Algèbre et géométrie pour l'Agrégation de Mathématiques
Deuxième édition
Chapitres modifiés

Jean-Étienne ROMBALDI

2 décembre 2024

Table des matières

Chapitre 1

Représentations d'un groupe fini

[1]Pour ce chapitre, G est un groupe multiplicatif d'élément neutre noté e, $\mathbb{K}$ est un corps commutatif de caractéristique nulle et E un $\mathbb{K}$-espace vectoriel. Nous préciserons quand G est fini, $\mathbb{K}=\mathbb{C}$ ou E est de dimension finie.

1.1 Définitions et exemples

Définition 1.1. *Une représentation linéaire de G dans E est un morphisme de groupes $\rho : G \to GL(E)$. On dit aussi que E est un G-module.*

On note (ρ, E) une telle représentation linéaire du groupe G et on dira simplement représentation.

Si ρ est constante égale à Id_E (*i. e.* $\rho(g) = Id_E$ pour tout $g \in G$), on dit alors que la représentation est triviale.

Pour E est de dimension $n \in \mathbb{N}^*$, on dit que la représentation est de dimension finie et la dimension de E est le degré de cette représentation. En se fixant une base de E, une représentation de G dans E revient à se donner un morphisme de groupes de G dans $GL_n(\mathbb{K})$. Désignant, pour tout $g \in G$, par $R(g) = ((\rho_{ij}(g)))_{1\leq i,j\leq n}$ la matrice de $\rho(g)$ dans une base $\mathcal{B}$ de E, on a pour g, h dans G, $R(g) \in GL_n(\mathbb{K})$ et $R(gh) = R(g)R(h)$, $R(g)^{-1} = R\left(g^{-1}\right)$.

Se donner une représentation linéaire de G dans E revient à se donner une action à gauche de G sur E, $(g, x) \in G \times E \mapsto g * x \in E$, qui est $\mathbb{K}$-linéaire, c'est-à-dire telle que $g*(\lambda x + \mu y) = \lambda g*x + \mu g*y$ pour tous λ, μ dans $\mathbb{K}$ et x, y dans E (pour tout $g \in G$, l'application $x \mapsto g*x$ est linéaire). En effet, si $\rho : G \to GL(E)$ est une une telle représentation, on définit alors une action sur le groupe G par :

$$\forall (g, x) \in G \times E,\ g * x = \rho(g)(x)$$

puisque, pour tous g, g' dans G et tout x dans E, on a $e*x = \rho(e)(x) = Id_E(x) = x$ et $g*(g'*x) = \rho(g)(\rho(g')(x)) = \rho(g) \circ \rho(g')(x) = \rho(gg')(x) = (gg')*x$. Cette

1. Ce chapitre était présent dans la première édition et a été supprimé dans la deuxième.

action est bien $\mathbb{K}$-linéaire puisque :

$$g*(\lambda x+\mu y)=\rho(g)(\lambda x+\mu y)=\lambda\rho(g)(x)+\mu\rho(g)(y)=\lambda g*x+\mu g*y$$

Réciproquement, soit $(g,x)\mapsto g*x$ une action à gauche $\mathbb{K}$-linéaire de G sur E. Pour tout $g\in E$, l'application $\rho(g):x\in E\mapsto g*x\in E$ est $\mathbb{K}$-linéaire et bijective. En effet, de la linéarité de l'action, on déduit que $\rho(g)\in\mathcal{L}(E)$, de $e*x=x$ pour tout $x\in E$, on déduit que $\rho(e)=Id_E$ et avec $g*\left(g^{-1}*x\right)=\left(gg^{-1}\right)*x=e*x=x$, $g^{-1}*(g*x)=x$, on déduit que $\rho(g)\circ\rho\left(g^{-1}\right)=\rho\left(g^{-1}\right)\circ\rho(g)=Id_E$, ce qui signifie que $\rho(g)$ est bijective d'inverse $\rho\left(g^{-1}\right)$. Enfin, avec $g*(g'*x)=(gg')*x$, pour tous g,g',x, on déduit que $\rho(gg')=\rho(g)\circ\rho(g')$, c'est-à-dire que l'application ρ est un morphisme de groupes de G dans $GL(E)$.

Exemples 1.1

1. *Un groupe diédral de type $\mathcal{D}_{2n}$ est isomorphe au sous-groupe de $GL_2(\mathbb{R})$ engendré par $R=\begin{pmatrix}\cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right)\\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right)\end{pmatrix}$ et $S=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, ce qui nous donne une représentation de degré 2 de $\mathcal{D}_{2n}$ (voir le paragraphe* **??**).
2. *Pour G fini et E de dimension $\operatorname{card}(G)$, en notant $\mathcal{B}=(e_k)_{k\in G}$ une base de E, on définit une représentation de G dans E en posant $\rho(g)(e_k)=e_{gk}$ pour tout $(g,k)\in G^2$. C'est la représentation régulière de G sur E.*
3. *Si $G=\mathfrak{S}_n$ est le groupe symétrique d'ordre n et E est de dimension n, en désignant par $\mathcal{B}=(e_k)_{1\leq k\leq n}$ une base de E, on définit une représentation de $\mathfrak{S}_n$ dans E en posant $\rho(\sigma)(e_k)=e_{\sigma(k)}$ pour tous $\sigma\in\mathfrak{S}_n$ et $k\in\{1,\cdots,n\}$. C'est la représentation de G sur E par permutation. La trace de $\rho(\sigma)$ est le nombre de points fixes de la permutation σ.*
4. *Si $G=\langle a\rangle=\left\{e,a,\cdots,a^{m-1}\right\}$ est un groupe cyclique d'ordre m, on se donne un isomorphisme u_0 de E et on définit l'application $\rho:G\to GL(E)$ par :*

   $$\forall k\in\{0,\cdots,m-1\},\ \rho\left(a^k\right)=u_0^k$$

   C'est une représentation de G sur E si, et seulement si, on a $u_0^m=Id_E$. En effet si ρ est une représentation, on a alors $u_0^m=\rho(a^m)=\rho(e)=Id_E$. Réciproquement, si $u_0^m=Id_E$, on a alors pour tous j,k compris entre 0 et $m-1$:

   $$\rho\left(a^ja^k\right)=\rho\left(a^{j+k}\right)=u_0^{j+k}=u_0^ju_0^k=\rho\left(a^j\right)\rho\left(a^k\right)\ \text{ si } j+k\leq m-1$$

   $$\begin{aligned}\rho\left(a^ja^k\right)&=\rho\left(a^{j+k-m}a^m\right)=\rho\left(a^{j+k-m}\right)\\&=u_0^{j+k-m}=u_0^{j+k}=u_0^ju_0^k=\rho\left(a^j\right)\rho\left(a^k\right)\ \text{ si } m\leq j+k\leq 2m-2\end{aligned}$$

   et ρ est bien une représentation.
5. *Soient $((\rho_i,E_i))_{1\leq i\leq p}$ une famille de représentations du groupe G dans des $\mathbb{K}$-espaces vectoriels $E_1,\cdots,E_p$ avec $p\geq 2$. On définit une représentation de G dans la somme directe $E=\bigoplus_{i=1}^{p}E_i$ en posant :*

   $$\forall g\in G,\ \forall(x_1,\cdots,x_p)\in\prod_{i=1}^{p}E_i,\ \rho(g)\left(\sum_{i=1}^{p}x_i\right)=\sum_{i=1}^{p}\rho_i(g)(x_i)$$

En effet, comme $\rho_i(g) \in GL(E_i)$ *pour* $1 \leq i \leq p$, *on a* $\rho(g) \in \mathcal{L}(E)$. *L'égalité* $\sum_{i=1}^{p} \rho_i(g)(x_i) = 0$ *équivaut à* $\rho_i(g)(x_i) = 0$ *pour tout* i *compris entre* 1 *et* p, *soit à* $x_i = 0$ *puisque chaque* $\rho_i(g)$ *est un isomorphisme, donc* $\rho(g) \in GL(E)$ *et on a bien une représentation. On dit que* (ρ, E) *est la somme directe des représentations* (ρ_i, E_i), *ce que l'on note* $(\rho, E) = \left(\bigoplus_{i=1}^{p} \rho_i, \bigoplus_{i=1}^{p} E_i\right)$. *Dans le cas où tous les* E_i *sont de dimension finie, en désignant par* $\mathcal{B}_i$ *une base de* E_i, *pour tout* $g \in G$, *la matrice de* $\rho(g)$ *dans la base* $\bigcup_{i=1}^{p} \mathcal{B}_i$ *de* E *est la matrice diagonale par blocs* $R(g) = \operatorname{diag}(R_1(g), \cdots, R_p(g))$, *où* $R_i(g)$ *est la matrice de* $\rho_i(g)$ *dans* $\mathcal{B}_i$.

Définition 1.2. *Si* (ρ, E) *est une représentation de* G, *on dit alors que* $\ker(\rho) = \{g \in G \mid \rho(g) = Id_E\}$ *est le noyau de la représentation. La représentation est dite fidèle si son noyau est réduit à l'élément neutre de* G.

Exemples 1.2

1. *Si* G *est d'ordre* n *et* E *de dimension* n, *une représentation régulière de* G *dans* E *(exemple 2) est fidèle. En effet si* g *est dans le noyau de* ρ, *on alors* $e_{gk} = \rho(g)(e_k) = e_k$ *pour tout* $k \in G$, *donc* $gk = k$ *pour tout* $k \in G$ *et* $g = e$.
2. *Si* G *est le groupe* $\mathcal{S}_n$ *des permutations de* $\{1, \cdots, n\}$, *l'application* ρ *qui associe à toute permutation* $\sigma \in \mathcal{S}_n$ *la matrice de passage* $R(\sigma)$ *de la base canonique* $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ *de* $\mathbb{K}^n$ *à la base* $\mathcal{B}_\sigma = \left(e_{\sigma(j)}\right)_{1 \leq j \leq n}$ *est un morphisme de groupes injectif de* $\mathcal{S}_n$ *dans* $GL_n(\mathbb{K})$, *c'est donc une représentation fidèle de* $\mathcal{S}_n$.
3. *Soient* $G = \langle a \rangle$ *un groupe cyclique d'ordre* m, $u_0 \in GL(E)$ *tel que* $u_0^m = Id_E$ *et* $\rho : G \to GL(E)$ *la représentation définie par* $\rho\left(a^k\right) = u_0^k$ *pour tout* k *compris entre* 0 *et* $m - 1$ *(exemple 4). Si* u_0 *est d'ordre* m, *cette représentation est alors fidèle. En effet, si* $a^k \in \ker(\rho)$ *avec* k *compris entre* 0 *et* $m - 1$, *on a alors* $u_0^k = Id_E$ *et nécessairement* $k = 0$, *donc* $\ker(\rho) = \{e\}$ *et* ρ *est fidèle. Sinon, l'ordre* r *de* u_0 *est un diviseur strict de* m, *soit* $r \in \{1, \cdots, m-1\}$ *et* $a^r \in \ker(\rho)$ *avec* $a^r \neq e$, *donc* ρ *n'est pas fidèle.*

1.2 Représentations irréductibles

Définition 1.3. *Si* (ρ, E) *est une représentation de* G, *on dit alors qu'un sous-espace vectoriel* F *de* E *est* G*-invariant (ou stable par* G*) si* F *est stable par tous les* $\rho(g)$, *ce qui signifie que* $\rho(g)(F) \subset F$ *pour tout* $g \in G$.

Les sous-espaces $\{0\}$ et E sont toujours G-invariant.

Si F est un sous-espace vectoriel de E de dimension finie qui est G-invariant, on a alors $\rho(g)(F) = F$ puisque $\rho(g)$ est un isomorphisme.

Si F est un sous-espace vectoriel de E qui est G-invariant, la représentation $\rho : G \to GL(E)$ induit alors une représentation $\rho' : G \to GL(F)$. On dit alors que ρ' est une sous-représentation de ρ.

Définition 1.4. *Si (ρ, E) est une représentation de G, on dit alors que $E^G = \{x \in E \mid \forall g \in G,\ \rho(g)(x) = x\}$ est l'ensemble des points fixes de G dans E.*

Pour tous x, y dans E^G, $\lambda \in \mathbb{K}$ et $g \in G$, on a :

$$\rho(g)(\lambda x + y) = \lambda \rho(g)(x) + \rho(g)(y) = \lambda x + y$$

donc E^G est un sous-espace vectoriel de E qui est G-invariant.

Définition 1.5. *On dit qu'une représentation de G dans E est irréductible (ou simple) si E n'est pas réduit au vecteur nul et les seuls sous-espaces G-invariants sont $\{0\}$ et E.*

Exemples 1.3

1. *Si G est d'ordre n et E de dimension n, une représentation régulière de G dans E (exemple 2) n'est pas irréductible. En effet, pour $x = \sum_{k \in G} e_k$ et tout $g \in G$, on a $\rho(g)(x) = \sum_{k \in G} \rho(g)(e_k) = \sum_{k \in G} e_{gk} = \sum_{h \in G} e_h = x$ puisque l'application $k \mapsto gk$ est une permutation de G. Donc la droite vectorielle $D = \mathbb{K}x$ dirigée par x est G-invariante non triviale. La restriction de ρ à D est la représentation triviale puisque $\rho(g)(x) = x$ pour tout $g \in G$.*
2. *Reprenant l'exemple 4 avec $\mathbb{K} = \mathbb{C}$ et E de dimension finie, comme $u_0^m = Id_E$, l'endomorphisme u_0 est annulé par le polynôme $X^m - 1$ qui est scindé à racines simples dans $\mathbb{C}[X]$, il est donc diagonalisable. Désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E formé de vecteurs propres de u_0, $\mathcal{B}$ est aussi une base de vecteurs propres de $\rho(a^k) = u_0^k$ pour tout k compris entre 0 et $m-1$, donc chaque droite vectorielle $E_i = \mathbb{C}e_i$, pour i compris entre 1 et n, est G-invariante. Donc cette représentation de G n'est pas irréductible.*

Définition 1.6. *Soient E, F deux $\mathbb{K}$-espaces vectoriels et (ρ, E), (σ, F) deux représentations de G. On dit que $u \in \mathcal{L}(E, F)$ est G-linéaire (ou que c'est un G-morphisme, ou que c'est un opérateur d'entrelacement) si on a $u \circ \rho(g) = \sigma(g) \circ u$ pour tout $g \in G$. Si de plus u est bijective, on dit alors que c'est un G-isomorphisme ou que les représentations sont équivalentes.*

Dire que $u \in \mathcal{L}(E, F)$ est G-linéaire se traduit aussi par $\sigma(g) \circ u \circ \rho\left(g^{-1}\right) = u$ pour tout $g \in G$.

Dire les représentations (ρ, E) et (σ, F) sont équivalentes revient à dire qu'il existe un isomorphisme u de E sur F tel que $\rho(g) = u^{-1} \circ \sigma(g) \circ u$ pour tout $g \in G$ et dans le cas de la dimension finie, cela signifie qu'il existe une matrice

inversible P telle que $R(g) = P^{-1}S(g)P$ pour tout $g \in G$ (les matrices $R(g)$, de $\rho(g)$ dans une base de E, et $S(g)$, de $\sigma(g)$ dans une base de F, sont semblables).

On note $\mathcal{L}_G(E,F)$ le sous-espace vectoriel de $\mathcal{L}(E,F)$ constitué des applications G-linéaires.

Lemme 1.1 *Soient (ρ, E) et (σ, F) deux représentations du même groupe G dans des $\mathbb{K}$-espaces vectoriels E et F.*

1. *L'application τ qui associe à $g \in G$ l'isomorphisme $\tau(g)$ de $\mathcal{L}(E,F)$ défini par $\tau(g)(u) = \sigma(g) \circ u \circ \rho\left(g^{-1}\right)$ pour tout $u \in \mathcal{L}(E,F)$ est une représentation de G dans $\mathcal{L}(E,F)$. Si E et F sont de dimension finie, cette représentation est de degré $\deg(\rho, E)\deg(\sigma, F)$.*
2. *L'espace des points fixes de G dans cette représentation $(\tau, \mathcal{L}(E,F))$ est l'espace des applications G-linéaires, soit $\mathcal{L}(E,F)^G = \mathcal{L}_G(E,F)$.*

Preuve.

1. Pour tout $g \in G$ et tout $u \in \mathcal{L}(E,F)$, on a $\rho\left(g^{-1}\right) \in GL(E)$ et $\sigma(g) \in GL(F)$, donc $\tau(g)(u) = \sigma(g) \circ u \circ \rho\left(g^{-1}\right) \in \mathcal{L}(E,F)$. Pour tous scalaires λ, μ et tous morphismes u, v dans $\mathcal{L}(E,F)$, on a :
$$\tau(g)(\lambda u + \mu v) = \sigma(g) \circ (\lambda u + \mu v) \circ \rho\left(g^{-1}\right) = \lambda\tau(g)(u) + \mu\tau(g)(v)$$
donc $\tau(g)$ est bien une application linéaire de $\mathcal{L}(E,F)$ dans $\mathcal{L}(E,F)$. Pour u dans $\mathcal{L}(E,F)$, on a $\tau(e)(u) = \sigma(e) \circ u \circ \rho\left(e^{-1}\right) = u$, donc $\tau(e) = Id_{\mathcal{L}(E,F)}$. Pour g, h dans G et u dans $\mathcal{L}(E,F)$, on a :
$$\begin{aligned}\tau(gh)(u) &= \sigma(gh) \circ u \circ \rho\left(h^{-1}g^{-1}\right) = \sigma(g) \circ \left(\sigma(h) \circ u \circ \rho\left(h^{-1}\right)\right) \circ \rho\left(g^{-1}\right) \\ &= \sigma(g) \circ (\tau(h)(u)) \circ \rho\left(g^{-1}\right) = \tau(g)(\tau(h)(u))\end{aligned}$$
donc $\tau(gh) = \tau(g) \circ \tau(h)$ et $\tau(g)$ est inversible d'inverse $\tau\left(g^{-1}\right)$. En définitive, τ est bien un morphisme de groupes de G dans $GL(\mathcal{L}(E,F))$ et $(\tau, \mathcal{L}(E,F))$ est bien une représentation de G. Si E et F sont de dimension finie, cette représentation est alors de degré égal à $\dim(\mathcal{L}(E,F)) = \deg(\rho, E)\deg(\sigma, F)$.
2. On a :
$$\begin{aligned}\mathcal{L}(E,F)^G &= \{u \in \mathcal{L}(E,F) \mid \forall g \in G,\ \tau(g)(u) = u\} \\ &= \left\{u \in \mathcal{L}(E,F) \mid \forall g \in G,\ \sigma(g) \circ u \circ \rho\left(g^{-1}\right) = u\right\} = \mathcal{L}_G(E,F)\end{aligned}$$

□

Lemme 1.2 *Soient E, F deux $\mathbb{K}$-espaces vectoriels, (ρ, E), (σ, F) deux représentations de G et $u \in \mathcal{L}_G(E,F)$. Les espaces vectoriels $\ker(u)$ et $\mathrm{Im}(u)$ sont G-invariants dans E et F respectivement.*

Preuve. Pour tout $g \in G$ et tout $x \in \ker(u)$, on a :
$$u(\rho(g)(x)) = u \circ \rho(g)(x) = \sigma(g) \circ u(x) = \sigma(g)(u(x)) = \sigma(g)(0) = 0$$
donc $\rho(g)(x) \in \ker(u)$. Le sous-espace $\ker(u)$ est donc g-invariant dans E. Pour tout $g \in G$ et tout $y = u(x) \in \mathrm{Im}(u)$, on a :
$$\sigma(g)(y) = \sigma(g) \circ u(x) = u \circ \rho(g)(x) = u(\rho(g)(x)) \in \mathrm{Im}(u)$$
Le sous-espace $\mathrm{Im}(u)$ est donc G-invariant dans F. □

Lemme 1.3 (Schur) *Soient E, F deux $\mathbb{K}$-espaces vectoriels et (ρ, E), (σ, F) deux représentations irréductibles de G.*

1. *Si E et F ne sont pas isomorphes, on a alors $\mathcal{L}_G(E,F) = \{0\}$.*
2. *Si $\mathbb{K}$ est algébriquement clos et E, F sont isomorphes et de dimension finie, l'espace $\mathcal{L}_G(E,F)$ est alors de dimension 1 sur $\mathbb{K}$ (c'est donc un corps).*

Preuve.

1. Supposons qu'il existe une application G-linéaire $u \in \mathcal{L}_G(E,F)$ non nulle. Comme (ρ, E) est irréductible et $\ker(u)$ est G-invariant dans E distinct de E, on a $\ker(u) = \{0\}$, donc u est injective. Comme (σ, F) est irréductible et $\mathrm{Im}(u)$ est G-invariant dans F non réduit à $\{0\}$, on a $\mathrm{Im}(u) = F$, donc u est surjective et c'est un isomorphisme. On en déduit que $\mathcal{L}_G(E,F) = \{0\}$ si E et F ne sont pas isomorphes.
2. Le corps $\mathbb{K}$ étant algébriquement clos et $E \backsimeq F$ de dimension finie, toute application G-linéaire $u \in \mathcal{L}_G(E,F)$ identifiée à un endomorphisme de E admet une valeur propre $\lambda \in \mathbb{K}$ et le sous-espace propre $E_\lambda = \ker(u - \lambda Id_E)$ est G-invariant dans E (car $u - \lambda Id_E \in \mathcal{L}_G(E,E)$), non réduit au vecteur nul, c'est donc E tout entier si (ρ, E) est irréductible, ce qui signifie que u est une homothétie. On a donc $\mathcal{L}_G(E,F) \backsimeq \mathbb{K}$. On peut aussi vérifier que $\mathcal{L}_G(E,F)$ est un anneau dont tous les éléments non nuls sont inversibles, c'est donc un corps.

□

Théorème 1.1.

Soient G fini, E, F deux $\mathbb{K}$-espaces vectoriels, (ρ, E), (σ, F) deux représentations de G, $u \in \mathcal{L}(E,F)$ et $\widehat{u} = \dfrac{1}{\mathrm{Card}(G)} \displaystyle\sum_{g \in G} \sigma(g) \circ u \circ \rho\left(g^{-1}\right)$.

1. *$\widehat{u}$ est un G-morphisme de E dans F.*
2. *Si les représentations (ρ, E) et (σ, F) sont irréductibles et non G-isomorphes, on a alors $\widehat{u} = 0$.*
3. *Si $\mathbb{K}$ est algébriquement clos et $(\rho, E) = (\sigma, F)$ est irréductible de degré fini, on a alors $\widehat{u} = \dfrac{\mathrm{Tr}(u)}{\dim(E)} Id_E$ (homothétie de rapport $\dfrac{\mathrm{Tr}(u)}{\dim(E)}$).*

Preuve.

1. Pour tout $h \in G$, on a :

$$\begin{aligned}\sigma(h) \circ \widehat{u} \circ \rho\left(h^{-1}\right) &= \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \sigma(hg) \circ u \circ \rho\left((hg)^{-1}\right) \\ &= \frac{1}{\mathrm{Card}(G)} \sum_{k \in G} \sigma(k) \circ u \circ \rho\left(k^{-1}\right) = \widehat{u}\end{aligned}$$

du fait que l'application $k \mapsto g = h^{-1}k$ réalise une bijection de G sur lui même. Donc $\widehat{u} \in \mathcal{L}_G(E,F)$.

2. C'est une conséquence immédiate du lemme de Schur qui nous dit que E et F sont G-isomorphes si $\widehat{u} \in \mathcal{L}_G(E,F)$ est non nulle.
3. Pour $\mathbb{K}$ algébriquement clos, $E = F$ de dimension finie et ρ irréductible, le lemme précédent nous dit que $\mathcal{L}_G(E,E)$ est de dimension 1, il existe donc $\lambda \in \mathbb{K}$ tel que $\widehat{u} = \lambda Id_E$ et $\mathrm{Tr}(\widehat{u}) = \lambda \dim(E)$, avec :

$$\mathrm{Tr}(\widehat{u}) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Tr}\left(\sigma(g) \circ u \circ \rho\left(g^{-1}\right)\right) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Tr}(u) = \mathrm{Tr}(u)$$

ce qui donne bien $\lambda = \dfrac{\mathrm{Tr}(u)}{\dim(E)}$.

□

Le lemme qui suit nous dit que, sur un corps algébriquement clos, tout sous-espace G-invariant d'une représentation de degré fini d'un groupe fini admet un supplémentaire G-invariant.

Lemme 1.4 *On suppose que le groupe G est fini. On se donne une représentation (ρ, E) de G dans E, F un sous-espace vectoriel G-invariant de E et $\pi \in \mathcal{L}(E)$ un projecteur d'image F. L'application $\widehat{\pi} = \dfrac{1}{\mathrm{Card}(G)} \displaystyle\sum_{g \in G} \rho(g) \circ \pi \circ \rho\left(g^{-1}\right) \in \mathcal{L}_G(E,E)$ est un projecteur d'image F et $E = F \oplus H$, où H est un sous-espace vectoriel G-invariant de E.*

Preuve. On a vu avec le théorème précédent que $\widehat{\pi} \in \mathcal{L}_G(E,E)$. Pour tout $x \in E$ et $g \in G$, on a $\pi\left(\rho\left(g^{-1}\right)(x)\right) \in F$ et $\rho(g)\left(\pi\left(\rho\left(g^{-1}\right)(x)\right)\right) \in F$ puisque F est G-invariant, on a donc $\widehat{\pi}(x) \in F$, c'est-à-dire que $\widehat{\pi}$ est à valeurs dans F. D'autre part, pour tout $x \in F$, on a $\rho\left(g^{-1}\right)(x) \in F$ (F est G-invariant) donc $\pi\left(\rho\left(g^{-1}\right)(x)\right) = \rho\left(g^{-1}\right)(x) = \rho(g)^{-1}(x)$ et $\rho(g)\left(\pi\left(\rho\left(g^{-1}\right)(x)\right)\right) = x$. On a donc $\widehat{\pi}(x) = x$ pour tout $x \in F$ et $\mathrm{Im}(\widehat{\pi}) \subset F$, ce qui entraîne que $\widehat{\pi}$ est un projecteur d'image F. On a alors $E = \mathrm{Im}(\widehat{\pi}) \oplus \ker(\widehat{\pi}) = F \oplus H$, avec $H = \ker(\widehat{\pi})$ qui est G-invariant. □

Théorème 1.2. Maschke

On suppose que G est fini, que $\mathbb{K}$ est algébriquement clos et que (ρ, E) est une représentation de G dans E de degré fini. Dans ce cas, (ρ, E) est somme directe de sous-représentations irréductibles, c'est-à-dire qu'il existe des sous-espaces G-invariants et irréductibles $E_1, \cdots, E_p$ de E tels que $E = \displaystyle\bigoplus_{i=1}^{p} E_i$.

Preuve. On procède par récurrence sur le degré de la représentation. En dimension 1 toute représentation de G est irréductible. En supposant le résultat acquis pour les représentations de G de dimension $n \geq 1$, on se donne une représentation $\rho : G \to GL(E)$ de degré $n+1$. Si ρ est irréductible, c'est terminé, sinon il existe des sous-espaces vectoriels de E qui sont G-invariant et distincts de $\{0\}$ et de E. En désignant par F un tel sous-espace de dimension minimale, ce sous-espace G-invariant est irréductible et le lemme précédent nous dit qu'il admet un

supplémentaire H qui est G-invariant et distincts de $\{0\}$ et de E. Il suffit alors d'appliquer l'hypothèse de récurrence à $\rho : G \to GL(H)$ pour conclure. □

1.3 Caractères des groupes finis

Pour ce paragraphe et les suivants, le groupe G est fini et les espaces vectoriels considérés sont de dimension finie.

Si $\mathbb{K} = \mathbb{C}$ et G est commutatif, une représentation irréductible de G dans E est nécessairement de degré 1 (exercice 1.3), donc $GL(E)$ est isomorphe au groupe multiplicatif $\mathbb{K}^*$ et il existe une application $\chi : G \to \mathbb{K}^*$ telle que $\rho(g) = \chi(g) Id_E$ pour tout $g \in G$ et $\chi(g)$ est la trace de $\rho(g)$.

Pour G fini, non nécessairement commutatif, on donne la définition suivante.

Définition 1.7. *Si (ρ, E) est une représentation de G, son caractère est l'application $\chi_\rho : G \to \mathbb{K}$ définie par $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ pour tout $g \in G$.*

Définition 1.8. *On dit qu'une fonction $\chi : G \to \mathbb{K}$ est un caractère [resp. un caractère irréductible] de G s'il existe une représentation [resp. une représentation irréductible] (ρ, E) de G telle que $\chi = \chi_\rho$.*

On notera simplement χ pour χ_ρ quand la représentation est fixée.

Exemple 1.1 *Le caractère de la représentation triviale $\rho : g \mapsto Id_E$ est la fonction constante $\chi : g \mapsto n$.*

Des propriétés de la trace, on déduit facilement les résultats suivant.

Théorème 1.3.

Soient (ρ, E) une représentation de G et $\chi_\rho : G \to \mathbb{K}$ son caractère. On a :

1. *$\chi_\rho(e) = \deg(\rho, E) = \dim(E)$ (toutes les représentations de G de même caractère χ, ont le même degré $\chi(e)$) ;*
2. *pour tous g, h dans G, $\chi_\rho(gh) = \chi_\rho(hg)$ et $\chi_\rho\left(ghg^{-1}\right) = \chi_\rho(h)$ (χ_ρ est constant sur chaque classe de conjugaison de G) ;*
3. *si (ρ, E) est somme directe de $p \geq 2$ représentations de G, son caractère est alors la somme des caractères correspondants.*

Preuve.

1. On a $\chi_\rho(e) = \mathrm{Tr}(\rho(e)) = \mathrm{Tr}(Id_E) = \dim(E)$.
2. Pour g, h dans G, on a :

$$\chi_\rho(gh) = \mathrm{Tr}(\rho(gh)) = \mathrm{Tr}(\rho(g) \circ \rho(h)) = \mathrm{Tr}(\rho(h) \circ \rho(g)) = \chi_\rho(hg)$$

et $\chi_\rho\left(ghg^{-1}\right) = \chi\left(hg^{-1}g\right) = \chi(h)$.

3. Si $(\rho, E) = \left(\bigoplus_{i=1}^{p}\rho_i, \bigoplus_{i=1}^{p}E_i\right)$, en désignant par $\mathcal{B}_i$ une base de E_i, pour tout $g \in G$, la matrice de $\rho(g)$ dans la base $\bigcup_{i=1}^{p}\mathcal{B}_i$ de E est la matrice diagonale par blocs $R(g) = \operatorname{diag}(R_1(g), \cdots, R_p(g))$, où $R_i(g)$ est la matrice de $\rho_i(g)$ dans $\mathcal{B}_i$ et on a $\chi_\rho(g) = \operatorname{Tr}(R(g)) = \sum_{i=1}^{p}\operatorname{Tr}(R_i(g)) = \sum_{i=1}^{p}\chi_{\rho_i}(g)$.

□

Théorème 1.4.

Deux représentations de G équivalentes, ont même caractère.

Preuve. Si les représentations (ρ, E) et (σ, F) de G sont équivalentes, il existe alors un isomorphisme u de E sur F tel que $\rho(g) = u^{-1} \circ \sigma(g) \circ u$ pour tout $g \in G$ et on a $\operatorname{Tr}(\rho(g)) = \operatorname{Tr}(\sigma(g))$ pour tout $g \in G$. Donc $\chi_\rho = \chi_\sigma$. □

Nous verrons plus loin que la réciproque du théorème précédent est vraie.

Théorème 1.5.

On suppose que $\mathbb{K} = \mathbb{C}$ et on se donne une représentation (ρ, E) de G de caractère $\chi : G \to \mathbb{C}$.

1. *Si $g \in G$ est d'ordre r, $\chi(g)$ est alors somme de n racines r-ièmes de l'unité.*
2. *Pour tout $g \in G$, on a $\chi\left(g^{-1}\right) = \overline{\chi(g)}$ et $|\chi(g)| \leq \chi(e) = \dim(E)$.*
3. *Le noyau de (ρ, E) est $\ker(\rho) = \{g \in G \mid \chi(g) = \chi(e)\}$.*

Preuve.

1. Si $g \in G$ est d'ordre $r \geq 1$, l'isomorphisme $\rho(g)$ est diagonalisable et ses valeurs propres $\lambda_1, \cdots, \lambda_n$ sont des racines r-ièmes de l'unité (exercice 1.2), donc $\chi(g) = \operatorname{Tr}(\rho(g)) = \sum_{i=1}^{n}\lambda_i$ est somme de n racines r-ièmes de l'unité.
2. On a $|\lambda_i| = 1$ pour tout i compris entre 1 et n et les $\overline{\lambda_i} = \lambda_i^{-1}$ sont les valeurs propres de $\rho\left(g^{-1}\right) = \rho(g)^{-1}$, donc $|\chi(g)| \leq \sum_{i=1}^{n}|\lambda_i| = n = \dim(E) = \chi(e)$ et $\chi\left(g^{-1}\right) = \operatorname{Tr}\left(\rho\left(g^{-1}\right)\right) = \sum_{i=1}^{n}\lambda_i^{-1} = \sum_{i=1}^{n}\overline{\lambda_i} = \overline{\chi(g)}$.
3. Pour tout $g \in \ker(\rho)$, on a $\rho(g) = Id_E = \rho(e)$ et $\chi(g) = \operatorname{Tr}(\rho(g)) = n = \chi(e)$. Réciproquement, soit $g \in G$ tel $\chi(g) = \chi(e)$. En désignant par $\lambda_1, \cdots, \lambda_n$ les valeurs propres de $\rho(g)$, on a $\sum_{k=1}^{n}\lambda_k = n$, les $\lambda_k = e^{i\theta_k}$ étant des racines de l'unité. On a alors $\sum_{k=1}^{n}\cos(\theta_k) = n$ et nécessairement $|\cos(\theta_k)| = 1$ pour tout k

(sinon $n \leq \sum_{k=1}^{n} |\cos(\theta_k)| < n$, ce qui est impossible), soit $\lambda_k = \pm 1$ pour tout k et l'égalité $\sum_{k=1}^{n} \lambda_k = n$ impose $\lambda_k = 1$ pour tout k compris entre 1 et n (sinon, en séparant les -1 des 1 dans la somme, on aboutit à $p = n+q$ avec $0 \leq p \leq n-1$ et $1 \leq q \leq n$, ce qui est impossible). L'endomorphisme diagonalisable $\rho(g)$ a donc toutes ses valeurs propres égales à 1, c'est donc Id_E et $g \in \ker(\rho)$.

□

Définition 1.9. *Si (ρ, E) est une représentation de G, sa moyenne est l'application linéaire définie par* $\mu = \dfrac{1}{\mathrm{Card}(G)} \sum_{g \in G} \rho(g)$.

Lemme 1.5 *Soient (ρ, E) une représentation de G et μ sa moyenne.*

1. *μ est un projecteur.*
2. $E^G = \mathrm{Im}(\mu) = \ker(\mu - Id_E)$.
3. $\mathrm{Tr}(\mu) = \dim\left(E^G\right) = \dfrac{1}{\mathrm{Card}(G)} \sum_{g \in G} \chi(g)$.

Preuve.

1. Pour tout $g \in G$, on a :

$$\rho(g) \circ \mu = \frac{1}{\mathrm{Card}(G)} \sum_{h \in G} \rho(g) \circ \rho(h) = \frac{1}{\mathrm{Card}(G)} \sum_{h \in G} \rho(gh)$$

et du fait que l'application $k \mapsto h = g^{-1}k$ est une permutation de G, on déduit que $\rho(g) \circ \mu = \dfrac{1}{\mathrm{Card}(G)} \sum_{k \in G} \rho(k) = \mu$. Il en résulte que $\mu \circ \mu = \mu$, c'est-à-dire que μ est un projecteur.

2. Avec $(\mu - Id_E) \circ \mu = 0$, on déduit que $\mathrm{Im}(\mu) \subset \ker(\mu - Id_E)$ et du fait que pour tout $x \in \ker(\mu - Id_E)$, on a $x = \mu(x) \in \mathrm{Im}(\mu)$, on déduit l'égalité $\mathrm{Im}(\mu) = \ker(\mu - Id_E)$. Pour $x \in E^G$, on a :

$$\mu(x) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \rho(g)(x) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} x = x$$

c'est-à-dire que $E^G \subset \ker(\mu - Id_E)$. Réciproquement si $x = \mu(x)$, on a alors $\rho(g)(x) = (\rho(g) \circ \mu)(x) = \mu(x) = x$ pour tout $g \in G$ et $x \in E^G$. On a donc bien $E^G = \mathrm{Im}(\mu) = \ker(\mu - Id_E)$.

3. Comme μ est un projecteur, on a $\mathrm{Tr}(\mu) = \dim(\mathrm{Im}(\mu)) = \dim\left(E^G\right)$ avec :

$$\mathrm{Tr}(\mu) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Tr}(\rho(g)) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \chi(g)$$

□

Lemme 1.6 *Si E, F sont des espaces vectoriels (de dimension finie), $f \in \mathcal{L}(E)$, $g \in \mathcal{L}(F)$ et $\varphi : \mathcal{L}(E,F) \to \mathcal{L}(E,F)$ est l'application linéaire définie par :*

$$\forall u \in \mathcal{L}(E,F),\ \varphi(u) = g \circ u \circ f$$

on a alors $\mathrm{Tr}(\varphi) = \mathrm{Tr}(f)\,\mathrm{Tr}(g)$.

Preuve. On se donne une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E, une base $\mathcal{B}' = (e'_i)_{1\leq i\leq n}$ une base de F et on note $\mathcal{B}'' = (u_{ij})_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}$ la famille d'applications linéaires de E dans F définie par :

$$\forall k \in \{1,\cdots,n\},\ u_{ij}(e_k) = \begin{cases} 0 \text{ si } k \neq i \\ e'_j \text{ si } k = i \end{cases}$$

(soit en désignant par $(e_i^*)_{1\leq i\leq n}$ la base duale de $\mathcal{B}$, $u_{ij}(x) = e_i^*(x)\,e'_j$). On vérifie facilement que cette famille est une base de $\mathcal{L}(E,F)$ (il y a $nm = \dim(\mathcal{L}(E,F))$ éléments et $\sum_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \alpha_{ij}u_{ij} = 0$ appliqué à e_k donne $\sum_{j=1}^{m}\alpha_{kj}e'_j = 0$ qui entraîne la nullité de tous les coefficients α_{kj}), toute application linéaire $u \in \mathcal{L}(E,F)$ s'écrivant $u = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \alpha_{ij}u_{ij}$, où les coefficients α_{ij} sont définis par $u(e_k) = \sum_{j=1}^{m}\alpha_{kj}e'_j$ pour tout $k \in \{1,\cdots,n\}$ (c'est-à-dire que $((\alpha_{ij})) = {}^tA$, où A est la matrice de u dans les bases $\mathcal{B}$ et $\mathcal{B}'$). Pour $1 \leq r \leq n$ et $1 \leq s \leq m$, on a $\varphi(u_{rs}) = \sum_{\substack{1\leq i\leq n\\ 1\leq j\leq m}} \alpha_{ij}^{(r,s)}u_{ij}$ et $\mathrm{Tr}(\varphi) = \sum_{\substack{1\leq r\leq n\\ 1\leq s\leq m}} \alpha_{rs}^{(r,s)}$. Avec $\varphi(u_{rs})(e_k) = \sum_{j=1}^{m}\alpha_{kj}^{(r,s)}e'_j$ et :

$$\varphi(u_{rs})(e_k) = (g\circ(u_{rs})\circ f)(e_k) = (g\circ(u_{rs}))\left(\sum_{i=1}^{n} a_{ik}e_i\right)$$

$$= g(a_{rk}e'_s) = a_{rk}\sum_{j=1}^{m} b_{js}e'_j$$

on déduit que $\alpha_{kj}^{(r,s)} = a_{rk}b_{js}$, ce qui donne $\mathrm{Tr}(\varphi) = \sum_{\substack{1\leq r\leq n\\ 1\leq s\leq m}} a_{rr}b_{ss} = \mathrm{Tr}(f)\,\mathrm{Tr}(g)$.

□

On note $\mathbb{K}^G$ l'espace vectoriel des applications de G dans $\mathbb{K}$. Cet espace vectoriel est de dimension $\mathrm{card}(G)$.

Pour toute fonction $v \in \mathbb{K}^G$, on note v^* la fonction définie par $v^*(g) = v\left(g^{-1}\right)$ pour tout $g \in G$ et on définit sur $\mathbb{K}^G$ la forme bilinéaire $\langle\cdot \mid \cdot\rangle$ par :

$$\forall (u,v) \in \mathbb{K}^G \times \mathbb{K}^G,\ \langle u \mid v\rangle = \frac{1}{\mathrm{Card}(G)}\sum_{g\in G} u(g)\,v^*(g)$$

Lemme 1.7 *La forme bilinéaire $\langle \cdot \mid \cdot \rangle$ est symétrique et non dégénérée sur $\mathbb{K}^G$.*

Preuve. L'application $g \mapsto g^{-1}$ étant une permutation de G et le corps $\mathbb{K}$ commutatif, on déduit que la forme bilinéaire $\langle \cdot \mid \cdot \rangle$ est symétrique. Si $u \in \mathbb{K}^G$ est telle que $\langle u \mid v \rangle = 0$ pour tout $v \in \mathbb{K}^G$, en prenant pour fonction v la fonction caractéristique du singleton $\left\{h^{-1}\right\}$, où h est quelconque dans G, on a, $0 = \langle u \mid v \rangle = \dfrac{1}{\operatorname{Card}(G)} u(h)$ et $u(h) = 0$, donc u est l'application nulle. La forme bilinéaire $\langle \cdot \mid \cdot \rangle$ est donc non dégénérée. □

Si $\mathbb{K} = \mathbb{C}$ et v est un caractère, on a alors $v^*(g) = v\left(g^{-1}\right) = \overline{v(g)}$ et :

$$\langle u \mid v \rangle = \frac{1}{\operatorname{Card}(G)} \sum_{g \in G} u(g) \overline{v(g)}$$

L'application $\langle \cdot \mid \cdot \rangle$ ainsi définie est un produit scalaire hermitien sur $\mathbb{K}^G$.

Théorème 1.6.

Soient (ρ, E), (σ, F) deux représentations de G et χ_ρ, χ_σ leurs caractères respectifs.

1. *Le caractère de la représentation associée $(\tau, \mathcal{L}(E,F))$ (voir le lemme 1.1) est $\chi_\tau = \chi_\rho^* \chi_\sigma$.*
2. *On a $\langle \chi_\rho \mid \chi_\sigma \rangle = \dim\left(\mathcal{L}_G(E,F)\right)$, où $\mathcal{L}_G(E,F)$ est l'espace des applications G-linéaires de E dans F ($\langle \chi_\rho \mid \chi_\sigma \rangle$ est donc un entier).*
3. *Si E n'est pas réduit au vecteur nul, on a alors $\langle \chi_\rho \mid \chi_\rho \rangle \in \mathbb{N}^*$.*
4. *Si les représentations (ρ, E) et (σ, F) sont irréductibles, on a alors :*

$$(\langle \chi_\rho \mid \chi_\sigma \rangle \geq 1) \Leftrightarrow ((\rho, E) \text{ et } (\sigma, F) \text{ sont équivalentes}) \Leftrightarrow (\chi_\rho = \chi_\sigma)$$

Preuve.

1. Pour tous g dans G et u dans $\mathcal{L}(E,F)$, on a $\tau(g)(u) = \sigma(g) \circ u \circ \rho\left(g^{-1}\right)$ et, en utilisant le lemme précédent :

$$\chi_\tau(g) = \operatorname{Tr}(\tau(g)) = \operatorname{Tr}\left(\rho\left(g^{-1}\right)\right) \operatorname{Tr}(\sigma(g)) = \chi_\rho\left(g^{-1}\right) \chi_\sigma(g)$$

   On a donc bien $\chi_\tau = \chi_\rho^* \chi_\sigma$.

2. On a :

$$\begin{aligned} \langle \chi_\rho \mid \chi_\sigma \rangle = \langle \chi_\sigma \mid \chi_\rho \rangle &= \frac{1}{\operatorname{Card}(G)} \sum_{g \in G} \chi_\rho\left(g^{-1}\right) \chi_\sigma(g) \\ &= \frac{1}{\operatorname{Card}(G)} \sum_{g \in G} \chi_\tau(g) = \dim\left(\mathcal{L}(E,F)^G\right) \end{aligned}$$

   et avec $\mathcal{L}(E,F)^G = \mathcal{L}_G(E,F)$, on déduit que $\langle \chi_\rho \mid \chi_\sigma \rangle = \dim\left(\mathcal{L}_G(E,F)\right)$.

3. En particulier, on a $\langle \chi_\rho \mid \chi_\rho \rangle = \dim\left(\mathcal{L}_G(E,E)\right) \in \mathbb{N}^*$ si E n'est pas réduit au vecteur nul puisque $\mathcal{L}_G(E,E)$ contient Id_E qui est non nulle.

4. Si $\langle \chi_\rho \mid \chi_\sigma \rangle \geq 1$, on a alors $\dim(\mathcal{L}_G(E,F)) \geq 1$ et le lemme de Schur, pour (ρ, E) et (σ, F) irréductibles, nous dit que les représentations sont équivalentes et en conséquence, elles ont même caractère (théorème 1.4). Si $\chi_\rho = \chi_\sigma$, on a alors $\langle \chi_\rho \mid \chi_\sigma \rangle = \langle \chi_\rho \mid \chi_\rho \rangle \geq 1$ puisque E n'est pas réduit au vecteur nul ((ρ, E) étant irréductible, on a $E \neq \{0\}$).

□

Avec les notations du théorème précédent, pour $\mathbb{K} = \mathbb{C}$, on a $\chi_\tau = \overline{\chi_\rho}\chi_\sigma$.

Pour $\mathbb{K}$ algébriquement clos et (ρ, E) irréductible on a vu que $\mathcal{L}_G(E,E)$ est de dimension 1 (lemme 1.3), donc $\langle \chi_\rho \mid \chi_\rho \rangle = 1$.

Le théorème précédent nous dit que si χ_ρ, χ_σ sont les caractères de deux représentations irréductibles, ils sont orthogonaux dans $\mathbb{K}^G$ pour la forme bilinéaire $\langle \cdot \mid \cdot \rangle$ si, et seulement si, $\chi_\rho \neq \chi_\sigma$.

Corollaire 1.1. *Si $\chi_1, \cdots, \chi_p$ sont des caractères irréductibles distincts de G, ils sont alors linéairement indépendants dans $\mathbb{K}^G$ et $p \leq \mathrm{Card}(G)$.*

Preuve. Si $\sum_{j=1}^{p} \lambda_j \chi_j = 0$, on a alors $0 = \sum_{j=1}^{p} \lambda_j \langle \chi_j \mid \chi_i \rangle = \lambda_i \langle \chi_i \mid \chi_i \rangle$ pour tout i compris entre 1 et p, compte tenu de l'orthogonalité des χ_j avec $\langle \chi_i \mid \chi_i \rangle > 0$, ce qui donne $\lambda_i = 0$. Les χ_i sont donc linéairement indépendants dans $\mathbb{K}^G$ qui est de dimension $\mathrm{Card}(G)$ et nécessairement $p \leq \mathrm{Card}(G)$. □

On a donc au plus $\mathrm{Card}(G)$ caractères irréductibles sur G.

1.4 Fonctions centrales

On suppose que le groupe G est fini et que $\mathbb{K} = \mathbb{C}$.

Définition 1.10. *On appelle fonction centrale de G dans $\mathbb{C}$ toute application $\varphi : G \to \mathbb{C}$ constante sur les classes de conjugaison de G, c'est-à-dire telle que $\varphi(ghg^{-1}) = \varphi(h)$ pour tous g, h dans G.*

Le point **2.** du théorème 1.3 nous dit qu'un caractère est une fonction centrale.

Une fonction $\varphi : G \to \mathbb{C}$ est centrale si, et seulement si, $\varphi(gk) = \varphi(kg)$ pour tous g, k dans G.

On désigne par $\mathcal{H}$ le sous-espace de $\mathbb{C}^G$ formé des fonctions centrales sur G et on définit sur $\mathcal{H}$ un produit hermitien en posant :

$$\forall (\varphi, \psi) \in \mathcal{H}^2,\ \langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g)$$

Lemme 1.8 *Si $\varphi \in \mathcal{H}$ et (ρ, E) est une représentation de G de caractère χ, l'application $\rho_\varphi \in \mathcal{L}(E)$ définie par $\rho_\varphi = \dfrac{1}{\mathrm{Card}(G)} \sum_{g \in G} \varphi(g^{-1}) \rho(g)$ est un G-morphisme de E et, si de plus la représentation (ρ, E) est irréductible, ρ_φ est alors une homothétie de rapport $\dfrac{\langle \varphi \mid \chi \rangle}{\dim(E)}$.*

Preuve. Pour tout $h \in G$, on a $\rho_\varphi \circ \rho(h) = \dfrac{1}{\mathrm{Card}(G)} \sum_{g \in G} \varphi\left(g^{-1}\right) \rho(gh)$ et comme l'application $k \mapsto g = hkh^{-1}$ est une permutation de G, cela s'écrit :

$$\begin{aligned}\rho_\varphi \circ \rho(h) &= \frac{1}{\mathrm{Card}(G)} \sum_{k \in G} \varphi\left(hk^{-1}h^{-1}\right) \rho(hk) \\ &= \rho(h) \circ \frac{1}{\mathrm{Card}(G)} \sum_{k \in G} \varphi\left(k^{-1}\right) \rho(k) = \rho(h) \circ \rho_\varphi\end{aligned}$$

si φ est une fonction centrale. On a donc $\rho_\varphi \in \mathcal{L}_G(E, E)$. Si de plus (ρ, E) est irréductible, le lemme de Schur nous dit alors que $\mathcal{L}_G(E, E)$ est de dimension 1 et ρ_φ est une homothétie, soit $\rho_\varphi = \lambda Id_E$ et :

$$\begin{aligned}\lambda &= \frac{\mathrm{Tr}(\rho_\varphi)}{\dim(E)} = \frac{1}{\dim(E)} \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \varphi\left(g^{-1}\right) \chi(g) \\ &= \frac{1}{\dim(E)} \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \overline{\varphi(g)} \chi(g) = \frac{\langle \varphi \mid \chi \rangle}{\dim(E)}\end{aligned}$$

□

On a vu que les caractères irréductibles de G forment un système orthonormé de l'espace des fonctions centrales (théorème 1.6) et donc, il y a au plus $\mathrm{Card}(G)$ caractères irréductibles sur G. En fait ils en forment une base.

Théorème 1.7.

Les caractères irréductibles de G forment une base orthonormée de l'espace $\mathcal{H}$ des fonctions centrales sur G et le nombre de ces caractères irréductibles (qui est la dimension de $\mathcal{H}$) est égal au nombre des classes de conjugaison de G.

Preuve. Soit $\mathcal{F}$ le sous-espace vectoriel de $\mathcal{H}$ engendré par tous les caractères irréductibles de G, $\chi_1, \cdots, \chi_p$. Comme ces caractères forment un système orthonormé, ils sont linéairement indépendants et pour montrer qu'ils forment une base de $\mathcal{H}$, il nous suffit de prouver que l'orthogonal de $\mathcal{F}$ est réduit à $\{0\}$. Si $\varphi \in \mathcal{H}$ est orthogonal à $\mathcal{F}$, on a alors $\langle \varphi \mid \chi \rangle = 0$ pour tout caractère irréductible et la fonction ρ_φ associée par le procédé du lemme précédent à un tel caractère est nulle. Si (ρ, E) est une représentation de G, elle s'écrit alors $(\rho, E) = \bigoplus_{j=1}^{r} (\rho_j, E_j)$, où les (ρ_j, E_j) sont des représentions irréductibles de G. En notant $\rho_{j,\varphi}$ l'application associée à φ et (ρ_j, E_j) par le procédé du lemme précédent, on a pour tout $x = \sum_{j=1}^{r} x_j$, avec $x_j \in E_j$, $\rho_\varphi(x) = \sum_{j=1}^{r} \rho_\varphi(x_j) = \sum_{j=1}^{r} \rho_{j,\varphi}(x_j) = 0$. On a donc $\rho_\varphi = 0$ pour toute représentation de G. En utilisant la représentation régulière de G, on a $\sum_{g \in G} \varphi\left(g^{-1}\right) \rho(g) = 0$, les $\rho(g)$, pour $g \in G$ étant linéairement indépendants dans $GL\left(\mathbb{C}^G\right)$ (en effet si $\sum_{g \in G} \lambda_g \rho(g) = 0$, on a alors $\sum_{g \in G} \lambda_g \rho(g)(e_1) = \sum_{g \in G} \lambda_g e_g = 0$ et

$\lambda_g = 0$ pour tout $g \in G$), ce qui nous donne $\varphi\left(g^{-1}\right) = 0$ pour $g \in G$, c'est-à-dire que $\varphi = 0$. Comme $\mathcal{H}$ est l'espace des fonctions constantes sur les classes de conjugaison de G, sa dimension p est égale au nombre de ces classes. □

Pour la suite de ce paragraphe, on note :

— p la dimension de l'espace $\mathcal{H}$ des fonctions centrales sur G ;

— $(\chi_1, \cdots, \chi_p)$ la base de $\mathcal{H}$ formée de tous les caractères irréductibles de G ;

— $\overline{g_1}, \cdots, \overline{g_p}$ toutes les classes de conjugaison de G.

On rappelle qu'une fonction centrale φ est constante sur chaque classe de conjugaison $\overline{g_i}$, cette valeur constante étant $\varphi(g_i)$.

Théorème 1.8.

Pour $1 \leq i, j \leq p$, on a :

$$\sum_{g \in G} \overline{\chi_i(g)} \chi_j(g) = \begin{cases} \operatorname{Card}(G) & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

$$\sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k(g_j) = \begin{cases} \dfrac{\operatorname{Card}(G)}{\operatorname{Card}(\overline{g_i})} & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Preuve. Les premières formules traduisent simplement le fait que la famille $(\chi_i)_{1 \leq i \leq p}$ est orthogonale. Pour tout entier i compris entre 1 et p, on désigne par δ_i la fonction caractéristique de $\overline{g_i}$. Ces fonctions δ_i étant des fonctions centrales, elles s'écrivent $\delta_i = \sum_{k=1}^{p} \lambda_k \chi_k$, avec :

$$\lambda_k = \langle \delta_i \mid \chi_k \rangle = \frac{1}{\operatorname{Card}(G)} \sum_{g \in G} \delta_i(g) \chi_k\left(g^{-1}\right) = \frac{1}{\operatorname{Card}(G)} \sum_{g \in \overline{g_i}} \chi_k\left(g^{-1}\right)$$

et pour tout $g = hg_ih^{-1}$ dans $\overline{g_i}$, on a $\chi_k\left(g^{-1}\right) = \chi_k\left(g_i^{-1}\right) = \overline{\chi_k(g_i)}$, donc $\lambda_k = \dfrac{1}{\operatorname{Card}(G)} \operatorname{Card}(\overline{g_i}) \overline{\chi_k(g_i)}$, soit $\delta_i = \dfrac{\operatorname{Card}(\overline{g_i})}{\operatorname{Card}(G)} \sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k$. On en déduit que $1 = \delta_i(g_i) = \dfrac{\operatorname{Card}(\overline{g_i})}{\operatorname{Card}(G)} \sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k(g_i)$, soit $\sum_{k=1}^{p} |\chi_k(g_i)|^2 = \dfrac{\operatorname{Card}(G)}{\operatorname{Card}(\overline{g_i})}$. Et pour $j \neq i$, on a $0 = \delta_i(g_j) = \frac{\operatorname{Card}(\overline{g_i})}{\operatorname{Card}(G)} \sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k(g_j)$, soit $\sum_{k=1}^{p} \overline{\chi_k(g_i)} \chi_k(g_j) = 0$.

□

Corollaire 1.2. *En désignant, pour tout i compris entre 1 et p, par (ρ_i, E_i) une représentation irréductible de G de caractère χ_i, on a :*

$$\sum_{k=1}^{p} (\dim(E_k))^2 = \operatorname{Card}(G)$$

Preuve. Prenant $g_i = g_j = e$, on a $\overline{g_i} = \{e\}$ et :

$$\sum_{k=1}^{p} (\dim(E_k))^2 = \sum_{k=1}^{p} |\chi_k(g_i)|^2 = \frac{\mathrm{Card}(G)}{\mathrm{Card}(\overline{g_i})} = \mathrm{Card}(G)$$

□

Corollaire 1.3. *Il y a p représentations irréductibles de G, à isomorphisme près. Précisément, en désignant, pour tout i compris entre 1 et p, par (ρ_i, E_i) une représentation irréductible de G de caractère χ_i, ces représentations sont non G-isomorphes et toute représentation irréductible de G est G-isomorphe à l'une des représentations (ρ_i, E_i).*

Preuve. Soit (ρ, E) une représentation irréductible de G. Son caractère χ_ρ est l'un des caractères de base χ_k, où k est compris entre 1 et r. On a donc $\langle \chi_\rho \mid \chi_\rho \rangle = 1$ et les représentations (ρ, E) et (ρ_k, E_k) sont équivalentes (théorème 1.6). Pour $1 \leq j \neq k \leq r$, on a $\chi_j \neq \chi_k$ et les les représentations (ρ_j, E) et (ρ_k, E_k) ne sont pas équivalentes. □

Théorème 1.9.

Soient (ρ, E), (ρ', E') deux représentations de G décomposées en sommes directes de représentations irréductibles :

$$(\rho, E) = \bigoplus_{j=1}^{m} (\tau_j, F_j) \text{ et } (\rho', E') = \bigoplus_{j=1}^{m'} (\tau'_j, F'_j)$$

Les trois assertions suivantes sont équivalentes :

1. *les représentations (ρ, E) et (ρ', E') sont équivalentes ;*
2. *$\chi_\rho = \chi_{\rho'}$ (les représentations ont même caractère) ;*
3. *$m = m'$ et il existe une permutation $\sigma \in \mathcal{S}_n$ telle que, pour tout j compris entre 1 et m, (τ'_j, F'_j) est équivalente à $(\tau_{\sigma(j)}, F_{\sigma(j)})$.*

Preuve. Pour tout i compris entre 1 et p, (ρ_i, E_i) est une représentation irréductible de G de caractère χ_i. En désignant, pour i compris entre 1 et p, par m_i [resp. m'_i] le nombre de composantes irréductibles (τ_j, F_j) de (ρ, E) [resp. (τ'_j, F'_j) de (ρ', E')] équivalentes à (ρ_i, E_i), on a $\chi_\rho = \sum_{i=1}^{p} m_i \chi_i$ et $\chi_{\rho'} = \sum_{i=1}^{p} m'_i \chi_i$ et tenant compte de l'orthonormalité des χ_i, on a :

$$m_i = \langle \chi_\rho \mid \chi_i \rangle, \; m'_i = \langle \chi_{\rho'} \mid \chi_i \rangle, \; (1 \leq i \leq p)$$

On sait déjà que si les représentations (ρ, E) et (ρ', E') sont équivalentes, elles ont alors même caractère. Si $\chi_\rho = \chi_{\rho'}$, on a alors $m_i = m'_i$ pour tout i compris entre 1 et p, donc $m = \sum_{i=1}^{p} m_i = m'$ et les représentations (ρ, E) et (ρ', E') sont

équivalentes à une même représentation $\bigoplus_{i=1}^{p}\bigoplus_{k=1}^{m_i}(\rho_k, E_k)$ ($\bigoplus_{k=1}^{m_i}(\rho_k, E_k) = \{0\}$ si $m_i = 0$) et en conséquence elles sont équivalentes. □

Avec les notations de la démonstration précédente, on dit que, pour i compris entre 1 et p, m_i est la multiplicité de (ρ_i, E_i) dans (ρ, E).

Corollaire 1.4. *Les caractères de G sont les fonctions centrales de la forme $\chi = \sum_{i=1}^{p} m_i\chi_i$, où les m_i sont des entiers naturel.*
Si χ est un caractère non nul de G, $\langle\chi \mid \chi\rangle$ est alors un entier naturel non nul qui vaut 1 si, et seulement si, χ et irréductible.

Preuve. Soit χ un caractère de G. On a vu que les m_i sont les composantes de $\chi \in \mathcal{H}$ dans la base orthonormée $(\chi_i)_{1\leq i\leq p}$, donc $\chi = \sum_{i=1}^{p} m_i\chi_i$ et $\langle\chi \mid \chi\rangle = \sum_{i=1}^{p} m_i^2$, c'est donc un entier naturel non nul si $\chi \neq 0$. Si χ et irréductible, c'est l'un des χ_i et $\langle\chi \mid \chi\rangle = 1$. Réciproquement si $\langle\chi \mid \chi\rangle = 1$, on a alors $\sum_{i=1}^{p} m_i^2 = 1$, donc tous les m_i sont nuls nuls, sauf un qui vaut 1 et χ et irréductible. □

1.5 Caractères des groupes abéliens finis

On suppose toujours que le groupe G est fini et que $\mathbb{K} = \mathbb{C}$.

Théorème 1.10.

Le groupe G est abélien si, et seulement si, tous ses caractères irréductibles sont de degré 1.

Preuve. Pour $\mathbb{K} = \mathbb{C}$ et G abélien fini, toute représentation irréductible de G est nécessairement de degré 1 (exercice 1.3). On a vu que le nombre de représentations irréductibles de G est égal au nombre p de classes de conjugaisons et notant $((\rho_i, E_i))_{1\leq i\leq p}$ la famille de ces représentations, on a $\sum_{k=1}^{p} (\dim(E_k))^2 = \mathrm{Card}(G)$. Dans le cas où G est commutatif, les classes de conjugaison sont réduites à un élément, donc $p = \mathrm{Card}(G)$ et nécessairement $\dim(E_k) = 1$ pour tout k compris entre 1 et p. □

On se propose de démontrer que tout groupe abélien fini est produit de groupes cycliques. Au paragraphe **??** on donne une autre démonstration de ce résultat.

Lemme 1.9 *Tout groupe abélien d'ordre p^α où p est un nombre premier est produit de groupes cycliques.*

Preuve. Soit G un groupe abélien d'ordre p^α. Si $x \neq 1 \in G$, x est d'ordre p^k avec $k \leq \alpha$. Si G admet un élément d'ordre p^α, alors il est cyclique. Sinon soit x_0 un élément d'ordre maximal $\beta < \alpha$. On a $x_1 = x_0^{p^{\beta-1}} \neq 1$ de sorte qu'il existe un

caractère χ de G tel que $\chi(x_1) \neq 1$ en effet, d'après ce qui précède, si $\chi(x_1) = 1$ pour tout caractère irréductible de G on a pour toute fonction f sur G :

$$f(1) = \sum_{\chi \in \hat{G}} < f, \chi > \chi(1) = \sum_{\chi \in \hat{G}} < f, \chi > \chi(x_1) = f(x_1)$$

il suffit alors de prendre $f = \delta_{x_1}$ pour obtenir une contradiction. Le nombre complexe $\chi(x_0)$ est une racine p^β-ième de l'unité et c'est une racine primitive puisque $\chi(x_1) \neq 1$. L'homomorphisme χ est surjectif et envoie x_0 (qui est d'ordre p^β) sur un générateur du groupe des racines p^β-ième de l'unité : le groupe H engendré par x_0 est cyclique d'ordre p^β. Si $y \in G$ est d'ordre p^γ avec $\gamma \leq \beta$, $\chi(y)$ est une racine de l'unité d'ordre p^γ c'est donc aussi une racine p^β-ième de l'unité : il existe donc $h \in H$ tel que $\chi(h) = \chi(y)$. Il en résulte que $\chi(h^{-1}y) = 1$ *i.e.* que $h^{-1}y \in N = \ker \chi$. Pour tout $y \in G$ il existe donc $h \in H$ et $k \in K = \ker \chi$ tels que $y = hk$. Comme $H \cap K = \{1\}$ on en déduit que G est produit direct de H et K(utiliser $(h, k) \in H \times K \mapsto hk$). Or K est un groupe abélien d'ordre strictement inférieur à celui de G. Une récurrence simple montre alors que G est produit de groupes cycliques (d'ordres p^{α_i}). □

On a $\prod p^{\alpha_i} = p^\alpha$ d'où $\alpha = \sum \alpha_i$. De plus deux groupes $\prod \frac{\mathbb{Z}}{p^{\alpha_i}\mathbb{Z}}$ et $\prod \frac{\mathbb{Z}}{p^{\alpha'_i}\mathbb{Z}}$ ne sont isomorphes que si (α_i) et (α'_i) donnent la même partition de l'entier α : le nombre de groupes abéliens d'ordre p^α deux à deux non isomorphes est donc égal à $p(\alpha)$. (décompositions de α en somme d'entiers $0 < n_1 \leq \cdots \leq n_p$). On a $p(4) = 5$, $p(5) = 7$, $p(6) = 11$, *etc ...* Ce nombre croît très vite et peut se calculer par récurrence (on a $P(n) \sim \frac{\exp(\pi\sqrt{\frac{2n}{3}})}{4n\sqrt{3}}$ d'après Hardy et Ramanujan). Il permet de calculer le nombre de groupes abéliens d'ordre p^n donc des groupes abéliens finis. Du point de vue des séries formelles on a $1 + \sum p(n)X^n = \prod_k \frac{1}{1 - X^k}$.

Théorème 1.11.

Tout groupe abélien fini est produit de groupes cycliques.

Preuve. Soit G un groupe abélien d'ordre $m \cdot n$ où m et n sont deux entiers premiers entre eux. Soit H l'ensemble des éléments de G dont l'ordre divise m et K celui des éléments dont l'ordre divise n. H et K sont des sous-groupes de G puisque si $x \in H$ est d'ordre k et $y \in H$ d'ordre ℓ leur produit est d'ordre $\text{ppcm}(k, \ell)$ (car G est abélien) ordre qui divise m. Le même raisonnement s'applique à K. Les entiers m et n étant premiers entre eux, Tout élément de $H \cap K$ est d'ordre 1 donc $H \cap K = \{1\}$. De plus, $\varphi : (H, K) \to G$ défini par $\varphi(h, k) = hk$ est un morphisme injectif de groupes. Montrons qu'il est surjectif : m et n étant premiers entre eux, il existe des entiers u et v tels que $um + vn = 1$ de sorte que si $g \in G$ on a $g^{um+vn} = (g^n)^u(g^m)^v$. Mais l'ordre de $(g^n)^u$ divise m d'où $g^{un} \in H$ et l'ordre de $(g^m)^v$ divise n et $g^{vm} \in K$. On a donc $G = H \times K$. Il suffit alors de raisonner par récurrence pour voir que tout groupe abélien fini s'écrit comme produit de groupes cycliques. □

1.6 Exercices

Exercice 1.1. *Soit (ρ, E) une représentation de G de degré fini. Montrer que l'application $\rho^* : G \to GL(E^*)$ définie par $\rho^*(g) = {}^t\left(\rho\left(g^{-1}\right)\right)$ pour tout $g \in G$ est une représentation de G sur E^* de même degré.*

Solution. Pour tout $g \in G$, on a $\rho\left(g^{-1}\right) \in GL(E)$ et en dimension finie, sa transposée est dans $GL(E^*)$. Pour tout $g \in G$ et tout $\ell \in E^*$, on a :

$$\rho^*(g)(\ell) = {}^t\rho\left(g^{-1}\right)(\ell) = \ell \circ \rho\left(g^{-1}\right) = \ell \circ \rho(g)^{-1}$$

et pour $h \in G$:

$$\begin{aligned}\rho^*(gh)(\ell) &= \ell \circ \rho(gh)^{-1} = \ell \circ (\rho(g) \circ \rho(h))^{-1} \\ &= \ell \circ \rho(h)^{-1} \circ \rho(g)^{-1} = (\rho^*(g) \circ \rho^*(h))(\ell)\end{aligned}$$

donc ρ^* est bien un morphisme de groupes de G dans $GL(E^*)$.

Exercice 1.2. *Soit (ρ, E) une représentation de G. Dans le cas où le groupe G est fini et E est un $\mathbb{C}$-espace vectoriel de dimension finie, montrer que chaque isomorphisme $\rho(g)$ est diagonalisable et que ses valeurs propres sont des racines de l'unité.*

Solution. Comme G est fini, tout ses élément sont d'ordre fini, donc pour $g \in G$ d'ordre $r \geq 1$, on a $g^r = e$ et $\rho(g)^r = \rho(g^r) = \rho(e) = Id_E$, c'est-à-dire que l'endomorphisme $\rho(g)$ est annulé par le polynôme $X^r - 1$ qui est scindé à racines simples sur $\mathbb{C}$, en conséquence $\rho(g)$ est diagonalisable et ses valeurs propres sont des racines r-ièmes de l'unité.

Exercice 1.3. *On suppose que $\mathbb{K} = \mathbb{C}$ et que le groupe G est fini et commutatif. Montrer qu'une représentation linéaire irréductible de G dans E est nécessairement de degré* 1.

Solution. Si G est fini et commutatif, l'ensemble $\{\rho(g) \mid g \in G\}$ est alors une famille commutative d'endomorphismes de E diagonalisables (voir l'exercice 1.2) et en conséquence, il existe une base commune de diagonalisation. Si $x \in E \backslash \{0\}$ est un vecteur propre commun à tous les $\rho(g)$, où g décrit G, la droite vectorielle $\mathbb{C}x$ est alors G-invariante non réduite au vecteur nul, donc $E = \mathbb{C}x$ si la représentation est irréductible.

Exercice 1.4. *On propose ici une autre démonstration du théorème 1.2 dans le cas où $\mathbb{K}$ est le corps $\mathbb{R}$ des nombre réels [resp. le corps $\mathbb{C}$ des nombre complexes]. On se donne un groupe fini G et (ρ, E) une représentation de G dans un espace euclidien [resp. hermitien] E de dimension n, le produit*

scalaire euclidien [resp. hermitien] étant noté $\langle \cdot \mid \cdot \rangle$. On notera $\|\cdot\|$ la norme associée.

1. *Montrer que l'application :*

$$(x,y) \in E^2 \mapsto \langle x \mid y \rangle_\rho = \sum_{g \in G} \langle \rho(g)(x) \mid \rho(g)(y) \rangle$$

définit un produit scalaire euclidien [resp. hermitien] sur E et que pour tout $g \in G$, l'isomorphisme $\rho(g)$ est orthogonal [resp. unitaire] pour ce produit scalaire (on dit que la représentation (ρ, E) est orthogonale [resp. unitaire]). On notera $\|\cdot\|_\rho$ la norme associée.

2. *Montrer que si F est un sous-espace vectoriel G-invariant de E, son orthogonal $F^{\perp_\rho}$ relativement à $\langle \cdot \mid \cdot \rangle_\rho$ est aussi G-invariant.*
3. *Montrer que (ρ, E) est somme directe de sous-représentations irréductibles.*

Solution.

1. Pour x, y dans E, on a :

$$\langle x \mid y \rangle_\rho = \sum_{g \in G} \langle \rho(g)(x) \mid \rho(g)(y) \rangle = \sum_{g \in G} \langle \rho(g)(y) \mid \rho(g)(x) \rangle = \langle y \mid x \rangle_\rho$$

dans le cas euclidien et :

$$\langle x \mid y \rangle_\rho = \sum_{g \in G} \langle \rho(g)(x) \mid \rho(g)(y) \rangle = \sum_{g \in G} \overline{\langle \rho(g)(y) \mid \rho(g)(x) \rangle} = \overline{\langle y \mid x \rangle_\rho}$$

dans le cas hermitien. Chaque application $\rho(g)$ étant linéaire, l'application $\langle \cdot \mid \cdot \rangle_\rho$ est bilinéaire. Pour tout $x \in E$, on a $\langle x \mid x \rangle_\rho = \sum_{g \in G} \|\rho(g)(x)\|^2 \geq 0$ et l'égalité est réalisée si, et seulement si, $\rho(g)(x) = 0$ pour tout $g \in G$, ce qui équivaut à $x = 0$ puisque $\rho(G) \in GL(E)$. On a donc bien un produit scalaire euclidien [resp. hermitien] sur E. Pour tout $g \in G$ et tout $x \in E$, on a :

$$\begin{aligned} \|\rho(g)(x)\|_\rho^2 &= \sum_{h \in G} \|\rho(h) \circ \rho(g)(x)\|^2 = \sum_{h \in G} \|\rho(hg)(x)\|^2 \\ &= \sum_{k \in G} \|\rho(k)(x)\|^2 = \|x\|_\rho^2 \end{aligned}$$

puisque l'application $h \mapsto hg$ est une permutation de G. Donc $\rho(g)$ est orthogonal [resp. unitaire].

2. Soit F un sous-espace vectoriel G-invariant de E. Comme, pour tout $g \in G$ l'endomorphisme $\rho(g)$ est orthogonal [resp. unitaire] relativement à $\langle \cdot \mid \cdot \rangle_\rho$, on a $\langle \rho(g)(y) \mid x \rangle_\rho = \langle y \mid \rho(g)(x) \rangle_\rho = 0$ pour tout $y \in F^{\perp_\rho}$ et tout $x \in F$ puisque $\rho(g)(x) \in G$ (F est G-invariant), ce qui signifie que $F^{\perp_\rho}$ est G-invariant.
3. Il suffit d'écrire, pour (ρ, E) non irréductible, $E = F \oplus F^{\perp_\rho}$ et de raisonner par récurrence sur la dimension.

Exercice 1.5. *On suppose que E est de dimension n et que G est d'ordre n. Déterminer le caractère de la représentation régulière de G.*

Solution. En désignant par $\mathcal{B} = (e_k)_{k\in G}$ une base de $E = \mathbb{C}^G$ indexée par G, on rappelle que la représentation régulière de G est définie par $\rho(g)(e_k) = e_{gk}$ pour tout $(g,k) \in G^2$. Pour $g \in G$, la matrice $R(g)$ de $\rho(g)$ dans la base $\mathcal{B}$ est donc une matrice de permutation. Pour $g = e$, on a $R(e) = I_n$ et $\chi(g) = \mathrm{Tr}(\rho(e)) = n$, pour $g \neq e$, on a $\rho(g)(e_k) = e_{gk} \neq e_k$ pour tout $k \in G$, c'est-à-dire que $R(g)$ est la matrice d'une permutation sans points fixes, donc ses termes diagonaux sont nuls et sa trace $\chi(g)$ est nulle.

Exercice 1.6. *Calculer le caractère de la représentation par permutation.*

Solution. On rappelle que la représentation par permutation. est définie comme suit. $G = \mathfrak{S}_n$ étant le groupe symétrique d'ordre n, E étant de dimension n et $\mathcal{B} = (e_k)_{1\leq k\leq n}$ une base de E, cette représentation est définie par :

$$\forall \sigma \in \mathfrak{S}_n,\ \forall k \in \{1,\cdots,n\},\ \rho(\sigma)(e_k) = e_{\sigma(k)}$$

Pour $\sigma \in \mathfrak{S}_n$, la trace de $\rho(\sigma)$ est égale au nombre d'éléments de $\mathcal{B}$ invariants par σ, c'est à dire au nombre de points fixes de la permutation σ.

Exercice 1.7. *Montrer que tout caractère $\chi : \mathcal{S}_n \to \mathbb{C}$ du groupe symétrique $\mathcal{S}_n$ est à valeurs réelles.*

Solution. Une permutation est conjuguée à son inverse, donc $\chi(\sigma) = \chi\left(\sigma^{-1}\right) = \overline{\chi(\sigma)}$ pour tout $\sigma \in \mathcal{S}_n$ et χ est à valeurs réelles.

Exercice 1.8. *On suppose que $\mathbb{K} = \mathbb{C}$. Montrer que si (ρ, E) est une représentation de G et χ_ρ son caractère, le caractère de la représentation (ρ^*, E^*) (voir l'exercice 1.1) est alors $\overline{\chi_\rho}$.*

Solution. On rappelle que la représentation $\rho^* : G \to GL(E^*)$ est définie par $\rho^*(g) = {}^t\rho\left(g^{-1}\right)$ pour tout $g \in G$ et on a, pour tout $g \in G$, en désignant par $R(g)$ la matrice de $\rho(g)$ dans une base de E :

$$\begin{aligned}\chi_{\rho^*}(g) &= \mathrm{Tr}\left({}^t\rho\left(g^{-1}\right)\right) = \mathrm{Tr}\left({}^tR\left(g^{-1}\right)\right) = \mathrm{Tr}\left(R\left(g^{-1}\right)\right) = \mathrm{Tr}\left(\rho\left(g^{-1}\right)\right)\\ &= \chi_\rho\left(g^{-1}\right) = \overline{\chi_\rho(g)}\end{aligned}$$

Exercice 1.9. *Déterminer tous les caractères d'un groupe cyclique G d'ordre n.*

Solution. Si $G = \langle g_0\rangle$ est cyclique d'ordre n et g_0 un générateur, un caractère χ de G est uniquement déterminé par sa valeur en g_0. Avec $\chi(g_0)^n = \chi(g_0^n) = \chi(e) = 1$,

on déduit que $\chi(g_0)$ est une racine n-ième de l'unité, c'est-à-dire qu'il existe un entier r compris entre 0 et $n-1$ tel que $\chi(g_0) = \theta_r = e^{\frac{2ir\pi}{n}}$. Réciproquement pour tout entier r compris entre 0 et $n-1$, l'application :

$$\chi_r : g = g_0^k \in G \mapsto \chi_r(g) = \theta_r^k = e^{\frac{2ikr\pi}{n}}$$

définit un caractère de G. On a donc ainsi tous les caractères de G et il y en a n.

Exercice 1.10. *Soient p un nombre premier impair et χ un caractère du groupe multiplicatif $H = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ que l'on prolonge à $\frac{\mathbb{Z}}{p\mathbb{Z}}$ en posant $\chi\left(\overline{0}\right) = 0$. On note 1 le caractère constant égal à 1 sur H et si χ est un caractère de H, $\overline{\chi}$ est le caractère défini par $\overline{\chi}\left(\overline{k}\right) = \overline{\chi\left(\overline{k}\right)}$, où $\overline{k}$ est la classe de l'entier k modulo p. On note $\omega = e^{\frac{2i\pi}{p}}$ et α est le morphisme du groupe additif $\frac{\mathbb{Z}}{p\mathbb{Z}}$ dans le groupe multiplicatif $\mathbb{C}^*$ défini par $\alpha\left(\overline{k}\right) = \omega^k$ pour tout $k \in \mathbb{Z}$. Si χ est un caractère de H, on définit sa somme de Gauss par $G(\chi) = \sum_{g\in H} \alpha(g)\chi(g)$. Si χ et χ' sont deux caractères de G, on définit leur somme de Jacobi par $J(\chi,\chi') = \sum_{g\in H} \chi(g)\chi'\left(\overline{1}-g\right)$.*

1. *Déterminer tous les caractères de H.*
2. *Soit χ un caractère de H. Calculer $J(\chi,1)$ et $J(1,\chi)$.*
3. *Soit χ un caractère non constant de H. Calculer $J(\chi,\overline{\chi})$.*
4. *Soient χ et χ' deux caractères de H avec $\chi' \neq \overline{\chi}$. Montrer que $G(\chi)G(\chi') = J(\chi,\chi')G(\chi\chi')$.*
5. *Soit χ un caractère de H. Montrer que $G(\chi)G(\overline{\chi}) = p\chi\left(-\overline{1}\right)$ et $|G(\chi)| = \sqrt{p}$.*

Solution.

1. Pour $p \geq 3$ premier, le groupe multiplicatif $H = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est cyclique d'ordre $p-1$ (théorème **??**) et l'exercice précédent nous dit que ses caractères sont les applications définies par $\chi_r : g = g_0^k \in H \mapsto \chi_r(g) = e^{\frac{2ikr\pi}{p-1}}$, où g_0 est un générateur de H et r,k sont des entiers compris entre 0 et $p-2$.
2. En gardant les notations qui précèdent, on a pour r compris entre 0 et $p-2$ (en faisant attention au fait que $1\left(\overline{0}\right) = 0$) ;

$$J(\chi_r,1) = \sum_{g\in H-\left\{\overline{1}\right\}} \chi_r(g) = \sum_{k=0}^{p-2} e^{\frac{2ikr\pi}{p-1}} - 1 = \begin{cases} \frac{1-e^{\frac{2i(p-1)r\pi}{p-1}}}{1-e^{\frac{2ir\pi}{p-1}}} - 1 = -1 \text{ si } r \neq 0 \\ p-2 \text{ si } r = 0 \end{cases}$$

En tenant compte du fait que $\chi_r\left(\overline{0}\right)=0$ et que l'application $g\mapsto\overline{1}-g$ réalise une bijection de $H-\left\{\overline{1}\right\}$ sur lui même, on a :

$$J\left(1,\chi_r\right)=\sum_{g\in H-\left\{\overline{1}\right\}}\chi_r\left(\overline{1}-g\right)=\sum_{h\in H-\left\{\overline{1}\right\}}\chi_r\left(h\right)=J\left(\chi_r,1\right)$$

3. On a pour r compris entre 0 et $p-2$:

$$J\left(\chi_r,\overline{\chi_r}\right)=\sum_{g\in H}\chi_r\left(g\right)\overline{\chi_r}\left(\overline{1}-g\right)=\sum_{g\in H-\left\{\overline{1}\right\}}\chi\left(g\right)\overline{\chi}\left(\overline{1}-g\right)$$

En se donnant un générateur g_0 du groupe cyclique H, pour tout $g\in H-\left\{\overline{1}\right\}$ il existe un unique entier k compris entre 1 et $p-2$ tel que $g=g_0^k$ et un unique entier $\nu\left(k\right)$ compris entre 0 et $p-2$ tel que $\overline{1}-g=g_0^{\nu(k)}$. L'application ν ainsi définie est alors une injection de $\{1,\cdots,p-2\}$ dans $\{0,\cdots,p-2\}$. On a donc :

$$J\left(\chi_r,\overline{\chi_r}\right)=\sum_{k=1}^{p-2}\chi_r\left(g_0^k\right)\overline{\chi_r}\left(g_0^{\nu(k)}\right)$$

avec $\chi_r\left(g_0\right)=e^{\frac{2ir\pi}{p-1}}$, $\chi_r\left(g_0^k\right)=e^{\frac{2ikr\pi}{p-1}}$, $\overline{\chi_r}\left(g_0^{\nu(k)}\right)=\overline{e^{\frac{2i\nu(k)r\pi}{p-1}}}=e^{-\frac{2i\nu(k)r\pi}{p-1}}$ et $\chi_r\left(g_0^k\right)\overline{\chi_r}\left(g_0^{\nu(k)}\right)=e^{-\frac{2i(k-\nu(k))r\pi}{p-1}}=\chi_r\left(g_0^{k-\nu(k)}\right)$, ce qui nous donne :

$$J\left(\chi_r,\overline{\chi_r}\right)=\sum_{k=1}^{p-2}\chi_r\left(g_0^{k-\nu(k)}\right)$$

Des égalités $g=g_0^k$ et $\overline{1}-g=g_0^{\nu(k)}$, on déduit que $g_0^k=\overline{1}-g_0^{\nu(k)}$ et :

$$g_0^{k-\nu(k)}=\left(\overline{1}-g_0^{\nu(k)}\right)g_0^{-\nu(k)}=g_0^{-\nu(k)}-\overline{1}$$

donc $J\left(\chi_r,\overline{\chi_r}\right)=\sum_{k=1}^{p-2}\chi_r\left(g_0^{-\nu(k)}-\overline{1}\right)$. L'application $k\mapsto g_0^{-\nu(k)}-\overline{1}$ réalisant une injection de $\{1,\cdots,p-2\}$ dans H, le seul élément non atteint de H étant $-\overline{1}$ ($g_0^{-\nu(p)}\neq\overline{0}$ car $\overline{0}\notin H$), on en déduit que :

$$J\left(\chi_r,\overline{\chi_r}\right)=\sum_{g\in H-\left\{-\overline{1}\right\}}\chi_r\left(g\right)=\sum_{g\in H}\chi_r\left(g\right)-\chi\left(-\overline{1}\right)=-\chi\left(-\overline{1}\right)$$

4. On a :

$$G\left(\chi\right)G\left(\chi'\right)=\sum_{g\in H}\alpha\left(g\right)\chi\left(g\right)\sum_{h\in H}\alpha\left(h\right)\chi'\left(h\right)=\sum_{g\in H}\chi\left(g\right)\sum_{h\in H}\alpha\left(g+h\right)\chi'\left(h\right)$$

(α est un morphisme du groupe additif $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ dans le groupe multiplicatif $\mathbb{C}^*$). Pour g fixé dans H l'application $h\mapsto g+h$ étant une permutation de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, on peut écrire que :

$$G\left(\chi\right)G\left(\chi'\right)=\sum_{g\in H}\chi\left(g\right)\sum_{k\in\frac{\mathbb{Z}}{p\mathbb{Z}}}\alpha\left(k\right)\chi'\left(k-g\right)=\sum_{k\in\frac{\mathbb{Z}}{p\mathbb{Z}}}\alpha\left(k\right)\sum_{g\in H}\chi\left(g\right)\chi'\left(k-g\right)$$

Pour $k \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \left\{\overline{0}\right\} = H$, l'application $h \mapsto kh$ est une permutation de H, donc :

$$\begin{aligned}\sum_{g\in H} \chi(g)\,\chi'(k-g) &= \sum_{h\in H} \chi(kh)\,\chi'(k-kh)\\ &= \chi(k)\,\chi'(k)\sum_{h\in H} \chi(h)\,\chi'(e-h) = \chi(k)\,\chi'(k)\,J(\chi,\chi')\end{aligned}$$

Pour $k = \overline{0}$, on a :

$$\begin{aligned}\sum_{g\in H} \chi(g)\,\chi'(k-g) &= \sum_{g\in H} \chi(g)\,\chi'(-g) = \chi'\left(-\overline{1}\right)\sum_{g\in H} \chi(g)\,\chi'(g)\\ &= \chi'\left(-\overline{1}\right)\sum_{g\in H} (\chi\chi')(g) = 0\end{aligned}$$

si $\chi\chi' \neq 1$, ce qui est réalisé si $\chi' \neq \overline{\chi}$. Il reste donc :

$$G(\chi)\,G(\chi') = \sum_{k\in H} \alpha(k)\,\chi(k)\,\chi'(k)\,J(\chi,\chi') = J(\chi,\chi')\,G(\chi\chi')$$

5. On reprend les calculs précédents, avec $\chi' = \overline{\chi}$. Pour $k \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} - \left\{\overline{0}\right\}$ il n'y a pas de changement. Pour $k = \overline{0}$, on a :

$$\begin{aligned}\sum_{g\in H} \chi(g)\,\overline{\chi}(k-g) &= \sum_{g\in H} \chi(g)\,\overline{\chi}(-g) = \overline{\chi}\left(-\overline{1}\right)\sum_{g\in G} |\chi(g)|^2\\ &= (p-1)\,\overline{\chi}\left(-\overline{1}\right) = (p-1)\,\chi\left(-\overline{1}\right)\end{aligned}$$

ce qui nous donne $G(\chi)\,G(\overline{\chi}) = \alpha\left(\overline{0}\right)(p-1)\,\chi\left(-\overline{1}\right) + J(\chi,\overline{\chi})\displaystyle\sum_{k\in H}\alpha(k)$ avec $\alpha\left(\overline{0}\right) = 1$, $J(\chi,\overline{\chi}) = -\chi\left(-\overline{1}\right)$ et $\displaystyle\sum_{k\in H}\alpha(k) = \sum_{k\in \frac{\mathbb{Z}}{p\mathbb{Z}}}\alpha(k) - \alpha\left(\overline{0}\right) = -1$, donc $G(\chi)\,G(\overline{\chi}) = p\chi\left(-\overline{1}\right)$. Un calcul analogue donne $G(\chi)\,\overline{G(\chi)} = p$.

Chapitre 2

Déterminants (nouvelle version du 12/06/2021)

$\mathbb{K}$ est un corps commutatif de caractéristique différente de 2, E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$, $\mathcal{L}(E)$ est l'algèbre des endomorphismes de E et $GL(E)$ est le groupe des automorphismes de E. $E^* = \mathcal{L}(E, \mathbb{K})$ est l'espace des formes linéaires sur E (voir le chapitre **??**). Pour n, m entiers naturels non nuls, $\mathcal{M}_{m,n}(\mathbb{K})$ est l'espace des matrices à m lignes, n colonnes et à coefficients dans $\mathbb{K}$. Pour $m = n$, on note $\mathcal{M}_n(\mathbb{K})$ l'algèbre des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$, $GL_n(\mathbb{K})$ est le groupe des matrices inversibles dans $\mathcal{M}_n(\mathbb{K})$.

Pour tout entier $n \geq 1$, $\mathcal{S}_n$ est le groupe symétrique et pour toute permutation $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma)$ est la signature de σ (voir le chapitre **??**).

2.1 Formes multilinéaires alternées

Sauf précision contraire, p est un entier naturel supérieur ou égal à 2.

Définition 2.1. *Une forme p-linéaire sur l'espace E est une application $\varphi : E^p \to \mathbb{K}$ telle que pour tout k compris entre 1 et p et $(x_i)_{\substack{1 \leq i \leq p \\ i \neq k}}$ fixé dans E^{p-1} l'application partielle :*

$$\varphi_i : x \in E \mapsto \begin{cases} \varphi(x, x_2, \cdots, x_p) \text{ pour } k = 1 \\ \varphi(x_1, \cdots, x_{k-1}, x, x_{k+1}, \cdots, x_p) \text{ pour } 1 \leq k \leq p-1 \\ \varphi(x_1, \cdots, x_{p-1}, x) \text{ pour } k = p \end{cases}$$

est une forme linéaire sur E. On dit que φ est alternée, si de plus on a $\varphi(x_1, \cdots, x_p) = 0$ pour tout $(x_i)_{1 \leq i \leq p} \in E^p$ pour lequel il existe $j \neq k$ compris entre 1 et p tels que $x_i = x_j$.

Pour tout entier $p \geq 1$, on note $\mathcal{L}_p(E, \mathbb{K})$ l'ensemble des formes p-linéaires sur E (pour $p = 1$, $\mathcal{L}_1(E, \mathbb{K}) = E^*$).

Pour tous $\varphi \in \mathcal{L}_p(E,\mathbb{K})$, $(x_i)_{1\leq i\leq p} \in E^p$ et $(\lambda_i)_{1\leq i\leq p} \in \mathbb{K}^p$, on a en utilisant la multilinéarité, $\varphi(\lambda_1 x_1,\cdots,\lambda_p x_p) = \left(\prod_{i=1}^{p}\lambda_i\right)\varphi(x_1,\cdots,x_p)$. Il en résulte que $\varphi(0,\cdots,0)=0$. Dans le cas où tous les λ_i sont égaux à un même scalaire λ, on obtient $\varphi(\lambda x_1,\cdots,\lambda x_p) = \lambda^p\varphi(x_1,\cdots,x_p)$.

Théorème 2.1.

Pour tout $p\in\mathbb{N}^*$, $\mathcal{L}_p(E,\mathbb{K})$ est un $\mathbb{K}$-espace vectoriel de dimension n^p.

Preuve. Il est facile de vérifier que $\mathcal{L}_p(E,\mathbb{K})$ est un sous-espace vectoriel de l'espace $\mathbb{K}^{E^p}$ des applications de E^p dans $\mathbb{K}$.

Soit $\mathcal{B}=(e_i)_{1\leq i\leq n}$ une base de E. Pour tout $\varphi\in\mathcal{L}_p(E,\mathbb{K})$ et tout $(x_i)_{1\leq i\leq p}$ dans E^p, en notant pour j compris entre 1 et p, $x_j=\sum_{i=1}^{n}x_{i,j}e_i$ et en utilisant le caractère p-linéaire de φ, on a :

$$\varphi(x_1,\cdots,x_p)=\varphi\left(\sum_{i_1=1}^{p}x_{i_1,1}e_{i_1},x_2,\cdots,x_p\right)=\sum_{i_1=1}^{p}x_{i_1,1}\varphi(e_{i_1},x_2\cdots,x_p)$$

$$=\sum_{i_1=1}^{p}\sum_{i_2=1}^{p}x_{i_1,1}x_{i_2,2}\varphi(e_{i_1},e_{i_2},x_3\cdots,x_p)=\sum_{i_1=1}^{n}\cdots\sum_{i_p=1}^{n}x_{i_1,1}\cdots x_{i_p,p}\varphi\left(e_{i_1},\cdots,e_{i_p}\right)$$

$$=\sum_{1\leq i_1,\cdots,i_p\leq n}x_{i_1,1}\cdots x_{i_p,p}\varphi\left(e_{i_1},\cdots,e_{i_p}\right)$$

Il est clair que l'application :

$$\begin{array}{rccc}\Phi: & \mathcal{L}_p(E,\mathbb{K}) & \to & \mathbb{K}^{n^p}\\ & \varphi & \mapsto & \left(\varphi\left(e_{i_1},\cdots,e_{i_p}\right)\right)_{1\leq i_1,\cdots,i_p\leq n}\end{array}$$

est linéaire est injective. Pour tout vecteur $\alpha=\left(\alpha_{i_1,\cdots,i_p}\right)_{1\leq i_1,\cdots,i_p\leq n}\in\mathbb{K}^{n^p}$, l'application $\varphi:(x_1,\cdots,x_p)\mapsto\sum_{1\leq i_1,\cdots,i_p\leq n}\alpha_{i_1,\cdots,i_p}x_{i_1,1}\cdots x_{i_p,p}$ est p-linéaire, donc Φ est surjective et c'est un isomorphisme de $\mathcal{L}_p(E,\mathbb{K})$ sur $\mathbb{K}^{n^p}$. Il en résulte que $\dim(\mathcal{L}_p(E,\mathbb{K}))=n^p$. □

Si $\varphi\in\mathcal{L}_p(E,\mathbb{K})$ est alternée, on a alors $\varphi(x_1,\cdots,x_p)=0$ pour toute famille liée $(x_i)_{1\leq i\leq p}$ de vecteurs de E. Il en résulte que $\varphi(x_1,\cdots,x_p)$ est inchangé si on ajoute à l'un des vecteurs x_k une combinaison linéaire des autres vecteurs x_j (avec $j\neq k$).

Théorème 2.2.

Une forme p-linéaire φ sur E est alternée si, et seulement si, on a $\varphi\left(x_{\sigma(1)},\cdots,x_{\sigma(p)}\right)=\varepsilon(\sigma)\varphi(x_1,\cdots,x_p)$ pour toute permutation $\sigma\in\mathcal{S}_p$ et tout $(x_1,\cdots,x_p)\in E^p$.

Preuve. La signature étant un morphisme de groupes de $\mathcal{S}_p$ sur $\{-1,1\}$ et le groupe $\mathcal{S}_p$ étant engendré par les transpositions, il revient au même de montrer

que $\varphi \in \mathcal{L}_p(E,\mathbb{K})$ est alternée si, et seulement si, on a $\varphi\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right) = -\varphi(x_1,\cdots,x_p)$ pour toute transposition τ.

Supposons que $\varphi \in \mathcal{L}_p(E,\mathbb{K})$ soit alternée et soit $\tau=(j,k)$ une transposition avec $1 \leq j < k \leq p$. En écrivant que :

$$\begin{aligned}0 &= \varphi(x_1,\cdots,x_j+x_k,\cdots,x_j+x_k,\cdots,x_p)\\ &= \varphi(x_1,\cdots,x_j,\cdots,x_j,\cdots,x_p)+\varphi(x_1,\cdots,x_p)\\ &+ \varphi\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right)+\varphi(x_1,\cdots,x_k,\cdots,x_k,\cdots,x_p)\\ &= \varphi(x_1,\cdots,x_p)+\varphi\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right)\end{aligned}$$

on déduit que $\varphi\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right) = -\varphi(x_1,\cdots,x_p)$. Réciproquement, supposons cette condition vérifiée. Si $x_j = x_k$ pour deux indices $j<k$ compris entre 1 et p, on a alors, pour $\tau=(j,k)$:

$$\varphi(x_1,\cdots,x_p) = \varphi\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right) = -\varphi(x_1,\cdots,x_p)$$

et $\varphi(x_1,\cdots,x_p)=0$ pour $\mathbb{K}$ de caractéristique différente de 2. □

Le résultat qui suit nous montre comment transformer une forme p-linéaire en forme p-linéaire alternée.

Théorème 2.3.

Si $\varphi \in \mathcal{L}_p(E,\mathbb{K})$ est une forme p-linéaire, l'application $\widetilde{\varphi}$ définie sur E^p par :

$$\widetilde{\varphi}(x_1,\cdots,x_p) = \sum_{\sigma\in\mathcal{S}_p} \varepsilon(\sigma)\,\varphi\left(x_{\sigma(1)},\cdots,x_{\sigma(p)}\right)$$

est alors une forme p-linéaire alternée sur E.

Preuve. Pour tout $\sigma \in \mathcal{S}_p$, l'application $(x_1,\cdots,x_n) \mapsto \varphi\left(x_{\sigma(1)},\cdots,x_{\sigma(p)}\right)$ est une forme p-linéaire, donc il en est de même de $\widetilde{\varphi}$. Pour toute permutation $\tau \in \mathcal{S}_p$ et tout $(x_1,\cdots,x_p) \in E^p$, on a :

$$\begin{aligned}\widetilde{\varphi}\left(x_{\tau(1)},\cdots,x_{\tau(p)}\right) &= \sum_{\sigma\in\mathcal{S}_p} \varepsilon(\sigma)\,\varphi\left(x_{\sigma\circ\tau(1)},\cdots,x_{\sigma\circ\tau(p)}\right)\\ &= \sum_{\sigma'\in\mathcal{S}_p} \varepsilon\left(\sigma'\circ\tau^{-1}\right)\varphi\left(x_{\sigma'(1)},\cdots,x_{\sigma'(p)}\right)\\ = \sum_{\sigma'\in\mathcal{S}_p} \varepsilon(\sigma')\,\varepsilon\left(\tau^{-1}\right)\varphi\left(x_{\sigma'(1)},\cdots,x_{\sigma'(p)}\right) &= \varepsilon(\tau)\,\widetilde{\varphi}(x_1,\cdots,x_p)\end{aligned}$$

(l'application $\sigma \mapsto \sigma\circ\tau$ réalise une permutation de $\mathcal{S}_p$ et $\varepsilon\left(\tau^{-1}\right) = \varepsilon(\tau)$). Il en résulte que $\widetilde{\varphi}$ est une forme p-linéaire alternée sur E. □

2.2 Déterminants

On se donne une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E et pour tout $x = \sum_{i=1}^{n} x_i e_i \in E$, on note $X = (x_i)_{1\leq i\leq n}$ dans $\mathbb{K}^n$.

Théorème 2.4.

L'espace vectoriel $\mathcal{A}_n(E,\mathbb{K})$ *des formes n-linéaires alternées sur* E *est de dimension* 1 *engendré par l'application* $\det_{\mathcal{B}} : E^n \to \mathbb{K}$ *définie par :*

$$\det_{\mathcal{B}}(x_1,\cdots,x_n) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}$$

où $x_j = \sum_{i=1}^{n} x_{ij} e_i$ *pour tout* j *compris entre* 1 *et* n.

Preuve. Vérifions tout d'abord que l'application $\det_{\mathcal{B}}$ est n-linéaire alternée. En notant, pour tout j compris entre 1 et n et tout $x = \sum_{i=1}^{n} x_i e_i \in E$, $\pi_j(x) = x_j$, on a $\det_{\mathcal{B}}(x_1,\cdots,x_n) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \pi_{\sigma(i)}(x_i)$. Chaque application $\pi_{\sigma(i)}$ étant linéaire, l'application $(x_i)_{1\leq i\leq n} \mapsto \prod_{i=1}^{n} \pi_{\sigma(i)}(x_i)$ est n-linéaire et il en est de même de $\det_{\mathcal{B}}$ comme combinaison linéaire d'applications n-linéaires. Pour tout permutation τ, en effectuant le changement d'indice $k = \tau(i)$, on a :

$$\det_{\mathcal{B}}\left(x_{\tau(1)},\cdots,x_{\tau(n)}\right) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} \pi_{\sigma(i)}\left(x_{\tau(i)}\right) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} \pi_{\sigma\circ\tau^{-1}(k)}(x_k)$$

et en utilisant le fait que l'application $\sigma' \mapsto \sigma = \sigma'\circ\tau$ est une bijection de $\mathcal{S}_n$ sur lui même, on en déduit que :

$$\begin{aligned}\det_{\mathcal{B}}\left(x_{\tau(1)},\cdots,x_{\tau(n)}\right) &= \sum_{\sigma'\in\mathcal{S}_n} \varepsilon(\sigma'\circ\tau) \prod_{k=1}^{n} \pi_{\sigma'(k)}(x_k) \\ &= \varepsilon(\tau) \sum_{\sigma'\in\mathcal{S}_n} \varepsilon(\sigma') \prod_{k=1}^{n} \pi_{\sigma'(k)}(x_k) = \varepsilon(\tau)\det_{\mathcal{B}}(x_1,\cdots,x_n)\end{aligned}$$

ce qui signifie que $\det_{\mathcal{B}}$ est alternée. Pour $\varphi \in \mathcal{A}_n(E,\mathbb{K})$ et $(x_1,\cdots,x_n) \in E^n$, on a :

$$\begin{aligned}\varphi(x_1,\cdots,x_n) &= \sum_{1\leq i_1,\cdots,i_n\leq n} x_{i_1,1}\cdots x_{i_n,n}\varphi(e_{i_1},\cdots,e_{i_n}) \\ &= \sum_{\sigma\in\mathcal{F}_n} \prod_{i=1}^{n} x_{\sigma(i),i}\varphi\left(e_{\sigma(1)},\cdots,e_{\sigma(n)}\right)\end{aligned}$$

où $\mathcal{F}_n$ est l'ensemble des applications de $\{1,\cdots,n\}$ dans $\{1,\cdots,n\}$. Comme φ est alternée, on a $\varphi\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)=0$ pour σ non bijective et :

$$\begin{aligned}\varphi(x_1,\cdots,x_n)&=\sum_{\sigma\in\mathcal{S}_n}\prod_{i=1}^{n}x_{\sigma(i),i}\varphi\left(e_{\sigma(1)},\cdots,e_{\sigma(n)}\right)\\&=\left(\sum_{\sigma\in\mathcal{S}_n}\varepsilon(\sigma)\prod_{i=1}^{n}x_{\sigma(i),i}\right)\varphi(e_1,\cdots,e_n)\end{aligned}$$

soit $\varphi=\lambda\det_{\mathcal{B}}$ avec $\lambda=\varphi(e_1,\cdots,e_n)\in\mathbb{K}$ et $\det_{\mathcal{B}}\in\mathcal{A}_n(E,\mathbb{K})\setminus\{0\}$. En conclusion, $\mathcal{A}_n(E,\mathbb{K})$ est de dimension 1 engendré par $\det_{\mathcal{B}}$. □

Avec la démonstration précédente, on constate que $\det_{\mathcal{B}}$ est l'unique forme n-linéaire alternée sur E telle que $\varphi(e_1,\cdots,e_n)=1$.

Définition 2.2. *Avec les notations qui précèdent, on dit que* $\det_{\mathcal{B}}(x_1,\cdots,x_n)$ *est le déterminant dans la base* $\mathcal{B}$ *du n-uplet de vecteurs* $(x_i)_{1\leq i\leq n}$.

Pour $\varphi\in\mathcal{A}_n(E,\mathbb{K})$, on a $\varphi=\lambda\det_{\mathcal{B}}$ avec $\lambda=\varphi(e_1,\cdots,e_n)$ et en conséquence, $\varphi(x_1,\cdots,x_n)=\varphi(e_1,\cdots,e_n)\det_{\mathcal{B}}(x_1,\cdots,x_n)$ pour tout $(x_i)_{1\leq i\leq n}\in E^n$. On en déduit la formule de changement de base qui suit.

Théorème 2.5. Relation de Chasles

Si $\mathcal{B}'=(e'_i)_{1\leq i\leq n}$ *est une autre base de* E*, on a alors pour pour tout* $(x_i)_{1\leq i\leq n}\in E^n$ *:*

$$\begin{aligned}\det_{\mathcal{B}'}(x_1,\cdots,x_n)&=\det_{\mathcal{B}'}(e_1,\cdots,e_n)\det_{\mathcal{B}}(x_1,\cdots,x_n)\\&=\det_{\mathcal{B}'}(\mathcal{B})\det_{\mathcal{B}}(x_1,\cdots,x_n)\end{aligned}$$

On déduit du résultat précédent que $\det_{\mathcal{B}'}(\mathcal{B})\det_{\mathcal{B}}(\mathcal{B}')=\det_{\mathcal{B}'}(\mathcal{B}')=1$.

Théorème 2.6.

Soit $\mathcal{B}'=(x_i)_{1\leq i\leq n}$ *un n-uplet de vecteurs de* E*. Les assertions suivantes sont équivalentes :*

1. *la famille* $\mathcal{B}'$ *est liée ;*
2. *pour toute base* $\mathcal{B}$ *de* E, $\det_{\mathcal{B}}(\mathcal{B}')=0$ *;*
3. *il existe une base* $\mathcal{B}$ *de* E *telle que* $\det_{\mathcal{B}}(\mathcal{B}')=0$.

Preuve. (1) ⇒ (2) Si la famille $\mathcal{B}'$ est liée, on a alors $\varphi(x_1,\cdots,x_n)=0$ pour toute forme n-linéaire alternée et c'est en particulier vrai pour $\det_{\mathcal{B}}$, quelle que soit la base $\mathcal{B}$ de E.

(2) ⇒ (3) est évident.

(3) ⇒ (1) Soit $\mathcal{B}$ une base de E telle que $\det_{\mathcal{B}}(\mathcal{B}')=0$. Si la famille $\mathcal{B}'$ est libre, c'est alors une base de E et on a $1=\det_{\mathcal{B}'}(\mathcal{B}')=\det_{\mathcal{B}'}(\mathcal{B})\det_{\mathcal{B}}(\mathcal{B}')=0$, ce qui est impossible. □

Corollaire 2.1. *Soit $\mathcal{B}' = (x_i)_{1\leq i\leq n}$ un n-uplet de vecteurs de E. Cette famille est une base de E si, et seulement si, il existe une base $\mathcal{B}$ de E telle que $\det_{\mathcal{B}}(\mathcal{B}') \neq 0$.*

Le résultat qui suit nous permet de définir le déterminant d'un endomorphisme de E.

Théorème 2.7.

Pour tout endomorphisme $u \in \mathcal{L}(E)$, il existe un unique scalaire λ_u tel que pour toute forme $\varphi \in \mathcal{A}_n(E,\mathbb{K}) \setminus \{0\}$ et tout $(x_i)_{1\leq i\leq n} \in E^n$, on a :

$$\varphi(u(x_1),\cdots,u(x_n)) = \lambda_u \varphi(x_1,\cdots,x_n)$$

On a $\lambda_u = \det_{\mathcal{B}}(u(e_1),\cdots,u(e_n))$, où $\mathcal{B} = (e_i)_{1\leq i\leq n}$ est une base quelconque de E.

Preuve. Pour tout endomorphisme $u \in \mathcal{L}(E)$ et toute forme n-linéaire alternée $\varphi \in \mathcal{A}_n(E,\mathbb{K}) \setminus \{0\}$, l'application $\varphi \circ u : (x_i)_{1\leq i\leq n} \in E^n \mapsto \varphi(u(x_i))_{1\leq i\leq n}$ est aussi une forme n-linéaire alternée, donc il existe un scalaire λ_u tel que $\varphi \circ u = \lambda_u \varphi$ ($\dim(\mathcal{A}_n(E,\mathbb{K})) = 1$ et φ est non nulle). Si $\psi \in \mathcal{A}_n(E,\mathbb{K}) \setminus \{0\}$ est une autre forme n-linéaire alternée non nulle, on a alors $\psi = \rho\varphi$ et $\psi \circ u = \rho\varphi \circ u = \rho\lambda_u\varphi = \lambda_u\psi$, c'est-à-dire que le scalaire λ_u ne dépend pas de la forme n-linéaire alternée non nulle choisie. Prenant $\varphi = \det_{\mathcal{B}}$ puis $\varphi = \det_{\mathcal{B}'}$, où $\mathcal{B} = (e_i)_{1\leq i\leq n}$ et $\mathcal{B}' = (e'_i)_{1\leq i\leq n}$ sont des bases de E, on a $\det_{\mathcal{B}}(u(e_1),\cdots,u(e_n)) = \lambda_u = \det_{\mathcal{B}'}(u(e'_1),\cdots,u(e'_n))$. □

Définition 2.3. *Avec les notations du théorème précédent, on dit que le scalaire λ_u est le déterminant de u et on le note $\det(u)$.*

Le scalaire $\det(u)$ ne dépend que de u et pas du choix d'une base de E.

Si $(x_i)_{1\leq i\leq n} \in E^n$ et $u \in \mathcal{L}(E)$ est défini par $u(e_i) = x_i$ pour i compris entre 1 et n, on a alors $\det(u) = \det_{\mathcal{B}}(u(e_1),\cdots,u(e_n)) = \det_{\mathcal{B}}(x_1,\cdots,x_n)$, où $\mathcal{B} = (e_i)_{1\leq i\leq n}$ est une base quelconque de E.

Théorème 2.8.

On a $\det(Id) = 1$ et pour u, v dans $\mathcal{L}(E)$, $\lambda \in \mathbb{K}$, on a :

$$\det(\lambda u) = \lambda^n \det(u),\ \det(u\circ v) = \det(v\circ u) = \det(u)\det(v)$$

Un endomorphisme $u \in \mathcal{L}(E)$ est inversible si, et seulement si, $\det(u) \neq 0$ et dans ce cas, on a $\det\left(u^{-1}\right) = \dfrac{1}{\det(u)}$.

Preuve. Pour toute base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E, on a :

$$\det(Id) = \det_{\mathcal{B}}(Id(e_i))_{1\leq i\leq n} = \det_{\mathcal{B}}(\mathcal{B}) = 1$$

Avec la n-linéarité de $\det_{\mathcal{B}}$, on obtient :

$$\det(\lambda u) = \det_{\mathcal{B}}(\lambda u(e_i))_{1\leq i\leq n} = \lambda^n \det_{\mathcal{B}}(u(e_i))_{1\leq i\leq n} = \lambda^n \det(u)$$

Pour toute forme $\varphi \in \mathcal{A}_n(E,\mathbb{K}) \setminus \{0\}$ et tout $(x_i)_{1\leq i\leq n} \in E^n$, on a :

$$\varphi(u\circ v(x_1),\cdots,u\circ v(x_n)) = \det(v\circ u)\,\varphi(x_1,\cdots,x_n)$$

et aussi :

$$\begin{aligned}\varphi(u\circ v(x_1),\cdots,u\circ v(x_n)) &= \det(u)\,\varphi(v(x_1),\cdots,v(x_n))\\ &= \det(u)\det(v)\,\varphi(x_1,\cdots,x_n)\end{aligned}$$

donc $\det(u\circ v) = \det(u)\det(v)$. Comme $\det(u)\det(v) = \det(v)\det(u)$, on a aussi $\det(u\circ v) = \det(v\circ u)$.

Si $u \in GL(E)$, on a alors $1 = \det(Id) = \det\left(u\circ u^{-1}\right) = \det(u)\det\left(u^{-1}\right)$ et $\det(u) \neq 0$. Si $u \notin GL(E)$, on a alors $\det(u) = \det_{\mathcal{B}}(u(e_i))_{1<i<n} = 0$ puisque la famille $(u(e_i))_{1<i<n}$ est liée. □

L'application det est un morphisme de groupes surjectif de $GL(E)$ sur $\mathbb{K}^*$ et le noyau de ce morphisme est le groupe spécial linéaire $SL(E)$ qui est distingué de $GL(E)$ (le groupe linéaire $GL(E)$ est étudié en détail au chapitre **??**).

Si $A = ((a_{i,j}))_{1\leq i,j\leq n}$ est la matrice de $u \in \mathcal{L}(E)$ dans une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E, on a alors $u(e_j) = \sum_{i=1}^{n} a_{ij}e_i$ $(1 \leq i \leq n)$ et :

$$\det(u) = \det_{\mathcal{B}}(u(e_1),\cdots,u(e_n)) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} a_{\sigma(i),i}$$

Définition 2.4. *Si $A = ((a_{i,j}))_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$, le déterminant de A est le scalaire :*

$$\det(A) = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)\prod_{i=1}^{n} a_{\sigma(i),i} \tag{2.1}$$

Ce déterminant est le déterminant de la famille $(C_j)_{1\leq j\leq n}$ des vecteurs colonnes de A dans la base canonique de $\mathbb{K}^n$. C'est aussi le déterminant de l'endomorphisme de $\mathbb{K}^n$ canoniquement associé à la matrice A.

Si $u \in \mathcal{L}(E)$ a pour matrice $A \in \mathcal{M}_n(\mathbb{K})$ dans une base $\mathcal{B}$ de E, on a alors $\det(u) = \det(A)$. Comme deux matrices semblables dans $\mathcal{M}_n(\mathbb{K})$ définissent le même endomorphisme de $\mathbb{K}^n$ dans deux bases différentes, elles ont le même déterminant.

En identifiant $\mathcal{M}_n(\mathbb{K})$ à $\mathbb{K}^{n^2}$, l'application $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ est une fonction polynomiale homogène de degré n.

Théorème 2.9.

On a $\det(I_n) = 1$ *et pour* A, B *dans* $\mathcal{M}_n(\mathbb{K})$, $\lambda \in \mathbb{K}$, *on a :*

$$\det(\lambda A) = \lambda^n \det(A), \ \det\left({}^tA\right) = \det(A)$$

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

Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ *est inversible si, et seulement si,* $\det(A) \neq 0$ *et dans ce cas, on a* $\det\left(A^{-1}\right) = \dfrac{1}{\det(A)}$.

Preuve. Toutes les propriétés, exceptée celle sur la transposée se déduisent du théorème 2.8. Pour $A = ((a_{i,j}))_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$, on a :

$$\begin{aligned}\det(A) &= \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),\sigma^{-1}(\sigma(i))} \\ &= \sum_{\sigma\in\mathcal{S}_n} \varepsilon\left(\sigma^{-1}\right) \prod_{k=1}^{n} a_{k,\sigma^{-1}(k)} = \sum_{\tau\in\mathcal{S}_n} \varepsilon(\tau) \prod_{i=1}^{n} a_{k,\tau(k)} = \det\left({}^tA\right)\end{aligned}$$

puisque l'application $\sigma \mapsto \sigma^{-1}$ est une permutation de $\mathcal{S}_n$ et $\varepsilon\left(\sigma^{-1}\right) = \varepsilon(\sigma)$ pour tout $\sigma \in \mathcal{S}_n$. □

Avec le théorème précédent, on retrouve le fait que si A et B sont deux matrices semblables dans $\mathcal{M}_n(\mathbb{K})$, on a alors $\det(A) = \det(B)$.

2.3 Méthodes de calcul du déterminant d'une matrice

Le calcul du déterminant d'une matrice A d'ordre n par la formule (2.1) nécessite un nombre d'opérations de l'ordre de $n!$ ce qui est beaucoup trop pour la capacité d'un ordinateur actuel sachant que $n! \geq \left(\dfrac{n}{e}\right)^n$. Par exemple, pour $n = 30$, cela donne plus de 10^{30} opérations.

Des propriétés des formes multilinéaires alternées, on déduit les propriétés suivantes du déterminant, où $A \in \mathcal{M}_n(\mathbb{K})$ et $C_j = (a_{ij})_{1\leq i\leq n} \in \mathbb{K}^n$ est la colonne numéro j de A pour tout j compris entre 1 et n.

— En désignant pour toute permutation σ de $\{1, \cdots, n\}$ par A_σ la matrice $A_\sigma = \left(C_{\sigma(1)}, \cdots, C_{\sigma(n)}\right)$ déduite de A en faisant agir σ sur ses colonnes, on a $\det(A_\sigma) = \varepsilon(\sigma)\det(A)$.

— Si l'une des colonnes de A est combinaison linéaire des autres, on a alors $\det(A) = 0$. En particulier, $\det(A) = 0$ si l'une des colonnes de A est nulle.

— $\det(A)$ est linéaire par rapport à chacune des colonnes.

— $\det(A)$ est inchangé si on ajoute à une de ses colonnes une combinaison linéaire des autres.

— Les propriétés analogues sur les lignes de A sont vérifiées.

Exemple 2.1 *De la première propriété, on déduit que si P_σ est une matrice de permutation (matrice déduite de I_n en faisant agir σ sur les colonnes de I_n), on a alors* $\det(P_\sigma) = \varepsilon(\sigma)$.

On s'intéresse d'abord au calcul du déterminant d'une matrice triangulaire par blocs.

Lemme 2.1 *Pour toute matrice* $A = \begin{pmatrix} a_{11} & \alpha \\ 0 & B \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$, *où* $B \in \mathcal{M}_{n-1}(\mathbb{K})$, $a_{11} \in \mathbb{K}$ *et* $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$, *on a* $\det(A) = a_{11}\det(B)$.

Preuve. Si $a_{11} = 0$, la première colonne de la matrice A est alors nulle et on a $\det(A) = 0 = a_{11}\det(B)$. Si $a_{11} \neq 0$, on a alors $\det(A) = a_{11}^n \det(A')$ où $A' = \begin{pmatrix} 1 & \alpha' \\ 0 & B' \end{pmatrix}$ avec $\alpha' = \dfrac{1}{a_{11}}\alpha$ et $B' = \dfrac{1}{a_{11}}B$. En notant C'_j la colonne numéro j de A', pour $1 \leq j \leq n$, les opérations qui consistent à remplacer C'_j par $C'_j - \alpha'_j C'_1$ pour j compris entre 2 et n, ne changent pas la valeur de $\det(A')$, ce qui nous donne $\det(A') = \det\begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}$. L'application $\varphi : B' \in \mathcal{M}_{n-1}(\mathbb{K}) \mapsto \det\begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}$ est $(n-1)$-linéaire alternée sur les colonnes (en identifiant l'espace vectoriel $\mathcal{M}_{n-1}(\mathbb{K})$ à $\left(\mathbb{K}^{n-1}\right)^{n-1}$) avec $\varphi(I_{n-1}) = \det(I_n) = 1$, donc $\det(A') = \varphi(B') = \det(B') = \dfrac{1}{a_{11}^{n-1}}\det(B)$ et $\det(A) = a_{11}\det(B)$. □

Lemme 2.2 *Pour toute matrice triangulaire supérieure ou inférieure* $A = ((a_{i,j}))_{1 \leq i,j \leq n}$ *dans* $\mathcal{M}_n(\mathbb{K})$, *on a* $\det(A) = \prod_{i=1}^{n} a_{i,i}$.

Preuve. Se déduit par récurrence du lemme précédent et de $\det({}^tA) = \det(A)$. □

Lemme 2.3 *Pour toute matrice* $M = \begin{pmatrix} I_p & B \\ 0 & A \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$, *où* $p + q = n$, $A \in \mathcal{M}_q(\mathbb{K})$, $B \in \mathcal{M}_{p,q}(\mathbb{K})$, *on a* $\det(M) = \det(A)$.

Preuve. Pour $B \in \mathcal{M}_{p,q}(\mathbb{K})$ fixée, l'application $\varphi : A \in \mathcal{M}_q(\mathbb{K}) \mapsto \det\begin{pmatrix} I_p & B \\ 0 & A \end{pmatrix}$ est p-linéaire alternée sur les colonnes (en identifiant l'espace vectoriel $\mathcal{M}_q(\mathbb{K})$ à $(\mathbb{K}^q)^q$) avec $\varphi(I_q) = \det\begin{pmatrix} I_p & B \\ 0 & I_q \end{pmatrix} = 1$. On a donc, par définition du déterminant, $\varphi(A) = \det(A)$ pour toute matrice $A \in M_q(\mathbb{K})$. De manière analogue on montre que $\det\begin{pmatrix} A & B \\ 0 & I_q \end{pmatrix} = \det(A)$. □

Lemme 2.4 *Pour toute matrice* $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$, *où* $A \in \mathcal{M}_p(\mathbb{K})$, $B \in \mathcal{M}_{p,q}(\mathbb{K})$, $D \in \mathcal{M}_q(\mathbb{K})$, $p + q = n$, *on a* $\det(M) = \det(A)\det(D)$.

Preuve. Pour $(B,D)\in\mathcal{M}_{p,q}(\mathbb{K})\times\mathcal{M}_q(\mathbb{K})$ fixé, l'application $\varphi : A\in\mathcal{M}_p(\mathbb{K})\mapsto \det\begin{pmatrix} A & B\\ 0 & D\end{pmatrix}$ est p-linéaire alternée telle que $\varphi(I_p)=\det\begin{pmatrix} I_p & B\\ 0 & D\end{pmatrix}=\det(D)$, donc $\det(M)=\varphi(A)=\det(A)\det(D)$. □

Théorème 2.10.

Si $A=\begin{pmatrix} A_1 & B_{12} & \cdots & B_{1p}\\ 0 & \ddots & \ddots & \vdots\\ \vdots & \ddots & \ddots & B_{p-1,p-1}\\ 0 & \cdots & 0 & A_p\end{pmatrix}$ *est une matrice carrée où les* A_k *sont des matrices carrées, on a alors* $\det(A)=\prod_{k=1}^{p}\det(A_k)$.

Preuve. Se déduit de ce qui précède par récurrence sur p. □

Pour toute matrice $A=((a_{i,j}))_{1\leq i,j\leq n}\in\mathcal{M}_n(\mathbb{K})$ et tous i,j compris entre 1 et n, on note $A_{i,j}$ la matrice carrée d'ordre $n-1$ déduite de A en supprimant la ligne i et la colonne j. Le scalaire $\det(A_{i,j})$ est le mineur d'indice (i,j) et le scalaire $(-1)^{i+j}\det(A_{i,j})$ est le cofacteur d'indice (i,j).

Théorème 2.11.

Pour toute matrice $A\in\mathcal{M}_n(\mathbb{K})$, *on a les développements de* $\det(A)$ *suivant la colonne* $j\in\{1,\cdots,n\}$ *ou la ligne* $i\in\{1,\cdots,n\}$ *:*

$$\det(A)=\sum_{i=1}^{n}(-1)^{i+j}a_{i,j}\det(A_{i,j})=\sum_{j=1}^{n}(-1)^{i+j}a_{i,j}\det(A_{i,j})$$

Preuve. Fixons la colonne j et notons $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{K}^n$. La colonne C_j s'écrit $C_j=\sum_{i=1}^{n}a_{ij}e_i$ et en utilisant la linéarité du déterminant par rapport à la j-ième colonne, on a $\det(A)=\sum_{i=1}^{n}a_{ij}\det(B_{i,j})$, où B_{ij} est la matrice déduite de A en remplaçant C_j par e_i. En permutant la colonne j avec la colonne $j-1$, puis $j-1$ avec $j-2$, $\cdots$, 2 avec 1 et ensuite la ligne i avec la ligne $i-1$,

$i-1$ avec $i-2, \cdots, 2$ avec 1 (on ne fait rien pour $i=1$), on aboutit à :

$$\det(B_{i,j}) = (-1)^{i+j} \begin{vmatrix} 1 & a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in} \\ 0 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ 0 & a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{n,n} \end{vmatrix}$$
$$= (-1)^{i+j} \det(A_{i,j})$$

et on a le résultat annoncé. On procède de manière analogue pour la deuxième formule. □

Définition 2.5. *La comatrice d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice :*

$$C(A) = \left(\left((-1)^{i+j} \det(A_{i,j})\right)\right)_{1 \leq i,j \leq n}$$

des cofacteurs de A.

Théorème 2.12.

Pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, on a :

$$A \cdot {}^tC(A) = {}^tC(A) \cdot A = \det(A) I_n$$

Pour $\det(A) \neq 0$, A est inversible d'inverse $A^{-1} = \dfrac{1}{\det(A)} {}^tC(A)$.

Preuve. Pour $1 \leq i, j \leq n$, on note $c_{i,j} = (-1)^{i+j} \det(A_{i,j})$ le cofacteur d'indice (i,j). Le terme d'indice (i,j) du produit $A \cdot {}^tC(A)$ est $d_{i,j} = \sum_{k=1}^{n} a_{i,k} c_{j,k}$. Pour $i=j$, on a $d_{i,i} = \sum_{k=1}^{n} (-1)^{i+k} a_{i,k} \det(A_{i,k}) = \det(A)$ et pour $i \neq j$, on a $d_{i,j} = \sum_{k=1}^{n} (-1)^{j+k} a_{i,k} \det(A_{j,k}) = 0$ puisque c'est le développement du déterminant de la matrice ayant pour ligne $k \neq j$, celle de A et pour ligne j, la ligne i de A, donc elle a deux lignes identiques. On a donc $A \cdot {}^tC(A) = \det(A) I_n$, l'autre égalité se vérifiant de manière analogue. □

En identifiant $\mathcal{M}_n(\mathbb{K})$ à $\mathbb{K}^{n^2}$, on déduit du théorème précédent que pour A inversible, les coefficients de A^{-1} sont des fonctions rationnelles des coefficients a_{ij}.

Exemple 2.2 *Pour* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$, *on a :*

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Pour calculer un déterminant, on dispose aussi de la méthode des pivots de Gauss qui est basée sur les résultats suivants où une matrice de transvection est une matrice de la forme $I_n + \lambda E_{ij}$ en notant $(E_{i,j})_{1\leq i,j\leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$ (voir le paragraphe **??**).

Lemme 2.5 *Soit* $A \in \mathcal{M}_n(\mathbb{K})$ *de coefficient* a_{11} *non nul. Il existe des matrices de transvection* $P_1, \cdots, P_r$ *telles que :*

$$P_r \cdots P_1 A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22}^{(1)} & \cdots & a_{2n}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}^{(1)} & \cdots & a_{nn}^{(1)} \end{pmatrix}$$

Preuve. Voir [**?**]. □

Si le coefficient a_{11} est nul et qu'il existe un indice i compris entre 2 et n tel que $a_{i1} \neq 0$, on se ramène à l'hypothèse du lemme en permuttant les lignes 1 et i. Si tous les a_{i1} pour $1 \leq i \leq n$ sont nuls, le déterminant de A est alors nul.

Théorème 2.13.

Toute matrice $A \in GL_n(\mathbb{K})$ *peut être réduite à la forme triangulaire supérieure en la multipliant à gauche par des matrices de transvection ou de permutation.*

Preuve. Voir [**?**]. □

Le théorème précédent ramène au signe près le calcul du déterminant de A au déterminant d'une matrice triangulaire supérieure, le « signe près » étant $(-1)^p$, où p est le nombre de permutations effectuées dans l'algorithme de Gauss.

2.4 Quelques déterminants classiques

2.4.1 Déterminants de Vandermonde

À tout entier $n \geq 2$ et toute suite $(\alpha_k)_{1\leq k\leq n}$ d'éléments de $\mathbb{K}$, on associe la matrice de Vandermonde :

$$V(\alpha_1, \cdots, \alpha_n) = \left(\left(\alpha_j^{i-1}\right)\right)_{1\leq i,j\leq n} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

et on note $\Delta(\alpha_1, \cdots, \alpha_n)$, le déterminant de cette matrice.

Théorème 2.14.

La matrice de Vandermonde $V(\alpha_1, \cdots, \alpha_n)$ est inversible si, et seulement si, les α_k pour k compris entre 1 et n sont deux à deux distincts.

Preuve. S'il existe $i \neq j$ tels que $\alpha_i = \alpha_j$, la matrice $V(\alpha_1, \cdots, \alpha_n)$ a alors deux colonnes identiques, ce qui implique qu'elle est non inversible.

Réciproquement, si $V(\alpha_1, \cdots, \alpha_n)$ est non inversible, il en est alors de même de ${}^tV(\alpha_1, \cdots, \alpha_n) = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}$ et le système linéaire :

$$\sum_{j=1}^{n} \alpha_i^{j-1} x_j = 0 \ (1 \leq i \leq n)$$

a une solution $(x_j)_{1 \leq j \leq n}$ non nulle, ce qui revient à dire que $\alpha_1, \cdots, \alpha_n$ sont des racines du polynôme $P(X) = \sum_{j=1}^{n} x_j X^{j-1} \in \mathbb{K}_{n-1}[X] \setminus \{0\}$ et nécessairement il existe $i \neq j$ tels que $\alpha_i = \alpha_j$, sans quoi P aurait n racines distinctes en étant non nul de degré au plus égal à $n-1$, ce qui n'est pas possible. □

Le théorème précédent peut être utilisé pour prouver l'existence et l'unicité des polynômes d'interpolation de Lagrange.

Théorème 2.15.

Soit $(\alpha_k)_{1 \leq i \leq n}$ une famille de $n \geq 2$ scalaires deux à deux distincts. Pour toute famille de scalaires $(\beta_k)_{1 \leq i \leq n}$, il existe un unique polynôme $P \in \mathbb{K}_{n-1}[x]$ tel que $P(\alpha_k) = \beta_k$ pour tout k compris entre 0 et n.

Preuve. L'application $\varphi_n : \mathbb{K}_{n-1}[X] \to \mathbb{K}^n$ définie par $\varphi_n(P) = (P(\alpha_k))_{1 \leq k \leq n}$ pour tout $P \in \mathbb{K}_{n-1}[X]$ est linéaire et sa matrice dans les bases canoniques de $\mathbb{K}_{n-1}[X]$ et $\mathbb{K}^n$ est la matrice inversible :

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} = {}^tV(\alpha_1, \cdots, \alpha_n)$$

c'est donc un isomorphisme de $\mathbb{K}_{n-1}[X]$ sur $\mathbb{K}^n$ et tout vecteur $(\beta_k)_{1 \leq i \leq n} \in \mathbb{K}^n$ a un unique antécédent $P \in \mathbb{K}_{n-1}[X]$. □

Théorème 2.16.

On a $\Delta(\alpha_1, \cdots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$.

Preuve. Pour $n=2$, on a $\Delta(\alpha_1,\alpha_2)=\begin{vmatrix}1&1\\ \alpha_1&\alpha_2\end{vmatrix}=\alpha_2-\alpha_1$. En supposant le résultat acquis pour $n-1\geq 2$, on propose trois méthodes de démonstration par récurrence.

1. En retranchant, pour $i=n,n-1,\cdots,2$, à la ligne i de $V(\alpha_1,\cdots,\alpha_n)$ sa ligne $i-1$ multipliée par α_1, on obtient :

$$\Delta(\alpha_1,\cdots,\alpha_n)=\begin{vmatrix}1&1&\cdots&1\\ 0&\alpha_2-\alpha_1&\cdots&\alpha_n-\alpha_1\\ \vdots&\vdots&\ddots&\vdots\\ 0&\alpha_2^{n-2}(\alpha_2-\alpha_1)&\cdots&\alpha_n^{n-2}(\alpha_n-\alpha_1)\end{vmatrix}$$

$$=\begin{vmatrix}\alpha_2-\alpha_1&\alpha_3-\alpha_1&\cdots&\alpha_n-\alpha_1\\ \alpha_2(\alpha_2-\alpha_1)&\alpha_3(\alpha_3-\alpha_1)&\cdots&\alpha_n(\alpha_n-\alpha_1)\\ \vdots&\vdots&\ddots&\vdots\\ \alpha_2^{n-2}(\alpha_2-\alpha_1)&\alpha_3^{n-2}(\alpha_3-\alpha_1)&\cdots&\alpha_n^{n-2}(\alpha_n-\alpha_1)\end{vmatrix}$$

soit par n-linéarité du déterminant :

$$\Delta(\alpha_1,\cdots,\alpha_n)=\left(\prod_{k=2}^{n}(\alpha_k-\alpha_1)\right)\begin{vmatrix}1&\cdots&1\\ \alpha_2&\cdots&\alpha_n\\ \vdots&\ddots&\vdots\\ \alpha_2^{n-2}&\cdots&\alpha_n^{n-2}\end{vmatrix}$$

$$=\left(\prod_{k=2}^{n}(\alpha_k-\alpha_1)\right)\Delta(\alpha_2,\cdots,\alpha_n)$$

et avec l'hypothèse de récurrence, cela donne :

$$\Delta(\alpha_1,\cdots,\alpha_n)=\left(\prod_{k=2}^{n}(\alpha_k-\alpha_1)\right)\prod_{2\leq i<j\leq n}^{n}(\alpha_j-\alpha_i)$$

$$=\prod_{1\leq i<j\leq n}^{n}(\alpha_j-\alpha_i)$$

2. Le déterminant étant une forme n-linéaire alternée, on a pour tout polynôme P unitaire de degré $n-1$:

$$\begin{vmatrix}1&1&\cdots&1\\ \alpha_1&\alpha_2&\cdots&\alpha_n\\ \vdots&\vdots&\ddots&\vdots\\ P(\alpha_1)&P(\alpha_2)&\cdots&P(\alpha_n)\end{vmatrix}=\Delta(\alpha_1,\cdots,\alpha_n)$$

Prenant $P(X) = \prod_{k=1}^{n-1} (X - \alpha_k)$, on en déduit que :

$$\Delta(\alpha_1, \cdots, \alpha_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P(\alpha_n) \end{vmatrix} = P(\alpha_n)\,\Delta(\alpha_1, \cdots, \alpha_{n-1})$$
$$= \left(\prod_{k=1}^{n-1} (\alpha_n - \alpha_k)\right) \Delta(\alpha_1, \cdots, \alpha_{n-1})$$

et avec l'hypothèse de récurrence, cela donne :

$$\Delta(\alpha_1, \cdots, \alpha_n) = \left(\prod_{k=1}^{n-1} (\alpha_n - \alpha_k)\right) \prod_{1 \le i < j \le n-1}^{n} (\alpha_j - \alpha_i)$$
$$= \prod_{1 \le i < j \le n}^{n} (\alpha_j - \alpha_i)$$

3. Dans le cas où deux des α_k sont égaux, la formule est triviale. Dans le cas contraire, le polynôme $V(X) = V(\alpha_1, \cdots, \alpha_{n-1}, X)$ qui est de degré $n-1$ (développement par rapport à la dernière colonne) s'annule en $\alpha_1, \cdots, \alpha_{n-1}$ deux à deux distincts, donc il existe $\lambda \in \mathbb{K}$ telle que $V(X) = \lambda \prod_{k=1}^{n-1} (X - \alpha_k)$. En développant le déterminant $V(X)$ par rapport à la dernière colonne, on voit que λ qui est le coefficient de X^{n-1} est égal à $\Delta(\alpha_1, \cdots, \alpha_{n-1})$, ce qui nous donne par évaluation en α_n, $\Delta(\alpha_1, \cdots, \alpha_n) = \Delta(\alpha_1, \cdots, \alpha_{n-1}) \prod_{k=1}^{n-1} (\alpha_n - \alpha_k)$ et on conclut encore par récurrence.

□

Avec le théorème précédent, on retrouve le fait que $V(\alpha_1, \cdots, \alpha_n)$ est inversible si, et seulement si, les α_k pour k compris entre 1 et n sont deux à deux distincts.

Exemple 2.3 *Pour $n \geq 2$, on a :*

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{n-1} & \cdots & n^{n-1} \end{vmatrix} = \prod_{1 \le 1 < j \le n} (j - i) = \prod_{j=2}^{n} \prod_{i=1}^{j-1} (j - i) = \prod_{j=2}^{n} (j-1)! = \prod_{j=1}^{n-1} j!$$

Dans le cas où les α_k sont deux à deux distincts, on peut donner une expression de l'inverse d'une matrice de Vandermonde, en utilisant les polynômes d'interpolation de Lagrange. Pour ce faire, on introduit l'application linéaire $\varphi_n : \mathbb{K}_{n-1}[X] \to \mathbb{K}^n$ définie par $\varphi_n(P) = (P(\alpha_i))_{1 \le i \le n}$ pour tout $P \in \mathbb{K}_{n-1}[X]$. La matrice de φ_n

dans les bases canoniques $\mathcal{B}=(e_i)_{1\leq i\leq n}$ de $\mathbb{K}^n$ et $\mathcal{B}'=\left(X^{j-1}\right)_{1\leq j\leq n}$ de $\mathbb{K}_{n-1}[X]$ et $\mathbb{K}^n$ est donnée par :

$$\varphi_n\left(X^{j-1}\right)=\begin{pmatrix}\alpha_1^{j-1}\\ \alpha_2^{j-1}\\ \vdots\\ \alpha_n^{j-1}\end{pmatrix}\ (1\leq j\leq n)$$

ce qui nous dit que c'est la matrice transposée de Vandermonde ${}^tV(\alpha_1,\cdots,\alpha_n)$. En notant $\mathcal{L}=(L_i)_{1\leq i\leq n}$ la base de Lagrange définie par $L_i(X)=\prod_{\substack{j=1\\ j\neq i}}^{n}\frac{X-\alpha_j}{\alpha_i-\alpha_j}$, on a $L_i(\alpha_j)=\delta_{i,j}$ pour tous i,j compris entre 1 et n, soit $\varphi_n(L_i)=e_i$ et $\varphi_n^{-1}(e_i)=L_i$ pour tout i compris entre entre 1 et n, ce qui nous dit que ${}^tV(\alpha_1,\cdots,\alpha_n)^{-1}=P_{\mathcal{B}',\mathcal{L}}$ est la matrice de passage de la base canonique $\mathcal{B}'=\left(X^{j-1}\right)_{1\leq j\leq n}$ à la base de Lagrange $\mathcal{L}=(L_i)_{1\leq i\leq n}$ et $V(\alpha_1,\cdots,\alpha_n)^{-1}={}^tP_{\mathcal{B}',\mathcal{L}}$. Par exemple pour $n=2$, on a $V(\alpha_1,\alpha_2)^{-1}=\frac{1}{\alpha_2-\alpha_1}\begin{pmatrix}\alpha_2 & -1\\ -\alpha_1 & 1\end{pmatrix}$ et pour $n=3$:

$$L_1(X)=\frac{(X-\alpha_2)(X-\alpha_3)}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)},\ L_2(X)=\frac{(X-\alpha_1)(X-\alpha_3)}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)}$$
$$L_3(X)=\frac{(X-\alpha_1)(X-\alpha_2)}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)}$$

$$V(\alpha_1,\alpha_2,\alpha_3)^{-1}=\begin{pmatrix}\frac{\alpha_2\alpha_3}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} & -\frac{\alpha_2+\alpha_3}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)} & \frac{1}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}\\ \frac{\alpha_1\alpha_3}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)} & -\frac{\alpha_1+\alpha_3}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)} & \frac{1}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)}\\ \frac{\alpha_1\alpha_2}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)} & -\frac{\alpha_1+\alpha_2}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)} & \frac{1}{(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)}\end{pmatrix}$$
$$=\frac{1}{\Delta(\alpha_1,\alpha_2,\alpha_3)}\begin{pmatrix}\alpha_2\alpha_3(\alpha_3-\alpha_2) & -\left(\alpha_3^2-\alpha_2^2\right) & (\alpha_3-\alpha_2)\\ -\alpha_1\alpha_3(\alpha_3-\alpha_1) & \alpha_3^2-\alpha_1^2 & -(\alpha_3-\alpha_1)\\ \alpha_1\alpha_2(\alpha_2-\alpha_1) & -\left(\alpha_2^2-\alpha_1^2\right) & (\alpha_2-\alpha_1)\end{pmatrix}$$

Les matrices de Vandermonde peuvent être généralisées en considérant les matrices de la forme :

$$V(\alpha_1,\cdots,\alpha_n,P_1,\cdots,P_n)=((P_i(\alpha_j)))_{1\leq i,j\leq n}=\begin{pmatrix}P_1(\alpha_1) & \cdots & P_1(\alpha_n)\\ \vdots & \ddots & \vdots\\ P_n(\alpha_1) & \cdots & P_n(\alpha_n)\end{pmatrix}$$

où $(P_j)_{1\leq j\leq n}$ est une suite de polynômes dans $\mathbb{K}_{n-1}[X]$. Pour simplifier, on notera V_n une telle matrice. Cette matrice est une matrice de Vandermonde pour $P_j(X)=X^{j-1}$.

Théorème 2.17.

En notant $Q(P_1,\cdots,P_n)$ la matrice dont les colonnes sont formées des composantes de chaque polynôme P_k dans la base canonique de $\mathbb{K}_{n-1}[X]$, on a :

$$\det\begin{pmatrix} P_1(\alpha_1) & \cdots & P_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ P_n(\alpha_1) & \cdots & P_n(\alpha_n) \end{pmatrix} = \Delta(\alpha_1,\cdots,\alpha_n)\det(Q(P_1,\cdots,P_n))$$

Dans le cas particulier où chaque polynôme P_k, pour k compris entre 1 et $n-1$ est unitaire de degré $k-1$, on a $\det(A_n) = \Delta(\alpha_1,\cdots,\alpha_n)$.

Preuve. En notant $P_j(X) = \sum_{i=0}^{n-1} a_{ij}X^j$ pour tout entier j compris entre 1 et n, on a :

$$\begin{aligned} V_n &= \begin{pmatrix} a_{0,1} & \cdots & a_{n-1,1} \\ \vdots & \ddots & \vdots \\ a_{n,0} & \cdots & a_{n-1,n} \end{pmatrix} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \\ &= {}^tQ(P_1,\cdots,P_n)\,V(\alpha_1,\cdots,\alpha_n) \end{aligned}$$

où $Q(P_1,\cdots,P_n)$ est la matrice dont les colonnes sont formées des composantes de chaque polynôme P_j dans la base canonique de $\mathbb{K}_{n-1}[X]$ (dans le où la famille $(P_j)_{1\leq j\leq n}$ est libre, cette matrice est la matrice de passage de $\left(X^{j-1}\right)_{1\leq j\leq n}$ à $(P_j)_{1\leq j\leq n}$), donc $\det(V_n) = \Delta(\alpha_1,\cdots,\alpha_n)\det(Q(P_1,\cdots,P_n))$.

Dans le cas particulier où chaque polynôme P_k, pour k compris entre 1 et $n-1$ est unitaire de degré $k-1$, la matrice $Q(P_1,\cdots,P_n)$ est triangulaire supérieure avec tous ses termes diagonaux égaux à 1, donc $\det(Q(P_1,\cdots,P_n)) = 1$ et $\det(A_n) = \Delta(\alpha_1,\cdots,\alpha_n)$. □

Dans le cas où les α_k sont deux à deux distincts, en prenant pour polynômes P_j les polynômes de Lagrange $L_j(X) = \prod_{\substack{i=1\\ i\neq j}}^{n} \frac{X-\alpha_i}{\alpha_j-\alpha_i}$, on a :

$$V_n = I_n = {}^tQ(L_1,\cdots,L_n)\,V(\alpha_1,\cdots,\alpha_n)$$

ce qui nous permet de retrouver l'inverse $V(\alpha_1,\cdots,\alpha_n)^{-1} = {}^tQ(L_1,\cdots,L_n)$.

Exemple 2.4 *Prenant $\alpha_k = k$ et $P_k(X) = (X+k-1)^{n-1}$, on obtient :*

$$\det\begin{pmatrix} 1^{n-1} & 2^{n-1} & \cdots & n^{n-1} \\ 2^{n-1} & 3^{n-1} & \cdots & (n+1)^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ n^{n-1} & (n+1)^{n-1} & \cdots & (2n-1)^{n-1} \end{pmatrix} = (-1)^{\frac{n(n-1)}{2}}\left((n-1)!\right)^{n-1}$$

(exercice 2.7).

Les déterminants de Vandermonde peuvent aussi être utilisés pour prouver que les vecteurs propres non nuls d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ associés à des valeurs propres deux à deux distinctes sont linéairement indépendants (exercice 2.4) ou encore pour prouver le théorème d'analyse réelle qui suit.

Théorème 2.18.

Si f est une fonction de classe $\mathcal{C}^{n+1}$ de $\mathbb{R}$ dans $\mathbb{R}$, avec $n \geq 1$, telle que f et $f^{(n+1)}$ soient bornées sur $\mathbb{R}$, alors toutes les dérivées $f^{(k)}$, pour k compris entre 1 et n, sont également bornées sur $\mathbb{R}$.

Preuve. Pour tout réel x et tout entier p compris entre 1 et n, la formule de Taylor à l'ordre n sur l'intervalle $[x, x+p]$ s'écrit :

$$f(x+p) - f(x) - \frac{f^{(n+1)}(x+p\theta_p)}{(n+1)!}p^{n+1} = \sum_{k=1}^{n} \frac{f^{(k)}(x)}{k!}p^k$$

avec $0 < \theta_p < 1$, ce qui peut s'écrire matriciellement $V(x) = AU(x)$, où on a noté :

$$V(x) = \begin{pmatrix} f(x+1) - f(x) - \dfrac{f^{(n+1)}(x+\theta_1)}{(n+1)!} \\ \vdots \\ f(x+n) - f(x) - \dfrac{f^{(n+1)}(x+n\theta_n)}{(n+1)!}n^{n+1} \end{pmatrix}, \; U(x) = \begin{pmatrix} \dfrac{f^{(1)}(x)}{1!} \\ \vdots \\ \dfrac{f^{(n)}(x)}{n!} \end{pmatrix}$$

et $A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2^2 & \cdots & 2^n \\ \vdots & \vdots & \ddots & \vdots \\ n & n^2 & \cdots & n^n \end{pmatrix}$. On a alors :

$$\det(A) = n! \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{vmatrix} = n! \prod_{j=1}^{n-1} j! \neq 0$$

(exemple 2.3), c'est-à-dire que A est inversible. On peut donc écrire que $U(x) = A^{-1}V(x)$ et $\|U(x)\|_\infty \leq \left\|A^{-1}\right\|_\infty \|V(x)\|_\infty$, soit :

$$\begin{aligned} \max_{1\leq k\leq n} \left|\frac{f^{(k)}(x)}{k!}\right| &\leq \left\|A^{-1}\right\|_\infty \max_{1\leq k\leq n} \left|f(x+p) - f(x) - \frac{f^{(n+1)}(x+p\theta_p)}{(n+1)!}p^{n+1}\right| \\ &\leq \left\|A^{-1}\right\|_\infty \left(2\|f\|_\infty + \frac{n^{n+1}}{(n+1)!}\left\|f^{(n+1)}\right\|_\infty\right) \end{aligned}$$

le réel x étant quelconque. On a donc pour tout entier k compris entre 1 et n :

$$\left\|f^{(k)}\right\|_\infty \leq k!\left\|A^{-1}\right\|_\infty \left(2\|f\|_\infty + \frac{n^{n+1}}{(n+1)!}\left\|f^{(n+1)}\right\|_\infty\right)$$

□

2.4.2 Déterminants circulants

On se donne un entier $n \geq 2$, des nombres complexes $a_0, \cdots, a_{n-1}$ et on leur associe la matrice circulante :

$$C(a_0, \cdots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \ddots & a_{n-3} & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \ddots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix} = \left((a_{j-i \bmod n})\right)_{0 \leq i,j \leq n-1}$$

où $j - i \bmod n$ désigne le reste appartenant à $\{0, 1, \cdots, n-1\}$ dans la division euclidienne de $j - i$ par n, ce qui signifie que $a_{ij} = a_{j-i}$ pour $0 \leq i \leq j \leq n-1$ et $a_{ij} = a_{j+n-i}$ pour $j+1 \leq i \leq n-1$. Pour toute racine n-ième de l'unité $z \in \mathbb{C}$, on a $z^n = 1$ et en notant $Z = \left(z^j\right)_{0 \leq j \leq n-1}$ dans $\mathbb{C}^n$:

$$C(a_0, \cdots, a_{n-1})\, Z = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \ddots & a_{n-3} & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \ddots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix} \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{n-2} \\ z^{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} a_0 + a_1 z + \cdots + a_{n-2} z^{n-2} + a_{n-1} z^{n-1} \\ z\left(a_0 + a_1 z + \cdots + a_{n-2} z^{n-2} + a_{n-1} z^{n-1}\right) \\ \vdots \\ z^{n-2}\left(a_0 + a_1 z + \cdots + a_{n-2} z^{n-2} + a_{n-1} z^{n-1}\right) \\ z^{n-1}\left(a_0 + a_1 z + \cdots + a_{n-2} z^{n-2} + a_{n-1} z^{n-1}\right) \end{pmatrix} = P(z) \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{n-2} \\ z^{n-1} \end{pmatrix}$$

où $P(X) = \sum_{k=0}^{n-1} a_k X^k$, ce qui nous dit que $P(z)$ est vecteur propre de la matrice $C(a_0, \cdots, a_{n-1})$, le vecteur Z étant un vecteur propre associé. Ce résultat peut aussi se justifier en disant que, pour $0 \leq i \leq n-1$, la composante numéro de i de $C(a_0, \cdots, a_{n-1})\, Z$ est :

$$\sum_{j=0}^{n-1} a_{ij} z^j = \sum_{j=0}^{i-1} a_{j+n-i} z^j + \sum_{j=i}^{n-1} a_{j-i} z^j = z^i \left(\sum_{j=0}^{i-1} a_{j+n-i} z^{n+j-i} + \sum_{j=i}^{n-1} a_{j-i} z^{j-i} \right)$$

$$= z^i \left(\sum_{k=n-i}^{n-1} a_k z^k + \sum_{k=0}^{n-i-1} a_k z^k \right) = z^i \sum_{k=0}^{n-1} a_k z^k = z^i P(z)$$

En notant $\omega_n = e^{\frac{2i\pi}{n}}$, chaque racine n-ième de l'unité ω_n^k pour $0 \leq k \leq n-1$, nous donne la valeur propre $P\left(\omega_n^k\right)$ de $C(a_0, \cdots, a_{n-1})$ avec $Z_k = \left(\omega_n^{kj}\right)_{0 \leq j \leq n-1}$ comme vecteur propre associé.

Comme $\det(Z_0, \cdots, Z_{n-1}) = \Delta\left(1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\right) \neq 0$ (ces racines de l'unité sont deux à deux distinctes), la famille de vecteur propres $(Z_k)_{0 \leq k \leq n-1}$ est une base

de $\mathbb{C}^n$, ce qui nous dit que $C(a_0, \cdots, a_{n-1})$ est diagonalisable de valeurs propres $P(1), P(\omega_n), \cdots, P\left(\omega_n^{n-1}\right)$. Il en résulte que $\det C(a_0, \cdots, a_{n-1}) = \prod_{k=0}^{n-1} P\left(\omega_n^k\right)$.

2.4.3 Déterminants de Gram

$(E, \langle \cdot \mid \cdot \rangle)$ désigne un espace vectoriel réel préhilbertien et $(x_i)_{1 \leq i \leq n}$ est une famille de $n \geq 2$ vecteurs de E.

Définition 2.6. *On appelle matrice de Gram de $(x_i)_{1 \leq i \leq n}$, la matrice :*

$$G(x_1, \cdots, x_n) = ((\langle x_i \mid x_j \rangle))_{1 \leq i,j \leq n} = \begin{pmatrix} \langle x_1 \mid x_1 \rangle & \langle x_1 \mid x_2 \rangle & \cdots & \langle x_1 \mid x_n \rangle \\ \langle x_2 \mid x_1 \rangle & \langle x_2 \mid x_2 \rangle & \cdots & \langle x_2 \mid x_n \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle x_n \mid x_1 \rangle & \langle x_n \mid x_2 \rangle & \cdots & \langle x_n \mid x_n \rangle \end{pmatrix}$$

et le déterminant $g(x_1, \cdots, x_n)$ de cette matrice est appelé déterminant de Gram de la famille $(x_i)_{1 \leq i \leq n}$.

Théorème 2.19.

On a, $\operatorname{rg}(G(x_1, \cdots, x_n)) = \operatorname{rg}(x_1, \cdots, x_n)$.

Preuve. Si tous les vecteurs x_i sont nuls, la matrice de Gram correspondante est alors la matrice nulle et le résultat est évident. On suppose donc que les x_i ne sont pas tous nuls et on désigne par F le sous-espace vectoriel de E engendré par $\{x_1, \cdots, x_n\}$. Le procédé de Gram-Schmidt nous permet de construire une base orthonormée $(e_i)_{1 \leq i \leq p}$ de F, avec $1 \leq p \leq n$, et dans cette base on écrit $x_i = \sum_{k=1}^{p} a_{ki} e_k$. Pour i, j compris entre 1 et n, on a alors :

$$\langle x_i \mid x_j \rangle = \sum_{k=1}^{p} a_{ki} a_{kj} = (a_{1i}, \cdots, a_{pi}) \begin{pmatrix} a_{1j} \\ \vdots \\ a_{pj} \end{pmatrix}$$

soit, $G(x_1, \cdots, x_n) = {}^tAA$ où $A = ((a_{ij}))_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \in \mathcal{M}_{p,n}(\mathbb{R})$. Munissant $\mathbb{R}^n$ et $\mathbb{R}^p$ de leurs structures euclidiennes canoniques, on a $\langle {}^tAAX \mid X \rangle_{\mathbb{R}^n} = \langle AX \mid AX \rangle_{\mathbb{R}^p} = \|AX\|^2_{\mathbb{R}^p}$ pour tout $X \in \mathbb{R}^n$ et on en déduit que $\ker({}^tAA) = \ker(A)$, puis avec le théorème du rang que les matrices ${}^tAA$ et A ont même rang. On a donc $\operatorname{rg}(G(x_1, \cdots, x_n)) = \operatorname{rg}(A) = \operatorname{rg}(x_1, \cdots, x_n)$ puisque A est la matrice du système de vecteurs $(x_i)_{1 \leq i \leq n}$ dans la base $(e_i)_{1 \leq i \leq p}$. □

Corollaire 2.2. *On a $g(x_1, \cdots, x_n) \geq 0$ et la famille $(x_i)_{1 \leq i \leq n}$ est libre si, et seulement si, on a $g(x_1, \cdots, x_n) > 0$.*

Preuve. On reprend les notations de la démonstration du théorème 2.19. Si le système $(x_i)_{1 \leq i \leq n}$ est lié, on a alors $\operatorname{rg}(G(x_1, \cdots, x_n)) = \operatorname{rg}(A) < n$ et la matrice $G(x_1, \cdots, x_n)$ est non inversible dans $\mathcal{M}_n(\mathbb{R})$, son déterminant est donc nul. Si le système $(x_i)_{1 \leq i \leq n}$ est libre, on a alors $\operatorname{rg}(G(x_1, \cdots, x_n)) = \operatorname{rg}(A) = n$ et la matrice $G(x_1, \cdots, x_n)$ est inversible dans $\mathcal{M}_n(\mathbb{R})$, son déterminant est donc non nul. En considérant que la matrice $G(x_1, \cdots, x_n) = {}^tAA$ est symétrique positive ($\langle {}^tAAX \mid X \rangle_{\mathbb{R}^n} = \|AX\|^2_{\mathbb{R}^n} \geq 0$ pour tout $X \in \mathbb{R}^n$), on déduit que ce déterminant est strictement positif. □

Les déterminants de Gram peuvent être utilisés pour calculer la distance d'un point à un sous-espace vectoriel de dimension finie de E.

Théorème 2.20.

Soient F un sous-espace vectoriel de dimension finie de E et $(x_i)_{1 \leq i \leq n}$ une base de F. Pour tout x dans E, on a $d(x, F) = \sqrt{\dfrac{g(x_1, \cdots, x_n, x)}{g(x_1, \cdots, x_n)}}$ et la meilleure approximation de x par des éléments de F est le vecteur $y = \displaystyle\sum_{j=1}^{n} \frac{g_{j,x}(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)} x_j$, où $g_{j,x}(x_1, \cdots, x_n)$ est le déterminant de la matrice déduite de la matrice de Gram $G(x_1, \cdots, x_n)$ en remplaçant sa colonne numéro j par $\begin{pmatrix} \langle x_1 \mid x \rangle \\ \vdots \\ \langle x_n \mid x \rangle \end{pmatrix}$.

Preuve. En notant y la projection orthogonale de x sur F, on a :

$$d(x, F)^2 = \|x - y\|^2 = \|x\|^2 - \|y\|^2$$

et pour tout i compris entre 1 et n, $\langle x_i \mid x \rangle = \langle x_i \mid x - y \rangle + \langle x_i \mid y \rangle = \langle x_i \mid y \rangle$ du fait que $x - y \in F^{\perp}$ et $x_i \in F$. En utilisant la linéarité du déterminant par rapport à la dernière colonne, on en déduit que :

$$\begin{aligned} g(x_1, \cdots, x_n, x) &= \begin{pmatrix} \langle x_1 \mid x_1 \rangle & \cdots & \langle x_1 \mid x_n \rangle & \langle x_1 \mid y \rangle \\ \vdots & \ddots & \cdots & \vdots \\ \langle x_n \mid x_1 \rangle & \cdots & \langle x_n \mid x_n \rangle & \langle x_n \mid y \rangle \\ \langle x \mid x_1 \rangle & \cdots & \langle x \mid x_n \rangle & d(x, F)^2 + \|y\|^2 \end{pmatrix} \\ &= d(x, F)^2 \, g(x_1, \cdots, x_n) + g(x_1, \cdots, x_n, y) \\ &= d(x, F)^2 \, g(x_1, \cdots, x_n) \end{aligned}$$

(le système $\{x_1, \cdots, x_n, y\}$ étant lié, puisque $y \in F$, on a $g(x_1, \cdots, x_n, y) = 0$), soit $d(x, F) = \sqrt{\dfrac{g(x_1, \cdots, x_n, x)}{g(x_1, \cdots, x_n)}}$. D'autre part, la projection orthogonale y de x

sur F s'écrit $y = \sum_{j=1}^{n} a_j x_j$, les coefficients a_j étant solutions du système d'équations normales :

$$G(x_1, \cdots, x_n) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \langle x_1 \mid x \rangle \\ \vdots \\ \langle x_n \mid x \rangle \end{pmatrix}$$

et en utilisant les formules de Cramer, on obtient $a_j = \dfrac{g_{j,x}(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)}$ pour j compris entre 1 et n. □

En utilisant le procédé d'orthogonalisationn de Gram-Schmidt, on peut donner une expression du déterminant de Gram d'une famille libre. On rappelle que la mesure principale de l'angle géométrique de deux vecteurs x, y non nuls dans E est le réel $\theta \in [0, \pi]$ définie par $\langle x \mid y \rangle = \cos(\theta) \|x\| \|y\|$.

Théorème 2.21.

Soient $(x_i)_{1 \leq i \leq n}$ une famille libre de vecteurs dans $(E, \langle \cdot \mid \cdot \rangle)$, $F = \text{Vect}\{x_1, \cdots, x_n\}$ et $(e_i)_{1 \leq i \leq n}$ la base orthonormée de F déduite par le procédé de Gram-Schmidt avec la condition $\langle x_k \mid e_k \rangle > 0$ pour tout k compris entre 1 et n. On a :

$$\begin{aligned} g(x_1, \cdots, x_n) &= \prod_{k=2}^{n} \cos^2(x_k, e_k) \prod_{k=1}^{n} \|x_k\|^2 \\ &= \sin^2(x_1, x_2) \prod_{k=3}^{n} \cos^2(x_k, e_k) \prod_{k=1}^{n} \|x_k\|^2 \quad \textit{(pour } n \geq 3\textit{)} \end{aligned}$$

Preuve. La base orthonormée de F déduite de la base $(x_i)_{1 \leq i \leq n}$ par le procédé de Gram-Schmidt est définie par $e_k = \dfrac{1}{\|y_k\|} y_k$ pour $1 \leq k \leq n$, où $y_1 = x_1$ et $y_k = x_k - \sum_{j=1}^{k-1} \langle x_k \mid e_j \rangle e_j$ pour $2 \leq k \leq n$. La matrice de passage de $(e_i)_{1 \leq i \leq n}$ à $(x_i)_{1 \leq i \leq n}$ est alors donnée par :

$$A = \begin{pmatrix} \|y_1\| & \langle x_2 \mid e_1 \rangle & \cdots & \langle x_n \mid e_1 \rangle \\ 0 & \|y_2\| & \ddots & \vdots \\ \vdots & \ddots & \ddots & \langle x_n \mid e_{n-1} \rangle \\ 0 & \cdots & 0 & \|y_n\| \end{pmatrix}$$

et $g(x_1, \cdots, x_n) = \det(A)^2 = \prod_{k=1}^{n} \|y_k\|^2$ (voir ladémonstration du théorème 2.19). De $x_k = \|y_k\| e_k + \sum_{j=1}^{k-1} \langle x_k \mid e_j \rangle e_j$, pour k compris entre 2 et n, et de l'orthogonalité des e_j, on déduit que $\|y_k\| = \langle x_k \mid e_k \rangle = \|x_k\| \cos(x_k, e_k)$, ce qui donne en tenant

compte de $\|y_1\| = \|x_1\|$:

$$g(x_1, \cdots, x_n) = \prod_{k=2}^{n} \cos^2(x_k, e_k) \prod_{k=1}^{n} \|x_k\|^2$$

Pour $n \geq 3$, en écrivant que :

$$\|y_2\|^2 = \|x_2 - \langle x_2 \mid e_1 \rangle e_1\|^2 = \|x_2\|^2 - \langle x_2 \mid e_1 \rangle^2$$

avec $\langle x_2 \mid e_1 \rangle = \|x_2\| \cos(x_2, e_1) = \|x_2\| \cos(x_2, x_1)$, on obtient :

$$\|y_2\|^2 = \|x_2\|^2 \left(1 - \cos^2(x_2, x_1)\right) = \|x_2\|^2 \sin^2(x_1, x_2)$$

et $g(x_1, \cdots, x_n) = \sin^2(x_1, x_2) \prod_{k=3}^{n} \cos^2(x_k, e_k) \prod_{k=1}^{n} \|x_k\|^2$. □

Théorème 2.22. Inégalités de Hadamard

On a $0 \leq g(x_1, \cdots, x_n) \leq \prod_{k=1}^{n} \|x_k\|^2$, *la borne inférieure [resp. supérieure] étant atteinte si, et seulement si, la famille* $(x_i)_{1 \leq i \leq n}$ *est liée [resp. orthogonale].*

Preuve. Si la famille $(x_i)_{1 \leq i \leq n}$ est liée, on a alors $g(x_1, \cdots, x_n) = 0$. On suppose donc cette famille libre et dans ce cas, on a $g(x_1, \cdots, x_n) > 0$ et le théorème précédent nous dit que $g(x_1, \cdots, x_n) \leq \prod_{k=1}^{n} \|x_k\|^2$, l'égalité étant réalisée si, et seulement si, on a $\cos^2(x_k, e_k) = 1$ pour tout k compris entre 2 et n, ce qui compte tenu de $\|y_k\|^2 = \cos^2(x_k, e_k) \|x_k\|^2 = \|x_k\|^2 - \sum_{j=1}^{k-1} \langle x_k \mid e_j \rangle^2$ équivaut à $\langle x_k \mid e_j \rangle = 0$ pour tout j compris entre 1 et $k-1$, soit à $x_k = y_k = \|y_k\| e_k$ pour tout k compris entre 1 et n et la famille $(x_i)_{1 \leq i \leq n}$ est orthogonale. □

En notant $C_j = (a_{ij})_{1 \leq i \leq n} \in \mathbb{R}^n$ la colonne numéro j d'une matrice A dans $\mathcal{M}_n(\mathbb{R})$ et en munissant $\mathbb{R}^n$ de son produit scalaire canonique, on a :

$$\begin{aligned} {}^tAA &= \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{n,n} \end{pmatrix} \\ &= \begin{pmatrix} \langle C_1 \mid C_1 \rangle & \langle C_1 \mid C_2 \rangle & \cdots & \langle C_1 \mid C_n \rangle \\ \langle C_2 \mid C_1 \rangle & \langle C_2 \mid C_2 \rangle & \cdots & \langle C_2 \mid C_n \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle C_n \mid C_1 \rangle & \langle C_n \mid C_2 \rangle & \cdots & \langle C_n \mid C_n \rangle \end{pmatrix} \end{aligned}$$

et l'inégalité de Hadamard prend la forme :

$$(\det(A))^2 = \det\left({}^tAA\right) = g(C_1, \cdots, x_n) \leq \prod_{k=1}^{n} \|C_k\|^2$$

soit $|\det(A)| \leq \prod_{k=1}^{n} \|C_k\|$.

Exemple 2.5 *Prenant pour matrice A une matrice de Vandermonde* $V(\alpha_1, \cdots, \alpha_n)$, *où* $(\alpha_k)_{1\leq k\leq n} \in \mathbb{R}^n$, *on aboutit à :*

$$\prod_{1\leq i<j\leq n} |\alpha_j - \alpha_i| \leq \prod_{k=1}^{n} \sqrt{1 + \alpha_k^2 + \cdots + \alpha_k^{2(n-1)}}$$

prenant les α_k *dans* $[-1, 1]$, *on obtient* $\prod_{1\leq i<j\leq n} |\alpha_j - \alpha_i| \leq \prod_{k=1}^{n} \sqrt{n} = n^{\frac{n}{2}}$.

2.4.4 Déterminants de Cauchy

À tout entier $n \geq 2$ et toutes suites $(\alpha_k)_{1\leq k\leq n}$ et $(\beta_k)_{1\leq k\leq n}$ d'éléments de $\mathbb{K}$ telles $\alpha_i + \beta_j$ pour tous i, j compris entre 1 et n, on associe la matrice de Cauchy :

$$\left(\left(\frac{1}{\alpha_i + \beta_j}\right)\right)_{1\leq i,j\leq n} = \begin{pmatrix} \frac{1}{\alpha_1+\beta_1} & \cdots & \frac{1}{\alpha_1+\beta_{n-1}} & \frac{1}{\alpha_1+\beta_n} \\ \vdots & \ddots & \vdots & \vdots \\ \frac{1}{\alpha_{n-1}+\beta_1} & \cdots & \frac{1}{\alpha_{n-1}+\beta_{n-1}} & \frac{1}{\alpha_{n-1}+\beta_n} \\ \frac{1}{\alpha_n+\beta_1} & \cdots & \frac{1}{\alpha_n+\beta_{n-1}} & \frac{1}{\alpha_n+\beta_n} \end{pmatrix}$$

Théorème 2.23.

On a :

$$\det\left(\left(\frac{1}{\alpha_i + \beta_j}\right)\right)_{1\leq i,j\leq n} = \frac{\prod_{1\leq i<j\leq n} (\beta_j - \beta_i)(\alpha_j - \alpha_i)}{\prod_{1\leq i,j\leq n} (\alpha_i + \beta_j)}$$

(déterminant de Cauchy).

Preuve. S'il existe deux indices $i \neq j$ tels que $\alpha_j = \alpha_i$ [resp. $\beta_j = \beta_i$], la matrice de Cauchy $A_n = \left(\left(\frac{1}{\alpha_i + \beta_j}\right)\right)_{1\leq i,j\leq n}$ a alors deux lignes [resp. deux colonnes] identiques et son déterminant est nul. L'égalité annoncée est donc trivialement vérifiée dans ce cas. On suppose que les α_i, ainsi que les β_j sont deux à deux distincts et on désigne par F_n la fraction rationnelle $F_n(X) = \frac{\prod_{j=1}^{n-1} (X - \beta_j)}{\prod_{i=1}^{n} (X + \alpha_i)}$. Le numérateur de F_n est de degré $n-1$ et son dénominateur de degré n, on a donc une décomposition en éléments simples de la forme $F_n(X) = \sum_{k=1}^{n} \frac{\lambda_k}{X + \alpha_k}$, les co-

efficients λ_k étant donnés par $\lambda_k = \dfrac{\prod_{j=1}^{n-1}(\alpha_k+\beta_j)}{\prod_{\substack{i=1\\i\neq k}}^{n}(\alpha_k-\alpha_i)}$. En développant le déterminant suivant la dernière ligne, on a compte tenu de $F_n(\beta_j)=0$ pour tout j compris entre 0 et $n-1$:

$$D_n = \begin{vmatrix} \frac{1}{\alpha_1+\beta_1} & \cdots & \frac{1}{\alpha_1+\beta_{n-1}} & \frac{1}{\alpha_1+\beta_n} \\ \vdots & \ddots & \vdots & \vdots \\ \frac{1}{\alpha_{n-1}+\beta_1} & \cdots & \frac{1}{\alpha_{n-1}+\beta_{n-1}} & \frac{1}{\alpha_{n-1}+\beta_n} \\ F_n(\beta_1) & \cdots & F_n(\beta_{n-1}) & F_n(\beta_n) \end{vmatrix} = F_n(\beta_n)\det(A_{n-1})$$

D'autre part, en écrivant que $F_n(\beta_j) = \sum_{k=1}^{n} \dfrac{\lambda_k}{\beta_j+\alpha_k}$ et en utilisant le fait que det est une forme multilinéaire alternée, on a aussi $D_n = \lambda_n \det(A_n)$. On a donc $F_n(\beta_n)\det(A_{n-1}) = \lambda_n \det(A_n)$ et :

$$\det(A_n) = \frac{F_n(\beta_n)}{\lambda_n}\det(A_{n-1}) = \frac{\prod_{j=1}^{n-1}(\beta_n-\beta_j)(\alpha_n-\alpha_i)}{\prod_{i=1}^{n}(\beta_n+\alpha_i)\prod_{j=1}^{n-1}(\alpha_n+\beta_j)}\det(A_{n-1})$$

On conclut alors par récurrence sur $n \geq 2$. Pour $n=2$, on a :

$$\det(A_2) = \begin{vmatrix} \frac{1}{\alpha_1+\beta_1} & \frac{1}{\alpha_1+\beta_2} \\ \frac{1}{\alpha_2+\beta_1} & \frac{1}{\alpha_2+\beta_2} \end{vmatrix} = \frac{(\beta_2-\beta_1)(\alpha_2-\alpha_1)}{(\alpha_1+\beta_1)(\alpha_1+\beta_2)(\alpha_2+\beta_1)(\alpha_2+\beta_2)}$$

Et supposant le résultat acquis pour $n-1$, on a :

$$\begin{aligned}\det(A_n) &= \frac{\prod_{j=1}^{n-1}(\beta_n-\beta_j)(\alpha_n-\alpha_i)}{\prod_{i=1}^{n}(\beta_n+\alpha_i)\prod_{j=1}^{n-1}(\alpha_n+\beta_j)} \frac{\prod_{1\leq i<j\leq n-1}(\beta_j-\beta_i)(\alpha_j-\alpha_i)}{\prod_{1\leq i,j\leq n-1}(\alpha_i+\beta_j)} \\ &= \frac{\prod_{1\leq i<j\leq n}(\beta_j-\beta_i)(\alpha_j-\alpha_i)}{\prod_{i=1}^{n}(\beta_n+\alpha_i)\prod_{i=1}^{n}(\beta_{n-1}+\alpha_i)\cdots\prod_{i=1}^{n}(\beta_1+\alpha_i)} \\ &= \frac{\prod_{1\leq i<j\leq n}(\beta_j-\beta_i)(\alpha_j-\alpha_i)}{\prod_{1\leq i,j\leq n}(\alpha_i+\beta_j)}\end{aligned}$$

□

Exemple 2.6 *On se place sur l'espace préhilbertien $\mathcal{C}^0([0,1])$ muni du produit scalaire $(f,g) \mapsto \langle f \mid g\rangle = \int_0^1 f(t)\,g(t)\,dt$ et on se donne une suite strictement*

strictement croissante $(\lambda_k)_{k\in\mathbb{N}}$ *de réels positif à laquelle on associe la suite de fonctions* $(\theta_k)_{k\in\mathbb{N}}$ *définie par* $\theta_k(t) = t^{\lambda_k}$ *pour tout* $t \in [0,1]$. *Pour tout* $n \in \mathbb{N}^*$, *le déterminant de Gram de* $(\theta_0, \cdots, \theta_n)$ *est alors donné par :*

$$\begin{aligned} g(\theta_0, \cdots, \theta_n) &= \det\left(\left(\langle \theta_i \mid \theta_j \rangle\right)\right)_{0\leq i,j\leq n} = \det\left(\left(\int_0^1 t^{\lambda_i+\lambda_j} dt\right)\right)_{0\leq i,j\leq n} \\ &= \det\left(\left(\frac{1}{\lambda_i+\lambda_j+1}\right)\right)_{0\leq i,j\leq n} = \frac{\prod\limits_{0\leq i<j\leq n} (\lambda_j-\lambda_i)^2}{\prod\limits_{0\leq i,j\leq n} (\lambda_i+\lambda_j+1)} \\ &= \prod_{j=0}^{n} \frac{\prod\limits_{i=0}^{j-1} (\lambda_j-\lambda_i)^2}{\prod\limits_{i=0}^{n} (\lambda_j+\lambda_i+1)} \end{aligned}$$

Les matrices de Gram correspondantes au choix de $\lambda_k = k$ *pour tout* $k \in \mathbb{N}$ *(*$(\theta_k)_{k\in\mathbb{N}}$ *est la base canonique de l'espace des fonctions polynomiales sur* $[0,1]$*) sont les matrices de Hilbert* $H_n = \left(\left(\int_0^1 t^{i+j} dt\right)\right)_{0\leq i,j\leq n} = \left(\left(\frac{1}{i+j+1}\right)\right)_{0\leq i,j\leq n}$ *de déterminants :*

$$\det(H_n) = \prod_{j=0}^{n} \frac{\prod\limits_{i=0}^{j-1} (j-i)^2}{\prod\limits_{i=0}^{n} (i+j+1)} = \prod_{j=0}^{n} \frac{(j!)^3}{(n+j+1)!} = \frac{\left(\prod\limits_{j=2}^{n} j!\right)^4}{\prod\limits_{j=2}^{2n+1} j!}$$

Les déterminants de l'exemple précédent apparaissent dans la démonstration du résultat de densité suivant.

Théorème 2.24. Müntz

L'espace vectoriel $\mathrm{Vect}\{\theta_n \mid n \in \mathbb{N}\}$ *est dense dans l'espace préhilbertien* $\left(\mathcal{C}^0([0,1]), \langle \cdot \mid \cdot \rangle\right)$ *(convergence quadratique) si, et seulement si, on a* $\sum\limits_{n=1}^{+\infty} \frac{1}{\lambda_n} = +\infty$. *Si on suppose de plus que* $\lambda_0 = 0$ *et* $\lambda_1 \geq 1$, *alors l'espace vectoriel* $\mathrm{Vect}\{\theta_n \mid n \in \mathbb{N}\}$ *est dense dans* $\left(\mathcal{C}^0([0,1]), \|\cdot\|_\infty\right)$ *(convergence uniforme) si, et seulement si, on a* $\sum\limits_{n=1}^{+\infty} \frac{1}{\lambda_n} = +\infty$.

Exemple 2.7 *En notant* $(p_n)_{n\geq 1}$ *la suite des nombres premiers rangée dans l'ordre croissant,* $\mathrm{Vect}\{1, x^{p_n} \mid n \geq 1\}$ *est dense dans* $\left(\mathcal{C}^0([0,1]), \|\cdot\|_\infty\right)$.

2.5 Exemples d'utilisation du déterminant

2.5.1 Rang d'une matrice ou d'un endomorphisme

Pour tout matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ et tout entier j compris entre 1 et n, on note $C_j \in \mathbb{K}^m$ la colonne numéro j de A.

Définition 2.7. *Le rang d'une matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est la dimension du sous-espace vectoriel de $\mathbb{K}^m$ engendré par ses colonnes :*

$$\operatorname{rg}(A) = \dim(\operatorname{Vect}(C_1, \cdots, C_n))$$

Il est équivalent de dire que le rang de A est égal au nombre maximum de vecteurs colonnes de A linéairement indépendants dans $\mathbb{K}^n$.

Définition 2.8. *Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F. Le rang de u est la dimension de $\operatorname{Im}(u)$. On le note $\operatorname{rg}(u)$.*

Théorème 2.25. Du rang

Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F. On a $\dim(E) = \dim(\ker(u)) + \operatorname{rg}(u)$.

Preuve. Soit H un supplémentaire de $\ker(u)$ dans E et v la restriction de u à H, c'est-à-dire l'application v définie sur H par $v(x) = u(x)$ pour tout $x \in H$. Le noyau de cette application est $\ker(v) = H \cap \ker(u) = \{0\}$, ce qui signifie que v est injective de H dans F et réalise une bijection de H sur $\operatorname{Im}(v)$. En écrivant tout vecteur y de $\operatorname{Im}(u)$ sous la forme $y = u(x)$ avec $x \in E$ qui s'écrit $x = x_1 + x_2$ où $x_1 \in \ker(u)$ et $x_2 \in H$, on a $y = u(x_1) + u(x_2) = v(x_2)$, c'est-à-dire que y est dans $\operatorname{Im}(v)$. On a donc $\operatorname{Im}(u) \subset \operatorname{Im}(v)$ et comme $\operatorname{Im}(v) \subset \operatorname{Im}(u)$, on a en fait $\operatorname{Im}(v) = \operatorname{Im}(u)$ et v réalise un isomorphisme de H sur $\operatorname{Im}(u)$. Il en résulte que $\operatorname{rg}(u) = \dim(\operatorname{Im}(u)) = \dim(H) = \dim(E) - \dim(\ker(u))$. □

Théorème 2.26.

Le rang d'une matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est égal au rang de l'application linéaire $u \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$ canoniquement associé à la matrice A.

Preuve. En notant $\mathcal{B} = (e_k)_{1 \leq k \leq n}$ la base canonique de $\mathbb{K}^n$ et $\mathcal{B}' = (f_k)_{1 \leq k \leq m}$ celle de $\mathbb{K}^m$, pour tout j compris entre 1 et n, la colonne numéro j de A est $C_j = u(e_j)$ et on a :

$$\operatorname{rg}(A) = \operatorname{rg}(C_1, C_2, \cdots, C_n) = \operatorname{rg}(u(e_1), u(e_2), \cdots, u(e_n)) = \operatorname{rg}(u)$$

□

Théorème 2.27.

Si $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est la matrice de $u \in \mathcal{L}(E,F)$ dans des bases $\mathcal{B}$ de E et $\mathcal{B}'$ de F, on a alors $\operatorname{rg}(u) = \operatorname{rg}(A)$.

Preuve. Soient $\mathcal{B} = (e_k)_{1\leq k\leq n}$ une base de E, $\mathcal{B}' = (f_k)_{1\leq k\leq m}$ une base de F et $u \in \mathcal{L}(E,F)$ de matrice A dans ces bases. Dire que $x = \sum_{j=1}^{n} x_j e_j$ est dans le noyau de u équivaut à dire que $u(x) = 0$, ce qui se traduit par $AX = 0$, où $X = (x_j)_{1\leq j\leq n}$ est le vecteur de $\mathbb{K}^n$ formé des composantes de x dans la base $\mathcal{B}$. En désignant par v l'application linéaire canoniquement associée à A, on a $v(X) = AX = 0$, c'est-à-dire que X est dans le noyau de v. Réciproquement si $X \in \ker(v)$, on a $AX = 0$, ce qui équivaut à $u(x) = 0$, soit $x \in \ker(u)$. L'application $x \mapsto X$ réalise donc un isomorphisme de $\ker(u)$ sur $\ker(v)$ et $\dim(\ker(u)) = \dim(\ker(v))$, ce qui équivaut à $\operatorname{rg}(u) = \operatorname{rg}(v) = rg(A)$ en utilisant le théorème du rang. □

Définition 2.9. *Une matrice extraite de $A = ((a_{i,j}))_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \in \mathcal{M}_{m,n}(\mathbb{K})$ est une matrice $A_{I,J} = ((a_{i,j}))_{(i,j)\in I\times J}$, où :*

$$I = \{1 \leq i_1 < \cdots < i_q \leq m\} \text{ et } J = \{1 \leq j_1 < \cdots < j_p \leq n\}$$

Un déterminant extrait de A (ou de $\det(A)$) est le déterminant d'une matrice carrée extraite de A. Si δ_p est un déterminant extrait de A d'ordre p, on appelle bordant de δ tout déterminant δ_{p+1} extrait d'ordre $p+1$ de A tel que δ_p soit extrait de δ_{p+1}.

Théorème 2.28.

Une matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est de rang r si, et seulement si, il existe un déterminant extrait de A, δ_r d'ordre r et non nul tel que tous les bordants de δ_r sont nuls (si $r = \min(n,m)$, la deuxième condition n'est pas à prendre en compte).

Preuve. Voir [**?**], volume 1. □

Corollaire 2.3. *Le rang d'une matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ est l'ordre du plus grand déterminant extrait de A qui est non nul.*

2.5.2 Systèmes de Cramer

On appelle système de Cramer tout système linéaire $Ax = b$ d'inconnue $x \in \mathbb{K}^n$, où $A \in GL_n(\mathbb{K})$ et $b \in \mathbb{K}^n$. L'unique solution d'un tel système est $x = A^{-1}b$. En notant $x = (x_j)_{1\leq j\leq n} \in \mathbb{K}^n$ cette solution, on a $b = \sum_{j=1}^{n} x_j C_j$ et en utilisant le caractère multilinéaire alterné du déterminant, on a pour tout entier k compris

entre 1 et n :

$$\det(C_1,\cdots,C_{k-1},b,C_{k+1},\cdots,C_n)=\sum_{j=1}^{n}x_j\det(C_1,\cdots,C_{k-1},C_j,C_{k+1},\cdots,C_n)$$
$$=x_k\det(A)$$

soit $x_k=\dfrac{\det(C_1,\cdots,C_{k-1},b,C_{k+1},\cdots,C_n)}{\det(A)}$ pour $1\leq k\leq n$. En calculant un déterminant par la formule (2.1), cela nécessite $n!(n-1)$ multiplications et $(n!-1)$ additions, donc environ $nn!$ opérations élémentaires. Comme il y a $n+1$ déterminants à calculer puis n divisions à faire pour les formules de Cramer, on aura un total d'environ $n^2n!$ opérations élémentaires à effectuer, ce qui peut être beaucoup trop important pour de grandes valeurs de n.

Les formules de Cramer peuvent être utilisées pour déterminer l'ensemble des solutions d'un système linéaire de m équations à n inconnues $Ax=b$ d'inconnue $x\in\mathbb{K}^n$, où $A\in\mathcal{M}_{m,n}(\mathbb{K})\setminus\{0\}$ est de rang $r\in\{1,\min(n,m)\}$ et $b\in\mathbb{K}^m$.

Il existe des matrices carrées d'ordre r extraites de A de déterminant non nul (un tel déterminant est appelé déterminant principal de A) et toute matrice carrée extraite d'ordre plus grand ou égal à $r+1$ (s'il en existe) est de déterminant nul.

En effectuant au besoin des permutations de lignes ou de colonnes du système linéaire, on se ramène à une matrice A tel que la matrice $A_r=((a_{ij}))_{1\leq i,j\leq r}$ soit inversible. Le système linéaire :

$$\sum_{j=1}^{n}a_{ij}x_j=b_i\ \ (1\leq i\leq r)$$

est alors appelé système d'équations principales du système $Ax=b$.

Considérons d'abord le cas d'un système homogène $Ax=0$. Le système d'équations principales étant de rang r, l'ensemble de ses solutions est un sous-espace vectoriel de $\mathbb{K}^n$ de dimension $n-r$ et comme il contient l'ensemble $S(A,0)$ des solutions de $Ax=0$, qui est aussi de dimension $n-r$, ces deux espaces sont égaux. La résolution du système d'équations principales peut se faire en utilisant les formules de Cramer pour le système $A_rx^{(r)}=b^{(r)}$, où $x^{(r)}\in\mathbb{K}^r$ a pour composantes les inconnues principales $x_1,\cdots,x_r$ et $b^{(r)}=\left(-\sum_{j=r+1}^{n}a_{ij}x_j\right)_{1\leq i\leq r}\in\mathbb{K}^r$ (les sommes valant 0 pour $r=n$).

Exemple 2.8 *Considérons un système linéaire homogène de m équations à $m+1$ inconnues, $Ax=0$ avec $A=((a_{ij}))_{\substack{1\leq i\leq m\\1\leq j\leq m+1}}\in\mathcal{M}_{m,m+1}(\mathbb{K})$ de rang m, la matrice $((a_{ij}))_{1\leq i,j\leq m}$ étant inversible. Ce système est équivalent au système :*

$$\sum_{j=1}^{m}a_{ij}x_j=-a_{1,m+1}x_{m+1}\ \ (1\leq i\leq m)$$

où x_{m+1} est l'inconnue non principale. Sa solution est donnée par :

$$\begin{aligned} x_k &= \frac{\det(C_1,\cdots,C_{k-1},b_m,C_{k+1},\cdots,C_m)}{\det(A_m)} \\ &= -x_{m+1}\frac{\det(C_1,\cdots,C_{k-1},C_{m+1},C_{k+1},\cdots,C_m)}{\det(A_m)} \\ &= (-1)^{m+1-k}\,x_{m+1}\frac{\det(C_1,\cdots,C_{k-1},C_{k+1},\cdots,C_m,C_{m+1})}{\det(A_m)} \\ &= \frac{(-1)^{m+1}}{\det(A_m)}x_{m+1}\,(-1)^k\det(C_1,\cdots,C_{k-1},C_{k+1},\cdots,C_m,C_{m+1})\ \ (1\leq k\leq m) \end{aligned}$$

L'ensemble des solutions $S(A,0)$ est donc la droite vectorielle dirigée par le vecteur $v=(\alpha_k)_{1\leq k\leq m+1}$, où :

$$\alpha_k=(-1)^k\det(C_1,\cdots,C_{k-1},C_{k+1},\cdots,C_m,C_{m+1})\ \ (1\leq k\leq m)$$

et $\alpha_{m+1}=(-1)^{m+1}\det(A_m)$. Considérons, par exemple, le système :

$$\left\{\begin{array}{l} x+y+z-t=0 \\ 2x+y+z-2t=0 \\ x-y+z-3t=0 \end{array}\right.$$

Il équivaut au système d'inconnue non principale t :

$$\left\{\begin{array}{l} x+y+z=t \\ 2x+y+z=2t \\ x-y+z=3t \end{array}\right.$$

et de solution $x=t,\ y=-t,\ z=t$.

Revenons au système linéaire $Ax=b$ d'inconnue $x\in\mathbb{K}^n$, où $A\in\mathcal{M}_{m,n}(\mathbb{K})$ est de rang $r\geq 1$ et $b\in\mathbb{K}^m$. Ce système aura des solutions si, et seulement si, $b\in F=\mathrm{Vect}\{C_1,\cdots,C_n\}$, ce qui est équivalent à dire que $F=\mathrm{Vect}\{C_1,\cdots,C_n,b\}$ et revient à dire que $\mathrm{rg}(A,b)=\mathrm{rg}(A)=r$ et comme $\det(A_r)\neq 0$, cela équivaut à dire que :

$$\left|\begin{array}{ccccc} a_{11} & \cdots & a_{1r} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{r1} & & a_{rr} & b_r \\ a_{k1} & & a_{kr} & b_k \end{array}\right| = 0\ \ (r+1\leq k\leq n)$$

Si le système est compatible (*i.e.* l'ensemble de ses solutions est non vide), l'ensemble $S(A,b)$ des solutions de $Ax=b$ est alors un sous-espace affine de $\mathbb{K}^n$ de dimension $n-r$ dirigé par $S(A,0)$. L'ensemble des solutions du système d'équations principales est aussi un sous-espace affine de $\mathbb{K}^n$ de dimension $n-r$ et comme il contient $S(A,b)$, ces deux sous-espaces sont égaux. En définitive, quand il est compatible, le système $Ax=b$ est équivalent au système d'équations principales $A'_rx=b$, où $A'_r=((a_{ij}))_{\substack{1\leq i\leq r\\ 1\leq j\leq n}}$ (deux systèmes linéaires sont équivalents s'ils ont même ensemble de solutions). La résolution

de ce dernier système se faisant en utilisant les formules de Cramer pour le système $A_r x^{(r)} = b^{(r)}$, où $x^{(r)} \in \mathbb{K}^r$ a pour composantes les inconnues principales $x_1, \cdots, x_r$ et $b^{(r)} = \left(b_i - \sum_{j=r+1}^{n} a_{ij} x_j \right)_{1 \leq i \leq r} \in \mathbb{K}^r$ (les sommes valant 0 pour $r = n$). Nous avons donc montré le résultat suivant.

Théorème 2.29. Rouché-Fontené

Soient $A = ((a_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{m,n}(\mathbb{K})$ de rang $r \geq 1$ et $b \in \mathbb{K}^m$. On se donne une matrice $A_r = ((a_{ij}))_{(i,j) \in I \times J}$ dans $GL_r(\mathbb{K})$ extraite de A telle que $\det(A_r) \neq 0$.

1. *Le système $Ax = b$ est compatible si, et seulement si, $r = n$ ou $r \leq n-1$ et :*
$$\det \begin{pmatrix} A_r & (b_i)_{i \in I} \\ (a_{k,j})_{j \in J} & b_k \end{pmatrix} = 0 \ (k \in \{1, \cdots, n\} \setminus I)$$
2. *Si le système $Ax = b$ est compatible, il est alors équivalent au système d'équations principales $A'_r x = b$, où $A_r = ((a_{ij}))_{\substack{i \in I \\ 1 \leq j \leq n}}$ et les inconnues principales $(x_j)_{j \in J}$ s'obtienne comme solutions du système de Cramer $A_r x_r = b^{(r)}$, où $b^{(r)} \in \mathbb{K}^r$ est fonction de b et des inconnues non principales $(x_j)_{j \in \{1, \cdots, m\} \setminus J}$.*

2.5.3 Orientation d'un espace euclidien

E est un espace euclidien de dimension $n \geq 2$.

Théorème 2.30.

Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ sont deux bases orthonormées de E, alors la matrice de passage P de $\mathcal{B}$ à $\mathcal{B}'$ est une matrice orthogonale.

Preuve. L'application linéaire u définie par $u(e_j) = e'_j = \sum_{i=1}^{n} p_{ij} e_i$ pour tout j compris entre 1 et n est une isométrie puisqu'elle transforme une base orthonormée en base orthonormée et en conséquence sa matrice dans la base $\mathcal{B}$, qui n'est autre que la matrice $P = ((p_{ij}))_{1 \leq i,j \leq n}$, est orthogonale. □

Avec les notations du théorème précédent, on a $\det(P) = \det_{\mathcal{B}}(\mathcal{B}') = \pm 1$.

On définit une relation sur l'ensemble des bases orthonormées de E en disant qu'une base orthonormée $\mathcal{B}$ est en relation avec une base orthonormée $\mathcal{B}'$ si, et seulement si, la matrice de passage P de $\mathcal{B}$ à $\mathcal{B}'$ est dans $\mathcal{O}_n^+(\mathbb{R})$. On notera $\sim$ cette relation.

Théorème 2.31.

La relation $\sim$ ainsi définie est une relation d'équivalence et il y a exactement deux classes d'équivalence pour cette relation.

Preuve. Cette relation est réflexive puisque $I_n \in \mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{B} = I_d(\mathcal{B})$. Elle est symétrique puisque $P \in \mathcal{O}_n^+(\mathbb{R})$ entraîne $P^{-1} \in \mathcal{O}_n^+(\mathbb{R})$ et si P est la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, alors P^{-1} est la matrice de passage de $\mathcal{B}'$ à $\mathcal{B}$. Elle est transitive puisque le produit de deux matrices de $\mathcal{O}_n^+(\mathbb{R})$ est dans $\mathcal{O}_n^+(\mathbb{R})$ ($\mathcal{O}_n^+(\mathbb{R})$ est un groupe).

Soit $\mathcal{B} = (e_i)_{1\leq i\leq n}$ une base orthonormée de E fixée. Pour toute autre base orthonormée $\mathcal{B}' = (e'_i)_{1\leq i\leq n}$, en désignant par $P = ((p_{ij}))_{1\leq i,j\leq n}$ la matrice de passage P de $\mathcal{B}$ à $\mathcal{B}'$, on a soit $P \in \mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{B}' \sim \mathcal{B}$, soit $P \in \mathcal{O}_n^-(\mathbb{R})$ et en désignant par $\mathcal{B}^-$ la base orthonormée définie par $\mathcal{B}^- = (e_1, \cdots, e_{n-1}, -e_n)$, la matrice de passage P^- de $\mathcal{B}^-$ à $\mathcal{B}'$ est :

$$P^- = \begin{pmatrix} p_{11} & \cdots & \cdots & p_{1n} \\ \vdots & \ddots & & \vdots \\ & & \ddots & \\ p_{n-1,1} & & & p_{n-1,n} \\ -p_{nn} & \cdots & \cdots & -p_{nn} \end{pmatrix}$$

et $\det(P^-) = -\det(P) = 1$, donc $P^- \in \mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{B}' \sim \mathcal{B}^-$. Donc $\mathcal{B}'$ est soit dans la classe de $\mathcal{B}$, soit dans celle de $\mathcal{B}^-$ et ces deux classes sont distinctes puisque la matrice de passage de $\mathcal{B}$ à $\mathcal{B}^-$ est $\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{O}_n^-(\mathbb{R})$. On a donc deux classes distinctes. □

Définition 2.10. *Orienter l'espace euclidien E revient à choisir une des deux classes d'équivalence pour la relation $\sim$. Si l'espace E est orienté par le choix d'une classe d'équivalence $\overline{\mathcal{B}_0}$, où $\mathcal{B}_0$ est base orthonormée de E, on dit qu'une base orthonormée $\mathcal{B}$ est directe (ou qu'elle définit la même orientation que $\mathcal{B}_0$) si $\mathcal{B}$ est dans la classe d'équivalence de $\mathcal{B}_0$ et on dit que cette base $\mathcal{B}$ est indirecte (ou rétrograde) dans le cas contraire.*

Orienter l'espace euclidien E revient donc à choisir une base orthonormée $\mathcal{B}_0$.

L'espace $\mathbb{R}^n$, pour $n \geq 2$, est en général orienté par le choix de la base canonique.

Les isométries directes sont celles qui respectent l'orientation. Précisément, on a le résultat suivant.

Théorème 2.32.

Soient $\mathcal{B} = (e_i)_{1\leq i\leq n}$ une base orthonormée de E et u une application linéaire de E dans E. L'application u est une isométrie positive si, et seulement si, elle transforme $\mathcal{B}$ en une base orthonormée de E définissant la même orientation.

Preuve. Soient $u \in \mathcal{L}(E)$ et $\mathcal{B}' = (u(e_i))_{1\leq i\leq n}$. On a :

$$\left(u \in \mathcal{O}^+(E)\right) \Leftrightarrow (u \in \mathcal{O}(E) \text{ et } \det(u) = 1)$$

avec $\det(u) = \det_{\mathcal{B}}(\mathcal{B}')$, donc :

$$\begin{aligned}\left(u \in \mathcal{O}^+(E)\right) &\Leftrightarrow \left(\mathcal{B}' = (u(e_i))_{1\leq i\leq n} \text{ base orthonormée et } \det_{\mathcal{B}}(\mathcal{B}') = 1\right)\\ &\Leftrightarrow (\mathcal{B}' \sim \mathcal{B})\end{aligned}$$

□

2.5.4 Produit mixte et produit vectoriel

E est un espace euclidien de dimension $n \geq 3$ orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_i)_{1\leq i\leq n}$.

Si $\mathcal{B}$ est une autre base de E, alors pour tout n-uplet $(x_1, x_2, \cdots, x_n)$ de vecteurs de E, on a $\det_{\mathcal{B}_0}(x_1, x_2, \cdots, x_n) = \det_{\mathcal{B}_0}(\mathcal{B}) \det_{\mathcal{B}}(x_1, x_2, \cdots, x_n)$, donc le réel $\det_{\mathcal{B}}(x_1, x_2, \cdots, x_n)$ est indépendante du choix d'une base orthonormée directe $\mathcal{B}$ de E. On le note $[x_1, x_2, \cdots, x_n]$ et on dit que c'est le produit mixte des vecteurs ordonnés $x_1, x_2, \cdots, x_n$.

En remarquant que, pour tout $(n-1)$-uplet $x_1, x_2, \cdots, x_{n-1}$ de vecteurs de E, l'application $x \mapsto \det(x_1, x_2, \cdots, x_{n-1}, x)$ est une forme linéaire, on déduit qu'il existe un unique vecteur $a \in E$ tel que :

$$\forall x \in E,\ \det(x_1, \cdots, x_{n-1}, x) = \langle a \mid x\rangle \tag{2.2}$$

ce vecteur a étant fonction des vecteurs $x_1, x_2, \cdots, x_{n-1}$. On peut donc donner la définition suivante.

Définition 2.11. *Le produit vectoriel des $n-1$ vecteurs $x_1, x_2, \cdots, x_{n-1}$ de E est le vecteur a défini par* (2.2)*. On le note $x_1 \wedge x_2 \wedge ... \wedge x_{n-1}$.*

Dans la base orthonormée $\mathcal{B}_0$, en notant $x_j = \sum_{i=1}^{n} x_{ij} e_i$ pour tout j compris entre 1 et n, les réels $\det(x_1, x_2, \cdots, x_{n-1}, e_i) = \langle x_1 \wedge x_2 \wedge ... \wedge x_{n-1} \mid e_i\rangle$ sont les composantes du vecteur $x_1 \wedge x_2 \wedge ... \wedge x_{n-1}$ dans la base $\mathcal{B}_0$. On a donc :

$$x_1 \wedge ... \wedge x_{n-1} = \sum_{i=1}^{n} (-1)^{i+n} \delta_i e_i$$

en désignant par δ_i le déterminant de la matrice d'ordre $n-1$ déduite de la matrice $(X_1, \cdots, X_{n-1})$ en supprimant de cette matrice la ligne numéro i (X_i étant le vecteur de $\mathbb{R}^n$ formé des composantes de x_i dans la base $\mathcal{B}_0$).

On peut remarquer que $(-1)^{i+n}\delta_i$ est aussi le cofacteur $C_{i,n}(x_1, x_2, \cdots, x_{n-1})$ d'indice (i, n) de la matrice $(X_1, \cdots, X_{n-1}, 0)$ (*i.e.* celui en ligne i et colonne n).

En utilisant les propriétés du déterminant, on obtient le résultat suivant.

Théorème 2.33.

— *Le produit vectoriel est une application $(n-1)$-linéaire alternée de E^{n-1} dans E ;*

— *le vecteur* $x_1 \wedge x_2 \wedge ... \wedge x_{n-1}$ *est orthogonal à tous les vecteurs* x_i *pour* $1 \leq i \leq n-1$ *;*

— $x_1 \wedge x_2 \wedge ... \wedge x_{n-1} = 0$ *si, et seulement si, la famille* $(x_1, x_2, ..., x_{n-1})$ *est liée ;*

— *si la famille* $(x_1, x_2, ..., x_{n-1})$ *est libre, on a alors :*

$$\det(x_1, \cdots, x_{n-1}, x_1 \wedge ... \wedge x_{n-1}) = \|x_1 \wedge ... \wedge x_{n-1}\|^2 > 0$$

et la famille $(x_1, ..., x_{n-1}, x_1 \wedge ... \wedge x_{n-1})$ *est une base directe de* E *;*

— *si la famille* $(x_1, ..., x_{n-1})$ *est orthonormée, la famille* $(x_1, \cdots, x_{n-1}, x_1 \wedge ... \wedge x_{n-1})$ *est alors une base orthonormée directe de* E*.*

Preuve.

— Chacune des applications $(x_1, ..., x_{n-1}) \mapsto \det(x_1, \cdots, x_{n-1}, e_i)$ étant $(n-1)$-linéaire alternée, il en est de même de l'application

$$(x_1, ..., x_{n-1}) \mapsto x_1 \wedge ... \wedge x_{n-1} = \sum_{i=1}^{n} \det(x_1, \cdots, x_{n-1}, e_i)\, e_i$$

— Avec $\langle x_1 \wedge ... \wedge x_{n-1} \mid x_i \rangle = \det(x_1, \cdots, x_{n-1}, x_i) = 0$ pour $1 \leq i \leq n-1$, on déduit que $x_1 \wedge ... \wedge x_{n-1}$ est orthogonal à x_i.

— Si la famille $(x_i)_{1 \leq i \leq n-1}$ est liée, il en est alors de même de $(x_1, ..., x_{n-1}, x)$ pour tout $x \in E$ et $\langle x_1 \wedge ... \wedge x_{n-1} \mid x \rangle = \det(x_1, \cdots, x_{n-1}, x) = 0$, ce qui signifie que $x_1 \wedge ... \wedge x_{n-1} \in E^{\perp} = \{0\}$. Si la famille $(x_i)_{1 \leq i \leq n-1}$ est libre, elle se prolonge alors en une base $(x_1, \cdots, x_{n-1}, x)$ et on a $\langle x_1 \wedge ... \wedge x_{n-1} \mid x \rangle = \det(x_1, \cdots, x_{n-1}, x) \neq 0$, ce qui entraîne $x_1 \wedge ... \wedge x_{n-1} \neq 0$.

— Si la famille $(x_i)_{1 \leq i \leq n-1}$ est libre, on a alors $x_1 \wedge ... \wedge x_{n-1} \neq 0$, donc :

$$\det(x_1, \cdots, x_{n-1}, x_1 \wedge ... \wedge x_{n-1}) = \|x_1 \wedge ... \wedge x_{n-1}\|^2 \neq 0$$

et $(x_1, \cdots, x_{n-1}, x_1 \wedge ... \wedge x_{n-1})$ est une base directe de E.

— Si la famille $(x_i)_{1 \leq i \leq n-1}$ est orthonormée, elle est alors libre et la famille $(x_1, \cdots, x_{n-1}, x_1 \wedge ... \wedge x_{n-1})$ est une base directe de E. De plus le vecteur $x_1 \wedge ... \wedge x_{n-1}$ est orthogonal à l'hyperplan H engendré par $x_1, ..., x_{n-1}$. En prolongeant la famille $(x_i)_{1 \leq i \leq n-1}$ en une base orthonormée directe de E, $(x_1, ..., x_{n-1}, x_n)$, on a $x_1 \wedge ... \wedge x_{n-1} = \lambda x_n$ (ces deux vecteurs sont dans la droite $H^{\perp}$) et $\lambda = \langle x_1 \wedge ... \wedge x_{n-1} \mid x_n \rangle = \det(x_1, \cdots, x_{n-1}, x_n) = 1$, donc $x_1 \wedge ... \wedge x_{n-1} = x_n$ est de norme 1.

□

Le produit vectoriel peut être utilisé pour donner une expression relativement simple de la distance d'un point à un hyperplan.

Théorème 2.34.

Si H est un hyperplan de E et $(x_1, ..., x_{n-1})$ une base de H, alors la droite $D = H^\perp$ est dirigée par le vecteur $x_1 \wedge ... \wedge x_{n-1}$ et pour tout vecteur x de E, la projection orthogonale de x sur H est :

$$p_H(x) = x - \frac{\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle}{\|x_1 \wedge ... \wedge x_{n-1}\|^2}(x_1 \wedge ... \wedge x_{n-1})$$

et la distance de x à H est donnée par :

$$d(x, H) = \frac{|\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle|}{\|x_1 \wedge ... \wedge x_{n-1}\|} = \frac{|\det(x_1, \cdots, x_{n-1}, x)|}{\|x_1 \wedge ... \wedge x_{n-1}\|}$$

Preuve. Le vecteur $x_1 \wedge ... \wedge x_{n-1}$ étant orthogonal à tous les x_i qui engendrent H, est nécessairement dans $H^\perp$. Comme $H^\perp$ est une droite et $x_1 \wedge ... \wedge x_{n-1}$ non nul, la droite $D = H^\perp$ est dirigée par $x_1 \wedge ... \wedge x_{n-1}$. On a $d(x, H) = \|x - y\|$ où $y = p_H(x)$ est la projection orthogonale de x sur H. Comme $x - y \in H^\perp$, il existe un réel λ tel que $x - y = \lambda(x_1 \wedge ... \wedge x_{n-1})$ et avec $\lambda \|x_1 \wedge ... \wedge x_{n-1}\|^2 = \langle x - y \mid x_1 \wedge ... \wedge x_{n-1}\rangle = \langle x \mid x_1 \wedge ... \wedge x_{n-1}\rangle$ (puisque le vecteur y est dans H et $x_1 \wedge ... \wedge x_{n-1}$ dans $H^\perp$), on déduit que $\lambda = \frac{\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle}{\|x_1 \wedge ... \wedge x_{n-1}\|^2}$ et :

$$y = x - \frac{\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle}{\|x_1 \wedge ... \wedge x_{n-1}\|^2}(x_1 \wedge ... \wedge x_{n-1})$$

$$d(x, H) = \|x - y\| = \frac{|\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle|}{\|x_1 \wedge ... \wedge x_{n-1}\|}$$

□

Le théorème précédent nous dit aussi qu'une équation de l'hyperplan H de base $(x_1, ..., x_{n-1})$ est donnée par :

$$(x \in H) \Leftrightarrow (d(x, H) = 0) \Leftrightarrow (\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle = 0)$$

En prenant pour $(x_1, ..., x_{n-1})$ une base orthonormée de H, on a :

$$p_H(x) = x - \langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle (x_1 \wedge ... \wedge x_{n-1})$$

et $d(x, H) = |\langle x_1 \wedge ... \wedge x_{n-1} \mid x\rangle|$.

2.5.5 Le produit vectoriel en dimension 3

On suppose ici que E est un espace euclidien de dimension 3 orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_1, e_2, e_3)$.

Le produit vectoriel de $x = x_1e_1 + x_2e_2 + x_3e_3$ et $y = y_1e_1 + y_2e_2 + y_3e_3$ est le vecteur $z = z_1e_1 + z_2e_2 + z_3e_3$ défini par :

$$\begin{aligned} z_1 &= \langle x \wedge y \mid e_1 \rangle = \det(x, y, e_1) = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = x_2y_3 - x_3y_2 \\ z_2 &= \langle x \wedge y \mid e_2 \rangle = \det(x, y, e_2) = -\begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix} = x_3y_1 - x_1y_3 \\ z_3 &= \langle x \wedge y \mid e_3 \rangle = \det(x, y, e_3) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1y_2 - x_2y_1 \end{aligned}$$

Lemme 2.6 *Si (f_1, f_2, f_3) est une base orthonormée directe, on a alors :*

$$f_1 \wedge f_2 = f_3,\ f_2 \wedge f_3 = f_1,\ f_3 \wedge f_1 = f_2$$

Preuve. Pour $1 \leq i \neq j \leq 3$, le vecteur $f_i \wedge f_j$ est orthogonal au plan engendré par f_i, f_j, donc colinéaire à f_k où $\{k\} = \{1, 2, 3\} \setminus \{i, j\}$ et il existe un réel λ tel que $f_i \wedge f_j = \lambda f_k$. Ce réel λ est déterminé par $\lambda = \langle f_i \wedge f_j \mid f_k \rangle = \det(f_i, f_j, f_k) = \pm 1$. On a donc $f_i \wedge f_j = \det(f_i, f_j, f_k)\, f_k$, ce qui nous donne :

$$f_1 \wedge f_2 = \det(f_1, f_2, f_3)\, f_3 = f_3$$

$$f_1 \wedge f_3 = \det(f_1, f_3, f_2)\, f_2 = -f_2$$

$$f_2 \wedge f_3 = \det(f_2, f_3, f_1)\, f_1 = f_1$$

□

Le caractère 2-linéaire alterné du produit vectoriel se traduit par :

$$\begin{cases} (x + y) \wedge z = x \wedge z + y \wedge z \\ x \wedge (y + z) = x \wedge y + x \wedge z \\ (\lambda x) \wedge y = x \wedge (\lambda y) = \lambda (x \wedge y) \\ x \wedge y = -(y \wedge x) \end{cases}$$

pour tous vecteurs x, y, z et tout réel λ.

Avec la dernière propriété, on déduit que le produit vectoriel est non commutatif ($x \wedge y = -(y \wedge x) \neq y \wedge x$ pour y, x libre).

On a vu que $x \wedge y = 0$ équivaut à dire que x et y sont liés. On en déduit que le produit vectoriel est non associatif. Par exemple, on a :

$$e_1 \wedge (e_1 \wedge e_2) = e_1 \wedge e_3 = -e_2 \neq (e_1 \wedge e_1) \wedge e_2 = 0$$

De manière plus précise, on a les formules du double produit vectoriel suivantes.

Théorème 2.35.

Pour x, y, z dans E, on a :

$$\begin{aligned} x \wedge (y \wedge z) &= \langle x \mid z \rangle\, y - \langle x \mid y \rangle\, z \\ (x \wedge y) \wedge z &= \langle x \mid z \rangle\, y - \langle y \mid z \rangle\, x \end{aligned}$$

Preuve. Pour tout $x \in E$, on désigne par φ_x l'application linéaire définie par :

$$\forall x \in E,\ \varphi_x(t) = x \wedge t$$

On a alors, pour x, y, z dans E $x \wedge (y \wedge z) = \varphi_x \circ \varphi_y(z)$ et la matrice dans $\mathcal{B}_0$ de $\varphi_x \circ \varphi_y$ est :

$$\begin{aligned} A_x A_y &= \begin{pmatrix} 0 & x_3 & -x_2 \\ -x_3 & 0 & x_1 \\ x_2 & -x_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & y_3 & -y_2 \\ -y_3 & 0 & y_1 \\ y_2 & -y_1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -x_2y_2 - x_3y_3 & x_2y_1 & y_1x_3 \\ x_1y_2 & -x_1y_1 - x_3y_3 & x_3y_2 \\ x_1y_3 & x_2y_3 & -x_1y_1 - x_2y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1y_1 & x_2y_1 & y_1x_3 \\ x_1y_2 & x_2y_2 & x_3y_2 \\ x_1y_3 & x_2y_3 & x_3y_3 \end{pmatrix} - (x_1y_1 + x_2y_2 + x_3y_3) \begin{pmatrix} 1 & 0 & 0_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} - \langle x \mid y \rangle I_3 \end{aligned}$$

et on reconnaît la matrice dans $\mathcal{B}_0$ de l'application linéaire $t \mapsto \langle x \mid t \rangle y - \langle x \mid y \rangle t$. Il en résulte que :

$$(x \wedge y) \wedge z = -z \wedge (x \wedge y) = -(\langle z \mid y \rangle x - \langle z \mid x \rangle y) = \langle x \mid z \rangle y - \langle y \mid z \rangle x$$

On peut aussi se placer dans une base orthonormée directe adaptée. Pour y, z liés, on a $x \wedge (y \wedge z) = 0$. Si $y = 0$, on a alors $\langle x \mid z \rangle y - \langle x \mid y \rangle z = 0$, sinon on a $z = \lambda y$ et $\langle x \mid z \rangle y - \langle x \mid y \rangle z = \lambda(\langle x \mid y \rangle y - \langle x \mid y \rangle y) = 0$. Pour (y, z) libre, on utilise une base orthonormée directe $\mathcal{B} = (f_1, f_2, f_3)$ où $f_1 = \dfrac{1}{\|y\|} y$, $\operatorname{Vect}\{y, z\} = \operatorname{Vect}\{f_1, f_2\}$ et dans cette base $\mathcal{B}$, on a :

$$\begin{cases} x = x_1 f_1 + x_2 f_2 + x_3 f_3 \\ y = \|y\| f_1 = y_1 f_1 \\ z = z_1 f_1 + z_2 f_2 \end{cases}, \; y \wedge z = y_1 z_2 f_3$$

$$\begin{aligned} x \wedge (y \wedge z) &= y_1 z_2 (x_2 f_1 - x_1 f_2) = x_2 z_2 y - x_1 y_1 \left(z - \frac{z_1}{y_1} y \right) \\ &= (x_1 z_1 + x_2 z_2) y - \langle x \mid y \rangle z = \langle x \mid z \rangle y - \langle x \mid y \rangle z \end{aligned}$$

et la relation $x \wedge (y \wedge z) = \langle x \mid z \rangle y - \langle x \mid y \rangle z$ s'en déduit par anti-symétrie du produit vectoriel. □

Corollaire 2.4. (Formule de Lagrange). *Pour x, y dans E, on a $\langle x \mid y \rangle^2 + \|x \wedge y\|^2 = \|x\|^2 \|y\|^2$.*

Preuve. On a :

$$\begin{aligned} \|x \wedge y\|^2 &= \langle x \wedge y \mid x \wedge y \rangle = \det(x, y, x \wedge y) = \det(y, x \wedge y, x) = \langle y \wedge (x \wedge y) \mid x \rangle \\ &= \left\langle \|y\|^2 x - \langle x \mid y \rangle y \mid x \right\rangle = \|x\|^2 \|y\|^2 - \langle x \mid y \rangle^2 \end{aligned}$$

□

On rappelle que si x et y sont des vecteurs non nuls dans E, la mesure principale de leur angle géométrique est le réel $\theta \in [0,\pi]$ définie par $\langle x \mid y\rangle = \cos(\theta)\,\|x\|\,\|y\|$. L'identité de Lagrange nous dit alors que :

$$\begin{aligned}\|x\wedge y\|^2 &= \|x\|^2\,\|y\|^2 - \langle x \mid y\rangle^2\\ &= \|x\|^2\,\|y\|^2\left(1-\cos^2(\theta)\right) = \|x\|^2\,\|y\|^2\sin^2(\theta)\end{aligned}$$

et pour x, y linéairement indépendants, on a $x\wedge y \neq 0$ et $\|x\wedge y\| = \|x\|\,\|y\|\sin(\theta)$, cette dernière identité étant encore valable pour x, y liés puisque dans ce cas on a, $|\langle x \mid y\rangle| = \|x\|\,\|y\|$ et θ vaut 0 ou π.

On peut donner une définition géométrique du produit vectoriel en dimension 3 comme suit.

Pour x, y liés, on a $x\wedge y = 0$.

Pour x, y linéairement indépendants, on définit une base orthonormée (f_1, f_2) du plan P engendré par x, y avec $f_1 = \dfrac{1}{\|x\|}x$, puis on complète cette base en une base orthonormée directe $\mathcal{B} = (f_1, f_2, f_3)$ de E. On dit que le plan P est orienté par le choix de f_3.

La mesure principale $\theta \in\,]-\pi,\pi]$ de l'angle orienté des vecteurs x et y dans le plan P ainsi orienté est telle que la rotation ρ_θ d'angle θ transforme $f_1 = \dfrac{1}{\|x\|}x$ en $\dfrac{1}{\|y\|}y$.

Dans la base (f_1, f_2) de P, la matrice de ρ_θ est $R_\theta = \begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}$ et l'égalité $\rho_\theta\left(\dfrac{1}{\|x\|}x\right) = \dfrac{1}{\|y\|}y$ avec $x = \|x\|\,f_1$ se traduit par :

$$y = \|y\|\,\rho_\theta(f_1) = \|y\|\,(\cos(\theta)\,f_1 + \sin(\theta)\,f_2)$$

Comme $\mathcal{B} = (f_1, f_2, f_3)$ est une base orthonormée directe de E, les coordonnées de $x\wedge y$ dans cette base sont données par :

$$\begin{pmatrix}\|x\|\\0\\0\end{pmatrix}\wedge\begin{pmatrix}\|y\|\cos(\theta)\\\|y\|\sin(\theta)\\0\end{pmatrix} = \begin{pmatrix}0\\0\\\|x\|\,\|y\|\sin(\theta)\end{pmatrix}$$

c'est-à-dire que $x\wedge y = \|x\|\,\|y\|\sin(\theta)\,f_3$.

On a aussi $\|x\wedge y\| = \|x\|\,\|y\|\,|\sin(\theta)|$ et $\langle x \mid y\rangle = \|x\|\,\|y\|\cos(\theta)$ ($|\theta| \in [0,\pi]$ est la mesure principale de l'angle géométrique des vecteurs x, y). On retrouve ainsi l'identité de Lagrange :

$$\langle x \mid y\rangle^2 + \|x\wedge y\|^2 = \|x\|^2\,\|y\|^2\left(\cos^2(\theta)+\sin^2(\theta)\right) = \|x\|^2\,\|y\|^2$$

2.6 Exercices

Exercice 2.1. *On suppose que le corps* $\mathbb{K}$ *est infini et on se donne une matrice* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *dans* $\mathcal{M}_{2n}(\mathbb{K})$, *avec* A, B, C, D *dans* $\mathcal{M}_n(\mathbb{K})$ *telles que* C *et* D *commutent.*

1. *On suppose que* D *inversible et on pose* $T = \begin{pmatrix} D & 0 \\ -C & D^{-1} \end{pmatrix}$. *Calculer le produit* MT *et en déduire que* $\det(M) = \det(AD - BC)$.
2. *Désignant par* P *le polynôme défini par* $P(X) = \det \begin{pmatrix} A & B \\ C & D - XI_n \end{pmatrix}$ *(il s'agit ici du déterminant d'une matrice à coefficients dans le corps* $\mathbb{K}(X)$*), montrer que le polynôme* Q *défini par* $Q(X) = \det(D - XI_n)$ *n'a qu'un nombre fini de racines dans le corps* $\mathbb{K}$, *puis en déduire que* $\det(M) = \det(AD - BC)$.
3. *Montrer que pour* A, B *dans* $\mathcal{M}_n(\mathbb{R})$ *on a* $\det \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \geq 0$.

Solution.

1. En utilisant le fait que D et C commutent on a :

$$MT = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} D & 0 \\ -C & D^{-1} \end{pmatrix} = \begin{pmatrix} AD - BC & BD^{-1} \\ 0 & I_q \end{pmatrix}$$

   et $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC)$.

2. $Q(X) = \det(D - XI_n)$ est un polynôme de degré q, il n'a donc qu'un nombre fini de racines dans $\mathbb{K}$. En conséquence la matrice $D - XI_n$ est inversible pour une infinité de valeurs de X. Pour ces valeurs on a :

$$P(X) = \det \begin{pmatrix} A & B \\ C & D - XI_n \end{pmatrix} = \det(A(D - XI_n) - BC) = R(X)$$

   Les polynômes P et R prenant la même valeur pour une infinité de valeurs de X sont donc égaux. Prenant $X = 0$ on obtient $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC)$.

3. On a :

$$\begin{aligned} \det \begin{pmatrix} A & B \\ -B & A \end{pmatrix} &= \det\left(A^2 + B^2\right) = \det((A + iB)(A - iB)) \\ &= \det(A + iB) \det(A - iB) = |\det(A + iB)|^2 \geq 0 \end{aligned}$$

Exercice 2.2. *Soit $A \in \mathcal{M}_n(\mathbb{K})$. Montrer que :*

$$\operatorname{rg}(C(A)) = \begin{cases} n \text{ si } \operatorname{rg}(A) = n \\ 1 \text{ si } \operatorname{rg}(A) = n-1 \\ 0 \text{ si } \operatorname{rg}(A) \leq n-2 \end{cases}$$

Solution. Si $\operatorname{rg}(A) = n$, la matrice A est alors inversible, donc aussi la matrice $C(A) = \det(A)\ {}^t\left(A^{-1}\right)$. Si $\operatorname{rg}(A) = n-1$, il existe au moins un déterminant d'ordre $n-1$ extrait de A qui est non nul, donc $\operatorname{rg}(C(A)) \geq 1$. Comme ${}^tC(A) \cdot A = \det(A) I_n = 0$, on a $\operatorname{Im}(A) \subset \ker({}^tC(A))$, donc $\operatorname{rg}(A) \leq n - \operatorname{rg}(C(A))$ et $\operatorname{rg}(C(A)) \leq n - \operatorname{rg}(A) = 1$, ce qui nous donne $\operatorname{rg}(C(A)) = 1$. Si $\operatorname{rg}(A) = n-2$, tous les mineurs de A sont nuls et $C(A) = 0$.

Exercice 2.3. *Calculer le déterminant de l'endomorphisme τ de transposition défini par $\tau(A) = {}^tA$ pour tout $A \in \mathcal{M}_n(\mathbb{K})$.*

Solution. En utilisant le fait que $\mathcal{M}_n(\mathbb{K})$ est somme directe de l'espace $\mathcal{S}_n(\mathbb{K})$ des matrices symétriques et de l'espace $\mathcal{A}_n(\mathbb{K})$ des matrices anti-symétriques (tout $A \in \mathcal{M}_n(\mathbb{K})$ s'écrit $A = \frac{1}{2}(A + {}^tA) + \frac{1}{2}(A - {}^tA)$ et la matrice nulle est l'unique matrice à la fois symétrique et anti-symétrique), on se donne une base $\mathcal{B}$ de $\mathcal{M}_n(\mathbb{K})$ formée de la réunion d'une base $\mathcal{B}_1$ de $\mathcal{S}_n(\mathbb{K})$ et d'une base $\mathcal{B}_2$ de $\mathcal{A}_n(\mathbb{K})$. Pour tout $A \in \mathcal{B}_1$, on a $\tau(A) = A$ et pour tout $A \in \mathcal{B}_2$, on a $\tau(A) = -A$, l'espace $\mathcal{S}_n(\mathbb{K})$ étant de dimension $p = \dfrac{n(n+1)}{2}$ et $\mathcal{A}_n(\mathbb{K})$ de dimension $q = \dfrac{n(n-1)}{2}$. La matrice de τ dans la base $\mathcal{B}$ est donc $T = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$ et son déterminant est $\det(\tau) = \det(T) = (-1)^q$.

Exercice 2.4. *En utilisant un déterminant de Vandermonde, montrer que les vecteurs propres $x_1, \cdots, x_p$ non nuls d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ associés à des valeurs propres $\alpha_1, \cdots, \alpha_p$ deux à deux distinctes sont linéairement indépendants.*

Solution. On a $Ax_i = \alpha_i x_i$ pour $1 \leq i \leq p$ et pour tout entier naturel j, $A^j x_i = \alpha_i^j x_i$ pour $1 \leq i \leq p$. Si $\sum_{i=1}^{p} \lambda_i x_i = 0$, en appliquant A^j, pour $j \in \mathbb{N}$, on a $\sum_{i=1}^{p} \lambda_i \alpha_i^j x_i = 0$. On notant $x_i = (x_{i,k})_{1 \leq k \leq n}$, on a $\sum_{i=1}^{p} \lambda_i \alpha_i^j x_{i,k} = 0$ pour tout $j \in \mathbb{N}$, donc chaque vecteur $X_k = (\lambda_i x_{i,k})_{1 \leq i \leq p}$ est solution de $V(\alpha_1, \cdots, \alpha_p) X = 0$, ce qui donne $X_k = 0$ pour tout k compris entre 1 et n, soit $\lambda_i x_{i,k} = 0$ pour tout i compris entre 1 et p et tout k compris entre 1 et n. On a donc, pour tout i compris entre 1 et p, $\lambda_i x_i = 0$ et $\lambda_i = 0$ puisque $v_i \neq 0$.

Exercice 2.5. *On suppose que $\mathbb{K}$ est de caractéristique nulle et on se donne des scalaires $\alpha_0, \alpha_1, \cdots, \alpha_n$ deux à deux distincts. Montrer que pour tout polynôme $P \in \mathbb{K}[X]$ de degré n, la famille de polynômes $(P(X+\alpha_k))_{0\leq k\leq n}$ est une base de $\mathbb{K}_n[X]$.*

Solution. Notons $P_k(X) = P(X+\alpha_k)$ pour $0 \leq k \leq n$. Comme P est de degré n, la famille $\left(P^{(j)}\right)_{0\leq j\leq n}$, qui est échelonnée en degrés, est une base de $\mathbb{K}_n[X]$ (si $P(X) = \sum_{k=0}^{n} a_k X^k$, la matrice de ce système dans la base canonique de $\mathbb{K}_n[x]$ est alors triangulaire supérieure avec les $\dfrac{n!}{(n-j)!}a_n \neq 0$ pour éléments diagonaux). En utilisant la formule de Taylor-Lagrange, on a :

$$P_k(x) = P(x+\alpha_k) = \sum_{j=0}^{n} \frac{\alpha_k^j}{j!} P^{(j)}(x)$$

C'est à dire que la matrice du système $(P_k)_{0\leq k\leq n}$ dans la base $\left(\dfrac{1}{j!}P^{(j)}\right)_{0\leq j\leq n}$ est la matrice de Vandermonde $V(\alpha_0, \cdots, \alpha_n)$. Dans le cas particulier où les α_i sont deux à deux distincts cette matrice est inversible et en conséquence $(P_k)_{0\leq k\leq n}$ est une base de $\mathbb{K}_n[x]$.

Exercice 2.6. *On désigne par E l'espace vectoriel des applications de $\mathbb{R}$ dans $\mathbb{R}$. Montrer, pour tous réels $0 < a_1 < \cdots < a_n$, la famille :*

$$\mathcal{L} = \{f_{a_k} : x \mapsto \sin(a_k x) \mid 1 \leq k \leq n\}$$

est libre dans E.

Solution. Soient $0 < a_1 < \cdots < a_n$ et $\lambda_1, \cdots, \lambda_n$ des réels tels que :

$$\forall x \in \mathbb{R},\ \sum_{k=1}^{n} \lambda_k \sin(a_k x) = 0$$

Un développement limité en 0 nous donne $\sum_{k=1}^{n} \lambda_k a_k^{2p+1} = 0$ pour tout entier p compris en 0 et $n-1$. C'est–à–dire que $(\lambda_1 a_1, \cdots, \lambda_n a_n)$ est solution d'un système de Vandermonde :

$$\sum_{k=1}^{n} \lambda_k x_k^p = 0 \ \ (0 \leq p \leq n-1)$$

Les a_k étant strictement positifs et deux à deux distincts, on en déduit que les λ_k sont tous nuls. Ce qui prouve que le système $\mathcal{L}$ est libre dans E.

Exercice 2.7. *Soit* $A_n = \begin{pmatrix} 1^{n-1} & 2^{n-1} & \cdots & n^{n-1} \\ 2^{n-1} & 3^{n-1} & \cdots & (n+1)^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ n^{n-1} & (n+1)^{n-1} & \cdots & (2n-1)^{n-1} \end{pmatrix}$.

Montrer que :

$$\det(A_n) = (-1)^{\frac{n(n-1)}{2}} ((n-1)!)^n$$

Solution. On utilise le théorème 2.17 en prenant $\alpha_k = k$ et $P_k(X) = (X+k-1)^{n-1}$ pour $1 \leq k \leq n$. Dans ce cas, on a $\Delta(1, \cdots, n) = \prod_{j=1}^{n-1} j!$ (exemple 2.3), $P_1(X) = X^{n-1}$ et $P_k(X) = \sum_{i=0}^{n-1} \binom{n-1}{i} (k-1)^{n-1-i} X^i$ pour $2 \leq k \leq n$, donc :

$$\det(Q(P_1, \cdots, P_n)) = \begin{vmatrix} 0 & \binom{n-1}{0} & \binom{n-1}{0} 2^{n-1} & \cdots & \binom{n-1}{0} (n-1)^{n-1} \\ 0 & \binom{n-1}{1} & \binom{n-1}{1} 2^{n-2} & \cdots & \binom{n-1}{1} (n-1)^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \binom{n-1}{n-2} & \binom{n-1}{n-2} 2 & \cdots & \binom{n-1}{n-2} n-1 \\ 1 & \binom{n-1}{n-1} & \binom{n-1}{n-1} & \cdots & \binom{n-1}{n-1} \end{vmatrix}$$

$$= \prod_{i=0}^{n-1} \binom{n-1}{i} \begin{vmatrix} 0 & 1 & 2^{n-1} & \cdots & (n-1)^{n-1} \\ 0 & 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & 2 & \cdots & n-1 \\ 1 & 1 & 1 & \cdots & 1 \end{vmatrix}$$

soit :

$$\det(Q(P_1, \cdots, P_n)) = (-1)^{n+1} \prod_{i=1}^{n-2} \binom{n-1}{i} \begin{vmatrix} 1 & 2^{n-1} & \cdots & (n-1)^{n-1} \\ 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 2 & \cdots & n-1 \end{vmatrix}$$

$$= (-1)^{n+1} \prod_{i=1}^{n-2} \binom{n-1}{i} (n-1)! \begin{vmatrix} 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \\ 1 & 2^{n-3} & \cdots & (n-1)^{n-3} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & \cdots & 1 \end{vmatrix}$$

avec :

$$\begin{pmatrix} 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \\ 1 & 2^{n-3} & \cdots & (n-1)^{n-3} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} = P_\sigma \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & n-1 \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \end{pmatrix}$$

où P_σ est la matrice de pemutation associée à $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ n-1 & n-2 & \cdots & 1 \end{pmatrix}$, ce qui nous donne en notant $\lambda_n = (-1)^{n+1} \prod_{i=1}^{n-2} \binom{n-1}{i} (n-1)!$ et $\varepsilon(\sigma)$ la signature de la parmutation σ :

$$\begin{aligned} \det(Q(P_1, \cdots, P_n)) &= \lambda_n \varepsilon(\sigma) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & n-1 \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 2^{n-2} & \cdots & (n-1)^{n-2} \end{vmatrix} \\ &= \lambda_n \varepsilon(\sigma) \Delta(1, \cdots, n-1) \end{aligned}$$

avec :

$$\begin{aligned} \lambda_n \Delta(1, \cdots, n-1) &= (-1)^{n+1} ((n-1)!)^{n-1} \prod_{i=1}^{n-2} \frac{1}{i!(n-1-i)!} \prod_{j=1}^{n-2} j \\ &= (-1)^{n+1} ((n-1)!)^{n-1} \prod_{j=1}^{n-2} \frac{1}{j!} \end{aligned}$$

et :

$$\begin{aligned} \varepsilon(\sigma) &= \prod_{1 \le i < j \le n-1} \frac{\sigma(j) - \sigma(i)}{j-i} = \prod_{1 \le i < j \le n-1} \frac{(n-j) - (n-i)}{j-i} \\ &= \prod_{1 \le i < j \le n-1} (-1) = (-1)^{\frac{(n-1)(n-2)}{2}} \end{aligned}$$

donc :

$$\begin{aligned} \det(A_n) &= \Delta(1, \cdots, n) \det(Q(P_1, \cdots, P_n)) \\ &= \left(\prod_{j=1}^{n-1} j! \right) (-1)^{n+1} \varepsilon(\sigma) ((n-1)!)^{n-1} \prod_{j=1}^{n-2} \frac{1}{j!} \\ &= (-1)^{\frac{n(n-1)}{2}} ((n-1)!)^n \end{aligned}$$

Exercice 2.8. *Soient E un espace euclidien orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_i)_{1 \le i \le n}$ et σ une permutation de $\{1, 2, \cdots, n\}$. À quelle condition portant sur σ la base $\mathcal{B}_\sigma = \left(e_{\sigma(i)}\right)_{1 \le i \le n}$ est-elle directe ?*

Solution. Notant $\varepsilon(\sigma)$ la signature de σ, on a $\det_{\mathcal{B}_0}(\mathcal{B}_\sigma) = \varepsilon(\sigma) \det(I_n) = \varepsilon(\sigma)$ et $\mathcal{B}_\sigma$ est directe si, et seulement si, σ est une permutation paire.

Exercice 2.9. *Donner une équation du plan vectoriel P de $\mathbb{R}^3$ engendré par $u = (1,1,1)$ et $v = (1,2,3)$. Calculer la distance de $x = (1-1,1)$ à P.*

Solution. Ce plan est orthogonal au vecteur $u \wedge v = (1,-2,1)$, une équation est donc $x_1 - 2x_2 + x_3 = 0$ et la distance de $x = (1-1,1)$ à P est donnée par :

$$d(x,P) = \frac{|\langle u \wedge v \mid x\rangle|}{\|x_1 \wedge v\|} = \frac{4}{\sqrt{6}}$$

Exercice 2.10. *E est un espace euclidien orienté de dimension* 3.

1. *Montrer que, pour tous vecteurs x, y, z, t dans E, on a :*

$$\begin{aligned}\langle x \wedge y \mid z \wedge t\rangle &= \begin{vmatrix} \langle x \mid z\rangle & \langle y \mid z\rangle \\ \langle x \mid t\rangle & \langle y \mid t\rangle \end{vmatrix} \\ &= \langle x \mid z\rangle \langle y \mid t\rangle - \langle x \mid t\rangle \langle y \mid z\rangle\end{aligned}$$

   (pour $(z,t) = (x,y)$, on retrouve la formule de Lagrange).

2. *Soient x, y, z dans $E \setminus \{0\}$. À quelle condition a-t-on :*

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$

3. *Soient a, b dans E avec $a \neq 0$. Résoudre l'équation $a \wedge x = b$ (division vectorielle).*
4. *Montrer que pour x, y, z, t dans E, on a :*

$$(x \wedge y) \wedge (z \wedge t) = -\det(x,y,z)\, t + \det(x,y,t)\, z$$

   et $\det(t,y,z)\, x + \det(x,t,z)\, y + \det(x,y,t)\, z = \det(x,y,z)\, t$.

Solution.

1. On a :

$$\begin{aligned}\langle x \wedge y \mid z \wedge t\rangle &= \det(x, y, z \wedge t) = \det(y, z \wedge t, x) \\ &= \langle y \wedge (z \wedge t) \mid x\rangle = \langle \langle y \mid t\rangle z - \langle y \mid z\rangle t \mid x\rangle \\ &= \langle x \mid z\rangle \langle y \mid t\rangle - \langle x \mid t\rangle \langle y \mid z\rangle = \begin{vmatrix} \langle x \mid z\rangle & \langle y \mid z\rangle \\ \langle x \mid t\rangle & \langle y \mid t\rangle \end{vmatrix}\end{aligned}$$

2. En utilisant les formules de double produit vectoriel, on a :

$$x \wedge (y \wedge z) - (x \wedge y) \wedge z = \langle y \mid z\rangle x - \langle x \mid y\rangle z$$

   Si x et z sont liés, il existe alors un réel $\lambda \neq 0$ tel que $z = \lambda x$ et :

$$x \wedge (y \wedge z) - (x \wedge y) \wedge z = \lambda(\langle y \mid x\rangle x - \langle x \mid y\rangle x) = 0$$

Si x et z sont linéairement indépendants, on a alors :

$$\begin{aligned}(x \wedge (y \wedge z) - (x \wedge y) \wedge z = 0) &\Leftrightarrow (\langle y \mid z\rangle = \langle x \mid y\rangle = 0)\\ &\Leftrightarrow \left(y \in (\operatorname{vect}(x,z))^{\perp}\right)\end{aligned}$$

avec $(\operatorname{vect}(x,z))^{\perp} = \mathbb{R}(x \wedge z)$. On en déduit que :

$$(x \wedge (y \wedge z) = (x \wedge y) \wedge z) \Leftrightarrow (y \text{ et } x \wedge z \text{ sont liés})$$

En définitive, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ si, et seulement si, x et z sont liés ou x et z sont linéairement indépendants et y est orthogonal au plan engendré par x et z.

3. Notons $S = \{x \in E \mid a \wedge x = b\}$. Comme $a \wedge x$ est orthogonal au vecteur non nul a, on a $S = \emptyset$ si b n'est pas orthogonal à a. Supposons b orthogonal à a, soit que $\langle a \mid b\rangle = 0$. En utilisant la formule du double produit vectoriel, on a $a \wedge (a \wedge b) = \langle a \mid b\rangle a - \langle a \mid a\rangle b = -\|a\|^2 b$, donc le vecteur $x_0 = -\dfrac{1}{\|a\|^2} a \wedge b$ est une solution particulière. Si $x \in E$ est une autre solution, on a alors $a \wedge (x - x_0) = 0$, ce qui équivaut à dire que $x - x_0$ est colinéaire au vecteur a. L'ensemble des solutions est donc $S = \{x_0 + \lambda a \mid \lambda \in \mathbb{R}\}$, à savoir la droite affine passant par $x_0 = -\dfrac{1}{\|a\|^2} a \wedge b$ et dirigée par a.
4. En utilisant la formule du double produit vectoriel, on a :

$$(x \wedge y) \wedge (z \wedge t) = \langle x \wedge y \mid t\rangle z - \langle x \wedge y \mid z\rangle t = \det(x,y,t)\, z - \det(x,y,z)\, t$$

On a aussi :

$$(x \wedge y) \wedge (z \wedge t) = -(z \wedge t) \wedge (x \wedge y) = \det(z,t,x)\, y - \det(z,t,y)\, x$$

donc :

$$\begin{aligned}\det(x,y,t)\, z - \det(x,y,z)\, t &= \det(z,t,x)\, y - \det(z,t,y)\, x\\ &= -\det(x,t,z)\, y - \det(t,y,z)\, x\end{aligned}$$

soit $\det(t,y,z)\, x + \det(x,t,z)\, y + \det(x,y,t)\, z = \det(x,y,z)\, t$.

Exercice 2.11. *E est un espace euclidien de dimension 3 orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_1, e_2, e_3)$ et pour y dans E on désigne par φ_y l'endomorphisme de E défini par :*

$$\forall x \in E,\ \varphi_y(x) = x \wedge y$$

1. *Déterminer la matrice de φ_y dans la base $\mathcal{B}_0$.*
2. *Montrer que $\varphi_y^3 = -\|y\|^2 \varphi_y$.*
3. *En déduire une expression simplifiée de $e^{\varphi_y}(x)$ pour x, y dans E avec $y \neq 0$.*

Solution.

1. Les coordonnées dans la base $\mathcal{B}_0$ de $\varphi_y(x)$ sont :
$$\begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix} = \begin{pmatrix} 0 & y_3 & -y_2 \\ -y_3 & 0 & y_1 \\ y_2 & -y_1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$
ce qui nous donne la matrice A_y (anti-symétrique) de φ_y dans la base $\mathcal{B}_0$.
2. On a :
$$\begin{aligned} A_y^3 &= \begin{pmatrix} 0 & -y_2^2y_3 - y_1^2y_3 - y_3^3 & y_2y_3^2 + y_1^2y_2 + y_2^3 \\ y_1^2y_3 + y_2^2y_3 + y_3^3 & 0 & -y_1y_3^2 - y_1^3 - y_1y_2^2 \\ -y_1^2y_2 - y_2^3 - y_2y_3^2 & y_1y_2^2 + y_1y_1^3 + y_1y_3^2 & 0 \end{pmatrix} \\ &= -\left(y_1^2 + y_2^2 + y_3^2\right) \begin{pmatrix} 0 & y_3 & -y_2 \\ -y_3 & 0 & y_1 \\ y_2 & -y_1 & 0 \end{pmatrix} \end{aligned}$$
On peut aussi écrire $\varphi_y^2(x) = (x \wedge y) \wedge y = \langle x \mid y \rangle y - \|y\|^2 x$ et :
$$\varphi_y^3(x) = \langle x \mid y \rangle (y \wedge y) - \|y\|^2 (x \wedge y) = -\|y\|^2 \varphi_y(x)$$
3. On rappelle que l'exponentielle de φ_y est définie par $e^{\varphi_y} = \sum_{n=0}^{+\infty} \frac{1}{n!} \varphi_y^n$. De la question précédente, on déduit que pour tout $p \geq 0$, on a $\varphi_y^{2(p+1)} = \left(-\|y\|^2\right)^p \varphi_y^2$ et $\varphi_y^{2p+1} = \left(-\|y\|^2\right)^p \varphi_y$. Pour $p = 0$ c'est vrai et supposant le résultat acquis pour $p \geq 0$, on a :
$$\varphi_y^{2(p+2)} = \left(-\|y\|^2\right)^p \varphi_y^4 = \left(-\|y\|^2\right)^p \left(-\|y\|^2 \varphi_y^2\right) = \left(-\|y\|^2\right)^{p+1} \varphi_y^2$$
et $\varphi_y^{2p+3} = \left(-\|y\|^2\right)^p \varphi_y^3 = \left(-\|y\|^2\right)^{p+1} \varphi_y$. Il en résulte que :
$$\begin{aligned} e^{\varphi_y} &= Id + \left(\sum_{p=0}^{+\infty} \frac{1}{(2(p+1))!} \left(-\|y\|^2\right)^p\right) \varphi_y^2 + \left(\sum_{p=0}^{+\infty} \frac{1}{(2p+1)!} \left(-\|y\|^2\right)^p\right) \varphi_y \\ &= Id - \frac{1}{\|y\|^2} \left(\sum_{p=0}^{+\infty} \frac{(-1)^p \|y\|^{2p}}{(2p)!} - 1\right) \varphi_y^2 + \frac{1}{\|y\|} \left(\sum_{p=0}^{+\infty} \frac{(-1)^p \|y\|^{2p+1}}{(2p+1)!}\right) \varphi_y \\ &= Id + \frac{1}{\|y\|^2} (1 - \cos(\|y\|)) \varphi_y^2 + \frac{1}{\|y\|} (\sin(\|y\|)) \varphi_y \end{aligned}$$
soit pour tout $x \in E$:
$$\begin{aligned} e^{\varphi_y}(x) &= x - \frac{1}{\|y\|^2} (\cos(\|y\|) - 1) \left(\langle x \mid y \rangle y - \|y\|^2 x\right) + \frac{\sin(\|y\|)}{\|y\|} x \wedge y \\ &= x + (1 - \cos(\|y\|)) \left(\frac{\langle x \mid y \rangle}{\|y\|^2} y - x\right) + \frac{\sin(\|y\|)}{\|y\|} x \wedge y \\ &= \cos(\|y\|) x + (1 - \cos(\|y\|)) \frac{\langle x \mid y \rangle}{\|y\|^2} y + \frac{\sin(\|y\|)}{\|y\|} x \wedge y \end{aligned}$$

Exercice 2.12. *E est un espace euclidien de dimension 3 orienté. Montrer que $u \in \mathcal{L}(E)$ est anti-symétrique si, et seulement si, il existe un unique vecteur $a \in E$ tel que $u(x) = a \wedge x$ pour tout $x \in E$.*

Solution. Pour tout $a \in E$, l'application linéaire $u : x \mapsto a \wedge x$ est bien anti-symétrique. En effet, pour x, y dans E, on a :

$$\begin{aligned}\langle u(x) \mid y\rangle &= \langle a \wedge x \mid y\rangle = \det(a, x, y) = -\det(a, y, x) = -\langle a \wedge y \mid x\rangle \\ &= -\langle u(y) \mid x\rangle = -\langle x \mid u(y)\rangle\end{aligned}$$

donc $u^* = -u$.

Soit $u \in \mathcal{L}(E)$ de matrice A dans la base orthonormée $\mathcal{B}_0$. La matrice de u^* dans la base $\mathcal{B}_0$ est ${}^tA$ et pour u anti-symétrique, on a $u^* = -u$, donc ${}^tA = -A$. Étant en dimension impaire, on a $\det(A) = \det({}^tA) = -\det(A)$ et $\det(A) = 0$. Il en résulte que $\ker(u)$ est de dimension $1, 2$ ou 3. Si $u = 0$, on a alors $u(x) = a \wedge x$ pour tout $x \in E$ avec $a = 0$. Pour $u \neq 0$, $\ker(u)$ est de dimension 1 ou 2. Pour tout $x \in \ker(u)$ et tout $y \in E$, on a $\langle x \mid u(y)\rangle = -\langle u(x) \mid y\rangle = 0$, donc $x \in (\operatorname{Im}(u))^{\perp}$. On a donc $\ker(u) \subset (\operatorname{Im}(u))^{\perp}$ et l'égalité avec les dimensions (le théorème du rang nous dit que $\dim(\ker(u)) = 3 - \dim(\operatorname{Im}(u)) = \dim\left((\operatorname{Im}(u))^{\perp}\right)$). On a donc $E = \operatorname{Im}(u) \oplus (\operatorname{Im}(u))^{\perp} = \operatorname{Im}(u) \oplus \ker(u)$. Si $\ker(u)$ est de dimension 2, $\operatorname{Im}(u)$ est alors de dimension 1, soit $\operatorname{Im}(u) = \mathbb{R} \cdot e$ avec $e \neq 0$. Il en résulte qu'il existe un réel non nul λ tel que $u(e) = \lambda e$ ($\lambda = 0$ donne $e \in \ker(u) \cap \operatorname{Im}(u)$ avec $e \neq 0$, ce qui n'est pas possible) et on a :

$$\lambda \|e\|^2 = \langle e \mid u(e)\rangle = -\langle u(e) \mid e\rangle = -\lambda \|e\|^2$$

donc $\lambda \|e\| = 0$ avec λ et $\|e\|$ non nul, ce qui n'est pas possible. En définitive $\ker(u)$ est de dimension 1 et $\operatorname{Im}(u)$ de dimension 2. En désignant par (f_1, f_2, f_3) une base orthonormée directe telle que f_1 dirige $\ker(u)$ et (f_2, f_3) engendre $\operatorname{Im}(u)$, la matrice de u dans cette base est anti-symétrique de la forme $A' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \alpha \\ 0 & -\alpha & 0 \end{pmatrix}$ ($\operatorname{Im}(u)$ est stable par u) avec $\alpha \neq 0$. Pour $x = x_1 f_1 + x_2 f_2 + x_3 f_3$ dans E, on a alors :

$$u(x) = \alpha(x_3 f_2 - x_2 f_3) = (-\alpha f_1) \wedge x = a \wedge x$$

S'il existe un autre vecteur $b \in E$ tel que $u(x) = b \wedge x$ pour tout $x \in E$, on a alors $u(a) = a \wedge a = 0 = b \wedge a$, les vecteur a et b sont liés. Si $a = 0$, on a alors $u(x) = b \wedge x = 0$ pour tout $x \in E$ et b est nul (sinon en prenant x linéairement indépendant de b, on a $b \wedge x \neq 0$). Si $a \neq 0$, il existe alors un réel λ tel que $b = \lambda a$ et $u(x) = a \wedge x = \lambda a \wedge x$ pour tout $x \in E$. Pour x indépendant de a, on a $a \wedge x \neq 0$ et nécessairement $\lambda = 1$, soit $b = a$.

Chapitre 3

Idéaux d'un anneau commutatif unitaire (nouvelle version du 12/12/2024)

Pour ce chapitre, sauf précision contraire, $\mathbb{A}$ désigne un anneau commutatif unitaire et on note 0 et 1 (ou $0_{\mathbb{A}}$ et $1_{\mathbb{A}}$ s'il y a ambiguïté) les éléments neutres pour l'addition et la multiplication de $\mathbb{A}$, avec $0 \neq 1$; $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$ l'ensemble des éléments non nuls de $\mathbb{A}$; $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles (ou des unités) de $\mathbb{A}$.

On convient que les sous-anneaux de $\mathbb{A}$ contiennent l'unité $1_{\mathbb{A}}$ et qu'un morphisme d'anneaux commutatifs unitaires $\varphi : \mathbb{A} \to \mathbb{B}$ est tel que $\varphi(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps commutatif, sont supposés connus (voir le chapitre **??** pour l'étude de $\mathbb{K}[X]$).

On peut aussi considérer des anneaux non commutatifs. En pratique nous rencontrerons l'anneau $\mathcal{M}_n(\mathbb{K})$ des matrices carrées d'ordre $n \geq 2$ à coefficients dans un corps commutatif $\mathbb{K}$ (pour $n = 1$, $\mathcal{M}_n(\mathbb{K}) = \mathbb{K}$) ou encore l'anneau $\mathcal{L}(E)$ des endomorphismes d'un $\mathbb{K}$-espace vectoriel E (de dimension finie ou pas).

3.1 Rappels de notions de base sur les anneaux

Définition 3.1. *L'anneau $\mathbb{A}$ est* intègre *s'il n'admet pas de diviseurs de 0, c'est-à-dire que pour a, b dans $\mathbb{A}$, l'égalité $a \cdot b = 0$ est réalisée si, et seulement si, $a = 0$ ou $b = 0$, ce qui équivaut aussi à dire que $a \cdot b \neq 0$ si, et seulement si, $a \neq 0$ et $b \neq 0$.*

Exemples 3.1

— *Un corps est intègre (si $y \neq 0$ et $xy = 0$, on a alors $x = (xy)\, y^{-1} = 0$).*

— *Un sous-anneau d'un anneau intègre est intègre.*

— *L'anneau* $\mathbb{A}[X]$ *des polynômes à coefficients dans l'anneau* $\mathbb{A}$ *est intègre si, et seulement si,* $\mathbb{A}$ *est intègre (théorème* **??***).*

Étant donné un anneau intègre $\mathbb{A}$, la relation $\mathcal{R}$ définie sur le produit $\mathbb{A} \times \mathbb{A}^*$ par :

$$((a,b)\ \mathcal{R}\ (a',b')) \Leftrightarrow (ab' = a'b)$$

est une relation d'équivalence et les opérations internes d'addition et de multiplication définies sur $\mathbb{A} \times \mathbb{A}^*$ par :

$$(a,b) + (c,d) = (ad+bc, bd)\,,\ (a,b)\cdot(c,d) = (ac, bd)$$

sont compatibles avec $\mathcal{R}$. Ces opérations passent donc au quotient $(\mathbb{A} \times \mathbb{A}^*)/\mathcal{R}$.

En notant $\frac{a}{b}$ la classe d'équivalence de $(a,b) \in \mathbb{A} \times \mathbb{A}^*$, on a $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ et $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

On vérifie que $(\mathbb{A} \times \mathbb{A}^*)/\mathcal{R}$ muni de ces deux lois est un anneau commutatif unitaire, le neutre pour l'addition étant $\frac{0}{1} = \frac{0}{b}$, où $b \in \mathbb{A}^*$, l'opposé de $\frac{a}{b}$ étant $\frac{-a}{b}$ et le neutre pour le produit étant $\frac{1}{1} = \frac{b}{b}$, où $b \in \mathbb{A}^*$. Tout élément non nul $\frac{a}{b}$ est inversible d'inverse $\frac{b}{a}$, donc $(\mathbb{A} \times \mathbb{A}^*)/\mathcal{R}$ est un corps.

On dit que $(\mathbb{A} \times \mathbb{A}^*)/\mathcal{R}$ est le *corps des fractions* de $\mathbb{A}$ et on le note $\mathrm{Fr}(\mathbb{A})$.

On vérifie que l'application $\varphi : a \in \mathbb{A} \mapsto \frac{a}{1} \in \mathrm{Fr}(\mathbb{A})$ est un morphisme d'anneau injectif, ce qui permet de voir l'anneau intègre $\mathbb{A}$ comme sous-anneau du corps $\mathrm{Fr}(\mathbb{A})$.

Pour $\mathbb{A} = \mathbb{Z}$, $\mathrm{Fr}(\mathbb{Z})$ est le corps $\mathbb{Q}$ des nombres rationnels et pour $\mathbb{A} = \mathbb{K}[X]$, où $\mathbb{K}$ est un corps commutatif, $\mathrm{Fr}(\mathbb{K}[X])$ est le corps $\mathbb{K}(X)$ des fractions rationnelles à coefficients dans $\mathbb{K}$.

Définition 3.2. *Deux éléments* a, b *d'un anneau* $\mathbb{A}$ *sont dits* associés *s'il existe un élément inversible* $u \in \mathbb{A}^\times$ *tel que* $b = ua$.

Les unités de $\mathbb{A}$ sont les éléments associés à 1.
a et b sont associés si, et seulement si, a divise b et b divise a.

Définition 3.3. *Un élément* p *d'un anneau intègre* $\mathbb{A}$ *est dit* irréductible *si* $p \neq 0$, p *n'est pas inversible et les seuls diviseurs de* p *sont les éléments inversibles ou les éléments de* $\mathbb{A}$ *associés à* p, *ce qui signifie que :*

$$(p = ab) \Rightarrow (a \text{ ou } b \text{ est inversible})$$

Si $p \in \mathbb{A}$ est irréductible, il en est alors de même de up pour tout u inversible dans $\mathbb{A}$. En effet, si $up = vw$, on a alors $p = \left(u^{-1}v\right) w$ et $u^{-1}v$ ou w est inversible, l'élément $u^{-1}v$ étant inversible si, et seulement si, v l'est.

Dans un corps $\mathbb{K}$, il n'y a pas d'élément irréductible puisque $\mathbb{K}^\times = \mathbb{K}^*$.

Définition 3.4. *Un élément p d'un anneau intègre $\mathbb{A}$ est dit* premier *si $p \neq 0$, p n'est pas inversible et :*

$$(p \text{ divise } ab) \Rightarrow (p \text{ divise } a \text{ ou } p \text{ divise } b)$$

Par récurrence, on vérifie que si $p \in \mathbb{A}$ intègre est premier et divise un produit $\prod_{k=1}^{r} a_k$, il divise alors l'un des a_k.

Lemme 3.1 *Un élément premier dans un anneau intègre $\mathbb{A}$ est irréductible.*

Preuve. Soit $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$ premier. Si $p = ab$, il divise alors ab et étant premier, il divise a ou b. Comme a et b jouent des rôles symétriques, on peut supposer que p divise a, c'est-à-dire qu'il existe $q \in \mathbb{A}$ tel que que $a = qp$ et dans ce cas, on a $p = ab = qpb$, soit $qb = 1$ puisque $p \neq 0$ dans $\mathbb{A}$ qui est intègre, ce qui signifie que $b \in \mathbb{A}^\times$. En conclusion p est irréductible. □

En général un élément irréductible d'un anneau intègre n'est pas nécessairement premier (exercice 3.2).

Nous verrons plus loin que dans un anneau factoriel (définition 3.9) ou principal (définition 4.1), il y a équivalence entre premier et irréductible.

3.2 Généralités sur les idéaux d'un anneau unitaire

Si $\varphi : \mathbb{A} \to \mathbb{B}$ est un morphisme d'anneaux commutatifs unitaires, son noyau $\ker(\varphi)$ est alors un sous-groupe de $\mathbb{A}$ et pour tout $a \in \ker(b)$, tout $b \in \mathbb{A}$, on a $\varphi(ab) = \varphi(a)\varphi(b) = 0_{\mathbb{B}}$, donc $ab \in \ker(\varphi)$. Ces propriétés se traduisent en disant que $\ker(\varphi)$ est un idéal de $\mathbb{A}$.

Définition 3.5. *Un* idéal *de $\mathbb{A}$ est un sous-groupe additif I de $\mathbb{A}$ tel que :*

$$\forall (a,b) \in I \times \mathbb{A},\ ab \in I$$

(on dit que I est absorbant *pour le produit).*

Après avoir introduit la notion d'anneau quotient (paragraphe 3.4), nous verrons, que tout idéal de $\mathbb{A}$ est le noyau d'un morphisme d'anneaux (corollaire 3.2).

Dans le cas d'un anneau unitaire non commutatif, on définit les notions d'idéal à droite (pour $(a,b) \in I \times \mathbb{A},\ ab \in I$), à gauche (pour $(a,b) \in I \times \mathbb{A},\ ba \in I$) ou bilatère (pour $(a,b) \in I \times \mathbb{A},\ ab$ et ba sont dans I). Au paragraphe 3.3 nous décrirons en particulier les idéaux bilatères de $\mathcal{L}(E)$.

Exemples 3.2

— *$\{0\}$ et $\mathbb{A}$ sont des idéaux de $\mathbb{A}$.*

— *Si $(I_k)_{k\in K}$ est une famille d'idéaux de $\mathbb{A}$, $I = \bigcap_{k\in K} I_k$ est alors un idéal.*

— *Si* $I_0 \subset I_1 \subset \cdots \subset I_n \subset \cdots$ *est une suite croissante d'idéaux de* $\mathbb{A}$, *la réunion* $I = \bigcup_{k=0}^{+\infty} I_k$ *est alors un idéal de* $\mathbb{A}$. *En effet,* I *est non vide et pour* a, b *dans* I *et* c *dans* $\mathbb{A}$, *il existe deux entiers* n, m *tels que* $a \in I_n$, $b \in I_m$, *donc* a *et* b *sont dans* I_p, *où* $p = \max(n, m)$ *(la suite* $(I_n)_{n\in\mathbb{N}}$ *est croissante) et* $a - b \in I_p \subset I$, $ac \in I_p \subset I$.

— *Pour tout* $a \in \mathbb{A}$, *l'ensemble* $(a) = a \cdot \mathbb{A} = \{qa,\ q \in \mathbb{A}\}$ *des multiples de* a *dans* $\mathbb{A}$ *est un idéal. Un tel idéal est dit* principal *et on dit que c'est l'idéal engendré par* a. *Pour tous* a, b *dans* $\mathbb{A}$, *on a :*

$$(a \text{ divise } b) \Leftrightarrow ((b) \subset (a))$$

Pour $\mathbb{A}$ *intègre, on a :*

$$(a \text{ et } b \text{ sont associés}) \ \Leftrightarrow ((a) = (b))$$

— *Plus généralement, pour toute suite* $(a_k)_{1\leq k\leq p}$ *d'éléments de* $\mathbb{A}$, *l'ensemble* $(a_1, \cdots, a_p) = \left\{\sum_{k=1}^{p} q_k a_k,\ (q_k)_{1\leq k\leq p} \in \mathbb{A}^p\right\}$ *est un idéal. On dit que c'est l'idéal engendré par* $\{a_1, \cdots, a_p\}$ *et qu'il est* de type fini.

— *Si* $(I_k)_{1\leq k\leq p}$ *est une famille d'idéaux de* $\mathbb{A}$, *l'ensemble :*

$$\sum_{k=1}^{p} I_k = \left\{\sum_{k=1}^{p} x_k,\ (x_k)_{1\leq k\leq p} \in \prod_{k=1}^{p} I_k\right\}$$

est un idéal. Pour $I_k = (a_k)$, *on a* $\sum_{k=1}^{p} (a_k) = (a_1, \cdots, a_p)$.

Lemme 3.2 *Soit* I *un idéal (à gauche ou à droite ou bilatère) de* $\mathbb{A}$ *(commutatif ou pas). On a* $I = \mathbb{A}$ *si, et seulement si,* I *contient un élément inversible.*

Preuve. La condition nécessaire est évidente. Réciproquement s'il existe u inversible dans I, on a alors pour tout $a \in \mathbb{A}$, $a = u \cdot \left(u^{-1}a\right) \in I$ [resp. $a = \left(au^{-1}\right) \cdot u \in I$] et $I = \mathbb{A}$. □

Lemme 3.3 *Soit* $\varphi : \mathbb{A} \to \mathbb{B}$ *un morphisme d'anneaux.*

1. *Pour tout idéal* J *de* $\mathbb{B}$, $\varphi^{-1}(J)$ *est un idéal de* $\mathbb{A}$. *En particulier le noyau* $\ker(\varphi) = \varphi^{-1}(\{0\})$ *est un idéal de* $\mathbb{A}$.
2. *Si* φ *est surjectif, alors pour tout idéal* I *de* $\mathbb{A}$, $\varphi(I)$ *est un idéal de* $\mathbb{B}$ *et l'application* Φ *qui associe à tout idéal* J *de* $\mathbb{B}$ *l'idéal* $\varphi^{-1}(J)$ *de* $\mathbb{A}$ *réalise une bijection de l'ensemble des idéaux de* $\mathbb{B}$ *dans l'ensemble des idéaux de* $\mathbb{A}$ *qui contiennent* $\ker(\varphi)$.

Preuve.
1. Soient J un idéal de $\mathbb{B}$ et $I = \varphi^{-1}(J) = \{a \in \mathbb{A},\ \varphi(a) \in J\}$. On a $0_{\mathbb{A}} \in I$ car $\varphi(0_{\mathbb{A}}) = 0_{\mathbb{B}} \in J$. Pour tous a et b dans I, on a $\varphi(a) \in J$ et $\varphi(b) \in J$, donc

$\varphi(a-b)=\varphi(a)-\varphi(b)\in J$ et $a-b\in I$. Pour $a\in I$ et $b\in\mathbb{A}$, on a $\varphi(a)\in J$, donc $\varphi(ab)=\varphi(a)\varphi(b)\in J$ et $ab\in I$. En définitive, I est un idéal de $\mathbb{A}$.

2. Soient I un idéal de $\mathbb{A}$ et $J=\varphi(I)=\{\varphi(a),\ a\in I\}$. On a $0_{\mathbb{B}}=\varphi(0_{\mathbb{A}})\in J$ et pour $\varphi(a),\varphi(b)$ dans J, on a $a-b\in I$, donc $\varphi(a)-\varphi(b)=\varphi(a-b)\in J$. Pour $\varphi(a)\in J$ et $c\in\mathbb{B}$, dans le cas où φ est surjective, il existe $b\in\mathbb{A}$ tel que $c=\varphi(b)$ et $\varphi(a)\cdot c=\varphi(a)\varphi(b)=\varphi(ab)\in J(I)$. En définitive, J est un idéal de $\mathbb{B}$.

Pour tout idéal J de $\mathbb{B}$ et tout $a\in\ker(\varphi)$, on a $\varphi(a)=0_{\mathbb{B}}\in J$, soit $a\in\varphi^{-1}(J)$, donc $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$ qui contient $\ker(\varphi)$. Comme φ est surjective, on a $\varphi\left(\varphi^{-1}(Y)\right)=Y$ pour toute partie Y de $\mathbb{B}$ (on a toujours $\varphi\left(\varphi^{-1}(Y)\right)\subset Y$ et pour tout $b\in Y$, il existe $a\in\mathbb{A}$ tel que $b=\varphi(a)$ par surjectivité de φ, donc $a\in\varphi^{-1}(Y)$ et $b\in\varphi\left(\varphi^{-1}(Y)\right)$, ce qui nous donne l'égalité $\varphi\left(\varphi^{-1}(Y)\right)=Y$), donc l'application Φ est injective. Si I est un idéal de $\mathbb{A}$ qui contient $\ker(\varphi)$, l'ensemble $J=\varphi(I)$ est un idéal de $\mathbb{B}$ puisque φ est surjective et $\Phi(J)=\varphi^{-1}(\varphi(I))=I$ (il est clair que $I\subset\varphi^{-1}(\varphi(I))$ et pour $a\in\varphi^{-1}(\varphi(I))$, on a $\varphi(a)\in\varphi(I)$, soit $\varphi(a)=\varphi(b)$ avec $b\in I$, donc $a-b\in\ker(\varphi)\subset I$ et $a\in I$). L'application Φ est donc surjective. □

Si φ n'est pas surjectif, $\varphi(I)$ n'est pas nécessairement un idéal de $\mathbb{B}$. Par exemple si φ est l'injection canonique de $\mathbb{Z}$ dans $\mathbb{R}$, $\varphi(\mathbb{Z})=\mathbb{Z}$ n'est pas un idéal de $\mathbb{R}$ car par exemple, $\dfrac{1}{2}\cdot 1\notin\mathbb{Z}$.

3.3 Idéaux de $\mathcal{L}(E)$

On s'intéresse dans ce paragraphe aux idéaux de l'anneau non commutatif $\mathcal{L}(E)$ des endomorphismes de E, où E est un espace vectoriel sur un corps commutatif $\mathbb{K}$, pour $\dim(E)\geq 2$.

Théorème 3.1.

Si l'espace vectoriel E est de dimension finie, les seuls idéaux bilatères de $\mathcal{L}(E)$ sont $\{0\}$ et $\mathcal{L}(E)$.

Preuve. On suppose que E est de dimension n. Pour $n=1$, $\mathcal{L}(E)\backsimeq\mathbb{K}$ et ses seuls idéaux sont $\{0\}$ et $\mathcal{L}(E)$ (exercice 3.1). Pour $n\geq 2$, si $\mathcal{B}=(e_i)_{1\leq i\leq n}$ est une base de E, on lui associe alors la base $(u_{ij})_{1\leq i,j\leq n}$ de $\mathcal{L}(E)$ définie par :

$$u_{ij}(e_k)=\delta_{j,k}e_i=\begin{cases}0 \text{ si } k\neq j\\ e_i \text{ si } k=j\end{cases}\quad(1\leq i,j,k\leq n)$$

(les matrices E_{ij} de u_{ij} dans la base $\mathcal{B}$ pour $1\leq i,j\leq n$ forment la base canonique de $\mathcal{M}_n(\mathbb{K})$).

On vérifie facilement que :

$$u_{ij}\circ u_{pq}=\delta_{j,p}u_{iq}=\begin{cases}0 \text{ si } j\neq p\\ u_{iq} \text{ si } j=p\end{cases}\quad(1\leq i,j,p,q\leq n)$$

Pour tout $u = \sum_{1\leq p,q\leq n} a_{pq}u_{pq} \in \mathcal{L}(E)$ et pour $1 \leq i,j,r,s \leq n$ on a :

$$u_{ij} \circ u = \sum_{1\leq p,q\leq n} a_{pq}u_{ij} \circ u_{pq} = \sum_{q=1}^{n} a_{jq}u_{iq}$$

et $u_{ij} \circ u \circ u_{rs} = \sum_{q=1}^{n} a_{jq}u_{iq} \circ u_{rs} = a_{jr}u_{is}$.

Si I est un idéal bilatère de $\mathcal{L}(E)$ non réduit à $\{0\}$, il contient au moins un élément u non nul. Dans la base $\mathcal{B}$ de $\mathcal{L}(E)$, on a $u = \sum_{1\leq p,q\leq n} a_{pq}u_{pq}$ et il existe des indices j,r compris entre 1 et n tels que $a_{j,r} \neq 0$. Comme I est un idéal bilatère de $\mathcal{L}(E)$, pour tous i,s compris entre 1 et n, on a $a_{jr}u_{is} = u_{ij} \circ u \circ u_{rs} \in I$ et prenant $s = i$, on déduit que pour tout i compris entre 1 et n, on a $a_{jr}u_{ii} = u_{ij} \circ u \circ u_{ri} \in I$, donc $a_{jr}Id = a_{jr}\sum_{i=1}^{n} u_{ii} \in I \cap \mathrm{GL}(E)$ et $I = \mathcal{L}(E)$. En conclusion $\{0\}$ et $\mathcal{L}(E)$ sont les seuls idéaux bilatère de $\mathcal{L}(E)$.

On peut procéder autrement, en utilisant le fait que deux endomorphismes de même rang dans $\mathcal{L}(E)$ sont équivalents (exercice 3.3).

Soient $I \neq \{0\}$ un idéal de $\mathcal{L}(E)$ et $u \in I \setminus \{0\}$ de rang $r \in \{1,\cdots,n\}$. Si $r = n$, u est alors inversible et $I = \mathcal{L}(E)$. Si $r < n$, I contient alors tous les endomorphismes de rang r puisqu'ils sont tous équivalents. En désignant par $\mathcal{B} = (e_i)_{1\leq i\leq n}$ une base de E et par p,q les endomorphismes de rang r de E de matrices respectives $A_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ et $B_r = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & I_{r-2} & 0 \\ 0 & 0 & 0 & 0_{n-r} \end{pmatrix}$ dans la base $\mathcal{B}$, l'endomorphisme $q-p$ de matrice $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0_{n-2} \end{pmatrix}$ dans $\mathcal{B}$ est de rang 1 et dans I, donc I contient tous les endomorphismes de rang 1. Il en résulte que I contient $Id = \sum_{\ell=1}^{n} u_{\ell\ell}$ qui est somme de n endomorphismes de rang 1 et $I = \mathcal{L}(E)$.
□

Avec l'exercice 3.5, on s'intéresse aux idéaux bilatères de $\mathcal{L}(E)$ pour E de dimension infinie.

Corollaire 3.1. *Si E,F sont deux $\mathbb{K}$-espaces vectoriels de dimension finie, tout morphisme d'anneaux $\varphi : \mathcal{L}(E) \to \mathcal{L}(F)$ est alors injectif.*

Preuve. $\ker(\varphi)$ est un idéal bilatère de $\mathcal{L}(E)$ distinct de $\mathcal{L}(E)$ car $\varphi(I_d) = I_d$, donc il est réduit à $\{0\}$ et φ est injectif. □

Dans le cas où E est de dimension finie, nous allons voir que les idéaux à droite [resp. à gauche] de $\mathcal{L}(E)$ sont de la forme $\{u \in \mathcal{L}(E),\ \mathrm{Im}(u) \subset F\}$ [resp. $\{u \in \mathcal{L}(E),\ \ker(u) \supset F\}$] où F est un sous-espace vectoriel de E.

Pour tout sous-espace vectoriel F de E, on note $I_F = \{u \in \mathcal{L}(E),\ \mathrm{Im}(u) \subset F\}$ et pour tout idéal à droite I de $\mathcal{L}(E)$, on note $F_I = \sum_{u\in I} \mathrm{Im}(u)$.

Lemme 3.4 *Si $I \neq \{0\}$ est un idéal à droite de $\mathcal{L}(E)$, c'est alors un sous-espace vectoriel de $\mathcal{L}(E)$ et il existe une famille finie $(v_k)_{1\leq k\leq p}$ d'éléments de I telle que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$.*

Preuve. Pour $I = \{0\}$, on a $F_I = \{0\}$. Si $I \neq \{0\}$ est un idéal à droite de $\mathcal{L}(E)$, c'est aussi un sous-espace vectoriel de $\mathcal{L}(E)$ (pour $\lambda \in \mathbb{K}$ et $u \in I$, on a $\lambda u = u \circ (\lambda I_d) \in I$) et comme E est de dimension finie, on dispose d'une base $(v_k)_{1\leq k\leq p}$ de I. Pour tout $u = \sum_{k=1}^{p} \lambda_k v_k \in I$, on a $\mathrm{Im}(u) \subset \sum_{k=1}^{p} \mathrm{Im}(v_k)$, ce qui nous donne $\sum_{u\in I} \mathrm{Im}(u) \subset \sum_{k=1}^{p} \mathrm{Im}(v_k) \subset \sum_{u\in I} \mathrm{Im}(u)$ et l'égalité $\sum_{u\in I} \mathrm{Im}(u) = \sum_{k=1}^{p} \mathrm{Im}(v_k)$. □

Lemme 3.5 *Si $F \neq \{0\}$ est un sous-espace vectoriel de E, l'ensemble I_F est alors un idéal à droite de $\mathcal{L}(E)$ et $F_{I_F} = F$.*

Preuve. Une projection sur F parallèlement à un supplémentaire de F est dans I_F et pour u, v dans I_F, on a $\mathrm{Im}(u - v) \subset \mathrm{Im}(u) + \mathrm{Im}(v) \subset F$, donc I_F est un sous-groupe additif de $\mathcal{L}(E)$.

Pour $u \in I_F$ et $v \in \mathcal{L}(E)$, on a $\mathrm{Im}(u \circ v) \subset \mathrm{Im}(u) \subset F$, donc I_F est un idéal à droite de $\mathcal{L}(E)$. Pour tout $u \in I_F$, on a $\mathrm{Im}(u) \subset F$, donc $F_{I_F} = \sum_{u\in I_F} \mathrm{Im}(u) \subset F$. En désignant par p_F une projection sur F parallèlement à un supplémentaire de F, on a $p_F \in I_F$ et $F = \mathrm{Im}(p_F) \subset F_{I_F} = \sum_{u\in I_F} \mathrm{Im}(u)$, d'où l'égalité $F_{I_F} = F$. □

Théorème 3.2.

Si E est un espace vectoriel de dimension finie, les idéaux à droite de $\mathcal{L}(E)$ sont de la forme $I_F = \{u \in \mathcal{L}(E),\ \mathrm{Im}(u) \subset F\}$, où F est un sous-espace vectoriel de E.

Preuve. Pour $I = \{0\}$, on a $I = I_{\{0\}}$.

Soient $I \neq \{0\}$ un idéal à droite de $\mathcal{L}(E)$ et $(v_k)_{1\leq k\leq p}$ une base de I telle que $F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$ (lemme 3.4).

Pour tout $u = \sum_{k=1}^{p} \lambda_k v_k \in I$, on a $\mathrm{Im}(u) \subset F_I = \sum_{k=1}^{p} \mathrm{Im}(v_k)$, donc $I \subset I_{F_I}$.

Pour $u \in I_{F_I}$, on a $\mathrm{Im}\,(u) \subset F_I = \sum_{k=1}^{p} \mathrm{Im}\,(v_k)$. En désignant par $(e_j)_{1\leq j\leq n}$ une base de E, pour tout j compris entre 1 et n, on peut écrire $u\,(e_j) = \sum_{k=1}^{p} v_k\,(x_{j,k})$, où les $x_{j,k}$ sont dans E. En désignant par $v : E^p \to E$ l'application linéaire définie par $v\,(x_1, \cdots, x_p) = \sum_{k=1}^{p} v_k\,(x_k)$ et par $\varphi : E \to E^p$ l'application linéaire définie par $\varphi\,(e_j) = (x_{j,k})_{1\leq k\leq p}$, on a $u\,(e_j) = v\,(x_{j,1}, \cdots, x_{j,p}) = v \circ \varphi\,(e_j)$, pour tout j compris entre 1 et n, soit $u = v \circ \varphi$. Notant $\varphi = (\varphi_j)_{1\leq j\leq p}$, les φ_j étant dans $\mathcal{L}\,(E)$, on a $u = v \circ \varphi = \sum_{k=1}^{p} v_k \circ \varphi_k \in I$ puisque les v_k sont dans l'idéal à droite I. En définitive, on a $I = I_{F_I}$. □

On a aussi $I = p_F \circ \mathcal{L}\,(E) = \{p_F \circ v,\ v \in \mathcal{L}\,(E)\}$. En effet, pour tout $v \in \mathcal{L}\,(E)$, on a $\mathrm{Im}\,(p_F \circ v) \subset \mathrm{Im}\,(p_F) = F$, donc $p_F \circ v \in I$ et $p_F \circ \mathcal{L}\,(E) \subset I$. Pour $u \in I$, on a $\mathrm{Im}\,(u) \subset F$, donc $p_F \circ u = u \in p_F \circ \mathcal{L}\,(E)$ et l'égalité $I = p_F \circ \mathcal{L}\,(E)$.

Théorème 3.3.

Si E est un espace vectoriel de dimension finie, les idéaux à gauche de $\mathcal{L}\,(E)$ sont de la forme $J_F = \{u \in \mathcal{L}\,(E),\ \ker\,(u) \supset F\}$, où F est un sous-espace vectoriel de E.

Preuve. On peut procéder comme pour les idéaux à droite (voir [**?**], volume 1, exercice 6.25), mais utiliser la dualité est plus rapide.

On vérifie d'abord que, pour tout sous-espace vectoriel F de E, J_F est un idéal à gauche de $\mathcal{L}\,(E)$.

Pour $F = E$, on a $J_F = \{0\}$. La projection parallèlement à F sur un supplémentaire de F est dans J_F et pour u, v dans J_F, on a $F \subset \ker\,(u) \cap \ker\,(v) \subset \ker\,(u - v)$, donc J_F est un sous-groupe additif de $\mathcal{L}\,(E)$. Pour $u \in J_F$ et $v \in \mathcal{L}\,(E)$, on a $F \subset \ker\,(u) \subset \ker\,(v \circ u)$, donc J_F est un idéal à gauche de $\mathcal{L}\,(E)$.

On désigne par E^* le dual de E et pour tout idéal à gauche I de $\mathcal{L}\,(E)$, on note ${}^tI = \{\,{}^tu,\ u \in I\}$. On vérifie alors que ${}^tI$ est un idéal à droite de $\mathcal{L}\,(E^*)$, ce qui nous permet de conclure. Avec ${}^t\,(u - v) = {}^tu - {}^tv$, ${}^t\,(u \circ v) = {}^tv \circ {}^tu$ et le fait qu'en dimension finie tout $w \in \mathcal{L}\,(E^*)$ est de la forme $w = {}^tu$ (en effet, si $(e_j)_{1\leq j\leq n}$ est une base de E, $\left(e_j^*\right)_{1\leq j\leq n}$ sa base duale, on a $w\left(e_j^*\right) = \sum_{i=1}^{n} \alpha_{ji} e_i^*$ et définissant $u \in \mathcal{L}\,(E)$ par $u\,(e_j) = \sum_{i=1}^{n} \alpha_{ij} e_i$, on a $w\left(e_j^*\right)(e_k) = \sum_{i=1}^{n} \alpha_{ji} e_i^*\,(e_k) = \alpha_{jk}$ et ${}^tu\left(e_j^*\right)(e_k) = e_j^* \circ u\,(e_k) = e_j^*\left(\sum_{i=1}^{n} \alpha_{ik} e_i\right) = \alpha_{jk}$), on déduit que ${}^tI$ est un idéal à droite de $\mathcal{L}\,(E^*)$. Il existe donc un sous-espace vectoriel G de E^* tel que l'on ait ${}^tI = \{w \in \mathcal{L}\,(E^*),\ \mathrm{Im}\,(w) \subset G\}$. En notant $F = \{x \in E,\ \forall \varphi \in G,\ \varphi\,(x) = 0\}$ l'orthogonal de G dans E, pour tout $u \in I$, on a $\mathrm{Im}\,({}^tu) \subset G$, ce qui implique que $\ker\,(u) = (\mathrm{Im}\,({}^tu))^\circ \supset G^\circ = F$. Réciproquement, si $u \in \mathcal{L}\,(E)$ est tel que

$\ker(u) \supset F$, on a alors $\mathrm{Im}({}^t u) = (\ker(u))^\perp \subset F^\perp = G$, donc ${}^t u \in {}^t I$, soit ${}^t u = {}^t v$ avec $v \in I$ et $u = v \in I$. En conclusion, les idéaux à gauche de $\mathcal{L}(E)$ sont de la forme $J_F = \{u \in \mathcal{L}(E),\ \ker(u) \supset F\}$ où F est un sous-espace vectoriel de E. □

En désignant par p_G un projecteur de E sur un supplémentaire G de E parallèlement à F, on a $F = \ker(p_G)$, donc $p_G \in I$ et $\mathcal{L}(E) \circ p_G \subset I$. Pour $u \in I$, on a $\ker(u) \supset F$, donc pour tout $x = x_F + x_G$ avec $(x_F, x_G) \in F \times G$, on a $u(x) = u(x_G) = u \circ p_G(x)$, soit $u = u \circ p_G \in \mathcal{L}(E) \circ p_G$ et l'égalité $I = \mathcal{L}(E) \circ p_G$.

3.4 Anneaux quotients par un idéal bilatère

Définition 3.6. *Soit I un idéal de $\mathbb{A}$. On dit que a est* congru *à b modulo I dans $\mathbb{A}$ si $b - a \in I$. On note alors $a \equiv b\ (I)$.*

Cette relation de congruence modulo I est une relation d'équivalence sur $\mathbb{A}$ et pour tout $a \in \mathbb{A}$, on note $\overline{a} = \{b \in \mathbb{A},\ b \equiv a\ (I)\} = a + I$ la classe d'équivalence correspondante. L'ensemble de ces classes d'équivalence modulo I est noté $\dfrac{\mathbb{A}}{I}$.

Pour $I = \{0\}$, dire que $b \equiv a\ (I)$ équivaut à $a = b$, donc $\dfrac{\mathbb{A}}{I}$ est isomorphe à $\mathbb{A}$.

Pour $I = \mathbb{A}$, il y a une seule classe d'équivalence, soit $\dfrac{\mathbb{A}}{I} = \{\overline{0}\}$.

Théorème 3.4.

Il existe une unique structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{A}}{I}$ telle que la surjection canonique $\pi_I : a \in \mathbb{A} \to \overline{a} = a + I \in \dfrac{\mathbb{A}}{I}$ soit un morphisme d'anneaux.

Preuve. Pour a, b, c, d dans $\mathbb{A}$ tels que $a \equiv b \bmod(I)$ et $c \equiv d \bmod(I)$, on a $(b+d) - (a+c) = (b-a) + (d-c) \in I$ et $bd - ac = b(d-c) + c(b-a) \in I$, donc $a + c \equiv b + d \bmod(I)$ et $ac \equiv bd \bmod(I)$. La relation de congruence modulo I est donc compatible avec la somme et le produit. On en déduit qu'on définit deux opérations internes sur $\dfrac{\mathbb{A}}{I}$ en posant $x + y = \overline{a+b}$ et $xy = \overline{ab}$ pour tous $x = \overline{a}$ et $y = \overline{b}$ dans $\dfrac{\mathbb{A}}{I}$. En effet, si a' est un autre représentant de x et b' un autre représentant de y, on a alors $a \equiv a'$ et $b \equiv b'$ modulo I, ce qui entraîne $a+b \equiv a'+b'$ et $ab \equiv a'b'$ modulo I, soit $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$, ce qui prouve que ces définitions de $x+y$ et xy ne dépendent pas des choix des représentants de x et y. On vérifie ensuite facilement que ces deux lois confèrent à $\dfrac{\mathbb{A}}{I}$ une structure d'anneau commutatif unitaire et que π_I est bien un morphisme d'anneaux. Réciproquement s'il existe une structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{A}}{I}$ qui fait de π_I un

morphisme d'anneaux, on a alors pour tous $x = \pi_I(a), y = \pi_I(b)$ dans $\frac{\mathbb{A}}{I}$:

$$\begin{cases} x+y = \pi_I(a) + \pi_I(b) = \pi_I(a+b) = \overline{a+b} \\ xy = \pi_I(a)\,\pi_I(b) = \pi_I(ab) = \overline{ab} \end{cases}$$

ce qui prouve l'unicité. □

Avec le chapitre **??**, nous étudions le cas particulier important des anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Corollaire 3.2. *Les idéaux de $\mathbb{A}$ sont les noyaux de morphismes d'anneaux $\varphi : \mathbb{A} \to \mathbb{B}$ où $\mathbb{B}$ est un anneau commutatif, unitaire.*

Preuve. Si $\varphi : \mathbb{A} \to \mathbb{B}$ est un morphisme d'anneaux, on a vu que $\ker(\varphi)$ est un idéal de $\mathbb{A}$ (lemme 3.3). Réciproquement si I est un idéal de $\mathbb{A}$, on a alors $I = \ker(\pi_I)$, où π_I désigne la surjection canonique de $\mathbb{A}$ sur l'anneau quotient $\frac{\mathbb{A}}{I}$. □

Corollaire 3.3. *Il y a une bijection entre les idéaux de $\frac{\mathbb{A}}{I}$ et les idéaux de $\mathbb{A}$ qui contiennent I.*

Preuve. Résulte du fait que π_I est un morphisme d'anneaux surjectif de $\mathbb{A}$ sur $\frac{\mathbb{A}}{I}$ de noyau $\ker(\pi_I) = I$ (lemme 3.3). □

3.5 Idéaux premiers et maximaux

Définition 3.7. *Un* idéal I *de $\mathbb{A}$ est dit* premier *s'il est distinct de $\mathbb{A}$ et si pour tous a, b dans $\mathbb{A}$, on a $ab \in I$ si, et seulement si, $a \in I$ ou $b \in I$.*

L'idéal $\{0\}$ est premier si, et seulement si, $\mathbb{A}$ est intègre.

Exemple 3.1 *Dans l'anneau $\mathbb{A} = \mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, l'ensemble $I = \{f \in \mathbb{A},\ f(0) = 0\}$ est un idéal premier. En effet, I est un idéal comme noyau du morphisme d'anneaux $f \in \mathbb{A} \mapsto f(0) \in \mathbb{R}$ et pour $fg \in I$, on a $f(0)\,g(0) = 0$, donc $f(0) = 0$ ou $g(0) = 0$, c'est-à-dire $f \in I$ ou $g \in I$.*

Définition 3.8. *Un idéal I de $\mathbb{A}$ est dit* maximal *s'il est distinct de $\mathbb{A}$ et si I et $\mathbb{A}$ sont les seuls idéaux de $\mathbb{A}$ qui contiennent I.*

Le lemme de Zorn qui nous dit qu'un ensemble ordonné inductif E (*i. e.* toute famille totalement ordonnée d'éléments de E possède un majorant) possède un élément maximal permet de montrer que tout idéal de $\mathbb{A}$ distinct de $\mathbb{A}$ est contenu dans un idéal maximal (théorème de Krull).

Théorème 3.5.

1. *Un idéal I de $\mathbb{A}$ est maximal si, et seulement si, l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est un corps.*
2. *Un idéal I de $\mathbb{A}$ est premier si, et seulement si, l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est intègre.*
3. *Un élément p de $\mathbb{A}$ intègre est premier si, et seulement l'idéal (p) est premier.*
4. *Un idéal maximal est premier.*
5. *Si un élément p de $\mathbb{A}$ intègre est tel que l'idéal (p) soit maximal, alors p est irréductible.*

Preuve.

1. Si I est un idéal maximal, pour $\overline{a} \neq \overline{0}$ dans $\dfrac{\mathbb{A}}{I}$, on a $a \notin I$ et l'idéal $(a)+I$ qui contient I est distinct de I, donc il est égal à $\mathbb{A}$ et $1 \in (a)+I$, ce qui signifie qu'il existe $(u,v) \in \mathbb{A} \times I$ tel que $1 = au + v$, donc $\overline{1} = \overline{au}$ et $\overline{a}$ est inversible. L'anneau $\dfrac{\mathbb{A}}{I}$ est donc un corps. Réciproquement si $\dfrac{\mathbb{A}}{I}$ est un corps et J est un idéal de $\mathbb{A}$ distinct de I qui contient I, il existe alors $a \in J \setminus I$, donc $\overline{a} \neq \overline{0}$ est inversible dans $\dfrac{\mathbb{A}}{I}$ et il existe $u \in \mathbb{A}$ tel que $\overline{au} = \overline{1}$, ce qui nous donne $1 = au + v$ avec $v \in I$, donc $1 \in J$ et $J = \mathbb{A}$. L'idéal I est donc maximal.

2. Si I est un idéal de $\mathbb{A}$, pour a, b dans $\mathbb{A}$, on a $\overline{a}\overline{b} = \overline{0}$ si, et seulement si, $ab \in I$, ce qui donne l'équivalence entre a premier dans $\mathbb{A}$ et (a) idéal premier de $\mathbb{A}$.

3. Pour $\mathbb{A}$ intègre, l'assertion :

$$(p \text{ divise } ab) \Leftrightarrow (p \text{ divise } a \text{ ou } p \text{ divise } b)$$

est équivalente à :

$$(ab \in (p)\ ) \Leftrightarrow (a \in (p)\ \text{ ou } b \in (p))$$

ce qui revient à dire que $p \in \mathbb{A}$ est premier si, et seulement l'idéal (p) est premier.

4. Si I est un idéal maximal, l'anneau $\dfrac{\mathbb{A}}{I}$ est un corps, donc il est intègre, ce qui revient à dire que I est premier.

5. Si (p) est maximal, il est alors premier, donc p est premier et en conséquence irréductible. □

Un idéal premier n'est pas nécessairement maximal et pour p irréductible dans $\mathbb{A}$ intègre, l'idéal (p) n'est pas nécessairement maximal (exercice 3.9).

3.6 Idéaux maximaux de $\mathcal{C}^0(K,\mathbb{R})$

À titre d'illustration du paragraphe précédent, on s'intéresse aux idéaux maximaux de l'anneau $\mathcal{C}^0(K,\mathbb{R})$ des fonctions continues définies sur un compact K d'un espace métrique (E,d) et à valeurs réelles. Cet anneau n'est pas intègre

en général. Par exemple, pour $f \in \mathcal{C}^0([a,b],\mathbb{R}) \setminus \{0\}$ nulle sur $\left[a, \dfrac{a+b}{2}\right]$ et $g \in \mathcal{C}^0([a,b],\mathbb{R}) \setminus \{0\}$ nulle sur $\left[\dfrac{a+b}{2}, b\right]$, on a $fg = 0$ avec $f \neq 0$ et $g \neq 0$.

On munit $\mathcal{C}^0(K,\mathbb{R})$ de la norme de la convergence uniforme :

$$f \mapsto \|f\|_\infty = \sup_{x \in K} |f(x)|$$

Lemme 3.6 *Tout idéal maximal de $\mathcal{C}^0(K,\mathbb{R})$ est fermé.*

Preuve. Soient I un idéal maximal de $\mathcal{C}^0(K,\mathbb{R})$ et $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions de I qui converge uniformément vers f sur K. Si $f \notin I$, l'idéal $(f)+I$ qui contient strictement I est alors égal à $\mathcal{C}^0(K,\mathbb{R})$ et en conséquence, il contient 1. On a donc $1 = uf + v$ où $(u,v) \in \mathcal{C}^0(K,\mathbb{R}) \times I$ et 1 est limite uniforme de la suite $(g_n)_{n\in\mathbb{N}} = (uf_n + v)_{n\in\mathbb{N}}$ de fonctions de I. Pour n assez grand, on aura alors $\|1 - g_n\|_\infty < 1$ avec $g_n \in I$ qui ne s'annule jamais, mais alors g_n est inversible dans I et $I = \mathcal{C}^0(K,\mathbb{R})$, ce qui n'est pas. On a donc $f \in I$ et I est fermé. □

Théorème 3.6.

Les morphismes d'anneaux de $\mathcal{C}^0(K,\mathbb{R})$ dans $\mathbb{R}$ sont les fonctions d'évaluation $\delta_{x_0} : f \in \mathcal{C}^0(K,\mathbb{R}) \mapsto f(x_0)$ où $x_0 \in K$ est uniquement déterminé.

Preuve. Il est clair que pour tout $x_0 \in K$, l'application δ_{x_0} est un morphisme d'anneaux surjectif de $\mathcal{C}^0(K,\mathbb{R})$ dans $\mathbb{R}$.

Si φ est un morphisme d'anneaux de $\mathcal{C}^0(K,\mathbb{R})$ dans $\mathbb{R}$, en identifiant l'ensemble des fonctions constantes à $\mathbb{R}$, il induit alors un morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$ et on a $\varphi(\lambda) = \lambda$ pour tout réel λ.

Supposons qu'il existe un morphisme d'anneaux $\varphi : \mathcal{C}^0(K,\mathbb{R}) \to \mathbb{R}$ qui ne soit pas de la forme δ_x, ce qui signifie que :

$$\forall x \in K,\ \exists f_x \in \mathcal{C}^0(K,\mathbb{R}),\ \varphi(f_x) \neq f_x(x)$$

En notant $g_x = f_x - \varphi(f_x)$ pour tout $x \in K$, on a $\varphi(g_x) = \varphi(f_x) - \varphi(f_x) = 0$. La fonction g_x étant continue telle que $g_x(x) \neq 0$, il existe un voisinage ouvert $\mathcal{V}_x$ de x dans K sur lequel elle ne s'annule jamais. Du recouvrement ouvert du compact K par les $\mathcal{V}_x$, on peut extraire un sous-recouvrement fini $(\mathcal{V}_{x_k})_{1\leq k\leq n}$ et la fonction $g = \sum_{k=1}^{n} g_{x_k}^2$ est continue sur K à valeurs strictement positives. Cette fonction g est donc inversible dans l'anneau $\mathcal{C}^0(K,\mathbb{R})$ telle que $\varphi(g) = \sum_{k=1}^{n} (\varphi(g_{x_k}))^2 = 0$, ce qui est impossible pour un morphisme d'anneaux unitaires. Il existe donc $x_0 \in K$ tel que $\varphi = \delta_{x_0}$.

Si x_0 et x_1 dans K sont tels que $\delta_{x_0} = \delta_{x_1}$, on a alors $f(x_0) = f(x_1)$ pour tout $f \in \mathcal{C}^0(K,\mathbb{R})$ et pour $f_0 : t \mapsto d(t,x_0)$, on obtient $f_0(x_1) = d(x_1,x_0) = f_0(x_0) = 0$, soit $x_1 = x_0$. En définitive, les δ_{x_0} sont les seuls morphismes d'anneaux unitaires de $\mathcal{C}^0(K,\mathbb{R})$ dans $\mathbb{R}$. □

Lemme 3.7 *Pour tout morphisme d'anneaux* $\varphi : \mathcal{C}^0(K,\mathbb{R}) \to \mathbb{R}$, *l'idéal* $\ker(\varphi)$ *est maximal dans* $\mathcal{C}^0(K,\mathbb{R})$.

Preuve. D'après le théorème précédent, il revient au même de vérifier que pour tout $x \in K$, l'idéal $\ker(\delta_x)$ est maximal dans $\mathcal{C}^0(K,\mathbb{R})$.

Si I est un idéal de $\mathcal{C}^0(K,\mathbb{R})$ qui contient strictement $\ker(\delta_x)$, il existe alors une fonction h dans $I \setminus \ker(\delta_x)$, donc $h(x) = \delta_x(h) \neq 0$ et pour toute fonction f dans $\mathcal{C}^0(K,\mathbb{R})$, la fonction $g = f - \dfrac{f(x)}{h(x)}h$ est dans $\ker(\delta_x)$. Il en résulte que $f = g + \dfrac{f(x)}{h(x)}h \in I$ (c'est un idéal et $g \in \ker(\delta_x) \subset I$). On a donc $I = \mathcal{C}^0(K,\mathbb{R})$.

On peut aussi vérifier que l'anneau quotient $\dfrac{\mathcal{C}^0(K,\mathbb{R})}{\ker(\delta_x)}$ est un corps. Comme δ_x est un morphisme d'anneaux surjectif de $\mathcal{C}^0(K,\mathbb{R})$ dans $\mathbb{R}$, il induit un isomorphisme de $\dfrac{\mathcal{C}^0(K,\mathbb{R})}{\ker(\delta_x)}$ sur $\mathbb{R}$, donc cet anneau quotient est un corps, ce qui revient à dire que l'idéal $\ker(\delta_x)$ est maximal. □

On peut vérifier que pour tout $x \in K$, l'idéal $\ker(\delta_x)$ n'est pas principal (voir l'exercice 3.6).

Théorème 3.7.

Les idéaux maximaux de $\mathcal{C}^0(K,\mathbb{R})$ *sont les* $\ker(\delta_x)$ *où* $x \in K$ *est uniquement déterminé.*

Preuve. On sait déjà que les idéaux $\ker(\delta_x)$ sont maximaux.

Soit I un idéal maximal de $\mathcal{C}^0(K,\mathbb{R})$. L'ensemble :

$$Z(I) = \{x \in K,\ \forall f \in I,\ f(x) = 0\} = \bigcap_{f\in I} f^{-1}(\{0\})$$

est un fermé de K comme intersection de fermés.

Si $Z(I) = \emptyset$, on obtient alors par passage au complémentaire, le recouvrement ouvert $K = \bigcup_{f\in I}\left(K \setminus f^{-1}\{0\}\right)$ du compact K duquel on extrait un sous-recouvrement fini, $K = \bigcup_{k=1}^{p}\left(K \setminus f_k^{-1}\{0\}\right)$ où les f_k, pour k compris entre 1 et p, sont dans I, ce qui nous donne $\bigcap_{k=1}^{p} f_k^{-1}\{0\} = \emptyset$. En utilisant les équivalences :

$$\left(x \in \bigcap_{k=1}^{p} f_k^{-1}\{0\}\right) \Leftrightarrow (f_1(x) = \cdots = f_p(x) = 0) \Leftrightarrow \left(\sum_{k=1}^{n} f_k^2(x) = 0\right)$$

où $f = \sum_{k=1}^{n} f_k^2 \in I$, l'égalité $\bigcap_{k=1}^{p} f_k^{-1}\{0\} = \emptyset$ équivaut à dire que $f(x) \neq 0$ pour tout $x \in K$, donc la fonction $f = \sum_{k=1}^{n} f_k^2$ qui est dans l'idéal I est inversible dans

l'anneau $\mathcal{C}^0(K,\mathbb{R})$, ce qui revient à dire que $I=\mathcal{C}^0(K,\mathbb{R})$, soit une impossibilité pour I maximal.

L'ensemble $Z(I)$ est donc non vide et en prenant $x\in Z(I)$, on a les inclusions $I\subset\ker(\delta_x)\subsetneq\mathcal{C}^0(K,\mathbb{R})$, ce qui implique que $I=\ker(\delta_x)$.

Si pour x,y dans K, on a $\ker(\delta_x)=\ker(\delta_x)$, toute fonction continue nulle en x est nulle en y, c'est donc le cas pour $f_x:t\mapsto d(t,x)$ et on a $f_x(y)=d(y,x)=0$, soit $y=x$. L'application $x\mapsto\ker(\delta_x)$ réalise donc une bijection de K sur l'ensemble des idéaux maximaux de $\mathcal{C}^0(K,\mathbb{R})$. □

Corollaire 3.4. *Les automorphismes de $\mathcal{C}^0(K,\mathbb{R})$ sont les application $f\mapsto f\circ\psi$, où ψ est un homéomorphisme de K.*

Preuve. Il est clair que pour tout homéomorphisme $\psi:K\to K$, l'application $f\mapsto f\circ\psi$ est un automorphisme de $\mathcal{C}^0(K,\mathbb{R})$ d'inverse $f\mapsto f\circ\psi^{-1}$.

Soit φ un automorphisme de $\mathcal{C}^0(K,\mathbb{R})$. Pour tout $x\in K$, l'application $\delta_x\circ\varphi$ est un morphisme d'anneaux de $\mathcal{C}^0(E,\mathbb{R})$ dans $\mathbb{R}$, donc il existe un unique $y\in E$ tel que $\delta_x\circ\varphi=\delta_y$, ce qui permet de définir la fonction $\psi:x\mapsto y$. Les relations $\delta_x\circ\varphi=\delta_{\psi(x)}$ se traduisent par $\varphi(f)(x)=f(\psi(x))$ pour tout $x\in K$ et tout $f\in\mathcal{C}^0(E,\mathbb{R})$, soit par $\varphi(f)=f\circ\psi$ pour tout $f\in\mathcal{C}^0(E,\mathbb{R})$ et il s'agit alors de vérifier que ψ est un homéomorphisme de K.

Si $(x_n)_{n\in\mathbb{N}}$ est une suite d'éléments de K qui converge vers $x\in K$, on a alors pour toute fonction $f\in\mathcal{C}^0(K,\mathbb{R})$:

$$\lim_{n\to+\infty}f(\psi(x_n))=\lim_{n\to+\infty}\varphi(f)(x_n)=\varphi(f)(x)=f(\psi(x))$$

Prenant $f_x:t\mapsto d(t,\psi(x))$, on en déduit que $\lim\limits_{n\to+\infty}d(\psi(x_n),\psi(x))=0$, ce qui signifie que $(\psi(x_n))_{n\in\mathbb{N}}$ converge vers $\psi(x)$. La fonction ψ est donc continue. En remplaçant φ par φ^{-1}, on dispose d'une fonction continue $\tau:K\to K$ telle que $\delta_x\circ\varphi^{-1}=\delta_{\tau(x)}$ pour tout $x\in K$. On a alors, pour tout $x\in K$:

$$\delta_{\psi\circ\tau(x)}=\delta_{\tau(x)}\circ\varphi=\delta_x\circ\varphi^{-1}\circ\varphi=\delta_x$$

et $\delta_{\tau\circ\psi(x)}=\delta_{\psi(x)}\circ\varphi^{-1}=\delta_x\circ\varphi\circ\varphi^{-1}=\delta_x$, donc $\psi\circ\tau(x)=\tau\circ\psi(x)=x$, ce qui signifie que ψ est bijective d'inverse égal à τ qui est continue, c'est donc un homéomorphisme de K. □

3.7 Anneaux factoriels

Définition 3.9. *On dit que l'*anneau $\mathbb{A}$ *est* factoriel *s'il est intègre et si tout élément a non nul et non inversible de $\mathbb{A}$ s'écrit de manière unique comme produit d'éléments irréductibles, ce qui signifie que :*

— *il existe un élément inversible u et des éléments irréductibles $p_1,\cdots,p_r$ tels que $a=u\prod\limits_{k=1}^{r}p_k$;*

— *si on a deux décompositions* $a = u\prod_{k=1}^{r} p_k = v\prod_{k=1}^{s} q_k$, *où* u, v *sont inversibles et* $p_1, \cdots, p_r$, $q_1, \cdots, q_s$ *sont irréductibles, on a alors* $r = s$ *et il existe une permutation* σ *de* $\{1, \cdots, r\}$ *telle que, pour tout* k *compris entre* 1 *et* r, q_k *est associé à* $p_{\sigma(k)}$.

Dans un anneau factoriel, une décomposition en facteurs irréductibles s'écrit aussi $a = u\prod_{k=1}^{m} p_k^{\alpha_k}$, où u est inversible, les p_k sont irréductibles deux à deux non associés et les α_k sont des entiers naturels non nuls. Le nombre $\ell(a) = \sum_{k=1}^{m} \alpha_k$ de facteurs irréductibles qui interviennent dans une telle décomposition est uniquement déterminé par a. Par abus de langage, on dira « la décomposition » de a en facteurs irréductibles.

Théorème 3.8.

L'anneau $\mathbb{A}$ *est factoriel si, et seulement si, il est intègre et :*

1. *toute suite croissante d'idéaux principaux de* $\mathbb{A}$ *est stationnaire ;*
2. *tout élément irréductible de* $\mathbb{A}$ *est premier.*

Preuve. Soit $\mathbb{A}$ un anneau factoriel. Par définition, il est intègre.

Soit $(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \cdots$ une suite croissante d'idéaux principaux de $\mathbb{A}$. S'il existe un entier n_0 tel que a_{n_0} soit inversible, on a alors $(a_{n_0}) = \mathbb{A}$ et comme $(a_{n_0}) \subset (a_n) \subset \mathbb{A}$, pour tout $n \geq n_0$, on a $(a_n) = \mathbb{A}$. La suite est donc stationnaire. En supposant tous les a_n non nuls et non inversibles, on désigne, pour tout $n \in \mathbb{N}$, par $\ell_n = \ell(a_n)$ le nombre de facteurs irréductibles qui interviennent dans la décomposition en facteurs irréductibles de a_n. L'inclusion $(a_n) \subset (a_{n+1})$ revient à dire que a_{n+1} divise a_n et en conséquence $\ell_{n+1} \leq \ell_n$ (par unicité de la décomposition, tous les facteurs irréductibles de a_{n+1} se retrouvent dans ceux de a_n), donc $(\ell_n)_{n\in\mathbb{N}}$ est une suite décroissante d'entiers naturels et nécessairement, elle est stationnaire. Il existe donc un entier n_0 tel que $\ell_n = \ell_{n_0}$ pour tout $n \geq n_0$, donc a_n et a_{n_0} ont exactement les mêmes facteurs irréductibles et ils sont associés, ce qui signifie que $(a_{n_0}) = (a_n)$ pour tout $n \geq n_0$. La suite $((a_n))_{n\in\mathbb{N}}$ est donc stationnaire.

Soit $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$ irréductible divisant ab où a, b sont non nuls. Il existe alors un élément q de $\mathbb{A}$ tel que $ab = pq$. Si a [resp. b] est inversible, on a alors $b = p\left(qa^{-1}\right)$ [resp. $a = p\left(qb^{-1}\right)$] et p divise b [resp. a]. Si a et b sont non inversibles, il en est de même de q (p est irréductible) et utilisant les décompositions en facteurs irréductibles de a, b, q, on a $u\prod_{i=1}^{r} p_i \prod_{j=1}^{s} q_j = p\prod_{k=1}^{m} r_k$ où $u \in \mathbb{A}^\times$ et les p_i, q_j, r_k sont irréductibles. De l'unicité de cette décomposition, on déduit que p est associé à un p_i ou un q_j et en conséquence, il divise u ou v. En définitive p est premier.

Réciproquement, supposons que $\mathbb{A}$ soit intègre et que les deux propriétés de l'énoncé du théorème soient vérifiées. On se donne $a \in \mathbb{A}^* \setminus \mathbb{A}^\times$. On montre tout

d'abord que a admet un diviseur irréductible. Si ce n'est pas le cas, on peut alors construire une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{A}$ telle que :

$$\begin{cases} a_0 = a \in \mathbb{A}^* \setminus \mathbb{A}^\times \\ \forall n \in \mathbb{N},\ a_n \in \mathbb{A}^* \setminus \mathbb{A}^\times,\ a_{n+1} \text{ n'est pas associé à } a_n \text{ et } a_{n+1} \text{ divise } a_n \end{cases}$$

Pour ce faire, on procède par récurrence. On pose $a_0 = a \in \mathbb{A}^* \setminus \mathbb{A}^\times$. Supposons construit une suite $(a_k)_{0\leq k\leq n}$ d'éléments de $\mathbb{A}^*\setminus\mathbb{A}^\times$, telle que, pour tout k compris entre 0 et $n-1$, a_{k+1} n'est pas associé à a_k et a_{k+1} divise a_k. Comme a_n divise $a_0 = a$ qui n'admet pas de diviseur irréductible, a_n est réductible et il s'écrit $a_n = a_{n+1}b_{n+1}$ avec a_{n+1} et b_{n+1} dans $\mathbb{A}^* \setminus \mathbb{A}^\times$, donc a_{n+1} est un diviseur de a_n non associé à a_n. Mais une telle construction nous donne une suite strictement croissante $((a_n))_{n\in\mathbb{N}}$ d'idéaux principaux de $\mathbb{A}$, ce qui contredit le premier point. On en déduit alors l'existence d'une décomposition de a en facteurs irréductibles. Pour ce faire on construit des diviseurs irréductibles de a comme suit :

— si a est irréductible, on pose $p_1 = a$ et c'est terminé ;

— supposant construits, pour $n \geq 1$, des diviseurs irréductibles $p_1, \cdots, p_n$ de a, si $a_n = \dfrac{a}{p_1 \cdot \cdots \cdot p_n}$ est inversible c'est terminé, sinon p_{n+1} est un diviseur irréductible de a_n.

Un tel algorithme s'arrête nécessairement au bout d'un nombre fini d'étapes. En effet, dans le cas contraire on dispose d'une suite infinie $(a_n)_{n\in\mathbb{N}^*}$ d'éléments de $\mathbb{A}$ telle que $a_{n+1} = \dfrac{a}{p_1 \cdot \cdots \cdot p_{n+1}} = \dfrac{a_n}{p_{n+1}}$, soit $a_n = p_{n+1}a_{n+1}$ multiple de a_{n+1} non associé à a_n, donc $((a_n))_{n\in\mathbb{N}^*}$ est une suite strictement croissante d'idéaux principaux de $\mathbb{A}$, ce qui contredit le premier point. Il existe donc un entier $n \geq 1$ tel que $a_n = \dfrac{a}{p_1 \cdot \cdots \cdot p_n} \in \mathbb{A}^\times$ et $a = a_n \displaystyle\prod_{k=1}^{n} p_k$ est une décomposition de a en facteurs irréductibles.

Il nous reste à montrer l'unicité d'une telle décomposition. Supposons que l'on ait $a = u\displaystyle\prod_{k=1}^{r} p_k = v\prod_{j=1}^{s} q_j$, où $s \geq r \geq 1$, u, v sont inversibles et les p_k, q_j sont irréductibles. On vérifie par récurrence sur $r \geq 1$ que $s = r$ et qu'il existe une permutation σ de $\{1, \cdots, r\}$ telle que, pour tout k compris entre 1 et r, q_k est associé à $p_{\sigma(k)}$. Pour $r = 1$, on a $up_1 = v\displaystyle\prod_{j=1}^{s} q_j$, donc p_1 qui est irréductible et en conséquence premier (deuxième condition) va diviser l'un des q_j et quitte à modifier la numérotation, on peut supposer que p_1 divise q_1, ce qui signifie qu'il est associé à q_1 (ces deux éléments sont irréductibles), soit $q_1 = u_1p_1$ et dans l'anneau intègre $\mathbb{A}$, on en déduit, dans le cas où $s \geq 2$, que $\displaystyle\prod_{j=2}^{s} q_j \in \mathbb{A}^\times$, ce qui contredit l'irréductibilité des q_j. On a donc $s = 1$. Supposant le résultat acquis pour $r \geq 1$, deux décompositions $a = u\displaystyle\prod_{k=1}^{r+1} p_k = v\prod_{j=1}^{s} q_j$ avec $s \geq r+1$ entraînent que p_{r+1} est associé à l'un des q_j, disons q_s (en modifiant la numérotation si nécessaire),

donc $u\prod_{k=1}^{r} p_k = w\prod_{j=1}^{s-1} q_j$ avec w inversible et l'hypothèse de récurrence permet de conclure. □

Corollaire 3.5. (Euclide) *Dans un anneau factoriel, un élément est irréductible si, et seulement si, il est premier.*

Le corollaire précédent nous dit que dans un anneau factoriel, si p irréductible divise un produit $\prod_{k=1}^{r} a_k$, il divise alors l'un des a_k.

Exemple 3.2 *Les anneaux $\mathbb{Z}\left[i\sqrt{n}\right]$ ne sont pas factoriels pour $n \geq 3$, puisque 2 est irréductible non premier dans un tel anneau (voir l'exercice 3.2).*

3.8 Exercices

Exercice 3.1.

1. *Montrer que $\mathbb{A}$ est un corps si, et seulement si, les seuls idéaux de $\mathbb{A}$ sont $\{0\}$ et $\mathbb{A}$.*
2. *Montrer que $\mathbb{A}$ est un corps si, et seulement si, il est intègre avec un nombre fini d'idéaux.*
3. *Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif. Montrer qu'un morphisme d'anneaux φ de $\mathbb{K}$ dans un anneau $\mathbb{B}$ est nécessairement injectif.*

Solution.

1. Si $\mathbb{A}$ est un corps et I est un idéal de $\mathbb{A}$ non réduit à $\{0\}$, tout élément non nul de I est inversible, donc $I = \mathbb{A}$. Réciproquement si $\{0\}$ et $\mathbb{A}$ sont les seuls idéaux de $\mathbb{A}$, on a alors $(a) = \mathbb{A}$ pour tout $a \in \mathbb{A}^*$, donc $1 \in (a)$ et il existe $q \in \mathbb{A}$ tel que $1 = qa$, ce qui signifie que a est inversible. On a donc $\mathbb{A}^* = \mathbb{A}^\times$ et $\mathbb{A}$ est un corps.
2. Si $\mathbb{A}$ est un corps, il est alors intègre avec deux d'idéaux, $\{0\}$ et $\mathbb{A}$. Réciproquement, si $\mathbb{A}$ est intègre avec un nombre fini d'idéaux, pour tout $a \in \mathbb{A}^*$ la famille d'idéaux $\left((a^n)\right)_{n\in\mathbb{N}}$ est alors finie et il existe deux entiers $m > n \geq 0$ tels que $(a^n) = (a^m)$, ce qui revient à dire que a^n et a^m sont associés, soit qu'il existe une unité $u \in \mathbb{A}^\times$ tel que $a^n = ua^m$ et comme $\mathbb{A}$ est intègre, il en résulte que $ua^{m-n} = 1$ et a est inversible d'inverse ua^{m-n-1}. L'anneau $\mathbb{A}$ est donc un corps.
3. Comme $\varphi(1_\mathbb{K}) = 1_\mathbb{B}$, le noyau de φ est un idéal strict de $\mathbb{K}$, il est donc réduit à $\{0_\mathbb{K}\}$ et φ est injective.

Exercice 3.2. *On se donne $n \in \mathbb{N}^*$ et on note :*

$$\mathbb{Z}\left[i\sqrt{n}\right] = \left\{P\left(i\sqrt{n}\right),\ P \in \mathbb{Z}[X]\right\}$$

1. *Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe et que $\mathbb{Z}[i\sqrt{n}] = \left\{a + ib\sqrt{n},\ (a,b) \in \mathbb{Z}^2\right\}$.*
2. *Déterminer l'ensemble des éléments inversibles de $\mathbb{Z}[i\sqrt{n}]$.*
3. *Quels sont les entiers naturels $p \geq 2$ qui sont premiers dans $\mathbb{N}$ et réductibles dans $\mathbb{Z}[i\sqrt{n}]$?*
4. *Montrer que pour $n \geq 3$, 2 est irréductible et non premier dans $\mathbb{Z}[i\sqrt{n}]$.*

Solution.

1. L'application d'évaluation $\varphi : P \in \mathbb{Z}[X] \mapsto P(i\sqrt{n}) \in \mathbb{C}$ étant un morphisme d'anneaux, son image $\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$ (c'est le plus petit sous-anneau de $\mathbb{C}$ qui contient $\mathbb{Z}$ et $i\sqrt{n}$). Pour tout $P \in \mathbb{Z}[X]$, on a $\overline{P(i\sqrt{n})} = Q(i\sqrt{n})$ où $Q(X) = P(-X) \in \mathbb{Z}[X]$, donc $\mathbb{Z}[i\sqrt{n}]$ est stable par conjugaison complexe. En effectuant la division euclidienne dans $\mathbb{Z}[X]$ par le polynôme unitaire X^2+n (théorème **??**), tout polynôme $P \in \mathbb{Z}[X]$ s'écrit sous la forme $P(X) = Q(X)\left(X^2+n\right) + aX + b$ où $(a,b) \in \mathbb{Z}^2$, ce qui implique que $P(i\sqrt{n}) = a + ib\sqrt{n}$. On a donc $\mathbb{Z}[i\sqrt{n}] = \left\{a + ib\sqrt{n},\ (a,b) \in \mathbb{Z}^2\right\}$ et cet anneau est isomorphe à l'anneau quotient $\dfrac{\mathbb{Z}[X]}{\ker(\varphi)} = \dfrac{\mathbb{Z}[X]}{(X^2+n)}$.
2. Si $u = a + ib\sqrt{n}$ est inversible dans $\mathbb{Z}[i\sqrt{n}]$, il existe alors $v \in \mathbb{Z}[i\sqrt{n}]$ tel que $uv = 1$ et on a $|u|^2|v|^2 = 1$ dans $\mathbb{N}$, ce qui impose $|u|^2 = |v|^2 = 1$. Réciproquement, si $u \in \mathbb{Z}[i\sqrt{n}]$ est tel que $|u|^2 = u\overline{u} = 1$, comme $\overline{u} \in \mathbb{Z}[i\sqrt{n}]$, cet élément u est inversible dans $\mathbb{Z}[i\sqrt{n}]$. On a donc pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}[i\sqrt{n}]^\times = \{u \in \mathbb{Z}[i\sqrt{n}],\ |u| = 1\}$. Pour $n = 1$ et $u = a + ib$ inversible dans $\mathbb{Z}[i]$, on a $a^2 + b^2 = 1$ avec $\left(a^2, b^2\right) \in \mathbb{N}^2$, ce qui équivaut à $\left(a^2, b^2\right) = (1,0)$ ou $\left(a^2, b^2\right) = (0,1)$ ou encore à $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$. On a donc $\mathbb{Z}[i]^\times \subset \{-1, 1, -i, i\}$, l'inclusion réciproque se vérifiant facilement. Pour $n \geq 2$ et $u = a + ib\sqrt{n}$ inversible dans $\mathbb{Z}[i\sqrt{n}]$ on a $a^2 + nb^2 = 1$ avec $\left(a^2, b^2\right) \in \mathbb{N}^2$, ce qui équivaut à $b = 0$ et $a = \pm 1$. On a donc pour $n \geq 2$, $\mathbb{Z}[i\sqrt{n}]^\times \subset \{-1, 1\}$, l'inclusion réciproque étant vérifiée pour tout anneau unitaire.
3. Si $p \geq 2$ est un entier naturel premier dans $\mathbb{N}$ et réductible dans $\mathbb{Z}[i\sqrt{n}]$, il s'écrit alors $p = uv$ avec u, v non inversibles dans $\mathbb{Z}[i\sqrt{n}]$ et on a $p^2 = |u|^2|v|^2$ dans $\mathbb{N}$ avec $|u|^2 \neq 1$ et $|v|^2 \neq 1$, ce qui impose $|u|^2 = |v|^2 = p$ puisque p est premier dans $\mathbb{N}$. L'entier p est donc de la forme $p = a^2 + nb^2$. Réciproquement si p est premier dans $\mathbb{N}$ de la forme $p = a^2 + nb^2$, il s'écrit $p = u\overline{u}$ où $u = a + ib\sqrt{n}$ et $\overline{u} = a - ib\sqrt{n}$ sont non inversibles (puisque $|u|^2 = |\overline{u}|^2 = p \geq 2$) donc p est réductible dans $\mathbb{Z}[i\sqrt{n}]$.
4. Pour $n \geq 3$, l'égalité $a^2 + nb^2 = 2$ impose $b = 0$ et $a^2 = 2$ avec a entier, ce qui est impossible, donc 2 est irréductible dans $\mathbb{Z}[i\sqrt{n}]$. Pour $n = 2$, $2 = \left(i\sqrt{2}\right)\left(-i\sqrt{2}\right)$ est réductible et non premier. Pour $n \geq 3$ entier impair, 2 divise $(1 + i\sqrt{n})(1 - i\sqrt{n}) = 1 + n$ et ne divise pas $1 \pm i\sqrt{n}$, donc il est non premier.

Pour $n \geq 4$ pair, 2 divise $(2+i\sqrt{n})(2-i\sqrt{n}) = 4+n$ et ne divise pas $2 \pm i\sqrt{n}$, donc il est non premier.

Exercice 3.3. *Soit E un $\mathbb{K}$-espace vectoriel.*

1. *Montrer que la restriction de $u \in \mathcal{L}(E)$ à tout supplémentaire H de $\ker(u)$ dans E réalise un isomorphisme de H sur $\mathrm{Im}(u)$.*
2. *Dans le cas où E est de dimension finie $n \geq 1$, montrer que deux endomorphismes u et v de même rang r dans $\mathcal{L}(E)$ sont équivalents. Ce résultat peut être utilisé pour démontrer le théorème 3.1 qui décrit les idéaux bilatères de $\mathcal{L}(E)$ pour E de dimension finie.*

Solution.

1. Soient $u \in \mathcal{L}(E)$ et H un supplémentaire de $\ker(u)$ dans E. Tout $y \in \mathrm{Im}(u)$ s'écrit $y = u(x)$ avec $x = x_1 + x_2$, où $(x_1, x_2) \in H \times \ker(u)$, donc $y = u(x_1)$ et $u_{|H}$ est surjectif. Si $x \in \ker\left(u_{|H}\right)$, on a alors $x \in H \cap \ker(u) = \{0\}$, donc $x = 0$ et $u_{|H}$ est injectif.
2. Soient u et v dans $\mathcal{L}(E)$ de même rang r. Pour $r = 0$, on a $u = v = 0$. Pour $r = n$, ces endomorphismes sont des isomorphismes, donc pour toute base $(e_j)_{1\leq j<n}$, les familles $(u(e_j))_{1\leq j<n}$ et $(v(e_j))_{1\leq j<n}$ sont aussi des bases de E et désignant par φ l'isomorphisme de E défini par $\varphi(u(e_j)) = v(e_j)$ pour tout j compris entre 1 et n, on a $v = \varphi \circ u$. Pour $1 \leq r \leq n-1$, on a $E = H \oplus \ker(u) = K \oplus \ker(v)$ avec $\dim(H) = \dim(K) = r$. On désigne par $(e_j)_{1\leq j<r}$ une base de H [resp. par $\left(e'_j\right)_{1\leq j<r}$ une base de K] que l'on complète par une base $(e_j)_{r+1\leq j\leq n}$ de $\ker(u)$ [resp. par une base $\left(e'_j\right)_{r+1\leq j<n}$ de $\ker(v)$]. On vérifie alors que la famille de vecteurs $(f_j)_{1\leq j<r} = (u(e_j))_{1\leq j<r}$ [resp. que la famille $\left(f'_j\right)_{1\leq j<r} = \left(v\left(e'_j\right)\right)_{1\leq j<r}$] est libre dans E. En effet, si $0 = \sum_{j=1}^{r} \lambda_j u(e_j) = u\left(\sum_{j=1}^{r} \lambda_j e_j\right)$, on a alors $\sum_{j=1}^{r} \lambda_j e_j \in H \cap \ker(u) = \{0\}$, donc $\sum_{j=1}^{r} \lambda_j e_j = 0$ et tous les λ_j sont nuls. On peut donc la compléter en une base $(f_j)_{1\leq j<n}$ [resp. en une base $\left(f'_j\right)_{1\leq j<n}$] de E. Définissant φ et ψ dans $\mathrm{GL}(E)$ par $\varphi(f_j) = f'_j$ et $\psi(e_j) = e'_j$ pour tout j compris entre 1 et n, on a :

$$\varphi(u(e_j)) = \varphi(f_j) = f'_j = v\left(e'_j\right) = v(\psi(e_j)) \ (1 \leq j \leq r)$$

et :

$$\varphi(u(e_j)) = \varphi(0) = 0 = v\left(e'_j\right) = v(\psi(e_j)) \ (r+1 \leq j \leq n)$$

soit $\varphi \circ u = v \circ \psi$, ou encore $v = \varphi \circ u \circ \psi^{-1}$. Tout cela peut se résumer en disant que, dans deux bases adaptées de E, la matrice de $v \in \mathcal{L}(E)$ de rang r est $A_r = \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$.

Exercice 3.4. *Soit E un $\mathbb{R}$-espace vectoriel de dimension $n \geq 2$. Montrer que si p est une semi-norme non nulle sur $\mathcal{L}(E)$ telle que $p(u \circ v) \leq p(u)\, p(v)$ pour tous u, v dans $\mathcal{L}(E)$ (on dit que p est sous-multiplicative), c'est alors une norme.*

Solution. $I = \{u \in \mathcal{L}(E),\ p(u) = 0\}$ est un idéal bilatère de $\mathcal{L}(E)$ différent de $\mathcal{L}(E)$, c'est donc $\{0\}$ (on a $p(0) = 0$ car $p(\lambda u) = |\lambda|\, p(u)$, $p(u - v) \leq p(u) + p(v)$, donc I est un sous-groupe additif de $\mathcal{L}(E)$, de $p(u \circ v) \leq p(u)\, p(v)$ on déduit que I est un idéal bilatère et de $p \neq 0$, que $I \neq \mathcal{L}(E)$).

Exercice 3.5. *Soit E un $\mathbb{K}$-espace vectoriel de dimension infinie.*

1. *Montrer que $I_0 = \{u \in \mathcal{L}(E),\ \mathrm{rg}(u)$ est fini$\}$ est un idéal bilatère non trivial de $\mathcal{L}(E)$, puis que tout idéal bilatère non réduit à $\{0\}$ de $\mathcal{L}(E)$ contient I_0.*
2. *On suppose que E est de dimension infinie dénombrable. Montrer que I_0 est l'unique idéal bilatère non trivial de $\mathcal{L}(E)$.*
3. *Dans le cas où E est de dimension infinie non dénombrable, donner un exemple d'idéal bilatère non trivial de $\mathcal{L}(E)$ qui contient strictement I_0.*

Solution.

1. Avec $0 \in I_0$ et $\mathrm{Im}(u - v) \subset \mathrm{Im}(u) + \mathrm{Im}(v)$, on déduit que I_0 est un sous-groupe additif de $\mathcal{L}(E)$. Pour $u \in I_0$ et $v \in \mathcal{L}(E)$ on a $u \circ v \in I_0$ puisque $\mathrm{Im}(u \circ v) \subset \mathrm{Im}(u)$ et $v \circ u \in I_0$ puisque pour toute base $(u(x_k))_{1 \leq k \leq r}$ de $\mathrm{Im}(u)$, $(v(u(x_k)))_{1 \leq k \leq r}$ est un système générateur de $\mathrm{Im}(v \circ u)$ (pour $u = 0$, on a $v \circ u = 0$). On a $I_0 \neq \{0\}$ puisqu'il contient toute projection sur une droite et $I_0 \neq \mathcal{L}(E)$ puisque l'identité n'est pas dans I_0. Soient $J \neq \{0\}$ un idéal bilatère de $\mathcal{L}(E)$ et $u \in I_0$. Si $u = 0$, il est alors dans J. Supposons $u \neq 0$ et soit H un supplémentaire de $\ker(u)$ dans E. Comme u est de rang fini, H qui est isomorphe à $\mathrm{Im}(u)$ est de dimension finie. Soit $(e_j)_{1 \leq j \leq r}$ une base de H que l'on complète par une base $(e_k)_{k \in K}$ de $\ker(u)$. On se donne $v \in J \setminus \{0\}$ et $y = v(x) \in E \setminus \{0\}$ (ce qui est possible puisque $v \neq 0$) et on définit les familles $(u_j)_{1 \leq j \leq r}$ et $(v_j)_{1 \leq j \leq r}$ dans $\mathcal{L}(E)$ par :

$$u_j(e_k) = \begin{cases} x \text{ si } k = j \in \{1, \cdots, r\} \\ 0 \text{ si } k \neq j,\ k \in \{1, \cdots, r\} \cup K \end{cases}$$

et :

$$\begin{cases} v_j(y) = e_j \\ v_j(z) = 0 \text{ pour } z \text{ dans un supplémentaire de } \mathbb{K}y \end{cases}$$

On a alors $v_j \circ v \circ u_j(e_j) = v_j \circ v(x) = v_j(y) = e_j$ pour $1 \leq j \leq r$ et pour $k \neq j$ dans $\{1, \cdots, r\} \cup K$, $v_j \circ v \circ u_j(e_k) = 0$, donc :

$$u(e_j) = u \circ v_j \circ v \circ u_j(e_j) = \left(\sum_{i=1}^{r} u \circ v_i \circ v \circ u_i \right)(e_j)$$

pour $1 \leq j \leq r$ et $0 = u(e_k) = \left(\sum_{i=1}^{r} u \circ v_i \circ v \circ u_i\right)(e_k)$ pour $k \in K$. En définitive, on a $u = \sum_{i=1}^{r} u \circ v_i \circ v \circ u_i \in J$ et $I_0 \subset J$. En conclusion, I_0 est le plus petit idéal bilatère non trivial de $\mathcal{L}(E)$.

2. Soit J un idéal bilatère de $\mathcal{L}(E)$ qui contient strictement I_0 et $u \in J \setminus I_0$. Cet endomorphisme u est de rang infini dénombrable et $\mathrm{Im}(u)$ est isomorphe à E (si $(e_j)_{j\in\mathbb{N}}$ est une base de E et $(e'_j)_{j\in\mathbb{N}}$ une base de $\mathrm{Im}(u)$, l'application linéaire φ définie par $\varphi(e_j) = e'_j$ pour tout $j \in \mathbb{N}$ réalise alors un isomorphisme de E sur $\mathrm{Im}(u)$). On peut donc écrire que $E = \ker(u) \oplus H = K \oplus \mathrm{Im}(u)$ et on dispose d'isomorphismes $\varphi : \mathrm{Im}(u) \to E$, $v : H \to \mathrm{Im}(u)$, $w = v^{-1} \circ \varphi^{-1} : E \to H$. L'endomorphisme $\psi = \varphi \circ u \circ w$ est alors dans J et c'est un automorphisme. En effet si $\varphi \circ u \circ w(x) = 0$, on a alors $u(w(x)) = 0$, soit $w(x) \in H \cap \ker(u)$, donc $w(x) = 0$ et $x = 0$. Pour $y \in E$, on a $\varphi^{-1}(y) \in \mathrm{Im}(u)$, donc $\varphi^{-1}(y) = u(z)$ avec $z = z_1 + z_2$, où $(z_1, z_2) \in \ker(u) \times H$, ce qui nous donne $\varphi^{-1}(y) = u(z_2)$ avec $z_2 = w(x)$, soit $\varphi^{-1}(y) = u(w(x))$ et $y = \varphi \circ u \circ w(x)$. En conclusion, $\varphi \circ u \circ w \in J \cap \mathrm{GL}(E)$ et $J = \mathcal{L}(E)$.

3. Dans le cas où E est de dimension infinie non dénombrable, l'ensemble :

$$I_0 = \{u \in \mathcal{L}(E),\ \mathrm{rg}(u) \text{ est fini ou infini dénombrable}\}$$

est un idéal bilatère non trivial de $\mathcal{L}(E)$ qui contient strictement I_0.

Exercice 3.6. *Soit K un compact d'un espace métrique (E, d).*

1. *Montrer que pour tout morphisme d'anneaux $\varphi : \mathcal{C}^0(K, \mathbb{R}) \to \mathbb{R}$, l'idéal $\ker(\varphi)$ n'est pas principal.*
2. *Soit φ un automorphisme de l'anneau $\mathcal{C}^0(K, \mathbb{R})$. Montrer que l'image par φ d'un idéal maximal de $\mathcal{C}^0(K, \mathbb{R})$ est un idéal maximal.*

Solution.

1. D'après le théorème 3.6, il revient au même de vérifier que pour tout $x \in K$, l'idéal $\ker(\delta_x)$ n'est pas principal. Si pour $x \in K$, l'idéal $\ker(\delta_x)$ est principal, il existe alors une fonction $f \in \mathcal{C}^0(K, \mathbb{R})$ nulle en x telle que $\ker(\delta_x) = (f)$. La fonction $\sqrt{|f|}$ étant dans $\ker(\delta_x)$, il existe une fonction $g \in \mathcal{C}^0(K, \mathbb{R})$ telle que $\sqrt{|f|} = fg$, ce qui nous donne $|f| = f^2 g^2$, soit $|f|\left(1 - |f| g^2\right) = 0$ et f est nulle sur une boule ouverte $B(x, \alpha)$ (avec $\alpha > 0$) puisque $1 - |f| g^2$ vaut 1 en x, ce qui implique que toutes les fonctions de $\ker(\delta_x)$ sont nulles sur $B(x, \alpha)$. Considérant la fonction $f_x : t \mapsto d(t, x)$ qui est dans $\ker(\delta_x)$, on aboutit à une contradiction puisque f_x s'annule uniquement en x.
2. Soit I un idéal maximal de $\mathcal{C}^0(K, \mathbb{R})$. Comme φ est surjectif, $\varphi(I)$ est un idéal de $\mathcal{C}^0(K, \mathbb{R})$ ($\varphi(I)$ est un sous-groupe de $\mathcal{C}^0(K, \mathbb{R})$ et pour $\varphi(f) \in \varphi(I)$ et $h \in \mathcal{C}^0(K, \mathbb{R})$, dans le cas où φ est surjective, il existe $g \in \mathcal{C}^0(K, \mathbb{R})$ tel que $h = \varphi(g)$ et $\varphi(f) \cdot h = \varphi(fg) \in \varphi(I)$). Si J est un idéal de $\mathcal{C}^0(K, \mathbb{R})$ qui contient strictement $\varphi(I)$, $\varphi^{-1}(J)$ est alors un idéal de $\mathcal{C}^0(K, \mathbb{R})$ qui contient

strictement I (φ est un automorphisme de $\mathcal{C}^0(K,\mathbb{R})$), donc $\varphi^{-1}(J)=\mathcal{C}^0(K,\mathbb{R})$ et $J=\mathcal{C}^0(K,\mathbb{R})$.

Exercice 3.7. *On se donne un espace métrique (E,d) et $\mathcal{C}^0(E,\mathbb{R})$ est l'anneau des fonctions continues de E dans $\mathbb{R}$. Pour tout idéal I de $\mathcal{C}^0(E,\mathbb{R})$, on note $Z(I)=\{x\in E,\ \forall f\in I,\ f(x)=0\}$.*

1. *Montrer que les fermés de E, sont les ensembles $Z(I)$.*
2. *On suppose que $I=(f_1,\cdots,f_p)$ est un idéal de type fini de $\mathcal{C}^0(E,\mathbb{R})$. Montrer que $Z(I)=\emptyset$ si, et seulement si, $I=\mathcal{C}^0(E,\mathbb{R})$.*
3. *On suppose que l'espace métrique E est compact et on se donne un idéal I de $\mathcal{C}^0(E,\mathbb{R})$. Montrer que $Z(I)=\emptyset$ si, et seulement si, $I=\mathcal{C}^0(E,\mathbb{R})$.*
4. *Réciproquement, montrer que si $Z(I)\neq\emptyset$ pour tout idéal propre I de $\mathcal{C}^0(E,\mathbb{R})$ (*i. e. *$I\neq\mathcal{C}^0(E,\mathbb{R})$), l'espace métrique E est alors compact.*

Solution.

1. Pour toute fonction $f\in\mathcal{C}^0(E,\mathbb{R})$ l'ensemble $f^{-1}\{0\}$ est un fermé de E comme image réciproque du fermé $\{0\}$ de $\mathbb{R}$ par la fonction continue f, donc pour tout idéal I de $\mathcal{C}^0(E,\mathbb{R})$, l'ensemble $Z(I)=\bigcap_{f\in I}f^{-1}\{0\}$ est fermé dans E comme intersection de fermés. Réciproquement, soit $\mathcal{F}$ un fermé de E. Si $\mathcal{F}=E$, on a alors $\mathcal{F}=Z(\{0\})$. Sinon, le complémentaire $\mathcal{O}=E\setminus\mathcal{F}$ est un ouvert non vide E et pour tout $x\in\mathcal{O}$, il existe un réel $r_x>0$ tel que la boule ouverte $B(x,r_x)$ de centre x et de rayon r_x soient contenue dans $\mathcal{O}$. Pour tout $x\in E$, la fonction $f_x:t\mapsto f_x(t)=\max(0,r_x-d(t,x))$ est continue sur E (en utilisant l'inégalité triangulaire pour la distance d, on vérifie que la fonction $t\mapsto d(t,x)$ est continue et pour u,v continues, $\max(u,v)=\dfrac{u+v}{2}+\dfrac{|v-u|}{2}$ est continue), puis avec :
$$\mathcal{F}=E\setminus\mathcal{O}=E\setminus\left(\bigcup_{x\in\mathcal{O}}B(x,r_x)\right)=\bigcap_{x\in\mathcal{O}}(E\setminus B(x,r_x))$$
on déduit que :
$$(t\in\mathcal{F})\Leftrightarrow(\forall x\in\mathcal{O},\ \|t-x\|\geq r_x)\Leftrightarrow(\forall x\in\mathcal{O},\ f_x(t)=0)$$
soit $\mathcal{F}=\bigcap_{x\in\mathcal{O}}f_x^{-1}\{0\}=Z(I)$ où I est l'idéal engendré par les f_x, x décrivant l'ouvert $\mathcal{O}$, soit $I=\left\{\sum_{x\in J}u_xf_x \text{ où } J\subset\mathcal{O} \text{ est fini et } u_x\in\mathcal{C}^0(E,\mathbb{R})\right\}$.
2. Si $I=\mathcal{C}^0(E,\mathbb{R})$ (qui est bien de type fini engendré par la fonction constante égale à 1), il contient alors les constantes non nulles et on a $Z(I)=\emptyset$. Pour

$I = \left\{ \sum_{k=1}^{p} u_k f_k,\ (u_i)_{1\leq i\leq p} \in \left(\mathcal{C}^0(K,\mathbb{R})\right)^p \right\}$, on a $Z(I) = \bigcap_{k=1}^{p} f_k^{-1}\{0\}$, soit :

$$(x \in Z(I)) \Leftrightarrow (f_1(x) = \cdots = f_p(x) = 0) \Leftrightarrow \left(\sum_{k=1}^{n} f_k^2(x) = 0\right)$$

où $f = \sum_{k=1}^{n} f_k^2 \in I$. Dire que $Z(I) = \emptyset$ équivaut donc à dire que $f(x) \neq 0$ pour tout $x \in E$, donc la fonction $f = \sum_{k=1}^{n} f_k^2$ qui est dans l'idéal I est inversible dans l'anneau $\mathcal{C}^0(K,\mathbb{R})$, ce qui revient à dire que $I = \mathcal{C}^0(K,\mathbb{R})$.

3. La condition suffisante est déjà traitée. Si $Z(I) = \emptyset$, on a alors :

$$Z(I) = \bigcap_{f\in I} f^{-1}\{0\} = \emptyset$$

et en passant au complémentaire, on obtient le recouvrement ouvert du compact E, $E = \bigcup_{f\in I} \left(E \setminus f^{-1}\{0\}\right)$ duquel on peut extraire un sous-recouvrement fini, $E = \bigcup_{k=1}^{p} \left(E \setminus f_k^{-1}\{0\}\right)$ où les f_k pour $1 \leq k \leq p$ sont dans I, ce qui nous donne $Z(f_1,\cdots,f_p) = \bigcap_{k=1}^{p} f_k^{-1}\{0\} = \emptyset$ qui équivaut à $(f_1,\cdots,f_p) = \mathcal{C}^0(E,\mathbb{R})$ et impose $I = \mathcal{C}^0(E,\mathbb{R})$.

4. Réciproquement, on suppose que $Z(I)$ est non vide pour tout idéal propre de $\mathcal{C}^0(E,\mathbb{R})$. Soit $E = \bigcup_{j\in J} \mathcal{O}_j$ un recouvrement ouvert de E. Chaque fermé $\mathcal{F}_j = E \setminus \mathcal{O}_j$ s'écrit $\mathcal{F}_j = Z(I_j)$, où I_j est un idéal de $\mathcal{C}^0(E,\mathbb{R})$ et en désignant par I l'idéal engendré par $\bigcup_{j\in J} I_j$ (*i. e.* $I = \left\{ \sum_{\text{finie}} f_j,\ \text{où } f_j \in I_j \right\}$), on a $Z(I) = \bigcap_{j\in J} Z(I_j) = \bigcap_{j\in J} (E \setminus \mathcal{O}_j) = \emptyset$, donc $I = \mathcal{C}^0(E,\mathbb{R})$ et il existe des indices $j_j,\cdots,j_p$ dans J tels que $1 = \sum_{k=1}^{k} f_k$, où $f_k \in I_{j_k}$. Il en résulte que $Z(f_1,\cdots,f_p) = \bigcap_{k=1}^{p} f_k^{-1}\{0\} = \emptyset$ et comme $\bigcap_{k=1}^{p} Z(I_{j_k})$ est contenu dans $\bigcap_{k=1}^{p} f_k^{-1}\{0\}$, on a $\bigcap_{k=1}^{p} Z(I_{j_k}) = \emptyset$ et $\bigcup_{k=1}^{p} (E \setminus Z(I_{j_k})) = \bigcup_{k=1}^{p} (E \setminus \mathcal{F}_{j_k}) = \bigcup_{k=1}^{p} \mathcal{O}_{j_k}$, ce qui nous donne un recouvrement ouvert fini de E. L'espace métrique E est donc compact.

Exercice 3.8.

1. *Montrer que* $\mathrm{Nil}(\mathbb{A}) = \{a \in \mathbb{A},\ \exists n \in \mathbb{N}^*\ ;\ a^n = 0\}$ *est un idéal de* $\mathbb{A}$. *Les éléments de* $\mathrm{Nil}(\mathbb{A})$ *sont dits nilpotents et* $\mathrm{Nil}(\mathbb{A})$ *est le nilradical de* $\mathbb{A}$.
2. *Montrer que la somme d'un élément nilpotent et d'un élément inversible est inversible dans* $\mathbb{A}$.
3. *Que vaut* $\mathrm{Nil}\left(\dfrac{\mathbb{A}}{\mathrm{Nil}(\mathbb{A})}\right)$ *?*
4. *Soit* $n \geq 2$ *un entier naturel. Quels sont les éléments nilpotents de* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *?*
5. *Montrer que pour tout idéal* I *de* $\mathbb{A}$, $\sqrt{I} = \{a \in \mathbb{A},\ \exists n \in \mathbb{N}\ ;\ a^n \in I\}$ *est un idéal de* $\mathbb{A}$ *qui contient* I. *On dit que* $\sqrt{I}$ *est le radical de* I.
6. *Que vaut* $\sqrt{\{0\}}$ *?*
7. *Montrer que* $\sqrt{\sqrt{I}} = \sqrt{I}$ *et* $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ *pour* I, J *idéaux de* $\mathbb{A}$.
8. *Soit* $p \geq 2$ *un nombre premier. Que vaut* $\sqrt{p\mathbb{Z}}$ *?*
9. *Soit* $n \geq 2$ *un entier. Que vaut* $\sqrt{n\mathbb{Z}}$ *?*

Solution.

1. Comme $0 \in \mathrm{Nil}(\mathbb{A})$, cet ensemble est non vide. Pour tout $a \in \mathrm{Nil}(\mathbb{A})$, il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$ et on a $(-a)^n = (-1)^n a^n = 0$, donc $-a \in \mathrm{Nil}(\mathbb{A})$. Pour a, b dans $\mathrm{Nil}(\mathbb{A})$ et n, m dans $\mathbb{N}^*$ tels que $a^n = a^m = 0$, on a :

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k} = 0$$

(l'utilisation de la formule du binôme est justifiée par la commutativité de $\mathbb{A}$ et pour $0 \leq k \leq n-1$, on a $n+m-k \geq m+1$, donc $b^{n+m-k} = 0$; pour $n \leq k \leq n+m$, on a $a^k = 0$), donc $a+b \in \mathrm{Nil}(\mathbb{A})$. En définitive $\mathrm{Nil}(\mathbb{A})$ est un sous-groupe additif de $\mathbb{A}$. Comme $\mathbb{A}$ est commutatif, pour $a \in \mathrm{Nil}(\mathbb{A})$, $n \in \mathbb{N}^*$ tel que $a^n = 0$ et $b \in \mathbb{A}$, on a $(ab)^n = a^n b^n = 0$, donc $ab \in \mathrm{Nil}(\mathbb{A})$. En conclusion, $\mathrm{Nil}(\mathbb{A})$ est un idéal de $\mathbb{A}$.

2. Soit $(a, b) \in \mathrm{Nil}(\mathbb{A}) \times \mathbb{A}^\times$. On a $a + b = b(1-h)$ où $h = -b^{-1}a$ est nilpotent. Il existe donc $n \in \mathbb{N}^*$ tel que $h^n = 0$ et on a $(1-h)\sum_{k=0}^{n-1} h^k = 1 - h^n = 1$, donc $1-h$ est inversible et il en est de même de $a+b$.

3. Si $\overline{a} \in \mathrm{Nil}\left(\dfrac{\mathbb{A}}{\mathrm{Nil}(\mathbb{A})}\right)$, il existe alors $n \in \mathbb{N}^*$ tel que $\overline{a}^n = \overline{0}$, donc $a^n \in \mathrm{Nil}(\mathbb{A})$ et il existe $m \in \mathbb{N}^*$ tel que $(a^n)^m = a^{nm} = 0$ et $a \in \mathrm{Nil}(\mathbb{A})$, soit $\overline{a} = \overline{0}$. On a donc $\mathrm{Nil}\left(\dfrac{\mathbb{A}}{\mathrm{Nil}(\mathbb{A})}\right) = \left\{\overline{0}\right\}$, c'est-à-dire que $\overline{0}$ est l'unique élément nilpotent de l'anneau quotient $\dfrac{\mathbb{A}}{\mathrm{Nil}(\mathbb{A})}$.

4. Soit $n=\prod_{k=0}^{r} p_k^{\alpha_k}$ la décomposition de $n\geq 2$ en facteurs premiers et $m=\prod_{k=0}^{r} p_k$. Pour $q=\max_{1\leq k\leq r}\alpha_k$, l'entier m^q est divisible par n, donc $\overline{m}^q=\overline{0}$ et $\overline{m}$ est nilpotent. On a donc $(\overline{m})\subset \mathrm{Nil}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)$. Réciproquement si $\overline{a}$ est nilpotent, il existe alors un entier $q\in\mathbb{N}^*$ tel que $\overline{a}^q=\overline{0}$, ce qui signifie que a^q est divisible par n, donc par tous les p_k et a est divisible par tous les p_k, donc par le produit $m=\prod_{k=0}^{r} p_k$ (les p_k sont premiers deux à deux distincts). Il en résulte que $\overline{a}\in(\overline{m})$. En définitive, $\mathrm{Nil}\left(\dfrac{\mathbb{Z}}{\prod_{k=0}^{r} p_k^{\alpha_k}\mathbb{Z}}\right)=\left(\overline{\prod_{k=0}^{r} p_k}\right)$. Cet idéal est réduit à $\left\{\overline{0}\right\}$ si, et seulement si, tous les α_k sont égaux à 1.

5. Comme $0\in\sqrt{\mathbb{A}}$, cet ensemble est non vide. Pour tout $a\in\sqrt{\mathbb{A}}$, il existe $n\in\mathbb{N}$ tel que $a^n\in I$ et on a $(-a)^n=(-1)^n a^n\in I$, donc $-a\in\sqrt{\mathbb{A}}$. Pour a,b dans $\sqrt{\mathbb{A}}$ et n,m dans $\mathbb{N}$ tels que $a^n\in I$ et $a^m\in I$, on a :
$$(a+b)^{n+m}=\sum_{k=0}^{n+m}\binom{n+m}{k}a^k b^{n+m-k}\in I$$
(l'utilisation de la formule du binôme est justifiée par la commutativité de $\mathbb{A}$ et pour $0\leq k\leq n-1$, on a $n+m-k\geq m+1$, donc $b^{n+m-k}\in I$; pour $n\leq k\leq n+m$, on a $a^k\in I$), donc $a+b\in\sqrt{\mathbb{A}}$. En définitive $\sqrt{\mathbb{A}}$ est un sous-groupe additif de $\mathbb{A}$. Comme $\mathbb{A}$ est commutatif, pour $a\in\sqrt{\mathbb{A}}$, $n\in\mathbb{N}$ tel que $a^n\in I$ et $b\in\mathbb{A}$, on a $(ab)^n=a^n b^n\in I$, donc $ab\in\sqrt{\mathbb{A}}$. En conclusion, $\sqrt{\mathbb{A}}$ est un idéal de $\mathbb{A}$. Il est clair que $\sqrt{I}$ contient I (prendre $n=1$).

6. Pour $a\in\mathbb{A}$, on a :
$$\left(a\in\sqrt{\{0\}}\right)\Leftrightarrow(\exists n\in\mathbb{N},\ a^n=0)\Leftrightarrow(a\in\mathrm{Nil}\,(\mathbb{A}))$$
donc $\sqrt{\{0\}}=\mathrm{Nil}\,(\mathbb{A})$.

7. On a déjà $\sqrt{\sqrt{I}}\supset\sqrt{I}$. Pour $a\in\sqrt{\sqrt{I}}$, il existe $n\in\mathbb{N}$ tel que $a^n\in\sqrt{I}$, donc il existe $m\in\mathbb{N}$ tel que $(a^n)^m=a^{nm}\in I$ et $a\in\sqrt{I}$. Donc $\sqrt{\sqrt{I}}=\sqrt{I}$. On a $\sqrt{I\cap J}\subset\sqrt{I}\cap\sqrt{J}$ et pour $a\in\sqrt{I}\cap\sqrt{J}$, il existe n,m dans $\mathbb{N}$ tels que $a^n\in I$ et $a^m\in J$, donc $a^{n+m}\in I\cap J$ et $a\in\sqrt{I\cap J}$. On a donc $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$.

8. Pour $a\in\mathbb{Z}$, on a :
$$\left(a\in\sqrt{p\mathbb{Z}}\right)\Leftrightarrow(\exists n\in\mathbb{N},\ p\text{ divise }a^n)\Leftrightarrow(p\text{ divise }a)\Leftrightarrow(a\in p\mathbb{Z})$$
donc $\sqrt{p\mathbb{Z}}=p\mathbb{Z}$. Un idéal tel que $\sqrt{I}=I$ est dit radical.

9. Soit $n=\prod_{k=0}^{r} p_k^{\alpha_k}$ la décomposition de $n\geq 2$ en facteurs premiers et $m=\prod_{k=0}^{r} p_k$. Pour $q=\max_{1\leq k\leq r}\alpha_k$, l'entier m^q est divisible par n, donc $m^q\in n\mathbb{Z}$, soit $m\in\sqrt{n\mathbb{Z}}$

et $m\mathbb{Z} \subset \sqrt{n\mathbb{Z}}$. Réciproquement si $a \in \sqrt{n\mathbb{Z}}$, il existe alors un entier $q \in \mathbb{N}$ tel que $a^q \in n\mathbb{Z}$, ce qui signifie que a^q est divisible par n, donc par tous les p_k et a est divisible par tous les p_k, donc par le produit $m = \prod_{k=0}^{r} p_k$ (les p_k sont premiers deux à deux distincts). Il en résulte que $\sqrt{n\mathbb{Z}} \subset n\mathbb{Z}$ et qu'on a l'égalité $\sqrt{\left(\prod_{k=0}^{r} p_k^{\alpha_k}\right)\mathbb{Z}} = \left(\prod_{k=0}^{r} p_k\right)\mathbb{Z}$.

Exercice 3.9. *Vérifier qu'un idéal premier n'est pas nécessairement maximal et que si p est irréductible dans $\mathbb{A}$ intègre, l'idéal (p) n'est pas nécessairement maximal.*

Solution. Dans un anneau $\mathbb{A}$ intègre, l'idéal $\{0\}$ est premier non maximal en général (prendre $\mathbb{A} = \mathbb{Z}$). L'idéal (X) est premier dans $\mathbb{Z}[X]$ car $\dfrac{\mathbb{Z}[X]}{(X)}$ est isomorphe à $\mathbb{Z}$ qui est intègre et comme $\mathbb{Z}$ n'est pas un corps, (X) n'est pas maximal. On peut aussi considérer l'anneau $\mathbb{R}[X,Y]$ où l'idéal (X) est premier non maximal. Si, pour p irréductible, (p) est maximal, il est alors premier et p est premier. Comme un élément irréductible n'est pas nécessairement premier (par exemple on a vu avec l'exercice 3.2 que, pour $n \geq 3$, 2 est irréductible non premier dans $\mathbb{Z}[i\sqrt{n}]$), le fait que p soit irréductible n'entraîne pas nécessairement que (p) soit maximal.

Exercice 3.10. *On suppose que $\mathbb{A}$ est fini.*

1. *Montrer qu'un élément non nul de $\mathbb{A}$ est soit inversible, soit un diviseur de zéro. En déduire qu'un anneau commutatif et unitaire qui est fini est intègre si, et seulement si, c'est un corps.*
2. *Montrer que dans un anneau fini tout idéal premier est maximal.*

Solution.

1. Pour $a \in \mathbb{A}\setminus\{0\}$, l'application $\mu_a : x \mapsto ax$ est un morphisme du groupe additif $(\mathbb{A}, +)$ et on a deux possibilités.
   - Soit μ_a est surjectif et dans ce cas le neutre 1 pour le produit a un antécédent a', donc $aa' = 1$ et a est inversible dans $\mathbb{A}$.
   - Soit μ_a est non surjectif et dans ce cas il est non injectif puisque $\mathbb{A}$ est fini, donc $\ker(\mu_a) \neq \{0\}$ et il existe $b \in \mathbb{A}\setminus\{0\}$ tel que $ab = 0$, ce qui signifie que a est un diviseur de 0.

   Par exemple, un élément de $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\overline{0}\}$ est soit inversible, soit un diviseur de $\overline{0}$. Dans le cas où $\mathbb{A}$ est fini et intègre, il est sans diviseurs de zéro, donc tous ses éléments non nuls sont inversibles et c'est un corps. Réciproquement, un corps est toujours intègre.
2. Si I est un idéal premier de $\mathbb{A}$, l'anneau $\dfrac{\mathbb{A}}{I}$ est intègre et comme il est fini, c'est un corps et I est maximal.

Chapitre 4

Anneaux principaux (nouvelle version du 12/12/2024)

On garde les notations et conventions du chapitre 3.

4.1 Définitions et exemples

Définition 4.1. *On dit que l'*anneau $\mathbb{A}$ *est* principal, *s'il est intègre et si tout idéal de* $\mathbb{A}$ *est principal (*i. e. *de la forme* $(a) = \{qa,\ q \in \mathbb{A}\}$*).*

Exemples 4.1

- *Un corps est un anneau principal (les idéaux sont* (0) *et* (1)*).*
- *En utilisant le théorème de division euclidienne, on vérifie que l'anneau* $\mathbb{Z}$ *des entiers relatifs, l'anneau* $\mathbb{D}$ *des nombres décimaux, l'anneau* $\mathbb{K}[X]$ *des polynômes à coefficients dans un corps commutatif* $\mathbb{K}$*, les anneaux* $\mathbb{Z}[i]$ *et* $\mathbb{Z}\left[i\sqrt{2}\right]$ *sont principaux (théorèmes 5.5, 4.1,* **??***, et 5.9).*

Les anneaux euclidiens qui sont des exemples importants d'anneaux principaux sont étudiés au chapitre 5.

Avec le théorème **??**, nous verrons que pour $\mathbb{A}$ intègre, l'anneau $\mathbb{A}[X]$ est principal si, et seulement si, $\mathbb{A}$ est un corps.

Exemples 4.2

- $\mathbb{Z}[X]$ *n'est pas principal (voir l'exercice 4.1 pour une preuve directe de ce résultat).*
- $\mathbb{K}[X, Y] = \mathbb{K}[X][Y]$ *n'est pas principal puisque* $\mathbb{K}[X]$ *n'est pas un corps (*X *qui est non nul ne peut être inversible dans* $\mathbb{K}[X] \setminus \{0\}$ *à cause des degrés).*

Le caractère principal de l'anneau $\mathbb{D}$ des nombres décimaux peut se déduire du résultat suivant conséquence du caractère principal de $\mathbb{Z}$.

Théorème 4.1.

Tout sous-anneau du corps $\mathbb{Q}$ des nombres rationnels est principal.

Preuve. Tout sous-anneau $\mathbb{A}$ de $\mathbb{Q}$ contient $\mathbb{Z}$ puisqu'il est unitaire. Soit I un idéal de $\mathbb{A}$ non réduit à $\{0\}$ (le résultat est trivial si $I = \{0\}$). L'intersection $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc principal et il existe un entier a tel que $I \cap \mathbb{Z} = a\mathbb{Z}$ ($a = \min(I \cap \mathbb{N}^*)$). Comme $a \in I$, on a $(a) = a\mathbb{A} \subset I$. Tout élément r de $I \subset \mathbb{Q}$ s'écrit $r = \dfrac{p}{q}$ avec p et q premiers entre eux et $qr = p \in I \cap \mathbb{Z}$ (r est dans I et q dans $\mathbb{Z} \subset \mathbb{A}$), il existe donc un entier k tel que $qr = ka$, ce qui donne $r = \dfrac{ka}{q} = \dfrac{k}{q}a$. Par ailleurs le théorème de Bézout nous dit qu'il existe deux entiers u et v tels que $up + vq = 1$, donc $\dfrac{1}{q} = ur + v \in \mathbb{A}$ ($v \in \mathbb{Z} \subset \mathbb{A}$ et $r \in I$, donc $ur \in I \subset \mathbb{A}$), $\dfrac{k}{q} \in \mathbb{A}$ et $r = \dfrac{k}{q}a \in (a) = a\mathbb{A}$. Donc $I = (a)$ et $\mathbb{A}$ est principal. □

Le caractère principal de l'anneau $\mathbb{D}$ des nombres décimaux peut aussi se déduire du résultat plus général suivant relatif à l'*anneau localisé* $S^{-1}\mathbb{A}$ de $\mathbb{A}$ associé à une partie multiplicative S de $\mathbb{A}^*$ (*i. e.* telle que pour tout $(a, b) \in S^2$, $ab \in S$).

Théorème 4.2.

Soient $\mathbb{A}$ un anneau intègre, $\mathbb{K}$ son corps des fractions et S une partie multiplicative de $\mathbb{A}^*$ qui contient 1. *L'ensemble :*

$$S^{-1}\mathbb{A} = \left\{ \frac{a}{s},\ a \in \mathbb{A} \text{ et } s \in S \right\}$$

est un sous-anneau du corps $\mathbb{K}$ qui contient $\mathbb{A}$ et si $\mathbb{A}$ est principal, il en est alors de même de $S^{-1}\mathbb{A}$.

Preuve. Comme $1 \in S$, on a $a = \dfrac{a}{1} \in S^{-1}\mathbb{A}$ pour tout $a \in \mathbb{A}$. Pour tous $x = \dfrac{a}{s}$ et $y = \dfrac{b}{t}$ dans $S^{-1}\mathbb{A}$ avec a, b dans $\mathbb{A}$ et s, t dans S, on a $x - y = \dfrac{at - bs}{st} \in S^{-1}\mathbb{A}$ et $xy = \dfrac{ab}{st} \in S^{-1}\mathbb{A}$ puisque S est stable pour le produit et contenue dans $\mathbb{A}$. Donc $S^{-1}\mathbb{A}$ est bien un sous-anneau de $\mathbb{K}$ qui contient $\mathbb{A}$.

Pour $\mathbb{A}$ principal, si J un idéal de $S^{-1}\mathbb{A}$, l'ensemble :

$$I = \left\{ a \in \mathbb{A},\ \exists s \in S \text{ tel que } \frac{a}{s} \in J \right\}$$

est alors un idéal de $\mathbb{A}$ contenu dans J. En effet, $0 \in I$, donc I est non vide et pour $a \in I$ et $s \in S$ tel que $\dfrac{a}{s} \in J$, on a $a = \dfrac{a}{s}s \in J$ puisque J est un idéal, donc $I \subset J$. Pour a, b dans I et s, t dans S, tels que $\dfrac{a}{s}$ et $\dfrac{b}{s}$ soient dans J, on a $\dfrac{a}{st} = \dfrac{a}{s}\dfrac{1}{t} \in J$ et $\dfrac{b}{st} = \dfrac{b}{t}\dfrac{1}{s} \in J$ puisque J est un idéal, ce qui nous donne $\dfrac{a-b}{st} = \dfrac{a}{st} - \dfrac{b}{st} \in J$, donc $a - b \in I$ et I est un sous-groupe additif de $\mathbb{A}$. Enfin, pour tout $c \in \mathbb{A}$, on a $\dfrac{ac}{s} = \dfrac{a}{s}c \in J$, donc $ac \in I$ et I est un idéal de $\mathbb{A}$. Comme $\mathbb{A}$ est principal, il existe

$a_0 \in \mathbb{A}$ tel que $I = (a_0)$ et $\left(S^{-1}\mathbb{A}\right) \cdot a_0 \subset J$ (puisque $a_0 \in I \subset J$ et J est un idéal). Enfin, pour $x = \dfrac{a}{s}$ dans J avec $a \in \mathbb{A}$ et $s \in S$, on a $a \in I$, donc $a = qa_0$ avec $q \in \mathbb{A}$ et $x = \dfrac{q}{s}a_0 \in \left(S^{-1}\mathbb{A}\right) \cdot a_0$. En conclusion, $J = \left(S^{-1}\mathbb{A}\right) \cdot a_0$ est principal. □

Exemples 4.3

— *Pour* $\mathbb{A} = \mathbb{Z}$ *et* $S = \{10^n,\ n \in \mathbb{N}\}$, *on retrouve l'anneau principal des nombres décimaux.*

— *Pour* $\mathbb{A} = \mathbb{K}[X]$ *où* $\mathbb{K}$ *est un corps commutatif et* $S = \{X^n,\ n \in \mathbb{N}\}$, *on déduit que l'anneau* $\mathbb{D} = \left\{ \dfrac{P(X)}{X^n},\ P \in \mathbb{K}[X] \text{ et } n \in \mathbb{N} \right\}$ *est principal.*

Le résultat qui suit peut être utilisé pour montrer qu'un anneau est principal. Voir l'exercice 4.3 pour deux exemples.

Lemme 4.1 *Si l'anneau* $\mathbb{A}$ *est isomorphe à un anneau* $\mathbb{B}$ *principal il est alors principal.*

Preuve. Soient $\mathbb{B}$ un anneau principal et $\varphi : \mathbb{A} \to \mathbb{B}$ un isomorphisme d'anneaux. Si I est un idéal de $\mathbb{A}$, son image $\varphi(I)$ est alors un idéal de $\mathbb{B}$ (φ est surjectif, lemme 3.3) et il existe $b = \varphi(a) \in \mathbb{B}$ tel que $\varphi(I) = \varphi(a) \cdot \mathbb{B}$. Comme φ est un isomorphisme d'anneaux, on a $I = \varphi^{-1}(\varphi(I)) = \varphi^{-1}(\varphi(a)) = a \cdot \mathbb{A}$. L'anneau $\mathbb{A}$ est donc principal. □

On désigne par $\mathbb{K}[[X]]$ l'ensemble des séries formelles à une indéterminée et à coefficients dans un corps commutatif $\mathbb{K}$.

On rappelle qu'une série formelle à une indéterminée à coefficients dans $\mathbb{K}$ est une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$. On note $\displaystyle\sum_{n\in\mathbb{N}} a_n X^n$ une telle série formelle.

On définit une addition et une multiplication sur $\mathbb{K}[[X]]$ par :

$$\sum_{n\in\mathbb{N}} a_n X^n + \sum_{n\in\mathbb{N}} b_n X^n = \sum_{n\in\mathbb{N}} (a_n + b_n) X^n,\ \left(\sum_{n\in\mathbb{N}} a_n X^n\right)\left(\sum_{n\in\mathbb{N}} b_n X^n\right) = \sum_{n\in\mathbb{N}} c_n X^n$$

où $c_n = \displaystyle\sum_{k=0}^{n} a_k b_{n-k}$ pour tout $n \in \mathbb{N}$. On vérifie facilement que $\mathbb{K}[[X]]$ muni de ces lois est un anneau commutatif qui contient $\mathbb{K}[X]$.

On définit la valuation d'une série formelle $S = \displaystyle\sum_{n\in\mathbb{N}} a_n X^n$ par :

$$\operatorname{val}(S) = \begin{cases} +\infty \text{ si } S = 0_{\mathbb{K}} \\ \min\{n \in \mathbb{N},\ a_n \neq 0_{\mathbb{K}}\} \text{ si } S \neq 0_{\mathbb{K}} \end{cases}$$

On vérifie facilement que pour toutes séries formelles S, T, on a :

$$\operatorname{val}(S+T) \geq \min(\operatorname{val}(S), \operatorname{val}(T)) \text{ et } \operatorname{val}(ST) = \operatorname{val}(S) + \operatorname{val}(T)$$

et on en déduit que $\mathbb{K}[[X]]$ est intègre.

Lemme 4.2 *Soient* $S=\sum_{n\in\mathbb{N}}a_nX^n$ *et* $T=\sum_{n\in\mathbb{N}}b_nX^n$ *deux séries formelles avec* $\operatorname{val}(T)=0$ *(soit* $b_0\neq 0_{\mathbb{K}}$*). Pour tout entier naturel* n*, il existe un unique couple* $(Q_n,R_n)\in\mathbb{K}_n[X]\times\mathbb{K}[[X]]$ *tel que* $S=TQ_n+X^{n+1}R_n$.

Preuve. Pour montrer l'existence du couple (Q_n,R_n), on raisonne par récurrence sur $n\geq 0$. Pour $n=0$, il suffit d'écrire :

$$\begin{aligned}S&=a_0+X\sum_{n=1}^{+\infty}a_nX^{n-1}=\frac{a_0}{b_0}\sum_{n\in\mathbb{N}}b_nX^n+X\sum_{n=1}^{+\infty}\left(a_n-\frac{a_0}{b_0}b_n\right)X^{n-1}\\&=TQ_0+XR_0\end{aligned}$$

en notant $Q_0=\dfrac{a_0}{b_0}$ et $R_0=\sum_{n\in\mathbb{N}}\left(a_{n+1}-\dfrac{a_0}{b_0}b_{n+1}\right)X^n$. Supposant le résultat acquis pour $n\geq 0$, on a $S=TQ_n+X^{n+1}R_n$ et $R_n=\alpha_nT+XS_n$ avec $\alpha_n\in\mathbb{K}$ et $S_n\in\mathbb{K}[[X]]$, ce qui nous donne :

$$\begin{aligned}S&=TQ_n+X^{n+1}(\alpha_nT+XS_n)=T\left(Q_n+\alpha_nX^{n+1}\right)+X^{n+2}S_n\\&=TQ_{n+1}+X^{n+2}R_{n+1}\end{aligned}$$

avec $Q_{n+1}=Q_n+\alpha_nX^{n+1}\in\mathbb{K}_{n+1}[X]$ et $R_{n+1}=S_n\in\mathbb{K}[[X]]$. Pour l'unicité, il suffit de montrer que si $TQ_n+X^{n+1}R_n=0_{\mathbb{K}}$ avec $(Q_n,R_n)\in\mathbb{K}_n[X]\times\mathbb{K}[[X]]$, on a alors $Q_n=0_{\mathbb{K}}$ et $R_n=0_{\mathbb{K}}$. Supposons que $TQ_n+X^{n+1}R_n=0_{\mathbb{K}}$. Si $Q_n\neq 0_{\mathbb{K}}$, on a alors $R_n\neq 0_{\mathbb{K}}$ ($\mathbb{K}[[X]]$ est intègre), $\operatorname{val}(TQ_n)=\operatorname{val}(T)+\operatorname{val}(Q_n)=\operatorname{val}(Q_n)\leq n$ et $\operatorname{val}\left(-X^{n+1}R_n\right)=n+1+\operatorname{val}(R_n)\geq n+1$, ce qui est en contradiction avec $TQ_n=-X^{n+1}R_n$. On a donc $Q_n=0_{\mathbb{K}}$ et $R_n=0_{\mathbb{K}}$. □

Dans le cas où S et T sont des polynômes, avec $T(0)\neq 0_{\mathbb{K}}$, on retrouve le théorème de division suivant les puissances croissantes dans $\mathbb{K}[X]$.

Lemme 4.3 *Le groupe des éléments inversibles de* $\mathbb{K}[[X]]$ *est :*

$$(\mathbb{K}[[X]])^{\times}=\{S\in\mathbb{K}[[X]],\ \operatorname{val}(S)=0\}$$

Preuve. Si $S=\sum_{n\in\mathbb{N}}a_nX^n\in\mathbb{K}[[X]]$ est inversible, il existe alors une série formelle $T=\sum_{n\in\mathbb{N}}b_nX^n\in\mathbb{K}[[X]]$ telle que $ST=1_{\mathbb{K}}$ et on a en particulier $a_0b_0=1_{\mathbb{K}}$, ce qui impose $a_0\neq 0_{\mathbb{K}}$ et signifie que $\operatorname{val}(S)=0$. Réciproquement, si $\operatorname{val}(S)=0$, pour tout $n\in\mathbb{N}$, on peut trouver un unique couple $(Q_n,R_n)\in\mathbb{K}_n[X]\times\mathbb{K}[[X]]$ tel que $1_{\mathbb{K}}=SQ_n+X^{n+1}R_n$ (lemme 4.2). En écrivant $Q_n(X)=\sum_{k=0}^{n}b_{n,k}X^k$, on a pour $m>n\geq 0$:

$$\begin{aligned}1_{\mathbb{K}}&=SQ_m+X^{m+1}R_m\\&=S\left(\sum_{k=0}^{n}b_{m,k}X^k\right)+X^{n+1}\left(S\sum_{k=n+1}^{m}b_{m,k}X^{k-n-1}+X^{m-n}R_m\right)\\&=SQ_n+X^{n+1}R_n\end{aligned}$$

et avec l'unicité d'une telle décomposition, on déduit que $Q_n = \sum_{k=0}^{n} b_{m,k} X^k$, soit $b_{m,k} = b_{n,k}$ pour tout k compris entre 0 et n. En notant $b_k = b_{k,k}$ pour tout $k \geq 0$, on a $b_{n,k} = b_{k,k} = b_k$ pour tout k compris entre 0 et n et $Q_n(X) = \sum_{k=0}^{n} b_k X^k$, la suite $(b_k)_{k\in\mathbb{N}}$ étant uniquement déterminée. Les relations $1_{\mathbb{K}} = SQ_n + X^{n+1}R_n$ pour $n \geq 0$ nous donne $a_0 b_0 = 1_{\mathbb{K}}$ et pour $n \in \mathbb{N}^*$, le coefficient de X^n est $\sum_{k=0}^{n} a_k b_{n-k} = 0_{\mathbb{K}}$, donc en notant $T = \sum_{n\in\mathbb{N}} b_n X^n$, on a $ST = 1_{\mathbb{K}}$ et T est l'inverse de S dans $\mathbb{K}[[X]]$. □

Théorème 4.3.

L'anneau $\mathbb{K}[[X]]$ est principal. Plus précisément, les idéaux non réduit à $\{0\}$ de $\mathbb{K}[[X]]$ sont de la forme $(X^n) = X^n \cdot \mathbb{K}[[X]]$.

Preuve. Soit I un idéal de l'anneau $\mathbb{K}[[X]]$ non réduit à $\{0\}$. L'ensemble $\{\mathrm{val}(S),\ S \in I \setminus \{0\}\}$ étant une partie non vide de $\mathbb{N}$, elle admet un plus petit élément, c'est-à-dire qu'il existe $S_0 \in I \setminus \{0\}$ tel que $n = \mathrm{val}(S_0) = \min_{S\in I\setminus\{0\}} \mathrm{val}(S)$. Une telle série est de la forme $S_0 = \sum_{k\geq n} a_k X^k = X^n \sum_{k\geq 0} a_{n+k} X^k$ avec $a_n \neq 0$, donc $S = \sum_{k\geq 0} a_{n+k} X^k$ est de valuation nulle, c'est-à-dire inversible et $X^n = S_0 S^{-1}$ est dans I. On a donc $(X^n) \subset I$. Si $S \in I \setminus \{0\}$, on a alors $\mathrm{val}(S) \geq n$, donc $S = X^n \sum_{k\geq 0} b_{n+k} X^k \in (X^n)$. Il en résulte que $I \subset (X^n)$ et $I = (X^n)$. L'anneau $\mathbb{K}[[X]]$ est donc principal. □

Au paragraphe 5 nous verrons que $\mathbb{K}[[X]]$ est euclidien.

Le lemme qui suit nous donne une description des éléments irréductibles d'un anneau principal, cette caractérisation pouvant être utilisée pour vérifier qu'un anneau n'est pas principal.

Lemme 4.4 *Soit $\mathbb{A}$ un anneau principal.*

1. *Un élément $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$ est irréductible si, et seulement si, il est premier.*
2. *Pour tout $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$, on a :*

$$((p) \text{ premier}) \Leftrightarrow (p \text{ premier}) \Leftrightarrow (p \text{ irréductible}) \Leftrightarrow ((p) \text{ maximal})$$

Preuve. On sait déjà que pour $\mathbb{A}$ intègre (non nécessairement principal), un élément premier est irréductible (lemme 3.1) et qu'un élément p de $\mathbb{A}$ est premier si, et seulement l'idéal (p) est premier (théorème 3.5).

1. Soient $\mathbb{A}$ principal et $p \in \mathbb{A}^* \setminus \mathbb{A}^\times$ irréductible qui divise ab. Comme l'anneau $\mathbb{A}$ est principal, l'idéal $I = (p, a)$ est engendré par un élément δ (δ est un pgcd de p et a dans $\mathbb{A}$), soit $I = (\delta)$. De $p \in I$, on déduit que δ divise p, donc δ est soit inversible, soit associé à p, puisque p est irréductible. Dans le cas où δ est inversible, on a $(\delta) = \mathbb{A}$, donc $1 \in I$, soit $1 = up + va$ avec u, v dans $\mathbb{A}$ et p divise $b = upv + abv$. Dans le cas où δ est associé à p, on a $(\delta) = (p)$, donc $a \in (p)$ et p divise a.

2. Si (p) maximal, il alors premier (théorème 3.5), donc p est premier et irréductible.
3. Il reste à montrer que si $p \in \mathbb{A}$ est irréductible, alors l'idéal (p) est maximal. Un élément irréductible p de $\mathbb{A}$ est non inversible, donc $(p) \neq \mathbb{A}$. Si $J = (a)$ est un idéal de $\mathbb{A}$ (qui est principal) qui contient (p), a divise alors p et on a soit a inversible, donc $J = \mathbb{A}$, soit a associé à p et $J = (p)$. L'idéal (p) est donc maximal. □

L'implication « $\mathbb{A}[X]$ principal entraîne $\mathbb{A}$ est un corps » du théorème **??** peut se montrer comme suit en utilisant le résultat précédent. Si $\mathbb{A}[X]$ est principal, il est alors intègre, donc $\mathbb{A}$ est intègre. L'application $\varphi : P \in \mathbb{A}[X] \mapsto P(0) \in \mathbb{A}$ est un morphisme d'anneaux surjectif dont le noyau est $\ker(\varphi) = (X)$, donc $\dfrac{\mathbb{A}[X]}{(X)}$ est isomorphe à $\mathbb{A}$ et cet anneau quotient est intègre, ce qui revient à dire que (X) est premier donc maximal puisque $\mathbb{A}[X]$ est principal, ce qui revient aussi à dire que $\dfrac{\mathbb{A}[X]}{(X)}$ est un corps et il en est de même de $\mathbb{A}$.

Exemple 4.1 *Les anneaux $\mathbb{Z}[i\sqrt{n}]$ ne sont pas principaux pour $n \geq 3$, puisque 2 y est irréductible non premier (voir l'exercice 3.2).*

Du théorème 3.8, on déduit le suivant.

Théorème 4.4.

Un anneau principal est factoriel.

Preuve. Soit $\mathbb{A}$ un anneau principal. Le lemme 4.4 nous dit que les irréductibles de $\mathbb{A}$ sont les éléments premiers. Il suffit donc d'après le théorème 3.8 de montrer que toute suite croissante d'idéaux principaux de $\mathbb{A}$ est stationnaire. Soit $(a_0) \subset (a_1) \subset \cdots \subset (a_n) \subset \cdots$ une suite croissante d'idéaux de $\mathbb{A}$. Comme $I = \bigcup_{k=0}^{+\infty} (a_k)$ est un idéal de l'anneau principal $\mathbb{A}$, il existe un élément a de $\mathbb{A}$ tel que $I = (a)$. En désignant par n_0 le plus petit entier naturel tel que $a \in (a_{n_0})$, on a $I = (a) \subset (a_{n_0}) \subset I$ et $I = (a_{n_0})$. Il en résulte que pour tout entier naturel p, on a $a_{n_0+p} \in (a_{n_0})$, donc $(a_{n_0+p}) \subset (a_{n_0}) \subset (a_{n_0+p})$ et $(a_{n_0+p}) = (a_{n_0})$. La suite $((a_k))_{k\in\mathbb{N}}$ est donc stationnaire. □

Le lemme qui suit nous dit qu'il existe des anneaux non principaux, dont tous les idéaux sont principaux.

Lemme 4.5 *Soient $\mathbb{A}$ un anneau principal et $I = (a)$ un idéal non trivial de $\mathbb{A}$ (*i. e. *$I \neq \{0\}$ et $I \neq \mathbb{A}$). Tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux de la forme $\left(\overline{b}\right)$ où $b \in \mathbb{A}$ est un diviseur de a et l'anneau $\dfrac{\mathbb{A}}{(a)}$ est principal si, et seulement si, a est premier ou encore irréductible.*

Preuve. Soit $I = (a)$ un idéal de l'anneau principal $\mathbb{A}$ avec $a \neq 0$ et a non inversible. Si J est un idéal de $\dfrac{\mathbb{A}}{I}$, en désignant par π_I la surjection canonique de

$\mathbb{A}$ sur $\dfrac{\mathbb{A}}{I}$, $\pi_I^{-1}(J)$ est un idéal de $\mathbb{A}$ qui contient I, donc $\pi_I^{-1}(J) = (b) \supset (a)$ et b divise a. De plus, comme π_I est surjectif, on a $J = \pi_I\left(\pi_I^{-1}(J)\right) = \pi_I(b\mathbb{A}) = \left(\overline{b}\right)$. Tous les idéaux de $\dfrac{\mathbb{A}}{I} = \dfrac{\mathbb{A}}{(a)}$ sont donc principaux de la forme $\left(\overline{b}\right)$ où $b \in \mathbb{A}$ est un diviseur de a. L'anneau $\dfrac{\mathbb{A}}{I}$ est donc principal si, et seulement si, il est intègre, ce qui revient à dire que l'idéal $I = (a)$ est premier, ce qui revient à dire que a est premier, ou encore irréductible, ou encore que (p) est maximal, ou encore que $\dfrac{\mathbb{A}}{I}$ est un corps (lemme 4.4). □

Pour $I = \{0\}$, $\dfrac{\mathbb{A}}{I} \backsimeq \mathbb{A}$ est principal et pour $I = \mathbb{A}$, $\dfrac{\mathbb{A}}{I} = \left\{\overline{0}\right\}$.

4.2 Anneaux à pgcd

Pour ce paragraphe, l'anneau $\mathbb{A}$ est supposé intègre.

Définition 4.2. *Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \cdots, a_r$ des éléments de $\mathbb{A}^*$. On dit que ces éléments admettent un* plus grand commun diviseur *s'il existe $\delta \in \mathbb{A}^*$ tel que :*

$$\begin{cases} \forall k \in \{1, \cdots, r\},\ \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, \cdots, a_r \text{ divise } \delta \end{cases} \tag{4.1}$$

Lemme 4.6 *Deux plus grands communs diviseurs d'une famille $(a_i)_{1 \le i \le r}$ d'éléments de $\mathbb{A}^*$ sont associés.*

Preuve. Si δ et δ' sont deux plus grands communs diviseurs de $a_1, \cdots, a_r$, on a alors δ qui divise δ' et δ' qui divise δ, donc δ et δ' sont associés. □

En cas d'existence, on note $\operatorname{pgcd}(a_1, \cdots, a_r)$ ou $a_1 \wedge \cdots \wedge a_r$ un plus grand commun diviseur de $a_1, \cdots, a_r$, c'est un élément de $\mathbb{A}^*$ défini à association près.

Pour $a \in \mathbb{A}^*$ et $b \in \mathbb{A}^\times$, on a $\operatorname{pgcd}(a, b) \in \mathbb{A}^\times$.

Pour toute permutation σ de $\{1, \cdots, r\}$, on a en cas d'existence :

$$\operatorname{pgcd}(a_1, \cdots, a_r) = \operatorname{pgcd}\left(a_{\sigma(1)}, \cdots, a_{\sigma(r)}\right)$$

(commutativité du pgcd).

Définition 4.3. *On dit que l'anneau $\mathbb{A}$ est un anneau à* pgcd *si deux éléments quelconques a, b de $\mathbb{A}^*$ admettent un* pgcd.

Si $\mathbb{A}$ est un anneau à pgcd, alors toute famille $\{a_1, \cdots, a_r\}$ de $r \ge 2$ éléments de $\mathbb{A}^*$ admet un pgcd. En effet, c'est vrai pour $r = 2$ et supposant le résultat acquis pour $r \ge 2$, $\delta = \operatorname{pgcd}(\operatorname{pgcd}(a_1, \cdots, a_r), a_{r+1})$ est un pgcd de $a_1, \cdots, a_{r+1}$. En effet, δ divise $\operatorname{pgcd}(a_1, \cdots, a_r)$ et a_{r+1}, donc il divise tous les a_k pour $1 \le k \le r+1$.

Si d est un diviseur commun à $a_1, \cdots, a_{r+1}$, c'est aussi un diviseur commun à $a_1, \cdots, a_r$, donc il divise $\operatorname{pgcd}(a_1, \cdots, a_r)$ et comme il divise a_{r+1}, il divise δ. On

a donc $\text{pgcd}\,(a_1,\cdots,a_r,a_{r+1}) = \text{pgcd}\,(\text{pgcd}\,(a_1,\cdots,a_r),a_{r+1})$ à une unité près (associativité du pgcd).

Théorème 4.5.

Un anneau principal $\mathbb{A}$ est un anneau à pgcd. *Précisément, pour toute famille $\{a_1,\cdots,a_r\}$ de $r\geq 2$ éléments de $\mathbb{A}^*$, il existe un élément δ de $\mathbb{A}^*$ tel que $(a_1,\cdots,a_r)=(\delta)$ et cet élément s'écrit $\delta=\sum_{k=1}^{r}u_ka_k$, où $u_1,\cdots,u_r$ sont des éléments de $\mathbb{A}$ et δ est un* pgcd *de $a_1,\cdots,a_r$.*

Preuve. Un anneau principal est intègre. L'existence de δ se déduit du fait que $(a_1,\cdots,a_r)$ est un idéal de l'anneau principal $\mathbb{A}$.

Comme $\delta\in(\delta)=(a_1,\cdots,a_r)$, il existe $(u_k)_{1\leq k\leq r}\in\mathbb{A}^r$ tel que $\delta=\sum_{k=1}^{r}u_ka_k$. De $(a_k)\subset(\delta)$ pour tout k compris entre 1 et r, on déduit que δ divise a_k. Si $d\in\mathbb{A}$ est un diviseur commun aux a_k, il divise aussi $\delta=\sum_{k=1}^{r}u_ka_k$. □

La relation $\delta=\sum_{k=1}^{r}u_ka_k$ est l'*identité de Bézout.*

Nous verrons qu'un anneau euclidien est principal, donc à pgcd (théorème 5.1) et que l'on dispose dans un tel anneau de l'algorithme d'Euclide pour obtenir le pgcd de deux éléments non nuls. Cet algorithme permet également de déterminer u et v dans $\mathbb{A}$ tels que $au+bv=a\wedge b$ (paragraphe 5.2).

Lemme 4.7 *Soient $\mathbb{A}$ un anneau factoriel et a,b deux éléments non nuls et non inversibles de $\mathbb{A}$. En notant $a=u\prod_{k=1}^{r}p_k^{m_k}$, $b=v\prod_{k=1}^{r}p_k^{n_k}$, les décompositions de a et b en facteurs irréductibles, où u et v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels (certains de ces entiers pouvant être nuls), on a :*

$$(a\ \textit{divise}\ b)\Leftrightarrow(\forall k\in\{1,\cdots,r\},\ m_k\leq n_k)$$

Preuve. Dire que a divise b équivaut à dire qu'il existe $q_1\in\mathbb{A}^*$ tel que $b=aq_1$. Si q_1 est inversible, a et b sont alors associés et $m_k=n_k$ pour tout entier k compris entre 1 et r. Sinon, les facteurs irréductibles de q_1 sont dans ceux de b et en écrivant $q_1=\prod_{k=1}^{r}p_k^{s_k}$ où les s_k sont des entiers naturels, on a $b=v\prod_{k=1}^{r}p_k^{n_k}=u\prod_{k=1}^{r}p_k^{m_k+s_k}$ et de l'unicité de la décomposition en facteurs irréductibles, on déduit que $n_k=m_k+s_k\geq m_k$ pour $1\leq k\leq r$. La réciproque est évidente. □

Théorème 4.6.

Un anneau factoriel $\mathbb{A}$ *est à* pgcd. *Plus précisément, pour* $a = u\prod_{k=1}^{r} p_k^{m_k}$, $b = v\prod_{k=1}^{r} P_k^{n_k}$ *dans* $\mathbb{A}^* \setminus \mathbb{A}^\times$, *où* u, v *sont inversibles, les* p_k *sont irréductibles deux à deux non associés et les* n_k, m_k *sont des entiers naturels (certains de ces entiers pouvant être nuls), on a* $a \wedge b = \prod_{k=1}^{r} p_k^{\min(m_k,n_k)}$.

Preuve. Un anneau factoriel est intègre et le lemme précédent nous dit que $\delta = \prod_{k=1}^{r} p_k^{\min(m_k,n_k)}$ divise a et b. Si d est un diviseur de a et b, il s'écrit sous la forme $d = \prod_{k=1}^{r} p_k^{s_k}$ où les s_k sont des entiers naturels tels que $s_k \leq m_k$ et $s_k \leq n_k$ pour tout k compris entre 1 et r, on a donc $s_k \leq \min(m_k, n_k)$ pour tout k compris entre 1 et r et d divise δ. En conclusion, δ est bien un pgcd de a et b. □

Remarque 4.1 *Du théorème précédent, on déduit que dans un anneau factoriel, pour tous* $\lambda, a_0, \cdots, a_n$ *dans* $\mathbb{A}^*$, *on a* $\operatorname{pgcd}(\lambda a_0, \cdots, \lambda a_n) = \lambda \operatorname{pgcd}(a_0, \cdots, a_n)$ *(homogénéité du* pgcd*).*

Définition 4.4. *Soient* $r \in \mathbb{N} \setminus \{0, 1\}$ *et* $a_1, \cdots, a_r$ *des éléments tous non nuls dans un anneau à* pgcd $\mathbb{A}$. *On dit que* $a_1, \cdots, a_r$ *sont* premiers entre eux *dans leur ensemble (ou étrangers) si leur* pgcd *est dans* $\mathbb{A}^\times$. *Pour* $r = 2$, *on dira simplement que* a_1 *et* a_2 *sont premiers entre eux.*

Comme, dans un anneau à pgcd, tout élément associé à un pgcd de $a_1, \cdots, a_r$ est aussi un pgcd de $a_1, \cdots, a_r$ et considérant que 1 est associé à tout élément inversible de $\mathbb{A}$, on peut écrire que $a_1, \cdots, a_r$ sont premiers entre eux dans leur ensemble si, et seulement si, $\operatorname{pgcd}(a_1, \cdots, a_r) = 1$.

Théorème 4.7.

Soient $r \in \mathbb{N} \setminus \{0, 1\}$, $a_1, \cdots, a_r$ *des éléments tous non nuls dans un anneau à* pgcd $\mathbb{A}$. *En désignant par* d *un diviseur commun à* $a_1, \cdots, a_r$ *et en écrivant* $a_k = d\alpha_k$ *pour tout* k *compris entre* 1 *et* r, *on a :*

$$(d = \operatorname{pgcd}(a_1, \cdots, a_r)) \Leftrightarrow (\operatorname{pgcd}(\alpha_1, \cdots, \alpha_r) = 1)$$

Preuve. Si d est un pgcd de $(a_i)_{1\leq i\leq r}$, en notant $\delta' = \operatorname{pgcd}(\alpha_i)_{1\leq i\leq r}$, on a alors $a_k = d\alpha_k = d\delta'\beta_k$ pour tout k compris entre 1 et r, donc $d\delta'$ est un diviseur commun des a_k et en conséquence il divise d, ce qui impose $\delta' \in \mathbb{A}^\times$. Réciproquement, on suppose que $\operatorname{pgcd}(\alpha_i)_{1\leq i\leq r} = 1$. Comme d est un diviseur commun des a_k, il divise $\delta = \operatorname{pgcd}(a_i)_{1\leq i\leq r}$, donc $\delta = qd$. En écrivant que $a_k = \delta\beta_k = qd\beta_k = d\alpha_k$ pour tout k compris entre 1 et r, on a $q\beta_k = \alpha_k$, donc q est un diviseur commun

aux α_k et nécessairement il est inversible puisque les α_k sont premiers entre eux. En définitive d et δ sont associés et d est un pgcd de $a_1, \cdots, a_r$. □

Le théorème précédent dit en particulier que pour $\alpha_1, \cdots, \alpha_r$ premiers entre eux dans un anneau à pgcd $\mathbb{A}$, on a pour tout $d \in \mathbb{A}^*$, $\text{pgcd}\,(d\alpha_1, \cdots, d\alpha_r) = d$, ce qui se déduit aussi de l'homogénéité du pgcd.

Théorème 4.8. Gauss

Deux élément non nuls a et b d'un anneau à pgcd $\mathbb{A}$ *sont premiers entre eux si, et seulement si, pour tout $c \in \mathbb{A}^*$, a divise bc entraîne que a divise c.*

Preuve. Soient a et b premiers entre eux dans $\mathbb{A}$. Pour $c \in \mathbb{A}^*$, on a $\text{pgcd}\,(ac, bc) = c$, donc si a divise bc, c'est alors un diviseur commun à ac et bc et en conséquence un diviseur de leur pgcd qui vaut c.

Réciproquement, on suppose que pour tout $c \in \mathbb{A}^*$, si a divise bc il divise alors c. Soit d un diviseur commun de a et b avec $a = d\alpha$ et $b = d\beta$. Comme d divise $\alpha b = \alpha d\beta = a\beta$, il divise α, soit $a = d\alpha$ divise α et d est inversible. En conclusion a et b sont premiers entre eux. □

Des résultats qui précèdent, on peut déduire qu'un anneau à pgcd est un anneau à ppcm et réciproquement.

Définition 4.5. *Soient $r \in \mathbb{N} \setminus \{0, 1\}$ et $a_1, \cdots, a_r$ des éléments de $\mathbb{A}^*$. On dit que ces éléments admettent un* plus petit commun multiple *s'il existe $\mu \in \mathbb{A}^*$ tel que :*

$$\begin{cases} \forall k \in \{1, \cdots, r\},\ \mu \text{ est multiple de } a_k \\ \text{tout multiple commun à } a_1, \cdots, a_r \text{ est multiple de } \delta \end{cases}$$

Lemme 4.8 *Deux plus petit communs multiples d'une famille $\{a_1, \cdots, a_r\}$ d'éléments de $\mathbb{A}^*$ sont associés.*

Preuve. Si μ et μ' sont deux plus petit communs multiples de $a_1, \cdots, a_r$, on a alors μ qui divise μ' et μ' qui divise μ, donc μ et μ' sont associés. □

En cas d'existence, on note $\text{ppcm}\,(a_1, \cdots, a_r)$ ou $a_1 \vee \cdots \vee a_r$ un plus petit commun multiple de $a_1, \cdots, a_r$, c'est un élément de $\mathbb{A}^*$ défini à association près.

Pour $a \in \mathbb{A}^*$ et $b \in \mathbb{A}^\times$, on a $\text{ppcm}\,(a, b) = a$.

Pour toute permutation σ de $\{1, \cdots, r\}$, on a en cas d'existence :

$$\text{ppcm}\,(a_1, \cdots, a_r) = \text{ppcm}\left(a_{\sigma(1)}, \cdots, a_{\sigma(r)}\right)$$

(commutativité du ppcm).

Comme pour le pgcd, on vérifie l'associativité du ppcm :

$$\text{ppcm}\,(a_1, \cdots, a_r, a_{r+1}) = \text{ppcm}\,(\text{ppcm}\,(a_1, \cdots, a_r), a_{r+1})$$

Théorème 4.9.

L'anneau $\mathbb{A}$ *est à* pgcd *si, et seulement si, deux éléments quelconques* a, b *de* $\mathbb{A}^*$ *admettent un* ppcm. *Dans ce cas, on a* $ab = \text{pgcd}\,(a,b) \cdot \text{ppcm}\,(a,b)$ *à une unité près.*

Preuve. Supposons que l'anneau $\mathbb{A}$ soit à pgcd. En notant, pour a, b dans $\mathbb{A}^*$, $\delta = \text{pgcd}\,(a,b)$, $a = \delta\alpha$ et $b = \delta\beta$, on vérifie que $\mu = \dfrac{ab}{\delta} = \delta\alpha\beta$ est un ppcm de a et b. Tout d'abord, $\mu = \delta\alpha\beta = a\beta = \alpha b$ est multiple commun de a et b. Si m est multiple commun de a et b, on a alors $m = ua = vb$, soit $u\delta\alpha = v\delta\beta$ et $u\alpha = v\beta$, donc α divise $v\beta$ en étant premier avec β, ce qui impose qu'il divise v, ce qui nous donne $v = \alpha w$ et $m = vb = w\alpha b = w\mu$ est multiple de μ. En conclusion $\mu = \dfrac{ab}{\delta}$ est un ppcm de a et b et $ab = \delta\mu = \text{pgcd}\,(a,b) \cdot \text{ppcm}\,(a,b)$ à une unité près. Réciproquement, supposons que tout couple (a,b) d'éléments de $\mathbb{A}^*$ admette un ppcm μ. Comme ab est multiple commun de a et b, il existe $\delta \in \mathbb{A}^*$ tel que $ab = \delta\mu$. On vérifie alors que δ est un pgcd de a et b. Comme μ est multiple de a, on a $ab = \delta\mu = \delta ua$, soit $b = \delta u$ et δ divise b. De façon analogue, on voit que δ divise a. Soit d un diviseur commun de a et b avec $a = d\alpha$, $b = d\beta$, donc $d\alpha\beta = a\beta = \alpha b$ est multiple commun de a et b, ce qui entraîne qu'il est multiple de μ, soit $d\alpha\beta = w\mu$ et $\delta\mu = ab = dw\mu$, donc $\delta = dw$, c'est-à-dire que d divise δ. □

Dans le cas d'un anneau principal $\mathbb{A}$, on a le résultat important suivant qui permet de caractériser les éléments premiers entre eux.

Théorème 4.10. Bézout

Soient $r \in \mathbb{N}\backslash\{0,1\}$ *et* $a_1, \cdots, a_r$ *des éléments tous non nuls dans anneau principal* $\mathbb{A}$. *Ces éléments sont premiers entre eux dans leur ensemble si, et seulement si, il existe* $(u_k)_{1\leq k\leq r} \in \mathbb{A}^r$ *tel que* $\displaystyle\sum_{k=1}^{r} u_k a_k = 1$.

Preuve. L'égalité de Bézout pour le pgcd dans un anneau principal nous donne la condition est nécessaire. Réciproquement s'il existe $u_1, \cdots, u_p$ dans $\mathbb{A}$ tels que $\displaystyle\sum_{k=1}^{r} u_k a_k = 1$, on en déduit alors que $\delta = a_1 \wedge \cdots \wedge a_r$, qui divise tous les a_k, va diviser $1 = \displaystyle\sum_{k=1}^{r} u_k a_k$, ce qui signifie qu'il est inversible, c'est-à-dire que $a_1, \cdots, a_r$ sont premiers entre eux dans leur ensemble. □

De ce théorème, on déduit simplement quelques conséquences tout aussi importantes, certains de ces résultats étant déjà vus dans le cas d'un anneau à pgcd.

Corollaire 4.1. *Soient* a, b, c *non nuls dans un anneau principal* $\mathbb{A}$. *Si* c *est premier avec* a *alors* $a \wedge b = a \wedge (bc)$ *(le* pgcd *de deux éléments est inchangé si on multiplie l'un d'eux par un élément premier avec l'autre).*

Preuve. Soient $\delta = a \wedge b$ et $\delta' = a \wedge (bc)$. Comme δ divise a et b, il divise a et bc ainsi que leur pgcd δ'. De $au + cv = 1$, on déduit que $abu + bcv = b$ et δ' qui divise a et bc va diviser a et b ainsi que leur pgcd δ. En définitive δ et δ' sont associés, ce qui signifie que $a \wedge b = a \wedge (bc)$. □

Corollaire 4.2. *Soient $a_1, \cdots, a_r$ (avec $r \geq 2$) et c tous non nuls dans un anneau principal $\mathbb{A}$. Si c est premier avec chacun des a_k, pour tout k compris entre 1 et r, il est alors premier avec leur produit $\prod_{k=1}^{r} a_k$.*

Preuve. En utilisant le corollaire précédent, on a :

$$c \wedge \prod_{k=1}^{r} a_k = c \wedge \left(a_1 \prod_{k=2}^{r} a_k \right) = c \wedge \prod_{k=2}^{r} a_k$$

puisque a_1 est premier avec c et par récurrence finie, on déduit que :

$$c \wedge \prod_{k=1}^{r} a_k = c \wedge \prod_{k=2}^{r} a_k = c \wedge \prod_{k=3}^{r} a_k = \cdots = c \wedge a_r = 1$$

puisque chaque a_k, pour k compris entre 1 et r, est premier avec c. □

Corollaire 4.3. (Gauss) *Soient a, b, c non nuls dans un anneau principal $\mathbb{A}$. Si a divise bc et a est premier avec b alors a divise c.*

Preuve. Comme a et b sont premiers entre eux, il existe u, v dans $\mathbb{A}$ tels que $au + bv = 1_{\mathbb{A}}$ et pour tout $c \in \mathbb{A}$, on a $acu + bcv = c$, de sorte que si a divise bc, il va alors diviser $c = acu + bcv$. □

Théorème 4.11.

Soient $r \in \mathbb{N} \setminus \{0, 1\}$, $a_1, \cdots, a_r$ des éléments tous non nuls dans un anneau principal $\mathbb{A}$ et $\delta = a_1 \wedge \cdots \wedge a_r$. Il existe des éléments de $\mathbb{A}$, $a'_1, \cdots, a'_r$ premiers entre eux dans leur ensemble, tels que $a_k = \delta a'_k$ pour tout k compris entre 1 et r.

Preuve. Comme, pour tout k compris entre 1 et r, δ divise a_k, il existe $a'_k \in \mathbb{A}^*$ tel que $a_k = \delta a'_k$ et on a $\delta = \sum_{k=1}^{r} u_k a_k = \delta \sum_{k=1}^{r} u_k a'_k$ avec $\delta \neq 0$, ce qui entraîne $\sum_{k=1}^{r} u_k a'_k = 1$. □

On peut aussi justifier l'existence du ppcm dans un anneau principal en utilisant les idéaux.

Théorème 4.12.

Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \cdots, a_r$ des éléments tous non nuls dans un anneau principal $\mathbb{A}$. Il existe μ dans $\mathbb{A}$ tel que $(a_1) \cap \cdots \cap (a_r) = (\mu)$ et μ est ppcm *de $a_1, \cdots, a_r$.*

Preuve. L'existence de μ se déduit du fait que $(a_1) \cap \cdots \cap (a_r)$ est un idéal de l'anneau principal $\mathbb{A}$. Comme $\mu \in (\mu) \subset (a_k)$ pour tout k compris entre 1 et r, μ est multiple commun des a_k. Si m est un multiple commun de tous les a_k, il est alors dans l'idéal $(a_1) \cap \cdots \cap (a_r) = (\mu)$, donc multiple de μ. □

Corollaire 4.4. *Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \cdots, a_r$ des éléments tous non nuls dans un anneau principal $\mathbb{A}$. Si les a_k, pour k compris entre 1 et r, sont deux à deux premiers entre eux, on a alors* $\text{ppcm}(a_1, \cdots, a_r) = \prod_{k=1}^{r} a_k$ *à une unité près.*

Preuve. Il s'agit de montrer que pour $a_1, \cdots, a_r$ deux à deux premiers entre eux, on a $\bigcap_{k=1}^{r} (a_k) = \left(\prod_{k=1}^{r} a_k\right)$, ce qui peut se faire par récurrence sur $r \geq 2$. Comme $a_1 a_2$ est multiple de a_1 et a_2, on a toujours $(a_1 a_2) \subset (a_1) \cap (a_2)$. Tout a dans $(a_1) \cap (a_2)$ s'écrit $a = q_1 a_1 = q_2 a_2$, donc a_1 divise $q_2 a_2$ en étant premier avec a_2, ce qui impose que a_1 divise q_2, soit $q_2 = q_3 a_1$ et $a = q_2 a_2 = q_3 a_1 a_2$ est dans $(a_1 a_2)$, ce qui nous donne l'égalité $(a_1 a_2) = a(a_1) \cap (a_2)$. Supposant le résultat acquis pour $r \geq 2$, soient $a_1, \cdots, a_{r+1}$ deux à deux premiers entre eux dans $\mathbb{A}^*$. Comme a_{r+1} est premier avec tous les a_k, pour k compris entre 1 et r, il est premier avec le produit $\prod_{k=1}^{r} a_k$ et $\left(\prod_{k=1}^{r+1} a_k\right) = \left(\prod_{k=1}^{r} a_k\right) \cap (a_{r+1}) = \bigcap_{k=1}^{r+1} (a_k)$. □

4.3 Le théorème chinois

Pour ce paragraphe, l'anneau $\mathbb{A}$ est supposé principal, on se donne une suite $(a_j)_{1 \leq j \leq r}$ de $r \geq 2$ éléments non nuls et non inversibles de $\mathbb{A}$ et on note $a = \prod_{j=1}^{r} a_j$.

Pour tout indice j compris entre 1 et r, π_j désigne la surjection canonique de $\mathbb{A}$ sur l'anneau quotient $\dfrac{\mathbb{A}}{(a_j)}$.

Le produit cartésien $\prod_{j=1}^{r} \dfrac{\mathbb{A}}{(a_j)}$ est naturellement muni d'une structure d'anneau commutatif unitaire avec les lois $+$ et $\cdot$ définies par :

$$\begin{cases} (\pi_j(x_j))_{1 \leq j \leq r} + (\pi_j(y_j))_{1 \leq j \leq r} = (\pi_j(x_j + y_j))_{1 \leq j \leq r} \\ (\pi_j(x_j))_{1 \leq j \leq r} \cdot (\pi_j(y_j))_{1 \leq j \leq r} = (\pi_j(x_j \cdot y_j))_{1 \leq j \leq r} \end{cases}$$

On note π la surjection canonique de $\mathbb{A}$ sur l'anneau quotient $\dfrac{\mathbb{A}}{(a)}$.

On désigne par $(b_j)_{1\leq j\leq r}$ la suite d'éléments de $\mathbb{A}$ définie par $b_j = \dfrac{a}{a_j} = \prod_{\substack{i=1\\ i\neq j}}^{r} a_i$ pour $1 \leq j \leq r$.

Lemme 4.9 *Si les a_j, pour j compris entre 1 et r, sont deux à deux premiers entre eux, les b_j, pour j compris entre 1 et r, sont alors premiers entre eux dans leur ensemble.*

Preuve. Si les b_j ne sont pas premiers entre eux dans leur ensemble, il existe alors un élément premier p de $\mathbb{A}$ qui divise tous les b_j (l'anneau $\mathbb{A}$ étant principal est factoriel). Comme p divise $b_1 = \prod_{i=2}^{r} a_i$, il divise un a_i pour $2 \leq i \leq r$, mais divisant b_i, il divise un a_k pour $1 \leq k \neq i \leq r$, ce qui contredit le fait que a_i et a_k sont premiers entre eux. □

Théorème 4.13. Chinois

Supposant les a_j, pour $1 \leq j \leq r$, deux à deux premiers entre eux, l'application $\varphi : x \in \mathbb{A} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \prod_{j=1}^{r} \dfrac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux surjectif de noyau $\ker(\varphi) = \left(\prod_{j=1}^{r} a_j\right)$ et φ induit un isomorphisme d'anneaux $\overline{\varphi} : \pi(x) \in \dfrac{\mathbb{A}}{\left(\prod_{j=1}^{r} a_j\right)} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \prod_{j=1}^{r} \dfrac{\mathbb{A}}{(a_j)}$ d'inverse $\overline{\varphi}^{-1} : (\pi_j(x_j))_{1\leq j\leq r} \in \prod_{j=1}^{r} \dfrac{\mathbb{A}}{(a_j)} \mapsto \overline{\sum_{i=1}^{r} x_i u_i b_i} \in \dfrac{\mathbb{A}}{\left(\prod_{j=1}^{r} a_j\right)}$ où $(u_j)_{1\leq j\leq r}$ est une suite d'éléments de $\mathbb{A}$ telle que $\sum_{j=1}^{r} u_j b_j = 1$.

Preuve. Il est clair que $\varphi : x \in \mathbb{A} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \prod_{j=1}^{r} \dfrac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux. Son noyau est formé des multiples de tous les a_j, donc de leur ppcm $a = \prod_{j=1}^{r} a_j$ puisque les a_j sont deux à deux premiers entre eux. Comme les $b_i = \dfrac{a}{a_i}$ sont premiers entre eux dans leur ensemble (lemme précédent), le théorème de Bézout nous dit qu'il existe une suite $(u_i)_{1\leq i\leq r}$ d'éléments de $\mathbb{A}$ telle que $\sum_{i=1}^{r} u_i b_i = 1$. Pour $1 \leq j \leq r$, on a $\pi_j(b_i) = \pi_j(0)$ pour $i \neq j$ puisque b_i est multiple de a_j, ce

qui nous donne $\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i b_i\right) = \pi_j(u_j)\,\pi_j(b_j)$. Donc $\pi_j(b_j)$ est inversible dans $\dfrac{\mathbb{A}}{(a_j)}$ d'inverse $\pi_j(u_j)$). Pour $(\pi_j(x_j))_{1\leq j\leq r}$ donné dans $\prod_{j=1}^{r}\dfrac{\mathbb{A}}{(a_j)}$, en posant $x = \sum_{i=1}^{r} x_i u_i b_i$, on a $\pi_j(x) = \pi_j(x_j)\,\pi_j(u_j)\,\pi_j(b_j) = \pi_j(x_j)$ pour tout j compris entre 1 et r, soit $\varphi(x) = (\pi_j(x_j))_{1\leq j\leq r}$. Le morphisme φ est donc surjectif et il se factorise en un isomorphisme :

$$\begin{array}{rccc} \overline{\varphi}: & \dfrac{\mathbb{A}}{\left(\prod_{j=1}^{r} a_j\right)} = \dfrac{\mathbb{A}}{\ker(\varphi)} & \to & \prod_{j=1}^{r}\dfrac{\mathbb{A}}{(a_j)} \\ & \pi(x) & \mapsto & (\pi_j(x))_{1\leq j\leq r} \end{array}$$

Avec la surjectivité, on a prouvé que l'inverse de $\overline{\varphi}$ est défini par :

$$\begin{array}{rccc} \overline{\varphi}^{-1}: & \prod_{j=1}^{r}\dfrac{\mathbb{A}}{(a_j)} & \to & \dfrac{\mathbb{A}}{\left(\prod_{j=1}^{r} a_j\right)} \\ & (\pi_j(x_j))_{1\leq j\leq r} & \mapsto & \overline{\sum_{i=1}^{r} x_i u_i b_i} \end{array}$$

□

4.4 Nombres algébriques et transcendants

Si $\mathbb{K}$ et $\mathbb{L}$ sont deux corps commutatifs tels que $\mathbb{K}\subset\mathbb{L}$, on dit alors que $\mathbb{L}$ est une *extension* de $\mathbb{K}$. Une extension $\mathbb{L}$ du corps commutatif $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$. Sa dimension est appelée *degré de l'extension* et est notée $[\mathbb{L}:\mathbb{K}]$.

Le lemme qui suit nous sera utile.

Lemme 4.10 *Si $\mathbb{K}\subset\mathbb{M}\subset\mathbb{L}$ sont trois corps commutatif, l'extension $\mathbb{K}\subset\mathbb{L}$ est de degré fini si, et seulement si, les extensions $\mathbb{K}\subset\mathbb{M}$ et $\mathbb{M}\subset\mathbb{L}$ sont de degrés finis et dans ce cas, on a $[\mathbb{L}:\mathbb{K}] = [\mathbb{L}:\mathbb{M}]\,[\mathbb{M}:\mathbb{K}]$.*

Preuve. Si les extensions $\mathbb{K}\subset\mathbb{M}$ et $\mathbb{M}\subset\mathbb{L}$ sont de degrés finis, on dispose alors d'une base $(e_i)_{1\leq i\leq p}$ du $\mathbb{K}$-espace vectoriel $\mathbb{M}$ et d'une base $(f_j)_{1\leq j\leq q}$ du $\mathbb{M}$-espace vectoriel $\mathbb{L}$. Tout $x\in\mathbb{L}$ s'écrit $x = \sum_{j=1}^{q} x_j f_j$, chaque $x_j\in\mathbb{M}$ s'écrivant $x_j = \sum_{i=1}^{p} x_{ij} e_i$ où les $x_{ij}\in\mathbb{K}$, donc $x = \sum_{\substack{1\leq i\leq p\\ 1\leq j\leq q}} x_{ij} e_i f_j$, ce qui nous dit que $(e_i f_j)_{\substack{1\leq i\leq p\\ 1\leq j\leq q}}$ est un système générateur du $\mathbb{K}$-espace vectoriel $\mathbb{L}$ qui est donc de dimension finie. Si

$\sum_{\substack{1\leq i\leq p\\1\leq j\leq q}} x_{ij}e_if_j = 0$, les x_{ij} étant dans $\mathbb{K}$, on a alors $\sum_{j=1}^{q}\left(\sum_{i=1}^{p}x_{ij}e_i\right)f_j = 0$ où les $\sum_{i=1}^{p}x_{ij}e_i$ sont dans $\mathbb{M}$, ce qui implique que $\sum_{i=1}^{p}x_{ij}e_i = 0$ pour tout j compris entre 1 et q et entraîne la nullité de tous les x_{ij}. En définitive la famille $(e_if_j)_{\substack{1\leq i\leq p\\1\leq j\leq q}}$ est libre et c'est une base du $\mathbb{K}$-espace vectoriel $\mathbb{L}$. On a donc $[\mathbb{L}:\mathbb{K}] = pq = [\mathbb{L}:\mathbb{M}]\,[\mathbb{M}:\mathbb{K}]$.

Réciproquement, si $[\mathbb{L}:\mathbb{K}]$ est fini, de l'inclusion $\mathbb{M}\subset\mathbb{L}$ entre $\mathbb{K}$-espaces vectoriels, on déduit que $[\mathbb{M}:\mathbb{K}]$ est fini. Une base $(g_k)_{1\leq k\leq n}$ du $\mathbb{K}$-espace vectoriel $\mathbb{L}$ étant aussi une famille génératrice du $\mathbb{M}$-espace vectoriel $\mathbb{L}$, il en résulte que $[\mathbb{L}:\mathbb{M}]$ est fini. □

On se donne une extension $\mathbb{L}$ d'un corps commutatif $\mathbb{K}$.

Pour tout $\alpha\in\mathbb{L}$, *l'application d'évaluation* $\varphi_\alpha : P\in\mathbb{K}[X]\mapsto P(\alpha)\in\mathbb{L}$ est un morphisme d'anneaux d'image $\mathbb{K}[\alpha] = \{P(\alpha),\ P\in\mathbb{K}[X]\}$ qui est un sous-anneau de $\mathbb{L}$ (c'est le plus petit sous-anneau de $\mathbb{L}$ qui contient $\mathbb{K}$ et α) et de noyau $\mathcal{I}_\alpha = \{P\in\mathbb{K}[X],\ P(\alpha)=0\}$ qui est un idéal de $\mathbb{K}[X]$. Cet idéal est *l'idéal annulateur* de α.

On note $\mathbb{K}(\alpha)$ le plus petit sous-corps de $\mathbb{L}$ qui contient $\mathbb{K}$ et α, à savoir l'intersection de tous les sous-corps de $\mathbb{L}$ qui contiennent $\mathbb{K}$ et α. Ce sous-corps contient l'anneau $\mathbb{K}[\alpha]$.

Plus généralement, pour toute suite $(\alpha_k)_{1\leq k\leq n}$ de $n\geq 1$ éléments de $\mathbb{L}$, on note $\mathbb{K}[\alpha_1,\cdots,\alpha_n] = \{P(\alpha_1,\cdots,\alpha_n),\ P\in\mathbb{K}[X_1,\cdots,X_n]\}$ le sous-anneau de $\mathbb{L}$ qui est l'image du morphisme d'anneaux $P\in\mathbb{K}[X_1,\cdots,X_n]\mapsto P(\alpha_1,\cdots,\alpha_n)\in\mathbb{L}$ et $\mathbb{K}(\alpha_1,\cdots,\alpha_n)$ le plus petit sous-corps de $\mathbb{L}$ qui contient $\mathbb{K}$ et $\alpha_1,\cdots,\alpha_n$. C'est l'intersection de tous les sous-corps de $\mathbb{L}$ qui contiennent $\mathbb{K}$ et $\alpha_1,\cdots,\alpha_n$ et il contient $\mathbb{K}[\alpha_1,\cdots,\alpha_n]$.

Pour $n\geq 2$ et toute partition $\{1,\cdots,n\} = \{j_1,\cdots,j_p\}\cup\{k_1,\cdots,k_{n-p}\}$, on a $\mathbb{K}\subset\mathbb{K}\left(\alpha_{j_1},\cdots,\alpha_{j_p}\right)\subset\mathbb{K}(\alpha_1,\cdots,\alpha_n)$ et :

$$\mathbb{K}(\alpha_1,\cdots,\alpha_n) = \mathbb{K}\left(\alpha_{j_1},\cdots,\alpha_{j_p}\right)\left(\alpha_{k_1},\cdots,\alpha_{k_{n-p}}\right)$$

Définition 4.6. *On dit qu'un élément α de $\mathbb{L}$ est* algébrique *sur $\mathbb{K}$ si son idéal annulateur $\mathcal{I}_\alpha$ n'est pas réduit à $\{0\}$. Un élément de $\mathbb{L}$ qui n'est pas algébrique sur $\mathbb{K}$ est dit* transcendant *sur $\mathbb{K}$.*

Pour la suite de ce paragraphe, $\mathbb{L}$ est le corps $\mathbb{C}$ des nombres complexes et $\mathbb{K}$ est un sous-corps de $\mathbb{C}$. Un tel corps $\mathbb{K}$ contient nécessairement $\mathbb{Q}$.

Dire que $\alpha\in\mathbb{C}$ est algébrique sur $\mathbb{K}$ revient donc à dire qu'il existe P dans $\mathbb{K}[X]\setminus\{0\}$ tel que $P(\alpha)=0$. Un tel polynôme annulateur P est non constant et peut être pris unitaire en divisant tous ses coefficients par son coefficient dominant. Pour $\mathbb{K}=\mathbb{Q}$ il peut être pris dans $\mathbb{Z}[X]\setminus\{0\}$ en le multipliant par le ppcm des dénominateurs de tous ses coefficients.

On note $\overline{\mathbb{K}}$ l'ensemble de tous les nombres complexes algébriques sur $\mathbb{K}$.

En écrivant que $\mathbb{Q}[X] = \bigcup_{n\in\mathbb{N}}\mathbb{Q}_n[X]$, on déduit que $\mathbb{Q}[X]$ est dénombrable, soit $\mathbb{Q}[X] = \{P_k,\ k\in\mathbb{N}\}$, les P_k étant des polynômes à coefficients rationnels.

Donc l'ensemble $\overline{\mathbb{Q}} = \bigcup_{k\in\mathbb{N}} P_k^{-1}\{0\}$ des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable et l'ensemble $\mathbb{C}\setminus\overline{\mathbb{Q}}$ des nombres complexes transcendants est infini non dénombrable.

Exemples 4.4

- *Pour tous $n\in\mathbb{N}^*$ et $r\in\mathbb{Q}_+^*$, $\sqrt[n]{r}$ est algébrique sur $\mathbb{Q}$.*
- *Le nombre complexe i est algébrique sur $\mathbb{Q}$ et sur $\mathbb{R}$.*
- *Les réels e et π sont transcendants sur $\mathbb{Q}$.*
- *Pour tout $n\in\mathbb{N}^*$, $\zeta(2n) = r_n\pi^{2n}$ où $r_n\in\mathbb{Q}_+^*$, est transcendant sur $\mathbb{Q}$.*

On peut admettre le résultat suivant de démonstration difficile.

Théorème 4.14. Hermite-Lindemann

Pour tout nombre algébrique non nul α, le réel e^α est transcendant.

Exemples 4.5 *Les nombres e, π et $\zeta(2p) = r\pi^{2p}$ où $r\in\mathbb{Q}_+^*$ sont transcendants, cela pouvant aussi se justifier sans le théorème précédent.*

Théorème 4.15.

Si $\alpha\in\mathbb{C}$ est algébrique sur $\mathbb{K}$, il existe alors un unique polynôme unitaire $P_\alpha\in\mathbb{K}[X]$ tel que $\mathcal{I}_\alpha = (P_a)$ et ce polynôme P_α est l'unique polynôme unitaire irréductible de $\mathbb{K}[X]$ qui annule α. De plus, P_α est non constant et ses racines complexes sont toutes simples.

Preuve. Pour tout $\alpha\in\mathbb{C}$, l'ensemble $\mathcal{I}_\alpha = \ker(\varphi_\alpha)$ est un idéal de l'anneau principal $\mathbb{K}[X]$. Dans le cas où α est algébrique sur $\mathbb{K}$, cet idéal n'est pas réduit à $\{0\}$ et il existe un unique polynôme unitaire non nul $P_\alpha\in\mathbb{K}[X]$ tel que $\mathcal{I}_\alpha = (P_a)$ (théorème **??**).

On rappelle que P_α est le polynôme unitaire de $\mathcal{I}_\alpha$ de degré minimum, ce qui implique qu'un polynôme non nul de degré strictement inférieur à celui de P_α ne peut annuler α.

Si $P_\alpha = QR$ avec Q, R dans $\mathbb{K}[X]$, on a alors $Q(\alpha)R(\alpha) = 0$ et $Q(\alpha) = 0$ ou $R(\alpha) = 0$, ce qui équivaut à dire que Q ou R est dans l'idéal $\mathcal{I}_\alpha$. Ces polynômes étant de degré inférieur ou égal à celui de P_α, l'un des deux est nécessairement constant. On a donc ainsi prouvé que P_α est irréductible dans $\mathbb{K}[X]$. Réciproquement si P est un polynôme unitaire irréductible de $\mathbb{K}[X]$ qui annule α, il est alors dans $\mathcal{I}_\alpha$, donc proportionnel à P_α et nécessairement égal à P_α puisque irréductible et unitaire. D'où l'unicité.

Le polynôme P_α qui est unitaire et annule α est non constant, donc de degré au moins égal à 1. Comme P_α est irréductible dans $\mathbb{K}[X]$, il est premier avec son polynôme dérivé $P'_\alpha\in\mathbb{K}[X]$, donc d'après le théorème de Bézout, il existe U, V dans $\mathbb{K}[X]$ tel que $UP_\alpha + VP'_\alpha = 1$, ce qui implique que P_α et P'_α ne peuvent avoir de racine complexe en commun. Les racines complexes de P_α sont donc toutes simples. □

Avec les hypothèses et notations du théorème précédent, on dit que P_α est le *polynôme minimal* de α et son degré est le degré de α sur $\mathbb{K}$. Il est noté $d(\alpha, \mathbb{K})$.

Pour tout $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{K}$ de degré $d = d(\alpha, \mathbb{K}) \geq 2$, en notant $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_d$ les d racines complexes (distinctes, car toutes simples) de P_α et $\sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq d} \alpha_{i_1} \cdots \alpha_{i_k}$ pour $1 \leq k \leq d$ les fonctions symétriques élémentaires correspondantes, des égalités dans $\mathbb{C}[X]$:

$$P_\alpha(X) = X^d + \sum_{k=0}^{d-1} a_k X^k = \prod_{k=1}^{d} (X - \alpha_k) = X^d + \sum_{k=1}^{d} (-1)^k \sigma_k X^{d-k}$$

(théorème **??**), on déduit que les $\sigma_k = (-1)^k a_{d-k}$ sont tous dans $\mathbb{K}$.

Les zéros $\alpha_2, \cdots, \alpha_d$ de P_α sont les *conjugués* de α. Ce sont des nombres algébriques sur $\mathbb{K}$ de même polynôme minimal P_α.

Lemme 4.11 *Pour tout $\alpha \in \mathbb{C}$, on a :*

$$(\alpha \in \mathbb{K}) \Leftrightarrow (\mathbb{K}[\alpha] = \mathbb{K}) \Leftrightarrow (d(\alpha, \mathbb{K}) = 1)$$

Preuve. Il est clair que pour tout $\alpha \in \mathbb{C}$ on a $\mathbb{K} \subset \mathbb{K}[\alpha]$. Si $\alpha \in \mathbb{K}$, on a alors $P(\alpha) \in \mathbb{K}$ pour tout $P \in \mathbb{K}[X]$ puisque $\mathbb{K}$ est un corps, ce qui implique que $\mathbb{K}[\alpha] = \mathbb{K}$. Si $\mathbb{K}[\alpha] = \mathbb{K}$, on a alors $\alpha \in \mathbb{K}$ et il est annulé par $X - \alpha$ qui est unitaire irréductible dans $\mathbb{K}[X]$, donc α est algébrique sur $\mathbb{K}$ de polynôme minimal $X - \alpha$ et $d(\alpha, \mathbb{K}) = 1$. Dire que $d(\alpha, \mathbb{K}) = 1$ signifie que α est algébrique sur $\mathbb{K}$ de polynôme minimal $P_\alpha(X) = X + c \in \mathbb{K}[X]$, donc $\alpha = -c \in \mathbb{K}$. □

Le théorème qui suit peut être utilisé pour donner des exemples de nombres transcendants sur $\mathbb{Q}$.

Théorème 4.16. Liouville

Si α est un nombre algébrique sur $\mathbb{Q}$ de degré $d \geq 1$, il existe alors un réel $C_\alpha > 0$ telle que pour tout nombre rationnel $\frac{p}{q} \neq \alpha$ où $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a $\left|\alpha - \frac{p}{q}\right| \geq \frac{C_\alpha}{q^d}$.

Preuve. Pour $d = 1$, α est rationnel, soit $\alpha = \frac{a}{b}$ avec$(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Pour $r = \frac{p}{q} \in \mathbb{Q}$ distinct de α on a $0 < \left|\alpha - \frac{p}{q}\right| = \frac{|aq - bp|}{qb}$, donc $|aq - bp| \neq 0$ dans $\mathbb{N}$, ce qui équivaut à $|aq - bp| \geq 1$. On a donc $\left|\alpha - \frac{p}{q}\right| = \frac{|aq - bp|}{qb} \geq \frac{1}{b}\frac{1}{q}$.

Pour $d \geq 2$, le nombre α est irrationnel d'après le lemme 4.11. En notant P_α son polynôme minimal, il existe un entier naturel non nul n tel que $Q_\alpha = nP_\alpha \in \mathbb{Z}[X]$ et pour tout rationnel $r = \frac{p}{q}$, on a $q^d Q_\alpha(r) \in \mathbb{Z}$. De plus cet entier est non nul. En effet si $q^d Q_\alpha(r) = 0$, alors r est racine de Q_α et on a $Q_\alpha(X) = (X - r) R(X)$ avec $X - r$ et R dans $\mathbb{Q}[X]$ non constants (on a $d \geq 2$), en contradiction avec P_α irréductible dans $\mathbb{Q}[X]$. On a donc $\left|q^d (Q_\alpha(\alpha) - Q_\alpha(r))\right| = \left|q^d Q_\alpha(r)\right| \geq 1$.

D'autre part, le théorème des accroissements finis nous dit qu'il existe un réel s strictement compris entre α et r tel que $Q_\alpha(\alpha) - Q_\alpha(r) = (\alpha - r) Q'_\alpha(s)$. On distingue alors deux cas : soit $|\alpha - r| \leq 1$ et dans ce cas on a $s \in [\alpha - 1, \alpha + 1]$ de sorte que :

$$1 \leq \left|q^d Q_\alpha(r)\right| = q^d |\alpha - r| \, |Q'_\alpha(s)| \leq \left(\sup_{s \in [\alpha-1, \alpha+1]} |Q'_\alpha(s)| \right) q^d |\alpha - r|$$

donc $C_1 = \sup_{s \in [\alpha-1, \alpha+1]} |Q'_\alpha(s)| > 0$ et $|\alpha - r| \geq \dfrac{1}{C_1} \dfrac{1}{q^d}$; soit $|\alpha - r| > 1$ et dans ce cas on a $|\alpha - r| > \dfrac{1}{q^d}$. En posant $C_\alpha = \min\left(1, \dfrac{1}{C_1}\right)$, on a alors $\left|\alpha - \dfrac{p}{q}\right| \geq \dfrac{C_\alpha}{q^d}$. □

Corollaire 4.5. *Pour toute suite $(a_n)_{n \in \mathbb{N}^*}$ d'entiers compris entre 0 et 9 telle que a_n soit non nul à partir d'un certain rang, le réel $\xi = \sum_{n=1}^{+\infty} \dfrac{a_n}{10^{n!}}$ est transcendant.*

Preuve. Soit $n_0 \in \mathbb{N}^*$ tel que $a_n \neq 0$ pour tout $n \geq n_0$. En notant $p = 10^{k!} \sum_{n=1}^{k} \dfrac{a_n}{10^{n!}}$ et $q = 10^{k!}$ pour $k \geq n_0$, on a :

$$0 < \left|\xi - \frac{p}{q}\right| = \sum_{n=k+1}^{+\infty} \frac{a_n}{10^{n!}} \leq \frac{9}{10^{(k+1)!}} \sum_{n=0}^{+\infty} \frac{1}{10^n} = \frac{9}{10^{(k+1)!}} \frac{10}{9} \leq \frac{1}{q^k}$$

Si ξ est algébrique de degré $d \geq 1$, il existe alors un réel $C_\xi > 0$ tel que l'on ait $\dfrac{C_\xi}{q^d} \leq \left|\xi - \dfrac{p}{q}\right| \leq \dfrac{1}{q^k}$, soit $C_\xi \leq \dfrac{1}{q^{k-d}}$ pour tout $k \geq n_0$, ce qui conduit à une absurdité et faisant tendre k vers l'infini. En conclusion ξ est transcendant. □

On peut utiliser le corollaire précédent pour montrer qu'il y a autant de nombres transcendants que de réels. Pour ce faire on utilise l'application qui associe à $\xi = \sum_{n \in \mathbb{N}^*} \dfrac{a_n}{10^{n!}}$ le réel $\sum_{n \in \mathbb{N}^*} \dfrac{a_n}{10^n} \in]0, 1[$ et on vérifie que c'est une bijection (si $x \in]0, 1[$ est décimal on utilise son écriture décimale impropre comportant une infinité de 9).

En exploitant les propriétés de la matrice compagnon de P_α pour $\alpha \in \overline{\mathbb{K}}$, on peut vérifier que $\mathbb{K}[\alpha]$ est contenu dans $\overline{\mathbb{K}}$, ce que l'on retrouvera avec le fait que $\overline{\mathbb{K}}$ est un corps. Voir le paragraphe **??** pour plus de détails sur les matrices compagnons.

Précisément, on a le résultat suivant.

Théorème 4.17.

Si $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{K}$, il en est alors de même de $P(\alpha)$ pour tout polynôme $P \in \mathbb{K}[X]$ et en notant $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_d$ les racines complexes

de P_α, le polynôme minimal de $P(\alpha)$ est un diviseur de $\prod_{k=1}^{d}(X-P(\alpha_k))$ qui est dans $\mathbb{K}[X]$.

Preuve. Si α est algébrique sur $\mathbb{K}$ de degré 1, on a alors $\mathbb{K}[\alpha]=\mathbb{K}\subset\overline{\mathbb{K}}$.

Pour $\alpha\in\mathbb{C}$ algébrique sur $\mathbb{K}$ de degré $d=d(\alpha,\mathbb{K})\geq 2$, en associant à son polynôme minimal $P_\alpha(X)=X^d-\sum_{k=0}^{d-1}a_kX^k\in\mathbb{K}[X]$ sa matrice compagnon :

$$C_\alpha=\begin{pmatrix}0&\cdots&0&a_0\\1&\ddots&\vdots&a_1\\\vdots&\ddots&0&\vdots\\0&\cdots&1&a_{d-1}\end{pmatrix}\in\mathcal{M}_d(\mathbb{K})$$

on sait que P_α est le polynôme caractéristique et le polynôme minimal de C_α (théorème **??**). La matrice C_α dont le polynôme caractéristique est scindé à racines simples dans $\mathbb{C}$ (théorème 4.15) est diagonalisable, donc il existe $R\in GL_d(\mathbb{C})$ et $D\in\mathcal{M}_d(\mathbb{C})$ diagonale de termes diagonaux $\alpha_1,\cdots,\alpha_d$ telles que $C_\alpha=RDR^{-1}$. Il en résulte que $C_\alpha^k=RD^kR^{-1}$ pour tout $k\in\mathbb{N}$ et $P(C_\alpha)=RP(D)R^{-1}$ par linéarité pour tout polynôme $P\in\mathbb{K}[X]$, la matrice $P(D)$ étant diagonale de termes diagonaux $P(\alpha_1),\cdots,P(\alpha_d)$. Le polynôme caractéristique de la matrice $P(C_\alpha)$ est donc $\chi_{P(C_\alpha)}(X)=\prod_{k=1}^{d}(X-P(\alpha_k))$, ce polynôme étant dans $\mathbb{K}[X]$ puisque $P(C_\alpha)\in\mathcal{M}_d(\mathbb{K})$. Donc tout élément $P(\alpha)$ de $\mathbb{K}[\alpha]$ est algébrique sur $\mathbb{K}$ de polynôme minimal qui divise $\prod_{k=1}^{d}(X-P(\alpha_k))$ dans $\mathbb{K}[X]$. Le degré de $P(\alpha)$ est donc au plus égal à $d(\alpha,\mathbb{K})$. □

On peut remarquer que la matrice compagnon C_α est la matrice de l'endomorphisme $z\in\mathbb{K}[\alpha]\mapsto\alpha z\in\mathbb{K}[\alpha]$ dans la base $\left(\alpha^k\right)_{0\leq k\leq d-1}$ du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$.

On déduit du théorème précédent que pour tout $P\in\mathbb{K}[X]$, on a $\sum_{k=1}^{d}P(\alpha_k)\in\mathbb{K}$ (cette somme est l'opposé du coefficient de X^{d-1} dans $\prod_{k=1}^{d}(X-P(\alpha_k))\in\mathbb{K}[X]$). En particulier, on a $\sum_{k=1}^{d}\alpha_k^j\in\mathbb{K}$ pour tout $j\in\mathbb{N}$.

Théorème 4.18.

Pour tout $\alpha\in\mathbb{C}$, on a :

$$\left(\alpha\in\overline{\mathbb{K}}\right)\Leftrightarrow\left(\mathbb{K}[\alpha]=\mathbb{K}(\alpha)\right)\Leftrightarrow\left([\mathbb{K}[\alpha]:\mathbb{K}]<+\infty\right)$$

Preuve. Pour tout $\alpha \in \mathbb{C}$, $\mathbb{K}(\alpha)$ est un sous-corps de $\mathbb{C}$ qui contient α et $\mathbb{K}$, donc il contient $\mathbb{K}[\alpha]$.

Supposons que α soit algébrique sur $\mathbb{K}$ de polynôme minimal P_α. Pour montrer que $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$, il nous suffit de montrer que l'anneau unitaire $\mathbb{K}[\alpha]$ est un corps (par définition de $\mathbb{K}(\alpha)$), ce qui revient à montrer que tout élément non nul de $\mathbb{K}[\alpha]$ est inversible dans $\mathbb{K}[\alpha]$. Tout $x \in \mathbb{K}[\alpha]$ s'écrit $x = P(\alpha)$ avec $P \in \mathbb{K}[X]$. Par division euclidienne on peut écrire que $P = P_\alpha Q + R$ avec $R = 0$ ou $R \neq 0$ et R de degré strictement inférieur à celui de P_α et on a $x = R(\alpha)$. Si x n'est pas nul, il en est de même de R qui est premier avec le polynôme irréductible P_α, le théorème de Bézout nous dit alors qu'il existe deux polynômes U, V dans $\mathbb{K}[X]$ tels que $UP_\alpha + VR = 1$ et on a $V(\alpha)R(a) = 1$, ce qui signifie que $R(a)$ est inversible dans $\mathbb{K}[\alpha]$ d'inverse $V(a)$.

On peut aussi utiliser le morphisme d'anneaux $\varphi_\alpha : P \in \mathbb{K}[X] \mapsto P(\alpha) \in \mathbb{C}$ qui a pour noyau $\mathcal{I}_\alpha = (P_a)$ et pour image $\mathbb{K}[\alpha]$. Par passage au quotient, on déduit un isomorphisme d'anneaux de $\dfrac{\mathbb{K}[X]}{(P_a)}$ sur $\mathbb{K}[\alpha]$ et pour α algébrique le polynôme P_α est irréductible, donc $\dfrac{\mathbb{K}[X]}{(P_a)}$ est un corps ainsi que $\mathbb{K}[\alpha]$.

Supposons que $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$, c'est-à-dire que $\mathbb{K}[\alpha]$ soit un corps. Si $\alpha = 0$, il est alors algébrique, sinon il est inversible dans $\mathbb{K}[\alpha]$ et il existe un polynôme $P \in \mathbb{K}[X]$ tel que $\alpha P(\alpha) = 1$ et le polynôme $XP(X) - 1 \in \mathbb{K}[X]$ annule α, ce qui signifie que α est algébrique sur $\mathbb{K}$. Par division euclidienne tout polynôme $P \in \mathbb{K}[X]$ s'écrit $P = P_\alpha Q + R$ et $P(\alpha) = R(\alpha)$ est combinaison linéaire de $1, \alpha, \cdots, \alpha^{d(\alpha,\mathbb{K})-1}$, une telle écriture étant unique. Le $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$ est donc de dimension finie égale à $d(\alpha, \mathbb{K})$.

Si $[\mathbb{K}[\alpha] : \mathbb{K}]$ est fini égale à d, la famille $\left(\alpha^k\right)_{0 \leq k \leq d}$ est alors liée, ce qui se traduit en disant qu'il existe un polynôme non nul P de degré au plus égal à d dans $\mathbb{K}[X]$ tel que $P(\alpha) = 0$, donc α est algébrique. □

La démonstration précédente nous dit en particulier que si α est algébrique sur $\mathbb{K}$ de degré $d_\alpha = d(\alpha, \mathbb{K})$, $\mathbb{K}[\alpha]$ est alors un corps et $[\mathbb{K}[\alpha] : \mathbb{K}] = d_\alpha$, une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$ étant $\left(\alpha^k\right)_{0 \leq k \leq d_\alpha - 1}$.

Pour α transcendant sur $\mathbb{K}$, l'application $\varphi_\alpha : P \mapsto P(\alpha)$ réalise un isomorphisme de $\mathbb{K}[X]$ sur $\mathbb{K}[\alpha]$ et le corps $\mathbb{K}(\alpha)$ est isomorphe à $\mathbb{K}(X)$.

Théorème 4.19.

L'ensemble $\overline{\mathbb{K}}$ des nombres complexes algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{K}$.

Preuve. Tout élément de $\mathbb{K}$ étant algébrique sur $\mathbb{K}$, on a $\mathbb{K} \subset \overline{\mathbb{K}} \subset \mathbb{C}$.

Pour vérifier que $\overline{\mathbb{K}}$ est un sous-corps de $\mathbb{C}$, il suffit de montrer que si α, β sont dans $\overline{\mathbb{K}}$ avec $\beta \neq 0$, alors $-\alpha$, $\dfrac{1}{\beta}$, $\alpha + \beta$ et $\alpha\beta$ sont aussi dans $\overline{\mathbb{K}}$.

Si $P(X)=\sum_{k=0}^{n}a_kX^k$ est un polynôme non nul dans $\mathbb{K}[X]$ qui annule α, alors le polynôme $Q(X)=\sum_{k=0}^{n}(-1)^k a_kX^k$ est non nul dans $\mathbb{K}[X]$ et $Q(-\alpha)=P(\alpha)=0$, c'est-à-dire que $-\alpha$ est dans $\overline{\mathbb{K}}$.

Pour ce qui est de $\alpha+\beta$ et $\alpha\beta$, il s'agit de montrer que les $\mathbb{K}$-espaces vectoriels $\mathbb{K}[\alpha+\beta]$ et $\mathbb{K}[\alpha\beta]$ sont de dimensions finies (théorème 4.18). Ces espaces étant contenus dans $\mathbb{K}[\alpha][\beta]$, il nous suffit de montrer que ce dernier est de dimension finie. Comme α est algébrique sur $\mathbb{K}$, $\mathbb{K}[\alpha]$ est un sous-corps de $\mathbb{C}$ et un $\mathbb{K}$-espace vectoriel de dimension finie. De plus si β est algébrique sur $\mathbb{K}$, il l'est également sur $\mathbb{K}[\alpha]$ et $\mathbb{K}[\alpha][\beta]$ est de dimension finie sur $\mathbb{K}[\alpha]$. Avec la propriété de multiplicativité des degrés (lemme 4.10), on en déduit que :

$$[\mathbb{K}[\alpha][\beta]:\mathbb{K}]=[\mathbb{K}[\alpha][\beta]:\mathbb{K}[\alpha]][\mathbb{K}[\alpha]:\mathbb{K}]<+\infty$$

Enfin, si $\beta\in\mathbb{C}^*$ est algébrique sur $\mathbb{K}$ de polynôme minimal $P_\beta(X)=\sum_{k=0}^{d}a_kX^k$. Le polynôme $Q(X)=X^dP_\beta\left(\frac{1}{X}\right)=\sum_{k=0}^{d}a_{d-k}X^k$ est non nul dans $\mathbb{K}[X]$ et on a $Q\left(\frac{1}{\beta}\right)=\frac{P_\beta(\beta)}{\beta^d}=0$, c'est-à-dire que $\frac{1}{\beta}$ est algébrique sur $\mathbb{K}$. Sachant que $\mathbb{K}[\beta]=\mathbb{K}(\beta)$ est un corps, on a $\frac{1}{\beta}\in\mathbb{K}[\beta]$. □

Avec le théorème précédent, on retrouve le fait que si $\alpha\in\mathbb{C}$ est algébrique sur $\mathbb{K}$, il en est alors de même de $P(\alpha)$ pour tout $P\in\mathbb{K}[X]$ (théorème 4.17).

Le fait que $\overline{\mathbb{K}}$ est un sous-anneau de $\mathbb{C}$ peut aussi se justifier en faisant apparaître les nombres algébriques comme valeurs propres d'une matrice à coefficients dans $\mathbb{K}$.

Pour tout $\alpha\in\overline{\mathbb{K}}$ de polynôme minimal $P_\alpha(X)=X^d-\sum_{k=0}^{d-1}a_kX^k\in\mathbb{K}[X]$, en notant $V_\alpha=\left(\alpha^k\right)_{0\leq k\leq d-1}$ dans $\mathbb{C}^d\setminus\{0\}$, on a $\alpha V_\alpha=A_\alpha V_\alpha$ en désignant par $A_\alpha=\begin{pmatrix}0&1&0&\cdots&0\\0&0&\ddots&\ddots&\vdots\\\vdots&\ddots&\ddots&\ddots&0\\0&\cdots&0&0&1\\a_0&\cdots&\cdots&\cdots&a_{d-1}\end{pmatrix}$ la transposée de la matrice compagnon C_α de P_α, donc pour $\beta\in\overline{\mathbb{K}}$ de degré d', en notant $V=\left(\beta^jV_\alpha\right)_{0\leq j\leq d'-1}$ dans $\mathbb{C}^{dd'}$, on a :

$$\alpha V=\left(\beta^jA_\alpha V_\alpha\right)_{0\leq j\leq d'-1}=\begin{pmatrix}A_\alpha&0&\cdots&0\\0&A_\alpha&\ddots&\vdots\\\vdots&\ddots&\ddots&0\\0&\cdots&0&A_\alpha\end{pmatrix}\begin{pmatrix}V_\alpha\\\beta V_\alpha\\\vdots\\0\\\beta^{d'-1}V_\alpha\end{pmatrix}=AV$$

où $A \in \mathcal{M}_{dd'}(\mathbb{K})$, ce qui nous dit que le vecteur V (qui est non nul) est vecteur propre de la matrice A associé à la valeur propre α. De manière analogue, on a :

$$\beta V = \begin{pmatrix} \beta V_\alpha \\ \beta^2 V_\alpha \\ \vdots \\ \beta^{d'-1} V_\alpha \\ \left(b_0 + b_1\beta + \cdots + b_{d'-1}\beta^{d'-1}\right) V_\alpha \end{pmatrix}$$
$$= \begin{pmatrix} 0 & I_d & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & I_d \\ b_0 I_d & \cdots & 0 & b_{d'-1} I_d \end{pmatrix} \begin{pmatrix} V_\alpha \\ \beta V_\alpha \\ \vdots \\ 0 \\ \beta^{d'-1} V_\alpha \end{pmatrix} = BV$$

c'est-à-dire que le vecteur V est vecteur propre de la matrice $B \in \mathcal{M}_{dd'}(\mathbb{K})$ associé à la valeur propre β.

On a donc $(A-B)V = (\alpha - \beta)V$ avec V non nul dans $\mathbb{C}^{dd'}$, ce qui signifie que $\alpha - \beta$ est une valeur propre de la matrice $A - B$, donc une racine du polynôme caractéristique χ_{A-B} qui est dans $\mathbb{K}[X]$ puisque $A - B \in \mathcal{M}_{dd'}(\mathbb{K})$. Il en résulte que $\alpha - \beta$ est algébrique. De même avec $(AB)V = (\alpha\beta)V$ on déduit que $\alpha\beta$ est algébrique. En conclusion $\overline{\mathbb{K}}$ est un sous-anneau de $\overline{\mathbb{K}}$.

Ce résultat peut aussi se justifier en utilisant la notion de résultant (voir le théorème 2.3).

Le théorème 4.18 se généralise comme suit.

Théorème 4.20.

Pour toute suite $(\alpha_k)_{1\leq k\leq n}$ de nombres complexes, on a :

$$\left((\alpha_k)_{1\leq k\leq n} \in \overline{\mathbb{K}}^n\right) \Leftrightarrow (\mathbb{K}[\alpha_1, \cdots, \alpha_n] = \mathbb{K}(\alpha_1, \cdots, \alpha_n))$$
$$\Leftrightarrow ([\mathbb{K}[\alpha_1, \cdots, \alpha_n] : \mathbb{K}] < +\infty)$$

Preuve. On procède par récurrence sur l'entier $n \geq 1$. Pour $n = 1$, c'est le théorème 4.18. En supposant le résultat acquis au rang $n-1 \geq 1$, on se donne une suite $(\alpha_k)_{1\leq k\leq n}$ de $n \geq 2$ nombres complexes.

Si les α_k, pour $1 \leq k \leq n$, sont algébriques sur $\mathbb{K}$, on a alors $\mathbb{K}[\alpha_1] = \mathbb{K}(\alpha_1)$ et les α_k, pour $2 \leq k \leq n$, sont algébriques sur $\mathbb{K}(\alpha_1)$ puisque ce corps contient $\mathbb{K}$, donc le théorème précédent et l'hypothèse de récurrence appliquée au corps $\mathbb{K}(\alpha_1)$ nous permettent d'écrire que :

$$\mathbb{K}[\alpha_1, \cdots, \alpha_n] = \mathbb{K}[\alpha_1][\alpha_2, \cdots, \alpha_n] = \mathbb{K}(\alpha_1)[\alpha_2, \cdots, \alpha_n]$$
$$= \mathbb{K}(\alpha_1)(\alpha_2, \cdots, \alpha_n) = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$$

Supposons que $\mathbb{K}[\alpha_1, \cdots, \alpha_n] = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$. Si $\alpha_n = 0$, il est alors algébrique sur $\mathbb{K}(\alpha_1, \cdots, \alpha_{n-1})$, sinon il est inversible dans le corps $\mathbb{K}[\alpha_1, \cdots, \alpha_n]$ et il existe $P \in \mathbb{K}[X_1, \cdots, X_n] \setminus \{0\}$ tel que $\alpha_n P(\alpha_1, \cdots, \alpha_n) = 1$, ce qui nous dit

que α_n est annulé par $XP(\alpha_1,\cdots,\alpha_{n-1},X)-1\in\mathbb{K}(\alpha_1,\cdots,\alpha_{n-1})[X]\setminus\{0\}$, soit qu'il est algébrique sur $\mathbb{K}(\alpha_1,\cdots,\alpha_{n-1})$ et le théorème précédent nous dit que :

$$[\mathbb{K}[\alpha_1,\cdots,\alpha_n]:\mathbb{K}]=[\mathbb{K}(\alpha_1,\cdots,\alpha_n):\mathbb{K}]=[\mathbb{K}(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n):\mathbb{K}]<+\infty$$

Si $[\mathbb{K}[\alpha_1,\cdots,\alpha_n]:\mathbb{K}]<+\infty$, on déduit des inclusions $\mathbb{K}[\alpha_k]\subset\mathbb{K}[\alpha_1,\cdots,\alpha_n]$ entre $\mathbb{K}$-espaces vectoriels pour $1\leq k\leq n$, que les α_k sont tous algébriques sur $\mathbb{K}$. □

Le théorème précédent peut être utilisé pour vérifier que $\overline{\mathbb{K}}$ est un sous-anneau de $\mathbb{C}$. Si α,β sont dans $\overline{\mathbb{K}}$, on a alors $[\mathbb{K}[\alpha,\beta]:\mathbb{K}]<+\infty$, donc $\mathbb{K}[\alpha-\beta]$ et $\mathbb{K}[\alpha\beta]$ qui sont des $\mathbb{K}$-sous-espace vectoriel de $\mathbb{K}[\alpha,\beta]$ sont aussi de dimension finie sur $\mathbb{K}$, ce qui implique qu'ils sont algébriques sur $\mathbb{K}$.

Pour $\alpha\in\mathbb{C}$ algébrique sur $\mathbb{K}$ de degré $d_\alpha=d(\alpha,\mathbb{K})$, le corps :

$$\mathbb{K}[\alpha]=\left\{\sum_{k=0}^{d_\alpha-1}a_k\alpha^k,\ (a_k)_{0\leq k\leq d_\alpha-1}\in\mathbb{K}^{d_\alpha}\right\}$$

est une *extension de degré fini* de $\mathbb{K}$. Pour $\mathbb{K}=\mathbb{Q}$, on dit que c'est un *corps de nombres* de degré d_α.

Réciproquement, on peut montrer que si $\mathbb{L}$ est un extension de degré fini de $\mathbb{K}$, il existe alors un nombre algébrique α sur $\mathbb{K}$ tel que $\mathbb{L}=\mathbb{K}[\alpha]$.

Lemme 4.12 *Pour tous α,β dans $\overline{\mathbb{K}}$, il existe $\theta\in\overline{\mathbb{K}}$ tel que $\mathbb{K}(\alpha,\beta)=\mathbb{K}(\theta)$.*

Preuve. Pour $\alpha=\beta$, on a $\mathbb{K}(\alpha,\alpha)=\mathbb{K}(\alpha)$.

Si α est de degré 1 [resp. si β est de degré 1] il est alors dans $\mathbb{K}$ et on a $\mathbb{K}(\alpha,\beta)=\mathbb{K}(\beta)$ [resp. $\mathbb{K}(\alpha,\beta)=\mathbb{K}(\alpha)$].

En supposant $\alpha\neq\beta$ de degrés au moins égal à 2, on note $\alpha_1=\alpha,\alpha_2,\cdots,\alpha_d$ les racines complexes du polynôme minimal P_α de α et $\beta_1=\beta,\beta_2,\cdots,\beta_{d'}$ les racines complexes du polynôme minimal P_β de β. Le système d'équations d'inconnue t :

$$\alpha_j+t\beta_k=\alpha+t\beta\ \ (1\leq j\leq d,\ 2\leq k\leq d')$$

ayant un nombre fini de solutions, il existe $\lambda\in\mathbb{K}^*$ tel que $\alpha_j+\lambda\beta_k\neq\theta=\alpha+\lambda\beta$ pour tout j compris entre 1 et d et tout k compris entre 2 et d'. On a $\theta\in\mathbb{K}(\alpha,\beta)$, donc $\mathbb{K}(\theta)\subset\mathbb{K}(\alpha,\beta)$. Pour vérifier que $\mathbb{K}(\alpha,\beta)\subset\mathbb{K}(\theta)$, il nous suffit de montrer que $\beta\in\mathbb{K}(\theta)$, ce qui impliquera que $\alpha=\theta-\lambda\beta\in\mathbb{K}(\theta)$.

Le polynôme $Q(X)=P_\alpha(\theta-\lambda X)=P_\alpha(\alpha-\lambda(X-\beta))$ est dans $\mathbb{K}(\theta)[X]\setminus\{0\}$ tel que $Q(\beta)=P_\alpha(\alpha)=0$ et $Q(\beta_k)=P_\alpha(\theta-\lambda\beta_k)\neq0$ pour $2\leq k\leq d'$ puisque $\theta-\lambda\beta_k\neq\alpha_j$ pour $1\leq j\leq d$, donc le pgcd de P_β et Q dans $\mathbb{K}(\theta)[X]$ est de degré égal à 1 puisque P_β et Q ont une seule racine complexe en commun, soit $R(X)=\text{pgcd}(P_\beta(X),Q(X))=\mu X+\nu$ où $\mu\in\mathbb{K}(\theta)\setminus\{0\}$ et $\nu\in\mathbb{K}(\theta)$. Vu que $R=UP_\beta+VQ$ s'annule en β, on a $\mu\beta+\nu=0$ et en conséquence, $\beta=-\dfrac{\nu}{\mu}\in\mathbb{K}(\theta)$.

Comme α et β sont algébriques sur $\mathbb{K}$, on a $[\mathbb{K}[\theta]:\mathbb{K}]=[\mathbb{K}[\alpha,\beta]:\mathbb{K}]<+\infty$ (théorème 4.20), donc θ est algébrique sur $\mathbb{K}$. □

Lemme 4.13 *Pour toute suite $(\alpha_k)_{1\leq k\leq n}$ de $n\geq2$ nombres algébriques sur $\mathbb{K}$, il existe θ algébrique sur $\mathbb{K}$ tel que $\mathbb{K}(\alpha_1,\cdots,\alpha_n)=\mathbb{K}(\theta)$.*

Preuve. Pour $n=2$, c'est le lemme qui précède. Supposant le résultat acquis au rang $n-1\geq 2$, étant donné $(\alpha_k)_{1\leq k\leq n}\in\overline{\mathbb{K}}^n$, il existe α algébrique sur $\mathbb{K}$ tel que $\mathbb{K}(\alpha_1,\cdots,\alpha_{n-1})=\mathbb{K}(\alpha)$, donc :

$$\mathbb{K}(\alpha_1,\cdots,\alpha_n)=\mathbb{K}(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)=\mathbb{K}(\alpha)(\alpha_n)=\mathbb{K}(\theta)$$

où θ est algébrique sur $\mathbb{K}$. □

Le nombre complexe θ dans le lemme précédent étant algébrique sur $\mathbb{K}$, on a aussi $\mathbb{K}(\alpha_1,\cdots,\alpha_n)=\mathbb{K}[\theta]$.

Théorème 4.21. de l'élément primitif

Si $\mathbb{L}$ est une extension de degré fini de $\mathbb{K}$, il existe alors un nombre algébrique θ sur $\mathbb{K}$ tel que $\mathbb{L}=\mathbb{K}[\theta]$.

Preuve. Soit $\mathbb{L}$ une extension de degré $d\geq 1$ de $\mathbb{K}$ et $(\alpha_k)_{1\leq k\leq d}$ une base du $\mathbb{K}$-espace vectoriel $\mathbb{L}$. Tout élément x de $\mathbb{L}$ s'écrit de manière unique $x=\sum_{k=1}^{d}\lambda_k\alpha_k=P(\alpha_1,\cdots,\alpha_d)$ où $P(X_1,\cdots,X_d)=\sum_{k=1}^{d}\lambda_k X_k\in\mathbb{K}[X_1,\cdots,X_d]$, donc $\mathbb{L}\subset\mathbb{K}[\alpha_1,\cdots,\alpha_d]\subset\mathbb{K}(\alpha_1,\cdots,\alpha_d)$. Le corps $\mathbb{L}$ contenant $\mathbb{K}$ et les α_k pour $1\leq k\leq d$, il contient $\mathbb{K}(\alpha_1,\cdots,\alpha_n)$ qui est le plus petit de ces corps, d'où l'égalité $\mathbb{L}=\mathbb{K}(\alpha_1,\cdots,\alpha_d)$. En remarquant que tout $x\in\mathbb{L}$ est algébrique sur $\mathbb{K}$ (car $\left(x^k\right)_{0\leq k\leq d}$ formé de $d+1$ éléments est $\mathbb{K}$-liée), on déduit du lemme précédent qu'il existe un nombre algébrique θ sur $\mathbb{K}$ tel que $\mathbb{L}=\mathbb{K}[\theta]$. □

Dans le cas où $\mathbb{L}$ est une extension de degré 2 de $\mathbb{K}$, on dit que c'est une extension quadratique de $\mathbb{K}$ et il existe $\theta\in\mathbb{L}\setminus\mathbb{K}$ tel que $\theta^2\in\mathbb{K}$ et $\mathbb{L}=\mathbb{K}[\theta]$. En effet, on a $\mathbb{K}\not\subset\mathbb{L}$ car $[\mathbb{L}:\mathbb{K}]=2$ et pour tout $z\in\mathbb{L}\setminus\mathbb{K}$, $(1,z)$ est une base du $\mathbb{K}$ espace vectoriel de $\mathbb{L}$. Le système $\left(1,z,z^2\right)$ est alors lié et il existe a,b,c non tous nuls dans $\mathbb{K}$ tels que $az^2+bz+c=0$. Comme $(1,z)$ est libre, on a nécessairement $a\neq 0$ et l'équation précédente s'écrit $a\left(\left(z+\dfrac{b}{2a}\right)^2-\dfrac{b^2-4ac}{4a^2}\right)=0$. En posant $\theta=z+\dfrac{b}{2a}$, on a $\theta\in\mathbb{L}\setminus\mathbb{K}$, $\theta^2=\dfrac{b^2-4ac}{4a^2}\in\mathbb{K}$ et $(1,\theta)$ est une base du $\mathbb{K}$ espace vectoriel de $\mathbb{L}$, ce qui entraîne que $\mathbb{L}=\mathbb{K}[\theta]$.

En particulier si α est un réel algébrique de degré 2 sur $\mathbb{Q}$, il existe alors $\beta\in\mathbb{Q}_+^*$ tel que $\mathbb{K}[\alpha]=\mathbb{K}\left[\sqrt{\beta}\right]$.

Théorème 4.22.

Le corps $\overline{\mathbb{K}}$ des complexes algébriques sur $\mathbb{K}$ est algébriquement clos.

Preuve. On sait déjà que $\overline{\mathbb{K}}$ est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{K}$ (théorème 4.19).

Si $P(X)=\sum_{k=0}^{n}\alpha_k X^k$ est un polynôme de degré $n\geq 1$ dans $\overline{\mathbb{K}}[X]\subset\mathbb{C}[X]$, il admet alors une racine $\alpha\in\mathbb{C}$ qui est algébrique sur $\mathbb{K}(\alpha_1,\cdots,\alpha_n)=\mathbb{K}[\theta]=\mathbb{K}(\theta)$ où $\theta\in\overline{\mathbb{K}}$, donc $[\mathbb{K}(\theta,\alpha):\mathbb{K}(\theta)]=[\mathbb{K}(\theta)(\alpha):\mathbb{K}(\theta)]<+\infty$, ce qui implique

d'après le lemme 4.10 que $[\mathbb{K}(\theta,\alpha):\mathbb{K}] < +\infty$ (on a les extensions de corps $\mathbb{K} \subset \mathbb{K}(\theta) \subset \mathbb{K}(\theta)[\alpha]$ avec $[\mathbb{K}(\theta):\mathbb{K}] < +\infty$ et $[\mathbb{K}(\theta)(\alpha):\mathbb{K}(\theta)] < +\infty$), ce qui nous dit que $\alpha \in \overline{\mathbb{K}}$. Le corps $\overline{\mathbb{K}}$ est donc algébriquement clos. □

Le théorème qui suit nous donne une description des morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ pour α algébrique sur $\mathbb{K}$.

Théorème 4.23.

Soient $\alpha \in \mathbb{C}$ un nombre algébrique sur $\mathbb{K}$ de degré $d_\alpha = d(\alpha,\mathbb{K})$ et $P_\alpha \in \mathbb{K}[X]$ son polynôme minimal.

1. *Pour tout morphisme de $\mathbb{K}$-algèbres $\sigma : \mathbb{K}[\alpha] \to \mathbb{C}$, $\sigma(\alpha)$ est une racine de P_α.*
2. *Il y a exactement d_α morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$.*
3. *En notant $(\sigma_k)_{1\leq k\leq d_\alpha}$ la suite de tous les morphismes de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$, tout $\theta \in \mathbb{K}[\alpha]$ est algébrique sur $\mathbb{K}$ annulé par le polynôme $Q_\theta(X) = \prod_{k=1}^{d_\alpha} (X - \sigma_k(\theta))$ qui est une puissance de P_θ dans $\mathbb{K}[X]$.*

Preuve. Notons $(\alpha_k)_{1\leq k\leq d_\alpha}$ les racines complexes distinctes de P_α avec $\alpha_1 = \alpha$. Dans le cas où α est de degré 1, on a $\mathbb{K}[\alpha] = \mathbb{K}$ et $\sigma_1 : r \mapsto r$ est l'unique morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$. Les résultats annoncés sont alors des trivialités. On suppose donc que $d_\alpha \geq 2$.

1. Soit $\sigma : \mathbb{K}[\alpha] \to \mathbb{C}$ un morphisme de $\mathbb{K}$-algèbres. On a $\sigma(xy) = \sigma(x)\sigma(y)$ et $\sigma(ax+y) = a\sigma(x) + \sigma(y)$ pour tous x, y dans $\mathbb{K}[\alpha]$ et tout a dans $\mathbb{K}$, donc $(\sigma(\alpha))^k = \sigma(\alpha^k)$ pour tout $k \in \mathbb{N}$ (on a $\sigma(1) = 1$) et $P(\sigma(\alpha)) = \sigma(P(\alpha))$ pour tout $P \in \mathbb{K}[X]$, ce qui donne en particulier $P_\alpha(\sigma(\alpha)) = \sigma(P_\alpha(\alpha)) = \sigma(0) = 0$.

2. Il existe donc, pour tout morphisme de $\mathbb{K}$-algèbres σ de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$, un entier k compris entre 1 et d_α tel que $\sigma(\alpha) = \alpha_k$. Les α_k étant deux à deux distincts, cela défini exactement d_α tels morphismes de $\mathbb{K}$-algèbres (tout $z \in \mathbb{K}[\alpha]$ s'écrit de manière unique $z = \sum_{j=0}^{d_\alpha-1} a_j\alpha^j$, donc en posant $\sigma(\alpha) = \alpha_k$, on définit un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[\alpha]$ dans $\mathbb{C}$ par $\sigma(z) = \sum_{j=0}^{d_\alpha-1} a_j\alpha_k^j$). Comme tout morphisme de corps, σ_k est injectif (le noyau de σ_k est un idéal strict du corps $\mathbb{K}[\alpha]$ car $\sigma_k(1) = 1$, donc réduit à $\{0\}$ et σ_k est injectif) et c'est un isomorphisme de $\mathbb{K}[\alpha]$ sur $\mathrm{Im}(\sigma_k) = \mathbb{K}[\alpha_k]$.

3. On sait déjà que le corps $\mathbb{K}[\alpha]$ est contenu dans $\overline{\mathbb{K}}$. Tout $\theta \in \mathbb{K}[\alpha]$ s'écrit $\theta = \sum_{j=0}^{d_\alpha-1} a_j\alpha^j = P(\alpha)$ avec $P(X) = \sum_{j=0}^{d_\alpha-1} a_jX^j \in \mathbb{K}[X]$, donc pour tout entier

k compris entre 1 et d_α, on a $\sigma_k(\theta) = \sum_{j=0}^{d_\alpha-1} a_j(\sigma_k(\alpha))^j = \sum_{j=0}^{d_\alpha-1} a_j\alpha_k^j = P(\alpha_k)$ et $Q_\theta(X) = \prod_{k=1}^{d_\alpha}(X - P(\alpha_k)) \in \mathbb{K}[X]$ d'après le théorème 4.17.

On note $P_\theta(X) = \prod_{k=1}^{d_\theta}(X - \theta_k)$ où $(\theta_k)_{1\leq k\leq d_\theta}$ est la suite des racines complexes deux à deux distinctes de P_θ. La restriction de chaque σ_k à $\mathbb{K}[\theta]$ est un morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[\theta]$ dans $\mathbb{C}$, donc il existe j compris entre 1 et d_θ tel que $\sigma_k(\theta) = \theta_j$ et on a $Q_\theta(\theta_j) = Q_\theta(\sigma_k(\theta)) = \sigma_k(Q_\theta(\theta)) = 0$ avec $Q_\theta \in \mathbb{K}[X]$. Il en résulte que $P_\theta = P_{\theta_j}$ divise Q_θ dans $\mathbb{K}[X]$ (P_θ est irréductible dans $\mathbb{K}[X]$ annulant θ_j, donc $P_\theta = P_{\theta_j}$). On a donc $Q_\theta = QP_\theta^r$ avec $r \geq 1$ et $Q \in \mathbb{K}[X]$ unitaire non divisible par P_θ. Si Q est non constant, il admet alors une racine complexe qui est aussi racine de Q_θ, cette racine est donc l'un des $\sigma_k(\theta) = P(\alpha_k)$ et on a $\sigma_k(Q(\theta)) = Q(\sigma_k(\theta)) = 0$, ce qui implique que $Q(\theta) = 0$ puisque σ_k est injectif et le polynôme minimal P_θ de θ devrait diviser Q, ce qui n'est pas. On a donc $Q = 1$ et $Q_\theta = P_\theta^r$. □

4.5 Entiers algébriques

Définition 4.7. *On dit qu'un nombre complexe α est un* entier algébrique *s'il est algébrique sur $\mathbb{Q}$ de polynôme minimal dans $\mathbb{Z}[X]$.*

Du fait que $P_\alpha \in \mathbb{Z}[X]$ pour α entier algébrique de degré d_α, on déduit que les expressions symétriques élémentaires des racines complexes de P_α sont des entiers relatifs. En adaptant la démonstration du théorème 4.17, on voit que $\sum_{k=1}^{d_\alpha}\alpha_k^j \in \mathbb{Z}$ pour tout $j \in \mathbb{N}$ où les α_k sont les racines complexes de P_α.

En effectuant la division euclidienne dans $\mathbb{Z}[X]$ par le polynôme unitaire P_α, on voit que $\mathbb{Z}[\alpha] = \left\{\sum_{k=0}^{d_\alpha} a_k\alpha^k,\ (a_k)_{0\leq k\leq d_\alpha-1} \in \mathbb{Z}^{d_\alpha}\right\}$ (c'est un groupe additif libre de type fini).

On note $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques.

Lemme 4.14 *Un nombre complexe α est un entier algébrique si, et seulement si, il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ tel que $P(\alpha) = 0$.*

Preuve. Si α est un entier algébrique, son polynôme minimal est alors unitaire dans $\mathbb{Z}[X]$ et annule α. Réciproquement, s'il existe P unitaire dans $\mathbb{Z}[X]$ tel que $P(\alpha) = 0$, on a alors $P = P_\alpha Q$ où P_α et Q sont dans $\mathbb{Q}[X]$, ce qui implique que P_α et Q sont en fait dans $\mathbb{Z}[X]$ (lemme **??**) et nous dit que α est un entier algébrique. □

Pour tout nombre algébrique $\alpha \in \overline{\mathbb{Q}}$ il existe un entier $n \geq 1$ tel que $n\alpha$ soit un entier algébrique. En effet, si $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ de polynôme

minimal $P_\alpha(X) = X^{d_\alpha} - \sum_{k=0}^{d_\alpha-1} r_k X^k$, en désignant par $n \in \mathbb{N}^*$ le ppcm des dénominateurs des coefficients r_k pour r compris entre 0 et $d_\alpha - 1$, on a alors $(n\alpha)^{d_\alpha} - \sum_{k=0}^{d_\alpha-1} n^{d_\alpha-k} r_k (n\alpha)^k = n^{d_\alpha} P_\alpha(\alpha) = 0$, ce qui nous dit que $n\alpha$ est un entier algébrique annulé par $P_{n\alpha}(X) = X^{d_\alpha} - \sum_{k=0}^{d_\alpha-1} n^{d_\alpha-k} r_k X^k \in \mathbb{Z}[X]$.

Un entier algébrique est rationnel si, et seulement si, il est entier.

Exemples 4.6

- *Pour tout nombre premier $p \geq 2$, $\alpha = \sqrt{p}$ est un entier algébrique de polynôme minimal $X^2 - p$.*
- *Pour tous nombres premiers $q > p \geq 2$, le réel $\alpha = \sqrt{p} + \sqrt{q}$ est un entier algébrique de degré 4 (exercice 4.6).*
- *Pour tout nombre premier $p \geq 2$, le nombre complexe $e^{\frac{2i\pi}{p}}$ est un entier algébrique de polynôme minimal le polynôme cyclotomique $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$ (voir l'exercice* **??** *pour l'irréductibilité de Φ_p dans $\mathbb{Q}[X]$).*

En vue de démontrer que l'ensemble $\overline{\mathbb{Z}}$ des entiers algébrique est un anneau nous donnons la caractérisation qui suit des entiers algébriques.

Pour toute suite $(\alpha_k)_{1\leq k\leq d}$ de $d \geq 1$ nombres complexes, l'ensemble :

$$\mathbb{Z}[\alpha_1, \cdots, \alpha_d] = \{P(\alpha_1, \cdots, \alpha_d),\ P \in \mathbb{Z}[X_1, \cdots, X_d]\}$$

est un sous-anneau de $\mathbb{C}$ comme image du morphisme d'anneaux $P \mapsto P(\alpha_1, \cdots, \alpha_d)$ de $\mathbb{Z}[X_1, \cdots, X_d]$ dans $\mathbb{C}$. C'est le plus petit sous-anneau de $\mathbb{C}$ qui contient $\mathbb{Z}$ et les α_k pour $1 \leq k \leq d$.

Lemme 4.15 *Si $(\alpha_k)_{1\leq k\leq d} \in \overline{\mathbb{Z}}^d$ est une suite de $d \geq 1$ entiers algébriques, le groupe additif $\mathbb{Z}[\alpha_1, \cdots, \alpha_d]$ est alors de type fini (*i. e. *engendré par un nombre fini d'éléments).*

Preuve. Pour tout entier k compris entre 1 et d, on note $P_k \in \mathbb{Z}[X]$ le polynôme minimal de α_k et d_k son degré. De l'égalité $P_k(\alpha_k) = 0$, on déduit que $\alpha_k^{d_k}$ est combinaison linéaire à coefficients entiers de $1, \alpha_k, \cdots, \alpha_k^{d_k-1}$ et par récurrence, on en déduit qu'il en est de même de α_k^m pour tout entier $m \geq d_k$. Il en résulte que tout élément de $\mathbb{Z}[\alpha_1, \cdots, \alpha_d]$ est combinaison linéaire à coefficients entiers relatifs des $\prod_{k=1}^{d} \alpha_k^{m_k}$ où les exposants m_k pour $1 \leq k \leq d$ sont tels que $0 \leq m_k \leq d_k - 1$, ce qui nous dit que le groupe additif $\mathbb{Z}[\alpha_1, \cdots, \alpha_d]$ est de type fini engendré par $\left\{\prod_{k=1}^{d} \alpha_k^{m_k},\ 0 \leq m_k \leq d_k - 1\right\}$. □

Lemme 4.16 *Un nombre complexe α est un entier algébrique si, et seulement fini, il existe un sous-groupe additif $G \neq \{0\}$ de $\mathbb{C}$ de type fini tel que $\alpha G \subset G$.*

Preuve. Si $\alpha \in \mathbb{C}$ est un entier algébrique, le groupe additif $G = \mathbb{Z}[\alpha]$ est alors de type fini et pour tout $P \in \mathbb{Z}[X]$, on a $\alpha P(\alpha) = (XP)(\alpha) \in G$, donc $\alpha G \subset G$. Réciproquement, supposons qu'il existe un sous-groupe additif $G \neq \{0\}$ de $\mathbb{C}$ de type fini tel que $\alpha G \subset G$. En se donnant une partie génératrice $(z_k)_{1\leq k\leq m}$ de G, tout élément z de G s'écrit $z = \sum_{k=1}^{m} a_k z_k$ où $(a_k)_{1\leq k\leq m} \in \mathbb{Z}^m$. Pour tout entier k compris entre 1 et m, on a $\alpha z_k \in G$ puisque $\alpha G \subset G$, donc il existe $(a_{k,j})_{1\leq j\leq m} \in \mathbb{Z}^m$ tel que $\alpha z_k = \sum_{j=1}^{m} a_{k,j} z_j$, ce qui nous dit que $(z_k)_{1\leq k\leq m}$ est solution non nulle (car $G \neq \{0\}$) du système linéaire de m équations à m inconnues :

$$\sum_{j=1}^{m} (\delta_{k,j}\alpha - a_{k,j})\, z_j = 0 \ \ (1 \leq k \leq m)$$

et il en résulte que le déterminant de la matrice de ce système est nul, soit :

$$P(\alpha) = \begin{vmatrix} \alpha - a_{11} & -a_{12} & \cdots & -a_{1m} \\ -a_{21} & \alpha - a_{22} & \cdots & -a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{m1} & -a_{m2} & \cdots & \alpha - a_{mm} \end{vmatrix} = 0$$

où $P \in \mathbb{Z}[X] \setminus \{0\}$ est unitaire de degré d. Donc α est un entier algébrique. □

Théorème 4.24.

L'ensemble $\overline{\mathbb{Z}}$ des entiers algébriques est un sous-anneau de $\mathbb{C}$.

Preuve. On a déjà les inclusions $\mathbb{Z} \subset \overline{\mathbb{Z}} \subset \mathbb{C}$. Pour vérifier que $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$, il suffit de montrer que si α, β sont dans $\overline{\mathbb{Z}}$, alors $\alpha - \beta$ et $\alpha\beta$ sont aussi dans $\overline{\mathbb{Z}}$. Pour α, β dans $\overline{\mathbb{Z}}$, le groupe additif $\mathbb{Z}[\alpha, \beta]$ est de type fini et non réduit à $\{0\}$ (il contient $\mathbb{Z}$) et des inclusions $(\alpha - \beta)\mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta]$ et $(\alpha\beta)\mathbb{Z}[\alpha, \beta] \subset \mathbb{Z}[\alpha, \beta]$, il résulte que $\alpha - \beta$ et $\alpha\beta$ sont des entiers algébriques d'après le lemme précédent. □

On déduit du théorème précédent que si α est un entier algébrique, l'anneau $\mathbb{Z}[\alpha]$ est alors contenu dans $\overline{\mathbb{Z}}$.

Le théorème précédent peut aussi se montrer en faisant apparaître deux entiers algébriques non nuls α et β comme valeurs propres associées au même vecteur propre de deux matrices à coefficients entiers relatifs, la démonstration étant analogue à celle de la deuxième remarque qui suit le théorème 4.19. Il peut également se prouver en utilisant le résultant de deux polynômes (théorème 2.3).

Avec le théorème précédent, on retrouve le fait que $\overline{\mathbb{Q}}$ est un corps. Si α, β sont dans $\overline{\mathbb{Q}}$, il existe alors deux entiers $n \geq 1$ et $m \geq 1$ tels que $n\alpha \in \overline{\mathbb{Z}}$ et $m\beta \in \overline{\mathbb{Z}}$, donc $nm\alpha$ et $nm\beta$ sont dans $\overline{\mathbb{Z}}$ (c'est un groupe additif), ce qui implique que $nm(\alpha + \beta) = nm\alpha + nm\beta$ et $n^2m^2\alpha\beta \in \overline{\mathbb{Z}}$ (c'est un anneau), donc $\alpha + \beta$ et $\alpha\beta$

sont dans $\overline{\mathbb{Q}}$ (facile à voir puisque $nm \in \mathbb{Z}^*$). Donc $\overline{\mathbb{Q}}$ est donc un sous-anneau de $\mathbb{C}$. Le fait que tous les éléments de $\overline{\mathbb{Q}} \setminus \{0\}$ sont inversibles se prouve comme pour le théorème 4.19.

4.6 Exercices

Exercice 4.1. *Montrer directement que $\mathbb{Z}[X]$ n'est pas principal ?*

Solution. Considérons l'idéal $I = (2, X) = 2\mathbb{Z} + X\mathbb{Z}$ dans $\mathbb{Z}[X]$ et supposons qu'il existe $P \in \mathbb{Z}[X]$ tel que $I = (2, X) = (P)$. Comme $2 \in I$, il existe $Q \in \mathbb{Z}[X]$ tel que $2 = PQ$, donc P est constant divisant 2 et $P = \pm 1$ ou $P = \pm 2$. Comme $P \in I$, on a $P = 2A + XB$ avec A, B dans $\mathbb{Z}[X]$, donc $P = P(0) = 2A(0)$ est un entier pair, soit $P = \pm 2$. Comme $X \in I$, on a $X = QP$ avec $Q \in \mathbb{Z}[X]$ et l'évaluation en 1 nous donne $1 = P(1)Q(1) = 2a$ avec $a \in \mathbb{Z}$, ce qui est impossible.

Exercice 4.2. *Déterminer les éléments irréductibles de l'anneau $\mathbb{K}[[X]]$.*

Solution. Si $S \in \mathbb{K}[[X]]$ est irréductible, elle est alors non nulle et non inversible et sa valuation vaut 1. En effet, si $\operatorname{val}(S) = n \geq 2$, on a alors $S = X^n S_1$ avec S_1 inversible, donc $S = X\left(S^{n-1}S1\right)$ est réductible. On a donc $S = XS_1$ avec S_1 inversible. Réciproquement une telle série entière est irréductible (sinon, on a $S = UV$ avec $\operatorname{val}(U) \geq 1$, $\operatorname{val}(V) \geq 1$ et $\operatorname{val}(S) \geq 2$). Les éléments irréductibles de $\mathbb{K}[[X]]$ sont donc les séries formelles associées à X et la décomposition en facteurs irréductibles d'une série entière S non nulle et non inversible est $S = X^n S_1$ où $n = \operatorname{val}(S)$ et S_1 est inversible dans $\mathbb{K}[[X]]$.

Exercice 4.3. *Montrer que $\dfrac{\mathbb{K}[X,Y]}{(Y - X^2)}$ et $\dfrac{\mathbb{K}[X,Y]}{(XY - 1)}$ sont principaux.*

Solution.

1. Il est clair que l'application $\varphi : P(X,Y) \in \mathbb{K}[X,Y] \mapsto P\left(X, X^2\right) \in \mathbb{K}[X]$ est un morphisme d'anneaux. Pour tout $n \in \mathbb{N}$, on a $\varphi(X^n) = X^n$, donc sa restriction à $\mathbb{K}[X]$ est l'identité et ce morphisme est surjectif. Dans l'anneau $\mathbb{K}[X,Y] = \mathbb{K}[X][Y]$, on peut effectuer la division euclidienne de tout polynôme $P \in \mathbb{K}[X,Y]$ par $Y - X^2$ puisque le coefficient dominant de ce polynôme en Y est 1 (théorème **??**), soit $P(X,Y) = Q(X,Y)\left(Y - X^2\right) + R(X,Y)$ où R est de degré en Y strictement inférieur à 1, c'est-à-dire que $R = R(X)$ est dans $\mathbb{K}[X]$ et P est dans $\ker(\varphi)$ si, et seulement si, $R = 0$, ce qui revient à dire que $P(X,Y) = Q(X,Y)\left(Y - X^2\right)$ est dans l'idéal $\left(Y - X^2\right)$. En conclusion $\dfrac{\mathbb{K}[X,Y]}{(Y - X^2)} = \dfrac{\mathbb{K}[X,Y]}{\ker(\varphi)}$ est isomorphe à $\mathbb{K}[X]$ qui est principal, donc $\dfrac{\mathbb{K}[X,Y]}{(Y - X^2)}$ est principal.

2. L'application $\varphi : P(X,Y) \in \mathbb{K}[X,Y] \mapsto P\left(X, \frac{1}{X}\right) \in \mathbb{K}(X)$ est un morphisme d'anneaux. En écrivant tout polynôme $P \in \mathbb{K}[X,Y] = \mathbb{K}[X][Y]$ sous la forme $P(X,Y) = \sum_{k=0}^{n} A_k(X) Y^k$, où les A_k sont dans $\mathbb{K}[X]$, il existe $A \in \mathbb{K}[X]$ tel que $\varphi(P)(X) = \sum_{k=0}^{n} \frac{A_k(X)}{X^k} = \frac{A(X)}{X^n}$ dans $\mathbb{K}(X)$, donc $\mathrm{Im}(\varphi)$ est contenu dans $S^{-1}\mathbb{K}[X]$ où $S = \{X^n,\ n \in \mathbb{N}\}$. En écrivant toute fraction rationnelle $T \in S^{-1}\mathbb{K}[X]$ sous la forme $T(X) = \sum_{k=0}^{n} \frac{a_k X^k}{X^n}$, où $a_k \in \mathbb{K}$ pour $0 \leq k \leq n$, on a $T = \varphi(P)$ où $P(X,Y) = \sum_{k=0}^{n} a_k X^k Y^n$, donc $\mathrm{Im}(\varphi) = S^{-1}\mathbb{K}[X]$. On vérifie enfin que le noyau de φ est l'idéal $(XY-1)$. Dans $\mathbb{K}(X)[Y]$, on peut effectuer la division euclidienne de tout polynôme $P \in \mathbb{K}[X,Y]$ par $XY-1$, soit $P(X,Y) = Q(X,Y)(XY-1) + R(X,Y)$, où $Q(X,Y) \in \mathbb{C}(X)[Y]$ et R est de degré en Y strictement inférieur à 1, soit $R = R(X) \in \mathbb{K}(X)$. Donc P est dans le noyau de φ si, et seulement si, $R = 0$, ce qui revient à dire que $P(X,Y) = Q(X,Y)(XY-1)$. Il s'agit alors de vérifier que Q est dans $\mathbb{K}[X][Y]$. Pour $Q = 0$ c'est clair et pour $Q \neq 0$, on a $P(X,Y) = \sum_{k=0}^{n} A_k(X) Y^k$ et $Q(X,Y) = \sum_{k=0}^{n-1} B_k(X) Y^k$, où les A_k sont dans $\mathbb{K}[X]$ et les B_k sont dans $\mathbb{K}(X)$, de sorte que l'égalité $P(X,Y) = Q(X,Y)(XY-1)$ nous donne :

$$\begin{aligned} P(X,Y) &= \sum_{k=0}^{n-1} XB_k(X) Y^{k+1} - \sum_{k=0}^{n-1} B_k(X) Y^k \\ &= \sum_{k=1}^{n} XB_{k-1}(X) Y^k - \sum_{k=0}^{n-1} B_k(X) Y^k \\ &= XB_{n-1}(X) Y^k - B_0(X) + \sum_{k=1}^{n-1} (XB_{k-1}(X) - B_k(X)) Y^k \end{aligned}$$

et par récurrence finie, on en déduit que :

$$\begin{cases} B_0(X) = -A_0(X) \in \mathbb{K}[X] \\ B_k(X) = A_k(X) - XB_{k-1}(X) \in \mathbb{K}[X] \quad (1 \leq k \leq n-1) \end{cases}$$

soit $Q \in \mathbb{K}[X][Y]$. En conclusion $\frac{\mathbb{K}[X,Y]}{(XY-1)} = \frac{\mathbb{K}[X,Y]}{\ker(\varphi)}$ est isomorphe à $S^{-1}\mathbb{K}[X]$ qui est principal, donc $\frac{\mathbb{K}[X,Y]}{(XY-1)}$ est principal.

Exercice 4.4. *Montrer que, pour tout $n \in \mathbb{N}$, les idéaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont ses sous-groupes additifs. Déterminer tous les idéaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$. Quels sont les idéaux premiers, maximaux de $\mathbb{Z}$ et de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$?*

Solution.

1. Si I est un idéal de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, c'est en particulier un sous-groupe additif. Réciproquement si I est un sous-groupe additif de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, pour $\left(\overline{a}, \overline{b}\right) \in I \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}$, on a $\overline{a} \cdot \overline{b} = \pm\overline{|b|\, a} = \pm\, |b|\, \overline{a} = \pm\left(\overline{a} + \cdots + \overline{a}\right) \in I$ et I est un idéal de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.
2. Pour $n = 0$, on a $\dfrac{\mathbb{Z}}{0 \cdot \mathbb{Z}} = \mathbb{Z}$ qui est principal, ses idéaux étant les (q) où $q \in \mathbb{N}$. Pour $n = 1$, on a $\mathbb{Z}_1 = \left\{\overline{0}\right\}$. Pour $n \geq 2$, ce qui précède nous dit que les idéaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont les $(\overline{q})$ où $q \in \{1, \cdots, n\}$ est un diviseur de n. On peut vérifier que $\dfrac{\dfrac{\mathbb{Z}}{n\mathbb{Z}}}{(\overline{q})} = \dfrac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{q\frac{\mathbb{Z}}{n\mathbb{Z}}} \backsimeq \dfrac{\mathbb{Z}}{q\mathbb{Z}}$. En effet, comme q divise n, l'application $\varphi : \overline{k} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}} \mapsto \widehat{k} \in \mathbb{Z}_q$ est bien définie (si $\overline{k} = \overline{j}$, n divise alors $k - j$, donc q qui divise n divise aussi $k - j$ et $\widehat{k} = \widehat{j}$) et c'est un morphisme d'anneaux surjectif de noyau $\ker(\varphi) = \left\{\overline{k} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}} \mid q \text{ divise } k\right\} = \left\{\overline{jq} = j\overline{q} \mid j \in \mathbb{Z}\right\} = (\overline{q})$, donc $\dfrac{\dfrac{\mathbb{Z}}{n\mathbb{Z}}}{(\overline{q})}$ est isomorphe à $\dfrac{\mathbb{Z}}{q\mathbb{Z}}$.
3. Dans $\mathbb{Z}$ qui est principal, on a les équivalences :

$$((p) \text{ maximal}) \Leftrightarrow ((p) \text{ premier}) \Leftrightarrow (p \text{ premier})$$

(lemme 4.4). Pour $n \geq 2$, dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ qui est fini, il y a équivalence entre idéal premier et maximal (exercice 3.10) et on a vu que les idéaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont de la forme $I = (\overline{q})$ où $q = 0$ ou $q \neq 0$ est un diviseur de n. Pour n premier, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps et ses seuls idéaux sont $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\left\{\overline{0}\right\}$, seul $\left\{\overline{0}\right\}$ est maximal. Pour $n \geq 2$ non premier, on a deux possibilités, soit $I = (\overline{p})$ où $2 \leq p \leq n - 1$ est un diviseur premier de n et dans ce cas I est maximal (on a $I \neq \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ puisque $\overline{p}$ qui divise $\overline{0}$ n'est pas inversible et si $(\overline{p}) \subset J = (\overline{q})$ avec q qui divise n, on a alors $\overline{p} = \overline{aq}$, soit $p = aq + kn = aq + kjq$ et q divise p, donc $q = 1$ ou $q = p$, soit $J = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ ou $J = I$), soit $I = (\overline{q})$ où q est un diviseur non premier de n et I n'est pas maximal (pour $q = 1$, on a $I = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et pour $q \geq 2$, on a $q = ab$ avec

$2 \leq a, b \leq q-1$ et $I = \left(\overline{ab}\right) \subsetneq (\overline{a}) \subsetneq \dfrac{\mathbb{Z}}{n\mathbb{Z}}$). En définitive, les idéaux maximaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont les $(\overline{p})$ où p est un diviseur premier de n.

Exercice 4.5. *Montrer que si $[\mathbb{L} : \mathbb{K}]$ est fini, alors tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.*

Solution. Si $[\mathbb{L} : \mathbb{K}]$ est fini, alors pour tout α dans $\mathbb{L}$ le sous $\mathbb{K}$ espace vectoriel $\mathbb{K}[\alpha]$ de $\mathbb{L}$ est également de dimension finie (théorème 4.18), ce qui signifie que α est algébrique sur $\mathbb{K}$. Par exemple de $[\mathbb{C} : \mathbb{R}] = 2$ on déduit que tout nombre complexe est algébrique sur $\mathbb{R}$, ce qui peut aussi se voir directement en écrivant que pour tout $z = x + iy$ dans $\mathbb{C}$ on a $(z-x)^2 + y^2 = 0$.

Exercice 4.6. *Soit $p \geq 2$ un nombre premier.*

1. *Montrer que $\sqrt{p}$ est un entier algébrique de polynôme minimal $X^2 - p$. Préciser l'inverse de $z \in \mathbb{Q}\left[\sqrt{p}\right] \setminus \{0\}$.*
2. *Montrer que pour tout nombre premier $q > p$, $\sqrt{q} \notin \mathbb{Q}\left[\sqrt{p}\right]$.*
3. *Montrer que pour tout nombre premier $q > p$, le réel $\alpha = \sqrt{p} + \sqrt{q}$ est un entier algébrique de degré 4 en vérifiant que la famille $\left\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\right\}$ est une base de $\mathbb{Q}[\alpha]$.*
4. *Montrer que pour nombre premier $q > 2$, $\beta = \dfrac{\sqrt{2} + \sqrt{q}}{2}$ est un nombre algébrique, mais pas un entier algébrique.*

Solution.

1. Le réel $\sqrt{p}$ est annulé par $P(X) = X^2 - p \in \mathbb{Z}[X]$, c'est donc un entier algébrique. Le polynôme P est irréductible dans $\mathbb{Q}[X]$ puisque ses deux racines $\pm\sqrt{p}$ sont irrationnelles pour p premier, donc $\sqrt{p}$ est de degré 2 et on a $\mathbb{Q}\left[\sqrt{p}\right] = \left\{r + s\sqrt{p},\ (r,s) \in \mathbb{Q}^2\right\}$. Pour tout $z = r + s\sqrt{p} \in \mathbb{Q}\left[\sqrt{p}\right] \setminus \{0\}$ où $(r,s) \in \mathbb{Q}^2 \setminus \{(0,0)\}$, on a $\left(r + s\sqrt{p}\right)\left(r - s\sqrt{p}\right) = r^2 + ps^2 \in \mathbb{Q}_+^*$, donc $z^{-1} = \dfrac{r - s\sqrt{p}}{r^2 + ps^2}$ dans $\mathbb{Q}\left[\sqrt{p}\right]$.
2. Si $\sqrt{q} \in \mathbb{Q}\left[\sqrt{p}\right]$, on a alors $\sqrt{q} = r + s\sqrt{p}$ où $(r,s) \in \left(\mathbb{Q}^*\right)^2$ ($s = 0$ donne $\sqrt{q} = r \in \mathbb{Q}$ et $r = 0$ donne $\sqrt{\dfrac{q}{p}} = s \in \mathbb{Q}$, soit une impossibilité dans les deux cas pour $q > p$ premiers car $\sqrt{q}$ et $\sqrt{\dfrac{q}{p}}$ sont irrationnels), ce qui implique que $q = \left(r + s\sqrt{p}\right)^2 = r^2 + ps^2 + 2rs\sqrt{p} \in \mathbb{Q}$ avec $rs \neq 0$, donc $\sqrt{p} \in \mathbb{Q}$, ce qui n'est pas possible.
3. Pour $\alpha = \sqrt{p} + \sqrt{q}$, on a $\left(\alpha^2 - p - q\right)^2 = 4pq$, donc α est annulé par le polynôme $P(X) = X^4 - 2(p+q)X^2 + (p-q)^2$ et c'est un entier algébrique de degré au plus égal à 4, donc $[\mathbb{Q}[\alpha] : \mathbb{Q}] \leq 4$. De $\alpha^2 = p + q + 2\sqrt{pq} \in \mathbb{Q}[\alpha]$, on déduit

que $\sqrt{pq} \in \mathbb{Q}[\alpha]$, donc $\sqrt{pq}\alpha = p\sqrt{q} + q\sqrt{p} \in \mathbb{Q}[\alpha]$ et $p\alpha = p\sqrt{p} + p\sqrt{q} \in \mathbb{Q}[\alpha]$, ce qui implique que $\sqrt{pq}\alpha - p\alpha = (q-p)\sqrt{p} \in \mathbb{Q}[\alpha]$, donc $\sqrt{p} \in \mathbb{Q}[\alpha]$ et $\sqrt{q} = \alpha - \sqrt{p} \in \mathbb{Q}[\alpha]$. Montrons enfin que la famille $\left\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\right\}$ est libre dans $\mathbb{Q}[\alpha]$. Si a, b, c, d dans $\mathbb{Q}$ sont tels que $a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} = 0$, on a alors $\sqrt{q}\left(c + d\sqrt{p}\right) = -a - b\sqrt{p}$. Si $c + d\sqrt{p} = 0$, on a alors $a + b\sqrt{p} = 0$, donc $c = d = 0$ et $a = b = 0$ puisque $\sqrt{p}$ est irrationnel. Sinon, $c + d\sqrt{p}$ est inversible dans le corps $\mathbb{Q}\left[\sqrt{p}\right]$ et $\sqrt{q} = -\left(a + b\sqrt{p}\right)\left(c + d\sqrt{p}\right)^{-1} \in \mathbb{Q}\left[\sqrt{p}\right]$, ce qui n'est pas possible. La famille $\left\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\right\}$ est donc libre et c'est une base de $\mathbb{Q}[\alpha]$. Il en résulte que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$ et P est le polynôme minimal de α.

On peut aussi procéder comme suit. En notant $\alpha' = \sqrt{q} - \sqrt{p}$, on a $\alpha + \alpha' = 2\sqrt{q}$ et $\alpha\alpha' = q - p$, c'est-à-dire que α et α' sont les deux solutions de l'équation $P(X) = X^2 - 2\sqrt{q}X + q - p = 0$. Ils sont donc algébriques sur le corps $\mathbb{Q}\left[\sqrt{q}\right]$. Comme α n'est pas dans $\mathbb{Q}\left[\sqrt{q}\right]$ (sinon on a $\sqrt{p} = \alpha\sqrt{q} \in \mathbb{Q}\left[\sqrt{q}\right]$, soit $\sqrt{p} = r + s\sqrt{q}$ avec r, s rationnels et $p = r^2 + qs^2 + 2rs\sqrt{q}$ nous dit que $\sqrt{q}$ est rationnel), on en déduit qu'il est de degré 2 sur $\mathbb{Q}\left[\sqrt{q}\right]$ et on a $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \left[\mathbb{Q}[\alpha] : \mathbb{Q}\left[\sqrt{q}\right]\right]\left[\mathbb{Q}\left[\sqrt{q}\right] : \mathbb{Q}\right] = 4$, ce qui implique que P est le polynôme minimal de α.

4. Le réel $\beta = \dfrac{\sqrt{2} + \sqrt{q}}{2} = \dfrac{\alpha}{2}$ est un nombre algébrique de polynôme minimal $Q(X) = \dfrac{1}{16}P(2X)$ (on a $P(2\beta) = P(\alpha) = 0$ et $\mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$ est de degré 4). Si β est un entier algébrique, on a alors $Q(X) = X^4 - \dfrac{p+q}{2}X^2 + \dfrac{(p-q)^2}{16} \in \mathbb{Z}[X]$, donc $\dfrac{p+q}{2} \in \mathbb{N}^*$ et $\dfrac{(p-q)^2}{16} \in \mathbb{N}^*$, ce qui est impossible pour $p = 2$ et $q \geq 3$ impair.

Exercice 4.7. *Soient $2 \leq p < q$ deux nombres premiers. Montrer que $\alpha = \sqrt{p} + \sqrt[3]{q}$ est algébrique sur $\mathbb{Q}$, puis calculer son polynôme minimal.*

Solution. Posons $\beta = \sqrt[3]{q} - \sqrt{p}$. On a $\alpha + \beta = 2\sqrt[3]{q}$ et $\alpha\beta = \sqrt[3]{q^2} - p$, c'est-à-dire que α et β sont les solutions de l'équation $P(X) = X^2 - 2\sqrt[3]{q}X + \left(\sqrt[3]{q}\right)^2 - p = 0$. Ils sont donc algébriques sur le corps $\mathbb{Q}\left[\sqrt[3]{q}\right]$ (il est facile de vérifier que $\sqrt[3]{q}$ est algébrique sur $\mathbb{Q}$ de degré 3). Comme α n'est pas dans $\mathbb{Q}\left[\sqrt[3]{q}\right]$, il est de degré 2 sur $\mathbb{Q}\left[\sqrt[3]{q}\right]$ et on a $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \left[\mathbb{Q}[\alpha] : \mathbb{Q}\left[\sqrt[3]{q}\right]\right]\left[\mathbb{Q}\left[\sqrt[3]{q}\right] : \mathbb{Q}\right] = 6$. Avec $\left(\alpha - \sqrt{p}\right)^3 = q$, on déduit que $\alpha^3 - 3\alpha^2\sqrt{p} + 3p\alpha - p\sqrt{p} = q$, ce qui entraîne $\left(\alpha^3 + 3p\alpha - q\right)^2 = p\left(3\alpha^2 + p\right)^2$, c'est-à-dire que α est annulé par le polynôme :

$$\begin{aligned} P(X) &= \left(X^3 + 3pX - q\right)^2 - p\left(3X^2 + p\right)^2 \\ &= X^6 - 3pX^4 - 2qX^3 + 3p^2X^2 - 6pqX + q^2 - p^3 \end{aligned}$$

et ce polynôme est le polynôme minimal de α.

Exercice 4.8. *Soient p un nombre premier et ξ une racine primitive p^2-ième de l'unité. Montrer que ξ est algébrique sur $\mathbb{Q}$ et déterminer son polynôme minimal.*

Solution. Pour tout $n \in \mathbb{N}^*$, une racine n-ième de l'unité est algébrique sur $\mathbb{Q}$ puisque racine de $X^n - 1 = 0$. Si ξ est une racine primitive p^2-ième de l'unité, alors ξ^p est une racine p-ième de l'unité différente de 1 (ξ est d'ordre p^2 dans $(\mathbb{C}^*, \times)$), c'est-à-dire que ξ est annulé par le polynôme cyclotomique $\Phi_{p^2}(X) = \Phi_p(X^p)$ (corollaire **??**). On a $\Phi_{p^2}(X+1) = \sum_{k=0}^{p-1} ((X+1)^p)^k$ avec $\overline{(X+1)^p} = X^p + \overline{1}$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$, de sorte que :

$$\overline{\Phi_{p^2}(X+1)} = \sum_{k=0}^{p-1} \left(X^p + \overline{1}\right)^k = \overline{\Phi_p(X^p+1)}$$

avec $\overline{\Phi_p(X^p+1)} = X^{p(p-1)}$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ (voir l'exercice **??**). Ce dernier résultat se traduit en disant que tous les coefficients du polynôme $\Phi_{p^2}(X+1)$ sauf le coefficient dominant sont divisibles par p. Le coefficient constant $\Phi_{p^2}(1) = p$ n'étant pas divisible par p^2, le critère d'Eisenstein nous dit que $\Phi_{p^2}(X+1)$ est irréductible dans $\mathbb{Q}[X]$ et il en est de même de $\Phi_{p^2}(X)$. Le polynôme Φ_{p^2} est donc le polynôme minimal de toute racine primitive p^2-ième de l'unité. De manière générale, on peut vérifier que pour tout $n \in \mathbb{N}^*$, le polynôme cyclotomique Φ_n est irréductible dans $\mathbb{Q}[X]$ (théorème **??**).

Chapitre 5

Anneaux euclidiens (nouvelle version du 12/12/2024)

5.1 Définitions et premières propriétés

On appelle *stathme* sur un anneau $\mathbb{A}$ commutatif et intègre toute application $\varphi : \mathbb{A}^* \to \mathbb{N}$.

Définition 5.1. *Un anneau commutatif et intègre $\mathbb{A}$ est dit* euclidien*, s'il existe un stathme φ tel que pour tout couple (a,b) d'éléments de $\mathbb{A}$ avec $b \neq 0$, il existe un couple (q,r) dans $\mathbb{A}^2$ tel que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$.*

Avec les notations de la définition précédente, q est un quotient et r un reste dans la division euclidienne de a par b.

On notera $(\mathbb{A}, \varphi)$ un tel anneau euclidien ou tout simplement $\mathbb{A}$, quand le stathme φ est fixé.

Théorème 5.1.

Un anneau euclidien $(\mathbb{A}, \varphi)$ est principal. Précisément, pour tout idéal I de $\mathbb{A}$ non réduit à $\{0\}$, il existe $a_0 \in I \setminus \{0\}$ tel que $\varphi(a_0) = \min\limits_{a \in I \setminus \{0\}} \varphi(a)$ et $I = a_0\mathbb{A}$.

Preuve. Soient $(\mathbb{A}, \varphi)$ un anneau euclidien et I un idéal de $\mathbb{A}$. Si $I = \{0\}$, il est alors principal engendré par 0. Si $I \neq \{0\}$, on note alors $n_0 = \min\limits_{a \in I \setminus \{0\}} \varphi(a)$. Cette borne inférieure existe est atteinte puisque $\varphi(I \setminus \{0\})$ est une partie non vide de $\mathbb{N}$, c'est-à-dire qu'il existe $a_0 \in I \setminus \{0\}$ tel que $n_0 = \varphi(a_0) = \min \varphi(I \setminus \{0\})$. La division euclidienne d'un élément a de I par a_0 donne $a = qa_0 + r$ avec $r = 0$ puisque a_0 est de stathme minimal dans l'idéal $I \setminus \{0\}$ (si $r \neq 0$, alors $r = a - qa_0$ est dans $I \setminus \{0\}$ puisque I est un idéal et $\varphi(r) < \varphi(a_0) = n_0$, ce qui contredit la définition de n_0), donc $a = qa_0$ et $I \subset a_0\mathbb{A}$. Comme par ailleurs $a_0\mathbb{A} \subset I$ puisque I est un idéal, on a $I = a_0\mathbb{A}$. En définitive, $\mathbb{A}$ est principal. □

La réciproque du théorème précédent est fausse, il existe des anneaux principaux non euclidiens (voir le paragraphe 5.4).

Corollaire 5.1. *Un anneau euclidien est nécessairement unitaire.*

Preuve. $\mathbb{A}$ étant un idéal, il existe $a_0 \in \mathbb{A}$ tel que $\mathbb{A} = a_0\mathbb{A}$. Pour tout $a \in \mathbb{A}$, il existe alors un élément $q \in \mathbb{A}$ tel que $a = qa_0$. En particulier il existe $e \in \mathbb{A}$ tel que $a_0 = ea_0$ et en conséquence, pour tout $a = qa_0 \in \mathbb{A}$, on a $ae = qa_0e = qa_0 = a$, ce qui signifie que e est l'élément neutre de $\mathbb{A}$ pour le produit. □

Dans ce qui suit les anneaux considérés sont commutatifs, unitaires et intègres.

Si $\mathbb{A}$ est un corps, on a alors $a = bq$ avec $q = ab^{-1}$ pour tous $(a, b) \in \mathbb{A} \times \mathbb{A}^*$, donc $r = 0$ est un reste et toute application $\varphi : \mathbb{A}^* \to \mathbb{N}$ est un stathme.

On suppose *a priori* pour la suite de ce chapitre que l'anneau $\mathbb{A}$ n'est pas un corps.

Définition 5.2. *Si $(\mathbb{A}, \varphi)$ est un anneau euclidien, on dit alors que le stathme φ est croissant (pour l'ordre de la division) si on a $\varphi(ab) \geq \varphi(a)$ pour tout $(a, b) \in \mathbb{A}^* \times \mathbb{A}^*$.*

Dire qu'un stathme φ sur $\mathbb{A}^*$ est croissant revient aussi à dire que si a, c dans $\mathbb{A}^*$ sont tels que a divise c, on a alors $\varphi(a) \leq \varphi(c)$.

Le lemme qui suit nous dit que si $(\mathbb{A}, \varphi)$ est un anneau euclidien, on peut alors toujours se ramener à un stathme croissant.

Lemme 5.1 *Étant donné un anneau euclidien $(\mathbb{A}, \varphi)$, l'application $\overline{\varphi} : \mathbb{A}^* \to \mathbb{N}$ définie par $\overline{\varphi}(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$ pour tout $a \in \mathbb{A}^*$ est un stathme croissant et $(\mathbb{A}, \overline{\varphi})$ est un anneau euclidien.*

Preuve. Pour tout $a \in \mathbb{A}^*$, l'ensemble $\{\varphi(ax),\ x \in \mathbb{A}^*\}$ est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément, ce qui justifie la définition de l'entier $\overline{\varphi}(a)$. Pour a, b dans $\mathbb{A}^*$, on a $\overline{\varphi}(ab) = \min_{x \in \mathbb{A}^*} \varphi(abx) = \varphi(abx_0) \geq \overline{\varphi}(a)$. Soient a, b dans $\mathbb{A}$ avec $b \neq 0$ et $x_0 \in \mathbb{A}^*$ tel que $\overline{\varphi}(b) = \min_{x \in \mathbb{A}^*} \varphi(bx) = \varphi(bx_0)$. La division euclidienne dans $(\mathbb{A}, \varphi)$ de a par bx_0, $a = bqx_0 + r$ avec $r = 0$ ou $r \neq 0$ et $\overline{\varphi}(r) \leq \varphi(r) < \varphi(bx_0) = \overline{\varphi}(b)$, donne une division euclidienne dans $(\mathbb{A}, \overline{\varphi})$. □

Théorème 5.2.

Soit $(\mathbb{A}, \varphi)$ un anneau euclidien tel que le stathme φ soit croissant.

1. *Pour tout $(a, b) \in \mathbb{A}^* \times \mathbb{A}^*$, on a $\varphi(ab) \geq \varphi(a)$, l'égalité étant réalisée si, et seulement si, b est inversible. En particulier, on a $\varphi(-a) = \varphi(a)$ et $\varphi(ab) > \varphi(a)$ pour a, b non nuls avec b non inversible.*
2. *Pour tout $a \in \mathbb{A}^*$, on a $\varphi(a) = \min_{x \in \mathbb{A}^*} \varphi(ax)$.*
3. *On a $\varphi(1) = \min_{x \in \mathbb{A}^*} \varphi(x)$ et $\mathbb{A}^\times = \{a \in \mathbb{A}^*,\ \varphi(a) = \varphi(1)\}$.*

Preuve.

1. Soit $a \in \mathbb{A}^*$. Comme φ est croissant, on a $\varphi(a) \leq \varphi(ab)$ pour tout $b \in \mathbb{A}^*$. Si $b \in \mathbb{A}^\times$, on a alors $\varphi(ab) \geq \varphi(a)$ et $\varphi(a) = \varphi\left((ab)\,b^{-1}\right) \geq \varphi(ab)$, donc $\varphi(ab) = \varphi(a)$. Si $b \in \mathbb{A}^*$ est tel que $\varphi(a) = \varphi(ab)$, la division euclidienne de a par ab, $a = q(ab) + r$ impose $r = 0$, car sinon on a $r = a(1 - qb) \in \mathbb{A}^*$ avec $\varphi(a) \leq \varphi(a(1 - qb)) = \varphi(r) < \varphi(ab)$, en contradiction avec $\varphi(a) = \varphi(ab)$. On a donc $r = a(1 - qb) = 0$ avec $a \in \mathbb{A}^*$, ce qui impose $qb = 1$ et signifie que b est inversible.

2. Pour tout $x \in \mathbb{A}^*$, on a $\varphi(a) \leq \varphi(ax)$ et $\varphi(a) = \varphi(a \cdot 1)$ avec $1 \in \mathbb{A}^*$, donc $\varphi(a) = \min\limits_{x \in \mathbb{A}^*} \varphi(ax)$. En particulier, on a $\varphi(1) = \min\limits_{x \in \mathbb{A}^*} \varphi(x)$.

3. Pour $a \in \mathbb{A}^*$, on a $\varphi(a) = \varphi(1 \cdot a) = \varphi(1)$ si, et seulement si, $a \in \mathbb{A}^\times$, donc $\mathbb{A}^\times = \{a \in \mathbb{A}^*,\ \varphi(a) = \varphi(1)\}$. □

Nous avons vu avec le corollaire 4.4 qu'un anneau principal est factoriel (définition 3.9) et en conséquence il en est de même pour un anneau euclidien. La démonstration directe du fait qu'un anneau euclidien est factoriel est plus simple.

Théorème 5.3.

Un anneau euclidien $(\mathbb{A}, \varphi)$ est factoriel.

Preuve. Quitte à remplacer le stathme φ par le stathme $\overline{\varphi}$ défini avec le lemme 5.1, on peut supposer que φ est croissant. Pour l'existence d'une décomposition en facteurs irréductibles, on procède par récurrence sur $\varphi(a) \in \mathbb{N}$, pour $a \in \mathbb{A}^*$. Si $\varphi(a) = \varphi(1)$ (la valeur minimale du stathme φ d'après le théorème 5.2), a est alors inversible. Si $\mathbb{A}$ est un corps c'est alors terminé, sinon on se donne $a \in \mathbb{A}^*$ non inversible et on suppose que le résultat est acquis pour tous les éléments b de $\mathbb{A}^*$ tels que $\varphi(b) < \varphi(a)$. Si a est irréductible, c'est alors terminé, sinon il s'écrit $a = bc$ où b et c ne sont pas inversibles et on a $\varphi(b) < \varphi(bc) = \varphi(a)$, $\varphi(c) < \varphi(bc) = \varphi(a)$, donc l'hypothèse de récurrence nous dit que b et c sont des produits finis d'éléments irréductibles. Il en est alors de même de a. Si $a = \prod\limits_{k=1}^{r} p_k = \prod\limits_{j=1}^{s} q_j$ avec $1 \leq r \leq s$, les p_k et q_j étant irréductibles dans $\mathbb{A}$, p_1 est alors un élément irréductible de $\mathbb{A}$ qui divise le produit $\prod\limits_{j=1}^{s} q_j$ et en conséquence il divise l'un des q_i et comme p_1 et q_i sont irréductibles, ils sont nécessairement associés. Dans l'anneau intègre $\mathbb{A}$, on peut alors simplifier par p_1 et il nous reste $\prod\limits_{k=2}^{r} p_k = u \prod\limits_{\substack{j=1 \\ j \neq i}}^{s} q_j$, où u est un élément inversible de $\mathbb{A}$. Au bout de r étapes, on aboutit à $1 = v \prod\limits_{j \in J} q_j$, où v est un élément inversible de $\mathbb{A}$ et J une partie de $\{1, \cdots, s\}$ et comme les q_j sont irréductibles, cette partie est nécessairement vide, ce qui veut dire que $r = s$ et les p_k, q_j sont deux à deux associés. □

5.2 pgcd dans un anneau euclidien

Pour ce paragraphe, $(\mathbb{A}, \varphi)$ est un anneau euclidien qui n'est pas un corps.

Un anneau euclidien étant principal, il est à pgcd (théorème 4.5). Dans un tel anneau, on dispose de l'algorithme d'Euclide pour obtenir le pgcd de deux éléments non nuls, il permet également de déterminer des éléments u et v de $\mathbb{A}$ tels que $au + bv = a \wedge b$. Tout est basé sur le résultat suivant.

Lemme 5.2 *Soient a, b dans $\mathbb{A}^*$ et r un reste dans la division euclidienne de a par b. On a alors $a \wedge b = b$ si $r = 0$ ou $a \wedge b = b \wedge r$ si $r \neq 0$ (à un multiplicateur inversible près).*

Preuve. On a $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$. Si $r = 0$, alors b divise a, donc $(a, b) = (b)$ et $a \wedge b = b$. Si $r \neq 0$, $\delta = a \wedge b$ qui est un diviseur commun à a et b va diviser $r = a - bq$, c'est donc un diviseur commun à b et r et δ divise $\delta' = b \wedge r$. Comme $\delta' = b \wedge r$ est un diviseur commun à b et r, il divise aussi $a = bq + r$, c'est donc un diviseur commun à a et b et δ' divise δ. On a donc $\delta = u\delta'$ avec $\delta' \neq 0$ et $u \in \mathbb{A}^\times$. □

Le principe de l'algorithme d'Euclide est le suivant pour a, b dans $\mathbb{A}^*$ tels que $\varphi(a) \geq \varphi(b)$ (a et b jouent des rôles symétriques).

On note $r_0 = b$ et on désigne par r_1 un reste dans la division euclidienne de a par b. Si $r_1 = 0$, c'est alors terminé : $a \wedge b = r_0 = b$. Sinon, on a $\varphi(r_1) < \varphi(r_0)$ et d'après le lemme précédent $a \wedge b = r_0 \wedge r_1$. On désigne alors par r_2 un reste dans la division euclidienne de r_0 par r_1. Si $r_2 = 0$, c'est alors terminé : $a \wedge b = r_0 \wedge r_1 = r_1$. Sinon, on continu avec $r_0 \wedge r_1 = r_1 \wedge r_2$. On définit donc ainsi une suite $(r_n)_{n \geq 0}$ d'éléments de $\mathbb{A}$ par :

- $r_0 = b$;
- r_1 est un reste dans la division euclidienne de a par b ; on a donc $r_1 = 0$ ou $0 \leq \varphi(r_1) < \varphi(r_0)$;
- pour $n \geq 2$, si $r_{n-1} = 0$ alors $r_n = 0$, sinon r_n est un reste dans la division euclidienne de r_{n-2} par r_{n-1} et on a $r_n = 0$ ou $0 \leq \varphi(r_n) < \varphi(r_{n-1})$.

Il existe alors $p \in \mathbb{N}^*$ tel que $r_p = 0$, $0 \leq \varphi(r_{p-1}) < \cdots < \varphi(r_1) < \varphi(r_0)$ et $a \wedge b = r_0 \wedge r_1 = \cdots = r_{p-1} \wedge r_p = r_{p-1}$, c'est à dire que $a \wedge b$ est le dernier reste non nul dans cette suite finie de divisions euclidiennes. On a en fait construit avec l'algorithme d'Euclide, dans le cas où b ne divise pas a, deux suites $(r_n)_{0 \leq n \leq p}$ et $(q_n)_{1 \leq n \leq p}$ d'éléments de $\mathbb{A}$ de la manière suivante :

$$\begin{cases} a = q_1 r_0 + r_1 \ \ (r_1 \neq 0 \text{ et } \varphi(r_1) < \varphi(r_0)) \\ r_0 = q_2 r_1 + r_2 \ \ (r_2 \neq 0 \text{ et } \varphi(r_2) < \varphi(r_1)) \\ \vdots \\ r_{p-3} = q_{p-1} r_{p-2} + r_{p-1} \ \ (r_{p-1} \neq 0 \text{ et } \varphi(r_{p-1}) < \varphi(r_{p-2})) \\ r_{p-2} = q_p r_{p-1} + r_p \ \ (r_p = 0) \end{cases}$$

On vérifie alors qu'il existe u_k et v_k dans $\mathbb{A}$ tels que $r_k = au_k + bv_k$. Pour $k = 0$ et $k = 1$ on a $r_0 = b = a \cdot 0 + b \cdot 1$ et $r_1 = a \cdot 1 + b(-q_1)$. En supposant le résultat

acquis jusqu'à l'ordre $k-1$ pour $0 \leq k-1 \leq p-2$ on a :

$$\begin{aligned} r_k &= -q_k r_{k-1} + r_{k-2} = -q_k \left(au_{k-1} + bv_{k-1}\right) + au_{k-2} + bv_{k-2} \\ &= a\left(u_{k-2} - q_k u_{k-1}\right) + b\left(v_{k-2} - q_k v_{k-1}\right) = au_k + bv_k \end{aligned}$$

En particulier pour $k = p-1$ on a $a \wedge b = r_{p-1} = au_{p-1} + bv_{p-1} = au + bv$. Un tel couple (u, v) n'est pas unique puisque si (u, v) est une solution, pour tout $\lambda \in \mathbb{A}$, le couple $(u', v') = (u + \lambda b, v - \lambda a)$ est aussi solution.

Dans le cas de l'anneau des entiers relatifs, on peut donner une majoration du nombre de divisions euclidiennes que nécessite l'algorithme d'Euclide pour calculer le pgcd de deux entiers naturels $a > b \geq 1$. Pour ce faire nous utiliserons le résultat suivant sur la *suite de Fibonacci* définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour tout entier $n \geq 2$.

Lemme 5.3 *Pour tout $n \in \mathbb{N}$, on a $F_n = \dfrac{\varphi^n - (1-\varphi)^n}{\sqrt{5}}$ où $\varphi = \dfrac{1+\sqrt{5}}{2}$ est le le* nombre d'or.

Preuve. Le polynôme caractéristique de la relation de récurrence définissant la suite $(F_n)_{n\in\mathbb{N}}$ est $P(X) = X^2 - X - 1$ et ce polynôme a pour racines $\varphi = \dfrac{1+\sqrt{5}}{2}$ et $1 - \varphi = -\dfrac{1}{\varphi} = \dfrac{1-\sqrt{5}}{2}$ (somme et produit des racines). Il en résulte l'existence de deux constantes réelles α, β telles que $F_n = \alpha\varphi^n + \beta(1-\varphi)^n$ pour tout $n \in \mathbb{N}$. Les conditions initiales nous donnent $F_0 = \alpha + \beta = 0$ et $F_1 = \alpha\varphi + \beta(1-\varphi) = 1$, donc $\beta = -\alpha$ et $(2\varphi - 1)\alpha = 1$, soit $\alpha = \dfrac{1}{2\varphi - 1} = \dfrac{1}{\sqrt{5}}$ et $F_n = \dfrac{\varphi^n - (1-\varphi)^n}{\sqrt{5}}$ pour tout $n \in \mathbb{N}$. □

Théorème 5.4. Lamé

Le nombre de divisions euclidiennes que nécessite l'algorithme d'Euclide pour calculer le pgcd *de deux entiers naturels $a > b \geq 1$ est inférieur ou égal à 5 fois le nombre de chiffres de b dans son écriture décimale.*

Preuve. L'algorithme d'Euclide pour calculer le pgcd de a et b consiste à construire la suite d'entiers $(r_n)_{-1\leq n\leq p}$ comme suit :

- $r_{-1} = a$, $r_0 = b$, $0 \leq r_1 < r_0$ est le reste dans la division euclidienne de $r_{-1} = a$ par $r_0 = b$;
- si $r_1 = 0$, on a alors $p = 1$ et $a \wedge b = b$, sinon pour $1 \leq n \leq p-1$, $0 \leq r_n < r_{n-1}$ est le reste dans la division euclidienne de r_{n-2} par r_{n-1} ;
- $r_p = 0$.

On a $r_p = 0 < r_{p-1} < \cdots < r_1 < r_0$ et $a \wedge b = r_0 \wedge r_1 = \cdots = r_{p-1} \wedge r_p = r_{p-1}$, c'est à dire que $a \wedge b$ est le dernier reste non nul r_{p-1} dans cette suite de divisions euclidiennes. L'algorithme d'Euclide a donc nécessité $p-1$ divisions euclidiennes. La dernière division, qui donne un reste nul, n'est pas comptée.

Il existe alors deux suites d'entiers relatifs $(u_n)_{0\leq n\leq p-1}$ et $(v_n)_{0\leq n\leq p-1}$ telles que $r_n = au_n + bv_n$ pour tout n compris entre 0 et $p-1$.

On vérifie par récurrence finie que l'on a $r_{p-k} \geq F_k$ pour tout entier k compris entre 0 et p.

En effet, pour $k=0$, on a $r_p = 0 = F_0$. Pour $k=1$, on a $r_{p-1} \geq 1 = F_1$ (r_{p-1} est le dernier reste non nul). Supposant le résultat acquis jusqu'au rang $k-1$ avec $2 \leq k \leq p$. Par construction, on a :

$$r_{p-k} = q_{p-(k-2)} r_{p-(k-1)} + r_{p-(k-2)} \ \left(0 < r_{p-(k-2)} < r_{p-(k-1)}\right)$$

donc $q_{p-(k-2)} \geq 1$ puisque $0 < r_{p-(k-1)} < r_{p-k}$ et :

$$r_{p-k} \geq r_{p-(k-1)} + r_{p-(k-2)} \geq F_{k-1} + F_{k-2} = F_k$$

En particulier, on a pour $k=p$, $r_0 = b \geq F_p$.

En désignant par m le nombre de chiffres dans l'écriture de l'entier b en base 10, on a $b = \sum_{k=0}^{m-1} b_k 10^k$ où $b_{m-1} \geq 1$ et $10^{m-1} \leq b < 10^m$, donc $10^m \geq b+1$ et $m \geq \dfrac{\ln(b+1)}{\ln(10)} = \log_{10}(b+1)$. D'autre part, on a $b \geq F_p = \dfrac{\varphi^p - (1-\varphi)^p}{\sqrt{5}}$ avec $|1-\varphi| = \dfrac{\sqrt{5}-1}{2} < 1$, donc $\dfrac{|1-\varphi|^p}{\sqrt{5}} < 1$ et $b+1 \geq \dfrac{\varphi^p}{\sqrt{5}} + \left(1 - \dfrac{(1-\varphi)^p}{\sqrt{5}}\right) \geq \dfrac{\varphi^p}{\sqrt{5}}$, ce qui nous donne :

$$m \geq \log_{10}(b+1) \geq \log_{10}\left(\frac{\varphi^p}{\sqrt{5}}\right) = p\log_{10}(\varphi) - \log_{10}\left(\sqrt{5}\right)$$

et $p \leq \dfrac{m + \log_{10}\left(\sqrt{5}\right)}{\log_{10}(\varphi)}$.

On a donc $p-1 \leq \alpha m + \beta$ avec $\alpha = \dfrac{1}{\log_{10}(\varphi)} \backsimeq 4.78$, $\beta = \dfrac{\log_{10}\left(\sqrt{5}\right)}{\log_{10}(\varphi)} - 1 \backsimeq 0.67$. Comme $p-1$ est un entier, on a en fait $p-1 \leq [\alpha m + \beta]$. Il nous suffit donc de montrer que $f(m) = [\alpha m + \beta] \leq 5m$ pour tout $m \in \mathbb{N}^*$. Pour $m = 1, 2, 3$, on a :

$$f(1) = [\alpha + \beta] = 5,\ f(2) = [2\alpha + \beta] = 10,\ f(3) = [3\alpha + \beta] = 15$$

et pour $m \geq 4$, $\alpha m + \beta \backsimeq 4.785 \cdot m + 0.672 = 5m + (0.672 - 0.215 \cdot m)$ avec $0.215 \cdot m - 0.672 \geq 0.215 \cdot 4 - 0.672 \backsimeq 0.188 > 0$, donc $\alpha m + \beta \leq 5m$ et $p - 1 \leq 5m$, soit le résultat annoncé. □

5.3 Quelques exemples d'anneaux euclidiens

5.3.1 L'anneau $\mathbb{Z}$ des entiers relatifs

Lemme 5.4 *Soit α un réel. Pour tout couple d'entiers (a,b), avec $b \neq 0$, il existe un unique couple d'entiers (q,r) tel que $a = bq + r$ et $\alpha \leq r < \alpha + |b|$.*

Preuve. Soit $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ et $E = \{k \in \mathbb{Z},\ a - bk \geq \alpha\}$. Cet ensemble est non vide (comme $\lim_{k \to -\infty} (a - bk) = +\infty$, il existe $k \leq 0$ tel que $a - bk \geq \alpha$) et

majoré (la condition $a - bk \geq \alpha$ équivaut à $k \leq \dfrac{a-\alpha}{b}$), donc il admet un plus grand élément q et on a $q \in E$, $q+1 \notin E$, soit $qb \leq a - \alpha < (q+1)\,b$. En posant $r = a - bq$, on a $a = bq + r$ avec $\alpha \leq r = a - bq < \alpha + b = \alpha + |b|$. Pour $b \leq -1$, on a l'existence de $(q', r') \in \mathbb{Z}^2$ tel que $a = (-b)\,q' + r'$, $\alpha \leq r' < \alpha + |b|$ et il suffit de poser $q = -q'$, $r = r'$. Supposons qu'il existe deux couples d'entiers (q, r) et (q', r') tels que $a = bq + r = bq' + r'$ et $\alpha \leq r, r' < \alpha + |b|$. Si $q \neq q'$, on a alors $|r - r'| = |b\,(q - q')| \geq |b|$ avec r et r' dans l'intervalle $[\alpha, \alpha + |b|[$, ce qui est impossible (faire un dessin). On a donc $q = q'$ et $r = r'$, soit l'unicité du quotient et du reste. □

Pour $\alpha = 0$, on retrouve le théorème classique de division euclidienne avec un reste positif. Pour $\alpha = -\dfrac{|b|}{2}$, le reste est dans $\left[-\dfrac{|b|}{2}, \dfrac{|b|}{2}\right[$ et c'est le reste de plus petite valeur absolue.

Théorème 5.5.

L'anneau $\mathbb{Z}$ est euclidien pour le stathme $\varphi : n \in \mathbb{Z}^* \mapsto |n|$.

Preuve. Il suffit de prendre $\alpha = 0$ dans le lemme précédent. □

La condition $|r| < |b|$ n'assure pas l'unicité du quotient et du reste. Par exemple, on a deux divisions de 12 par 5 dans $(\mathbb{Z}, |\cdot|)$, $12 = 3 \times 5 - 3 = 2 \times 5 + 2$ (voir aussi l'exercice 5.2 pour cette question d'unicité du quotient et du reste).

Une application importante du théorème de division euclidienne dans $\mathbb{Z}$ est le théorème de numération dans une base.

Théorème 5.6.

Soit b un entier supérieure ou égal à 2. Pour tout $n \in \mathbb{N}^*$, il existe un unique entier p et un unique $(p+1)$-uplet $(n_k)_{0 \leq k \leq p} \in \mathbb{N}^{p+1}$ tels que $n_p \neq 0$, $0 \leq n_k \leq b-1$ pour tout $k \in \{0, 1, \cdots, p\}$ et $n = \displaystyle\sum_{k=0}^{p} n_k b^k$.

Preuve. En remarquant que $\mathbb{N}^* = \displaystyle\bigcup_{j=0}^{+\infty} \left[b^j, b^{j+1}\right[$, il suffit de montrer le résultat pour tout entier n dans $\left[b^j, b^{j+1}\right[$ où j décrit $\mathbb{N}$. Pour $j = 0$ tout $n \in [1, b[$ s'écrit sous la forme $n = \displaystyle\sum_{k=0}^{p} n_k b^k$ avec $p = 0$ et $n_0 = n$. Supposons le résultat acquis pour $j \geq 0$ et soit $n \in \left[b^{j+1}, b^{j+2}\right[$. En utilisant le théorème de division euclidienne on peut écrire $n = bq + n_0$ avec $0 \leq n_0 \leq b-1$. On a alors $bq = n - n_0 > b^{j+1} - b = b\left(b^j - 1\right)$, donc $q > b^j - 1$, soit $q \geq b^j$. On a également $q = \dfrac{n - n_0}{b} < b^{j+1} - \dfrac{n_0}{b} \leq b^{j+1}$. En définitive $q \in \left[b^j, b^{j+1}\right[$ et avec l'hypothèse de récurrence il s'écrit $q = \displaystyle\sum_{k=0}^{p} q_k b^k$ avec $q_p \neq 0$. D'où $n = bq + n_0 = \displaystyle\sum_{k=0}^{p+1} n_k b^k$ avec $n_k = q_{k-1}$ pour tout $k \in \{1, \cdots, p+1\}$. En particulier $n_{p+1} = q_p \neq 0$. Supposons

que l'on ait deux écritures $n = \sum_{k=0}^{p} n_k b^k = \sum_{k=0}^{p'} n'_k b^k$ avec $p' \geq p$, $0 \leq n_k \leq b-1$, $0 \leq n'_k \leq b-1$, $n_p \neq 0$ et $n'_{p'} \neq 0$. On a alors :

$$b^p \leq n \leq \sum_{k=0}^{p} (b-1)\, b^k = b^{p+1} - 1 < b^{p+1}$$

De même $b^{p'} \leq n < b^{p'+1}$. Donc $b^{p'} < b^{p+1}$ soit $b^{p'-p} < b$ et nécessairement $p = p'$. En remarquant que n_0 est le reste dans la division euclidienne de n par b, on déduit que $n_0 = n'_0$ puis par récurrence que $n_k = n'_k$ pour tout $k \in \{1, \cdots, p\}$. D'où l'unicité de la décomposition. □

Dans la décomposition $n = \sum_{k=0}^{p} n_k b^k$ on a $b^p \leq n < b^{p+1}$, c'est-à-dire que p est le plus grand entier vérifiant $b^p \leq n$.

Avec les notations du théorème précédent, on dit que l'écriture $n = \sum_{k=0}^{p} n_k b^k$ est la représentation en base b de l'entier n. On note $n = \overline{n_p \cdots n_1 n_0}^b$ et on dit que les n_k sont les chiffres dans l'écriture en base b de n.

5.3.2 L'anneau $\mathbb{D}$ des nombres décimaux

On peut définir l'anneau $\mathbb{D}$ des nombres décimaux comme le sous-anneau $\mathbb{Z}\left[\frac{1}{10}\right]$ de $\mathbb{Q}$ image de $\mathbb{Z}[X]$ par le morphisme d'anneaux $P \in \mathbb{Z}[X] \mapsto P\left(\frac{1}{10}\right) \in \mathbb{Q}$. Un nombre décimal est donc de la forme $x = P\left(\frac{1}{10}\right)$ où $P \in \mathbb{Z}[X]$.

On peut vérifier que l'application $P \in \mathbb{Z}[X] \mapsto P\left(\frac{1}{10}\right) \in \mathbb{D}$ passe au quotient en un isomorphisme de l'anneau $\frac{\mathbb{Z}[X]}{(10X-1)}$ sur $\mathbb{D}$ (exercice 5.3).

Une définition équivalente est donnée par le théorème qui suit.

Théorème 5.7.

Un nombre rationnel est décimal si, et seulement si, il est de la forme $\frac{a}{10^m}$ où a est un entier relatif et m est un entier naturel.

Preuve. Si $x = \sum_{k=0}^{m} \frac{a_k}{10^k}$ est décimal, en réduisant au même dénominateur, il s'écrit $\frac{a}{10^m}$ où $a \in \mathbb{Z}$. Réciproquement si $x = \frac{a}{10^m}$, on a alors la division euclidienne $a = a_0 10^m + r$ où $a_0 \in \mathbb{Z}$ et r est entier compris entre 0 et $10^m - 1$ qui s'écrit en

base 10 sous la forme $r = \sum_{k=0}^{n} r_k 10^k$ avec $n < m$, les r_k étant entiers compris entre 0 et 9, donc $x = a_0 + \sum_{k=0}^{n} \frac{r_k}{10^{m-k}}$ est décimal. □

Du théorème précédent, on déduit qu'un nombre décimal non nul peut s'écrire sous la forme $d = n2^p5^q$, où n, p, q sont des entiers relatifs avec $n \neq 0$ premier avec 10 et une telle décomposition est unique. En effet, si $n'2^{p'}5^{q'} = n2^p5^q$ où n, n' sont non nuls premiers avec 10, on a $n'2^{\alpha+p'}5^{\beta+q'} = n2^{\alpha+p}5^{\beta+q}$ en notant $\alpha = |p| + |p'|$ et $\beta = |q| + |q'|$, de sorte que les exposants de 2 et 5 qui apparaissent dans cette égalité sont positifs. L'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}$ impose alors que $\alpha + p' = \alpha + p$ et $\beta + q' = \beta + q$, soit $p = p'$ et $q = q'$, puis $n = n'$. Une telle écriture d'un nombre décimal est appelée *écriture canonique*.

L'anneau $\mathbb{D} = \mathbb{Z}\left[\frac{1}{10}\right]$ des décimaux n'est pas un corps. Un rationnel $r = \frac{a}{10^m}$ est inversible dans $\mathbb{D}$ si, et seulement si, il existe un entier relatif b et un entier naturel n tels que $\frac{a}{10^m}\frac{b}{10^n} = 1$, ce qui revient à dire que $ab = 10^{n+m}$ ou encore que 2 et 5 sont les seuls diviseurs premiers possibles de a et b. En définitive le groupe multiplicatif des nombres décimaux inversibles est $\mathbb{D}^\times = \left\{r = \pm 2^\alpha 5^\beta,\ (\alpha, \beta) \in \mathbb{Z}^2\right\}$.

On peut vérifier de diverses manières que l'anneau $\mathbb{D}$ des nombres décimaux est principal (voir les théorèmes 4.1 et 4.2). Ce caractère principal peut aussi se déduire du fait qu'il est euclidien.

Théorème 5.8.

L'anneau $\mathbb{D}$ des nombres décimaux est euclidien pour le stathme φ défini, en utilisant l'écriture canonique d'un nombre décimal, par :

$$\forall a = n2^p5^q \in \mathbb{D}^*,\ \varphi(a) = |n|$$

Preuve. On a bien $\varphi(a) \in \mathbb{N}$ pour tout $a \in \mathbb{D}^*$. Soient $a = n2^p5^q$ et $b = n'2^{p'}5^{q'}$ dans $\mathbb{D}^*$. La division euclidienne dans $\mathbb{Z}$, $n = q_1 n' + r_1$ avec $0 \leq r_1 < |n'|$, nous donne :

$$a = (q_1 n' + r_1)\, 2^p 5^q = \left(q_1 2^{p-p'} 5^{q-q'}\right) b + r_1 2^p 5^q = q_2 b + r_1 2^p 5^q$$

avec $q_2 = q_1 2^{p-p'} 5^{q-q'} \in \mathbb{D}$. Si $r_1 = 0$, on a alors $a = q_2 b + r_2$ avec $r_2 = 0$ et $q_2 \in \mathbb{D}$. Si $r_1 \neq 0$, de la décomposition en facteurs premiers de r_1, on déduit que $r_1 = s2^\alpha 5^\beta$, l'entier s étant non nul premier avec 10, ce qui nous donne $a = q_2 b + r_2$ avec $q_2 \in \mathbb{D}$ et $r_2 = s2^{p+\alpha}5^{q+\beta} \in \mathbb{D}^*$ tel que $\varphi(r_2) = |s| \leq r_1 < |n'| = \varphi(b)$. On a donc bien une division euclidienne dans $\mathbb{D}$ pour le stathme φ. □

On vérifie facilement que le stathme φ défini sur $\mathbb{D}$ est croissant. En effet, pour $a = n2^p5^q \in \mathbb{D}^*$ et $b = n'2^{p'}5^{q'} \in \mathbb{D}^*$, on a :

$$\varphi(ab) = \varphi\left(nn'2^{p+p'}5^{q+q'}\right) = |nn'| \geq |n| = \varphi(a)$$

Avec le théorème 5.2, on retrouve le fait que :

$$\mathbb{D}^\times = \{r = n2^p5^q,\ |n| = 1\} = \left\{r = \pm 2^p 5^q,\ (p, q) \in \mathbb{Z}^2\right\}$$

(on utilise l'écriture canonique d'un nombre décimal).

5.3.3 L'anneau des entiers de Gauss, théorème des deux carrés

Avec l'exercice 3.2 nous avons vu que pour tout $n \in \mathbb{N}^*$, l'ensemble :

$$\mathbb{Z}\left[i\sqrt{n}\right] = \left\{P\left(i\sqrt{n}\right),\ P \in \mathbb{Z}[X]\right\} = \left\{a + ib\sqrt{n},\ (a,b) \in \mathbb{Z}^2\right\}$$

est un sous-anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe.

Théorème 5.9.

Pour $n \in \mathbb{N}^*$, l'anneau $\mathbb{Z}\left[i\sqrt{n}\right]$ est euclidien si, et seulement si, on a $n \in \{1,2\}$.

Preuve. Pour $n \geq 3$, nous avons vu que 2 est irréductible non premier dans $\mathbb{Z}\left[i\sqrt{n}\right]$ (exercice 3.2), donc cet anneau n'est pas principal et en conséquence non euclidien.

Pour $n \in \{1,2\}$ et u, v non nuls dans $\mathbb{Z}\left[i\sqrt{n}\right]$, en écrivant que $\dfrac{u}{v} = x + iy\sqrt{n}$ où $(x,y) \in \mathbb{R}^2$, il existe $(a,b) \in \mathbb{Z}^2$ tel que $(x,y) \in \left[a - \dfrac{1}{2}, a + \dfrac{1}{2}\right[\times \left[b - \dfrac{1}{2}, b + \dfrac{1}{2}\right[$, donc $q = a + ib\sqrt{n} \in \mathbb{Z}\left[i\sqrt{n}\right]$ et :

$$\left|\frac{u}{v} - q\right|^2 = \left|(x-a) + i\,(y-b)\,\sqrt{n}\right|^2 = (x-a)^2 + n\,(y-b)^2 \leq \frac{n+1}{4} < 1$$

soit $|u - qv| < |v|$. En posant $r = u - qv$, on a $u = qv + r$ où $q \in \mathbb{Z}\left[i\sqrt{n}\right]$ et $r \in \mathbb{Z}\left[i\sqrt{n}\right]$ est tel que $\varphi(r) = |r|^2 < |v|^2 = \varphi(v)$, ce qui nous donne une division euclidienne dans $\mathbb{Z}\left[i\sqrt{n}\right]$ pour $n = 1, 2$. □

Pour $n = 1$, l'anneau $\mathbb{Z}[i]$ est l'anneau des *entiers de Gauss*. Il peut être utilisé pour caractériser les entiers naturels qui sont sommes de deux carrés d'entiers.

On note $\Sigma_2 = \left\{n \in \mathbb{N},\ \exists\,(a,b) \in \mathbb{Z}^2;\ n = a^2 + b^2\right\}$ l'ensemble des entiers naturels qui s'écrivent comme somme de deux carrés. On peut remarquer que Σ_2 est non vide, puisqu'il contient $0, 1, 2 = 1^2 + 1^2$ et plus généralement tous les carrés d'entiers $n = a^2 + 0$.

Un entier naturel $n \in \Sigma_2 \setminus \{0,1\}$ est nécessairement réductible dans $\mathbb{Z}[i]$. En effet un tel entier s'écrit $n = a^2 + b^2 = u \cdot \overline{u}$ avec $u = a + ib$ et $\overline{u} = a - ib$ non inversibles dans $\mathbb{Z}[i]$ puisque $|u|^2 = n \geq 2$ (avec l'exercice 3.2 nous avons vu que $\mathbb{Z}\left[i\sqrt{n}\right]^\times = \{u \in \mathbb{Z}\left[i\sqrt{n}\right],\ |u| = 1\}$).

Lemme 5.5 *Si $n \in \Sigma_2$, il est alors congru à 0, 1 ou 2 modulo 4. Dans le cas particulier où n est impair, il est congru à 1 modulo 4.*

Preuve. Pour tout $a \in \mathbb{Z}$, l'entier a^2 est congru à 0 ou 1 modulo 4 (pour $a = 2k$, on a $a^2 = 4k^2 \equiv 0 \bmod (4)$ et pour $a = 2k+1$, on a $a^2 = 4\left(k^2 + k\right) + 1 \equiv 1 \bmod (4)$), donc tout $n = a^2 + b^2 \in \Sigma_2$ est congru à 0, 1 ou 2 modulo 4. Un entier impair étant congru à 1 ou 3 modulo 4, sera congru à 1 modulo 4 s'il est dans Σ_2. □

Lemme 5.6 *L'ensemble Σ_2 est stable pour le produit, c'est-à-dire que le produit de deux entiers naturels qui sont somme de deux carrés est somme de deux carrés.*

Preuve. Soient $n = a^2 + b^2$ et $m = c^2 + d^2$ dans Σ_2, où a, b, c, d sont des entiers relatifs. En écrivant que $n = |u|^2$ et $m = |v|^2$ avec $u = a + ib$ et $v = c + id$ dans $\mathbb{Z}[i]$, on a :

$$nm = |u|^2 |v|^2 = |uv|^2 = |(ac - bd) + (ad + bc)\, i|^2 = (ac - bd)^2 + (ad + bc)^2$$

c'est-à-dire que nm est somme de deux carrés d'entiers. □

En utilisant la décomposition en facteurs premiers dans l'anneau $\mathbb{Z}$, il nous suffit donc de caractériser les nombres premiers qui sont sommes de deux carrés pour décrire Σ_2.

Lemme 5.7 *Un nombre premier impair $p \geq 3$ est congru à 1 modulo 4 si, et seulement si, $-\overline{1}$ est un carré dans $\mathbb{F}_p^* = \dfrac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{\overline{0}\}$, ce qui revient à dire qu'il existe un entier $a \geq 2$ tel que p divise $1 + a^2$.*

Preuve. Un nombre premier impair $p \geq 3$ est congru à 1 ou à 3 modulo 4.

Si p est congru à 1 modulo 4, il s'écrit alors $p = 4q + 1$ où $q \in \mathbb{N}^*$ et l'entier $m = \dfrac{p-1}{2} = 2q$ est pair non nul. Avec $2m = p - 1 \equiv -1 \bmod p$, on déduit que $m + 1 \equiv -m \bmod p$ et pour tout entier k compris entre 1 et $m - 1$, on a :

$$m + k + 1 \equiv -m + k = -(m - k) \bmod p$$

de sorte que :

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot \cdots \cdot m \cdot (m+1) \cdot \cdots \cdot (m+m) \\ &\equiv m!\,(-1)^m\, m \cdot (m-1) \cdot \cdots \cdot 1 = (m!)^2 \bmod p\end{aligned}$$

(m est pair). D'autre part, le théorème de Wilson nous dit que pour p premier, on a $(p-1)! \equiv -1 \bmod p$ (théorème **??**). On a donc $-\overline{1} = \overline{a}^2$ dans $\mathbb{F}_p^*$ où $a = m! \geq 2$, ce qui signifie que p divise $a^2 + 1$.

Si p est congru à 3 modulo 4, il s'écrit alors $p = 4q + 3$ où $q \in \mathbb{N}$ et l'entier $m = \dfrac{p-1}{2} = 2q + 1$ est impair. Si $-\overline{1}$ est un carré dans $\mathbb{F}_p^*$, il existe alors un entier a compris entre 1 et $p - 1$ tel que $-\overline{1} = \overline{a}^2$, ce qui implique que l'on a $\overline{a}^{p-1} = \overline{a}^{2m} = \left(-\overline{1}\right)^m = \left(-\overline{1}\right)^{2q+1} = -\overline{1}$, ce qui contredit le théorème de Fermat qui nous dit que $x^{p-1} = \overline{1}$ pour tout $x \in \mathbb{F}_p^*$ (on a $-\overline{1} \neq \overline{1}$ puisque $p \neq 2$).

En définitive, on a montré que p est congru à 1 modulo 4 si, et seulement si, $-\overline{1}$ est un carré dans $\mathbb{F}_p^*$. □

Théorème 5.10. Fermat

Un nombre premier $p \geq 2$ est somme de deux carrés d'entiers si, et seulement si, il est égal à 2 ou congru à 1 modulo 4.

Preuve. On sait déjà que $2 \in \Sigma_2$. Si p est un nombre premier impair somme de deux carrés, le lemme 5.5 nous dit alors qu'il est congru à 1 modulo 4.

Réciproquement, si p est un nombre premier impair congru à 1 modulo 4, le lemme 5.5 nous dit alors qu'il existe un entier $a \geq 2$ tel que p divise $1+a^2$ et p est nécessairement réductible dans $\mathbb{Z}[i]$ (sinon p est premier dans $\mathbb{Z}[i]$ puisque cet anneau est principal et p qui divise $(1+ia)(1-ia)$ dans $\mathbb{Z}[i]$ va diviser $1+ia$ ou $1-ia$, donc p divise 1 et a dans $\mathbb{Z}$, ce qui est impossible). Il existe donc u, v non inversibles dans $\mathbb{Z}[i]$ tels que $p = u \cdot v$, ce qui nous donne $p^2 = |u|^2 |v|^2$ dans $\mathbb{N}$ avec $|u|^2 \geq 2$ et $|v|^2 \geq 2$ et nécessairement $|u|^2 = |v|^2 = p$, soit $p = \alpha^2 + \beta^2$ est somme de deux carrés. □

Lemme 5.8 *Si $n \in \Sigma_2 \setminus \{0\}$ admet un diviseur premier p congru à 3 modulo 4, il est alors divisible par p^2 et $\dfrac{n}{p^2} \in \Sigma_2$.*

Preuve. Soit $n = a^2 + b^2 \in \Sigma_2 \setminus \{0\}$. Si p est un diviseur premier impair de n, on a alors dans $\mathbb{F}_p$, $\overline{a}^2 = -\overline{b}^2$. Si $\overline{a} \neq \overline{0}$ [resp. si $\overline{b} \neq \overline{0}$], il est alors inversible dans le corps $\mathbb{F}_p$ et $x = \dfrac{\overline{b}}{\overline{a}}$ [resp. $x = \dfrac{\overline{a}}{\overline{b}}$] est solution de $x^2 = -\overline{1}$, ce qui équivaut à dire d'après le lemme 5.5 que p est congru à 1 modulo 4. Donc pour p congru à 3 modulo 4, on a $\overline{a} = \overline{b} = \overline{0}$, ce qui signifie que p divise a et b, soit $a = p\alpha$, $b = p\beta$ et $n = a^2 + b^2 = p^2\left(\alpha^2 + \beta^2\right)$. □

Théorème 5.11. Fermat

Un entier $n \in \mathbb{N}^*$ est somme de deux carrés d'entiers si, et seulement si, ses éventuels diviseurs premiers congrus à 3 modulo 4 qui apparaissent dans sa décomposition en facteurs premiers y figurent avec un exposant pair.

Preuve. Pour la condition est nécessaire, on procède par récurrence sur $n \geq 1$. $n = 1$ n'a pas de diviseur premier. Supposons le résultat acquis pour les entiers de $\Sigma_2 \setminus \{0\}$ strictement inférieurs à n, où $n \in \Sigma_2 \setminus \{0\}$. Si n admet un diviseur premier p congru à 3 modulo 4, le lemme précédent nous dit alors que p^2 divise n et $\dfrac{n}{p^2} < n$ est dans $\Sigma_2 \setminus \{0\}$, donc ses éventuels diviseurs premiers congrus à 3 modulo 4 apparaissent avec une puissance paire et il en est de même pour n. Réciproquement supposons que la décomposition en facteurs premiers de $n \in \mathbb{N} \setminus \{0\}$ soit de la forme $n = 2^{m_1} p_2^{m_2} \cdots p_r^{m_r} q_1^{2r_1} \cdots q_s^{2r_s}$, où $m_1 \geq 0$, les p_j sont des nombres premiers congrus à 1 modulo 4 (s'il en existe) et les q_j des nombres premiers congrus à 3 modulo 4 (s'il en existe). Comme $1, 2$, les p_j et les q_j^2 sont dans Σ_2 qui est stable par multiplication, on en déduit que $n \in \Sigma_2$. □

5.3.4 Les anneaux $\mathbb{Z}[\omega]$ pour ω entier quadratique

On se donne un nombre complexe non réel $\omega = x + iy$ où $x \in \mathbb{R}$ et $y \in \mathbb{R}^*$ auquel on associe le sous-groupe additif de $\mathbb{C}$ engendré par 1 et ω :

$$\mathbb{Z} + \mathbb{Z}\omega = \left\{a + b\omega,\ (a,b) \in \mathbb{Z}^2\right\}$$

Lemme 5.9 *Le groupe additif $\mathbb{Z} + \mathbb{Z}\omega$ est un anneau si, et seulement si, ω est un entier quadratique, c'est-à-dire racine d'un polynôme de degré égal à 2, $P(X) = X^2 - \alpha X - \beta$ à coefficients entiers et irréductible dans $\mathbb{Q}[X]$.*

Preuve. Si $\mathbb{Z}+\mathbb{Z}\omega$ est un anneau, on a alors $\omega^2 \in \mathbb{Z}+\mathbb{Z}\omega$ et en conséquence, il existe $(\alpha,\beta) \in \mathbb{Z}^2$ tel que $\omega^2 = \alpha\omega+\beta$, ce qui signifie que $P(\omega)=0$, où $P(X) = X^2-\alpha X-\beta \in \mathbb{Z}[X]$. Les racines ω et $\overline{\omega}$ de ce polynômes étant non réelles, il en résulte que P est irréductible dans $\mathbb{Q}[X]$. Le nombre complexe ω est donc un entier algébrique de degré 2, soit un entier quadratique.

Réciproquement, si ω est un entier quadratique, il existe alors $(\alpha,\beta) \in \mathbb{Z}^2$ tel que $\omega^2 = \alpha\omega+\beta$ et pour tous $u = a+b\omega$, $v = c+d\omega$ dans $\mathbb{Z}[\omega]$, on a $u\cdot v = ac+(ad+bc)\,\omega+bd\omega^2 \in \mathbb{Z}[\omega]$, donc $\mathbb{Z}+\mathbb{Z}\omega$ est un sous-anneau de $\mathbb{C}$ (on a bien $1 \in \mathbb{Z}+\mathbb{Z}\omega$). □

On suppose dans ce qui suit que ω est un entier quadratique non réel de polynôme minimal $P_\omega(X) = X^2-\alpha X-\beta \in \mathbb{Z}[X]$. La division euclidienne dans $\mathbb{Z}[X]$ par le polynôme minimal P_ω nous montre que :

$$\mathbb{Z}+\mathbb{Z}\omega = \mathbb{Z}[\omega] = \{P(\omega),\ P \in \mathbb{Z}[X]\}$$

Théorème 5.12.

Soit ω un entier quadratique non réel.

1. *L'anneau $\mathbb{Z}[\omega]$ est stable par l'opération de conjugaison complexe $z \mapsto \overline{z}$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\overline{\omega}]$.*
2. *Pour tout entier relatif n, on a $\mathbb{Z}[\omega] = \mathbb{Z}[n+\omega]$.*
3. *Il existe un entier quadratique $\omega' = x'+iy'$ tel que $x' \in [0,1[$, $y'>0$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\omega']$.*

Preuve. Le conjugué $\overline{\omega}$ étant la deuxième racine de P_ω, c'est aussi un entier quadratique.

Pour tout entier relatif n, le nombre complexe $n+\omega$ est racine du polynôme $P_{n+\omega}(X) = X^2-(\alpha+2n)\,X-\left(\beta+n^2\right) \in \mathbb{Z}[X]$ qui est irréductible dans $\mathbb{Q}[X]$ puisque de racines $n+\omega$ et $n+\overline{\omega}$ non réelles, donc $n+\omega$ est aussi un entier quadratique.

1. Les deux racines du polynôme P_ω étant ω et $\overline{\omega}$, on a $\omega+\overline{\omega} = \alpha \in \mathbb{Z}$ et $|\omega|^2 = \omega\overline{\omega} = -\beta \in \mathbb{R}_+ \cap \mathbb{Z} = \mathbb{N}$. Il en résulte que $\overline{\omega} = \alpha-\omega \in \mathbb{Z}[\omega]$ et pour tout $z = a+b\omega \in \mathbb{Z}[\omega]$, on a $\overline{z} = a+b\overline{\omega} \in \mathbb{Z}[\omega]$, c'est-à-dire que $\mathbb{Z}[\omega]$ est stable par conjugaison complexe. Comme $\overline{\omega} \in \mathbb{Z}[\omega]$ et $\omega = \overline{\overline{\omega}} \in \mathbb{Z}[\overline{\omega}]$, on a $\mathbb{Z}[\overline{\omega}] \subset \mathbb{Z}[\omega]$ et $\mathbb{Z}[\omega] \subset \mathbb{Z}[\overline{\omega}]$, soit $\mathbb{Z}[\omega] = \mathbb{Z}[\overline{\omega}]$.

2. Pour tout $n \in \mathbb{Z}$, on a $n+\omega \in \mathbb{Z}[\omega]$ et $\omega = (n+\omega)-n \in \mathbb{Z}[n+\omega]$, donc $\mathbb{Z}[n+\omega] \subset \mathbb{Z}[\omega]$ et $\mathbb{Z}[\omega] \subset \mathbb{Z}[n+\omega]$, soit $\mathbb{Z}[\omega] = \mathbb{Z}[n+\omega]$.

3. En notant $n = [x]$ la partie entière de $x = \mathrm{Re}(\omega)$, on a $0 \leq x' = x-n < 1$ et $\mathbb{Z}[\omega] = \mathbb{Z}[x'+iy] = \mathbb{Z}[x'-iy]$, donc en notant $y = \mathrm{sgn}(y)\,y$, où $\mathrm{sgn}(y) = \dfrac{y}{|y|}$ est le signe de y (on a $y \neq 0$ puisque $\omega \in \mathbb{C}\setminus\mathbb{R}$), on a $\mathbb{Z}[\omega] = \mathbb{Z}[x'+iy']$ avec $x' \in [0,1[$ et $y'>0$. □

Théorème 5.13.

Si $\omega = x + iy$ est un entier quadratique non réel avec $x \in [0,1[$ et $y > 0$, on a alors $\omega = i\sqrt{n}$ ou $\omega = \dfrac{1+i\sqrt{4n-1}}{2}$ avec $n \in \mathbb{N}^*$. Pour ω dans $\left\{ i, i\sqrt{2}, \dfrac{1+i\sqrt{3}}{2}, \dfrac{1+i\sqrt{7}}{2}, \dfrac{1+i\sqrt{11}}{2} \right\}$ l'anneau $\mathbb{Z}[\omega]$ est euclidien pour le stathme $\varphi : z \in \mathbb{Z}[\omega] \mapsto |z|^2$.

Preuve. Les nombres complexes ω et $\overline{\omega}$ sont les deux racines du polynôme $P_\omega(X) = X^2 - \alpha X - \beta \in \mathbb{Z}[X]$ et on a :

$$x = \frac{\omega + \overline{\omega}}{2} = \frac{\alpha}{2} \in [0,1[\,,\ n = |\omega|^2 = -\beta \in \mathbb{N}$$

donc $\alpha = 0$ ou $\alpha = 1$ et $\beta = -n$ avec $n \in \mathbb{N}^*$, c'est à dire que $P_\omega(X) = X^2 + n$ ou $P_\omega(X) = X^2 - X + n = \left(X - \dfrac{1}{2}\right)^2 + \dfrac{4n-1}{4}$ avec $n \in \mathbb{N}^*$, donc $\omega = i\sqrt{n}$, ou $\omega = \dfrac{1+i\sqrt{4n-1}}{2}$ avec $n \in \mathbb{N}^*$ (on a $\mathrm{Im}(\omega) > 0$).

On vérifie que l'application $\varphi : z \mapsto |z|^2$ définit bien un stathme sur l'anneau $\mathbb{Z}[\omega]$. Pour tout $z = a + b\omega \in \mathbb{Z}[\omega]$, on a :

$$\varphi(z) = |z|^2 = z\overline{z} \in \mathbb{R}_+ \cap \mathbb{Z}[\omega] = \mathbb{N}$$

(on a $|z|^2 \geq 0$, $z\overline{z} \in \mathbb{Z}[\omega]$ puisque $\mathbb{Z}[\omega]$ est stable par conjugaison et $(1,\omega)$ est libre dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}$, puisque $\omega \in \mathbb{C} \setminus \mathbb{R}$, donc $u = a + b\omega \in \mathbb{R}_+ \cap \mathbb{Z}[\omega]$ impose $b = 0$ et $u = a \in \mathbb{N}$, soit $\mathbb{R}_+ \cap \mathbb{Z}[\omega] = \mathbb{N}$), donc φ est un stathme sur $\mathbb{Z}[\omega]$. Pour u, v dans $\mathbb{Z}[\omega]$ avec $v \neq 0$, on a $\dfrac{u}{v} = \dfrac{u\overline{v}}{|v|^2}$ avec $|v|^2 \in \mathbb{N}^*$ et $u\overline{v} \in \mathbb{Z}[\omega]$ puisque l'anneau $\mathbb{Z}[\omega]$ est stable par conjugaison complexe, donc $\dfrac{u}{v} = r + s\omega$ avec $(r,s) \in \mathbb{Q}^2$. Pour $q = a + b\omega \in \mathbb{Z}[\omega]$, on a :

$$\begin{aligned}\left|\frac{u}{v} - q\right|^2 &= |r - a + (s-b)\omega|^2 = |r - a + (s-b)x + i(s-b)y|^2 \\ &= |r - a + (s-b)x|^2 + |(s-b)y|^2\end{aligned}$$

Pour $b \in \mathbb{Z}$ tel que $s \in \left[b - \dfrac{1}{2}, b + \dfrac{1}{2}\right[$ et $a \in \mathbb{Z}$ tel que $r + (s-b)x \in \left[a - \dfrac{1}{2}, a + \dfrac{1}{2}\right[$, on a $\left|\dfrac{u}{v} - q\right|^2 \leq \dfrac{1+y^2}{4}$ ou encore $|u - qv|^2 < \dfrac{1+y^2}{4}|v|^2$. En posant $r = u - qv$ dans $\mathbb{Z}[\omega]$, on a $u = qv + r$ avec :

$$\varphi(r) = |r|^2 = |u - qv|^2 < \frac{1+y^2}{4}|v|^2 < |v|^2 = \varphi(v)$$

pour $y \in \left]0, \sqrt{3}\right[$. Donc $(\mathbb{Z}[\omega], \varphi)$ est euclidien pour $x \in [0,1[$ et $y \in \left]0, \sqrt{3}\right[$.

Avec le théorème 5.9, nous avons vu que l'anneau $\mathbb{Z}[i\sqrt{n}]$ est euclidien si, et seulement si, on a $n \in \{1,2\}$.

Pour $\omega = \dfrac{1+i\sqrt{4n-1}}{2}$ avec $n \in \mathbb{N}^*$ tel que $4n-1<12$, soit $1 \leq n < \dfrac{13}{4}$ ou encore $1 \leq n \leq 3$, on déduit de ce qui précède que $(\mathbb{Z}[\omega], \varphi)$ est euclidien.

En conclusion, pour $\omega \in \left\{ i, i\sqrt{2}, \dfrac{1+i\sqrt{3}}{2}, \dfrac{1+i\sqrt{7}}{2}, \dfrac{1+i\sqrt{11}}{2} \right\}$, l'anneau $\mathbb{Z}[\omega]$ est euclidien. □

On peut montrer que pour $n \geq 4$ l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{4n-1}}{2}\right]$ n'est pas euclidien (théorème 5.15). Pour certaines valeurs de n, il peut être principal non euclidien, c'est le cas pour $n=5$, soit pour $\omega = \dfrac{1+i\sqrt{19}}{2}$ (voir le paragraphe 5.4).

5.3.5 L'anneau des polynômes à coefficients dans un corps commutatif

Voir le théorème **??**.

5.3.6 L'anneau des séries formelles à coefficients dans un corps commutatif

Voir le paragraphe 4.1 pour la définition et quelques propriétés de l'anneau $\mathbb{K}[[X]]$ des séries formelles à une indéterminée et à coefficients dans un corps commutatif $\mathbb{K}$.

Théorème 5.14.

L'anneau $\mathbb{K}[[X]]$ des séries formelles à coefficients dans un corps commutatif $\mathbb{K}$ est euclidien pour le stathme :

$$\varphi : S \in \mathbb{K}[[X]] \setminus \{0_{\mathbb{K}}\} \mapsto \varphi(S) = \mathrm{val}(S)$$

Preuve. L'application φ est un stathme croissant. En effet, pour S, T dans $\mathbb{K}[[X]] \setminus \{0_{\mathbb{K}}\}$, on a $\mathrm{val}(S) \in \mathbb{N}$ et $\mathrm{val}(ST) = \mathrm{val}(S) + \mathrm{val}(T) \geq \mathrm{val}(S)$. Il reste à montrer qu'on a une division euclidienne. Soient S, T dans $\mathbb{K}[X] \setminus \{0_{\mathbb{K}}\}$ de valuations respectives n, m. On a alors $S = X^n S_1$ et $T = X^m T_1$ avec S_1, T_1 de valuation nulle, donc inversibles dans $\mathbb{K}[[X]]$ (lemme 4.3). Pour $m \leq n$, on écrit que $S = X^n S_1 = (X^m T_1)\left(X^{n-m} T_1^{-1} S_1\right) = TQ + 0_{\mathbb{K}}$ et pour $m > n$, on a $S = T \cdot 0_{\mathbb{K}} + S$ avec $\varphi(S) = \mathrm{val}(S) = n < m = \mathrm{val}(T) = \varphi(T)$. □

Avec le théorème précédent, on retrouve le fait que $\mathbb{K}[[X]]$ est principal (théorème 4.3).

5.4 Exemple d'anneau principal non euclidien

Nous avons vu qu'un anneau euclidien est principal (théorème 5.1). Dans le but de justifier que la réciproque est fausse, nous allons décrire un anneau qui est principal, mais non euclidien.

On désigne pour tout $n \in \mathbb{N}^*$ par ω_n l'entier quadratique $\dfrac{1+i\sqrt{4n-1}}{2}$ dont le polynôme minimal est $P_n(X) = X^2 - X + n$ (voir la démonstration du théorème 5.13).

Pour tout $u = a + b\omega_n \in \mathbb{Z}[\omega_n]$, on a :

$$\begin{aligned}|u|^2 &= (a+b\omega_n)(a+b\overline{\omega_n}) = a^2 + ab(\omega_n + \overline{\omega_n}) + b^2|\omega_n|^2 \\ &= a^2 + ab + nb^2 \in \mathbb{R}_+ \cap \mathbb{Z} = \mathbb{N}\end{aligned}$$

Pour $n \in \{1,2,3\}$, nous avons vu que l'anneau $\mathbb{Z}[\omega_n]$ est euclidien.

Lemme 5.10 *Le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}[\omega_n]$ est :*

$$(\mathbb{Z}[\omega_n])^\times = \{u \in \mathbb{Z}[\omega_n],\ |u| = 1\} = \begin{cases} \{-1,1\} & \text{pour } n \geq 2 \\ \{\pm 1, \pm\omega_1, \pm\overline{\omega_1}\} & \text{pour } n = 1 \end{cases}$$

Preuve. Si $u = a + b\omega_n \in \mathbb{Z}[\omega_n] \setminus \{0\}$ est inversible, il existe alors $v \in \mathbb{Z}[\omega_n]$ tel que $uv = 1$, donc $|u|^2|v|^2 = 1$ dans $\mathbb{N}^*$ et nécessairement $|u|^2 = 1$. Réciproquement, si $u \in \mathbb{Z}[\omega_n]$ est tel que $|u|^2 = u\overline{u} = 1$, il est alors inversible dans $\mathbb{Z}[\omega_n]$ d'inverse $\overline{u} \in \mathbb{Z}[\omega_n]$ (stabilité de $\mathbb{Z}[\omega_n]$ par conjugaison complexe). On a donc $(\mathbb{Z}[\omega_n])^\times = \{u \in \mathbb{Z}[\omega_n],\ |u| = 1\}$ où :

$$|u|^2 = a^2 + ab + nb^2 = \left(a + \frac{b}{2}\right)^2 + \left(n - \frac{1}{4}\right)b^2 = 1$$

Pour $n \geq 2$ et $u = a + b\omega_n \in (\mathbb{Z}[\omega_n])^\times$, on a $1 = |u|^2 \geq \left(n - \dfrac{1}{4}\right)b^2 \geq \dfrac{7}{4}b^2$ avec $b^2 \in \mathbb{N}$, ce qui impose $b = 0$ et $a^2 = 1$, soit $u = \pm 1$. On a donc $(\mathbb{Z}[\omega_n])^\times = \{-1,1\}$.

Pour $n = 1$ et $u = a + b\omega_n \in (\mathbb{Z}[\omega_1])^\times$, l'inégalité $1 \geq \dfrac{3}{4}b^2$ impose $b = 0$ et $a = \pm 1$ ou $b = \pm 1$ et $a(a \pm 1) = 0$, soit $u = \pm 1$ ou $u \in \{\pm\omega_1, \pm(1-\omega_1)\}$. On a donc $(\mathbb{Z}[\omega_n])^\times = \{\pm 1, \pm\omega_1, \pm(1-\omega_1)\} = \{\pm 1, \pm\omega_1, \pm\overline{\omega_1}\}$. □

Lemme 5.11 *Pour tout entier $n \geq 4$, les entiers ± 2 et ± 3 sont irréductibles dans $\mathbb{Z}[\omega_n]$.*

Preuve. Il nous suffit de vérifier que 2 et 3 sont irréductibles dans $\mathbb{Z}[\omega_n]$ puisque -1 est inversible dans $\mathbb{Z}[\omega_n]$.

Comme $(\mathbb{Z}[\omega_n])^\times = \{-1,1\}$, 2 et 3 sont non inversibles dans $\mathbb{Z}[\omega_n]$.

Si $2 = uv$ dans $\mathbb{Z}[\omega_n]$, on alors $4 = |u|^2|v|^2$ dans $\mathbb{N}^*$, ce qui implique que $|u|^2 \in \{1,2,4\}$. Le cas $|u|^2 = 1$ signifie que u est inversible ; le cas $|u|^2 = 4$ impose $|v|^2 = 1$ et signifie que v est inversible ; le cas $|u|^2 = a^2 + ab + nb^2 = 2$ impose $b \neq 0$ puisque $a^2 = 2$ est impossible dans $\mathbb{Z}$, mais alors :

$$2 = |u|^2 = \left(a + \frac{b}{2}\right)^2 + \left(n - \frac{1}{4}\right)b^2 \geq \frac{15}{4}$$

ce qui n'est pas possible.

Si $3 = uv$ dans $\mathbb{Z}[\omega_n]$, on alors $9 = |u|^2 |v|^2$ dans $\mathbb{N}^*$ et $|u|^2 \in \{1, 3, 9\}$. Les cas $|u|^2 = 1$ ou $|u|^2 = 9$ impliquent l'inversibilité de u ou celle de v ; le cas $|u|^2 = a^2 + ab + nb^2 = 3$ impose $b \neq 0$ puisque $a^2 = 3$ est impossible dans $\mathbb{Z}$, mais alors $3 = \left(a + \frac{b}{2}\right)^2 + \left(n - \frac{1}{4}\right) b^2 \geq \frac{15}{4}$, ce qui n'est pas possible. □

Théorème 5.15.

Pour tout entier $n \geq 4$, l'anneau $\mathbb{Z}[\omega_n]$ n'est pas euclidien.

Preuve. Supposons qu'il existe un stathme $\varphi : \mathbb{Z}[\omega_n]^* \to \mathbb{N}$ qui fasse de $\mathbb{Z}[\omega_n]$ un anneau euclidien. On désigne par u un élément de $\mathbb{Z}[\omega_n]$ tel que :

$$\varphi(u) = \min\{\varphi(v),\ v \in \mathbb{Z}[\omega_n] \setminus \{-1, 0, 1\}\}$$

Ce minimum est atteint puisque $\{\varphi(v),\ v \in \mathbb{Z}[\omega_n] \setminus \{-1, 0, 1\}\}$ est une partie non vide minorée de $\mathbb{N}$. Les inversibles de $\mathbb{Z}[\omega_n]$ étant les éléments de module égal à 1, soit -1 et 1, on a $|u|^2 \geq 2$ et :

$$\varphi(u) = \min\left\{\varphi(v),\ v \in \mathbb{Z}[\omega_n] \text{ et } |v|^2 \geq 2\right\}$$

Dans $\mathbb{Z}[\omega_n]$, on a une division euclidienne $2 = qu + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(u)$ qui impose $r \in \{-1, 1\}$ par minimalité de u.

— Si $r = 1$, on a alors $1 = qu$ avec u non inversible, soit une impossibilité.

— Si $r = 0$, on a alors $2 = qu$ avec u non inversible, donc q est inversible puisque 2 est irréductible dans $\mathbb{Z}[\omega_n]$, soit $q = \pm 1$ et $u = \pm 2$. La division euclidienne de ω_n par u donne alors $\omega_n = q(\pm 2) + r' = 2q' + r'$ avec $r' \in \{-1, 0, 1\}$, donc $\omega_n - r' = 2(a + b\omega_n)$, ce qui implique que $2a = -r'$ et $2b = 1$ puisque $(1, \omega_n)$ est $\mathbb{R}$-libre, soit une impossibilité pour b entier.

— Si $r = -1$, on a alors $3 = qu$ avec u non inversible, donc q est inversible puisque 3 est irréductible dans $\mathbb{Z}[\omega_n]$, soit $q = \pm 1$ et $u = \pm 3$. La division euclidienne de ω_n par u donne alors $\omega_n = 3q' + r'$avec $r' \in \{-1, 0, 1\}$, donc $\omega_n - r' = 3(a + b\omega_n)$, ce qui implique que $3a = -r'$ et $3b = 1$ puisque $(1, \omega_n)$ est $\mathbb{R}$-libre, soit une impossibilité pour b entier.

□

Pour ce qui suit, on se limite à $n = 5$, soit à l'anneau $\mathbb{Z}[\omega_5] = \mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ qui se trouve être principal et non euclidien.

Lemme 5.12 *Pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[\omega_5]$ ou $v \in \mathbb{Z}[\omega_5]$ tel que l'on ait $|z - u| < 1$ ou $|2z - v| < 1$.*

Preuve. Comme $(1, \omega_5)$ est une $\mathbb{R}$-base de $\mathbb{C}$, tout nombre complexe s'écrit de manière unique $z = x + y\omega_5$ avec $(x, y) \in \mathbb{R}^2$ et il existe un unique couple (a, b) d'entiers relatifs tel que :

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2}\right[\times \left[b - \frac{1}{2}, b + \frac{1}{2}\right[$$

donc, en notant $u = a + b\omega_5$ dans $\mathbb{Z}[\omega_5]$, on a :

$$\begin{aligned}|z-u|^2 &= (x-a)^2 + (x-a)(y-b) + 5(y-b)^2 \\ &\leq (x-a)^2 + |x-a|\,|y-b| + 5(y-b)^2 \leq \frac{1}{4} + \frac{1}{2}|y-b| + 5(y-b)^2\end{aligned}$$

Si $|y-b| \leq \dfrac{1}{3}$, il vient $|z-u|^2 \leq \dfrac{1}{4} + \dfrac{1}{6} + \dfrac{5}{9} = \dfrac{35}{36} < 1$. Si $\dfrac{1}{3} < |y-b| \leq \dfrac{1}{2}$, on a alors $\dfrac{1}{3} < y-b \leq \dfrac{1}{2}$ ou $-\dfrac{1}{2} < y-b \leq -\dfrac{1}{3}$, soit $2b + \dfrac{2}{3} < 2y \leq 2b+1$ ou $2b-1 < 2y \leq 2b - \dfrac{2}{3}$. Dans le premier cas, on pose $d = 2b+1$ et dans le second $d = 2b-1$, ce qui nous donne $|2y-d| \leq \dfrac{1}{3}$ et en désignant par c l'entier tel que $2x \in \left[c - \dfrac{1}{2}, c + \dfrac{1}{2}\right[$, en prenant $v = c + d\omega \in \mathbb{Z}[\omega_5]$, on a $|2z - v| < 1$. □

Théorème 5.16.

L'anneau $\mathbb{Z}[\omega_5]$ est principal.

Preuve. Soient I un idéal de $\mathbb{Z}[\omega_5]$ non réduit à $\{0\}$ et $u_0 = a + b\omega$ dans $\mathbb{Z}[\omega_5]$ tel que $|u_0|^2 = \min\left\{|u|^2,\ u \in I \setminus \{0\}\right\}$. Ce minimum existe car l'ensemble $\left\{|u|^2,\ u \in I \setminus \{0\}\right\}$ est une partie non vide de $\mathbb{N}^*$. Comme I est un idéal, on a déjà $(u_0) = \mathbb{Z}[\omega_5]\,u_0 \subset I$. Soient $v \in I$ et $z = \dfrac{v}{u_0}$. Supposons que $v \notin (u_0)$. Si $u \in \mathbb{Z}[\omega_5]$ est tel que $|z-u| < 1$, on a alors $0 < |v - u_0 u| < |u_0|$ et $v \notin I$ (sinon $v - u_0 u \in I$ puisque I est un idéal et $v - u_0 u = 0$ par définition de u_0), ce qui n'est pas. Si $u \in \mathbb{Z}[\omega_5]$ est tel que $|2z-u| < 1$, on a alors $0 < |2v - u_0 u| < |u_0|$ et $2v \notin I$, ce qui implique encore que $v \notin I$ ($v \in I$ entraîne $2v = v + v \in I$ puisque I est un groupe additif), ce qui n'est pas. L'hypothèse $v \notin (u_0)$ est donc impossible et $I \subset \mathbb{Z}[\omega_5]\,u_0$. On a donc $I = \mathbb{Z}[\omega_5]\,u_0$ et I est principal. □

5.5 Unicité de la division euclidienne

Pour ce paragraphe, $(\mathbb{A}, \varphi)$ est un anneau euclidien qui n'est pas un corps. Dans les exemples d'anneaux euclidiens que nous avons considérés, seuls les anneaux de polynômes à coefficients dans un corps commutatif, avec le degré pour stathme, assurent l'unicité du reste et du quotient dans la division euclidienne. En fait, ce sont les seuls cas possibles. Nous allons montrer plus précisément que si $(\mathbb{A}, \varphi)$ est un anneau euclidien qui n'est pas un corps et pour lequel il y a unicité du quotient et du reste dans la division euclidienne, cet anneau est alors isomorphe à un anneau de polynômes à coefficients dans un corps commutatif.

Le lemme qui suit nous dit que cette unicité est réalisée si, et seulement si, le stathme φ est croissant et vérifie une propriété supplémentaire vérifiée par le degré des polynômes.

Lemme 5.13 *Le quotient et le reste sont uniquement déterminés pour la division euclidienne dans* $(\mathbb{A}, \varphi)$ *si, et seulement si, le stathme* φ *est croissant tel que :*

$$\forall (a,b) \in \mathbb{A}^* \times \mathbb{A}^*,\ a \neq b \Rightarrow \varphi(a-b) \leq \max(\varphi(a), \varphi(b)) \tag{5.1}$$

Preuve. Supposons que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$ et soient a, b dans $\mathbb{A}^*$. Si $\varphi(ab) < \varphi(a)$, on a alors deux divisions euclidiennes de ab par a, $ab = ab + 0 = a0 + ab$ ($ab \neq 0$ puisque a, b sont non nuls dans $\mathbb{A}$ intègre), ce qui est contraire à notre hypothèse. On a donc $\varphi(ab) \geq \varphi(a)$, ce qui signifie que le stathme φ est croissant.

Supposant que $a \neq b$ et écrivant que $2a - b = 1 \cdot (a-b) + a = 2(a-b) + b$, les inégalités $\varphi(a) < \varphi(a-b)$ et $\varphi(b) < \varphi(a-b)$ nous donneraient deux divisions euclidiennes de $2a - b$ par $a - b$, ce qui n'est pas, donc l'une des deux inégalités $\varphi(a-b) \leq \varphi(a)$ ou $\varphi(a-b) \leq \varphi(b)$ est vérifiée, ce qui nous donne bien $\varphi(a-b) \leq \max(\varphi(a), \varphi(b))$.

Réciproquement supposons le stathme φ croissant, la condition (5.1) vérifiée et que l'on ait deux divisions euclidiennes, $a = bq + r = bq' + r'$. Si $q \neq q'$, on a alors $r - r' = b(q' - q) \neq 0$ ($\mathbb{A}$ est intègre). Si $r' = 0$, on a alors $r \neq 0$ et $\varphi(r) = \varphi(b(q'-q)) \geq \varphi(b)$, ce qui contredit $\varphi(r) < \varphi(b)$. On a donc $r' \neq 0$ et en permutant les rôles de r et r', on voit qu'on a également $r \neq 0$. Mais on aboutit alors à $\varphi(b) \leq \varphi(b(q'-q)) = \varphi(r - r') \leq \max(\varphi(r), \varphi(r')) < \varphi(b)$, ce qui n'est pas possible. On a donc $q = q'$ et $r = r'$. □

La propriété de croissance du stathme est vérifiée pour les exemples classiques d'anneaux euclidiens : $\mathbb{K}[X]$, $\mathbb{Z}$, $\mathbb{D}$ et $\mathbb{Z}[i]$. En fait, on a vu qu'on peut toujours se ramener à un stathme croissant (lemme 5.1), ce qui est intéressant pour caractériser les éléments inversibles de $\mathbb{A}$ (théorème 5.2).

On suppose pour la suite de cet paragraphe que le quotient et le reste sont uniquement déterminés pour la division euclidienne dans $(\mathbb{A}, \varphi)$, c'est-à-dire que :

$$\forall (a,b) \in \mathbb{A} \times \mathbb{A}^*,\ \exists!\,(q,r) \in \mathbb{A}^2,\ a = bq + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(b)$$

ce qui équivaut à dire que φ est croissant et que la propriété (5.1) est vérifiée.

Lemme 5.14 *L'ensemble* $\mathbb{K} = \mathbb{A}^\times \cup \{0\}$ *est un corps. Donc* $\mathbb{A}$ *est un* $\mathbb{K}$*-espace vectoriel.*

Preuve. On a $1 \in \mathbb{K}$ et pour a, b dans $\mathbb{K}$, ab est dans $\mathbb{K}$ puisque $\mathbb{A}^\times$ est un groupe multiplicatif. Il reste à montrer que pour a, b dans $\mathbb{K}$, $a - b$ est aussi dans $\mathbb{K}$. Si $a = b$, on a alors $a - b = 0 \in \mathbb{K}$; si $a = 0$ [resp. $b = 0$], on a alors $a - b = -b \in \mathbb{K}$ [resp. $a - b = a \in \mathbb{K}$]. Enfin si a, b sont dans $\mathbb{A}^*$ avec $a \neq b$, on a alors $\varphi(1) = \min\limits_{x \in \mathbb{A}^*} \varphi(x) \leq \varphi(a-b) \leq \max(\varphi(a), \varphi(b)) = \varphi(1)$ (troisième point du théorème 5.2), donc $\varphi(a-b) = \varphi(1)$ et $a - b \in \mathbb{K}$. Au final, $\mathbb{K}$ est un sous-anneau de $\mathbb{A}$ tel que tous les éléments de $\mathbb{K}^* = \mathbb{A}^\times$ sont inversible, c'est donc un corps. □

Lemme 5.15 *Pour* $a \neq b$ *dans* $\mathbb{A}^*$ *tels que* $\varphi(a) < \varphi(b)$, *on a* $\varphi(b-a) = \varphi(b)$.

Preuve. On a déjà $\varphi(b-a) \leq \max(\varphi(a), \varphi(b)) = \varphi(b)$.

Si $\varphi(b-a) < \varphi(b)$, on a alors $2b-a = 1\cdot b + (b-a) = 2b+(-a)$ avec $\varphi(b-a) < \varphi(b)$ et $\varphi(-a) = \varphi(a) < \varphi(b)$, donc $b-a = -a$ par unicité du reste et $b = 0$, ce qui n'est pas. On a donc $\varphi(b-a) = \varphi(b)$. □

Ayant supposé que A n'est pas un corps, on a $\mathbb{K} \subsetneq \mathbb{A}$ et il existe $x \in \mathbb{A}\setminus\mathbb{K}$ tel que $\varphi(x) = \min\limits_{y\in\mathbb{A}\setminus\mathbb{K}} \varphi(y)$.

Lemme 5.16 *On a $\varphi(x) > \varphi(1)$, la suite $(\varphi(x^n))_{n\in\mathbb{N}}$ est strictement croissante dans $\mathbb{N}$ et la famille $\mathcal{B}_x = (x^n)_{n\in\mathbb{N}}$ est libre dans le $\mathbb{K}$-espace vectoriel $\mathbb{A}$.*

Preuve. On a déjà $\varphi(1) = \min\limits_{y\in\mathbb{A}^*} \varphi(y) \leq \varphi(x)$ et $\varphi(x) \neq \varphi(1)$ puisque $x \notin \mathbb{A}^\times$. Comme $x \neq 0$ et $x \notin \mathbb{A}^\times$, on a $\varphi\left(x^{n+1}\right) = \varphi(x^n x) > \varphi(x^n)$. On en déduit que $\varphi(x^n) \geq n$ pour tout $n \in \mathbb{N}$ et $\lim\limits_{n\to+\infty} \varphi(x^n) = +\infty$. Dire que la famille $\mathcal{B}_x$ est libre, revient à dire que, pour tout entier $n \in \mathbb{N}$, la famille $\left(x^k\right)_{0\leq k\leq n}$ est libre. Soient $a_0, \cdots, a_n$ dans $\mathbb{K} = \mathbb{A}^\times \cup \{0\}$ tels que $\sum\limits_{k=0}^{n} a_k x^k = 0$. Si $a_0 \neq 0$, on a alors $a_0 \in \mathbb{A}^\times$ et $x\sum\limits_{k=1}^{n} \left(-a_0^{-1}a_k\right) x^k = 1$, donc $x \in \mathbb{A}^\times$, ce qui n'est pas. On a donc $a_0 = 0$. Supposant que $a_j = 0$ pour $0 \leq j \leq k \leq n-1$, on a $x^{k+1} \sum\limits_{j=k+1}^{n} a_j x^{j-k-1} = 0$, donc $\sum\limits_{j=k+1}^{n} a_j x^{j-k-1} = 0$ puisque $\mathbb{A}$ est intègre et $a_{k+1} = 0$. Les a_k sont donc tous nuls et $\left(x^k\right)_{0\leq k\leq n}$ est libre. □

Lemme 5.17 *Pour tout $a \in \mathbb{A}^*$, il existe un unique $n \in \mathbb{N}$ tel que $\varphi(a) = \varphi(x^n)$.*

Preuve. La suite $(\varphi(x^n))_{n\in\mathbb{N}}$ étant strictement croissante dans $\mathbb{N}$, il existe pour tout $a \in \mathbb{A}^*$ un unique $n \in \mathbb{N}$ tel que $\varphi(x^n) \leq \varphi(a) < \varphi\left(x^{n+1}\right)$ (comme $\varphi(a) \geq \varphi(1) = \varphi\left(x^0\right)$, l'ensemble $\left\{k \in \mathbb{N},\ \varphi\left(x^k\right) \leq \varphi(a)\right\}$ est non vide dans $\mathbb{N}$, il admet donc un plus petit élément qui vérifie $\varphi(x^n) \leq \varphi(a) < \varphi\left(x^{n+1}\right)$). Si $n = 0$, on a alors $\varphi(a) < \varphi(x)$, donc $a \in \mathbb{A}^\times$ (sinon $a \notin \mathbb{K}$ puisque $a \neq 0$ et $\varphi(x) \leq \varphi(a)$) et $\varphi(a) = \varphi(1)$. Si $n \geq 1$, on a la division euclidienne de a par x^n :

$$a = qx^n + r \text{ avec } r = 0 \text{ ou } r \neq 0 \text{ et } \varphi(r) < \varphi(x^n)$$

Si $q = 0$, on a alors $\varphi(a) = \varphi(r) < \varphi(x^n)$, ce qui n'est pas, donc $q \neq 0$. Pour $r = 0$, on a $\varphi(a) = \varphi(qx^n)$. Pour $r \neq 0$, on a $\varphi(-r) = \varphi(r) < \varphi(x^n) \leq \varphi(qx^n)$ et $\varphi(a) = \varphi(qx^n - (-r)) = \varphi(qx^n)$. Dans tous les cas, on a $\varphi(a) = \varphi(qx^n)$. On a la division euclidienne $q = \alpha x + \beta$ avec $\beta = 0$ ou $\beta \neq 0$ et $\varphi(\beta) < \varphi(x)$, donc $\beta \in \mathbb{K}$ dans les deux cas. Si $\alpha \neq 0$, on a alors $qx^n = \alpha x^{n+1} + \beta x^n$. Si $\beta = 0$, on a alors $\varphi(a) = \varphi(qx^n) = \varphi\left(\alpha x^{n+1}\right) \geq \varphi\left(x^{n+1}\right)$, ce qui n'est pas. On a donc $\beta \neq 0$, soit $\beta \in \mathbb{A}^\times$ et $\varphi(\beta x^n) = \varphi(x^n) < \varphi\left(x^{n+1}\right) \leq \varphi\left(\alpha x^{n+1}\right)$, donc $\varphi(a) = \varphi(qx^n) = \varphi\left(\alpha x^{n+1}\right) \geq \varphi\left(x^{n+1}\right)$, ce qui n'est pas. On a donc $\alpha = 0$ et $q = \beta \in \mathbb{A}^\times$ (q est non nul), ce qui nous donne $\varphi(a) = \varphi(x^n)$. La suite $(\varphi(x^n))_{n\in\mathbb{N}}$ étant strictement croissante, cet entier n est uniquement déterminé par a. □

Théorème 5.17.

La famille $\mathcal{B}_x = (x^n)_{n\in\mathbb{N}}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{A}$, c'est-à-dire que pour tout $a \in \mathbb{A}$, il existe un unique entier naturel n et une unique suite $(a_k)_{0\leq k\leq n}$ d'éléments de $\mathbb{K}$ telle que $a = \sum_{k=0}^{n} a_k x^k$, les a_k étant dans $\mathbb{K}$ avec $a_n \in \mathbb{A}^\times$. Ce que l'on peut noter $\mathbb{A} = \mathbb{K}[X]$. Il en résulte que l'anneau $\mathbb{A}$ est isomorphe à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans le corps commutatif $\mathbb{K}$.

Preuve. Comme $\mathcal{B}_x = (x^n)_{n\in\mathbb{N}}$ est libre dans le $\mathbb{K}$-espace vectoriel $\mathbb{A}$, il nous suffit de montrer que cette famille $\mathcal{B}_x$ est génératrice. Pour ce faire, on montre par récurrence sur $n \geq 0$ que tout $a \in \mathbb{A}^*$ tel que $\varphi(a) = \varphi(x^n)$ s'écrit $a = \sum_{k=0}^{n} a_k x^k$, les a_k étant dans $\mathbb{K}$ avec $a_n \in \mathbb{A}^\times$. Pour $n = 0$, $\varphi(a) = \varphi(1)$ signifie que $a = a_0 \in \mathbb{A}^\times$. Supposons le résultat acquis jusqu'au rang $n-1 \geq 0$ et soit $a \in \mathbb{A}^*$ tel que $\varphi(a) = \varphi(x^n)$. On a vu avec le lemme précédent que $a = qx^n + r$ avec $q \in \mathbb{A}^\times$ et $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(x^n)$, donc $\varphi(r) \leq \varphi\left(x^{n-1}\right)$. Pour $r = 0$, on a $a = a_n x^n$ avec $a_n = q \in \mathbb{A}^\times$ et pour $r \neq 0$, on a par hypothèse de récurrence, $r = \sum_{k=0}^{p} a_k x^k$ avec $0 \leq p \leq n-1$, $a_k \in \mathbb{K}$ pour tout k compris entre 0 et p et $a_p \in \mathbb{A}^\times$. Notant $a_n = q$, $a_{n-1} = \cdots = a_{p+1} = 0$ (éventuellement), on a bien $a = \sum_{k=0}^{n} a_k x^k$, les a_k étant dans $\mathbb{K}$ avec $a_n \in \mathbb{A}^\times$.

Il est clair que $\phi : P \in \mathbb{K}[X] \mapsto P(x) \in \mathbb{A}$ est un morphisme d'anneaux et on vient de voir qu'il est bijectif, c'est donc un isomorphisme de $\mathbb{K}[X]$ sur $\mathbb{A}$. □

5.6 Exercices

Exercice 5.1. *Soit $(\mathbb{A}, \varphi)$ un anneau euclidien. Montrer que si le stathme φ est constant, $\mathbb{A}$ est alors un corps.*

Solution. Si le stathme φ est constant, l'inégalité stricte $\varphi(r) < \varphi(b)$ n'est jamais vérifiée, donc la division euclidienne de $a \in \mathbb{A}$ par $b \in \mathbb{A}^*$ est de la forme $a = bq$. En particulier, on aura $1 = bq$ pour tout $b \in \mathbb{A}^*$, ce qui revient à dire que $\mathbb{A}$ est un corps.

Exercice 5.2. *Soient $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ ne divisant pas a.*

1. *Montrer que si $a = bq + r$ est une division euclidienne de a par b dans $(\mathbb{Z}, |\cdot|)$, il en existe alors une seule autre $a = bq' + r'$ avec $r \neq r'$ et $q \neq q'$.*

2. Montrer qu'il y a exactement deux divisions euclidiennes de a par b dans $(\mathbb{Z}, |\cdot|)$.

Solution. Si b divise a, le seul reste possible dans la division de a par b est 0 (dans ce cas b divise $r = a - bq$ avec $0 \leq |r| < |b|$, donc $r = 0$). Réciproquement un reste nul nous dit que b divise a. Pour $a \neq 0$ et $b \geq 1$ ne divisant pas a, les restes dans la division euclidienne de a par b sont donc nécessairement non nuls.

1. Supposons qu'il existe deux division euclidienne de a par b dans $(\mathbb{Z}, |\cdot|)$, soit $a = bq + r = bq' + r'$ avec $0 < |r|, |r'| < |b| = b$. Comme b ne divise pas a, les entiers r et r' sont dans $]-b, b[\setminus \{0\}$. Si $r \neq r'$, on a alors $q' \neq q$ et $b \leq b|q - q'| = |r' - r| < 2b$, donc $1 \leq |q - q'| < 2$ et $q = q' + 1$ ou $q = q' - 1$, soit $r' = r + b$ ou $r' = r - b$. Pour $r > 0$, on a $r + b > b$ et $r' = r - b \in]-b, b[$, pour $r < 0$, on a $r - b < -b$ et $r' = r + b \in]-b, b[$. On a donc $r' = r - \operatorname{sgn}(r) b$ et $q' = q + \operatorname{sgn}(r)$, où $\operatorname{sgn}(r)$ est le signe de r. Réciproquement on vérifie que si $a = bq + r$ est une division euclidienne dans $(\mathbb{Z}, |\cdot|)$, on en a une deuxième $a = bq' + r'$ en posant $r' = r - \operatorname{sgn}(r) b$ et $q' = q + \operatorname{sgn}(r)$. En effet, on a :

$$bq' + r' = b(q + \operatorname{sgn}(r)) + (r - \operatorname{sgn}(r) b) = bq + r = a$$

et $r' = r - \operatorname{sgn}(r) b \in]-b, b[$ (pour $r > 0$, on a $0 < r < b$, donc $-b < r - b < 0$ et pour $r < 0$, on a $-b < r < 0$, donc $0 < r + b < b$), avec $r' \neq r$.

2. On a déjà la division euclidienne classique $a = bq + r$ avec $0 < r < b$ et on vient de voir qu'en posant $r' = r - \operatorname{sgn}(r) b = r - b$, $q' = q + \operatorname{sgn}(r) = q + 1$, on en a une deuxième et c'est la seule possible.

Exercice 5.3. *Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est isomorphe à l'anneau quotient $\dfrac{\mathbb{Z}[X]}{(10X - 1)}$.*

Solution. Par définition des nombres décimaux, l'application $\varphi : P \mapsto P\left(\dfrac{1}{10}\right)$ réalise une surjection de $\mathbb{Z}[X]$ sur $\mathbb{D}$ et il est clair que cette application est un morphisme d'anneaux. Elle passe donc au quotient en un isomorphisme de l'anneau quotient $\dfrac{\mathbb{Z}[X]}{\ker(\varphi)}$ sur $\mathbb{D}$. Un polynôme $P \in \mathbb{Z}[X]$ est dans $\ker(\varphi)$ si, et seulement si, il est tel que $P\left(\dfrac{1}{10}\right) = 0$, ce qui implique l'existence de Q et R dans $\mathbb{Q}[X]$ tel que $P(X) = \left(X - \dfrac{1}{10}\right) Q(X) = (10X - 1) R(X)$. Si $P \in \ker(\varphi) \setminus \{0\}$, il est alors non constant et on a :

$$P(X) = \sum_{k=0}^{n} a_k X^k = (10X - 1) R(X) = (10X - 1) \sum_{k=0}^{n-1} b_k X^k$$

où $n \in \mathbb{N}^*$, les a_k sont dans $\mathbb{Z}$ et les b_k dans $\mathbb{Q}$. Il en résulte que $b_0 = -a_0 \in \mathbb{Z}$ et $b_k = a_k - 10 b_{k-1}$ pour $1 \leq k \leq n$, ce qui implique par récurrence que les b_k sont

dans $\mathbb{Z}$, soit que $R \in \mathbb{Z}[X]$ et $P \in (10X-1)$. L'inclusion $(10X-1) \subset \ker(\varphi)$ étant évidente, on a bien l'égalité $\ker(\varphi) = (10X-1)$ et l'isomorphisme entre $\mathbb{D}$ et l'anneau quotient $\dfrac{\mathbb{Z}[X]}{(10X-1)}$.

Exercice 5.4.

1. *Soit $p \geq 2$ un nombre premier. Montrer que tout $z \in \mathbb{Z}[i]$ tel que $|z|^2 = p$ est irréductible dans $\mathbb{Z}[i]$.*
2. *Les deux décompositions $5 = (1+2i)(1-2i) = (2+i)(2-i)$ contredisent-elles le fait que $\mathbb{Z}[i]$ est factoriel ?*
3. *Effectuer la division euclidienne de $u = 11+7i$ par $v = 18-i$ dans $\mathbb{Z}[i]$.*
4. *Calculer le* pgcd *de $u = a+ib$ et $v = b-ia$ dans $\mathbb{Z}[i]$.*

Solution.

1. Si $z = a+ib = uv$ dans $\mathbb{Z}[i]$, on a alors $|u|^2|v|^2 = a^2+b^2 = p$ dans $\mathbb{N}$, donc $|u|^2 = 1$ ou $|v|^2 = 1$, ce qui signifie que u ou v est inversible dans $\mathbb{Z}[i]$. Donc z est premier dans $\mathbb{Z}[i]$, ce qui revient à dire qu'il est irréductible (lemme 4.4).
2. Les éléments $1 \pm 2i$ et $2 \pm i$ sont irréductibles dans $\mathbb{Z}[i]$ d'après la question précédentes tels que $1+2i = i(2-i)$ et $1-2i = -i(2+i)$, donc on a bien une unique décomposition de 5 en facteurs irréductibles dans $\mathbb{Z}[i]$ à l'ordre et multiplication par une unité près et cela ne contredit pas la facorialité de $\mathbb{Z}[i]$.
3. On a $\dfrac{u}{v} = \dfrac{(11+7i)(18+i)}{325} = \dfrac{191}{325} + \dfrac{137}{325}i = x+iy$ avec :
$$(x,y) = \left(\frac{191}{325}, \frac{137}{325}\right) = (0.58\cdots, 0.42\cdots) \in \left[\frac{1}{2}, \frac{3}{2}\right[\times \left[-\frac{1}{2}, \frac{1}{2}\right[$$
En prenant $q = 1$ et $r = u - qv = -7+8i$, on a $11+7i = (18-i)+(-7+8i)$ avec $|-7+8i|^2 = 113 < |18-i|^2 = 325$.
4. On a $a+ib = i(b-ia)$, donc $u \wedge v = v$.