadratique en $(x_3, \ldots, x_n)$. On obtient ainsi
$$\begin{aligned} q(x) &= a\left(x_1 + \frac{C}{a}\right)\left(x_2 + \frac{B}{a}\right) + \left(D - \frac{BC}{a}\right) \\ &= \frac{a}{4}\left[\left(x_1 + x_2 + \frac{B+C}{a}\right)^2 - \left(x_1 - x_2 + \frac{C-B}{a}\right)^2\right] + \left(D - \frac{BC}{4}\right). \end{aligned}$$
Les deux premiers termes sont des carrés de formes linéaires. Notons L_1 la première forme linéaire, L_2 la seconde. Le troisième terme est une forme quadratique en $(x_3, \ldots, x_n)$. Par récurrence ce terme se décompose en somme de carrés de formes linéaires $L_3, \ldots, L_r$ en $(x_3, \ldots, x_n)$ linéairement indépendantes. Montrons que la famille $L_1, \ldots, L_r$ est linéairement indépendante : soit $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ tels que $\sum_{i=1}^r \lambda_i L_i = 0$. On évalue cette identité en $(x_1, x_2, 0, \ldots, 0)$ et on obtient :
$$\lambda_1(x_1 + x_2) + \lambda_2(x_1 - x_2) = 0.$$
En prenant $(x_1, x_2) = (1, 1)$ on en déduit que $\lambda_1 = 0$ puis en prenant $(x_1, x_2) = (1, 0)$ on en déduit ensuite que $\lambda_2 = 0$. On obient finalement une combinaison linéaire ne faisant intervenir que $L_3, \ldots, L_r$. Mais ces formes sont linéairement indépendantes, donc $\lambda_3 = \ldots = \lambda_r = 0$.

Ceci conclut la réduction de Gauss dans le cas quadratique.

Remarque 3.3.20 Nous avons traité ici uniquement le cas d'une forme quadratique sur un corps $\mathbb{K}$ de caractérsitique différente de 2. De fait le même résultat reste vrai pour des formes hermitiennes sur $\mathbb{C}$ en remplaçant partout $(\cdot)^2$ par $|\cdot|^2$.

Exemple 3.3.21 Si l'on part de $h(x, y) = x\bar{y} - \bar{x}y$. La réduction de Gauss nous donne $h(x, y) = \frac{1}{2}\left(|x + y|^2 - |x - y|^2\right)$ qui est donc une forme de signature $(1, 1)$.

Écrivons explicitement ce qu'il se passe pour les formes hermitiennes :
On travaille sur l'espace $E = \mathbb{C}^n$ avec une forme hermitiene
$$q(x) = q(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} h_{ii} x_i \bar{x}_j.$$
On a de plus pour tout i, j, $h_{ij} = \bar{h}_{ji}$, notamment les h_{ii} sont réels. Deux cas se présentent :

1. si $\exists i$ tel que $h_{ii} \neq 0$. Quitte à renuméroter on peut supposer que $h := h_{11} \neq 0$. Dans ce cas, on écrit :

$$q(x_1, \ldots, x_n) = h|x_1|^2 + \bar{x}_1 B(x_2, \ldots, x_n) + x_1 \bar{B}(x_2, \ldots, x_n) + C(x_2, \ldots, x_n),$$

où B est une forme linéaire en $(x_2, \ldots, x_n)$ et C est hermitienne en $(x_2, \ldots, x_n)$. Ceci nous permet de réécrire

$$q(x) = h\left|x_1 + \frac{B}{h}\right|^2 + \left(C - \frac{|B|^2}{h^2}\right).$$

Le terme $\left|x_1 + \frac{B}{h}\right|^2$ est le carré du module d'une forme linéaire et le second terme est une forme hermitienne en $(x_2, \ldots, x_n)$. Par récurrence, ce second terme se décompose en somme de carrés de module formes linéaires en $(x_2, \ldots, x_n)$ linéairement indépendantes. Comme x_1 n'intervient pas dans ces formes linéaires, la famille obtenue en ajoutant $\left(x_1 + \frac{B}{h}\right)$ reste linéairement inépendante.

2. Si $\forall i$, $h_{ii} = 0$ soit q est la forme nulle auquel cas le résultat est trivial, soit $\exists i < j$ tel que $h_{ij} \neq 0$. Quitte à renuméroter on peut supposer que $h := h_{12} \neq 0$. Dans ce cas, on écrit

$$q(x) = h\bar{x}_1 x_2 + \bar{h} x_1 \bar{x}_2 + x_1 B + \bar{x}_1 \bar{B} + x_2 C + \bar{x}_2 \bar{C} + D$$

où B et C sont des formes linéaires et D est hermitienne en $(x_3, \ldots, x_n)$. On obtient ainsi

$$q(x) \quad = \quad \left(x_1 + \frac{\bar{C}}{\bar{h}}\right)\left(\bar{h}\bar{x}_2 + B\right) + \left(\bar{x}_1 + \frac{C}{h}\right)\left(hx_2 + \bar{B}\right) + \left(D - \frac{B\bar{C}}{\bar{h}} - \frac{\bar{B}C}{h}\right).$$

On utilise alors, comme déjà indiqué, l'identité suivante :

$$x\bar{y} - \bar{x}y = \frac{1}{2}\left(|x + y|^2 - |x - y|^2\right).$$

Ceci nous permet d'en déduire :

$$q(x) = \frac{1}{2}\left[\left|x_1 + hx_2 + \bar{B} + \frac{\bar{C}}{\bar{h}}\right|^2 - \left|x_1 - hx_2 + \bar{B} - \frac{\bar{C}}{\bar{h}}\right|^2\right] + \left(D - \frac{B\bar{C}}{\bar{h}} - \frac{\bar{B}C}{h}\right).$$

Les deux premiers termes sont des carrés de modules de formes linéaires. Notons L_1 la première forme linéaire, L_2 la seconde. Le troisième terme est une forme hermitienne en $(x_3, \ldots, x_n)$. Par récurrence ce terme se décompose en somme de carrés de formes linéaires $L_3, \ldots, L_r$ en $(x_3, \ldots, x_n)$ linéairement indépendantes. Montrons que la famille $L_1, \ldots, L_r$ est linéairement indépendante : soit $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ tels que $\sum_{i=1}^{r} \lambda_i L_i = 0$. On évalue cette identité en $(x_1, x_2, 0, \ldots, 0)$ et on obtient :

$$\lambda_1(x_1 + hx_2) + \lambda_2(x_1 - hx_2) = 0.$$

En prenant $(x_1, x_2) = (1, 1)$ on en déduit que $\lambda_1 = 0$ puis en prenant $(x_1, x_2) = (1, 0)$ on en déduit ensuite que $\lambda_2 = 0$. On obient finalement une combinaison linéaire ne faisant intervenir que $L_3, \ldots, L_r$. Mais ces formes sont linéairement indépendantes, donc $\lambda_3 = \ldots = \lambda_r = 0$.

Ceci conclut la réduction de Gauss dans le cas quadratique.

Chapitre 4

Espaces préhilbertiens

Dans tout ce chapitre, on travaille soit avec le corps $\mathbb{K} = \mathbb{R}$, soit avec $\mathbb{K} = \mathbb{C}$ et Φ est une forme quadratique sur un $\mathbb{R}$-ev E (respectivement hermitienne sur un $\mathbb{C}$-ev E), de forme polaire φ.

4.1 Formes Positives

Définition 4.1.1 La forme Φ est *positive* si $\forall x \in E$, $\Phi(x) \geq 0$.

Remarque 4.1.2 En dimension finie, la signature d'une forme positive est de la forme $(\star, 0)$.

Théorème 4.1.3 ***(Cauchy-Schwarz)*** *Si Φ est positive, alors*

$$\forall x, y \in E, \quad |\varphi(x,y)|^2 \leq \Phi(x)\Phi(y).$$

De plus, si Φ est définie, on a égalité si et seulement si (x, y) est une famille liée.

Démonstration : Soient $x, y \in E$ et soit $\theta \in \mathbb{R}$. Si $\mathbb{K} = \mathbb{R}$ alors $\varphi(x,y) \in \mathbb{R}$. Si $\mathbb{K} = \mathbb{C}$ alors $\varphi(e^{i\theta}x, y) = e^{i\theta}\varphi(x,y)$. On choisit θ tel que $\varphi(e^{i\theta}x, y) \in \mathbb{R}$ et on travaille avec $e^{i\theta}x$ au lieu de x :

$$|\varphi(x,y)| = |\varphi(e^{i\theta}x, y)| \quad \text{et} \quad \Phi(x) = \Phi(e^{i\theta}x).$$

Ainsi on ne change rien à ce que l'on veut prouver en remplaçant x par $e^{i\theta}x$. On suppose donc désormais que $\varphi(x,y) \in \mathbb{R}$. Comme Φ est positive, on a

$$\forall \lambda \in \mathbb{R}, \ \Phi(\lambda x + y) = \lambda^2\Phi(x) + 2\lambda\varphi(x,y) + \Phi(y) \geq 0.$$

1. Si $\Phi(x) = 0$: alors pour tout $\lambda \in \mathbb{R}$ on a $2\lambda\varphi(x,y) + \Phi(y) \geq 0$ donc $\varphi(x,y) = 0$ et l'inégalité voulue est prouvée.
2. Sinon on a un trinôme du second degré, de discriminant

$$\Delta_{x,y} = 4\varphi(x,y)^2 - 4\Phi(x)\Phi(y)$$

qui doit être ≤ 0 d'où le résultat.

Si de plus Φ est définie et $x \neq 0$ alors $\Phi(x) \neq 0$ donc on voit que l'on a égalité si et seulement si $\Delta_{x,y} = 0$ ie si et seulement si il existe λ_0 tel que $\Phi(\lambda_0 x + y) = 0$ ie $\lambda_0 x + y = 0$ car Φ est définie. □

Corollaire 4.1.4 *Si Φ est positive alors $C_\Phi = \mathrm{Ker}(\Phi)$.*

Démonstration : Immédiat. □

Corollaire 4.1.5 ***(Minkowski)*** *Si Φ est positive, alors*

$$\forall x, y \in E, \quad \Phi(x+y)^{\frac{1}{2}} \leq \Phi(x)^{\frac{1}{2}} + \Phi(y)^{\frac{1}{2}}.$$

Démonstration : On traite les cas réel et complexe simultanément : soit $x, y \in E$, on a,

$$\begin{aligned} \Phi(x+y) &= \Phi(x) + \Phi(y) + \varphi(x,y) + \overline{\varphi(y,x)} \\ &= \Phi(x) + \Phi(y) + 2\mathrm{Re}(\varphi(x,y)) \\ &\leq \Phi(x) + \Phi(y) + 2|\varphi(x,y)| \\ &\leq \Phi(x) + \Phi(y) + 2\Phi(x)^{\frac{1}{2}}\Phi(y)^{\frac{1}{2}} \\ &= (\Phi(x)^{\frac{1}{2}} + \Phi(y)^{\frac{1}{2}})^2. \end{aligned}$$

Les nombres étant tous positifs, on conclut en prenant la racine carrée. □

4.2 Espaces préhilbertiens

On suppose désormais dans toute la suite du chapitre que la forme Φ est définie positive.

Définition 4.2.1 Soit $x \in E$. On pose $\|x\| := \Phi(x)^{\frac{1}{2}}$ et on dit que la forme polaire φ est un *produit scalaire* sur E. On le note $\langle x, y\rangle := \varphi(x,y)$. Par ailleurs on rapelle la définition d'une *norme sur le $\mathbb{K}$-ev E, euclidienne pour $\mathbb{K} = \mathbb{R}$*, respectivement *hermitienne pour $\mathbb{K} = \mathbb{C}$* : c'est une application $N : E \to \mathbb{R}^+$ telle que

1. $\forall x \in E$, $N(x) = 0 \iff x = 0$.
2. $\forall x \in E, \forall \lambda \in \mathbb{K}$, $N(\lambda x) = |\lambda| N(x)$.
3. $\forall x, y \in E$, $N(x+y) \leq N(x) + N(y)$.

Proposition 4.2.2 *L'application $\|\cdot\|$ précédemment définie est une norme.*

Démonstration : La forme étant définie positive, seul le dernier point reste à prouver : il s'agit de l'inégalité de Minkowski (corollaire 4.1.5). □

Définition 4.2.3 Si $\mathbb{K} = \mathbb{R}$ on dit que E est *préhilbertien* (respectivement *préhilbertien complexe* si $\mathbb{K} = \mathbb{C}$). Si de plus E est de dimension finie, on dit que E est *euclidien* (respectivement *hermitien*).

4.3 Orthogonalité

Rappel : $x \perp y \overset{\text{def}}{\iff} \langle x, y\rangle = 0$. De plus on dit qu'une famille d'éléments $(e_i)_{i\in I}$ de E est *orthogonale* si

$$\forall i \neq j, \quad \langle e_i, e_j\rangle = 0.$$

Notons qu'une telle famille est automatiquement libre.

Définition 4.3.1 Si une famille $(e_i)_{i\in I}$ d'éléments de E est orthogonale et telle que $\forall i \in I$, $\|e_i\| = 1$, on dit que la famille est *orhonormale*.

Soit $(e_1, \dots, e_n)$ une base orthogonale de E euclidien (respectivement hermitien) de dimension $n \leq +\infty$. Si, $x, y \in E$ on les décompose dans la base $(e_1, \dots, e_n)$ sous la forme

$$x = \sum_{i=1}^{n} x_i e_i, \quad \text{et} \quad y = \sum_{i=1}^{n} y_i e_i.$$

On a

$$\forall i, x_i = \langle e_i, x\rangle, \quad \text{et} \quad \langle x, y\rangle = \sum_{i=1}^{n} \bar{x}_i y_i.$$

Proposition 4.3.2 ***(Pythagore)*** *Si $(e_i)_{i\in I}$ est une famille finie orthogonale dans E, on a*

$$\left\| \sum_{i\in I} e_i \right\|^2 = \sum_{i\in I} \|e_i\|^2.$$

Démonstration : C'est un simple calcul :

$$\left\| \sum_{i\in I} e_i \right\|^2 = \langle \sum_i e_i, \sum_j e_j \rangle = \sum_{i,j} \langle e_i, e_j \rangle = \sum_{i\in I} \|e_i\|^2. \square$$

Théorème 4.3.3 ***(du parallélogramme)*** *Pour tout $x, y \in E$ préhilbertien (réel ou complexe), on a*

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2).$$

Démonstration : Immédiat. $\square$

4.4 Orthonormalisation de Gram-Schmidt

Théorème 4.4.1 ***(Gram-Schmidt)*** *Soit $(e_1, \dots, e_N)$ une famille libre de E préhilbertien (réel ou complexe). Il existe une famille $(\varepsilon_1, \dots, \varepsilon_N)$ orthonormée de E telle que*

$$\forall k \in \{1, \dots, N\}, \quad \text{Vect}(\varepsilon_1, \dots, \varepsilon_k) = \text{Vect}(e_1, \dots, e_k).$$

Démonstration : Il suffit de construire une famille de vecteurs $(v_1, \dots, v_n)$ orthogonale vérifiant $\text{Vect}(v_1, \dots, v_k) = \text{Vect}(e_1, \dots, e_k)$ pour tout k. On en déduit ensuite la famille voulue en posant pour tout i, $\varepsilon_i = v_i/\|v_i\|$. On construit la famille v_i par récurrence :

Le vecteur $v_1 = e_1$ convient.

Si on suppose $(v_1, \dots, v_{k-1})$ construit, on cherche v_k sous la forme

$$v_k = e_k + \lambda_{1,k} v_1 + \cdots + \lambda_{k-1,k} v_{k-1}.$$

On veut pour tout $i \leq k-1$ avoir $\langle v_i, v_k\rangle = 0$, ie

$$\forall i \leq k-1, \quad \langle v_i, e_k\rangle + \lambda_{i,k} = 0.$$

On voit que en posant $\lambda_{i,k} := \langle v_i, e_k \rangle$ on obtient un vecteur v_k comme voulu à savoir :

$$v_1 = e_1 \text{ et pour tout } k,\ v_k := e_k - \sum_{i=1}^{k-1} \langle v_i, e_k \rangle v_i.$$

Ceci donne une formule de récurrence explicite qui permet de conclure. □

Rappelons que si E est euclidien ou hermitien et si F est un sous-ev de E on sait que $E = F \oplus F^\perp$. Ainsi pour tout $x \in E$, il existe un unique couple $(x_F, x_{F^{bot}})$ tel que $x = x_F + x_{F^\perp}$.

Définition 4.4.2 L'application $p_F : E \to F,\ x \mapsto x_F$ s'appelle la *projection orthogonale sur* F (parallèlement à $F^\perp$).

Proposition 4.4.3 *Soient E euclidien ou hermitien, F est un sous-ev de E, p_F la projection orthogonale sur F et $x \in E$. En posant $d(x, F) := \inf_{y \in F} \|x - y\|$, on a*

$$d(x, F) = \|x - p_F(x)\|.$$

Démonstration : Soit $y \in F$. On a $x - y = x - p_F(x) + p_F(x) - y$. Or $x - p_F(x) \in F$ et $p_F(x) - y \in F$, donc par Pythagore, on a

$$\|x - y\|^2 = \|x - p_F(x)\|^2 + \|p_F(x) - y\|^2.$$

On voit ainsi que l'inf est visiblement atteint pour $y = p_F(x)$. □

4.5 Isométries, endomorphismes unitaires

Définition 4.5.1 Soit E euclidien ou hermitien et soit $f \in \mathrm{End}(E)$ telle que

$$\forall x \in E,\ \|f(x)\| = \|x\|.$$

1. Si E est euclidien, on dit que f est une *isométrie* (ou un *endomorphisme orthogonal*) ;
2. Si E est hermitien, on dit que f est un *endomorphisme unitaire*.

Remarque 4.5.2 Si f est orthogonal ou unitaire, alors f est injective donc bijective (on est en dimension finie).

Proposition 4.5.3 *Soit $f \in \mathrm{End}(E)$. Alors f est orthogonale (respectivement unitaire) si et seulement si*

$$\forall x, y \in E,\quad \langle f(x), f(y) \rangle = \langle x, y \rangle.$$

Démonstration : La formule entraîne immédiatement le caractère orthogonal (respectivement unitaire) de f en prenant $x = y$. Réciproquement, prouvons le cas hermitien (le cas euclidien se prouve de la même façon) : soit $a, b \in E$ on a

$$\langle a, b \rangle = \frac{1}{4} \left(\|a + b\|^2 - \|a - b\|^2 + i\|a - ib\|^2 - i\|a + ib\|^2 \right).$$

On applique ceci avec $a = \varphi(x)$ et $b = \varphi(y)$ et, en utilisant à chaque fois que $\|\varphi(u)\| = \|u\|$, un calcul direct permet de conclure. □

Proposition 4.5.4 *L'ensemble des endomorphismes orthogonaux sur E euclidien est un sous-groupe, noté $O(E)$ du groupe des automorphismes* $\mathrm{GL}(E)$ *de E. De même, l'ensemble des endomorphismes unitaires sur E hermitien est un sous-groupe, noté $U(E)$ du groupe des automorphismes* $\mathrm{GL}(E)$ *de E.*

Démonstration : Si f est orthogonal (respectivement unitaire) alors on a vu que f est bijective, donc appartient à $\mathrm{GL}(E)$. Si f et g sont orthogonaux (respectivement unitaires), on a

$$\forall x \in E, \quad \|fg(x)\| = \|g(x)\| = \|x\|$$

donc fg est encore orthogonal (respectivement unitaire). De plus l'identité est trivialement orthogonale (respectivement unitaire). Soit donc f orthogonal (respectivement unitaire) et notons f^{-1} son automorphisme réciproque. Soit $y \in E$. Il existe un unique $x \in E$ tel que $y = f(x)$ et on a

$$\|f^{-1}(y)\| = \|f^{-1}(f(x))\| = \|x\| = \|f(x)\| = \|y\|.$$

Donc f^{-1} est orthogonal (respectivement unitaire) ce qui permet de conclure. □

4.6 Propriétés matricielles

Proposition 4.6.1 *Soit E euclidien (respectivement hermitien) et soit $f \in \mathrm{End}(E)$. Alors f est une isométrie (respectivement un endomorphisme unitaire) si et seulement si l'image d'une base orthonormale de E par f est une base orthonormale de E.*

Démonstration : Si $(e_i)_{1\leq i\leq n}$ est une base orthonormale, alors on a

$$\forall i \neq j, \quad \langle f(e_i), f(e_j)\rangle = \langle e_i, e_j\rangle = \delta_{ij}.$$

Réciproquement, soient $x \in E$, et $(e_i)_{1\leq i\leq n}$ une base orthonormale telle que $(f(e_i))_{1\leq i\leq n}$ est orthonormale. En décomposant x dans la base e_i et en appliquant Pythagore, on vérifie immédiatement que $\|f(x)\| = \|x\|$. □

Applications : Soit B une base orthonormale de E et soit $f \in \mathrm{End}(E)$ unn endomorphisme orthogonal (respectivement unitaire). Notons A la matrice de f dans la base B. On a

$$A^*A = AA^* = I_n.$$

On voit notamment que cette égalité implique $|\det(f)| = 1$.

Définition 4.6.2 On note $O_n(\mathbb{R})$ l'ensemble $\{A \in M_n(\mathbb{R}) \mid {}^tAA = I_n\}$. C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ que l'on appelle *groupe orthogonal*. Le sous groupe $SO_n(\mathbb{R})$ de $O_n(\mathcal{R})$ constitué des matrices de déterminant 1 est appelé le *groupe spécial orthogonal*. De manière analogue, on note $U_n(\mathbb{C})$ l'ensemble $\{A \in M_n(\mathbb{C}) \mid A^*A = I_n\}$. C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ que l'on appelle *groupe unitaire*.

4.7 Endomorphismes adjoints

4.7.1 Définition

Définition 4.7.1 Soit E préhilbertien réel ou complexe. Soient $f, g \in \mathrm{End}(E)$. On dit que f et g sont *adjoints* si

$$\forall x, y \in E, \quad \langle f(x), y\rangle = \langle x, g(y)\rangle.$$

Remarque 4.7.2 Une fois fixé f, il existe au plus un endomorphisme g vérifiant la condition précédente.

Définition 4.7.3 Soit $f \in \mathrm{End}(E)$. S'il existe g comme précédemment, g est appelé *l'adjoint de* f. On le note f^*. Si de plus on a $f = f^*$, on dit que f est *autoadjoint*.

Remarque 4.7.4 Si f^* existe, on vérifie immédiatement que $(f^*)^* := f^{**}$ existe et vaut $f^{**} = f$.

4.7.2 Interprétation matricielle en dimension finie

On suppose désormais que E est de dimension finie et euclidien ou hermitien. Soit B une base orhonormée de E et soit $f \in \mathrm{End}(E)$. On note M la matrice de f dans la base B.

Problème : On cherche un $g \in \mathrm{End}(E)$ qui est l'adjoint de f.

Soit donc g un endomorphisme de E et notons N sa matrice dans la base B. On voit que

$$g \text{ est l'adjoint de } f \iff (\forall X, Y,\ \ (MX)^*Y = X^*(NY)) \iff (\forall X, Y\ \ X^*M^*Y = X^*NY)\,.$$

Ainsi g est l'adjoint de f si et seulement leurs matrices dans une base orthonormée vérifient $M^* = N$. Conlusion : nous venons de prouver la proposition suivante :

Proposition 4.7.5 *Si E et euclidien ou hermitien, si $f \in \mathrm{End}(E)$ alors f^* existe ; et si B est une base orthonormée de E on a $[f^*]_B = ([f]_B)^*$.*

Remarque 4.7.6 Si E est euclidien, on voit que f est autoadjoint si et seulement si sa matrice M dans une base orthonormée est symétrique ie vérifie ${}^tM = M$. Si E est hermitien, on voit que f et autoadjoint si et seulement si sa matrice dan sune base orthonormée est hermitienne ie vérifie $M^* = M$.

4.7.3 Réduction des endomorphismes auto-adjoints

Lemme 4.7.7 *Soit E euclidient ou hermitien et soit $f \in \mathrm{End}(E)$ autoadjoint. Si F est un s.e.v de E stable par f, alors $F^\perp$ est stable par f.*

Démonstration : Soit $x \in F^\perp$ on veut montrer que $f(x) \in F^\perp$ ie que pour tout $y \in F$, on a $\langle f(x), y\rangle = 0$. Or on a $\langle f(x), y\rangle = \langle x, f(y)\rangle$. Mais y est dans F et F est stable par f donc $f(y)$ est dans F donc $x \perp f(y)$, ce qui permet de conclure. □

Théorème 4.7.8 *Soit E euclidien (respectivement hermitien) et soit $f \in \mathrm{End}(E)$ autoadjoint. Il existe une base orthonormée dans laquelle la matrice de f est diagonale et de plus ses coefficients diagonaux sont tous réels.*

Démonstration : Par récurrence sur la dimension $n \geq 1$ de E. Si $n = 1$ c'est évident. Supposons le résultat vrai jusqu'au rang $n-1$ et prouvons le au rang n. On introduit la forme quadratique (respectivement hermitienne) $\Phi : E \to \mathbb{R}$, $x \mapsto \langle x, f(x)\rangle$. Sa forme polaire est $\varphi(x, y) = \langle x, f(y)\rangle$. On travaille en dimension finie, donc la sphère unitée $S := \{x \in E \mid \|x\| = 1\}$ est compacte et l'application Φ est continue. Donc il existe $x_0 \in S$ tel que $\Phi(x_0) = \sup_{x\in S} \Phi(x) =: \lambda$.

Introduisons par ailleurs la forme quadratique (respectivement hermitienne) $\Phi_1(x) := \lambda\|x\|^2 - \Phi(x)$. Par définition de λ, la forme Φ_1 est positive et comme $\Phi_1(x_0) = 0$ on voit qu'elle n'est pas définie. Elle est donc dégénérée par le corollaire 4.1.4. Ainsi, (la forme polaire de Φ_1 étant $\varphi_1(x,y) = \langle x, g(y)\rangle$ avec $g = \lambda\mathrm{Id} - f$), on voit qu'il existe $x \neq 0$ tel que

$$\forall y \in E, \quad \varphi_1(x,y) = 0 = \langle x, g(y)\rangle.$$

En particulier ceci prouve que g n'est pas surjective (car x n'est pas atteint) donc n'est pas injective (par le théorème du rang en dimension finie). Donc il existe e_1 un vecteur de norme 1 pour $\|\cdot\|$ tel que $g(e_1) = 0 = \lambda e_1 - f(e_1)$. Posons $H = (\mathrm{Vect}(e_1)^\perp$. Par la proposition précédente, H est stable par f et on peut donc lui appliquer l'hypothèse de récurrence : il existe $(e_2, \ldots, e_n)$ une base orthonormée de H telle que $f_{|H}$ est diagonale et dont les éléments diagonaux sont réels. On voit que la base $(e_1, \ldots, e_n)$ permet de conclure. □

Corollaire 4.7.9 *Soit $M \in M_n(\mathbb{R})$ (respectivement $M \in M_n(\mathbb{C})$) une matrice symétrique (respectivement hermitienne). Alors il existe une matrice C orthogonale (respectivement unitaire) telle que*

$$C^{-1}MC = C^*MC = D$$

où D est une matrice diagonale réelle.

Démonstration : On note $E := \mathbb{R}^n$ (respectivement $E := \mathbb{C}^n$). Munissons E du produit scalaire usuel :

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := \sum_{i=1}^{n} \bar{x}_i y_i.$$

Soit $f \in \mathrm{End}(E)$ tel que sa matrice dans la base canonique B de E est M. Comme f est autoadjoint (par hypothèse sur M) il existe par le théorème précédent une base B' orthonormée telle que $D := [f]_{B'}$ est diagonale réelle. Si on note C la matrice de passage de B à B' on obtient le résultat. □

Remarque 4.7.10 Le corollaire montre notamment que la forme quadratique $X \mapsto X^*MX$ est (définie) positive si et seulement si les coefficients diagonaux de la matrice D correspondante sont (stricement) positifs.

Corollaire 4.7.11 *Soit Φ une forme quadratique (respectivement hermitienne) sur E euclidien (respectivement hermitien). Il existe une base orthonormée de E dans laquelle la matrice de Φ est diagonale réelle.*

Démonstration : Soit B une base orthonormée de E et soit M la matrice de Φ dansla abse B. La matrice M est symétrique (respectivement hermitienne) et le corollaire précédent assur l'existence de C orthogonale (respectivement unitaire) telle que $D := C^*MC$ est diagonale réelle. La matrice C définit un changement de base orthogonal qui fait passer de la base B à une base orthonormale B' ; et la matrice de Φ dans la base B' est D. □

Remarque 4.7.12 Bien noter que la base est orthonormée pour le produit scalaire sur E et donc n'a rien avoir avec Φ.

Corollaire 4.7.13 *Soient M, N deux matrices symétriques (respectivement hermitiennes) telles que la matrice M est définie positive. Il existe une matrice C inversible telle que*

$$C^*MC = I_n \quad \text{et} \quad C^*NC = D$$

où D est diagonale réelle.

Démonstration : Sur $E := \mathbb{R}^n$ (respectivement $E := \mathbb{C}^n$), l'application $\varphi : (X, Y) \mapsto X^*MY$ est un produit scalaire et $\Psi : X \mapsto X^*NX$ est une forme quadratique (respectivement hermitienne) ; D'après le corollaire précédent, il existe une base B orthonormale pour le produit scalaire φ telle que la matrice D de Ψ dans B est diagonale réelle. Notons C la matrice de passage de la base canonique de E à B, on a $C^*MC = I_n$ et $C^*NC = D$. □

Chapitre 5

Groupes

5.1 Sous-groupes distingués, Quotient de groupes

On voudrait généraliser les constructions et énoncés concernant les quotients de groupes abéliens au cas de groupes non-nécessairement abéliens. Il convient pour cela d'introduire une définition :

Définition 5.1.1 Soit G un groupe et H un sous-groupe de G. On dit que H *est distingué dans* G et on note $H \triangleleft G$, si

$$\forall g \in G, \forall h \in H, \quad ghg^{-1} \in H.$$

Remarque 5.1.2 Notons que $H \triangleleft G$ ssi $\forall g \in G, \quad gHg^{-1} \subset H$.

Exemple 5.1.3 Donnons tout de suite quelques exemples de sous-groupes distingués :

1. G et $\{1\}$ sont distingués dans G.
2. Si $(G, +)$ est abélien, alors tout les sous-groupes de G sont abéliens
3. Si $\varphi : G \to F$ est un morphisme de groupes, alors $\mathrm{Ker}(\varphi)$ est distingué dans G.

Définition 5.1.4 On appelle *centre de* G, noté $Z(G)$ l'ensemble

$$Z(G) := \{x \in G \mid \forall g \in G, \ gx = xg\}.$$

Proposition 5.1.5 *Le centre est un sous-groupe distingué de* G.

Démonstration : Visiblement $1 \in Z(G)$ qui est donc non vide. Si $x, y \in Z(G)$ soit $g \in G$. On a

$$\begin{aligned} g(xy^{-1}) &= (gx)y^{-1} = (xg)y^{-1} = x(gy^{-1}) = x((g^{-1})^{-1}y^{-1}) \\ &= x(yg^{-1})^{-1} = x(g^{-1}y)^{-1} = x(y^{-1}g) \\ &= (xy^{-1})g. \end{aligned}$$

Ceci prouve que $Z(G)$ est un sous-groupe de G. Montrons qu'il est distingué : soit $x \in Z(G)$ et soit $g \in G$. On a

$$gxg^{-1} = (gx)g^{-1} = (xg)g^{-1} = x(gg^{-1}) = x.$$

En particulier gxg^{-1} est bien dans $Z(G)$. □

Proposition 5.1.6 *Si $\varphi : G \to G'$ est un morphisme de groupes, alors le noyau de φ est distingué dans G.*

Démonstration : Soit $x \in \mathrm{Ker}(\varphi)$ et soit $g \in G$. Comme φ est un morphisme, on a

$$\varphi(g^{-1}xg) = \varphi(g)^{-1}\varphi(x)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1$$

Ceci prouve que $\mathrm{Ker}(\varphi) \triangleleft G$. □

Armé de cette notion de sous-groupe distingué nous pouvons maintenant étendre les constructions et résultats du paragraphe précédent.

Soit G un groupe et H un sous-groupe de G. On cherche une condition nécessaire pour pouvoir mettre une structure de groupe sur le quotient G/H de sorte que la projection canonique π_H soit un morphisme de groupes. Rappelons que $G/H := \{xH \mid x \in G\}$ est l'ensemble des classes d'équivalences pour la relation de congruence modulo H définie par

$$\forall x, y \in G, \quad x \equiv y \bmod H \overset{\text{définition}}{\iff} y^{-1}x \in H.$$

Proposition 5.1.7 *Si G/H est un groupe tel que π_H est un morphisme de groupes, alors $H \triangleleft G$.*

Démonstration : Comme π_H est un morphisme, on doit avoir :

$$\forall x, y \in G, \quad xH \cdot yH = \pi_H(x) \cdot \pi_H(y) = \pi_H(xy) = xyH.$$

De plus cette loi doit être bien définie donc on a

$$\forall x, y, a, b \in G\, (a = x \bmod H \text{ et } b = y \bmod H) \Rightarrow ab = xy \bmod H.$$

Or par définition on a

$$\begin{aligned} ab = xy \bmod H \quad &\iff \quad abH = xyH \\ &\iff \quad y^{-1}x^{-1}abH = H \\ &\iff \quad y^{-1}x^{-1}ab \in H \end{aligned}$$

Appliquons ceci avec $b := y$ et $a := xh$ où $h \in H$ est un élément quelconque. On obtient que

$$\forall y \in G,\ \forall h \in H, \quad y^{-1}hy \in H,$$

autrement dit que H est distingué dans G. □

Réciproquement :

Proposition 5.1.8 *Soit $H \triangleleft G$. On peut munir G/H d'une structure de groupe, unique, telle que π_H est un morphisme de groupes.*

Démonstration : Pour que π_H soit un morphisme de groupes, on voit que l'on n'a pas le choix : si $X = \pi_H(x)$ et $Y = \pi_H(y)$ sont deux éléments quelconques de G/H, il faut poser

$$X \cdot Y := \pi_H(xy).$$

Comme H est distingué dans G cette loi est bien définie et on vérifie ensuite immédiatement qu'elle munie G/H d'une structure de groupe. □

Comme dans les cas des groupes commutatifs, il existe dans ce contexte une *factorisation canonique* des morphismes.

Théorème 5.1.9 *Soit $\varphi : G \to G'$ un morphisme de groupes et soit $H \triangleleft G$. Si $H \subset \mathrm{Ker}(\varphi)$, alors il existe un unique morphisme $\bar{\varphi} : G/H \to G'$ tel que $\varphi = \bar{\varphi} \circ \pi_H$.*

Démonstration : Il s'agit de la même preuve que dans la cas commutatif, l'hypothèse $H \triangleleft G$ étant là pour assurer que G/H est un groupe tel que π_H est un morphisme de groupes. □

Corollaire 5.1.10 *Si $\varphi : G \to G'$ est un morphisme de groupes, alors $G/\mathrm{Ker}(\varphi)$ est isomorphe à $\mathrm{Im}(\varphi)$.*

Démonstration : C'est la même preuve que dans le cas commutatif. □

Exemple 5.1.11 Soit $\mathbb{K}$ un corps et soit $n \geq 2$. Notons $\mathrm{GL}_n(\mathbb{K})$ le groupe des matrices carrées inversibles et notons $\mathrm{SL}_n(\mathbb{K})$ le noyau du morphisme déterminant $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$. Ce morphisme étant visiblement surjectif (un élément $x \in \mathbb{K}^\times$ ayant par exemple comme antécédent la matrice diagonale $\mathrm{diag}(x, 1, \ldots, 1)$), on obtient par le corollaire précédent l'isomorphisme

$$\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K}) \simeq \mathbb{K}^\times.$$

Proposition 5.1.12 *Soit G un groupe, soit $H \triangleleft G$ et soit $\pi_H : G \to G/H$ la projection canonique. Il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H. Elle est donnée par $E \mapsto \pi_H(E)$ de réciproque $\mathcal{E} \mapsto \pi_H^{-1}(\mathcal{E})$.*

Démonstration : Cf. DM 1 et son corrigé. □

La proposition précédente permet, connaissant les sous-groupes de $\mathbb{Z}$, de retrouver les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

5.2 Actions de groupes

Définition 5.2.1 Soit X un ensemble. On note $\mathcal{S}(X)$ l'ensemble des bijections de X dans X. On appelle cet ensemble l'*ensemble des permutations de X*.

Lemme 5.2.2 *Muni de la loi de composition, $\mathcal{S}(X)$ est un groupe de neutre Id_X et l'inverse de f est sa bijection réciproque.*

Démonstration : Immédiat. □

On reviendra plus loin sur l'étude de $\mathcal{S}(X)$ quand $X = \{1, \ldots, n\}$, avec $n \in \mathbb{N}^*$.

Théorème 5.2.3 ***(Cayley)*** *Soit G un groupe. Considérons l'application $\sigma : G \to \mathcal{S}(G)$, $g \mapsto \sigma_g$ avec $\sigma_g(h) := gh$ pour tout $h \in G$. Alors σ est un mrophisme de groupes injectif, autrement dit, G est isomorphe à un sous groupe d'un groupe de permutations.*

Démonstration : Pour tout g, il est clair que σ_g est bijectif (de bijection réciproque $\sigma_{g^{-1}}$) donc l'application est bien définie. C'est visiblement un morphisme de groupes et si $\sigma_g = \mathrm{Id}_G$ alors $g = \sigma_g(1) = 1$ d'où l'injectivité. □

Définition 5.2.4 Soit G un groupe et X un ensemble non vide. Supposons donnée un application

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x \quad \text{telle que} \quad \forall x \in X,\ 1 \cdot x = x \quad \text{et} \quad \forall g, g' \in G,\ g \cdot (g' \cdot x) = (gg') \cdot x.$$

On dit que G *opère sur* X ou qu'on a *une action de G sur X*.

Exemple 5.2.5

1. *Action par translation de G sur G : $G \times G \to G$, $(g, x) \mapsto gx$.*
2. *Action par conjuguaison de G sur $H \triangleleft G$: $G \times H \to H$, $(g, h) \mapsto ghg^{-1}$*

Théorème 5.2.6 *Il y a une bijection entre les actions de groupe de G sur X et les morphismes de G dans $\mathcal{S}(X)$, donnée par*

$$(G \times X \to X,\ (g,x) \mapsto g \cdot x) \ \mapsto (G \to \mathcal{S}(X),\ g \mapsto (x \mapsto g \cdot x)).$$

Démonstration : Il suffit d'expliciter la bijection réciproque : c'est l'application qui à un morphisme φ de G dans $\mathcal{S}(X)$ associe l'action $(g, x) \mapsto g \cdot x := (\varphi(g))(x)$. □

Définition 5.2.7 Une action est dite *fidèle* si le morphisme de G dans $\mathcal{S}(X)$ associé à l'action est injectif.

Définition 5.2.8 Une action est dite *transitive* si

$$\forall x, y \in X, \quad \exists g \in G,\ g \cdot x = y.$$

Exemple 5.2.9 : l'action par translation est fidèle et transitive. L'action par conjuguaison de $G \neq \{1\}$ sur son centre n'est pas fidèle ni transitive.

Définition 5.2.10 Soit G un groupe agissant sur un ensemble X et soit $x \in X$. On appelle *orbite de x*, l'ensemble

$$\omega(x) := \{y \in X \mid \exists g \in G\ g \cdot x = x\} = G \cdot x.$$

Notons que l'orbite de x contient toujours l'élément x.

Remarque 5.2.11 Si G agit sur X on peut considérer la relation d'équivalence donnée par

$$\forall x, y \in X,\ x \mathcal{R} y \iff \exists g \in G, \quad g \cdot x = y.$$

Par construction les classes d'équivalences pour cette relation sont les orbites de X pour l'action. En particulier on en déduit :

Proposition 5.2.12 *Les orbites forment une partition de X.*

Définition 5.2.13 Soit G un groupe agissant sur un ensemble X et soit $x \in X$. On appelle stabilisateur de x l'ensemble

$$\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\}.$$

Proposition 5.2.14 *Pour tout $x \in X$, l'ensemble* $\mathrm{Stab}(x)$ *est un sous groupe de G. De plus, l'application surjective de G dans $\omega(x)$, définie par $g \mapsto g \cdot x$, induit par passage au quotient une bijection de $G/\mathrm{Stab}(x)$ sur $\omega(x)$.*

Démonstration : On vérifie immédiatement que $\mathrm{Stab}(x)$ est un sous groupe. L'application considérée est surjective par définition de $\omega(x)$. Il suffit de prouver qu'elle est injective et bien définie par passage au quotient. Or on a

$$g \cdot x = g' \cdot x \iff (g'^{-1} g) \cdot x = x \iff g'^{-1} g \in \mathrm{Stab}(x).$$

Ceci prouve à la fois que l'aplication passe au quotient et qu'elle est injective sur le quotient. □

Corollaire 5.2.15 ***Équation aux classes*** *Soit G agissant sur un ensemble X fini non vide. On a*

$$\mathrm{Card}(X) = \sum_x \mathrm{Card}\omega(x) = \sum_x \mathrm{Card}G/\mathrm{Stab}(x),$$

la somme portant sur un système de représentants des orbites.

Démonstration : On utilise que les orbites forment une partition de X ainsi que la proposition précédente. □

Proposition 5.2.16 *Soit G agissant sur un ensemble X. Soient $x \in X$ et $g \in G$. On a*

$$\mathrm{Stab}(g \cdot x) = g\mathrm{Stab}(x)g^{-1}.$$

Démonstration : On raisonne par équivalences :

$$\begin{aligned}
\alpha \in \mathrm{Stab}(g \cdot x) &\iff \alpha \cdot (g \cdot x) = g \cdot x \\
&\iff (\alpha g) \cdot x = g \cdot x \\
&\iff (g^{-1}\alpha g) \cdot x = x \\
&\iff g^{-1}\alpha g \in \mathrm{Stab}(x) \\
&\iff \alpha \in g\mathrm{Stab}(x)g^{-1}.
\end{aligned}$$ □

Proposition 5.2.17 *Si G agit sur X et G et X sont finis alors, pour tout $x \in X$, on a :* $\omega(x)|\mathrm{Card}G$.

Démonstration : On utilise que $\omega(x)$ est de même cardinal que $G/\mathrm{Stab}(x)$ et que, G étant fini, ce cardinal est le quotient du cardinal de G par celui de $\mathrm{Stab}(x)$. □

5.3 Groupes de Sylows et p-groupes

5.3.1 Les p-groupes

Définition 5.3.1 Soit G un groupe fini de cardinal p^n avec p premier et $n \geq 0$. On dit que *G est un p-groupe.*

Lemme 5.3.2 *Soit G un p-groupe, opérant sur un ensemble fini X. Notons*

$$X^G := \{x \in X \mid \forall g \in G,\ g \cdot x = x\}.$$

On a

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) \bmod p.$$

Démonstration : On voit que $x \in \omega(x) \iff \omega(x) = \{x\}$. On peut ensuite appliquer l'équation aux classes :

$$\mathrm{Card}(X) = \sum_{x \in I_1} \mathrm{Card}(\omega(x)) + \sum_{x \in I_2} \mathrm{Card}(\omega(x)),$$

où I_1 est un système de représentants des orbites de cardinal 1 et I_2 de celles de cardinal au moins 2. On obtient donc

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) + \sum_{x \in I_2} \mathrm{Card}(\omega(x)).$$

Or on sait que le cardinal de l'orbite divise $p^n = \mathrm{Card}(G)$, donc si l'orbite est de cardinal au moins 2, alors son cardinal est nul modulo p. Ceci permet de conclure. □

Proposition 5.3.3 *Soit G un p-groupe non trivial. Alors le centre de G n'est pas réduit à $\{1\}$.*

Démonstration : On fait agir G sur lui même par conjuguaison. Pour cette action, l'ensemble X^G est exactement $Z(G)$. Donc le lemme précédent entraîne que $Z(G)$ est un multiple de p. Or $1 \in Z(G)$ donc le cardinal de $Z(G)$ est au moins p. □

5.3.2 Les p-Sylows : énoncé du théorème et applications

Dans tout ce paragraphe, G est un groupe fini de cardinal n. On se donne p un nombre premier et on écrit la décomposition de n : $n = p^r m$ avec m premier à p et $r \geq 0$.

Définition 5.3.4 Un sous-groupe de G de cardinal p^r est appelé un *p-Sylow de G.*

Théorème 5.3.5 *Avec les notations précédentes, on a*

1. *Il existe au moins un p-Sylow dans G. Si n_p est le nombre de p-Sylow, alors*

$$n_p = 1 \bmod p \quad \text{et} \quad n_p | m.$$

2. *Les p-Sylows sont deux à deux conjugués (ie pour tout p-Sylows P et Q, il existe $g \in G$ tel que $P = gQg^{-1}$).*

Corollaire 5.3.6 *Soit P un p-Sylow de G. Alors,*

$$P \triangleleft G \iff n_p = 1.$$

Démonstration : Si P est distingué dans G, alors comme les p-Sykow sont conjugués, ils sont en fait tous égaux à P, donc $n_p = 1$. Réciproquement, si $n_p = 1$ alors pour tout $g \in G$, on a gPg^{-1} est un p-Sylow, donc est égal à P, donc P est distingué dans G. □

5.3.3 Les p-Sylows : preuve du théorème

Commençons par traiter un cas particulier et prouvons qu'il existe dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ un p-sylow (que l'on va même décrire explicitement). Nous verrons ensuite comment nous ramener dans le cas général à ce cas particulier. Dans toute la suite p est un nombre premier et $n \in \mathbb{N}^*$.

Lemme 5.3.7 *Le cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ est $\prod_{i=0}^{n-1}(p^n - p^i)$.*

Démonstration : Se donner un matrice inversible à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ équivaut à se donner une application linéaire de $(\mathbb{Z}/p\mathbb{Z})^n$ dans lui même, qui est bijective. Ceci équivaut donc à se donner l'image $(f_1, \ldots, f_n)$ de la base canonique, de sorte que la famille $(f_1, \ldots, f_n)$ est une base. Ainsi le cardinal recherché est exactement le cardinal de l'ensemble des bases de l'espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^n$. Il nous reste à dénombrer l'ensemble des bases possibles :

Pour le premier vecteur, f_1 : tout élément de $(\mathbb{Z}/p\mathbb{Z})^n$ sauf zéro convient ; il y a donc $p^n - 1$ possibilités.

Pour le second vecteur, f_2 : tout élément qui n'est pas sur la droite engendrée par f_1, $\mathbb{Z}/p\mathbb{Z}f_1$ convient ; il a donc $p^n - p$ possibilités.

On itère l'argument et pour le dernier vecteur : tout élément qui n'est pas dans l'hyperplan $\mathbb{Z}/p\mathbb{Z}f_1 \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}f_{n-1}$ engendré par $f_1, \ldots, f_{n-1}$ convient : il y a donc $p^n - p^{n-1}$ possibilités.

En prenant le produit des diverses possibilités on conclut. □

Finalement en factorisant chaque terme $p^n - p^i$ sous la forme $p^i(p^{n-i} - 1)$, on voit que la cardinal de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ peut se réécrire :

$$\mathrm{Card}\left(\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})\right) = p^{\sum_{i=0}^{n-1} i}\left(\prod_{i=1}^{n}(p^i - 1)\right) = p^{\frac{n(n-1)}{2}}m \quad \text{avec } m \wedge p = 1.$$

IL s'agit donc de trouver un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p^{\frac{n(n-1)}{2}}$.

Lemme 5.3.8 *L'ensemble* $P := \{(a_{ij}) \in M_n(\mathbb{Z}/p\mathbb{Z}) \mid \forall i,\ a_i i = 1, \text{ et } \forall j < i,\ a_{ij} = 0\}$ *est un p-Sylow de* $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Démonstration : Tous les éléments de P sont de déterminant 1. Il est clair que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. De plus pour chaque a_{ij} avec $j > i$, on a p valeurs possibles. Il y a donc $p^{\sum_{i=1}^{n-1} i} = p^{\frac{n(n-1)}{2}}$ matrices dans P qui est donc un p-Sylow de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. □

Nous voulons utiliser ceci pour prouver l'existence d'un p-Sylow dans un groupe quelconque.

Lemme 5.3.9 *Soit G un groupe fini de cardinal n et soit p un nombre premier. Alors, G est isomorphe à un sous-groupe de* $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Démonstration : Par le théorème de Cayley, on sait que G est isomorphe à un sous-groupe de $\mathcal{S}_n$. Il suffit de prouver que S_n est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$ pour conclure. Pour cela on considère l'application φ de $\mathcal{S}_n$ dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ qui à une permutation σ associe la matrice de permutation M_σ définie par son action sur la base canonique par $e_i \mapsto e_{\sigma(i)}$. On vérifie que φ est un morphisme de groupes. De plus le noyau de φ est l'ensemble des σ tels que $M_\sigma = I_n$ ie tels que $e_{\sigma(i)} = e_i$ pour tout i, ie tels que $\sigma(i) = i$ pour tout i, ie tels que $\sigma = \mathrm{Id}$. Donc φ est injectif et ceci conclut. □

Le lemme suivant nous indique que si l'on connait un p-Sylow dans un groupe, on peut trouver un p-Sylow dans tous ses sou-groupes.

Lemme 5.3.10 *Soit $\mathcal{G}$ un groupe de cardinal $p^\alpha m$ avec $p \wedge m = 1$ et $\alpha \geq 1$. Soit $\mathcal{H}$ un sous-groupe de $\mathcal{G}$ et soit S un p-Sylow de $\mathcal{G}$. Il existe $a \in \mathcal{G}$ tel que $aSa^{-1} \cap \mathcal{H}$ est un p-Sylow de $\mathcal{H}$.*

Démonstration : On considère l'action de $\mathcal{G}$ sur $\mathcal{G}/S$ par translation : $(g, xS) \mapsto gxS$. Déterminons son stablisateur :

$$\begin{aligned}
\mathrm{Stab}(xS) &= \{g \in \mathcal{G} \mid gxS = xS\} \\
&= \{g \in \mathcal{G} \mid \forall s \in S\ gxs \in xS\} \\
&= \{g \in \mathcal{G} \mid gx \in xS\} \\
&= \{g \in \mathcal{G} \mid g \in xSx^{-1}\} = xSx^{-1}.
\end{aligned}$$

De plus on peut considérer la restriction de cette action du sous-groupe H sur l'ensemble $\mathcal{G}/S$. Dans ce cas le même calcul montrer que le stablisateur (que l'on note Stab_H) est

$$\mathrm{Stab}_H(xS) = xSx^{-1} \cap H.$$

Visiblement $\mathrm{Stab}_H(xS)$ est un sous-groupe de xSx^{-1} qui est un p-Sylow (car conjugué à S). Donc $\mathrm{Stab}_H(xS)$ est un p-groupe. Il est de plus inclus dans H. On cherche un x tel que $\mathrm{Stab}_H(xS)$ soit un p-groupe de cardinal maximal, ie tel que $\frac{|H|}{|\mathrm{Stab}_H(xS)|} \wedge p = 1$. Or on sait que $H/Stab_H(xS)$ est en bijection avec l'orbite $\omega_H(xS)$ de xS pour l'action de H sur $\mathcal{G}/S$. En appliquant l'equation aux classes, on a

$$|\mathcal{G}/S| = \sum_x |\omega_H(xS)|$$

où x varie dans un système de représentants des orbites. Si par l'absurde pour tout x on a : p divise $|\omega_H(xS)|$; alors p divise donc $|\mathcal{G}/S|$. Mais S est un p-Sylow de $\mathcal{G}$, donc p est premier avec $\mathcal{G}/S$. Ceci conclut. □

Preuve de l'existence d'un p-Sylow dans un groupe G : On plonge G de cardinal n dans $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et on applique le lemme précédent avec $\mathcal{G} = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $\mathcal{H} = G$. □

Théorème 5.3.11 ***(Complément à Sylow)*** *Si H est un sous groupe de G et si H est un p-groupe, alors il existe un p-Sylow de G contenant H.*

Preuve de ce théorème et du point (2) du théorème de Sylow : On introduit un p-Sylow S (dont on sait maintenant qu'il existe). Le lemme précédent nous donne l'existence d'un élément $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H. Mais H est un p-groupe, c'est donc son propre p-Sylow. Ainsi, $H \subset aSa^{-1}$ qui est un p-Sylow de G. Ceci prouve le théorème. Si on suppose de plus que H est lui même un p-Sylow, alors par cardinalité on voit que $H = aSa^{-1}$ donc tout les p-Sylow sont conjugués. □

Il nous reste maintenant à prouver l'assertion sur le nombre n_p de p-Sylow : on introduit pour cela l'ensemble X de tout les p-Sylow de G. On a $n_p = |X|$. On considère l'action de G sur X par conjuguaison : $(g, S) \mapsto gSg^{-1}$. Soit P un p-sylow de G. Ce groupe induti par restriction une action par conjuguaison de P sur X. De plus P est un p-groupe, donc en notant $X^P := \{S \in X \mid \forall g \in P,\ gSg^{-1} = S\}$, on a

$$n_p = |X| = |X^P| \bmod p.$$

De plus on a $gPg^{-1} = P$ pour tout $g \in P$ donc P est dans X^P. Montrons que c'est le seul élément :

soit S un p-Sylow et G tel que $\forall g \in P$, on a$gSg^{-1} = S$. Soit N le sous-groupe de G engendré par les éléments de S et ceux de P (un élément de N sécrit donc comme un produit de puissances (à coefficients dnas $\mathbb{Z}$) d'éléments de S et de P). Les groupes S et P sont inclus dans N. Ce sont donc des p-Sylow de N (car $N \subset G$), mais par définition, S est stable par conjugaison par tout élément de P et évidemment aussi également par tout élément de S. Donc

$$\forall g \in N,\ gSg^{-1} = S.$$

Autrement dit S est distingué dans N, c'est donc son unique p-Sylow. Donc $S = P$, ie $|X^P| = 1$ donc $n_p = 1 \bmod p$. De plus, les p-Sylow sont conjugués donc

$$|X| = |\omega(P)| = \frac{|G|}{|\mathrm{Stab}(P)|} \mid |G|.$$

Donc n_p divise $|G|$ et est premier avec p, donc n_p divise m. □

5.3.4 Quelques applications de Sylow

Corollaire 5.3.12 *Soit G un groupe de cardinal $n = p^r m$ avec p premier, $r \geq 1$ et m premier à p.*

1. *Pour tout $i \leq r$ il existe un sous-groupe H_i de G de cardinal p^i.*
2. *Si G est de plus un p-groupe, on peut même choisir les H_i distingués dans G.*

Démonstration : Nous allons démontrer le résultat en nous appuyant sur un théorème qui ne sera prouvé qu'au second semestre (le théorème de structure des groupes abéliens finis). Dans G il existe un p-Sylow P. Nous allons travailler dans P (qui est de cardinal p^r) et construire une suite de sous-groupes H_i, distingués dans P de cardinal p^i. Ceci prouvera les deux énoncés. On fait une preuve par récurrence sur r.

Si P est abélien, le théorème de structure des groupes abéliens finis (que l'on admet ici) nous assure que P est isomorphe à un produit $\prod_{i=1}^{s} \mathbb{Z}/p^{a_i}\mathbb{Z}$ avec $1 \leq a_1 \leq \ldots \leq a_s$. Dans un tel groupe il est facile de construire les groupes H_i.

Si P n'est pas abélien, alors son centre $Z(P)$ est non trivial (car P est un p-groupe) et différent de P, donc de cardinal p^s avec $1 \leq s \leq r-1$. Par hypothèse de récurrence on en déduit l'existence de $H_0, \ldots, H_s$, sous-groupes distingués dans $Z(P)$ (donc dans P vue la définition du centre) de cardinal respectif $p^0, \ldots, p^s$.

Par ailleurs, on peut considérer la projection canonique $\pi : P \to P/Z(P)$ (qui est un morphisme de groupes car $Z(P)$ est distingué dans P). Le groupe quotient $P/Z(P)$ est de cardinal p^{r-s} avec $1 \leq r-s \leq r-1$. En appliquant l'hypothèse de récurrence à $P/Z(P)$ on trouve des groupes $\mathcal{H}_{s+1}, \ldots, \mathcal{H}_{s+(r-s)} = \mathcal{H}_r$ de cardinal respectif $p^1, \ldots, p^{r-s}$, distingués dans $P/Z(P)$. En posant $H_{s+i} := \pi^{-1}(\mathcal{H}_{s+i})$ on obtient ainsi des sous-groupes contenant $Z(P)$, (dont on vérifie aisément qu'ils sont distingués dans P) de cardinal p^{s+i}. Le dernier point découle par factorisation canonique : le projection π restreinte à H_i est surjective sur $\mathcal{H}_i$ et de noyau $Z(P)$ (facile), donc le cardinal de H_i est la produit de celui de $Z(P)$ par celui de $\mathcal{H}_i$.

Finalement on a bien obtenu des H_i comme annoncé. □

Corollaire 5.3.13 *Soit G un groupe de cardinal $n = p^r m$ avec p premier, $r \geq 1$ et m premier à p. Il existe $x \in G$ d'ordre p.*

Démonstration : On applique le corollaire précédent avec $i = 1$. □

5.3.5 Un exemple

Lemme 5.3.14 *Soient P, Q deux sous-groupes distingués d'un groupe fini G, tels que $P \cap Q = \{1\}$ et $|P| \cdot |Q| = |G|$. Alors l'application*

$$\varphi : P \times Q \to G,\ (x, y) \mapsto xy$$

est un isomorphisme de groupes.

Démonstration : Si φ est un morphisme, il suffit par cardinalité de prouver que φ est injectif pour conclure. Or $xy = 1$ implique $x = y^{-1}$. Mais x est dans P et y^{-1} est dans Q. Donc $1 = x = y$, ie φ est injectif. Reste à prouver que φ est un morphisme : soit (a, b) et (x, y) deux couples de $P \times Q$.

$$\varphi((a,b)(x,y)) = \varphi(ax, by) = axby \ \text{ et } \ \varphi(a,b)\varphi - x, y) = abxy = ax(x^{-1}bx)y.$$

Montrons que $x^{-1}bx = b$ ce qui concluera. On a

$$x^{-1}bxb^{-1} = (x^{-1}bx)b^{-1} \in Q \text{ car } Q \text{ est distingué dans } G,$$

et

$$x^{-1}bxb^{-1} = x^{-1}(bx)b^{-1}) \in P \text{ car } P \text{ est distingué dans } G.$$

Finalement cet élément est dans $P \cap Q = \{1\}$ donc égal à 1. □

Corollaire 5.3.15 *Soit G un groupe de cardinal p^2. Alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.*

Démonstration : Si il y a dans G un élément d'ordre p^2. Alors G est cyclique engendré par cet élément, donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon tous les éléments sauf 1_G sont d'ordre p. Soit $x \neq 1$ d'ordre p. Notons P le groupe qu'il engendre. Soit $y \in G - P$: il est d'ordre p et on note Q le groupe qu'il engendre. Le groupe G est d'ordre p^2 donc abélien (cf. TD) donc P et Q sont distingués dans G. De plus $|P| \cdot |Q| = p^2 = |G|$. Enfin, si z est dans l'intersection de P et Q : soit $z = 1$, soit z est d'ordre p et engendre donc un sous-groupe de P d'ordre p, donc est égal à P et est de même égal à Q, donc $P = Q$ ce qui est impossible. Donc $P \cap Q = \{1\}$. Le lemme donne donc un isomorphisme entre G et $(\mathbb{Z}/p\mathbb{Z})^2$. □

Exemple : *Soit G un groupe de cardinal 245, alors G est cyclique isomorphe à $\mathbb{Z}/245\mathbb{Z}$ ou est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$.*
Démonstration : En appliquant le théorème de Sylow on voit que $n_7 = n_5 = 1$ donc l'unique 7-Sylow : P_7 est distingué dans G et de même, l'unique 5-Sylow, P_5 est distingué dans G. Si $x \in P_5 \cap P_7$ alors l'ordre de x divise 5 et divise 7^2 donc est égal à 1. Donc $\mathcal{P}_5 \cap P_7 = \{1\}$. Nous pouvons donc appliquer le lemme précédent : G ets isomorphe au produit $P_5 \times P_7$. De plus P_5 est de cardinal le nombre premier 5, donc est cyclique isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Le groupe P_7 est de cardinal 7^2 donc on peut appliquer le corollaire précédent : P_7 est isomorphe à $(\mathbb{Z}/7\mathbb{Z})^2$ ou à $\mathbb{Z}/7^2\mathbb{Z}$. Finalement en appliquant le lemme des restes Chinois on peut conclure. □

Chapitre 6

Groupe Symétrique

6.1 Le groupe symétrique $\mathcal{S}_n$

Définition 6.1.1 Soit$n \in \mathbb{N}^*$. On appelle *groupe symétrique* et on note $\mathcal{S}_n$ l'ensemble des bijections de $\{1, \ldots, n\}$ sur lui même. Une telle bijection s'appelle une *permutation*. On note t_{ij} ou (ij) la permutation qui envoie i sur j et j sur i et fixe les autres éléments. Une telle permutation s'appelle une *transposition*. Plus généralement on appelle *k-cycle* toute permutation de la forme $c_k := (a_1, \ldots, a_k)$ définie de la façon suivante :

$$c_k(a_i) = a_{i+1} \text{ pour } 1 \leq i \leq k-1, \quad c_k(a_k) = a_1, \quad \text{et} \quad c_k(x) = x \text{ pour tout } x \notin \{a_1, \ldots, a_k\}.$$

Proposition 6.1.2 *L'ensemble $\mathcal{S}_n$ muni de la composition est un groupe, de neutre $Id_{\{1,\ldots,n\}}$. L'inverse d'une permutation σ est sa bijection réciproque σ^{-1}. Le groupe $\mathcal{S}_n$ est de cardinal $n!$*

Démonstration : Immédiat. □

Définition 6.1.3 Soit $\sigma \in \mathcal{S}_n$ et soit $k \in \{1, \ldots, n\}$. L'ensemble

$$\omega(k) := \{\sigma^j(k) \mid j \in \mathbb{Z}\}$$

et appelé *l'orbite de k* (pour σ).

Remarque 6.1.4 Le groupe cyclique $< \sigma >$ opère sur $\{1, \ldots, n\}$ via $(\sigma^j, r) \mapsto \sigma^j(r)$. On constate que $\omega(k)$ est l'orbite de k pour cette action. En particulier les orbites forment une partition de $\{1, \ldots, n\}$.

Définition 6.1.5 Soit $\sigma \in \mathcal{S}_n$. Le sous-ensemble de $\{1, \ldots, n\}$, noté X_σ et défini par $X_\sigma := \{k \mid \sigma(k) \neq k\}$.

Proposition 6.1.6 *Soient $s, t \in \mathcal{S}_n$ deux permutations à supports disjoints (ie $X_s \cap X_t = \emptyset$). Alors $st = ts$.*

Démonstration : Soit $a \in X_t$. Par hypothèse, $a \notin X_s$ donc $s(a) = a$ donc $st(a) = s(t(a))$ et $ts(a) = t(s(a)) = t(a)$. De plus $t(a)$ est dans X_t (sinon on aurait $t(t(a)) = t(a)$ d'où, en composant par t^1, t(a)=a ce qui est impossible). Donc l'hypothèse implique que $t(a) \notin X_s$, donc $s(t(a)) = t(a)$. Si a est dans X_s un argument symétrique montre que $st(a) = ts(a) = s(a)$. Si a n'est ni dans X_s ni dans X_t alors $st(a) = a = ts(a)$. □

Théorème 6.1.7 *Toute permutation $\sigma \in \mathcal{S}_n$ se décompose en produit de cycles à supports deux à deux disjoints. De plus cette décomposition est unique à l'ordre des facteurs près.*

Démonstration : Pour l'existence, il suffit de se souvenir (avec la remarque 6.1) que $\{1, \dots, n\}$ est la réunion disjointes des orbites $\omega(i)$ et que sur une telle orbite, σ agit de façon cyclique. Notons $\omega(i_1), \dots, \omega(i_m)$ les différentes orbites. On a

$$\forall j \leq m, \quad \sigma_{|\omega(i_j)} = (i_j, \sigma(i_j), \dots, \sigma^{r_j}(i_j)) =: c_j.$$

Les c_j sont des cycles de support $\omega(i_j)$ deux à deux disjoints et visiblement on a $\sigma = \prod_{j=1}^{m} c_j$. Il reste à prouver l'unicité, à permutation des facteurs près :

□

Théorème 6.1.8 *Soit $n \geq 2$. Les transpositions engendrent le groupe $\mathcal{S}_n$*

Démonstration : Nous allons donner deux preuves différentes :

1. En utilisant le théorème précédent, on voit qu'il suffit de prouver que tout cycle est un produit de transposition. Or
$$(x_1, \dots, x_k) = (x_1 x_2)(x_2 x_3) \dots (x_{k-1} x_k).$$
2. Le seconde preuve se fait par récurrence sur n : le résultat est immédiat si $n = 2$. Si la propriété est vraie au rang $n-1$: soit $s \in \mathcal{S}_n$. Soit $s(n) = n$ et dans ce cas $s_{|\{1,\dots,n-1\}}$ est une permutation de $\mathcal{S}_{n-1}$ donc peut s'écrire comme un produit de transpositions. Le même produit donne la décomposition de s. Soit $s(n) = k < n$ dans ce cas $s' := (nk)s$ est une permutation de $\mathcal{S}_{n-1}$ que l'on peut donc décomposer en produit de transpositions $t_1 \dots t_r$. On voit que $s = (nk)t_1 \dots t_r$. □

Lemme 6.1.9 *Soit c un k-cycle. Son ordre est k.*

Démonstration : En considérant les indices modulo k, on a voit que $c^j(x_r) = x_{r+j}$ pour tout j et pour tout r : il s'agit d'une récurrence immédiate sur j. Notamment $c^k = Id$ donc k est un multiple de l'ordre de c. De plus si $j < k$ on a $c^j(x_1) = x_{j+1} \neq x_1$ donc c n'est pas d'ordre j. Donc l'ordre de c est k. □

Proposition 6.1.10 *Soit $s = \prod_{i=1}^{r} c_i$ un produit de cycles à supports deux à deux disjoints. Alors l'ordre de s est le ppcm des ordres des c_i.*

6.2 Le groupe alterné $\mathcal{A}_n$ et le morphisme signature

Lemme 6.2.1 *Les transpositions sont conjuguées dans $\mathcal{S}_n$.*

Démonstration : Soient (ab) et (ij) deux transpositions. On vérifie aisément la formule

$$\forall \sigma \in \mathcal{S}_n, \ \sigma(ij)\sigma^{-1} = (\sigma(i)\sigma(j)).$$

Posons donc $\sigma(i) := a$ et $\sigma(j) := b$. On complète par cardinalité, σ en une bijection de l'ensemble $\{1, \dots, n\} - \{a, b\}$ sur l'ensemble de même cardinal $\{1, \dots, n\} - \{i, j\}$. La permutation σ ainsi construite répond au problème. □

Théorème 6.2.2 *Il existe un unique morphisme surjectif* $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$. *Ce morphisme vaut* -1 *sur les transpositions.*

Démonstration : Existence : Soit f une fonction de $\mathbb{Z}^n$ dans $\mathbb{Z}$ et soit σ une permutation de $\mathcal{S}_n$. On définit une nouvelle fonction $\pi(\sigma)f$ par la formule

$$\pi(\sigma)f(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

On vérifie sans difficulté que $\pi(s)\pi(t) = \pi(st)$ pour toutes permutations s et t. Soit maintenant Δ la fonction de $\mathbb{Z}^n$ dans $\mathbb{Z}$ définie par

$$\Delta(x_1, \ldots, x_n) := \prod_{i=1}^{n} \prod_{j=i+1}^{n} (x_j - x_i).$$

Soit τ une transposition échangeant deux entiers fixés distincts, $1 \leq r < s \leq n$. On construit la fonction $\tau\Delta$ par la formule

$$\tau\Delta := \pi(\tau)\Delta(x_1, \ldots, x_n) := \prod_{i=1}^{n} \prod_{j=i+1}^{n} (x_{\tau(j)} - x_{\tau(i)}).$$

Pour le facteur $i = r$, $j = s$, l'application de τ échange le facteur $(x_s - x_r)$ en $(x_r - x_s)$. Pour les autres facteurs, nous pouvons les grouper par paires selon les trois situations suivantes :

$$(x_k - x_s)(x_k - x_r) \text{ si } k > s,$$

$$(x_s - x_k)(x_k - x_r) \text{ si } r < k < s,$$

$$(x_s - x_k)(x_r - x_k) \text{ si } k < r.$$

Chacune de ces paires reste inchangées lorsque l'on applique τ. Finalement on en déduit que

$$\tau\Delta = -\Delta.$$

Soit maintenant σ une permutation quelconque. On pose $\varepsilon(\sigma)$ le signe 1 ou -1 tel que $\sigma\Delta = \varepsilon(\sigma)\Delta$. Comme π est un morphisme on en déduit que ε est un morphisme. De plus il est visiblement non trivial, d'où l'existence.

Pour donner une idée de ce qu'il se passe, montrons, une fois l'existence garantie par ce qui précède, que $\varepsilon(t) = -1$ si t est une transposition : on sait par le lemme précédent que les transpositions sont conjuguées donc s'il existe τ une transposition telle que $\varepsilon(\tau) = -1$ alors $\varepsilon(t) = \varepsilon(\sigma\tau\sigma^{-1}) = \varepsilon(\tau) = -1$ pour toute transposition t. Supposons donc par l'absurde que pour toute transposition t on a $\varepsilon(t) = 1$. Dans ce cas pour tout produit σ de transposition on a encore $\varepsilon(\sigma) = 1$. Mais on sait que $\mathcal{S}_n$ est engendré par les transpositions, donc ε envoie $\mathcal{S}_n$ sur $\{1\}$: impossible.
Il reste à prouver l'unicité : soit ε et ε' deux morphismes non triviaux de $\mathcal{S}_n$ dans $\{\pm 1\}$. Soit $\sigma \in \mathcal{S}_n$. Il existe $t_1, \ldots, t_r$ des transpositions telles que $\sigma = t_1 \ldots t_r$. Donc $\varepsilon(\sigma) = \prod_{i=1}^{r} \varepsilon(t_i) = (-1)^r = \prod_{i=1}^{r} \varepsilon'(t_i) = \varepsilon'(\sigma)$. □

Définition 6.2.3 On appelle morphisme *signature* le morphisme donné par le théorème précédent.

Proposition 6.2.4 *Si c est un k-cycle on a $\varepsilon(c) = (-1)^{k+1}$.*

Démonstration : On a $c = (x_1, \ldots, x_k) = (x_1x_2)\ldots(x_{k-1}x_k)$. Donc $\varepsilon(c) = \prod_{i=1}^{k-1} \varepsilon(x_ix_{i+1}) = (-1)^{k+1}$. □

Définition 6.2.5 On pose $\mathcal{A}_n := \mathrm{Ker}(\varepsilon)$. On appelle ce sous-groupe distingué de $\mathcal{S}_n$ le *groupe alterné.*

Proposition 6.2.6 *Soit H un sous-groupe d'indice de 2 dans $\mathcal{S}_n$ (ie le cardinal du quotient $\mathcal{S}_n/H$ est 2). Alors $H = \mathcal{A}_n$.*

Démonstration : Comme l'indice est 2 on sait que H est distingué dans $\mathcal{S}_n$, donc l'ensemble quotient est naturellement muni d'une structure de groupe. Ce groupe étant de cardinal 2, il est isomorphe à $\{\pm 1\}$. Notons i cet isomorphisme. De plus la projection canonique $\pi : \mathcal{S}_n \to \mathcal{S}_n/H$ est sujective de noyau H. En composant à l'arrivée par le morphisme i, on obtient un nouveau morphisme : $\varphi = i \circ \pi \ : \ \mathcal{S}_n \to \{\pm 1\}$ qui est toujours surjectif de noyau H. Mais étant surjectif, φ est en fait égal au morphisme signature par unicité de ce dernier. Donc $H = \mathrm{Ker}(\varphi) = \mathrm{Ker}(\varepsilon) = \mathcal{A}_n$. □

6.3 Déterminant

Soit A un anneau commutatif et $n \geq 1$. On note $\mathcal{M}_n(A)$ l'anneau des matrices carrées de taille n à coefficients dans A.

Définition 6.3.1 Soit $M = m_{ij}$ une matrice de $\mathcal{M}_n(A)$. On définit le *déterminant de M* par la formule

$$\det(M) := \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.$$

Remarque 6.3.2 Si $n = 2$ on retrouve la formule classique $\det(M) = ad - bc$. Pour $n = 3$ on retrouve la "règle de Sarrus".

Lemme 6.3.3 *On a $\det({}^tM) = \det(M)$.*

Démonstration : Il suffit de réciter la définition du déterminant de la transposée et de faire un changement d'indice dans la somme ($\tau = \sigma^{-1}$) puis dans le produit ($j = \tau^{-1}(-i)$). □

Remarque 6.3.4 On veut pouvoir parler du *polynôme caractéristique* d'une matrice carrée de taille n, M à coefficients dans un corps K. Ce polynôme est défini par $\det(XI_n - M)$. Il faut pour cela interpréter $XI_n - M$ comme une matrice à coefficients dans un certain anneau commutatif A. La bonne manière de voir est de constater que $XI_n - M$ est un élément de $\mathcal{M}_n(K[X])$.