Préparation à l'agrégation de mathématiques
Notes du cours d'algèbre

Arnaud Durand

Philippe Lebacque

Table des matières

Chapitre 1. Rappels sur les groupes 5
1. Opération d'un groupe sur un ensemble 5
2. Produit direct de deux groupes 7
3. Produit semi-direct de deux groupes 8
4. Les théorèmes de Sylow 12

Chapitre 2. Corps finis 13
1. Rappels 13
2. Constructions de corps finis 15
3. Structure des corps finis 18
4. Prolongements 20

Chapitre 3. Réduction d'un endomorphisme 25
1. Polynôme minimal et polynôme caractéristique d'un endomorphisme 25
2. Sous-espaces stables 26
3. Sous-espaces cycliques et théorème de Cayley-Hamilton 27
4. Lemme de décomposition des noyaux 30
5. Invariants de similitude 31
6. Endomorphismes semi-simples 38
7. Réduction des endomorphismes normaux 41

Chapitre 4. Modules sur un anneau principal 49
1. Généralités sur les modules 49
2. Classes d'isomorphisme des modules de type fini sur un anneau principal 50
3. Applications 54

Bibliographie 69

Bibliographie 69

Index 69

CHAPITRE 1

Rappels sur les groupes

1. Opération d'un groupe sur un ensemble

Cette section contient des rappels sur les actions de groupes. Nous donnerons leur définition et quelques-unes de leurs propriétés. Nous finirons par une application aux p-groupes.

1.1. Définition.

DÉFINITION 1. Une *opération d'un groupe G sur un ensemble E* est la donnée d'une application

$$\begin{array}{rcl} G \times E & \to & E \\ (g, e) & \mapsto & g \cdot e \end{array}$$

telle que pour tous $e \in E$, $g, g' \in G$, on ait

(i). $(gg') \cdot e = g \cdot (g' \cdot e)$

(ii). $1 \cdot e = e$

De manière équivalente, il s'agit aussi de la donnée d'un morphisme de groupes

$$\begin{array}{rcl} \Psi : G & \to & \mathfrak{S}(E) \\ g & \mapsto & (e \mapsto g \cdot e) \end{array}$$

REMARQUE 1. On a $g \cdot e = \Psi(g)(e)$.

On dira que l'action de G sur E est transitive si pour tous $e, e' \in E$ il existe $g \in G$ telle que $g \cdot e = e'$. On dira que G opère fidèlement sur E si Ψ est injective.

1.2. Exemple. G agit sur lui-même par translation à gauche : pour $g, a \in G$ on pose $g \cdot a = ga$. G opère alors simplement transitivement, et donc fidèlement. On en déduit le théorème de Cayley :

THÉORÈME 1. *Si G est fini de cardinal n, G est isomorphe à un sous groupe de $\mathfrak{S}_n$.*

1.3. Orbites et stabilisateurs.

PROPOSITION 1. *Une opération du groupe G sur E définit une relation d'équivalence sur E :*

$$e \sim e' \iff \exists g \in G : e = g \cdot e'$$

Nous verrons bientôt que cette relation d'équivalence est primordiale dans l'étude des actions de groupes. Donnons quelques propriétés qui lui sont relatives.

DÉFINITION 2. Une classe d'équivalence par la relation $\sim$ est appelée *orbite*.

PROPOSITION 2. *L'orbite de e est*

$$\omega(e) = \{g \cdot e, g \in G\}$$

L'application

$$\begin{array}{rcl} G & \to & \omega(e) \\ g & \mapsto & g \cdot e \end{array}$$

est donc surjective et on a $g \cdot e = g' \cdot e$ si et seulement si $(g'^{-1}g) \cdot e = e$.

DÉFINITION 3. On appelle *stabilisateur* de e et on note $\mathrm{Stab}_G(e)$ le sous-groupe de G défini par

$$\mathrm{Stab}_G(e) = \{g : g \cdot e = e\}$$

Avec cette définition, on peut donc écrire que $g \cdot e = g' \cdot e$ si et seulement si $g\,\mathrm{Stab}_G(e) = g'\,\mathrm{Stab}_G(e)$. On en déduit la proposition suivante et son corollaire immédiat.

PROPOSITION 3. *$G/\mathrm{Stab}_G(e)$ est en bijection d'ensembles avec $\omega(e)$.*

Dans la suite, nous noterons $|E|$ le cardinal d'un ensemble E.

COROLLAIRE 1. *Si G est fini, $|\omega(e)|$ divise $|G|$.*

1.4. Equation aux classes. La dernière proposition concernant les actions de groupes que nous citerons est simple, mais pourtant très importante. Elle est connue sous le nom d'équation aux classes.

PROPOSITION 4 (Equation aux classes). *On note Ω l'ensemble des orbites de E sous l'action de G. Si E est fini, on a*

$$|E| = \sum_{\omega \in \Omega} |\omega|$$

DÉMONSTRATION. Il suffit de remarquer que les classes d'équivalence par la relation d'équivalence $\sim$ forment une partition de E. □

1.5. Une application à l'étude des p-groupes. Nous allons terminer cette section sur les opérations de groupes par une application à l'étude des p-groupes.

DÉFINITION 4. Soit p un nombre premier. On appelle *p-groupe* tout groupe fini dont l'ordre est une puissance de p.

PROPOSITION 5. *Le centre d'un p-groupe non trivial est non trivial.*

DÉMONSTRATION. Soit P un p-groupe non trivial. On fait opérer P sur lui-même par automorphisme intérieur.

$$\begin{array}{ccc} P \times P & \to & P \\ (g, x) & \mapsto & gxg^{-1} \end{array}$$

L'orbite de x est sa classe de conjugaison. Le stabilisateur de x est l'ensemble des éléments de P qui commutent avec x, c'est-à-dire le centralisateur de x

$$C_P(x) := \{g \in P : gx = xg\}$$

Faisons quelques remarques.

(i). Si $|\omega(x)| = 1$, $\mathrm{Stab}_P(x) = P$ donc $x \in Z(P)$ (le centre de P, *i.e.* l'ensemble des éléments qui commutent avec tous les éléments de P) et réciproquement.

(ii). Si $x \notin Z(P)$, $|\omega(x)|$ est une puissance de p non triviale, donc p divise $|\omega(x)|$.

On écrit alors l'équation aux classes.

$$|P| = \sum_{\omega} |\omega| = \underbrace{\sum_{|\omega|=1} |\omega|}_{=|Z(P)|} + \underbrace{\sum_{|\omega|>1} |\omega|}_{\in p\mathbb{N}}$$

On conclut en utilisant le fait que p divise $|P|$, donc divise $|Z(P)|$. □

2. Produit direct de deux groupes

Cette section a pour vocation de fixer les idées sur le produit direct de deux groupes. Nous ne rentrerons pas dans les détails.

2.1. Définition.

DÉFINITION 5. Le *produit direct de H et K* est l'ensemble $H \times K$ muni du produit

$$(h,k)(h',k') := (hh',kk')$$

2.2. Quelques propriétés. L'application

$$\begin{array}{ccc} H & \to & H \times K \\ h & \mapsto & (h,1) \end{array}$$

est un morphisme de groupes injectif. On note $\overline{H}$ son image. Il s'agit d'un sous-groupe de $H \times K$.

De même, l'application

$$\begin{array}{ccc} K & \to & H \times K \\ k & \mapsto & (1,k) \end{array}$$

est aussi un morphisme de groupes injectif. On note $\overline{K}$ son image. Il s'agit également d'un sous-groupe de $H \times K$.

PROPOSITION 6. *On dispose des propriétés suivantes.*

(i). $\overline{H}$ *et* $\overline{K}$ *commutent* *($(h,1)(1,k) = (h,k) = (1,k)(h,1)$).*

(ii). $(h,k) = (h,1)(1,k)$ *et* $H \times K =< \overline{H}, \overline{K} >$ *(le sous-groupe engendré par* $\overline{H}$ *et* $\overline{K}$*).*

(iii). $\overline{H} \cap \overline{K} = \{(1,1)\}$*, ce qui est équivalent au fait que la décomposition précédente de* (h,k) *en produit d'un élément de* $\overline{H}$ *par un élément de* $\overline{K}$ *est unique.*

Intéressons-nous maintenant au cas où le produit direct n'est pas construit à partir de deux groupes quelconques, mais au cas où il provient de deux sous-groupes d'un même groupe.

DÉFINITION 6. Soit G un groupe. Soient H et K deux sous-groupes de G. On dit que G est *produit direct de H et K* si l'application

$$\begin{array}{ccc} H \times K & \to & G \\ (h,k) & \mapsto & hk \end{array}$$

est un isomorphisme de groupes.

EXEMPLE 1. $H \times K$ est produit direct de $\overline{H}$ et $\overline{K}$.

La caractérisation du produit direct qui figure ci-dessous est certainement la proposition la plus importante de cette section.

PROPOSITION 7. *Soit G un groupe. Soient H et K deux sous-groupes de G. Alors G est produit direct de H et K si et seulement si*

(i). H *et* K *commutent,*

(ii). $H \cap K = \{1\}$*,*

(iii). $G =< H, K >$

DÉMONSTRATION. On considère l'application

$$\begin{array}{ccc} \varphi : H \times K & \to & G \\ (h,k) & \mapsto & hk \end{array}$$

- φ est un morphisme de groupes si et seulement si
$$\varphi(h,k)\varphi(h',k') = \varphi((h,k)(h',k'))$$
c'est-à-dire
$$hkh'k' = hh'kk'$$
soit encore
$$kh' = h'k$$
ce qui signifie que H et K commutent.
- On suppose que φ est un morphisme. On a
$$\ker(\varphi) = \{(h,k) : hk = 1\} = \{(h,h^{-1}), h \in H \cap K\}$$
donc φ est injectif si et seulement si $H \cap K = \{1\}$
- On suppose encore que φ est un morphisme. φ est surjectif si et seulement si $G = HK$, ce qui revient au fait que G est engendré par H et K, car ces deux groupes commutent.

□

REMARQUE 2. Supposons que l'on ait seulement

(i). H et K commutent,

(ii). $H \cap K = \{1\}$.

Alors $< H, K >$ est produit direct de H et K. En particulier, si H et K sont finis, on a $| < H, K > | = |H||K|$.

EXEMPLE 2. $\mathbb{Z}/6\mathbb{Z}$ est produit direct de $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$. On peut considérer l'application
$$\begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ x \mod 6 & \mapsto & (x \mod 2, x \mod 3) \end{array}$$

3. Produit semi-direct de deux groupes

Après avoir traité du produit direct de deux groupes, nous nous intéressons à leur produit semi-direct. Nous verrons ses principales propriétés. Nous finirons en montrant que certains groupes bien connus peuvent s'exprimer comme un produit semi-direct de deux groupes.

3.1. Définition.

DÉFINITION 7. Soient H et K deux groupes. Soit φ un morphisme de K dans $\mathrm{Aut}(H)$ (l'ensemble des automorphismes de H). On définit le *produit semi-direct de H par K via φ* comme l'ensemble $H \times K$ muni de la loi interne
$$(h,k)(h',k') := (h\varphi(k)(h'), kk')$$
On le note $H \rtimes_\varphi K$.

REMARQUE 3. Si φ est triviale, c'est-à-dire que pour tout $k \in K$, $\varphi(k) = \mathrm{Id}$, on retrouve le produit direct de H et K.

Vérifions que nous obtenons bien un groupe.

PROPOSITION 8. *La loi définie ci-dessus est une loi de groupe.*

DÉMONSTRATION. La démonstration est fastidieuse, mais ne présente aucune difficulté.

– associativité :

$$\begin{aligned}(h,k)\left((h',k')(h'',k'')\right) &= (h,k)(h'\varphi(k')(h''),k'k'')\\ &= (h\varphi(k)(h'\varphi(k')(h'')),kk'k'')\\ &= (h\varphi(k)(h')\varphi(k)(\varphi(k')(h'')),kk'k'')\\ &= (h\varphi(k)(h')\varphi(kk')(h''),kk'k'')\\ &= (h\varphi(k)(h'),kk')(h'',k'')\\ &= \left((h,k)(h',k')\right)(h'',k'')\end{aligned}$$

– élément neutre :

$$(h,k)(1,1) = (h\varphi(k)(1),k) = (h,k)$$
$$(1,1)(h,k) = (1\varphi(1)(h),k) = (h,k)$$

– inverse : montrons que l'inverse de (h,k) est $(\varphi(k^{-1})(h^{-1}),k^{-1})$

$$(h,k)(\varphi(k^{-1})(h^{-1}),k^{-1}) = (h\varphi(k)(\varphi(k^{-1})(h^{-1})),1) = (1,1)$$
$$(\varphi(k^{-1})(h^{-1}),k^{-1})(h,k) = (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h),1) = (1,1)$$

□

3.2. Quelques propriétés. L'application

$$\begin{array}{ccc} H & \to & H \rtimes_\varphi K \\ h & \mapsto & (h,1)\end{array}$$

est un morphisme de groupes injectif car

$$(h,1)(h',1) = (h\varphi(1)(h'),1) = (hh',1)$$

On note $\overline{H}$ son image. Il s'agit d'un sous-groupe de $H \rtimes_\varphi K$.

De même, l'application

$$\begin{array}{ccc} K & \to & H \rtimes_\varphi K \\ k & \mapsto & (1,k)\end{array}$$

est aussi un morphisme de groupes injectif. On note $\overline{K}$ son image. Il s'agit également d'un sous-groupe de $H \rtimes_\varphi K$.

PROPOSITION 9. *On dispose des propriétés suivantes.*

(i). $\overline{H} \cap \overline{K} = \{(1,1)\}$

(ii). *la conjugaison permet de retrouver l'action de $\varphi(k)$ sur h :*

$$\begin{aligned}(1,k)(h,1)(1,k^{-1}) &= (1\varphi(k)(h),k)(1,k^{-1})\\ &= (\varphi(k)(h)\varphi(k)(1),1)\\ &= (\varphi(k)(h),1)\end{aligned}$$

(iii). $H \rtimes_\varphi K = \overline{H}\,\overline{K}$ *car* $(h,k) = (h,1)(1,k)$ *(attention : on ne peut pas commuter ces deux éléments)*

(iv). $\overline{H}$ *est distingué dans* $H \rtimes_\varphi K$

Nous allons maintenant nous intéresser au cas où un groupe est produit semi-direct de deux de ses sous-groupes.

DÉFINITION 8. Soit G un groupe. Soient H et K deux sous-groupes de G. On suppose H distingué dans G (ce que l'on note $H \lhd G$). On a alors un morphisme de groupes de G dans $\mathrm{Aut}(H)$ induit par la conjugaison, que l'on peut restreindre à K. Plus précisément, on note

$$\begin{array}{ccc} \varphi : K & \to & \mathrm{Aut}(H) \\ g & \mapsto & (h \mapsto ghg^{-1})\end{array}$$

On dit que G est *produit semi-direct de H par K via φ* si et seulement si l'application

$$\begin{array}{rcl} H \rtimes_\varphi K & \to & G \\ (h,k) & \mapsto & hk \end{array}$$

est un isomorphisme de groupes.

Ci-dessous figure une caractérisation très importante du produit semi-direct.

PROPOSITION 10. *Soit G un groupe. Soit $H \lhd G$ et $K < G$. Alors G est produit semi-direct de H et K si et seulement si*

(i). $H \cap K = \{1\}$,

(ii). $G =< H, K >$

DÉMONSTRATION. On note

$$\begin{array}{rcl} \pi : H \rtimes_\varphi K & \to & G \\ (h,k) & \mapsto & hk \end{array}$$

- π est un morphisme si et seulement si φ est le morphisme de K dans $\mathrm{Aut}(H)$ induit par la conjugaison que nous avons évoqué dans la définition 8. En effet,
$$\begin{array}{rcl} & \pi(h,k)\pi(h',k') = \pi((h,k)(h',k')) & \\ \iff & hkh'k' = h\varphi(k)(h')kk' & \\ \iff & kh'k^{-1} = \varphi(k)(h') & \end{array}$$
- On suppose que π est un morphisme. On a
$$\ker(\pi) = \{(h,k) : hk = 1\} = \{(h,h^{-1}), h \in H \cap K\}$$
donc π est injectif si et seulement si $H \cap K = \{1\}$
- On suppose encore que π est un morphisme. π est surjectif si et seulement si $G = HK$, ce qui revient au fait que G est engendré par H et K, car K normalise H (*i.e.* pour tout $k \in K$, $kHk^{-1} = H$).

□

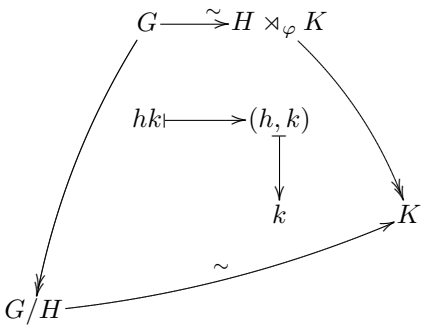
REMARQUES 1. Si H et K sont deux sous-groupes de G tels que

(i). H est normalisé par K,

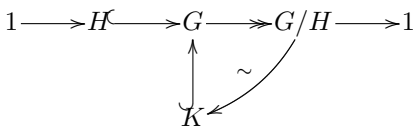
(ii). $H \cap K = \{1\}$.

Alors $< H, K >$ est produit semi-direct de H et K. En particulier, si H et K sont finis, on a $| < H, K > | = |H||K|$.

Si G est produit semi-direct de H par K, alors le quotient G/H est isomorphe à K.



La composée est un morphisme surjectif de noyau H, d'où la factorisation. On peut relever G/H en un facteur direct de G, qui est K.



G est produit direct de H et K si et seulement si H et K sont distingués. En effet, si $G = H \times K$, H centralise K (*i.e.* chaque élément de H appartient au centralisateur de chaque élément de K) et K normalise K, donc G normalise K. Réciproquement, on suppose $H \lhd G$ et $K \lhd G$. On a donc

$$\underbrace{h(\underbrace{khk^{-1}}_{\in H \lhd G}k^{-1})}_{\in H} \text{ et } \underbrace{(\underbrace{hkh^{-1}}_{\in K \lhd G})k^{-1}}_{\in K}$$

donc $hkh^{-1}k^{-1} \in H \cap K = \{1\}$. H centralise K, donc $G = H \times K$.

3.3. Exemples de produits semi-directs. Quelques groupes classiques peuvent être mis sous la forme d'un produit semi-direct.

EXEMPLE 3. – le groupe des permutations

$$\mathfrak{S}_n = \mathfrak{A}_n \rtimes < (1\ 2) >$$

– le groupe linéaire

$$\mathrm{GL}_n(\mathbb{K}) = \mathrm{SL}_n(\mathbb{K}) \rtimes \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & \lambda \end{pmatrix}, \lambda \in \mathbb{K}^* \right\}$$

– le groupe orthogonal

$$\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \rtimes \{1, \sigma\}$$

où σ est une réflexion

$$\sigma := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & -1 \end{pmatrix}$$

DÉFINITION 9. On appelle *n-ième groupe diédral* le groupe des isométries du plan qui conservent le polygône régulier à n sommets

$$\mathfrak{P}_n := \left\{ e^{i\frac{2k\pi}{n}}, k \in \{0, \ldots, n-1\} \right\}$$

Ce groupe sera noté D_{2n}.

Pour tout k, D_{2n} contient la rotation de centre 0 et d'angle $\frac{2k\pi}{n}$. Elle envoie le sommet 1 sur le sommet $e^{i\frac{2k\pi}{n}}$ et conserve $\mathfrak{P}_n$.

On pose $\mathrm{D}_{2n}^+ := \mathrm{D}_{2n} \cap \mathrm{SO}_2(\mathbb{R})$. C'est l'ensemble des rotations d'angle $\frac{2k\pi}{n}$ avec $k \in \{0, \ldots, n-1\}$, car une rotation qui conserve $\mathfrak{P}_n$ envoie un sommet sur un autre et on peut montrer que donc elle est de centre 0 et d'angle $\frac{2k\pi}{n}$. Alors, si l'on note ρ la rotation de centre 0 et d'angle $\frac{2\pi}{n}$, on a $\mathrm{D}_{2n}^+ =< \rho >$.

On dispose de la suite exacte suivante

$$1 \longrightarrow \mathrm{D}_{2n}^+ \hookrightarrow \mathrm{D}_{2n} \underset{}{\overset{\det}{\rightleftarrows}} \{-1, 1\} \longrightarrow 1$$

On exhibe une symétrie σ dans D_{2n}. Elle fournit un relèvement de -1. Alors

$$\mathrm{D}_{2n} = \{\mathrm{Id}, \rho, \dots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$$

On pose $K := \{\mathrm{Id}, \sigma\}$. On a $\sigma\rho^i\sigma^{-1} = \rho^{-i}$ donc $\mathrm{D}_{2n}^+ \lhd \mathrm{D}_{2n}$. En outre, l'intersection de D_{2n}^+ et K est l'identité. On en déduit que $< \mathrm{D}_{2n}^+, K >$ est produit semi-direct de D_{2n}^+ et K. Comme $< \mathrm{D}_{2n}^+, K >$ est d'ordre $2n$, on en déduit que $\mathrm{D}_{2n} =< \mathrm{D}_{2n}^+, K >$. Finalement, on a

$$\mathrm{D}_{2n} =< \rho > \rtimes \{\mathrm{Id}, \sigma\}$$

REMARQUE 4. On peut également définir le n-ième groupe diédral comme le produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ via l'application φ suivante

$$\begin{array}{rcl} \varphi : \mathbb{Z}/2\mathbb{Z} & \to & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ 0 & \mapsto & \mathrm{Id} \\ 1 & \mapsto & (x \mapsto -x) \end{array}$$

4. Les théorèmes de Sylow

Nous abordons à présent un résultat puissant en relation avec le théorème de Lagrange, particulièrement utile pour l'étude des groupes dont on ne détient d'information que sur son cardinal.

DÉFINITION 10. Soit G un groupe fini de cardinal n et p un nombre premier. Si $p^\alpha || n$, on appelle p-sous groupe de Sylow de G un sous groupe d'ordre p^α.

EXEMPLE 4. Soit $G = GL_n(\mathbb{F}_p)$. En comptant les bases de $\mathbb{F}_p^n$, on observe que

$$|G| = p^n(p^n - 1)(p^n - p)\dots(p^n - p^{n-1}).$$

On voit alors que $p^{\frac{n(n-1)}{2}} || n$. Un p-sous groupe de Sylow est alors l'ensemble des matrices supérieures strictes :

$$\{A = (a_{ij})) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1.\}$$

THÉORÈME 2. *Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p-Sylow.*

Via le théorème de Cayley, on peut plonger G dans $\mathfrak{S}_n$. On plonge alors $\mathfrak{S}_n$ de façon naturelle dans $GL_n(\mathbb{F}_p)$: étant donné la base canonique de $\mathbb{F}_p^n$, on associe à σ l'application $u_\sigma : e_i \mapsto e_{\sigma(i)}$. D'après l'exemple précédent, ce dernier a un p-Sylow et on conclut via le lemme suivant :

LEMME 1. *Soit G un groupe et H un sous groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

DÉMONSTRATION. On fait agir G (et donc H) par translation à gauche sur G/S. □

COROLLAIRE 2. *Si $|G| = p^\alpha m$, G contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.*

DÉMONSTRATION. On est ramené au cas des p-groupes qui se traite par récurrence (ayant toujours un centre non trivial). □

THÉORÈME 3. *Soit G un groupe de cardinal $|G| = p^\alpha m$, $p \nmid m$.*

(i). *Tout sous groupe de G qui est un p-groupe est contenu dans un p-Sylow de G.*

(ii). *Les p-Sylow de G sont tous conjugués (donc leur nombre k divise n).*

(iii). *On a $k \equiv 1[p]$ (donc $k|m$).*

Exemple d'application : un groupe d'ordre 63 n'est pas simple.

CHAPITRE 2

Corps finis

1. Rappels

1.1. Caractéristique d'un corps et sous-corps premier. Soit A un anneau. On a un morphisme d'anneaux

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \to & A \\ n & \mapsto & n \cdot 1 = \begin{cases} \underbrace{1 + \ldots + 1}_{n \text{ termes}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{-1 - \ldots - 1}_{-n \text{ termes}} & \text{si } n < 0 \end{cases} \end{array}$$

L'image de φ est le plus petit sous-anneau de A contenant 1, *i.e.* le sous-anneau engendré par 1. Ce sous-anneau est isomorphe à $\mathbb{Z}/\ker\varphi$. Comme $\mathbb{Z}$ est principal, on a $\ker\varphi = n\mathbb{Z}$.

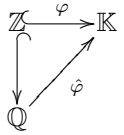
Définition 11. n est appelé la *caractéristique* de A.

Dans le cas particulier où A est intègre (par exemple, A est un corps), $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un sous-anneau de A intègre donc $n = 0$ ou n premier.

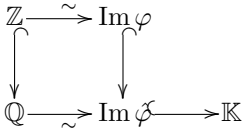
Remarque 5. La caractéristique est une propriété "locale" autour de 1 de l'anneau : si l'on ajoute des éléments à un anneau de caractéristique n, l'anneau obtenu a aussi n pour caractéristique.

Si $A = \mathbb{K}$ est un corps, sa caractéristique est 0 ou un nombre premier p.

– On suppose $\operatorname{Car}\mathbb{K} = 0$. Le sous-anneau engendré par 1 est isomorphe à $\mathbb{Z}$ (ce n'est pas un corps).

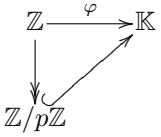


$\hat{\varphi}$ est défini par $\hat{\varphi}(\frac{a}{b}) = \varphi(a)\varphi(b)^{-1}$. On peut faire le rapprochement avec la définition du corps des fractions d'un anneau comme solution d'un problème universel : pour tout $A \xrightarrow{\varphi} \mathbb{L}$, il existe un prolongement de φ à un corps $\mathbb{K}$ (qui sera alors $\operatorname{Fr} A$) qui soit un morphisme de corps.



$\operatorname{Im}\hat{\varphi}$ est le plus petit sous-corps de $\mathbb{K}$: c'est le sous-corps premier de $\mathbb{K}$. Dans ce cas, il est isomorphe à $\mathbb{Q}$.

– On suppose $\mathrm{Car}\,\mathbb{K} = p$. Le sous-anneau engendré par 1 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, c'est aussi le sous-corps premier de $\mathbb{K}$.



DÉFINITION 12. Le plus petit sous-corps de $\mathbb{K}$ (celui engendré par 1) est appelé *sous-corps premier* de $\mathbb{K}$.

REMARQUES 2. Il est isomorphe à $\mathbb{Q}$ si $\mathrm{Car}\,\mathbb{K} = 0$ et à $\mathbb{Z}/p\mathbb{Z}$ si $\mathrm{Car}\,\mathbb{K} = p$.
Le sous-corps premier de $\mathbb{C}$ est $\mathbb{Q}$: on ne peut pas trouver de sous-corps fini de $\mathbb{C}$.

1.2. Séparabilité. Dans toute cette partie, $\mathbb{K}$ désigne un corps *commutatif*.

DÉFINITION 13. Soit P un polynôme irréductible sur $\mathbb{K}$. On dit que P est *séparable* si, dans un corps de décomposition, ses racines sont simples.

On considère l'opération de dérivation

$$\begin{array}{rcl} D : \mathbb{K}[X] & \to & \mathbb{K}[X] \\ \sum_i a_i X^i & \mapsto & \sum_i i a_i X^{i-1} \end{array}$$

LEMME 2. *Soit $P \in \mathbb{K}[X]$. Soit $a \in \mathbb{K}$. Alors $P = P(a) + DP(a)(X-a) + R(X)\cdot(X-a)^2$.*

DÉMONSTRATION. On écrit $P = b_0 + b_1(X-a) + \underbrace{b_2(X-a)^2 + \ldots}_{R(X)\cdot(X-a)^2}$. En spécialisant en a, on obtient $b_0 = P(a)$. En dérivant et en spécialisant en a, on a $b_1 = DP(a)$. □

COROLLAIRE 3. *Si a est racine du polynôme P, alors a est racine simple si et seulement si $DP(a) \neq 0$.*

COROLLAIRE 4. *Supposons P irréductible sur $\mathbb{K}$. P est non séparable si et seulement si $DP = 0$.*

DÉMONSTRATION. P est polynôme minimal de ses racines. P admet une racine multiple a si et seulement s'il existe a tel que $P(a) = DP(a) = 0$ si et seulement si P divise DP (car P polynôme minimal de a) si et seulement si $DP = 0$ (car $degDP < degP$). □

Deux cas peuvent alors se présenter
– On suppose $\mathrm{Car}\,\mathbb{K} = 0$. On note $P = \sum_i a_i X^i$. $DP = 0$ si et seulement si pour tout $i \geqslant 1$, $a_i = 0$, c'est-à-dire si P est constant. On en déduit que *tous les polynômes irréductibles sont séparables.*
– On suppose $\mathrm{Car}\,\mathbb{K} = p$. On note encore $P = \sum_i a_i X^i$. $DP = 0$ si et seulement si pour tout $i \geqslant 1$, $ia_i = 0$, c'est-à-dire si pour tout i premier avec p, $a_i = 0$, soit si $P = Q(X^p)$ avec $Q \in \mathbb{K}[X]$.

LEMME 3. *Si $\mathbb{K} = \mathbb{K}^p$, il existe Q tel que $P = Q(X^p)$ si et seulement s'il existe R tel que $P = R(X)^p$*

DÉMONSTRATION. Si A est un anneau de caractéristique p, on a dans $A[X,Y]$, $(X+Y)^p = X^p + Y^p$. Donc

$$P(X) = R(X)^p = \left(\sum_i b_i X^i\right)^p = \sum_i b_i^p X^{ip} = Q(X^p)$$

et

$$P(X) = Q(X^p) = \sum_i a_i X^{ip} = \sum_i b_i^p X^{ip} = \left(\sum_i b_i X^i\right)^p = R(X)^p$$

□

COROLLAIRE 5. *Si $\mathbb{K} = \mathbb{K}^p$, tout polynôme irréductible est séparable.*

DÉMONSTRATION. Si P est non séparable, on a $DP = 0$ donc il existe Q tel que $P(X) = Q(X^p)$, donc il existe R tel que $P(X) = R(X)^p$, donc P n'est pas irréductible. □

DÉFINITION 14. Un corps commutatif $\mathbb{K}$ est dit *parfait* si et seulement si soit $\operatorname{Car}\mathbb{K} = 0$, soit $\operatorname{Car}\mathbb{K} = p$ et $\mathbb{K} = \mathbb{K}^p$.

Si $\mathbb{K}$ est parfait, tous les polynômes irréductibles de $\mathbb{K}[X]$ sont séparables. On dit que *toutes les extensions algébriques de $\mathbb{K}$ sont séparables.*

Pour finir, donnons un exemple d'extension non séparable. Il s'agit de

$$\mathbb{Z}/p\mathbb{Z}(T^p) \subset \mathbb{Z}/p\mathbb{Z}(T)$$

En effet, $P = X^p - T^p$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}(T^p)$ et non séparable.

2. Constructions de corps finis

2.1. Structure d'espace vectoriel. Soit $\mathbb{K}$ un corps fini (*a priori* éventuellement non commutatif...). Soit $\mathbb{K}_0$ son sous-corps premier. Comme $\mathbb{K}_0$ est fini, il existe p premier tel que $\mathbb{K}_0 \simeq \mathbb{Z}/p\mathbb{Z}$. On a aussi $\operatorname{Car}(\mathbb{K}) = p$.

On munit $\mathbb{K}$ d'une structure de $\mathbb{K}_0$-espace vectoriel

$$\begin{array}{ccc} \mathbb{K}_0 \times \mathbb{K} & \to & \mathbb{K} \\ (\lambda, x) & \mapsto & \lambda x \end{array}$$

Comme $\mathbb{K}$ est fini, c'est un espace vectoriel de dimension finie. On note $n = [\mathbb{K} : \mathbb{K}_0]$. Alors $\mathbb{K}$ est de cardinal p^n.

2.2. Théorème de Wedderburn.

THÉORÈME 4 (Wedderburn). *Tout corps fini est commutatif.*

DÉMONSTRATION. Soit $\mathbb{K}$ un corps fini. On note $Z(\mathbb{K})$ son centre. C'est un sous-corps commutatif de $\mathbb{K}$. On note $q = |Z(\mathbb{K})|$. On peut munir $\mathbb{K}$ d'une structure de $Z(\mathbb{K})$-espace vectoriel

$$\begin{array}{ccc} Z(\mathbb{K}) \times \mathbb{K} & \to & \mathbb{K} \\ (\lambda, x) & \mapsto & \lambda x \end{array}$$

Comme $\mathbb{K}$ est fini, c'est un $Z(\mathbb{K})$-espace vectoriel de dimension finie, notée n. Alors $|\mathbb{K}| = q^n$.

Le groupe $\mathbb{K}^*$ opère sur $\mathbb{K}$ par automorphisme intérieur

$$\begin{array}{ccc} \mathbb{K}^* \times \mathbb{K} & \to & \mathbb{K} \\ (x, y) & \mapsto & xyx^{-1} \end{array}$$

Si $y \in \mathbb{K}$, son orbite est sa classe de conjugaison $\{xyx^{-1}, x \in \mathbb{K}^*\}$ et son stabilisateur est $\{x \in \mathbb{K}^* : xy = yx\}$.

On note $\mathbb{K}_y = \{x \in \mathbb{K} : xy = yx\}$. C'est un sous-corps de $\mathbb{K}$ qui contient $Z(\mathbb{K})$, donc qui peut être vu comme un $Z(\mathbb{K})$-espace vectoriel de dimension finie. On en déduit l'existence de n_y tel que $|\mathbb{K}_y| = q^{n_y}$.

Le stabilisateur de y est $\mathbb{K}_y^*$.

LEMME 4. $n_y | n$

DÉMONSTRATION. Nous proposerons deux démonstrations pour ce lemme. La première est la suivante. On munit $\mathbb{K}$ d'une structure de $\mathbb{K}_y$-espace vectoriel à gauche

$$\begin{array}{rcl} \mathbb{K}_y \times \mathbb{K} & \to & \mathbb{K} \\ (\lambda, x) & \mapsto & \lambda x \end{array}$$

Comme $\mathbb{K}$ est fini, il est de dimension finie d_y sur $\mathbb{K}_y$. On a donc $q^n = |\mathbb{K}| = |\mathbb{K}_y|^{d_y} = q^{n_y d_y}$, puis $n = n_y d_y$.

Ci-après figure la seconde démonstration du lemme. $\mathbb{K}_y^*$ est un sous-groupe de $\mathbb{K}^*$. D'après le théorème de Lagrange, on a $q^{n_y} - 1 | q^n - 1$. Soient s, r tels que $n = sn_y + r$ et $0 \leqslant r < n_y$. On a

$$\begin{aligned} q^n - 1 = q^{sn_y + r} - 1 &= q^r(q^{sn_y} - 1) + q^r - 1 \\ &= q^r(q^{n_y} - 1)(q^{(s-1)n_y} + \ldots + 1) + q^r - 1 \\ &= B(q^{n_y} - 1) + q^r - 1 \end{aligned}$$

On a $0 \leqslant r < n_y$. Donc $0 \leqslant q^r - 1 < q^{n_y} - 1$. Or $q^{n_y} - 1 | q^n - 1$. Donc $q^r - 1 = 0$, soit $r = 0$ (car $q \geqslant 2$). □

Reprenons la démonstration du théorème. On considère l'ensemble Ω des orbites et un représentant y_ω pour chaque orbite $\omega \in \Omega$. On écrit l'équation aux classes

$$|\mathbb{K}| = \sum_{\omega \in \Omega} |\omega| = \sum_{\omega \in \Omega} \frac{|\mathbb{K}^*|}{|\operatorname{Stab}_{\mathbb{K}^*} y_\omega|}$$

c'est-à-dire

$$q^n = \sum_{\omega \in \Omega} \frac{q^n - 1}{q^{n_{y_\omega}} - 1}$$

Or $|\omega| = 1$ si et seulement si $y_\omega \in Z(\mathbb{K})$ si et seulement si $n_{y_\omega} = n$. On peut donc écrire

$$q^n = \underbrace{q}_{\sum_{y_\omega \in Z(\mathbb{K})} 1} + \sum_{\substack{\omega \in \Omega \\ y_\omega \notin Z(\mathbb{K})}} \frac{q^n - 1}{q^{n_{y_\omega}} - 1}$$

On note $\Phi_d(X) \in \mathbb{Z}[X]$ le d-ième polynôme cyclotomique (il s'agit du produit de $X - \xi$, où ξ décrit les racines d-ièmes primitives de l'unité). Si n_{y_ω} divise strictement n, on a

$$q^n - 1 = \prod_{d|n} \Phi_d(q) = \prod_{d|n_{y_\omega}} \Phi_d(q) \prod_{\substack{d|n \\ d \nmid n_{y_\omega}}} \Phi_d(q) = (q^{n_{y_\omega}} - 1) \prod_{\substack{d|n \\ d \nmid n_{y_\omega}}} \Phi_d(q),$$

d'où l'on déduit que $\Phi_n(q)$ divise $\frac{q^n - 1}{q^{n_{y_\omega}} - 1}$. En s'aidant de l'équation aux classes, on a directement $\Phi_n(q)$ divise $q - 1$.

On remarque que pour tout $\alpha \in \mathbb{C}$ différent de 1 tel que $|\alpha| = 1$, on a $|q - \alpha| > |q - 1|$ (un dessin permet de se convaincre de cette propriété). Donc, si $n > 1$, on a $|\Phi_n(q)| > q - 1$. D'où $n = 1$, *i.e.* $\mathbb{K} = Z(\mathbb{K})$. □

2.3. Le corps fini à q éléments $\mathbb{F}_q$.

THÉORÈME 5. *Soit p un nombre premier. Soit q une puissance de p. Il existe un corps de cardinal q unique à isomorphisme près. Ce corps est le corps de décomposition du polynôme $X^q - X$ sur son sous-corps premier (lequel est isomorphe à $\mathbb{Z}/p\mathbb{Z}$). C'est aussi l'ensemble des racines de $X^q - X$ dans tout corps qui le contient.*

"Le" corps à q éléments est noté $\mathbb{F}_q$. En particulier, $\mathbb{Z}/p\mathbb{Z}$ en tant que corps est noté $\mathbb{F}_p$ (la notation $\mathbb{Z}/p\mathbb{Z}$ étant plutôt réservée à l'anneau).

On note $\mathbb{K}$ un corps commutatif de caractéristique p.

LEMME 5. *Le polynôme $X^q - X$ n'a que des racines simples dans $\mathbb{K}$.*

DÉMONSTRATION. Posons $P = X^q - X$. On a $DP = qX^{q-1} - 1 = -1$. Aucune racine de P ne peut être racine de DP donc les racines de P sont simples. □

LEMME 6. *L'application*

$$\begin{array}{rccc} \sigma : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & x^q \end{array}$$

est un morphisme de corps injectif appelé morphisme de Frobenius.

DÉMONSTRATION. D'abord, $\sigma(xy) = \sigma(x)\sigma(y)$ car $\mathbb{K}$ est supposé commutatif. Ensuite, $\sigma(x+y) = (x+y)^{p^\ell} = (x^p + y^p)^{p^{\ell-1}} = \ldots = x^{p^\ell} + y^{p^\ell} = \sigma(x) + \sigma(y)$. Enfin, σ est injectif car non nul ($\sigma(1) = 1$). □

COROLLAIRE 6. *$\{x \in \mathbb{K} : x^q = x\}$ est un sous-corps de $\mathbb{K}$. C'est l'ensemble des racines de $X^q - X$ dans $\mathbb{K}$.*

DÉMONSTRATION. (théorème 5) Démontrons l'existence. Soit $\mathbb{K} = D_{\mathbb{F}_p}(X^q - X)$ "le" corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Soit $S = \{x \in \mathbb{K} : x^q = x\}$. Le polynôme $X^q - X$ est scindé sur $\mathbb{K}$ et a toutes ses racines simples, d'après le lemme 5. Donc $|S| = q$. D'après le corollaire 6, S est un sous-corps de $\mathbb{K}$. C'est donc un corps de cardinal q.

On remarque que, $\mathbb{K}$ étant le plus petit sous-corps de $\mathbb{K}$ contenant les racines de $X^q - X$, c'est-à-dire contenant S, on a en fait $\mathbb{K} = S$.

Intéressons-nous à l'unicité. Soit $\mathbb{K}$ un corps à q éléments. Soit $\mathbb{K}_0$ son sous-corps premier. On a $|\mathbb{K}_0| = p$. Soit $x \in \mathbb{K}$. On a $x = 0$ ou $x^{q-1} = 1$, d'après le théorème de Lagrange. Donc $x^q = x$, puis $\mathbb{K} \subset \{x \in \mathbb{K} : x^q = x\}$. D'où l'égalité de ces deux derniers ensembles.

Le polynôme $X^q - X$ a au plus q racines et tous les éléments de $\mathbb{K}$ (il y en a q) sont racines. Donc il a exactement ses racines dans $\mathbb{K}$, *i.e.* il est scindé sur $\mathbb{K}$. Le plus petit sous-corps de $\mathbb{K}$ contenant les racines de $X^q - X$ est lui-même (tout élément de $\mathbb{K}$ est un de ses racines).

Donc $\mathbb{K}$ est corps de décomposition de $X^q - X$ sur $\mathbb{K}_0$. On en déduit l'unicité de $\mathbb{K}$ à isomorphisme près.

Soit maintenant $\mathbb{K}$ un corps à q éléments et $\mathbb{L}$ un sur-corps de $\mathbb{K}$. On a

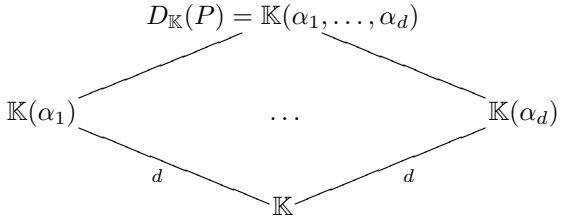
$$\mathbb{K} \subset \{x \in \mathbb{L} : x^q = x\} \subset \mathbb{L}$$

Mais $X^q - X$ a au plus q racines. Donc $\mathbb{K} = \{x \in \mathbb{L} : x^q = x\}$. Ceci implique que $\mathbb{K}$ est l'unique sous-corps à q éléments de $\mathbb{L}$. □

Donnons une application classique de ce résultat.

PROPOSITION 11. *Soit P un polynôme irréductible sur un corps fini $\mathbb{K}$. On note $\mathbb{L}$ un corps de rupture de P. Alors $\mathbb{L}$ est un corps de décomposition de P (*i.e. *P est scindé sur $\mathbb{L}$).*

DÉMONSTRATION. Soit $\mathbb{M}$ un corps de décomposition de P sur $\mathbb{K}$. Soient $\alpha_1, \ldots, \alpha_d$ les racines de P. Comme $\mathbb{M}$ est un corps fini, il contient un unique sous-corps de cardinal q^d. Donc les corps de rupture $\mathbb{K}(\alpha_i)$, qui sont de cardinal q^d, sont tous égaux : $\mathbb{K}(\alpha_1) = \ldots = \mathbb{K}(\alpha_n)$. On en déduit que $\mathbb{M} = \mathbb{K}(\alpha_1)$.



□

On dit alors que *toutes les extensions finies des corps finis sont normales.* Ces extensions sont aussi séparables : si $\mathbb{K}$ est fini de caractéristique p, le morphisme de $\mathbb{K}$ qui à x associe x^p est bijectif, donc $\mathbb{K} = \mathbb{K}^p$ et $\mathbb{K}$ est parfait. Alors, *toutes les extensions finies des corps finis sont séparables.*

EXEMPLE 5. Traitons le cas de $\mathbb{F}_4$. Ses éléments sont 0, 1, x et x^2, où x est une racine de X^2+X+1. En effet, on a $X^4-X = X(X-1)(X^2+X+1)$, c'est-à-dire, puisque nous travaillons en caractéristique 2, $X^4+X = X(X+1)(X^2+X+1)$. La table d'addition est la suivante

0	1	x	x^2
1	0	x^2	x
x	x^2	0	1
x^2	x	1	0

La table de multiplication est

1	x	x^2
x	x^2	1
x^2	1	x

3. Structure des corps finis

3.1. Structure du groupe multiplicatif.

THÉORÈME 6. *$\mathbb{F}_q^*$ est cyclique.*

On obtient ce résultat comme corollaire du théorème suivant.

THÉORÈME 7. *Soit $\mathbb{K}$ un corps commutatif. Soit G un sous-groupe fini de $\mathbb{K}^*$. Alors G est cyclique.*

DÉMONSTRATION. Soit G un sous-groupe fini de $\mathbb{K}^*$. On pose $n = |G|$. Si d est un diviseur de n, on note G_d le sous-ensemble de G formé des éléments d'ordre d. On a

$$G = \bigsqcup_{d|n} G_d$$

LEMME 7. *$|G_d| \leqslant \varphi(d)$ (où φ désigne la fonction d'Euler).*

DÉMONSTRATION. Plus précisément, nous allons démontrer que soit G_d est vide, soit $|G_d| = \varphi(d)$. Supposons G_d non vide et fixons $g_0 \in G_d$. Soit $g \in G_d$. $< g >$ est de cardinal d. $< g >$ est aussi inclus dans l'ensemble des racines du polynôme $X^d - 1$ dans $\mathbb{K}$ qui est de cardinal au plus d. D'où l'égalité de $< g >$ et de cet ensemble. g_0 est une racine de $X^d - 1$. Donc $g_0 \in < g >$, puis $< g_0 > \subset < g >$. Comme g_0 est d'ordre d, on en déduit que $< g > = < g_0 >$. g est donc un générateur du groupe cyclique $< g_0 >$ qui a pour ordre d. On en déduit que $|G_d| = \varphi(d)$. □

On peut écrire

$$n = |G| = \sum_{d|n} |G_d| \leqslant \sum_{d|n} \varphi(d) = n$$

Donc toutes les inégalités sont des égalités. En particulier, on a $|G_n| = \varphi(n)$ et donc G_n n'est pas vide. □

Nous en déduisons de manière triviale un résultat à mettre en relation avec le théorème de l'élément primitif.

COROLLAIRE 7. *Toute extension finie d'un corps fini est monogène.*

DÉMONSTRATION. Soient $\mathbb{K} \subset \mathbb{L}$, avec $\mathbb{L}$ fini. On note ξ un générateur de $\mathbb{L}^*$. Alors, on a $\mathbb{L} = \mathbb{K}(\xi)$. □

3.2. Sous-corps d'un corps fini. Soient $\mathbb{K} \subset \mathbb{M}$ deux corps finis. On cherche à décrire les sous-corps de $\mathbb{M}$ contenant $\mathbb{K}$. Dans le cas particulier où $\mathbb{K}$ est le sous-corps premier de $\mathbb{M}$, on obtient les sous-corps de $\mathbb{M}$.

On pose $q = |\mathbb{K}|$. En notant $n = [\mathbb{M} : \mathbb{K}]$, on a $|\mathbb{M}| = q^n$.

PROPOSITION 12. *Soit $\mathbb{L}$ un sous-corps de $\mathbb{M}$ contenant $\mathbb{K}$. Alors*

(i). *$\mathbb{L}$ est de cardinal q^d, avec $d|n$,*

(ii). *$\mathbb{L}$ est l'ensemble des racines du polynôme $X^{q^d} - X$ dans $\mathbb{M}$.*

DÉMONSTRATION. La multiplicativité du degré s'écrit ici :

$$\underbrace{[\mathbb{M} : \mathbb{K}]}_{n} = [\mathbb{M} : \mathbb{L}] \cdot \underbrace{[\mathbb{L} : \mathbb{K}]}_{d}$$

La seconde partie de la proposition se déduit du fait que $\mathbb{L}$ est un sous-corps de $\mathbb{M}$ de cardinal q^d et du théorème 5. □

LEMME 8. *Si $d|n$, alors $X^{q^d} - X | X^{q^n} - X$*

DÉMONSTRATION. $d|n$ donc $n = \ell d$. On a $q^n - 1 = q^{\ell d} - 1 = (q^d - 1)(q^{(\ell-1)d} + \ldots + 1)$, donc $q^d - 1 | q^n - 1$. En utilisant la même identité remarquable, on montre que $X^{q^d-1} - 1 | X^{q^n-1} - 1$. En multipliant par X, on a le résultat voulu. □

PROPOSITION 13. *Soit $d|n$. Alors $\mathbb{M}$ contient un sous-corps de cardinal q^d contenant $\mathbb{K}$.*

DÉMONSTRATION. On note S l'ensemble des racines de $X^{q^d} - X$ dans $\mathbb{M}$. $X^{q^d} - X | X^{q^n} - X$ et $X^{q^n} - X$ est scindé à racines simples sur $\mathbb{M}$, donc $X^{q^d} - X$ l'est aussi. On en déduit que $|S| = q^d$. En outre, on sait que S est un sous-corps de $\mathbb{M}$ (voir le corollaire 6). Enfin, si $x^q = x$, $x^{q^d} = x$, donc S est un sur-corps de $\mathbb{K}$. □

Récapitulons ces résultats dans le théorème suivant.

THÉORÈME 8. *L'application*

$$\begin{array}{rcl} \{\mathbb{L} \text{ corps} : \mathbb{K} \subset \mathbb{L} \subset \mathbb{M}\} & \to & \{d \in \mathbb{N} : d|n\} \\ \mathbb{L} & \mapsto & [\mathbb{L} : \mathbb{K}] \end{array}$$

est une bijection croissante d'ensembles partiellement ordonnés (le premier par l'inclusion, le second par la divisibilité). Sa réciproque est

$$\begin{array}{rcl} \{d \in \mathbb{N} : d|n\} & \to & \{\mathbb{L} \text{ corps} : \mathbb{K} \subset \mathbb{L} \subset \mathbb{M}\} \\ d & \mapsto & \{\text{racines de } X^{q^d} - X\} \end{array}$$

On peut écrire

$$\mathbb{K} \subset \mathbb{L} \subset \mathbb{L}' \subset \mathbb{M} \iff [\mathbb{L} : \mathbb{K}] | [\mathbb{L}' : \mathbb{K}]$$

3.3. Polynômes irréductibles sur un corps fini. Soit $\mathbb{K}$ un corps fini de cardinal q.

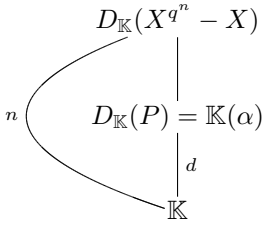
LEMME 9. *Soit $P \in \mathbb{K}[X]$ irréductible. On note d le degré de P. Alors $P | X^{q^d} - X$.*

DÉMONSTRATION. Un corps de rupture de P est de degré d sur $\mathbb{K}$, donc de cardinal q^d. Soit $\mathbb{L}$ un tel corps. On a $\mathbb{L} = \mathbb{K}(\alpha)$, où α est une racine de P. En outre, $|\mathbb{L}| = q^d$. Donc α est racine de $X^{q^d} - X$. Or P est le polynôme minimal de α sur $\mathbb{K}$. Donc $P | X^{q^d} - X$ (on retrouve que P est scindé sur $\mathbb{L}$). □

REMARQUE 6. $P | X^{q^n} - X$ pour tout n multiple de d.

PROPOSITION 14. *Soit P un diviseur irréductible de $X^{q^n}-X$ dans $\mathbb{K}[X]$. Alors le degré de P divise n.*

DÉMONSTRATION. Comme $P|X^{q^n}-X$, $\mathbb{F}_{q^n}$ contient un corps de rupture de P de degré $\deg P$ sur $\mathbb{K}$. Donc $\deg P|n$.



□

THÉORÈME 9. *Soit $n\in\mathbb{N}\backslash\{0\}$. On note $\mathcal{I}_d(q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires et de degré d. Alors "la" décomposition en produit d'irréductibles de $X^{q^n}-X$ dans $\mathbb{F}_q[X]$ est*

$$X^{q^n}-X=\prod_{d|n}\prod_{P\in\mathcal{I}_d(q)}P$$

DÉMONSTRATION. Nous savons déjà que :
- $\forall d|n, \forall P\in\mathcal{I}_d(q), P|X^{q^n}-X$,
- si P est un diviseur irréductible de $X^{q^n}-X$ supposé unitaire, alors il existe $d|n$ tel que $P\in\mathcal{I}_d(q)$.

Donc

$$X^{q^n}-X=\prod_{d|n}\prod_{P\in\mathcal{I}_d(q)}P^{m_P}$$

avec $m_P\geqslant 1$. Or $X^{q^n}-X$ n'a que des racines simples dans une extension suffisament grande, donc ne peut être divisible par le carré d'un irréductible. Donc $m_P=1$. □

REMARQUE 7. Cette décomposition de $X^{q^n}-X$ permet de classer les éléments de $\mathbb{F}_{q^n}$ de la manière suivante.

$$\underbrace{X^{q^n}-X}_{\text{éléments de } \mathbb{F}_{q^n}}=\prod_{d|n}\underbrace{\prod_{P\in\mathcal{I}_d(q)}P}_{\substack{\text{éléments de } \mathbb{F}_{q^d} \text{ qui ne sont}\\ \text{pas dans } \mathbb{F}_{q^e} \text{ pour } e|d, e\neq d}}$$

Par exemple, pour $p=2$ et $n=2$,

$$\underbrace{X^4+X}_{\mathbb{F}_4}=\underbrace{X(X+1)}_{\mathbb{F}_2}\underbrace{(X^2+X+1)}_{\mathbb{F}_4\backslash\mathbb{F}_2}$$

4. Prolongements

4.1. Représentation d'un corps fini comme quotient d'un anneau de polynômes. Soit P un polynôme de degré n irréductible sur $\mathbb{F}_q$. Alors $\mathbb{F}_q[X]/(P)$ est de cardinal q^n.

Soit un entier $n\geqslant 1$. On choisit un polynôme P irréductible de degré n sur $\mathbb{F}_p$. Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.

Il existe un tel polynôme irréductible de degré n. En effet, si ξ est un générateur de $\mathbb{F}_{p^n}^*$, le corps engendré par ξ sur $\mathbb{F}_p$ ne peut être que $\mathbb{F}_{p^n}$, donc son polynôme minimal est de degré n.

En fait, il en existe plusieurs. Il n'y a pas unicité d'une telle représentation de $\mathbb{F}_{p^n}$.

EXEMPLE 6. Pour commencer, considérons l'extension $\mathbb{F}_2 \subset \mathbb{F}_8$. On a

$$\begin{aligned} X^8+X &= X(X+1)(X^6+X^5+X^4+X^3+X^2+X+1) \\ &= X(X+1)\underbrace{(X^3+X+1)(X^3+X^2+1)}_{\text{2 irréductibles de degré 3}} \end{aligned}$$

Donc $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$ ou encore $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X^2+1)$.

Continuons avec l'extension $\mathbb{F}_2 \subset \mathbb{F}_{16}$. On a

$$\begin{aligned} X^{16}+X = \quad & \overbrace{X(X+1)\underbrace{(X^2+X+1)}_{\substack{\text{le seul irréductible}\\ \text{de degré 2}}}}^{X^4+X} \\ & \underbrace{(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1)}_{\text{3 irréductibles de degré 4}} \end{aligned}$$

En effet, si $P = X^4+aX^3+bX^2+cX+d$ est irréductible, on a $1 = P(0) = d$ et $1 = P(1) = a+b+c$. Les possibilités pour P sont donc $X^4+X^3+X^2+X+1$, X^4+X^3+1, X^4+X+1, mais pas $(X^2+X+1)^2$ qui n'est pas irréductible. On a finalement par exemple $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4+X^3+X^2+X+1)$.

Dans la décomposition précédente de $X^{16}+X$, on peut également lire des informations sur le groupe multiplicatif $\mathbb{F}_{16}^*$.

$$\begin{aligned} X^{16}+X = \quad & X\underbrace{(X+1)}_{1}\underbrace{(X^2+X+1)}_{\substack{\text{2 éléments d'ordre 3}\\ (X^2+X+1 \mid X^3+1)}}\underbrace{(X^4+X^3+X^2+X+1)}_{\substack{\text{4 éléments d'ordre 5}\\ (X^4+X^3+X^2+X+1 \mid X^5+1)}} \\ & \underbrace{(X^4+X^3+1)(X^4+X+1)}_{\varphi(15)=8 \text{ éléments d'ordre 15}} \end{aligned}$$

4.2. Critères d'irréductibilité de polynômes. Soit $P \in \mathbb{F}_q[X]$. On se pose la question de savoir si P est irréductible.

On note $n = \deg P$. P irréductible sur $\mathbb{F}_q$ si et seulement si P n'a pas de racine dans une extension de $\mathbb{F}_q$ de degré $< n$ et même $\leqslant \frac{n}{2}$ (si l'on s'intéresse au plus petit diviseur).

REMARQUES 3. Soient $P, Q \in \mathbb{K}[X]$ et une extension $\mathbb{K} \subset \mathbb{L}$. On a $P \wedge_{\mathbb{K}} Q = P \wedge_{\mathbb{L}} Q$.

P a une racine dans $\mathbb{F}_{q^d}$ si et seulement si P a une racine commune avec $X^{q^d}-X$ si et seulement si $P \wedge (X^{q^d}-X) \neq 1$.

On en déduit le critère suivant :

$$P \text{ irréductible} \iff \begin{cases} P \wedge (X^q - X) &= 1 \\ P \wedge (X^{q^2} - X) &= 1 \\ & \vdots \\ P \wedge (X^{q^{\lfloor \frac{n}{2} \rfloor}} - X) &= 1 \end{cases}$$

Les informations que nous venons de donner quant à l'irréductibilité d'un polynôme de $\mathbb{F}_q[X]$ permettent de s'intéresser au problème de l'irréductibilité d'un polynôme de $\mathbb{Z}[X]$.

Pour étudier ce problème, on dispose d'abord du critère d'Eisenstein.

En outre, on peut utiliser le critère de réduction présenté ci-après. On remarque que si $P = QR$ dans $\mathbb{Z}[X]$, alors $\bar{P} = \bar{Q}\bar{R}$ dans $\mathbb{F}_p[X]$. On est donc ramené à chercher s'il existe un nombre premier p tel que P soit irréductible modulo p. (On peut être amené à conduire des raisonnements plus compliqués, mais qui utilisent le même argument : imaginons par exemple que modulo 2, P soit produit d'un irréductible

de degré 1 et d'un irréductible de degré 4, et que modulo 3, P soit produit d'un irréductible de degré 2 et d'un irréductible de degré 3, alors P est irréductible).

Il est à noter que ce critère ne fonctionne pas toujours. Par exemple, le polynôme X^4+1 est irréductible dans $\mathbb{Z}[X]$ (c'est un polynôme cyclotomique), alors qu'il est réductible modulo p pour tout nombre premier p.

4.3. Algorithme de Berlekamp. C'est un algorithme qui permet de décomposer un polynôme $P \in \mathbb{F}_q[X]$ en produit d'irréductibles (voir [**7**]).

Quitte à considérer le polynôme $\frac{P}{P \wedge P'}$, on peut supposer que $P = P_1 \dots P_k$, les P_i étant irréductibles non associés deux à deux. D'après le lemme chinois, il existe un isomorphisme d'anneaux

$$\varphi : \mathbb{F}_q[X]/(P) \to \mathbb{F}_q[X]/(P_1) \times \dots \times \mathbb{F}_q[X]/(P_k)$$

Considérons $H = \{x \in \mathbb{F}_q[X]/(P) : x^q = x\}$. Alors on a

$$\begin{aligned}\varphi(H) &= \left\{ (x_1, \dots, x_k) \in \prod_{i=1}^{k} \mathbb{F}_q[X]/(P_i) : \forall i, x_i^q = x_i \right\} \\ &\simeq \prod_{i=1}^{k} \underbrace{\{x_i \in \mathbb{F}_q[X]/(P_i) : x_i^q = x_i\}}_{\text{sous-corps à } q \text{ éléments de } \mathbb{F}_q[X]/(P_i)}\end{aligned}$$

Donc H est en bijection avec $(\mathbb{F}_q)^k$.

LEMME 10. *Soit*

$$\begin{array}{rcl} \eta : \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ x & \mapsto & x^q - x \end{array}$$

η est un endomorphisme du $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_q[X]/(P)$ de noyau H.

DÉMONSTRATION. $\eta(x+y) = (x+y)^q - (x+y) = (x^q - x) + (y^q - y) = \eta(x) + \eta(y)$ et $\eta(\lambda x) = (\lambda x)^q - \lambda x = \lambda^q x^q - \lambda x \underbrace{=}_{\text{car } \lambda \in \mathbb{F}_q} \lambda(x^q - x) = \lambda \eta(x)$. C'est donc bien un endomorphisme dont H est le noyau par définition. □

COROLLAIRE 8. *H est un sous-espace vectoriel de dimension k.*

On peut ainsi calculer k : on commence par calculer la matrice de η sur la base $(1, X, \dots, X^{\deg P - 1})$. On calcule le rang de cette matrice et on en déduit la dimension de H, *i.e.* la valeur de k.

On suppose $k > 1$ (si $k = 1$, P est irréductible). On peut déterminer $h \in H \backslash \mathbb{F}_q \cdot 1$ (*i.e.* h non constant). Soit $\hat{h}$ relevant h dans $\mathbb{F}_q[X]$, avec $\deg \hat{h} < \deg P$. On a $\eta(h) = 0$ si et seulement si $P | \hat{h}^q - \hat{h} = \prod_{\lambda \in \mathbb{F}_q} (\hat{h} - \lambda)$. On en déduit que

$$P = \prod_{\lambda \in \mathbb{F}_q} (P \wedge (\hat{h} - \lambda))$$

On remarque que si $\lambda \neq \mu$, $(\hat{h} - \lambda) - (\hat{h} - \mu) = \mu - \lambda \in \mathbb{F}_q^*$, donc $(\hat{h} - \lambda) \wedge (\hat{h} - \mu) = 1$. En outre, $\deg(P \wedge (\hat{h} - \lambda)) < \deg P$. On obtient donc une factorisation non triviale de P. On réitère le processus et on cherche les multiplicités si nécessaire.

4.4. Algèbres de polynômes sur un corps fini. Soit $\mathbb{K}$ un corps. On note $\mathcal{F}(\mathbb{K}^n, \mathbb{K})$ l'ensemble des applications de $\mathbb{K}^n$ dans $\mathbb{K}$. C'est une $\mathbb{K}$-algèbre. On a un morphisme de $\mathbb{K}$-algèbres

$$\begin{array}{rcl} \mathbb{K}[X_1, \dots, X_n] & \to & \mathcal{F}(\mathbb{K}^n, \mathbb{K}) \\ P & \mapsto & (\tilde{P} : (x_1, \dots, x_n) \mapsto P(x_1, \dots, x_n)). \end{array}$$

PROPOSITION 15. *Si $\mathbb{K}$ est infini, ce morphisme est injectif.*

DÉMONSTRATION. Le résultat se démontre par récurrence sur n. Supposons $\tilde{P} = 0$. On note $P = \sum_i Q_i(X_1, \ldots, X_{n-1}) X_n^i$. Pour tous $a_1, \ldots, a_{n-1}$, le polynôme $\sum_i Q_i(a_1, \ldots, a_{n-1}) X_n^i$ est nul sur $\mathbb{K}$. Le seul polynôme ayant une infinité de racines est 0. Donc le polynôme est nul, *i.e.* pour tout i, $Q_i(a_1, \ldots, a_{n-1}) = 0$. On applique alors l'hypothèse de récurrence à chaque Q_i : $\tilde{Q}_i = 0 \Rightarrow Q_i = 0$. Donc $P = 0$. □

REMARQUE 8. Le morphisme n'est pas surjectif : pour s'en convaincre, il suffit de considérer une fonction nulle partout sauf en un point.

PROPOSITION 16. *Si $\mathbb{K}$ est un corps fini de cardinal q, ce morphisme n'est pas injectif. Son noyau est l'idéal $(X_1^q - X_1, \ldots, X_n^q - X_n)$. En revanche, il est surjectif.*

DÉMONSTRATION. Le calcul du noyau se fait par récurrence sur n. Soit P tel que $\tilde{P} = 0$. On a $P = \sum_i Q_i'(X_1, \ldots, X_{n-1}) X_n^i$. On écrit P sous la forme $P = (X_n^q - X_n)R + \sum_{i<q} Q_i(X_1, \ldots, X_{n-1}) X_n^i$. Pour tous $a_1, \ldots, a_n \in \mathbb{K}$, on a $\tilde{P}(a_1, \ldots, a_n) = 0$ donc $\sum_{i<q} Q_i(a_1, \ldots, a_{n-1}) a_n^i = 0$. Le polynôme $\sum_{i<q} Q_i(a_1, \ldots, a_{n-1}) X_n^i$ admet au moins q racines et est de degré $< q$, donc il est nul. Alors, pour tout $i < q$, $Q_i(a_1, \ldots, a_{n-1}) = 0$. Donc, pour tout $i < q$, $\tilde{Q}_i = 0$. On applique aux Q_i l'hypothèse de récurrence. Donc $Q_i \in (X_1^q - X_1, \ldots, X_{n-1}^q - X_{n-1})$, puis $P \in (X_1^q - X_1, \ldots, X_n^q - X_n)$.

Etudions la surjectivité. Toute fonction $f \in \mathcal{F}(\mathbb{K}^n, \mathbb{K})$ peut s'écrire

$$f = \sum_{(x_1, \ldots, x_n)} f(x_1, \ldots, x_n) \mathbb{1}_{(x_1, \ldots, x_n)}.$$

On remarque que $x \mapsto 1 - x^{q-1}$ est la fonction indicatrice de 0 sur $\mathbb{K}$. Donc $(x_1, \ldots, x_n) \mapsto \prod_{i=1}^n (1 - x_i^{q-1})$ est la fonction indicatrice de $(0, \ldots, 0)$ sur $\mathbb{K}^n$. Alors, $(x_1, \ldots, x_n) \mapsto \prod_{i=1}^n (1 - (x_i - y_i)^{q-1})$ est la fonction indicatrice du point $(y_1, \ldots, y_n)$ sur $\mathbb{K}^n$. □

CHAPITRE 3

Réduction d'un endomorphisme

Commençons par fixer quelques notations. Soit $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie n. On note $\mathcal{L}(E)$ l'algèbre des endomorphismes de E. On note $\mathcal{GL}(E)$ le groupe des automorphismes de E. $\mathrm{M}_n(\mathbb{K})$ désignera l'algèbre des matrices $n \times n$ à coefficients dans $\mathbb{K}$ et $\mathrm{GL}_n(\mathbb{K})$ le groupe linéaire des matrices inversibles.

Le problème que nous étudierons est le suivant. $\mathcal{GL}(E)$ opère sur $\mathcal{L}(E)$ par conjugaison :

$$\begin{array}{rcl} \mathcal{GL}(E) \times \mathcal{L}(E) & \to & \mathcal{L}(E) \\ (w, u) & \mapsto & w^{-1}uw \end{array}$$

Deux endomorphismes d'une même orbite sont dits semblables. Une orbite est appelée classe de similitude.

Le but est de caractériser de façon effective les classes de similitude. On remarque que deux endomorphismes u et v sont semblables si et seulement si u et v ont même matrice dans des bases éventuellement différentes. Nous serons amenés à chercher pour telle matrice une matrice simple, d'où le terme réduction.

1. Polynôme minimal et polynôme caractéristique d'un endomorphisme

Soit $u \in \mathcal{L}(E)$.

1.1. Polynôme minimal. On définit un morphisme de $\mathbb{K}$-algèbres

$$\begin{array}{rcl} \varphi_u : \mathbb{K}[X] & \to & \mathcal{L}(E) \\ P & \mapsto & P(u) \end{array}$$

Son image est la sous-algèbre commutative $\mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\}$.

Son noyau est un idéal de $\mathbb{K}[X]$. Comme $\mathcal{L}(E)$ est de dimension finie, φ_u ne peut être injectif. Comme $\mathbb{K}[X]$ est principal, $\ker \varphi_u$ également. Il admet un unique générateur unitaire appelé polynôme minimal de u et noté π_u.

On a $\mathbb{K}[u] \simeq \mathbb{K}[X]/(\pi_u)$. En particulier, $\dim \mathbb{K}[u] = \deg \pi_u$.

Remarques 4. Ceci est faux en général si E est de dimension infinie. Par exemple,

$$\begin{array}{rcl} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & XP \end{array}$$

n'a pas de polynôme minimal, ni même de polynôme annulateur non nul.

On a, pour $u \in \mathcal{L}(E)$ et $w \in \mathcal{GL}(E)$, pour tout polynôme P, $P(w^{-1}uw) = w^{-1}P(u)w$. Donc l'idéal annulateur de u est celui de $w^{-1}uw$. Le polynôme minimal est un invariant de la classe de similitude.

1.2. Polynôme caractéristique. On commence par définir le polynôme caractéristique d'une matrice $A \in \mathrm{M}_n(\mathbb{K})$ en posant

$$\chi_A = \det(XI_n - A)$$

C'est le déterminant de la matrice $XI_n - A \in \mathrm{M}_n(\mathbb{K}[X])$.

On remarque que, si $P \in \mathrm{GL}_n(\mathbb{K})$,

$$\begin{aligned}\chi_{PAP^{-1}} &= \det(XI_n - PAP^{-1}) \\ &= \det(P(XI_n - A)P^{-1}) \\ &= \det P \det(XI_n - A) \det P^{-1} \\ &= \det(XI_n - A) \\ &= \chi_A\end{aligned}$$

DÉFINITION 15. Toutes les matrices de l'endomorphisme u ont le même polynôme caractéristique que l'on appelle *polynôme caractéristique de* u et que l'on note χ_u.

REMARQUE 9. Le polynôme caractéristique est aussi un invariant de la classe de similitude.

2. Sous-espaces stables

Soit $u \in \mathcal{L}(E)$.

DÉFINITION 16. Soit F un sous-espace vectoriel de E. On dit que F est *stable* par u (ou u-stable) si $u(F) \subset F$.

REMARQUE 10. Si F est u-stable et G est un supplémentaire de F, alors la matrice de u dans une base associée à la somme directe $F \oplus G$ s'écrit

$$\begin{pmatrix} \bigstar & \bigstar \\ 0 & \bigstar \end{pmatrix} \begin{matrix} \}F \\ \}G \end{matrix}$$

où $\bigstar$ désigne des coefficients sur lesquels on ne connait aucune information particulière *a priori*.

EXEMPLE 7.
- Si F est u-stable de dimension 1, F est une droite propre : $F = \mathbb{K}e$ et $u(e) = \lambda e$.
- Un sous-espace d'un sous-espace propre est stable : $F \subset \ker(u - \lambda \mathrm{Id})$.
- $\ker v$ et $\mathrm{Im}\, v$ sont u-stables, lorsque v et u commutent.
- $\{0\}$ et E sont u-stables.

REMARQUE 11. Si F est un sous-espace vectoriel u-stable, alors u induit sur F un endormorphisme

$$\begin{array}{rccc} u_F : & F & \to & F \\ & x & \mapsto & u(x) \end{array}$$

En prenant G un supplémentaire de F, $\mathcal{B}_F$ une base de F et $\mathcal{B}_G$ une base de G, la matrice de u dans la base $\mathcal{B}_F \cup \mathcal{B}_G$ est

$$\begin{pmatrix} A & \bigstar \\ 0 & \bigstar \end{pmatrix} \begin{matrix} \}F \\ \}G \end{matrix}$$

où A est la matrice de u_F dans la base $\mathcal{B}_F$.

On en déduit que le polynôme caractéristique de u_F divise celui de u : $\chi_{u_F} | \chi_u$.

On a aussi $\pi_u(u) = 0$ donc $\pi_u(u_F) = 0$. Alors $\pi_{u_F} | \pi_u$.

PROPOSITION 17. *Si $E = F \oplus G$, avec F et G u-stables, alors $\chi_u = \chi_{u_F}\chi_{u_G}$ et $\pi_u = \pi_{u_F} \vee \pi_{u_G}$.*

La démonstration de ce résultat est laissée en exercice.

PROPOSITION 18. *Soit $Q \in \mathbb{K}[X]$. Posons $F = \ker Q(u)$. (F est donc u-stable.) Alors $\pi_{u_F} = \pi_u \wedge Q$.*

DÉMONSTRATION. On sait d'une part que π_{u_F} divise π_u. D'autre part, $Q(u_F) = Q(u)_F = 0$. Donc $\pi_{u_F}|Q$. On en déduit que $\pi_{u_F}|\pi_u \wedge Q$.

Soit $R = \pi_u \wedge Q$. Comme $R|Q$, on a $\ker R(u) \subset \ker Q(u)$. En écrivant, d'après le théorème de Bézout, $R = A\pi_u + BQ$, on a $R(u) = B(u)Q(u)$, donc $\ker Q(u) \subset \ker R(u)$ et $F = \ker R(u)$.

Posons $R = \pi_{u_F} S$. On sait que $R|\pi_u$, donc il existe T tel que $\pi_u = RT$. Alors $R(u)T(u) = 0$ donc $\operatorname{Im} T(u) \subset \ker R(u)$. On a $\ker R(u) = F \subset \ker \pi_{u_F}(u)$. Donc $\operatorname{Im} T(u) \subset \ker \pi_{u_F}(u)$, puis $\pi_{u_F}(u)T(u) = 0$.

On a donc $\pi_u = RT = \underbrace{\pi_{u_F} T}_{\substack{\text{annule } u \\ \text{et divise } \pi_u}} S$. Par minimalité de π_u, on a $S \in \mathbb{K}[X]^*$ et $R \in \mathbb{K}^* \pi_{u_F}$. □

3. Sous-espaces cycliques et théorème de Cayley-Hamilton

DÉFINITION 17. Soit $x \in E$. On appelle *sous-espace u-cyclique engendré par x* le plus petit sous-espace vectoriel u-stable qui contient x. On le note $< x >_u$.

Un tel sous-espace existe car une intersection de sous-espaces u-stables est u-stable :

$$< x >_u = \bigcap_{\substack{F\, u-\text{stable} \\ x \in F}} F$$

PROPOSITION 19. *On a* $< x >_u = \{P(u)(x), P \in \mathbb{K}[X]\}$.

La démonstration de cette proposition est laissée en exercice.

PROPOSITION 20. *Soit* $x \in E$. *Soit* $F =< x >_u$. *Soit* $P \in \mathbb{K}[X]$. *On a l'équivalence suivante*

$$P(u_F) = 0 \iff P(u)(x) = 0$$

DÉMONSTRATION. L'implication directe est triviale, car $x \in F$. Traitons l'implication réciproque. Soit $y \in F$. Il existe $Q \in \mathbb{K}[X]$ tel que $y = Q(u)(x)$. On a $P(u)(y) = P(u)(Q(u)(x)) = Q(u)(P(u)(x)) = 0$, donc $P(u_F) = 0$. □

PROPOSITION 21. *Soit* $x \in E$ *et* $F =< x >_u$. *Soit* d *l'entier défini par*

$$\begin{cases} (x, u(x), \ldots, u^{d-1}(x)) \text{ libre} \\ (x, u(x), \ldots, u^{d}(x)) \text{ liée} \end{cases}$$

Alors $(x, u(x), \ldots, u^{d-1}(x))$ *est une base de* F *et* $\dim F = d$. *En outre, la matrice de* u_F *dans cette base est de la forme*

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & a_d \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_2 \\ 0 & \cdots & 0 & 1 & a_1 \end{pmatrix}$$

et $\pi_{u_F} = X^d - a_1 X^{d-1} - a_2 X^{d-2} - \ldots - a_d$.

DÉMONSTRATION. $(x, u(x), \ldots, u^{d-1}(x))$ est libre si et seulement si pour tout $P \in \mathbb{K}[X]$ tel que $\deg P < d$ et $P(u)(x) = 0$, on ait $P = 0$. $(x, u(x), \ldots, u^{d}(x))$ est liée si et seulement si il existe un polynôme $P \in \mathbb{K}[X]_d$ non nul tel que $P(u)(x) = 0$. On en déduit que le polynôme minimal de u_F est exactement de degré d.

Soit $(\lambda_0, \ldots, \lambda_d) \in \mathbb{K}^{d+1} \backslash \{0\}$ tel que $\lambda_0 + \lambda_1 x + \ldots + \lambda_d u^d(x) = 0$. On a $\lambda_d \neq 0$ sinon $(x, u(x), \ldots, u^{d-1}(x))$ serait liée. En divisant par λ_d, on obtient une égalité de la forme

$$u^d(x) = a_d x + a_{d-1} u(x) + \ldots + a_1 u^{d-1}(x)$$

Le polynôme $X^d - a_1X^{d-1} - a_2X^{d-2} - \ldots - a_d$ est le polynôme P de plus petit degré parmi les non nuls vérifiant $P(u)(x) = 0$. C'est donc π_{u_F}.

Par hypothèse, $(x, u(x), \ldots, u^{d-1}(x))$ est une famille libre de F. Montrons qu'elle est génératrice. Soit $Q \in \mathbb{K}[X]$. On a $Q = R\pi_{u_F} + S$ avec $\deg S < \deg \pi_{u_F} = d$. $Q(u)(x) = S(u)(x) \in \text{Vect}(x, u(x), \ldots, u^{d-1}(x))$.

On écrit la matrice de u_F dans cette base

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & a_d \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_2 \\ 0 & \cdots & 0 & 1 & a_1 \end{pmatrix} \begin{matrix} \}x \\ \vdots \\ \vdots \\ \}u^{d-2}(x) \\ \}u^{d-1}(x) \end{matrix}$$

□

Définition 18. Soit $P \in \mathbb{K}[X]$ unitaire. On note $d = \deg P$. On pose $P = X^d - a_1X^{d-1} - \ldots - a_d$. On appelle *matrice compagnon* associée à P la matrice $d \times d$ suivante :

$$\begin{pmatrix} 0 & \cdots & \cdots & 0 & a_d \\ 1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_2 \\ 0 & \cdots & 0 & 1 & a_1 \end{pmatrix}$$

On la note $\mathcal{C}(P)$.

Exemple 8. Soit $x \in E$ et $F =< x >_u$. u_F admet comme matrice la matrice compagnon associée à π_{u_F}.

Proposition 22. *Soit u un endomorphisme de E qui admet comme matrice la matrice compagnon associée à un polynôme P. Alors E est u-cyclique (*i.e. *il existe $x \in E$ tel que $E =< x >_u$) et $P = \chi_u = \pi_u$.*

Démonstration. Soit $(e_1, \ldots, e_d)$ une base de E sur laquelle la matrice de u est $\mathcal{C}(P)$. Alors $E =< e_1 >_u$. En effet, $\text{Vect}(e_1, \ldots, e_d) = \text{Vect}(e_1, \ldots, u^{d-1}(e_1))$.

On sait alors que les coefficients de $u^d(e_1)$ sur la base $(e_1, \ldots, u^{d-1}(e_1)) = (e_1, \ldots, e_d)$ définissent ceux du polynôme minimal :

$$\pi_{u_F} = X^d - a_1X^{d-1} - \ldots - a_d$$

Calculons χ_u. On a

$$\chi_u = \begin{vmatrix} X & 0 & \cdots & 0 & -a_d \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & -a_2 \\ 0 & \cdots & 0 & -1 & X-a_1 \end{vmatrix}$$

$$= \sum_{i=1}^{d-1}(-1)^{i+d}(-a_{d-i+1})$$

$$\begin{vmatrix} X & 0 & \cdots & \cdots & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ -1 & \ddots & \ddots & & \vdots & \vdots & & & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots & \vdots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots & & & & \vdots \\ 0 & \cdots & 0 & -1 & X & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & -1 & X & 0 & \cdots & 0 \\ \vdots & & & & \vdots & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & & \vdots & \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & \vdots & \vdots & & \ddots & \ddots & X \\ 0 & \cdots & \cdots & \cdots & 0 & 0 & \cdots & \cdots & 0 & -1 \end{vmatrix} \begin{matrix} \uparrow \\ \vdots \\ i-1 \\ \vdots \\ \downarrow \\ \uparrow \\ \vdots \\ d-i \\ \vdots \\ \downarrow \end{matrix}$$

$$+ (X-a_1)\begin{vmatrix} X & 0 & \cdots & \cdots & 0 \\ -1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -1 & X \end{vmatrix}$$

$$= \sum_{i=1}^{d-1}(-1)^{i+d}(-a_{d-i+1})X^{i-1}(-1)^{d-i} + (X-a_1)X^{d-1} = P$$

□

COROLLAIRE 9. *Soit F un sous-espace vectoriel u-cyclique. Alors $\pi_{u_F} = \chi_{u_F}$.*

THÉORÈME 10 (Cayley-Hamilton). *π_u divise χ_u.*

DÉMONSTRATION. Soit $x \in E$. On pose $F =< x >_u$. D'après le corollaire 9, on a $\pi_{u_F} = \chi_{u_F}$. Donc, $\chi_{u_F}(u)(x) = 0$. Or $\chi_{u_F} | \chi_u$. Donc $\chi_u(u)(x) = 0$, puis $\chi_u(u) = 0$. On en déduit que $\pi_u | \chi_u$.

Nota bene : Il existe de nombreuses démonstrations de ce théorème. Certaines utilisent la densité de certains espaces, lorsque $\mathbb{K}$ est égal à $\mathbb{R}$ ou $\mathbb{C}$. Une autre consiste à démontrer l'identité remarquable suivante

$$\det\left(\begin{pmatrix} X_{1,1} & \cdots & X_{n,1} \\ \vdots & & \vdots \\ X_{n,1} & \cdots & X_{n,n} \end{pmatrix} - X\,\mathrm{I}_n\right)\begin{pmatrix} X_{1,1} & \cdots & X_{n,1} \\ \vdots & & \vdots \\ X_{n,1} & \cdots & X_{n,n} \end{pmatrix} = 0$$

□

4. Lemme de décomposition des noyaux

4.1. Enoncé et premières conséquences. Soit $u \in \mathcal{L}(E)$.

LEMME 11 (Décomposition des noyaux). *Soit P un polynôme de $\mathbb{K}[X]$ tel que $P(u) = 0$. On suppose que $P = P_1 \dots P_r$ où les P_i sont premiers entre eux deux à deux. Alors E admet la décomposition en somme directe de sous-espaces stables suivante*

$$E = \bigoplus_{i=1}^{r} \ker P_i(u)$$

En outre, les projecteurs associés à cette décomposition sont des polynômes en u.

DÉMONSTRATION. On a $P = P_1 \dots P_r$. Si $i \in \{1, \dots, r\}$, on pose $Q_i = \prod_{j \neq i} P_j = \frac{P}{P_i}$. Comme les P_i sont premiers entre eux deux à deux, les Q_i sont premiers entre eux dans leur ensemble. (En effet, si A est un diviseur irréductible de Q_i, il existe $j \neq i$ tel que A divise P_j et aucun autre des P_k, donc $A \nmid Q_j$.) D'après le théorème de Bézout, il existe des polynômes $A_1, \dots, A_r$ tels que $\sum_i A_i Q_i = 1$.

On pose pour tout i, $\pi_i = A_i Q_i(u) \in \mathbb{K}[u]$. On a $\sum_i \pi_i = \mathrm{Id}$. En outre, si $i \neq j$, $P | Q_i Q_j$, donc $P | (A_i Q_i)(A_j Q_j)$, puis $\pi_i \pi_j = 0$. On sait alors que les π_i sont des projecteurs et donc que

$$\begin{cases} E &= \bigoplus_i \operatorname{Im} \pi_i \\ \ker \pi_j &= \bigoplus_{j \neq i} \operatorname{Im} \pi_j \end{cases}$$

$P_i(u)\pi_i = 0$ car $P | P_i A_i Q_i$. Donc $\operatorname{Im} \pi_i \subset \ker P_i(u)$.

Réciproquement, soit $x \in \ker P_i(u)$. Soit $j \neq i$. P_i divise $A_j Q_j$, donc $\pi_j(x) = 0$. On a $x = \sum_j \pi_j(x) = \pi_i(x) \in \operatorname{Im} \pi_i$. D'où $\ker P_i(u) \subset \operatorname{Im} \pi_i$. □

On décompose le polynôme minimal de u en produit de puissances d'irréductibles deux à deux non associés :

$$\pi_u = P_1^{\alpha_1} \dots P_r^{\alpha_r}$$

Alors le lemme de décomposition des noyaux assure que

$$E = \bigoplus_{i=1}^{r} \ker P_i^{\alpha_i}(u)$$

Sur $\ker P_i^{\alpha_i}(u)$, le polynôme minimal de la restriction de u est $P_i^{\alpha_i}$ (voir la proposition 18).

DÉFINITION 19. Les sous-espaces vectoriels $\ker P_i^{\alpha_i}(u)$ sont appelés les *sous-espaces caractéristiques* de u.

PROPOSITION 23. *Soit P un polynôme. On a*

$$\{0\} \subset \ker P(u) \subset \ker P^2(u) \subset \dots \subset \ker P^i(u) \subset \dots$$

Si $\ker P^i(u) = \ker P^{i+1}(u)$, alors $\ker P^{i+1}(u) = \ker P^{i+2}(u)$. La suite est donc strictement croissante, puis stationnaire : il existe un entier α tel que

$$\begin{cases} \forall i < \alpha, \ker P^i(u) \subsetneq \ker P^{i+1}(u) \\ \forall i \geqslant \alpha, \ker P^i(u) = \ker P^{i+1}(u) \end{cases}$$

On a alors

$$\ker P^{\alpha}(u) = \bigcup_{i \in \mathbb{N}} \ker P^i(u)$$

La démonstration est laissée au lecteur.

PROPOSITION 24. *Lorsque P est un diviseur irréductible du polynôme minimal de u,*

$$\bigcup_{i\in\mathbb{N}} \ker P^i(u) = \ker P^\alpha(u)$$

où α est la multiplicité de P dans π_u.

DÉMONSTRATION. Pour $i < \alpha$, on a $\pi_{u_{\ker P^i(u)}} = P^i$ et $\pi_{u_{\ker P^{i+1}(u)}} = P^{i+1}$, d'après la proposition 18. Nécessairement, on a $\ker P^i(u) \subsetneq \ker P^{i+1}(u)$. En outre, on a $\pi_{u_{\ker P^{\alpha+1}(u)}} = P^\alpha$, donc $P^\alpha(u)$ est nul sur $\ker P^{\alpha+1}(u)$, d'où l'égalité $\ker P^{\alpha+1}(u) = \ker P^\alpha(u)$. □

4.2. Application à la décomposition de Dunford.

THÉORÈME 11 (Décomposition de Dunford). *On suppose π_u scindé. Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que d est diagonalisable, n est nilpotent, $dn = nd$ et $u = d + n$. En outre, d et n sont des polynômes en u.*

REMARQUE 12. En étudiant une réduction commune à d et n (d et n commutent), on obtient la réduction de Jordan de u.

DÉMONSTRATION. On a $\pi_u = \prod_{i=1}^r (X-\lambda_i)^{\alpha_i}$. Alors $E = \bigoplus_{i=1}^r \ker(u-\lambda_i \operatorname{Id})^{\alpha_i}$. On introduit $\pi_1, \dots, \pi_r$ les projecteurs associés à cette décomposition. Pour tout i, on définit d_i et n_i de la sorte :

$$u_{\ker(u-\lambda_i \operatorname{Id})^{\alpha_i}} = \underbrace{\lambda_i \operatorname{Id}_{\ker(u-\lambda_i \operatorname{Id})^{\alpha_i}}}_{d_i} + \underbrace{(u-\lambda_i \operatorname{Id})_{\ker(u-\lambda_i \operatorname{Id})^{\alpha_i}}}_{n_i}$$

On remarque que n_i est bien nilpotent, puisque $n_i^{\alpha_i} = 0$. On a finalement

$$u = \underbrace{\sum_{i=1}^r \lambda_i \pi_i}_{d} + \underbrace{\sum_{i=1}^r (u-\lambda_i \operatorname{Id})\pi_i}_{n}$$

On peut aisément montrer que d est diagonalisable, que n est nilpotent et que d et n commutent. Comme pour tout i, $\pi_i \in \mathbb{K}[u]$, alors d et n appartiennent à $\mathbb{K}[u]$.

Traitons l'unicité. On suppose avoir aussi $u = d' + n'$ avec d' diagonalisable, n' nilpotent, $d'n' = n'd'$. On sait donc que d' et n' commutent avec u, donc avec d et n qui sont des polynômes en u.

On a $d' - d = n' - n$. D'une part, $d' - d$ est diagonalisable, car deux endomorphismes diagonalisables qui commutent ont une base commune de diagonalisation. D'autre part, $n' - n$ est nilpotent, car n et n' sont nilpotents et commutent. On a donc un morphisme à la fois diagonalisable et nilpotent, il est nécessairement nul. □

COROLLAIRE 10. *Soit $M \in \mathrm{M}_n(\mathbb{R})$. M admet une décomposition de Dunford (D,N) dans $\mathrm{M}_n(\mathbb{C})$. On a en outre $D, N \in \mathrm{M}_n(\mathbb{R})$.*

DÉMONSTRATION. $\mathbb{C}$ est algébriquement clos, donc le polynôme minimal de M est scindé. Donc, il existe un unique couple $(D,N) \in \mathrm{M}_n(\mathbb{C})^2$ tel que $M = D + N$, D diagonalisable, N nilpotente et $DN = ND$. M est réelle, donc $M = \overline{M}$. Donc $M = \overline{D} + \overline{N}$, avec $\overline{D}$ diagonalisable, $\overline{N}$ nilpotente et $\overline{D}\,\overline{N} = \overline{N}\,\overline{D}$. Par unicité, on a $D = \overline{D}$ et $N = \overline{N}$. Donc D et N sont réelles.

Attention ! D n'est pas nécessairement diagonalisable dans $\mathrm{M}_n(\mathbb{R})$. □

5. Invariants de similitude

Soit $u \in \mathcal{L}(E)$.

5.1. Résultats préliminaires.

PROPOSITION 25. *Il existe un sous-espace u-cyclique F de E tel que $\pi_{u_F} = \pi_u$.*

La démonstration de cette proposition nécessite plusieurs lemmes. Le lecteur remarquera qu'elle est très similaire à la démonstration du fait que, dans un groupe abélien, il existe un élément d'ordre l'exposant du groupe.

LEMME 12. *Supposons $\pi_u = P^\alpha$, avec P irréductible. Alors il existe un sous-espace u-cyclique F tel que $\pi_{u_F} = \pi_u$.*

DÉMONSTRATION. On a $\{0\} \subsetneq \ker P(u) \subsetneq \ldots \subsetneq \ker P^\alpha(u) = E$. On prend $x \in E \backslash \ker P^{\alpha-1}(u)$. Alors, si $F =< x >_u$, $\pi_{u_F} = P^\alpha$ (car π_{u_F} divise P^α et car $P^{\alpha-1}(u)(x) \neq 0$). □

LEMME 13. *Soient x et y tels que les polynômes $\pi_{u_{<x>_u}}$ et $\pi_{u_{<y>_u}}$ soient premiers entre eux. Alors $\pi_{u_{<x+y>_u}} = \pi_{u_{<x>_u}} \pi_{u_{<y>_u}}$.*

DÉMONSTRATION. Posons $P = \pi_{u_{<x>_u}}$ et $Q = \pi_{u_{<y>_u}}$. On a $P(u)(x) = 0$ et $Q(u)(y) = 0$, donc $PQ(u)(x) = 0$ et $PQ(u)(y) = 0$, puis $PQ(u)(x+y) = 0$. On pose $R = \pi_{u_{<x+y>_u}}$. Alors $R|PQ$.

En écrivant $x = (x+y) - y$, on peut montrer que $P|QR$. On a $P \wedge Q = 1$. D'après le lemme de Gauss, on a $P|R$. De même, on peut montrer que $Q|R$. Donc $PQ = P \vee Q|R$. □

DÉMONSTRATION. (proposition 25) On écrit $\pi_u = \prod_{i=1}^r P_i^{\alpha_i}$, où les P_i sont irréductibles. Pour tout i, il existe $x_i \in E$ tel que $\pi_{u_{<x_i>_u}} = P_i^{\alpha_i}$. On a $\pi_{u_{<\sum_i x_i>_u}} = \pi_u$. □

5.2. Invariants de similitude et réduction de Frobenius.

THÉORÈME 12 (Réduction de Frobenius). *Soit $u \in \mathcal{L}(E)$. Il existe un unique entier r et une unique famille de polynômes unitaires $Q_1, \ldots, Q_r$ soumis à la condition $Q_r| \ldots |Q_1$ tels que u admette pour matrice*

$$\begin{pmatrix} \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix}$$

REMARQUES 5. C'est la famille de polynômes qui est unique, pas la matrice. Il y a plusieurs bases possibles qui permettent d'obtenir une telle matrice.

Deux endomorphismes u et v sont semblables si et seulement si ils ont le même ensemble de matrices. Donc u et v sont semblables si et seulement si ils correspondent, via ce théorème, à la même famille de polynômes.

DÉFINITION 20. Les polynômes $Q_1, \ldots, Q_r$ sont appelés les *invariants de similitude* de u.

PROPOSITION 26. *On a $\pi_u = Q_1$ et $\chi_u = \prod_{i=1}^r Q_i$.*

DÉMONSTRATION. D'après le théorème 12, on peut écrire

$$E = \bigoplus_{i=1}^r F_i$$

avec F_i u-stable et U_{F_i} admet $\mathcal{C}(Q_i)$ comme matrice. D'après la proposition 22, F_i est u-cyclique et $\chi_{u_{F_i}} = \pi_{u_{F_i}} = Q_i$. On a alors

$$\pi_u = \bigvee_{i=1}^r \pi_{u_{F_i}} = \bigvee_{i=1}^r Q_i = Q_1$$

et

$$\chi_u = \prod_{i=1}^{r} \pi_{u_{F_i}} = \prod_{i=1}^{r} Q_i$$

□

COROLLAIRE 11. *$\pi_u|\chi_u|(\pi_u)^r$, donc π_u et χ_u ont les mêmes diviseurs irréductibles.*

DÉMONSTRATION. (théorème 12) L'existence se démontre par récurrence sur n. D'abord, la proposition 25 assure qu'il existe un sous-espace u-cyclique F_1 tel que $\pi_{u_{F_1}} = \pi_u$.

La preuve consiste en le fait d'exhiber un supplémentaire u-stable de F_1. Soit x un u-générateur de F_1. Soit $d_1 = \dim F_1$. Alors $(x, u(x), \ldots, u^{d_1-1}(x))$ est une base de F_1. Il existe donc une forme linéaire λ telle que

$$\begin{cases} \lambda(x) = \ldots = \lambda(u^{d_1-2}(x)) = 0 \\ \lambda(u^{d_1-1}(x)) = 1 \end{cases}$$

Posons $G =< \lambda >^\circ_{{}^t u}$, l'orthogonal de $< \lambda >_{{}^t u}$, où ${}^t u$ est l'endomorphisme transposé de u défini par

$$\begin{array}{rcl} {}^t u : E^* & \to & E^* \\ \lambda & \mapsto & \lambda \circ u \end{array}$$

Montrons que G est un supplémentaire u-stable de F_1.

Montrons que G est u-stable. Soit $y \in G$. Pour tout i, on a $\lambda \circ u^i(y) = 0$. Donc, pour tout i, on a $\lambda \circ u^i(u(y)) = 0$. D'où $u(y) \in G$.

Montrons que $F_1 \cap G = \{0\}$. Soit $y \in F_1 \cap G$. On peut écrire $y = \alpha_0 x + \alpha_1 u(x) + \ldots + \alpha_{d_1-1} u^{d_1-1}(x)$. On suppose que $\forall k > j$, $\alpha_k = 0$. On a $0 = \lambda \circ u^{d_1-1-j}(y) = \lambda(\alpha_0 u^{d_1-1-j}(x) + \alpha_1 u^{d_1-j}(x) + \ldots + \alpha_j u^{d_1-1}(x)) = \alpha_j$. On en déduit que $\alpha_0 = \ldots = \alpha_{d_1} = 0$, *i.e.* $y = 0$.

Montrons que $\dim G = \operatorname{codim} F_1$. On sait déjà que $\dim G \leqslant \operatorname{codim} F_1$. On a $G =< \lambda >^\circ_{{}^t u}$, donc $\dim G = \operatorname{codim} < \lambda >_{{}^t u}$ (car $\dim F + \dim F^\circ = \dim E$). Or $\dim < \lambda >_{{}^t u} = \deg \pi_{{}^t u_{<\lambda>_{{}^t u}}} \leqslant \deg \pi_{{}^t u} = \deg \pi_u = \dim F_1$, car $\pi_{{}^t u} = \pi_u$.

Nota bene : L'application

$$\begin{array}{rcl} \mathcal{L}(E) & \to & \mathcal{L}(E^*) \\ u & \mapsto & {}^t u \end{array}$$

est un anti-isomorphisme d'algèbres (${}^t(v \circ u) = {}^t u \circ {}^t v$). Pour tout $P \in \mathbb{K}[X]$, on a $P({}^t u) = {}^t P(u)$. On en déduit que u et ${}^t u$ ont le même idéal annulateur, donc le même polynôme minimal.

On en déduit que $\dim G \geqslant \operatorname{codim} F_1$.

Une fois G construit, on applique l'hypothèse de récurrence à u_G : on a $Q_r|\ldots|Q_2$ et u_G admet pour matrice

$$\begin{pmatrix} \mathcal{C}(Q_2) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix}$$

Comme $E = F_1 \oplus G$, u admet pour matrice

$$\begin{pmatrix} \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix}$$

Comme $Q_2 = \pi_{u_G}$ et $Q_1 = \pi_u$, on a aussi $Q_2|Q_1$.

Reste à démontrer l'unicité de la famille $Q_1, \ldots, Q_r$ (voir [8]). On suppose avoir deux familles $Q_r|\ldots|Q_1$ et $R_s|\ldots|R_1$ telles que $E = F_1 \oplus \ldots \oplus F_r$ et $E =$

$G_1 \oplus \ldots \oplus G_s$, où chaque F_i est un sous-espace u-cyclique tel que $\pi_{u_{F_i}} = Q_i$ et chaque G_j est un sous-espace u-cyclique tel que $\pi_{u_{G_j}} = R_j$.

On sait déjà que $\pi_u = Q_1$ et $\pi_u = R_1$. Donc $Q_1 = R_1$.

La suite de notre démonstration nécessite un lemme.

LEMME 14. *Soit F un sous-espace u-cyclique. Soit $Q \in \mathbb{K}[X]$. Alors $Q(u)(F)$ est encore un sous-espace u-cyclique et*

$$\pi_{u_{Q(u)(F)}} = \frac{\pi_{u_F}}{\pi_{u_F} \wedge Q}$$

DÉMONSTRATION. Soit x tel que $F =< x >_u$. On a $F = \{P(u)(x), P \in \mathbb{K}[X]\}$, donc $Q(u)(F) = \{Q(u)(P(u)(x)), P \in \mathbb{K}[X]\} = \{P(u)(Q(u)(x)), P \in \mathbb{K}[X]\}$. D'où $Q(u)(F) =< Q(u)(x) >_u$. $Q(u)(F)$ est donc u-cyclique.

Soit $P \in \mathbb{K}[X]$. On a

$$\begin{array}{rcl}
P(u_{Q(u)(F)}) = 0 & \iff & P(u)(Q(u)(F)) = 0 \\
& \iff & P(u)(Q(u)(x)) = 0 \\
& \iff & PQ(u)(x) = 0 \\
& \iff & PQ(u(F)) = 0 \\
& \iff & PQ(u_F) = 0 \\
& \iff & \pi_{u_F} | PQ \\
& \iff & \frac{\pi_{u_F}}{\pi_{u_F} \wedge Q} \left| \frac{PQ}{\pi_{u_F} \wedge Q} \right. \\
& \iff & \frac{\pi_{u_F}}{\pi_{u_F} \wedge Q} | P
\end{array}$$

La dernière équivalence fait appel au théorème de Gauss. □

Reprenons la preuve du théorème. On démontre l'unicité par récurrence sur i. L'hypothèse de récurrence sera $\forall j \leqslant i, Q_j = R_j$.

On applique $Q_i(u)$ aux deux décompositions $E = F_1 \oplus \ldots \oplus F_r$ et $E = G_1 \oplus \ldots \oplus G_s$. Comme tous les sous-espaces sont u-stables, on a $Q_i(u)(E) = Q_i(u)(F_1) \oplus \ldots \oplus Q_i(u)(F_{i-1})$ (car pour $j \geqslant i$, $Q_j | Q_i$ donc $Q_i(u)(F_j) = 0$) et $Q_i(u)(E) = Q_i(u)(G_1) \oplus \ldots \oplus Q_i(u)(G_s)$.

D'après le lemme et l'hypothèse de récurrence, pour tout $\ell < i$, le polynôme minimal des restrictions de u à $Q_i(u)(F_\ell)$ et $Q_i(u)(G_\ell)$ est le même (c'est $\frac{Q_\ell}{Q_i}$). Ce sont des sous-espaces u-cycliques, donc en particulier, ils ont la même dimension.

Alors $\dim Q_i(u)(E) = \sum_{l=1}^{i-1} \dim Q_i(u)(F_l) = \sum_{\ell=1}^{i-1} \dim Q_i(u)(G_\ell)$, ce qui impose $\bigoplus_{j \geqslant i} Q_i(u)(G_j) = \{0\}$. Donc $Q_i(u)(G_i) = \{0\}$, puis $R_i | Q_i$. Par symétrie, on obtient l'égalité. □

5.3. Réduction de Jordan et autres applications.

5.3.1. *Cas particulier d'un endomorphisme nilpotent.* u est nilpotent si et seulement si $\pi_u = X^d$, où d est l'indice de nilpotence de u. Le théorème 12 assure qu'il existe un unique entier r et une unique famille de polynômes $Q_r | \ldots | Q_1$ tels que u admette pour matrice

$$\begin{pmatrix} \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix}$$

On a $Q_1 = \pi_u = X^d$ donc pour tout i, $Q_i = X^{d_i}$, avec $d_1 = d$ et $d_1 \geqslant \ldots \geqslant d_r$. Or la matrice compagnon associée au polynôme X^{d_i} est

$$\begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \begin{matrix} \uparrow \\ \vdots \\ d_i \\ \vdots \\ \downarrow \end{matrix}$$

On appelle une telle matrice bloc de Jordan et on la note $J(0, d_i)$. Réciproquement, un bloc de Jordan de valeur propre nulle est une matrice compagnon associée à une puissance de X.

Pour un endomorphisme u nilpotent, le théorème 12 est équivalent au théorème donnant la réduction de Jordan de u. On en déduit, grâce au lemme des noyaux, le théorème de jordanisation dans le cas où π_u est scindé.

THÉORÈME 13 (Réduction de Jordan). *On suppose π_u scindé. Alors, dans une certaine base, u a pour matrice une matrice diagonale par blocs formée de blocs de Jordan*

$$J(\lambda, d) = \begin{pmatrix} \lambda & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix} \begin{matrix} \uparrow \\ \vdots \\ d \\ \vdots \\ \downarrow \end{matrix}$$

DÉMONSTRATION. Donnons une démonstration rapide de ce résultat. Notons $\pi_u = \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i}$. Alors $E = \bigoplus_{i=1}^{r} \ker(u - \lambda_i \operatorname{Id})^{\alpha_i}$. Sur chaque $F_i = \ker(u - \lambda_i \operatorname{Id})^{\alpha_i}$, l'endomorphisme $u_{F_i} - \lambda_i \operatorname{Id}_{F_i}$ est nilpotent. Il existe donc une base de F_i dans laquelle il a pour matrice une matrice diagonale par blocs formée de blocs de Jordan $J(0, d_{i,j})$. Dans cette même base, la matrice de u est donc la matrice diagonale par blocs formée des blocs de Jordan $J(\lambda_i, d_{i,j})$. D'où le résultat. □

5.3.2. *En guise de réciproque.* Supposons que l'on connaisse la réduction de Jordan d'un endomorphisme. Comment calculer ses invariants de similitude ?

On note $\lambda_1, \ldots, \lambda_s$ les valeurs propres de u. Pour chaque λ_i, on note $d_{i,1} \geqslant \ldots \geqslant d_{i,r_i}$ les tailles des r_i blocs de Jordan de diagonale λ_i. La matrice considérée est la matrice diagonale par blocs suivante

$$\begin{pmatrix} J(\lambda_1, d_{1,1}) & & & & & & & \\ & \ddots & & & & & 0 & \\ & & J(\lambda_1, d_{1,r_1}) & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & & J(\lambda_s, d_{s,1}) & & \\ & 0 & & & & & \ddots & \\ & & & & & & & J(\lambda_s, d_{s,r_s}) \end{pmatrix}$$

On remarque alors que

$$Q_1 = \pi_u = \bigvee_{i=1}^{s} \pi_{u_{\ker(X-\lambda_i)^{d_{i,1}}}} = \prod_{i=1}^{s} (X - \lambda_i)^{d_{i,1}}$$

Un bloc de Jordan correspond à un sous-espace cyclique engendré par le premier vecteur colonne. Donc, pour tout i, il existe x_i tel que le bloc de Jordan $J(\lambda_i, d_{i,1})$ corresponde au sous-espace $< x_i >_u$. Alors, en posant $F =< x_1 + \ldots + x_s >_u$, F est un sous-espace cyclique correspondant aux blocs de Jordan $J(\lambda_1, d_{1,1}), \ldots, J(\lambda_s, d_{s,1})$. On a $\pi_{u_F} = Q_1$, donc F correspond aussi à la matrice compagnon associée au polynôme Q_1 (voir la démonstration de la proposition 25). On note G le supplémentaire de F correspondant aux blocs restants. On recommence le processus sur u_G. On obtient

$$Q_2 = \pi_{u_G} = \prod_{r_i \geqslant 2} (X - \lambda_i)^{d_{i,2}}$$

puis

$$Q_3 = \prod_{r_i \geqslant 3} (X - \lambda_i)^{d_{i,3}}$$

etc. On pose $r = \max(r_1, \ldots, r_s)$. La famille construite convient. Par unicité, les polynômes $Q_1, \ldots, Q_s$ sont les invariants de similitude de u.

EXEMPLE 9. Traitons le cas de la matrice

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

En utilisant la méthode exposée précédemment, on montre que les invariants de similitude de cette matrice sont

$$\begin{cases} Q_1 &= X^2(X-1)(X-2)^2 \\ Q_2 &= (X-1)(X-2) \\ Q_3 &= X-2 \end{cases}$$

5.3.3. *Extension du corps de base.* Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps. Soit $M \in \mathrm{M}_n(\mathbb{K}) \subset \mathrm{M}_n(\mathbb{L})$.

PROPOSITION 27. *Les invariants de similitude de M sont les mêmes dans $\mathrm{M}_n(\mathbb{K})$ et dans $\mathrm{M}_n(\mathbb{L})$.*

DÉMONSTRATION. On note $Q_1, \ldots, Q_r$ les invariants de similitude de M dans $\mathrm{M}_n(\mathbb{K})$. Il existe alors $P \in \mathrm{GL}_n(\mathbb{K})$ vérifiant

$$M = P \begin{pmatrix} \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix} P^{-1}$$

Cette égalité reste vraie dans $\mathrm{M}_n(\mathbb{L})$. Par unicité, on en déduit que $Q_1, \ldots, Q_r$ sont les invariants de M dans $\mathrm{M}_n(\mathbb{L})$. □

COROLLAIRE 12. *Soient $M, N \in \mathrm{M}_n(\mathbb{K})$. M et N sont semblables dans $\mathrm{M}_n(\mathbb{K})$ si et seulement si elles sont semblables dans $\mathrm{M}_n(\mathbb{L})$.*

Ce corollaire permet de démontrer un résultat classique.

PROPOSITION 28. *Soit $M \in \mathrm{M}_n(\mathbb{K})$. Alors M et ${}^tM$ sont semblables.*

Nous donnerons deux preuves de ce résultat.

DÉMONSTRATION. (1) Commençons par supposer que M est un bloc de Jordan

$$M = \begin{pmatrix} \lambda & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & \lambda \end{pmatrix} \begin{matrix} \uparrow \\ \vdots \\ n \\ \vdots \\ \downarrow \end{matrix}$$

Alors

$${}^tM = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

Si l'on note $(e_1, \ldots, e_n)$ une base et l'on appelle u l'endomorphisme dont la matrice dans la base $(e_1, \ldots, e_n)$ est M. Dans la base $(e_n, \ldots, e_1)$, la matrice de u est ${}^tM$. M et ${}^tM$ sont donc semblables.

Supposons π_M scindé. La matrice M admet une réduite de Jordan : il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que

$$M = P \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix} P^{-1}$$

On a

$${}^tM = {}^tP^{-1} \begin{pmatrix} {}^tJ_1 & & 0 \\ & \ddots & \\ 0 & & {}^tJ_s \end{pmatrix} {}^tP$$

Or pour tout i, il existe Q_i inversible telle que ${}^tJ_i = Q_i J_i Q_i^{-1}$. Donc, on a

$${}^tM = {}^tP^{-1} \underbrace{\begin{pmatrix} Q_1 & & 0 \\ & \ddots & \\ 0 & & Q_s \end{pmatrix}}_{Q} \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix} \underbrace{\begin{pmatrix} Q_1^{-1} & & 0 \\ & \ddots & \\ 0 & & Q_s^{-1} \end{pmatrix}}_{Q^{-1}} {}^tP$$

Finalement,

$${}^tM = \underbrace{{}^tP^{-1}QP^{-1}}_{S^{-1}} \underbrace{P \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix} P^{-1}}_{M} \underbrace{PQ^{-1}\,{}^tP}_{S}$$

Plaçons-nous dans le cas général. On considère une extension de $\mathbb{K}$ dans laquelle π_M est scindé. On est ramené au cas précédent. □

DÉMONSTRATION. (2) Tout part de la remarque suivante : E est u-cyclique si et seulement si $\pi_u = \chi_u$. Soit Q un polynôme unitaire de degré n. La matrice compagnon $\mathcal{C}(Q)$ vérifie alors $\pi_{\mathcal{C}(Q)} = \chi_{\mathcal{C}(Q)}$. Comme $\mathcal{C}(Q)$ et sa transposée ont des polynômes caractéristiques et minimaux égaux, on a $\pi_{{}^t\mathcal{C}(Q)} = \chi_{{}^t\mathcal{C}(Q)}$. Donc E est ${}^t\mathcal{C}(Q)$-cyclique. ${}^t\mathcal{C}(Q)$ est donc semblable à la matrice compagnon associée à son polynôme minimal, c'est-à-dire Q. De cette propriété découle le résultat. □

6. Endomorphismes semi-simples

6.1. Généralités.

DÉFINITION 21. Soit $u \in \mathcal{L}(E)$. On dit que u est *simple* si les seuls sous-espaces vectoriels u-stables sont triviaux (*i.e.* sont soit $\{0\}$, soit E tout entier).

EXEMPLE 10. Si $\dim E = 1$, tout endomorphisme de E est simple.

PROPOSITION 29. *Soit $u \in \mathcal{L}(E)$. u est simple si et seulement si E est u-cyclique et π_u est irréductible.*

DÉMONSTRATION. ($\Rightarrow$) Soit $y \in E\backslash\{0\}$. $< y >_u \supsetneq \{0\}$ donc $< y >_u = E$. E est donc u-cyclique.

Soit P un diviseur irréductible de π_u. Alors $\ker P(u)$ est un sous-espace vectoriel u-stable non nul. C'est donc E. Donc $\pi_u | P$, puis $P = \pi_u$ à un inversible près.

($\Leftarrow$) Soit F un sous-espace vectoriel u-stable non nul. Soit $y \in F\backslash\{0\}$. Soit $G =< y >_u$. On a $\pi_{u_G} | \pi_u$. Or $G \supsetneq \{0\}$, donc $\deg \pi_{u_G} \geqslant 1$. Par irréductibilité de π_u, on a $\pi_{u_G} = \pi_u$. Comme G est u-cyclique, on a $\dim G = \deg \pi_{u_G} = \deg \pi_u = \dim E$, E étant u-cyclique lui aussi. On a donc $E = G \subset F$. □

COROLLAIRE 13. *Dans le cas où $\mathbb{K}$ est algébriquement clos, s'il existe un endomorphisme simple, E est une droite.*

DÉFINITION 22. Soit $u \in \mathcal{L}(E)$. Un sous-espace vectoriel F est dit *u-simple* si F est non nul, F est u-stable et u_F est simple.

On déduit de la proposition 29 que F est u-simple si et seulement si F est u-cyclique et π_{u_F} est irréductible.

DÉFINITION 23. Soit $u \in \mathcal{L}(E)$. On dit que u est *semi-simple* si E se décompose comme une somme directe de sous-espaces u-simples.

REMARQUE 13. Si $\mathbb{K}$ est algébriquement clos, u est semi-simple si et seulement si il est diagonalisable. En effet, un sous-espace u-simple est une droite propre.

THÉORÈME 14. *Soit $u \in \mathcal{L}(E)$. u est semi-simple si et seulement si tout sous-espace u-stable admet un supplémentaire u-stable.*

DÉMONSTRATION. ($\Rightarrow$) On a $E = F_1 \oplus \ldots \oplus F_r$, avec F_i u-simple. On remarque que si G est un sous-espace stable, soit $F_i \subset G$, soit $F_i + G = F_i \oplus G$ (puisque $F_i \cap G$ est un sous-espace stable inclus dans F_i).

On montre, par récurrence descendante sur $\dim F$ que tout sous-espace vectoriel u-stable F admet un supplémentaire u-stable. Soit F u-stable. Si $\dim F < n$, il existe i tel que F_i ne soit pas inclus dans F. Alors $F_i + F = F_i \oplus F$. On applique l'hypothèse de réucurrence à $F_i \oplus F$.

($\Leftarrow$) Cette partie de la démonstration nécessite un lemme.

LEMME 15. *Tout sous-espace vectoriel u-stable non nul contient un sous-espace vectoriel u-simple.*

DÉMONSTRATION. Soit $F \supsetneq \{0\}$ u-stable. Soit P un diviseur irréductible de π_{u_F}. Soit y un élément non nul de $\ker P(u) \cap F$. Alors $< y >_u$ est un sous-espace u-simple contenu dans F (car $\pi_{u_{<y>_u}} = P$). □

Finissons la preuve du théorème. Soit F un sous-espace vectoriel de dimension maximale parmi ceux qui se décomposent en somme directe de sous-espaces u-simples. Si $F \subsetneq E$, il existe un supplémentaire u-stable G non nul de F. D'après le lemme, G contient un sous-espace u-simple, noté G_0. Alors $F \oplus G_0$ est somme directe de sous-espaces u-simples et $F \oplus G_0 \supsetneq F$, ce qui contredit la définition de F. Donc $F = E$. □

6.2. Polynôme minimal d'un endomorphisme semi-simple.

THÉORÈME 15. *Soit $u \in \mathcal{L}(E)$. u est semi-simple si et seulement si le polynôme minimal de u n'est pas divisible par le carré d'un polynôme non inversible (*i.e. *la décomposition en irréductibles de π_u est de la forme $\prod_i P_i$, où les P_i sont irréductibles et deux à deux non associés).*

DÉMONSTRATION. ($\Rightarrow$) On suppose u semi-simple. Alors $E = \bigoplus_{i=1}^{r} F_i$, où F_i est u-simple. En particulier, $\pi_{u_{F_i}}$ est irréductible. Alors $\pi_u = \bigvee_{i=1}^{r} \pi_{u_{F_i}} = \prod_{i=1}^{q} P_i$, où les P_i sont distincts et choisis parmi les $\pi_{u_{F_i}}$.

($\Leftarrow$) On suppose que l'on a $\pi_u = \prod_{i=1}^{q} P_i$, où les P_i sont irréductibles et deux à deux non associés. D'après le lemme de décomposition des noyaux, on peut écrire $E = \bigoplus_{i=1}^{q} \ker P_i(u)$. Le polynôme minimal de la restriction de u à $\ker P_i(u)$ est P_i. D'après le théorème 12, $\ker P_i(u)$ se décompose en somme directe de sous-espaces u-cycliques : $\ker P_i(u) = \bigoplus_{j=1}^{r_i} F_{i,j}$. Comme P_i est irréductible, $\pi_{u_{F_{i,j}}} = P_i$. Donc $F_{i,j}$ est u-simple.

REMARQUE 14. Si l'on connait la théorie des modules sur les anneaux principaux, on peut montrer que $\ker P_i(u)$ est un $\mathbb{K}[X]/(P_i)$-espace vectoriel. En choisissant une base, on montre qu'il existe une décomposition $\ker P_i(u) = \bigoplus_j F_{i,j}$, avec les $F_{i,j}$ u-simples, *i.e.* les $F_{i,j}$ sont des $\mathbb{K}[X]/(P_i)$-droites.

□

COROLLAIRE 14. *Soit $M \in \mathrm{M}_n(\mathbb{K})$. Soit $\mathbb{L}$ une extension de $\mathbb{K}$ dans laquelle π_M est scindé. Si M est diagonalisable dans $\mathrm{M}_n(\mathbb{L})$, alors M est semi-simple sur $\mathbb{K}$. La réciproque est vraie si l'extension $\mathbb{K} \subset \mathbb{L}$ est séparable.*

DÉMONSTRATION. Si M est diagonalisable dans $\mathrm{M}_n(\mathbb{L})$, alors son polynôme minimal n'a que des racines simples. Donc ce polynôme ne peut être divisible par un carré non inversible dans $\mathbb{K}[X]$ (on utilise ici le fait que π_M est le même sur $\mathbb{K}$ et sur $\mathbb{L}$).

Réciproquement, si M est semi-simple sur $\mathbb{K}$, on a $\pi_M = P_1 \dots P_q$, où les P_i sont des irréductibles non associés deux à deux. Dans une extension $\mathbb{L}$ de $\mathbb{K}$ où π_M est scindé, P_i et P_j ne peuvent avoir une racine commune si $i \neq j$ (on peut invoquer le fait que P_i et P_j ont le même *pgcd* dans $\mathbb{K}$ et dans $\mathbb{L}$). Si l'extension est séparable, on a de plus que chaque P_i n'a que des racines simples. □

COROLLAIRE 15. *Si u est semi-simple, pour tout sous-espace vectoriel F u-stable, u_F est semi-simple.*

DÉMONSTRATION. $\pi_{u_F} \mid \pi_u$. □

REMARQUE 15. Si u est semi-simple, on décompose π_u en produit d'irréductibles $\pi_u = P_1 \dots P_q$. Alors $E = \bigoplus_{i=1}^{q} \ker P_i(u)$. Si F est u-stable, le lemme de décomposition des noyaux appliqué à u_F donne

$$F = \bigoplus_{i=1}^{q} \ker P_i(u_F) = \bigoplus_{i=1}^{q} (\ker P_i(u) \cap F)$$

Si en outre u est diagonalisable, pour tout i, on a $P_i = X - \lambda_i$. Tout sous-espace vectoriel de $\ker P_i(u)$ étant u-stable, on en déduit que F est u-stable si et seulement si $F = \bigoplus_{i=1}^{q} F_i$, où les F_i sont des sous-espaces vectoriels de $\ker P_i(u)$.

PROPOSITION 30. *Soient u et v deux endomorphismes semi-simples. Alors u et v sont semblables si et seulement si $\chi_u = \chi_v$.*

DÉMONSTRATION. ($\Rightarrow$) C'est vrai même si u et v ne sont pas semi-simples.

($\Leftarrow$) Si on a $\chi_u = \chi_v = \prod_{i=1}^{q} P_i^{\alpha_i}$, où les P_i sont irréductibles deux à deux non associés, alors u et v admettent comme matrice

$$\begin{pmatrix}
\mathcal{C}(P_1) & & \uparrow & & & \\
& \ddots & \alpha_1 \text{ blocs} & & & \\
& \mathcal{C}(P_1) & \downarrow & & & \\
& & \mathcal{C}(P_2) & & \uparrow & \\
& & & \ddots & \alpha_2 \text{ blocs} & \\
& & & \mathcal{C}(P_2) & \downarrow & \\
& & & & \ddots &
\end{pmatrix}$$

Ils sont donc semblables. □

6.3. Lien avec la décomposition de Dunford.

THÉORÈME 16. *On note $\lambda_1, \dots, \lambda_r$ les racines de π_u dans une cloture algébrique de $\mathbb{K}$. On suppose l'extension $\mathbb{K} \subset \mathbb{K}(\lambda_1, \dots, \lambda_r)$ séparable. Même si π_u n'est pas scindé et si l'on ne dispose pas de $\lambda_1, \dots, \lambda_r$, on peut donner d semi-simple et n nilpotent dans $\mathbb{K}[u]$ tels que $u = d + n$ et $dn = nd$.*

DÉMONSTRATION. On note $\pi_u = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, où les P_i sont des polynômes irréductibles unitaires disctincts. On pose $Q = P_1 \dots P_r$ (en pratique, on peut calculer Q sans connaitre les P_i, puisque $Q = \frac{P}{P \wedge P'}$). On pose $s = \max(\alpha_1, \dots, \alpha_r)$. Comme $\pi_u \mid Q^s$, on a $Q(u)^s = 0$. $Q'(u)$ est inversible, puisque que $Q' \wedge \pi_u = 1$ (par séparabilité de l'extension considérée).

On pose (ce qui n'est pas sans rappeler la méthode de Newton)

$$\left\{ \begin{array}{rcl} x_0 & = & u \\ x_{n+1} & = & x_n - \frac{Q(x_n)}{Q'(x_n)} \end{array} \right.$$

On va montrer par récurrence que cette suite est bien définie et que pour tout n, $Q(x_n) \in (Q(u)^{2^n})$. Le résultat est immédiat au rang 0. On le suppose vrai au rang n. Q' étant un polynôme, on a $Q'(x_{n+1}) - Q'(x_n) \in (x_{n+1} - x_n)$. Par définition de x_{n+1}, on a $x_{n+1} - x_n \in (Q(x_n))$. Donc $Q'(x_{n+1}) = Q'(x_n) + Q(x_n)v$, avec $v \in \mathbb{K}[u]$, est nilpotent, puisque somme d'un élément inversible et d'un élément nilpotent. En outre,

$$Q(x_{n+1}) = Q\left(x_n - \frac{Q(x_n)}{Q'(x_n)}\right) = \underbrace{Q(x_n) - \frac{Q(x_n)}{Q'(x_n)} Q'(x_n)}_{=0} + \left(\frac{Q(x_n)}{Q'(x_n)}\right)^2 w \in (Q(x_n)^2)$$

D'où le résultat au rang $n+1$.

$Q(x_n) \in (Q(u)^{2^n})$ et $Q(u)^s = 0$, donc pour n tel que $2^n \geqslant s$, $Q(x_n) = 0$. On note $d = x_{\lfloor \frac{\log r}{\log 2} \rfloor + 1} \in \mathbb{K}[u]$. On a $Q(d) = 0$, donc $\pi_d \mid Q$ est sans facteur carré, donc d est semi-simple. On pose $n = u - d \in \mathbb{K}[u]$. n est nilpotent :

$$n = x_0 - x_{\lfloor \frac{\log r}{\log 2} \rfloor + 1} = \sum_{i=0}^{\lfloor \frac{\log r}{\log 2} \rfloor} \underbrace{(x_i - x_{i+1})}_{\in (Q(x_i)) \Rightarrow \text{ nilpotent}}$$

Enfin, comme d et n sont des polynômes en u, ils commutent. □

7. Réduction des endomorphismes normaux

7.1. Définitions. Dans cette partie, $\mathbb{K}$ est le corps $\mathbb{R}$ ou $\mathbb{C}$. E désigne un $\mathbb{R}$-espace vectoriel euclidien ou un $\mathbb{C}$-espace vectoriel hermitien. On note $< .,. >$ le produit scalaire.

Soit $u \in \mathcal{L}(E)$. On rappelle qu'il existe un unique endomorphisme de E, appelé adjoint de u et noté u^* vérifiant $\forall x, y \in E, < u(x), y >=< x, u^*(y) >$. Si $\mathcal{B} = (e_1, \ldots, e_n)$ désigne une base orthonormée de E et si l'on définit la famille $(a_{i,j})$ par $u(e_i) = \sum_j a_{i,j} e_j$, alors $a_{i,j} =< u(e_i), e_j >=< e_i, u^*(e_j) >$. On en déduit que la matrice de u^* dans la base $\mathcal{B}$, *i.e.* l'adjointe de la matrice M de u sur $\mathcal{B}$, est $M^* = {}^t\bar{M}$.

Définition 24. Un endomorphisme u est dit *normal* si $uu^* = u^*u$.

Exemples 1.
- Si $u = u^*$, on dit que u est auto-adjoint. Dans le cas réel, il est dit symétrique. Dans le cas complexe, il est dit hermitien.
- Si $u = -u^*$, on dit, dans le cas réel, que u est antisymétrique et, dans le cas complexe, que u est antihermitien.
- Si $u^* = u^{-1}$, on dit, dans le cas réel, que u est orthogonal et, dans le cas complexe, que u est unitaire.

7.2. Réduction.

Proposition 31. *Soit u un endomorphisme normal. Soit F un sous-espace u-stable. Alors $F^\perp$ est u-stable. En outre, u_F est un endomorphisme normal de F est $(u_F)^* = (u^*)_F$.*

Remarque 16. On a $E = F \oplus F^\perp$. Donc, F admet un supplémentaire u-stable : son orthogonal. En particulier, u est semi-simple.

Démonstration. $E = F \oplus F^\perp$. Sur une base orthonormée adaptée à cette décomposition, la matrice de u s'écrit

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \begin{matrix} \}F \\ \}F^\perp \end{matrix}$$

Comme cette base est orthonormée, la matrice de u^* est

$$M^* = \begin{pmatrix} A^* & 0 \\ B^* & C^* \end{pmatrix}$$

Comme $uu^* = u^*u$, on a $MM^* = M^*M$. Or

$$MM^* = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \begin{pmatrix} A^* & 0 \\ B^* & C^* \end{pmatrix} = \begin{pmatrix} AA^* + BB^* & BC^* \\ CB^* & CC^* \end{pmatrix}$$

et

$$M^*M = \begin{pmatrix} A^* & 0 \\ B^* & C^* \end{pmatrix} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \begin{pmatrix} A^*A & A^*B \\ B^*A & B^*B + C^*C \end{pmatrix}$$

On a donc $AA^* + BB^* = A^*A$, puis en prenant la trace, $\mathrm{Tr}(BB^*) = 0$, d'où $B = 0$. On a aussi $A^*A = AA^*$ et $C^*C = CC^*$. On en déduit donc que $F^\perp$ est u-stable (car $B = 0$), que $(u_F)^* = (u^*)_F$ et que u_F est normal (car $A^*A = AA^*$). □

Théorème 17. *Soit $u \in \mathcal{L}(E)$. u est normal si et seulement si il admet sur une base* orthonormée *une matrice de la forme :*

- *si $\mathbb{K} = \mathbb{C}$,*

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

– *si* $\mathbb{K} = \mathbb{R}$,

$$\begin{pmatrix} \lambda_1 & & & & & & & \\ & \ddots & & & & & 0 & \\ & & \lambda_r & & & & & \\ & & & a_1 & -b_1 & & & \\ & & & b_1 & a_1 & & & \\ & & & & & \ddots & & \\ & 0 & & & & & a_s & -b_s \\ & & & & & & b_s & a_s \end{pmatrix}$$

DÉMONSTRATION. On suppose $\mathbb{K} = \mathbb{C}$. ($\Leftarrow$) u est normal si et seulement si sa matrice dans une base orthonormée est normale. On constate qu'une matrice diagonale est normale. On en déduit que u est normal.

($\Rightarrow$) Soit e un vecteur propre normé de u. On a $E = \mathbb{C}e \oplus (\mathbb{C}e)^\perp$ et on sait que $u_{(\mathbb{C}e)^\perp}$ est un endomorphisme normal. On conclut par récurrence sur $\dim E$.

On suppose $\mathbb{K} = \mathbb{R}$. ($\Leftarrow$) Une matrice diagonale est normale et une matrice de similitude directe aussi, puisque

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix}$$

et

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix}$$

($\Rightarrow$) Cette partie de la démonstration nécessite quelques lemmes.

LEMME 16. *Soit u un endomorphisme d'un $\mathbb{R}$-espace vectoriel euclidien E. Alors u admet une droite stable ou un plan stable.*

DÉMONSTRATION. Si π_u admet une racine réelle, alors u admet une droite stable.

Sinon, π_u admet un diviseur irréductible de degré 2. Soit P un tel diviseur. Alors pour tous $x \in \ker P(u)\backslash\{0\}$, $< x >_u$ est un sous-espace u-cyclique sur lequel le polynôme minimal de u est P, c'est donc un plan. □

On remarque que si l'on est capable de majorer le degré des irréductibles, on peut majorer la dimension des sous-espaces stables.

LEMME 17. *Soit* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$. *$M$ est normale si et seulement si soit $b = c$ (dans ce cas, M est diagonalisable), soit $b = -c$ et $a = d$.*

DÉMONSTRATION. Calculons

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}$$

et

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix}$$

Donc M est normale si et seulement si

$$\begin{cases} b^2 &= c^2 \\ (a-d)(b-c) &= 0 \end{cases}$$

si et seulement si

$$b = c \text{ ou } \begin{cases} b &= -c \\ a &= d \end{cases}$$

Dans le cas où $b = c$, on a $\chi_M = X^2 - (a+d)X + ad - b^2$. Le discriminant s'écrit $\Delta = (a-d)^2 + 4b^2 > 0$, sauf si $a = d$ et $b = 0$, qui constitue un cas trivial. M est donc diagonalisable. □

REMARQUE 17. Un endomorphisme symétrique admet donc une valeur propre. On peut en déduire, par récurrence, qu'un tel endomorphisme est diagonalisable.

Montrons le résultat par récurrence sur $\dim E$.

Si u admet une valeur propre réelle, on note e un vecteur propre normé de u associé à cette valeur propre. On a $E = \mathbb{R}e \oplus (\mathbb{R}e)^\perp$. On sait alors que $u_{(\mathbb{R}e)^\perp}$ est normal et on lui applique l'hypothèse de récurrence.

Sinon, u admet un plan stable $\mathcal{P}$. u_P est normal et sans valeur propre, donc il admet sur une base orthonormée de P une matrice de la forme

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

On a $E = \mathcal{P} \oplus \mathcal{P}^\perp$. $u_{\mathcal{P}^\perp}$ est normal et on lui applique l'hypothèse de récurrence. □

COROLLAIRE 16 (Etude de cas particuliers). *Du théorème de réduction des endomorphismes normaux, on peut déduire que :*

- *u est hermitien si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ avec } \lambda_j \in \mathbb{R}$$

- *u est antihermitien si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ avec } \lambda_j \in i\mathbb{R}$$

- *u est unitaire si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ avec } |\lambda_j| = 1$$

- *u est symétrique si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \text{ avec } \lambda_j \in \mathbb{R}$$

– *u est antisymétrique si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} 0 & & & & & & & \\ & \ddots & & & & & 0 & \\ & & 0 & & & & & \\ & & & 0 & -b_1 & & & \\ & & & b_1 & 0 & & & \\ & & & & & \ddots & & \\ & 0 & & & & & 0 & -b_s \\ & & & & & & b_s & 0 \end{pmatrix}, \text{ avec } b_j \neq 0$$

– *u est orthogonal si et seulement si il admet sur une base orthonormée une matrice de la forme*

$$\begin{pmatrix} \pm 1 & & & & & & & \\ & \ddots & & & & & 0 & \\ & & \pm 1 & & & & & \\ & & & a_1 & -b_1 & & & \\ & & & b_1 & a_1 & & & \\ & & & & & \ddots & & \\ & 0 & & & & & a_s & -b_s \\ & & & & & & b_s & a_s \end{pmatrix}, \text{ avec } a_j^2 + b_j^2 = 1$$

REMARQUE 18. Les endomorphismes semi-simples sont tous des endomorphismes normaux pour un certain produit scalaire.

7.3. Applications en topologie.

7.3.1. *Connexité de $\mathrm{U}_n(\mathbb{C})$ et $\mathrm{SO}_n(\mathbb{R})$.* Les résultats énoncés dans cette partie peuvent se retrouver dans [**10**].

PROPOSITION 32. *$\mathrm{U}_n(\mathbb{C})$ est connexe. $\mathrm{O}_n(\mathbb{R})$ a deux composantes connexes : $\mathrm{SO}_n(\mathbb{R})$ et $\mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R})$.*

DÉMONSTRATION. $\mathrm{U}_n(\mathbb{C})$ est connexe par arcs. Si $M \in \mathrm{U}_n(\mathbb{C})$, il existe $P \in \mathrm{U}_n(\mathbb{C})$ et $\theta_1, \ldots, \theta_n$ tels que

$$M = P^* \begin{pmatrix} e^{\imath\theta_1} & & 0 \\ & \ddots & \\ 0 & & e^{\imath\theta_n} \end{pmatrix} P$$

On pose

$$\begin{array}{rcl} \varphi : [0,1] & \to & \mathrm{U}_n(\mathbb{C}) \\ t & \mapsto & P^* \begin{pmatrix} e^{\imath t\theta_1} & & 0 \\ & \ddots & \\ 0 & & e^{\imath t\theta_n} \end{pmatrix} P \end{array}$$

φ est un chemin continu dans $\mathrm{U}_n(\mathbb{C})$ qui relie I_n à M.

$\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs. Si $M \in \mathrm{SO}_n(\mathbb{R})$, il existe $P \in \mathrm{O}_n(\mathbb{R})$, $\theta_1, \ldots, \theta_r$, p et q tels que

$$M = {}^tP \begin{pmatrix} \mathrm{I}_p & & & & 0 \\ & -\mathrm{I}_q & & & \\ & & \cos\theta_1 & -\sin\theta_1 & \\ & & \sin\theta_1 & \cos\theta_1 & \\ 0 & & & & \ddots \end{pmatrix} P$$

Comme $\det M = 1$, q est pair. On peut donc écrire

$$-I_q = \begin{pmatrix} \cos\pi & -\sin\pi & & \\ \sin\pi & \cos\pi & & \\ & & \ddots & \end{pmatrix}$$

Alors il existe $\theta'_1, \ldots, \theta'_{r+\frac{q}{2}}$ tels que

$$M = {}^tP \begin{pmatrix} \mathrm{I}_p & & & 0 \\ & \cos\theta'_1 & -\sin\theta'_1 & \\ & \sin\theta'_1 & \cos\theta'_1 & \\ 0 & & & \ddots \end{pmatrix} P$$

On pose

$$\begin{array}{rcl} \varphi : [0,1] & \to & \mathrm{SO}_n(\mathbb{R}) \\ t & \mapsto & {}^tP \begin{pmatrix} \mathrm{I}_p & & & 0 \\ & \cos(\theta'_1 t) & -\sin(\theta'_1 t) & \\ & \sin(\theta'_1 t) & \cos(\theta'_1 t) & \\ 0 & & & \ddots \end{pmatrix} P \end{array}$$

φ est un chemin continu dans $\mathrm{SO}_n(\mathbb{R})$ qui relie I_n à M.

Si $\sigma \in \mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R})$, alors

$$\begin{array}{rcl} \mathrm{SO}_n(\mathbb{R}) & \to & \mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R}) \\ M & \mapsto & \sigma M \end{array}$$

est un homéomorphisme donc $\mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R})$ est aussi connexe. Comme le déterminant est continu et que $\det \mathrm{SO}_n(\mathbb{R}) = \{1\}$ et $\det \mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R}) = \{-1\}$, $\mathrm{SO}_n(\mathbb{R})$ et $\mathrm{O}_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R})$ ne peuvent être dans un même composante connexe. □

Remarque 19. Dans un groupe topologique, la composante connexe à laquelle appartient 1 est un sous-groupe distingué. Les autres composantes connexes sont les classes modulo ce sous-groupe.

Proposition 33. *$\mathrm{U}_n(\mathbb{C})$ et $\mathrm{O}_n(\mathbb{R})$ sont compacts.*

Démonstration. Celle-ci est laissée en exercice. □

7.3.2. *Décomposition polaire.*

Proposition 34. *On note $\mathrm{S}_n^{++}(\mathbb{R})$ l'ensemble des matrices symétriques définies positives. On a un homéomorphisme*

$$\begin{array}{rcl} \varphi : \mathrm{O}_n(\mathbb{R}) \times \mathrm{S}_n^{++}(\mathbb{R}) & \to & \mathrm{GL}_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array}$$

Démonstration. φ est continue (en tant que restriction de l'application bilinéaire continue $\mathrm{M}_n(\mathbb{R}) \times \mathrm{M}_n(\mathbb{R}) \to \mathrm{M}_n(\mathbb{R}) : (A, B) \mapsto AB$).

Soit $M \in \mathrm{GL}_n(\mathbb{R})$ Supposons que l'on puisse écrire $M = OS$. Alors ${}^tMM = {}^tS\,{}^tOOS = S^2$.

Lemme 18. ${}^tMM \in \mathrm{S}_n^{++}(\mathbb{R})$

Proposition 35. *Soit $N \in \mathrm{S}_n^{++}(\mathbb{R})$. Il existe un unique $S \in \mathrm{S}_n^{++}(\mathbb{R})$ tel que $N = S^2$.*

DÉMONSTRATION. Traitons l'existence de S. Il existe $P \in \mathrm{O}_n(\mathbb{R})$ et $\lambda_1, \dots, \lambda_n > 0$ tels que

$$N = {}^tP \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} P$$

On peut écrire $N = S^2$ avec

$$S = {}^tP \begin{pmatrix} \sqrt{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\lambda_n} \end{pmatrix} P$$

Intéressons-nous maintenant à l'unicité de S.

- *Première méthode.* Si $N = S^2$, on note (λ_i) la famille des valeurs propres de N avec leur multiplicité. D'après le lemme de décomposition des noyaux, on a
$$\ker(N - \lambda_i \mathrm{I}_n) = \ker(S - \sqrt{\lambda_i}\,\mathrm{I}_n) \oplus \underbrace{\ker(S + \sqrt{\lambda_i}\,\mathrm{I}_n)}_{\substack{=\{0\},\text{ sinon } S \text{ aurait} \\ \text{une valeur propre négative}}}$$
Or $E = \bigoplus_i \ker(N - \lambda_i \mathrm{I}_n)$. Donc S est unique.
- *Deuxième méthode.* Il existe un polynôme Q (polynôme d'interpolation de Lagrange) tel que pour tout i, $Q(\lambda_i) = \sqrt{\lambda_i}$. On en déduit que la matrice S construite précédemment vérifie $S = Q(N)$. Soit T une autre solution : $T^2 = N = S^2$. Ainsi S est un polynôme en $N = T^2$, donc S est un polynôme en T. Donc $ST = TS$. On peut alors écrire $(S-T)(S+T) = 0$. $S+T$ est la somme de deux matrices définies positives, donc est définie positive. $S+T$ est donc inversible. Finalement, $S = T$.

□

Revenons à la preuve du théorème. Si $M = OS$, on a $S^2 = {}^tMM$. S est nécessairement l'unique racine carrée définie positive de ${}^tMM$, donc est unique. On pose alors $O = MS^{-1}$. On a ${}^tOO = {}^tS^{-1}\,{}^tMMS^{-1} = S^{-1}S^2S^{-1} = \mathrm{I}_n$. Donc $O \in \mathrm{O}_n(\mathbb{R})$. On a ainsi la bijectivité de φ.

Montrons que φ^{-1} est continue. Soit (M_i) une suite de matrices de $\mathrm{GL}_n(\mathbb{R})$ qui converge vers une matrice $M \in \mathrm{GL}_n(\mathbb{R})$. Soient $M_i = O_iS_i$ et $M = OS$ les décompositions polaires correspondantes.

LEMME 19. *O est l'unique valeur d'adhérence de la suite (O_i).*

DÉMONSTRATION. Soit U une valeur d'adhérence de (O_i). Soit ψ telle que $O_{\psi(i)} \to U$. Comme $M = \lim_i M_i = \lim_i O_iS_i$, on en déduit que $S_{\psi(i)}$ converge vers ${}^tUOS$. Comme $S_{\psi(i)} \in \mathrm{S}_n^{++}(\mathbb{R})$, on a ${}^tUOS \in \mathrm{S}_n^{+}(\mathbb{R})$. Or ${}^tUOS \in \mathrm{GL}_n(\mathbb{R})$, donc ${}^tUOS \in \mathrm{S}_n^{++}(\mathbb{R})$. L'unicité de la décomposition polaire d'une telle matrice montre que ${}^tUO = \mathrm{I}_n$, *i.e.* $U = O$. □

Comme $\mathrm{O}_n(\mathbb{R})$ est compact, on en déduit que la suite (O_i) converge vers O et donc (S_i) converge vers S. □

COROLLAIRE 17. *$\mathrm{GL}_n(\mathbb{R})$ a deux composantes connexes : $\mathrm{GL}_n^+(\mathbb{R}) = \{M : \det M > 0\}$ et $\mathrm{GL}_n^-(\mathbb{R}) = \{M : \det M < 0\}$.*

DÉMONSTRATION. $\mathrm{S}_n^{++}(\mathbb{R})$ est convexe, donc connexe. (On peut même montrer, grâce à l'exponentielle, que $\mathrm{S}_n^{++}(\mathbb{R})$ est homéomorphe à $\mathbb{R}^{\frac{n(n+1)}{2}}$.) □

COROLLAIRE 18. *$\mathrm{O}_n(\mathbb{R})$ est un sous-groupe compact maximal de $\mathrm{GL}_n(\mathbb{R})$.*

DÉMONSTRATION. Soit $G \supset \mathrm{O}_n(\mathbb{R})$ un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. Soit $M \in G$. Soit $M = OS$ sa décomposition polaire. On a $S \in G$. Donc, pour tout i, $S^i \in G$. G est compact donc la suite $(\|S_i\|)$ est bornée et les valeurs propres de S sont $\leqslant 1$. S'il existait une valeur propre < 1, la limite d'une sous-suite convergente de S^i ne serait pas inversible. Donc $S = \mathrm{I}_n$. □

CHAPITRE 4

Modules sur un anneau principal

1. Généralités sur les modules

Soit A un anneau intègre commutatif.

DÉFINITION 25. Un *A-module* est la donnée de $(M, +, \cdot)$ tel que
- $(M, +)$ soit un groupe additif,
- $A \times M \to M$ soit une loi externe

vérifiant
- $\forall a \in A, \forall m, m' \in M, a(m + m') = am + am'$
- $\forall a, a' \in A, \forall m \in M, (aa')m = a(a'm)$
- $\forall a, a' \in A, \forall m \in M, (a + a')m = am + a'm$
- $\forall m \in M, 1m = m$.

Il est élémentaire de définir les notions de sous-module, de A-morphisme, de quotient, de somme directe, de noyau et d'image à partir de ce que l'on connait des espaces vectoriels.

DÉFINITION 26. Soit M un A-module et X une partie de M. Il existe un plus petit sous-module de M qui contient X. Il s'agit de l'intersection de tous les sous-modules de M qui contiennent X. On l'appelle *sous-module engendré par X* et on le note $< X >$.

PROPOSITION 36.

$$< X >= \left\{ \sum_{i=1}^{k} a_i x_i, k \in \mathbb{N}, a_i \in A, x_i \in X \right\}$$

DÉFINITION 27. Si X vérifie $< X >= M$, on dit que X est une *partie génératrice* de M. M est dit de type fini s'il admet une partie génératrice finie.

REMARQUE 20. Un A-module de type fini peut avoir des sous-modules qui ne sont pas de type fini.

EXEMPLE 11. On considère le module $A = A \cdot 1$. Les sous-modules de A sont les idéaux de A et réciproquement.

DÉFINITION 28. Un anneau A est dit *noetherien* si tous ses idéaux sont de type fini.

THÉORÈME 18. *Si A est noetherien, un A-module de type fini a tous ses sous-modules de type fini.*

EXEMPLE 12. Si $\mathbb{K}$ est un corps, $\mathbb{K}[X_i, i \in \mathbb{N}]$ est un anneau non noetherien, puisque l'idéal engendré par $(X_i, i \in \mathbb{N})$ n'est pas de type fini.

DÉFINITION 29.
- Une partie X de M est dite *libre* si pour toute famille presque nulle (λ_x), telle que $\sum_{x \in X} \lambda_x x = 0$, on a pour tout x, $\lambda_x = 0$.
- Si une partie X de M est à la fois libre et génératrice, on dit que c'est une *base* de M.

– On dit que M est un *module libre* si il admet une base. Dans ce cas, si X est une base de M, on obtient un isomorphisme de A-modules

$$\begin{array}{rcl} A^{(X)} & \to & M \\ (\lambda_x)_{x\in X} & \mapsto & \sum_{x\in X} \lambda_x x \end{array}$$

Dans le cas où X est finie, on démontre que toutes les bases ont le même cardinal, que l'on appelle *rang* du module.

DÉMONSTRATION. La démonstration de l'existence du rang est basée sur le théorème suivant.

THÉORÈME 19 (Krull). *Tout anneau unitaire admet un idéal maximal (donc un quotient qui est un corps).*

On suppose avoir deux bases : une de cardinal n et l'autre de cardinal m. On a donc $A^n \simeq A^m$. On note $\mathcal{M}$ un idéal maximal de A. On a donc $A^n/\mathcal{M}A^n \simeq A^m/\mathcal{M}A^m$, puis $(A/\mathcal{M})^n \simeq (A/\mathcal{M})^m$, ce qui impose $n = m$. □

PROPOSITION 37. *Soit X une base de A^n. Les bases de A^n sont les PX avec $P \in \mathrm{GL}_n(A)$, où $\mathrm{GL}_n(A) = \{P \in \mathrm{M}_n(A) : \exists Q \in \mathrm{M}_n(A) : PQ = \mathrm{I}_n\} = \{P \in \mathrm{M}_n(A) : \det P \in A^*\}$.*

DÉMONSTRATION. ($\Rightarrow$) Si P admet une inverse Q dans $\mathrm{M}_n(A)$, $PQ = \mathrm{I}_n$, donc $\det P \det Q = 1$, puis $\det P \in A^*$.
($\Leftarrow$) $P\,{}^tComP = (\det P)\,\mathrm{I}_n$. Si $\det P \in A^*$, P a pour inverse $(\det P)^{-1}\,{}^tComP$ qui appartient à $\mathrm{M}_n(A)$. □

DÉFINITION 30. On suppose A intègre. Un élément $m \in M$ est de *torsion* s'il existe $a \neq 0$ tel que $am = 0$, *i.e.* $\{m\}$ n'est pas libre.
On appelle *sous-module de torsion* de M le sous-ensemble formé par ses éléments de torsion. On le note M_T ou $\mathrm{Tor}\, M$.

DÉMONSTRATION. Soient $m, m' \in M$. Il existe $a \neq 0$ et $a' \neq 0$ tels que $am = 0$ et $a'm' = 0$. On a $aa'(m + m') = 0$ et $aa' \neq 0$. Soit maintenant $b \neq 0$. On a $a(bm) = bam = 0$ et $ba \neq 0$. □

PROPOSITION 38. – *Si M est un A-module libre, $M_T = \{0\}$.*
– $(M/M_T)_T = \{0\}$.

DÉMONSTRATION. Soit X une base de M. Soit $m \in M_T$. Il existe une famille $(\lambda_x) \in A^{(X)}$ telle que $m = \sum_x \lambda_x x$. Il existe $a \neq 0$ tel que $am = 0$. On a $\sum_x a\lambda_x x = 0$. Donc, pour tout x, $a\lambda_x = 0$, puis $\lambda_x = 0$.
Soit $m \in M$ et $\bar{m}$ sa classe dans M/M_T. Si $\bar{m} \in (M/M_T)_T$, il existe $a \neq 0$ tel que $a\bar{m} = 0$, donc $am \in M_T$. Il existe $b \neq 0$ tel que $b(am) = 0$. On a donc $m \in M_T$, puis $\bar{m} = 0$. □

2. Classes d'isomorphisme des modules de type fini sur un anneau principal

Soit A un anneau principal.

DÉFINITION 31. Soit M un A-module. On appelle *idéal annulateur* de M l'idéal $\mathrm{Ann}\, M = \{a \in A : aM = 0\}$.

PROPOSITION 39. *Si M est de type fini, on a l'équivalence $M = M_T \iff \mathrm{Ann}\, M \neq \{0\}$.*

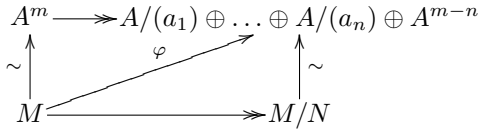
THÉORÈME 20 (Classes d'isomorphisme de A-modules). *Soit M un A-module de type fini. Alors il existe deux entiers naturels uniques r et s et une suite d'éléments de $A\backslash(A^* \cup \{0\})$ $a_s \mid \ldots \mid a_1$ unique aux inversibles près tels que*

$$M \simeq A/(a_1) \oplus \ldots \oplus A/(a_s) \oplus A^r$$

Ceci décrit les classes d'isomorphisme de A-modules.

THÉORÈME 21 (De la base adaptée). *Soit M un A-module libre de rang m et soit N un sous-module de M. Alors N est un A-module libre de rang $n \leqslant m$ et, plus précisément, il existe une base $\{e_1, \ldots, e_m\}$ de M et des éléments non nuls $a_n \mid \ldots \mid a_1$ de A tels que $(a_1 e_1, \ldots, a_n e_n)$ soit une base de N. Les $a_1, \ldots, a_n$ sont alors uniques aux inversibles près.*

REMARQUES 6. Avec les notations du théorème, on a $M/N \simeq A/(a_1) \oplus \ldots \oplus A/(a_n) \oplus A^{m-n}$. On a le diagramme suivant



φ est un morphisme surjectif de noyau N. Par factorisation de ce morphisme, on a le résultat.

Faire le quotient de M par N revient à quotienter composante par composante, d'où le nom de "base adaptée".

On obtient que l'unicité dans le théorème 20 implique l'unicité dans le théorème 21. En effet supposons avoir des éléments non nuls $a_n \mid \ldots \mid a_1$ de A tels que $(a_1 e_1, \ldots, a_n e_n)$ soit une base de N. Soit ℓ défini par a_i inversible pour tout $i \geqslant \ell$ et a_i non inversible pour tout $i < l$. On a, d'après ce qui précède, $M/N \simeq A/(a_1) \oplus \ldots \oplus A/(a_{\ell-1}) \oplus A^{m-n}$. L'unicité dans le théorème 20 assure que $m-n$ est unique (donc n est unique) et l'unicité aux inversibles près de $a_1, \ldots, a_{\ell-1}$. En outre, pour $i \geqslant \ell$, $a_i = 1$ aux inversibles près. On en déduit l'unicité dans le théorème 21.

Soit M un A-module de type fini et $\{m_1, \ldots, m_n\}$ une partie génératrice de M. Alors on définit un morphisme surjectif

$$\begin{array}{rcl} \varphi : A^n & \twoheadrightarrow & M \\ (a_1, \ldots, a_n) & \mapsto & \sum_{i=1}^n a_i m_i \end{array}$$

On a donc $M \simeq A^n / \ker \varphi$.

Supposons montrée l'existence dans le théorème 21 : il existe $(e_1, \ldots, e_n)$ base de A^n, il existe $m \leqslant n$ et il existe des éléments non nuls $a_m \mid \ldots \mid a_1$ de A tels que $(a_1 e_1, \ldots, a_m e_m)$ soit une base de $\ker \varphi$. On a, d'après notre remarque précédente, $A^n / \ker \varphi \simeq A/(a_1) \oplus \ldots \oplus A/(a_n) \oplus A^{m-n}$, d'où $M \simeq A/(a_1) \oplus \ldots \oplus A/(a_n) \oplus A^{m-n}$. On retire les a_i inversibles et on obtient une décomposition de M telle qu'elle est décrite dans le théorème 20.

DÉMONSTRATION. Nous allons commencer par démontrer l'existence dans le théorème 21.

LEMME 20. *Soit M un A-module de type fini. Soit α une forme linéaire (*i.e. *un morphisme $M \to A$) non nulle. Alors $\alpha(M)$ est un idéal principal non nul de A. Si $m_0 \in M$ vérifie $\alpha(M) = (\alpha(m_0))$, on a $M = Am_0 \oplus \ker \alpha$.*

DÉMONSTRATION. Soit $m \in M$. $\alpha(m) \in (\alpha(m_0))$, donc il existe $a \in A$ tel que $\alpha(m) = a\alpha(m_0)$. On a $m = \underbrace{am_0}_{\in Am_0} + \underbrace{(m - am_0)}_{\in \ker \alpha}$. Donc $M = Am_0 + \ker \alpha$.

Supposons $am_0 \in \ker\alpha$. On a $0 = \alpha(am_0) = a\underbrace{\alpha(m_0)}_{\neq 0}$, donc $a = 0$, puis $am_0 = 0$. Finalement, $M = Am_0 \oplus \ker\alpha$. □

LEMME 21. *Soit M un A-module libre de rang m. Soit α une forme linéaire non nulle de M. Alors $\ker\alpha$ est un A-module libre de rang $m-1$.*

DÉMONSTRATION. Le résultat se démontre par récurrence sur m. On note $(e_1, \dots, e_m)$ une base de M. On appelle $(e_1^*, \dots, e_m^*)$ sa base duale. Alors $\ker e_i^* = \bigoplus_{j\neq i} Ae_j$.

On prend m_0 dans M tel que $\alpha(M) = (\alpha(m_0))$, si bien que l'on a $M = Am_0 \oplus \ker\alpha$.

Si $\ker\alpha \neq \{0\}$, il existe i tel que $e_i^*(\ker\alpha) \neq \{0\}$. $e^*_{i|\ker\alpha}$ est donc une forme linéaire non nulle. On lui applique le lemme précédent : il existe $m_1 \in \ker\alpha$ tel que $\ker\alpha = Am_1 \oplus \ker e^*_{i|\ker\alpha}$. Ainsi, on a $M = Am_0 \oplus Am_1 \oplus (\ker e_i^* \cap \ker\alpha)$.

$\ker e_i^* \cap \ker\alpha$ est le noyau de la forme linéaire $\alpha_{|\ker e_i^*}$ définie sur $\ker e_i^*$, qui est un module libre de rang $m-1$. D'après l'hypothèse de récurrence, $\ker e_i^* \cap \ker\alpha$ est un module libre de rang au moins $m-2$. Or $M = Am_0 \oplus Am_1 \oplus (\ker e_i^* \cap \ker\alpha)$. $\ker\alpha = Am_1 \oplus (\ker e_i^* \cap \ker\alpha)$ est donc un module libre de rang $m-1$.

On remarque que $Am_1 \simeq A$, car m_1 n'est pas de torsion, puisque $(\ker\alpha)_T \subset M_T = \{0\}$, car M libre. □

Revenons à la démonstration de l'existence dans le théorème 21. Soit M un module libre de rang m et N un sous-module de M. On pose $\mathcal{F} = \{\alpha(N), \alpha \in \mathrm{Hom}_A(M, A)\}$. $\mathcal{F}$ est un ensemble d'idéaux de A. On en cherche un maximal (c'est possible, car A est noetherien, puisque principal ; en outre, on peut identifier un tel idéal maximal : on associe à tout idéal I non nul de $\mathcal{F}$ un entier n_I qui est le nombre d'irréductibles comptés avec leurs multiplicités d'une décomposition en produit d'irréductibles d'un générateur de I, on choisit alors I tel que n_I soit minimal). Soit donc I un idéal maximal pour l'inclusion dans $\mathcal{F}$. Soient $\alpha \in \mathrm{Hom}_A(M, A)$ tel que $I = \alpha(N)$, $b \in A$ tel que $I = (b)$ et $f \in N$ tel que $b = \alpha(f)$. On peut supposer $N \neq \{0\}$. Dans ce cas, $\mathcal{F} \neq \{0\}$ et $b \neq 0$.

LEMME 22. *Pour tout $\beta \in \mathrm{Hom}_A(M, A), b \mid \beta(f)$*

DÉMONSTRATION. Soit $d = b \wedge \beta(f)$. Comme A est principal, on a une relation de Bézout : il existe $x, y \in A$ tels que $xb + y\beta(f) = d$. On a $(x\alpha + y\beta)(f) = d$. Alors $(x\alpha + y\beta)(N) \supset (d) \supset (b) = \alpha(N)$. Comme $\alpha(N)$ est maximal dans $\mathcal{F}$, on en déduit qu'il y a égalité partout, donc $(d) = (b)$, puis $b \mid \beta(f)$. □

LEMME 23. *Il existe $e \in M$ tel que $\alpha(e) = 1$ et $f = be$.*

DÉMONSTRATION. Soit $(e_1, \dots, e_m)$ une base de M et $(e_1^*, \dots, e_m^*)$ sa base duale. On a $f = \sum_{i=1}^m e_i^*(f)e_i$ et pour tout i, $b \mid e_i^*(f)$. Il existe donc $c_1, \dots, c_m$ dans A tels que pour tout i, $bc_i = e_i^*(f)$. Alors on a $f = b\sum_{i=1}^m c_i e_i$, puis $f = be$ en posant $e = \sum_{i=1}^m c_i e_i$. On en déduit $\alpha(e) = 1$. □

Reprenons la démonstration du théorème. On a $\alpha(N) = (b) = (\alpha(f))$. On en déduit que $N = Af \oplus (\ker\alpha \cap N)$.

Comme $\alpha(e) = 1$, on a $\alpha(M) \supset (\alpha(e)) = A$, d'où $\alpha(M) = (\alpha(e))$, puis $M = Ae \oplus \ker\alpha$.

On sait que $\ker\alpha$ est un A-module libre de rang $m-1$. On suppose par récurrence qu'il existe une base adaptée à son sous-module $\ker\alpha \cap N$: il existe $(e'_1, \dots, e'_{m-1})$ une base de $\ker\alpha$, il existe $n \leqslant m$ et des éléments non nuls $a_{n-1} \mid \dots \mid a_1$ tels que $(a_1e'_1, \dots, a_{n-1}e'_{n-1})$ soit une base de $\ker\alpha \cap N$.

On pose $e_1 = e'_1, \ldots, e_{n-1} = e'_{n-1}, e_n = e$ et $e_i = e'_{i-1}$ pour tout $i > n$. Comme $M = Ae \oplus \ker\alpha$, $(e_1, \ldots, e_m)$ est une base de M.

On pose $a_n = b$. Comme $N = Abe \oplus (\ker\alpha \cap N)$, $(a_1e_1, \ldots, a_ne_n)$ est une base de N. En particulier, N est libre, de rang n.

On remarque que $\alpha(a_{n-1}e_{n-1} + a_ne_n) = a_n = b$ et $a_{n-1}e_{n-1} + a_ne_n \in N$. On en déduit que $b \mid \beta(a_{n-1}e_{n-1} + a_ne_n)$, pour toute forme linéaire β. En particulier, pour $\beta = e^*_{n-1}$, on a $a_n \mid a_{n-1}$.

Démontrons maintenant l'unicité dans le théorème 20. Supposons pouvoir écrire $M \simeq A/(a_1)\oplus\ldots\oplus A/(a_s)\oplus A^r$, avec $a_s \mid \ldots \mid a_1$, et $M \simeq A/(b_1)\oplus\ldots\oplus A/(b_t)\oplus A^q$, avec $b_t \mid \ldots \mid b_1$. Montrons que $r = q$, $s = t$ et pour tout i, $a_i = b_i$ aux inversibles près.

LEMME 24. $(A/(a_1) \oplus \ldots \oplus A/(a_s) \oplus A^r)_T = A/(a_1) \oplus \ldots \oplus A/(a_s)$.

Remarquons que $\mathrm{Ann}(A/(a)) = (a)$. On a donc $\mathrm{Ann}(\bigoplus_i A/(a_i)) = \bigcap_i (a_i) = (a_1)$. Du lemme, on déduit $A/(a_1) \oplus \ldots \oplus A/(a_s) \simeq A/(b_1) \oplus \ldots \oplus A/(b_t)$. En considérant l'idéal annulateur, on a $a_1 = b_1$.

LEMME 25. *Si $M \simeq A/(a_1) \oplus \ldots \oplus A/(a_s) \oplus A^r$, alors $M/M_T \simeq A^r$*

DÉMONSTRATION. On a un isomorphisme $\varphi : M \xrightarrow{\sim} A/(a_1)\oplus\ldots\oplus A/(a_s)\oplus A^r$. Donc $\varphi(M_T) = \varphi(M)_T = A/(a_1) \oplus \ldots \oplus A/(a_s)$. Par passage au quotient, on a

$$\begin{array}{ccc} M & \longrightarrow & A/(a_1) \oplus \ldots \oplus A/(a_s) \oplus A^r \\ \downarrow & & \downarrow \\ M/M_T & \longrightarrow & (A/(a_1) \oplus \ldots \oplus A/(a_s) \oplus A^r)/(A/(a_1) \oplus \ldots \oplus A/(a_s)) \simeq A^r \end{array}$$

□

On déduit directement de ce lemme que $r = q$ (c'est le rang du module libre M/M_T).

REMARQUE 21. On a obtenu que M est libre si et seulement $M_T = \{0\}$.

LEMME 26. *Soit $b \in A\backslash\{0\}$. Soit $a \in A$. On a $bA/(a) \simeq A/(a')$, où $a' = \frac{a}{a\wedge b}$.*

DÉMONSTRATION. On a le diagramme suivant

$$\begin{array}{ccc} A & \twoheadrightarrow & A/(a) \\ & \searrow^{\varphi} & \downarrow \\ & & bA/(a) \end{array}$$

φ est un morphisme surjectif, déterminons son noyau.

Soit $y \in A$. $y \in \ker\varphi \iff by \in (a) \iff a \mid by \iff \frac{a}{a\wedge b} \mid \frac{b}{a\wedge b}y \iff a' \mid y \iff y \in (a')$. Donc $\ker\varphi = (a')$. □

LEMME 27. *Soit $b \in A\backslash\{0\}$. Soit $a \in A$. On a $(A/(a))/(bA/(a)) \simeq A/(a \wedge b)$.*

DÉMONSTRATION. On a le diagramme suivant

$$A \xrightarrow{\varphi} A/(a) \twoheadrightarrow (A/(a))/(bA/(a))$$

φ est un morphisme surjectif, déterminons son noyau.

Soit $y \in A$. On a $y \in \ker\varphi \iff y + (a) \in bA/(a) \iff \exists x \in A : y + (a) = bx + (a) \iff \exists x, z \in A : y = bx + za \iff y \in (a) + (b) \iff y \in (a \wedge b)$. □

Rappelons que l'on a, à ce stade de la démonstration, $A/(a_1) \oplus \ldots \oplus A/(a_s) \simeq M \simeq A/(b_1) \oplus \ldots \oplus A/(b_t)$.

Soit p un diviseur irréductible de a_s. On a $pM \simeq A/(a'_1) \oplus \ldots \oplus A/(a'_s)$, où $a'_i = \frac{a_i}{p}$. On a aussi $M/pM \simeq (A/(p))^s$.

Comme $a_1 = b_1$, il existe ℓ tel que pour tout $i \leqslant \ell$, $p \mid b_i$, et pour tout $i > \ell$, $p \nmid b_i$. On a $pM \simeq A/(b'_1) \oplus \ldots \oplus A/(b'_\ell) \oplus A/(b_{\ell+1}) \oplus \ldots \oplus A/(b_t)$, où $b'_i = \frac{b_i}{p}$, pour $i \leqslant \ell$. On a aussi $M/pM \simeq (A/(p))^\ell$.

La structure de A-module de M/pM provient d'une structure de $A/(p)$-espace vectoriel ($A/(p)$ est un corps). On en déduit que $\ell = s$ (c'est la dimension de M/pM vu comme $A/(p)$-espace vectoriel).

On en déduit que $s \leqslant t$. Par symétrie, on a $s = t$.

D'où $\ell = t$. On en déduit que $A/(a'_1) \oplus \ldots \oplus A/(a'_s) \simeq pM \simeq A/(b'_1) \oplus \ldots \oplus A/(b'_t)$. On conclut par récurrence sur le nombre de diviseurs irréductibles de a_1 comptés avec leurs multiplicités. On en déduit que $a_i = b_i$ aux inversibles près.

L'initialisation de la récurrence correspond à a_1 irréductible, qui est un cas trivial (dans ce cas, tous les a_i et b_i sont égaux).

□

3. Applications

3.1. Cas particulier des groupes abéliens.

3.1.1. *Théorème de décomposition des groupes abéliens.* Un groupe abélien est naturellement muni d'une structure de $\mathbb{Z}$-module :

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (n, g) & \mapsto & n \cdot g = \begin{cases} \underbrace{g + \ldots + g}_{n \text{ termes}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{-g - \ldots - g}_{-n \text{ termes}} & \text{si } n < 0 \end{cases} \end{array}$$

Remarque 22.
- Un morphisme de groupes abéliens est aussi un morphisme de $\mathbb{Z}$-modules.
- Un sous-groupe d'un groupe abélien est un sous-$\mathbb{Z}$-module.

Soit G un groupe abélien. Soit $g \in G$. g est de torsion si et seulement si $\exists n \neq 0 : ng = 0$ si et seulement si $\exists n > 0 : ng = 0$ si et seulement si g est d'ordre fini. On en déduit la proposition suivante :

Proposition 40. *Le sous-module de torsion de G est le sous-groupe formé par les éléments d'ordre fini dans G.*

Le théorème 20 s'écrit dans ce contexte de la manière suivante.

Théorème 22 (Décomposition des groupes abéliens). *Soit G un groupe abélien de type fini. Alors il existe deux uniques entiers r et s et une unique famille d'entiers naturels > 1 vérifiant $n_s \mid \ldots \mid n_1$ tels que $G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_s\mathbb{Z} \oplus \mathbb{Z}^r$.*

Dans le cas particulier où G est fini, on a :
- $r = 0$,
- $n_1\mathbb{Z} = \operatorname{Ann} G$. Donc n_1 est le *ppcm* des ordres des éléments de G, c'est-à-dire l'exposant du groupe G. n_1 est également l'ordre d'un élément de G, c'est donc le plus grand ordre possible.
- $|G| = \prod_{i=1}^s n_i$

Dans le cas d'un groupe abélien, on peut retrouver assez facilement l'unicité des n_i. Prenons en effet $n_s \mid \ldots \mid n_1$ et $m_t \mid \ldots \mid m_1$ tels que $\bigoplus_{i=1}^s \mathbb{Z}/n_i\mathbb{Z} = \bigoplus_{i=1}^t \mathbb{Z}/m_i\mathbb{Z}$. Le lecteur montrera les résultats suivants :

(i). $\forall d \in \mathbb{N}^*, \forall n \in \mathbb{N}^*, |d\mathbb{Z}/n\mathbb{Z}| = \frac{n}{d \wedge n}$.

(ii). $\forall d \in \mathbb{N}^*, \prod_{i=1}^{s}(d \wedge n_i) = \prod_{i=1}^{t}(d \wedge m_i)$.

(iii). $s = t$ et $\forall i, n_i = m_i$.

Le lecteur montrera également que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/a \wedge b\mathbb{Z} \times \mathbb{Z}/a \vee b\mathbb{Z}$, en
- utilisant le théorème 22,
- décomposant a et b en puissances de nombres premiers et en utilisant le lemme chinois,
- exhibant un isomorphisme.

3.1.2. *Exemples d'application.*

Structure du groupe multiplicatif d'un corps commutatif. Donnons une autre démonstration du théorème 7 qui assure que tout sous-groupe fini G du groupe multiplicatif d'un corps commutatif est cyclique.

DÉMONSTRATION. D'après le théorème 22, on a $G \simeq G_1 \oplus \ldots \oplus G_s$, où $G_i \simeq \mathbb{Z}/n_i\mathbb{Z}$ et $n_i \mid n_{i-1}$. Donc tous les éléments de G sont racines du polynôme $X^{n_1} - 1$. Or ce polynôme a au plus n_1 racines. Donc $|G| \leqslant n_1$, ce qui impose $s = 1$. □

Le problème de Galois inverse pour les groupes abéliens. L'extension galoisienne

$$\begin{array}{c} \mathbb{K} = D_{\mathbb{Q}}(P) \\ | \\ \mathbb{Q} \end{array}$$

correspond au groupe de Galois $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. On s'intéresse à la question suivante : quels sont les groupes finis qui sont des groupes de Galois d'extensions galoisiennes de $\mathbb{Q}$?

Cette question est très difficile et le problème est encore ouvert. Cependant, on connait des groupes finis qui sont des groupes de Galois d'extensions galoisiennes de $\mathbb{Q}$: par exemple, les groupes abéliens finis.

THÉORÈME 23. *Les groupes abéliens finis sont des groupes de Galois d'extensions galoisiennes de* $\mathbb{Q}$.

La démonstration repose sur les propositions suivantes que nous ne démontrerons pas.

PROPOSITION 41. *On considère l'extension cyclotomique galoisienne de degré* $\deg \Phi_n = \varphi(n)$

$$\begin{array}{c} \mathbb{Q}(e^{\frac{2\imath\pi}{n}}) = D_{\mathbb{Q}}(\Phi_n) \\ | \\ \mathbb{Q} \end{array}$$

On a

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(e^{\frac{2\imath\pi}{n}})) = \{\sigma : e^{\frac{2\imath\pi}{n}} \mapsto e^{\frac{2\imath k\pi}{n}}, k \wedge n = 1\} \simeq (\mathbb{Z}/n\mathbb{Z})^*$$

PROPOSITION 42. *On considère une extension galoisienne* $\mathbb{Q} - \mathbb{K}$. *On note* $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. *Soit* H *un sous-groupe de* G. *On pose* $\mathbb{K}^H = \{x \in \mathbb{K} : \forall \sigma \in H, \sigma(x) = x\}$. *On a alors*

$$\begin{array}{c} \mathbb{K} \\ | \\ \mathbb{K}^H \\ | \\ \mathbb{Q} \end{array}$$

Alors l'extension $\mathbb{Q} - \mathbb{K}^H$ *est galoisienne si et seulement si* $H \lhd G$. *Dans ce cas,* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K}^H) \simeq G/H$.

Montrons maintenant le lemme suivant.

LEMME 28. *Soit G un groupe abélien fini. Il existe un entier n tel que G est isomorphe à un quotient de $(\mathbb{Z}/n\mathbb{Z})^*$.*

DÉMONSTRATION. On cherche un n convenable sous la forme $n = p_1 \dots p_t$ où les p_i sont premiers deux à deux distincts. Alors

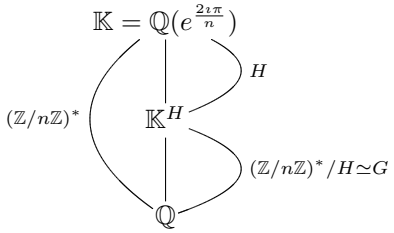
$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{t} (\mathbb{Z}/p_i\mathbb{Z})^* \simeq \prod_{i=1}^{t} \mathbb{Z}/(p_i - 1)\mathbb{Z}$$

D'après le théorème 22, il existe s et $n_s \mid \dots \mid n_1$ tels que $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_s\mathbb{Z}$.

Pour que G soit isomorphe à un quotient de $(\mathbb{Z}/n\mathbb{Z})^*$, il suffit que $s = t$ et que pour tout i, $\mathbb{Z}/n_i\mathbb{Z}$ soit isomorphe à un quotient de $(\mathbb{Z}/p_i\mathbb{Z})^*$, c'est-à-dire $s = t$ et pour tout i, $n_i \mid p_i - 1$ (car les quotients d'un groupe cyclique $\mathbb{Z}/k\mathbb{Z}$ sont, à isomorphisme près, les groupes cycliques $\mathbb{Z}/\ell\mathbb{Z}$, avec $\ell \mid k$).

Il suffit maintenant de prouver l'existence de s nombres premiers $p_1, \dots, p_s$ tels que pour tout i, $n_i \mid p_i - 1$. Le théorème de la progression arithmétique de Dirichlet assure qu'il existe une infinité de nombres premiers $p = 1 \mod n_1$. On prend les s premiers : $p_1, \dots, p_s$. On a $n_i \mid n_1 \mid p_i - 1$. □

DÉMONSTRATION. (théorème 23) Il existe n et $H \lhd (\mathbb{Z}/n\mathbb{Z})^*$ tels que $G \simeq (\mathbb{Z}/n\mathbb{Z})^*/H$. On a alors



Le groupe G est bien groupe de Galois d'une extension galoisienne : $\mathbb{Q} - \mathbb{K}^H$. □

3.2. Structure de $\mathbb{K}[X]$-module induite par un endomorphisme sur un espace vectoriel de dimension finie. Soit $\mathbb{K}$ un corps commutatif. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$. On munit E de la loi externe

$$\begin{array}{rcl} \mathbb{K}[X] \times E & \to & E \\ (P, x) & \mapsto & P(u)(x) \end{array}$$

On vérifie qu'on munit ainsi E d'une structure de $\mathbb{K}[X]$-module. On le note E_u.

REMARQUES 7.
- Un sous-module de E_u est un sous-espace u-stable de E.
- Un endomorphisme de E_u est un endomorphisme de E qui commute avec u.
- Un sous-espace vectoriel u-cyclique de E est un sous-module monogène de E_u (d'où la notation $< x >_u$).
- E_u est de torsion et $\operatorname{Ann} E_u = (\pi_u)$.

LEMME 29. *Soit $Q \in \mathbb{K}[X]$. Soit F un sous-espace vectoriel u-stable de E (*i.e. *un sous-$\mathbb{K}[X]$-module de E_u). Alors F est isomorphe en tant que $\mathbb{K}[X]$-module à $\mathbb{K}[X]/(Q)$ si et seulement si F est u-cyclique et $\pi_{u_F} = Q$.*

DÉMONSTRATION. ($\Rightarrow$) Il existe $\psi : \mathbb{K}[X]/(Q) \to F$ un isomorphisme de $\mathbb{K}[X]$-module. Soit $x = \psi(1)$. Alors on a $\psi(P(X)) = P \cdot \psi(1) = P \cdot x = P(u)(x)$. Comme ψ est surjectif, F est u-cyclique. L'injectivité de ψ, quant à elle, assure que $P(u)(x) = 0$ si et seulement si $Q \mid P$, c'est-à-dire que $Q = \pi_{u_F}$.

($\Leftarrow$) Réciproquement, si F est u-cyclique de polynôme minimal Q, on a un morphisme surjectif

$$\begin{array}{ccc} \mathbb{K}[X] & \to & F \\ P & \mapsto & P(u)(x) \end{array}$$

de noyau $\pi_{u_F} = Q$. □

Appliquons à E_u le théorème 20. On obtient l'existence d'un unique entier s et d'une famille de polynômes $Q_s \mid \ldots \mid Q_1$ unique aux inversibles près tels que $E_u \simeq \bigoplus_{i=1}^{s} \mathbb{K}[X]/(Q_i)$. Pour tout i, on appelle F_i le sous-$\mathbb{K}[X]$-module de E_u qui est l'image de $\mathbb{K}[X]/(Q_i)$ par l'isomorphisme $\bigoplus_{i=1}^{s} \mathbb{K}[X]/(Q_i) \to E_u$. On a $E_u = \bigoplus_{i=1}^{s} F_i$ (somme directe de sous-$\mathbb{K}[X]$-modules de E_u), donc $E = \bigoplus_{i=1}^{s} F_i$ (somme directe de sous-espaces vectoriels u-stables de E). En outre, pour tout i, $F_i \simeq \mathbb{K}[X]/(Q_i)$. D'après le lemme, pour tout i, F_i est un sous-espace u-cyclique de E et $\pi_{u_{F_i}} = Q_i$. On retrouve le théorème 12 sur les invariants de similitude.

Proposition 43. *Soient $u, v \in \mathcal{L}(E)$. Alors u et v sont semblables si et seulement si les $\mathbb{K}[X]$-modules E_u et E_v sont isomorphes.*

Remarque 23. La classe d'isomorphisme du $\mathbb{K}[X]$-module E_u caractérise la classe de similitude de u dans $\mathcal{L}(E)$.

Démonstration. Soit w un automorphisme de l'espace vectoriel E. w est un isomorphisme de $\mathbb{K}[X]$-modules de E_u dans E_v si et seulement si

$$\begin{array}{ll} & \forall P \in \mathbb{K}[X], \forall x \in E, w(P \cdot x) = P \cdot w(x) \\ \iff & \forall P \in \mathbb{K}[X], \forall x \in E, w(P(u)(x)) = P(v)w(x) \\ \iff & \forall P \in \mathbb{K}[X], wP(u) = P(v)w \\ \iff & wu = vw \end{array}$$

□

Remarque 24. On appelle module simple un module qui n'a aucun sous-module non trivial. Ainsi, un endomorphisme u est simple si et seulement si E_u est un module simple. Certaines notions vues dans le cadre des endomorphismes d'un espace vectoriel apparaissent comme des cas particuliers de notions plus générales concernant les modules sur les anneaux principaux. Nous n'entrerons pas dans les détails ici.

3.3. Classes d'équivalence de matrices à coefficients dans un anneau principal.

3.3.1. *Cas général.* Soit A un anneau principal. Soient $M, N \in \mathrm{M}_{m,n}(A)$.

Définition 32. M et N sont dites *équivalentes* si et seulement si il existe des matrices $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que $M = PNQ$.

Proposition 44. *La relation "être équivalente" est une relation d'équivalence.*

Remarque 25. Soit $M \in \mathrm{M}_{m,n}(A)$. M définit canoniquement un morphisme $A^n \to A^m$, noté abusivement M. Deux matrices M et N sont équivalentes si et seulement si l'ensemble des matrices de M pour des bases quelconques de A^n et A^m est égal à l'ensemble des matrices de N pour des bases quelconques de A^n et A^m si et seulement si M et N ont une matrice en commun.

Théorème 24. *Soit $M \in \mathrm{M}_{m,n}(A)$. Alors il existe un unique entier $r = \operatorname{rg} M$ et une famille d'éléments non nuls de A $a_r \mid \ldots \mid a_1$ unique aux inversibles près tels*

que M soit équivalente à la matrice

$$\begin{pmatrix} a_1 & & & & & \\ & \ddots & & 0 & & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

REMARQUE 26. $r \leqslant \min(m,n)$ est le rang de la matrice M.

DÉMONSTRATION. On a $M : A^n \to A^m$. On montre que $\ker M$ est facteur direct de A^n. En effet, si $x \in A^n$ est tel qu'il existe $\alpha \neq 0$ vérifiant $\alpha x \in \ker M$, alors $x \in \ker M$ (on a ainsi $(A^n/\ker M)_T = \{0\}$).

D'après le théorème 21, il existe $(e_1, \dots, e_n)$ une base de A^n, il existe $s \leqslant n$ et il existe $b_s \mid \dots \mid b_1$ non nuls tels que $(b_1 e_1, \dots, b_s e_s)$ est une base de $\ker M$. Comme $b_i e_i \in \ker M$, d'après la remarque ci-dessus, $e_i \in \ker M$. Les b_i sont donc inversibles et $\ker M = \bigoplus_{i=1}^{s} Ae_i$. On a donc $A^n = \ker M \oplus \bigoplus_{i>s} Ae_i$.

Montrons maintenant que $\operatorname{Im} M = \bigoplus_{i>s} AMe_i$. On sait déjà que l'image de M est égale à $\sum_{i=1}^{n} AMe_i = \sum_{i>s} AMe_i$, car pour tout $i \leqslant s$, $Me_i = 0$. Soit $(x_i)_{i>s} \in A^{n-s}$ tels que $\sum_{i>s} x_i M e_i = 0$. On a alors $\sum_{i>s} x_i e_i \in \ker M$. Comme $\ker M \cap \bigoplus_{i>s} Ae_i = \{0\}$, on a $\sum_{i>s} x_i e_i = 0$, donc pour tout $i > s$, $x_i = 0$.

On applique le théorème 21 au sous-module $\operatorname{Im} M$ de A^m : il existe $(f_1, \dots, f_m)$ une base de A^m, il existe $r \leqslant m$ et il existe $a_r \mid \dots \mid a_1$ non nuls tels que $(a_1 f_1, \dots, a_r f_r)$ est une base de $\operatorname{Im} M$. On a clairement $r = n - s$.

Il existe $g_1, \dots, g_r \in A^n$ tels que $Mg_i = a_i f_i$. Montrons que

$$A^n = \underbrace{\bigoplus_{i=1}^{s} Ae_i}_{\ker M} \oplus \bigoplus_{i=1}^{r} Ag_i$$

Soit $e \in A^n$. On a $Me = \sum_{i=1}^{r} x_i a_i f_i$, car $\operatorname{Im} M = \bigoplus_{i>s} AMe_i$. Donc $Me = M \sum_{i=1}^{r} x_i g_i$, puis $e - \sum_{i=1}^{r} x_i g_i \in \ker M$. On a donc $A^n = \ker M + \sum_{i=1}^{r} Ag_i$. Supposons avoir $f \in \ker M$ et $x_i \in A$ tels que $f + \sum_{i=1}^{r} x_i g_i = 0$. On a $0 = M(f + \sum_{i=1}^{r} x_i g_i) = \sum_{i=1}^{r} x_i a_i f_i$. Donc pour tout i, $x_i = 0$. On en déduit aussi que $f = 0$.

La matrice de M dans la base $(g_1, \dots, g_r, e_1, \dots, e_s)$ de A^n et dans la base $(f_1, \dots, f_m)$ de A^m s'écrit

$$D = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & 0 & & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

En appelant P et Q les matrices de passage convenables, on a $M = PDQ$.

Montrons que les a_i sont uniques aux inversibles près. On a le diagramme commutatif suivant

$$\begin{array}{ccc} A^n & \xrightarrow{M} & A^m \\ {\scriptstyle Q}\downarrow{\scriptstyle \sim} & & {\scriptstyle \sim}\uparrow{\scriptstyle P} \\ A^n & \xrightarrow{D} & A^m \end{array}$$

Il existe un automorphisme de A^m (c'est P) qui envoie $\operatorname{Im} D$ sur $\operatorname{Im} M$. Soit $(h_1, \dots, h_m)$ la base canonique de A^m. On a $\operatorname{Im} D = \bigoplus_{i=1}^{r} Aa_i h_i$. Sur la base $(Ph_1, \dots, Ph_m)$, on a $\operatorname{Im} M = \bigoplus_{i=1}^{r} Aa_i Ph_i$. $(Ph_1, \dots, Ph_m)$ est une base adaptée à l'image de M. Les a_i sont alors uniques aux inversibles près (on invoque l'unicité du théorème 21). □

La proposition suivante donne l'expression des a_i en fonction des coefficients de la matrice M.

PROPOSITION 45. *Soit $M \in \mathrm{M}_{m,n}(A)$. Soit $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$. Soient $a_1, \dots, a_r$ des éléments non nuls de A tels que $a_r \mid \dots \mid a_1$ et*

$$M = P \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & 0 & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix} Q$$

Alors

- *r est le plus grand entier s tel qu'il existe un mineur de taille s extrait de M et non nul,*
- *a_r est le pgcd des coefficients de M,*
- *pour $1 \leqslant i < r$, a_i est le quotient du pgcd des mineurs de taille $r+1-i$ extraits de M et du pgcd des mineurs de taille $r-i$ extraits de M.*

REMARQUE 27. On redémontre ainsi l'unicité des coefficients a_i aux inversibles près (puisqu'un *pgcd* est unique aux inversibles près).

DÉMONSTRATION. Soit $M \in \mathrm{M}_{m,n}(A)$. On note $\mathcal{I}_j(M)$ l'idéal engendré par les mineurs de taille j extraits de M, pour $1 \leqslant j \leqslant \min(m,n)$.

On note

$$D = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & 0 & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

Alors, pour $j > r$, on a $\mathcal{I}_j(D) = (0)$ et, pour $j \leqslant r$, $\mathcal{I}_j(D) = (a_{i_1} \dots a_{i_j}, 1 \leqslant i_1 < \dots < i_j \leqslant r) = (a_r \dots a_{r+1-j})$.

Montrons que $\mathcal{I}_j(M)$ reste constant dans la classe d'équivalence de M.

REMARQUE 28. On a $\mathcal{I}_j(M) = \mathcal{I}_j({}^tM)$. Il suffit donc de montrer que pour toute matrice $P \in \mathrm{GL}_m(A)$, pour toute matrice $M \in \mathrm{M}_{m,n}(A)$, $\mathcal{I}_j(PM) = \mathcal{I}_j(M)$. En effet, on aurait alors $\mathcal{I}_j(PMQ) = \mathcal{I}_j(MQ) = \mathcal{I}_j({}^t(MQ)) = \mathcal{I}_j({}^tQ\,{}^tM) = \mathcal{I}_j({}^tM) = \mathcal{I}_j(M)$.

Il suffit même de démontrer que pour toute matrice $P \in \mathrm{GL}_m(A)$, pour toute matrice $M \in \mathrm{M}_{m,n}(A)$, $\mathcal{I}_j(PM) \subset \mathcal{I}_j(M)$, puisqu'alors $\mathcal{I}_j(M) = \mathcal{I}_j(P^{-1}PM) \subset \mathcal{I}_j(PM)$ et on a égalité des deux idéaux.

Montrons donc que pour toute matrice $P \in \mathrm{GL}_m(A)$, pour toute matrice $M \in \mathrm{M}_{m,n}(A)$, $\mathcal{I}_j(PM) \subset \mathcal{I}_j(M)$.

Soit Δ un mineur de taille j extrait de PM. On note $PM = (x_{i,k})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant k\leqslant n}}$, $P = (p_{i,k})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant k\leqslant m}}$ et $M = (m_{i,k})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant k\leqslant n}}$. On a $x_{i,k} = \sum_{\ell=1}^{m} p_{i,\ell} m_{\ell,k}$, donc

$$\begin{aligned}
\Delta &= \begin{vmatrix} x_{i_1,k_1} & \cdots & x_{i_1,k_j} \\ \vdots & & \vdots \\ x_{i_j,k_1} & \cdots & x_{i_j,k_j} \end{vmatrix} \\
&= \begin{vmatrix} \sum_{\ell=1}^{m} p_{i_1,\ell} m_{\ell,k_1} & \cdots & \sum_{\ell=1}^{m} p_{i_1,\ell} m_{\ell,k_j} \\ \vdots & & \vdots \\ \sum_{\ell=1}^{m} p_{i_j,\ell} m_{\ell,k_1} & \cdots & \sum_{\ell=1}^{m} p_{i_j,\ell} m_{\ell,k_j} \end{vmatrix} \\
&= \sum_{\ell_1=1}^{m} \cdots \sum_{\ell_j=1}^{m} p_{i_1,\ell_1} \dots p_{i_j,\ell_j} \underbrace{\begin{vmatrix} m_{\ell_1,k_1} & \cdots & m_{\ell_1,k_j} \\ \vdots & & \vdots \\ m_{\ell_j,k_1} & \cdots & m_{\ell_j,k_j} \end{vmatrix}}_{\text{mineur de taille } j \text{ extrait de } M} \in \mathcal{I}_j(M)
\end{aligned}$$

D'où $\mathcal{I}_j(PM) \subset \mathcal{I}_j(M)$. □

3.3.2. *Cas particulier où l'anneau A est euclidien.* On suppose A euclidien. Dans ce cas, on dispose d'un algorithme qui prend en entrée $M \in \mathrm{M}_{m,n}(A)$ et sort $a_r \mid \dots \mid a_1$ tels que M est équivalente à

$$\begin{pmatrix} a_1 & & & & & \\ & \ddots & & & 0 & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

On redémontre ainsi la partie existence du théorème 24.

Faisons quelques rappels utiles à la compréhension de cet algorithme.

Définition 33. On appelle *matrices d'opérations élémentaires* les matrices inversibles suivantes.

– *Les matrices de transposition.* Soit $i \neq j$. On note

$$\tau_{i,j} = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & (i,i) & & & & & & 0 & \\ & & 1 & \downarrow & & & & & & & \\ & & & 0 & & & & 1 & \leftarrow & (i,j) & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & (j,i) & \rightarrow & 1 & & & & 0 & & & \\ & & & & & & & \uparrow & 1 & & \\ & 0 & & & & & & (j,j) & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix}$$

On a $\det \tau_{i,j} = -1$, donc $\tau_{i,j} \in \mathrm{GL}_n(A)$. Les matrices de transposition engendrent les matrices de permutation $(\delta_{i,\sigma(j)})_{1\leqslant i,j\leqslant n}, \sigma \in \mathfrak{S}_n$.

– *Les matrices de transvection.* Soit $a \in A$ et $i \neq j$. On note

$$T_{i,j,a} = \begin{pmatrix} 1 & & & (i,j) & 0 \\ & \ddots & & \downarrow & \\ & & \ddots & a & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

On a $\det T_{i,j,a} = 1$, donc $T_{i,j,a} \in \mathrm{GL}_n(A)$. Les matrices de transvection engendrent $\mathrm{SL}_n(A)$ (voir [**11**]).

– *Les matrices de dilatation.* Soit $a \in A^*$. On note

$$D_a = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & a \end{pmatrix}$$

On a $\det D_a = a \in A^*$, donc $D_a \in \mathrm{GL}_n(A)$.

Intéressons-nous à ce que l'on obtient en multipliant une matrice $M \in \mathrm{M}_{m,n}(A)$ par une matrice d'opération élémentaire.

PROPOSITION 46. *Soit $M \in \mathrm{M}_{m,n}(A)$. On note*

$$M = \begin{pmatrix} L_1 \\ \vdots \\ L_m \end{pmatrix} = (C_1 \cdots C_n)$$

– *Multiplication par une matrice de permutation.*
  – *Soit $\sigma \in \mathfrak{S}_n$. On pose $\Sigma = (\delta_{i,\sigma(j)})_{1 \leqslant i,j \leqslant n}$. Alors*

$$M\Sigma = \begin{pmatrix} C_{\sigma(1)} & \cdots & C_{\sigma(n)} \end{pmatrix}$$

  et, en particulier,

$$M\tau_{i,j} = (C_1 \quad \cdots \quad C_{i-1} \quad C_j \quad C_{i+1} \quad \cdots \quad C_{j-1} \quad C_i \quad C_{j+1} \quad \cdots \quad C_n)$$

  où $\tau_{i,j}$ désigne la matrice associée à la transposition (i,j).
  – *Soit $\sigma \in \mathfrak{S}_m$. On pose $\Sigma = (\delta_{i,\sigma(j)})_{1 \leqslant i,j \leqslant m}$. Alors*

$$\Sigma M = \begin{pmatrix} L_{\sigma(1)} \\ \vdots \\ L_{\sigma(m)} \end{pmatrix}$$

et, en particulier,

$$\tau_{i,j}M = \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ L_j \\ L_{i+1} \\ \vdots \\ L_{j-1} \\ L_i \\ L_{j+1} \\ \vdots \\ L_m \end{pmatrix}$$

– *Multiplication par une matrice de transvection.*
  – *Soit une matrice de transvection* $T_{i,j,a} \in \mathrm{GL}_n(A)$. *Alors*

$$MT_{i,j,a} = \begin{pmatrix} C_1 & \cdots & C_{j-1} & C_j + aC_i & C_{j+1} & \cdots & C_n \end{pmatrix}$$

  – *Soit une matrice de transvection* $T_{i,j,a} \in \mathrm{GL}_m(A)$. *Alors*

$$T_{i,j,a}M = \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ L_i + aL_j \\ L_{i+1} \\ \vdots \\ L_m \end{pmatrix}$$

– *Multiplication par une matrice de dilatation.*
  – *Soit une matrice de dilatation* $D_a \in \mathrm{GL}_n(A)$. *Alors*

$$MD_a = \begin{pmatrix} C_1 & \cdots & C_{n-1} & aC_n \end{pmatrix}$$

  – *Soit une matrice de dilatation* $D_a \in \mathrm{GL}_m(A)$. *Alors*

$$D_aM = \begin{pmatrix} L_1 \\ \vdots \\ L_{m-1} \\ aL_m \end{pmatrix}$$

On appelle G_m (*respectivement* G_n) le sous-groupe de $\mathrm{GL}_m(A)$ (*respectivement* $\mathrm{GL}_n(A)$) engendré par les matrices d'opérations élémentaires.

En effectuant une suite d'opérations élémentaires sur M, la matrice obtenue est de la forme PMQ, où $P \in G_m$ et $Q \in G_n$.

On note ν un stathme de A. Si $M = (m_{i,j})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} \in \mathrm{M}_{m,n}(A)\backslash\{0\}$, on pose $\nu(M) = \min(\nu(m_{i,j}), m_{i,j} \neq 0)$.

PROPOSITION 47. *L'algorithme suivant permet d'obtenir à partir de M la matrice*

$$D = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & 0 & \\ & & a_r & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

telle que $a_r \mid \ldots \mid a_1$ et qu'il existe $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ vérifiant $M = PDQ$.

DÉMONSTRATION. On montre aisément ce résultat par induction sur $(m + n, \nu(M))$. □

Voici l'*algorithme*.

- Première étape :

$$M \leftarrow \Sigma M \Sigma'$$

  Σ et Σ' sont des matrices de permutation choisies de sorte que $\nu(m_{1,1}) = \nu(M)$ après modification de M.
- Deuxième étape :
  - On suppose qu'il existe $i > 1$ tel que $m_{1,1} \nmid m_{1,i}$. Alors il existe $q, r \in A$ tels que $m_{1,i} = qm_{1,1} + r$ avec $r \neq 0$ et $\nu(r) < \nu(m_{1,1})$.

$$M \leftarrow MT_{1,i,-q}$$

    Ceci revient en fait à $C_i \leftarrow C_i - qC_1$. $\nu(M)$ a strictement diminué.
  - On suppose que pour tout $i > 1$, $m_{1,1} \mid m_{1,i}$. Alors pour tout i, il existe $q_i \in A$ tel que $m_{1,i} = q_i m_{1,1}$.

$$M \leftarrow MT_{1,2,-q_2} \ldots T_{1,n,-q_n}$$

    M devient alors $\begin{pmatrix} m_{1,1} & 0 & \cdots & \cdots & 0 \\ & & \bigstar & & \end{pmatrix}$.
  - On suppose qu'il existe $j > 1$ tel que $m_{1,1} \nmid m_{j,1}$. Alors il existe $q, r \in A$ tels que $m_{j,1} = qm_{1,1} + r$ avec $r \neq 0$ et $\nu(r) < \nu(m_{1,1})$.

$$M \leftarrow T_{j,1,-q}M$$

    Ceci revient en fait à $L_j \leftarrow L_j - qL_1$. $\nu(M)$ a strictement diminué.
  - On suppose que pour tout $j > 1$, $m_{1,1} \mid m_{j,1}$. Alors pour tout j, il existe $q_j \in A$ tel que $m_{j,1} = q_j m_{1,1}$.

$$M \leftarrow T_{m,1,-q_m} \ldots T_{2,1,-q_2}M$$

    M devient alors $\begin{pmatrix} m_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \bigstar & \\ 0 & & & \end{pmatrix}$.
  - On suppose que pour tous $i, j > 1$, $m_{1,1} \mid m_{i,j}$. Il existe donc $q_{i,j} \in A$ tel que $m_{i,j} = q_{i,j} m_{1,1}$.

$$M \leftarrow (q_{i,j})_{\substack{2 \leqslant i \leqslant m \\ 2 \leqslant j \leqslant n}}$$

    La taille de la matrice a strictement diminué.

– On suppose qu'il existe $i, j > 1$ tels que $m_{1,1} \nmid m_{i,j}$.

$$M \leftarrow T_{1,i,1}M$$

M devient alors $\begin{pmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ 0 & & & \\ \vdots & & m_{i,j} & \\ 0 & & & \end{pmatrix}$.

Il existe $q, r \in A$ tels que $m_{i,j} = qm_{1,1} + r$ avec $r \neq 0$ et $\nu(r) < \nu(m_{1,1})$.

$$M \leftarrow MT_{1,j,-q}$$

$\nu(M)$ a strictement diminué.

3.4. Calcul effectif des invariants de similitude et autres applications.

3.4.1. *Calcul des invariants de similitude d'une matrice.*

PROPOSITION 48. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$. Soit M une matrice de u. Soient $Q_r \mid \ldots \mid Q_1$ les invariants de similitude de u. Alors les invariants de la classe d'équivalence dans $\mathrm{M}_n(\mathbb{K}[X])$ de la matrice $X\,\mathrm{I}_n - M$ sont $\underbrace{1, \ldots, 1}_{n-r \text{ facteurs}}, Q_r, \ldots, Q_1$.*

COROLLAIRE 19. *On dispose d'un algorithme pour calculer les invariants de similitude de u.*

DÉMONSTRATION. $\mathbb{K}[X]$ est euclidien. □

DÉMONSTRATION. (proposition 48) Commençons par traiter le cas d'une matrice compagnon. Soit P un polynôme unitaire de degré d. Montrons qu'il existe deux matrices $U, V \in \mathrm{GL}_n(\mathbb{K}[X])$ telles que

$$X\,\mathrm{I}_n - \mathcal{C}(P) = U \begin{pmatrix} P & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} V$$

On note $P = X^d - a_1X^{d-1} - \ldots - a_d$. Alors

$$X\,\mathrm{I}_n - \mathcal{C}(P) = \begin{pmatrix} X & 0 & \cdots & 0 & -a_d \\ -1 & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & X & -a_2 \\ 0 & \cdots & 0 & -1 & X - a_1 \end{pmatrix}$$

$$(\forall i \geqslant 1, L_{n-i} \leftarrow L_{n-i} + XL_{n-i+1} + \ldots + X^i L_n)$$

$$\sim \begin{pmatrix} 0 & \cdots & \cdots & 0 & X^d - a_1X^{d-1} - \ldots - a_d \\ -1 & \ddots & & \vdots & \vdots \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & X^2 - a_1X - a_2 \\ 0 & \cdots & 0 & -1 & X - a_1 \end{pmatrix}$$

$$\sim \begin{pmatrix} P(X) & 0 & \cdots & \cdots & 0 \\ P_2(X) & -1 & \ddots & & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots \\ P_{d-1}(X) & \vdots & \ddots & \ddots & 0 \\ P_d(X) & 0 & \cdots & 0 & -1 \end{pmatrix}$$

$$\left(C_1 \leftarrow C_1 + \sum_{i=2}^{d} P_i C_i\right)$$

$$\sim \begin{pmatrix} P(X) & 0 & \cdots & \cdots & 0 \\ 0 & -1 & \ddots & & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & -1 \end{pmatrix}$$

Dans le cas général, on appelle $Q_r \mid \ldots \mid Q_1$ les invariants de similitude de M. Il existe une matrice $W \in \mathrm{GL}_n(\mathbb{K})$ telle que

$$M = W \begin{pmatrix} \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & \mathcal{C}(Q_r) \end{pmatrix} W^{-1}$$

On a donc

$$X\,\mathrm{I}_n - M = W \begin{pmatrix} X\,\mathrm{I}_{d_1} - \mathcal{C}(Q_1) & & 0 \\ & \ddots & \\ 0 & & X\,\mathrm{I}_{d_r} - \mathcal{C}(Q_r) \end{pmatrix} W^{-1}$$

où $d_i = \deg Q_i$. On sait alors qu'il existe des matrices $U_i, V_i \in \mathrm{GL}_{d_i}(\mathbb{K})$ telles que

$$X\,\mathrm{I}_{d_i} - \mathcal{C}(Q_i) = U_i \begin{pmatrix} Q_i & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix} V_i$$

Alors

$$X\,\mathrm{I}_n - M = \overbrace{W \begin{pmatrix} U_1 & & 0 \\ & \ddots & \\ 0 & & U_r \end{pmatrix}}^{\mathcal{U}\in \mathrm{GL}_n(\mathbb{K}[X])} \begin{pmatrix} Q_1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & 0 & & \\ & & & 1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & Q_r & & & \\ & & & & & & 1 & & \\ & & 0 & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix} \underbrace{\begin{pmatrix} V_1 & & 0 \\ & \ddots & \\ 0 & & V_r \end{pmatrix} W^{-1}}_{\mathcal{V}\in \mathrm{GL}_n(\mathbb{K}[X])}$$

Quitte à permuter les lignes et les colonnes de la matrice ainsi obtenue, on a le résultat. □

3.4.2. *Résolution d'équations diophantiennes du premier degré.* On considère l'équation

$$a_1x_1 + \ldots + a_nx_n = b$$

avec $a_1, \ldots, a_n, b \in \mathbb{Z}$. Ceci revient à considérer le système

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} = b$$

On peut supposer $|a_1| = \min_i |a_i|$. Pour tout j, on écrit $a_j = b_ja_1 + r_j$ avec soit $r_j = 0$, soit $r_j \neq 0$ et $|r_j| < |a_j|$, si bien que l'équation diophantienne considérée équivaut à

$$a_1 \underbrace{(x_1 + b_2x_2 + \ldots + b_nx_n)}_{X_1} + (r_2x_2 + \ldots + r_nx_n) = 0$$

On a fait strictement diminuer le stathme.

Si $r_2 = \ldots = r_n = 0$, alors le système a des solutions si et seulement si $a_1 \mid b$. Dans ce cas, les solutions sont $(\frac{b}{a_1} - \sum_{i=2}^n b_ix_i, x_2, \ldots, x_n)$, où $x_2, \ldots, x_n \in \mathbb{Z}^{n-1}$.

Sinon, on répète le processus.

De manière plus générale, on peut résoudre en utilisant l'algorithme présenté précédemment un système d'équations du type $AX = B$, avec $A \in \mathrm{M}_{m,n}(\mathbb{Z})$ et $B \in \mathbb{Z}^m$.

3.4.3. *Génération de* $\mathrm{GL}_n(A)$. A est toujours supposé euclidien.

Toute matrice de $\mathrm{GL}_n(A)$ est équivalente à l'identité : pour tout $A \in \mathrm{GL}_n(A)$, il existe deux matrices U et V, produits de matrices d'opérations élémentaires, vérifiant $UAV = \mathrm{I}_n$, *i.e.* $A = U^{-1}V^{-1}$.

$\mathrm{GL}_n(A)$ est donc engendré par les matrices d'opérations élémentaires (voir [**11**]).

3.4.4. *Méthode du pivot de Gauss.* On travaille sur un corps. On part de l'équation $MX = B$ et, en multipliant à gauche par des matrices d'opérations élémentaires, on obtient l'équation $TX = B'$, où la matrice T est triangulaire supérieure. On peut donc plus facilement trouver X.

On peut utiliser la même méthode pour inverser une matrice.

Citons également deux propositions que le lecteur démontrera en exercice ou pourra trouver dans [**5**].

PROPOSITION 49 (Décomposition LU). *Soit M une matrice carrée. Il existe une matrice L triangulaire inférieure et une matrice U triangulaire supérieure telles que $M = LU$ si et seulement si pour tout i, le mineur fondamental extrait de M de taille i (*i.e. *le déterminant de la sous-matrice contenant les i premières lignes et les i premières colonnes de M) est non nul.*

SI M admet une décomposition LU, il y a unicité de L et U à leur diagonale près : plus précisément, si $M = LU = L'U'$, alors il existe D diagonale telle que $L' = LD$ et $U' = D^{-1}U$.

PROPOSITION 50 (Décomposition de Cholesky). *Dans le cas réel, M est symétrique définie positive si et seulement si il existe une matrice triangulaire supérieure T telle que $M = {}^tTT$ si et seulement si pour tout i, le mineur fondamental extrait de M de taille i est strictement positif.*

La matrice T ainsi obtenue est unique si l'on impose à ses coefficients diagonaux d'être strictement positifs.

3.4.5. *Autres applications.* Calcul du rang, présentation de $\mathrm{GL}_2(\mathbb{Z})$, *etc.*

Bibliographie

[1] Y. Amice, *Les nombres p-adiques*, Collection SUP : Le Mathématicien, No. 14, Presses Universitaires de France, Paris, 1975.

[2] J.-M. Arnaudiès, *Les cinq polyèdres réguliers de* $\mathbb{R}^3$ *et leurs groupes*, Centre de documentation universitaire, Paris, 1969.

[3] M. Berger, *Géométrie*, 1990.

[4] A. Bouvier et D. Richard, *Groupes : observation, théorie, pratique*, Hermann, Paris, 1974.

[5] P. Ciarlet, *Introduction à l'analyse numérique matricielle et à l'optimisation*, Collection Mathématiques appliquées pour la maîtrise, Dunod, 1998.

[6] L. Comtet, *Analyse combinatoire*, Presses Universitaires de France, Paris, 1970.

[7] M. Demazure, *Cours d'algèbre*, 1997.

[8] R. Goblot, *Algèbre linéaire*, 1995.

[9] R.L. Graham, D.E. Knuth et O. Patashnik, *Concrete mathematics : a foundation for computer science*, Addison-Wesley, Reading, MA, 1989.

[10] R. Mneimné et F. Testard, *Introduction à la théorie des groupes de Lie classiques*, Hermann, Paris, 1986.

[11] D. Perrin, *Cours d'algèbre*, Ellipses, Paris, 1998.

[12] J.-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1970.