Algèbre L3B

Claire Amiot

Automne 2020

Table des matières

Groupes

Chapitre I

Généralités sur les groupes

1 Définition, premiers exemples

1.1 Loi de composition interne

Définition 1.1 Soit E un ensemble non vide. Une *loi de composition interne* $*$ sur E est la donnée d'une application

$$\begin{aligned} E \times E &\to E \\ (x, y) &\mapsto x * y \end{aligned}$$

. Elle est dite *associative* si pour tous x, y et z éléments de E, on a $(x*y)*z = x*(y*z)$.

Elle est dite *commutative* si pour tous x, y de E, on a $x*y = y*x$.

Exemple : $+$ et . sont des lci associatives et commutatives sur $\mathbb{N}$, $\mathbb{Z}$.

Définition 1.2 Soit $*$ un lci sur E. Un élément $e \in E$ est dit *neutre* pour $*$ si pour tout x de E, on a $e*x = x*e = x$.

Proposition 1.3
Si $*$ possède un neutre dans E, il est unique.

Définition 1.4 Soit $*$ une lci sur E de neutre e. Un élément $x \in E$ possède un *inverse* (ou *symétrique*) si il existe $x' \in E$ tel que $x*x' = x'*x = e$. on dit que x est *inversible*.

Proposition 1.5
Soit $*$ une lci associative, et e un élément neutre. Si x possède un inverse, il est unique. On le notera x^{-1}.
Si x est inversible, alors x^{-1} est inversible et on a $(x^{-1})^{-1} = x$.
Si x et y sont inversibles, alors $x*y$ aussi et on a $(x*y)^{-1} = y^{-1}*x^{-1}$.

Démonstration : Soient y et z deux éléments satisfaisant (G3), alors

$$\begin{aligned} y &= y*e && \text{par (G2)} \\ &= y*(x*z) && \text{par (G3)} \\ &= (y*x)*z && \text{par (G1)} \\ &= e*z && \text{par (G3)} \\ &= z && \text{par (G2).} \end{aligned}$$

□

1.2 Définition

Définition 1.6 Un *groupe* $(G,*)$ est un ensemble G muni d'une application (appelée *loi de composition interne*)

$$\begin{aligned} G \times G &\to G \\ (x,y) &\mapsto x*y \end{aligned}$$

telle que

(G1) pour tous x, y et z éléments de G, on a $(x*y)*z = x*(y*z)$ (la loi $*$ est *associative*) ;
(G2) il existe $e \in G$ tel que, pour tout $x \in G$, $x*e = e*x = x$;
(G3) pour tout $x \in G$ il existe $y \in G$ tel que $x*y = y*x = e$.

Lorsque la loi $*$ est aussi commutative (i.e. pour tous x, y dans G, $x*y = y*x$) alors le groupe G est dit *abélien*.

Exemple 1.7 — $(\mathbb{Z},+)$ est un groupe. Le neutre est 0, l'inverse de $x \in \mathbb{Z}$ est $-x$.

— $(\mathbb{N}, +)$ n'est pas un groupe. 0 est neutre, mais les éléments $\geqslant 1$ n'ont pas d'inverse.
— $(\mathbb{R}, +)$ est un groupe, mais $(\mathbb{R}, .)$ n'est pas un groupe. 1 est neutre pour tous les $x \neq 0$, mais $0.1 = 0 \neq 1$.
— $(\mathbb{R}^*, .)$ est un groupe. L'élément neutre est 1, l'inverse d'un $x \in \mathbb{R}$ est donné par $x^{-1} = \frac{1}{x}$. $(\mathbb{C}^*, .)$ est aussi un groupe.
— L'ensemble $\mathbb{N}$ muni de la loi $(x, y) \mapsto x^y$ n'est pas un groupe. La loi puissance n'est pas associative. $3^{(1^2)} = 3^1 = 3 \neq (3^1)^2 = 3^2 = 9$.

Tous ces exemples de groupes sont abéliens. (Attention loi puissance n'est pas non plus commutative $3^2 \neq 2^3$.)

Notation : Pour un groupe quelconque, on prend souvent la notation multiplicative, c'est-à-dire on note xy, ou $x.y$ au lieu de $x * y$. Dans ce cas, le neutre est noté 1_G ou 1. Si x est dans G et $n \in \mathbb{Z}$, on définit

$$\begin{aligned} x^n &= \underbrace{x.x.\ldots.x}_{n \text{ fois}} && \text{si } n \geqslant 1 \\ &= \underbrace{x^{-1}.x^{-1}.\ldots.x^{-1}}_{-n \text{ fois}} && \text{si } n \leqslant -1 \\ &= 1 && \text{si} n = 0 \end{aligned}$$

Attention, si G n'est pas commutatif, $(xy)^n \neq x^n y^n$ en général.

Lorsque G est abélien, on prend aussi souvent la notation additive, c'est-à-dire, on note $x + y$. Dans ce cas le neutre est noté 0_G ou 0 et l'inverse $-x$. Si x est dans G et $n \in \mathbb{N}$, on note nx l'élément $nx = \underbrace{x + x + \ldots + x}_{n \text{ fois}}$.

On peut noter G le groupe $(G, .)$ lorsque la loi est sous-entendue.

Proposition 1.8
Soit G un groupe. On a les propriétés suivantes

1. $\forall m, n \in \mathbb{Z}$, $\forall x \in G$, $x^{n+m} = x^n.x^m$,
2. $\forall x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.

Démonstration : laissée en exercice □

1.3 Groupes finis, table de multiplication

Définition 1.9 Lorsque l'ensemble G est fini, on dit que le groupe G est fini. Le cardinal de G est appelé *l'ordre* de G, il est noté $|G|$ ou $\sharp G$.

Soit $(G, .)$ un groupe fini de cardinal n. Notons $g_1, g_2, \dots g_n$ ses éléments. On peut alors écrire sa table de multiplication :

	g_1	g_2	g_3	$\cdots$	g_n
g_1	g_1^2	g_1g_2	g_1g_3	$\cdots$	g_1g_n
g_2	g_2g_1	g_2^2	g_2g_3	$\cdots$	g_2g_n
g_3	g_3g_1	g_3g_2	g_3^2	$\cdots$	g_3g_n
$\vdots$	$\vdots$				
g_n	g_ng_1	g_ng_2	g_ng_3	$\cdots$	g_n^2

La table de multiplication décrit entièrement la loi du groupe.

Exercice 1.10 Vérifier que la table suivante correspond à une loi d'un groupe à deux éléments :

	a	b
a	a	b
b	b	a

Montrer que la loi donnée par la table suivante n'est pas une loi de groupe :

	a	b
a	a	b
b	b	b

1.4 Exemples

1. Si E est un espace vectoriel (sur $\mathbb{R}$ ou $\mathbb{C}$), alors $(E, +)$ est un groupe, de neutre le vecteur nul. Par exemple $(\mathbb{R}^n, +)$ est un groupe, ou bien encore $(\mathbb{R}[X], +)$ ou $(\mathcal{M}_n(\mathbb{C}), +)$.
2. Pour $k = \mathbb{R}$ ou $\mathbb{C}$. Le groupe $(\mathrm{GL}_n(k), .)$ est un groupe non abélien.
3. Soit E un k-espace vectoriel, alors l'ensemble des applications linéaires bijectives de E dans E(ou endomorphismes inversibles de E) munie la loi de composition $\circ$ est un groupe. Le neutre de $(\mathrm{GL}(E), \circ)$ est l'application identité Id_E. C'est aussi un groupe non abélien.
4. Notons s_x la symétrie orthogonale par rapport à l'axe des x dans $\mathbb{R}^2$, s_y la symétrie orthogonale par rapport à l'axe des y, et s_0 la symétrie centrale de centre 0. Alors l'ensemble $\{Id_{\mathbb{R}^2}, s_x, s_y, s_0\}$ muni de la loi

de composition est un groupe fini. Sa table de multiplication est la suivante :

	I	s_x	s_y	s_0
I	I	s_x	s_y	s_0
s_x	s_x	I	s_0	s_y
s_y	s_y	s_0	I	s_x
s_0	s_0	s_y	s_x	I

5. Pour $p = 0, \dots 3$ notons r_p la rotation de centre 0 d'angle $\frac{p\pi}{2}$ dans $\mathbb{R}^2$. Alors l'ensemble $\{r_0, r_1, r_2, r_3\}$ muni de la composition est un groupe. Sa table de multiplication est la suivante :

	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

6. Soit E un ensemble fini, alors l'ensemble des bijections de E dans E muni de la loi de composition est un groupe. Il est non abélien dés que $\sharp E \geqslant 3$. Il est fini et son cardinal est $(\sharp E)!$. On l'appelle le *groupe des permutations* de E, ou le *groupe symétrique de E*. On l'étudiera plus en détail dans un autre chapitre.

2 Morphismes

2.1 Définition et exemples

Définition 2.1 Soient G et G' deux groupes. Un *morphisme* de G dans G' est une application $f : G \to G'$ telle que

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

Lorsque $G = G'$ on parle d'endomorphisme. Lorsque f est inversible (c'est-à-dire qu'il existe un morphisme de groupe $h : G' \to G$ tel que $f \circ h = \mathrm{Id}_{G'}$ et $h \circ f = \mathrm{Id}_G$, on parle d'*isomorphisme*. Et si de plus $G = G'$ f est appelé *automorphisme*.

Lemme 2.2
Soit f un morphisme de G dans G'. Alors on a les propriétés :

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

Démonstration : Exercice. □

Proposition 2.3
Soit $\varphi : G \to H$ et $\psi : H \to K$ deux morphismes de groupes, alors $\psi \circ \varphi : G \to K$ est un morphisme de groupes.

Démonstration : Soit x, y dans G, alors on a

$$\psi \circ \varphi(xy) = \psi(\varphi(x).\varphi(y)) = (\psi \circ \varphi(x)).(\psi \circ \varphi(y)).$$

□

Proposition 2.4
Un morphisme de groupe est un isomorphisme si et seulement si il est bijectif.

Démonstration : Il est clair que si f est inversible, alors elle est bijective. Supposons f bijective et notons h la bijection réciproque. Il faut montrer que h est un morphisme. Soient $x', y' \in G'$, notons $x = h(x')$ et $y = h(y')$, tels que $x' = g(x)$ et $y' = g(y)$. On a donc

$$h(x'y') = h(g(x)g(y)) = h(g(xy)) = xy = h(x')h(y').$$

□

La notion d'isomorphisme est primordiale. Lorsqu'on se donne un groupe G, on veut comprendre sa structure "à isomorphisme près", c'est à dire à quel groupe "connu" il est isomorphe.

Exemple 2.5

1. Soit $p \in \mathbb{Z}$. La multiplication par p est un morphisme de $\mathbb{Z}$ dans lui même. Ce n'est pas un isomorphisme sauf si $p = \pm 1$.
2. $\exp : \mathbb{R} \to \mathbb{R}^*$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, .)$.
3. L'application déterminant est un morphisme de $\mathrm{GL}_n(k)$ dans $(k^*, .)$.
4. La conjugaison $(z \mapsto \overline{z})$ est un automorphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}, +)$ et de $(\mathbb{C}^*, .)$ dans $(\mathbb{C}^*, .)$.
5. Soit G le groupe des rotations défini dans le paragraphe 1. L'application $G \to \mathcal{U}_4$ qui à r_p associe $e^{\frac{pi\pi}{2}}$ pour $p = 0, \ldots, 3$ est un isomorphisme de groupe.
6. Soit G un groupe, et $x \in G$. L'application $n \mapsto x^n$ est un morphisme de $\mathbb{Z}$ dans G.
7. Soit E un espace vectoriel de dimension n. Chaque choix de base de E donne un isomorphisme de $\mathrm{GL}(E)$ dans $\mathrm{GL}_n(k)$.
8. Soit G un groupe, et $g \in G$. Alors l'application $\phi_g : G \to G$ définie par

$$\phi_g(x) := gxg^{-1}$$

est un automorphisme de G. Il est appelé *conjugaison par g*.

2.2 Noyau et image

Définition 2.6 Soient G et G' deux groupes et soit f un morphisme de G dans G'. Alors on définit

— le *noyau* de f $\mathrm{Ker} f := \{x \in G \text{ t.q. } f(x) = 1_{G'}\} \subset G$.

— l'*image* de f $\mathrm{Im}\, f := \{f(x), x \in G\} \subset G'$.

Exemple 2.7

1. Le noyau de la multiplication par p est $\{0\}$. Son image est $p\mathbb{Z}$.
2. $\mathrm{Ker} \exp = \{0\}$, et $\mathrm{Im} \exp =]0, +\infty[$
3. $\mathrm{Ker} \det = \{M \in \mathrm{GL}_n,\ \det M = 1\}$, $\mathrm{Im} \det = k^*$.

Lemme 2.8
Un morphisme f entre deux groupes G et G' est injectif si et seulement si $\mathrm{Ker} f = \{1_{G'}\}$.

Démonstration : Supposons f injectif. Soit $x \in \mathrm{Ker} f$, alors $f(x) = 1_{G'} = f(1_G)$. Donc $x = 1_G$.

Supposons maintenant que $\mathrm{Ker} f = \{1_{G'}\}$. Soient x et y dans G tels que $f(x) = f(y)$. Alors on a

$$1_{G'} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

donc xy^{-1} est dans $\mathrm{Ker} f$. Par hypothése, on a donc $xy^{-1} = 1_G$, c'est-à-dire $x = y$. □

3 Sous-groupes

3.1 Définition

Définition 3.1 Soit $(G, .)$ un groupe. Un sous-ensemble $H \subset G$ de G est un *sous-groupe* de G si les trois conditions suivantes sont vérifiées :

(SG1) $e \in H$;
(SG2) $\forall x, y \in H \quad x.y \in H$ (H est stable par la loi de groupe de G) ;
(SG3) $\forall x \in H \quad x^{-1} \in H$ (H est stable par passage à l'inverse).

En d'autres termes, $(H, .)$ est un groupe.

Il est facile de voir que si G est un groupe, alors G et $\{1_G\}$ sont des sous-groupes de G (appelés sous-groupes triviaux).

Remarque 3.2 Soit $(G, .)$ un groupe et $H \subset G$. Alors H est un sous-groupe de G si et seulement si $e \in H$ et pour tous $x, y \in H$, $x.y^{-1} \in H$.

Proposition 3.3
Soit $f : G \to G'$ un morphisme de groupes.

1. Soit H un sous-groupe de G, alors $f(H) = \{f(h),\ h \in H\}$ est un sous-groupe de G'. En particulier $\mathrm{Im}\, f$ est un sous-groupe de G'.
2. Soit H' un sous-groupe de G' Alors $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ est un sous-groupe de G. En particulier $\mathrm{Ker} f$ est un sous-groupe de G

Démonstration : à faire plus tard. □

3.2 Exemples

1. $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, il est isomorphe à $\mathbb{Z}$.
2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$ qui est lui même un sous-groupe de $(\mathbb{C}, +)$.
3. $(]0, +\infty[, .)$, ainsi que $(\{1, -1\}, .)$ sont des sous-groupes de $(\mathbb{R}^*, .)$, $]0, +\infty[$ est l'image du morphisme exponentielle.
4. L'ensemble $\mathcal{U} = \{z \in \mathbb{C} \text{ tel que } ||z|| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, .)$.
5. Soit $n \in \mathbb{N}^*$. L'ensemble $\mathcal{U}_n = \{z \in \mathbb{C} \text{ tel que } z^n = 1\}$ des racines $n$iémes de l'unité est un sous-groupe de $\mathcal{U}$ et donc de $(\mathbb{C}^*, .)$.
6. L'ensemble $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \text{ tel que } \det M = 1\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, c'est le noyau du déterminant.
7. L'ensemble $\{M \in \mathrm{GL}_n(\mathbb{R}) \text{ tel que } {}^tM.M = I_n\}$ muni de la loi de multiplication est un groupe.
8. Soit G un groupe, alors $Z(G) = \{z \in G,\ \forall g \in G gz = zg\}$ est un sous-groupe de G appelé le centre de G. Le groupe G est abélien si et seulement si $Z(G) = G$. Le centre de $\mathrm{GL}_n(k)$ est l'ensemble des matrices de la forme λI_n avec $\lambda \in k^*$ (preuve ?).

La conjugaison étant un morphisme de groupe, on en déduit :

Proposition 3.4
Soit H un sous-groupe d'un groupe G. Alors pour tout $x \in G$, $xHx^{-1} = \{xhx^{-1},\ h \in H\}$ est un sous-groupe de G.

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

Théorème 3.5
Tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$.

Démonstration : Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Supposons $H \neq \{0\}$. Soit $x \neq 0 \in H$. Alors x et $-x$ sont dans H, donc H contient des entiers strictement positifs. Notons n le plus petit entier $\geqslant 1$ contenu dans H. On va montrer que $n\mathbb{Z} = H$.

Tout d'abord, pour tout $p \in \mathbb{N}$, $pn = n + n + \ldots + n \in H$ et $-pn = -(pn) \in H$ donc $n\mathbb{Z} \subset H$.

Soit maintenant $x \in H$. Ecrivons la division euclidienne de x par n, $x = nq + r$ avec $0 \leqslant r \leqslant n - 1$. Alors

$$r = \underbrace{x}_{\in H} - \underbrace{nq}_{\in n\mathbb{Z} \subset H} \in H.$$

Par minimalité de n, on a donc $r = 0$, c'est-à-dire $x = nq \in n\mathbb{Z}$. □

3.4 Sous-groupes engendrés

Proposition 3.6
Soit G un groupe et H_1 et H_2 deux sous-groupes de G, alors $H_1 \cap H_2$ est un sous-groupe de G.

Plus généralement, si I est un ensemble, et qu'on a pour tout $i \in I$ un sous-groupe H_i de G, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration : Exercice. □

Attention, $H_1 \cup H_2$ n'est en général pas un sous-groupe de G.

Proposition 3.7
Soit $p, q \in \mathbb{N}$ alors $p\mathbb{Z} \cap q\mathbb{Z} = \text{ppcm}(p, q)\mathbb{Z}$.

Définition 3.8 Soit X un sous-ensemble d'un groupe G. Alors on appelle *sous-groupe engendré* par X l'intersection de tous les sous-groupes de G contenant X. C'est un sous-groupe par la proposition 3.6. Il est noté $\langle X \rangle$.

Proposition 3.9

— Le sous-groupe $\langle X \rangle$ est le plus petit sous-groupe de G contenant X, c'est-à-dire que si K est un sous-groupe de G qui contient X alors $\langle X \rangle \subset K$.

— $x \in \langle X \rangle$ si et seulement si il existe $x_1, \ldots, x_n \in X$ tels que $x = x_1^{\pm 1} \ldots x_n^{\pm}$.

Proposition 3.10

Soit $p, q \in \mathbb{N}$ alors $\langle p, q \rangle = \text{pgcd}(p, q)\mathbb{Z}$.

Exemple 3.11

1. $\langle G \rangle = G$. $\langle e \rangle = \{e\}$
2. $\mathcal{U}_n = \langle e^{\frac{2i\pi}{n}} \rangle$.
3. $\mathbb{Z} = \langle 1 \rangle$.
4. $G = \langle r_1 \rangle$ dans l'exemple 5 du paragraphe 1.
5. $G = \langle s_x, s_y \rangle$ dans l'exemple 4 du paragraphe 1.

3.5 Groupes cycliques, ordre d'un élément

Définition 3.12 Un (sous-)groupe G est dit *monogène* s'il est engendré par un seul élément.

Un (sous-)groupe monogène et fini est dit *cyclique*.

Exemple 3.13 $\mathbb{Z}$ est une groupe monogène infini. $\mathcal{U}_n$ est un groupe cyclique.

Définition 3.14 Soit $a \in G$. Si il existe $n \in \mathbb{N}$ tel que $a^n = e$, alors a est dit *d'ordre fini*. L'*ordre* de a est le plus petit entier strictement positif n tel que $a^n = e$.

Proposition 3.15

Soit G un groupe et $x \in G$. On a les propriétés suivantes

1. $\langle x \rangle = \{x^n,\ n \in Z\}$.
2. $\langle x \rangle$ est un sous-groupe abélien.

3. Soit $p \geqslant 1$ l'ordre de x, et soit $n \in \mathbb{Z}$ tel que $x^n = e$. Alors p divise n.
4. $\langle x \rangle$ est fini, si et seulement si x est d'ordre fini. Dans ce cas $\langle x \rangle = \{e, x, x^2, \ldots, x^{p-1}\}$ où p est l'ordre de x, et l'ordre de $\langle x \rangle$ est p.

Démonstration :

1. $x \in \langle x \rangle$, donc $x^n \in \langle x \rangle$ pour tout $n \in \mathbb{Z}$. Donc $\{x^n,\ n \in Z\} \subset \langle x \rangle$. De plus il est clair que $\{x^n,\ n \in Z\}$ est un sous-groupe de G. Donc on a bien égalité.
2. $x^p x^q = x^{p+q} = x^{q+p} = x^q x^p$.
3. Soit $n = pq + r$ la division euclidienne de n par p. Alors $e = x^n = x^{pq+r} = (x^p)^q.x^r = x^r$. Or $0 \leqslant r \leqslant p-1$, comme p est le plus petit entier strictement positif vérifiant $x^p = e$, on a nécessairement $r = 0$. Autrement dit p divise n.
4. Si $\langle x \rangle$ est fini, il existe des entiers $p \neq q$ tels que $x^p = x^q$. Supposons $p > q$. Alors on a $x^{p-q} = x^p x^{-q} = x^q x^{-q} = 1_G$. Donc x est d'ordre fini. Réciproquement, soit x d'ordre fini. Notons p son ordre. On va montrer que $\langle x \rangle = \{e, x, x^2, \ldots, x^{p-1}\}$, ce qui entrainera la finitude de $\langle x \rangle$. Par 1., il suffit de montrer que $x^n \in \{e, x, x^2, \ldots, x^{p-1}\}$ pour tout $n \in \mathbb{Z}$. Soit $n \in \mathbb{Z}$ et notons r le reste de la division euclidienne de n par p. Alors $n = pq + r$ avec $0 \leqslant r \leqslant p-1$. On a alors $x^n = x^{pq+r} = (x^p)^q.x^r = e^q.x^r = x^r$. Autrement dit, $x^n \in \{e, x, x^2, \ldots, x^{p-1}\}$.
   Vérifions maintenant que tous ces éléments sont différents. Si $x^i = x^j$, alors $x^{i-j} = e$, donc p divise $i - j$. Si $0 \leqslant i, j \leqslant p-1$, cela implique $i - j = 0$.

□

4 Construction de nouveaux groupes à partir de groupes

4.1 Produit de groupes

Proposition 4.1
Soit $(G_1, \bullet)$ et $(G_2, \star)$ deux groupes. Alors on peut munir $G_1 \times G_2$ d'une structure de groupe en posant $(x_1, x_2) * (y_1, y_2) := (x_1 \bullet y_1, x_2 \star y_2)$ pour tous $x_1, y_1 \in G_1$ et $x_2, y_2 \in G_2$.

Le groupe $G_1 \times G_2$ est appelé le *produit direct* de G_1 par G_2.
On vérifie facilement les choses suivantes :

— L'élément neutre de $G_1 \times G_2$ est $(1_{G_1}, 1_{G_2})$.
— L'inverse de (x_1, x_2) est (x_1^{-1}, x_2^{-1}).
— L'inclusion $G_1 \to G_1 \times G_2$ envoyant g_1 sur $(g_1, 1_{G_2})$ est un morphisme de groupe injectif dont l'image est isomorphe à G_1.
— La projection $p_1 : G_1 \times G_2 \to G_1$ est un morphisme surjectif de groupes dont le noyau est isomorphe à G_2.
— Le groupe $G_1 \times G_2$ est fini si et seulement si G_1 et G_2 sont finis, et dans ce cas $|G_1 \times G_2| = |G_1|.|G_2|$.
— Le groupe $G_1 \times G_2$ est abélien si et seulement si G_1 et G_2 le sont.

Démonstration :Exercice. □

Exemple 4.2 Le groupe $(\mathbb{R}^2, +)$ est le produit direct de $(\mathbb{R}, +)$ par $(\mathbb{R}, +)$.

4.2 Groupe de fonctions

Proposition 4.3
Soit X un ensemble et $(G, .)$ un groupe. Alors l'ensemble G^X des applications de X dans G est un groupe pour la loi $*$ définie par : $(\phi * \psi)(x) := \phi(x).\psi(x)$ pour tout $\phi, \psi \in G^X$ et tout $x \in X$.

On vérifie aussi le propriétés suivantes :

— L'élément neutre de G^X est l'application qui à tout $x \in X$ associe 1_G.
— L'inverse de $\phi \in G^X$ est l'application ψ telle que $\psi(x) = \phi(x)^{-1}$ pour tout $x \in X$.
— Si G est abélien, alors G^X est aussi abélien.

Démonstration : Tout d'abord $*$ est bien une loi interne pour G^X au sens où si ϕ et ψ sont des applications de X dans G alors $\phi * \psi$ définit bien une application de X dans G.

Vérifions les propriétés $(G1)$, $(G2)$ et $(G3)$ pour $(G^X, *)$.

(G1) Soient ϕ ,ψ et η dans G^X. Alors pour tout $x \in X$ on a

$$\begin{aligned}((\phi * \psi) * \eta)(x) &= (\phi * \psi)(x).\eta(x) && \text{par définition de } *\\ &= (\phi(x).\psi(x)).\eta(x)\\ &= \phi(x).(\psi(x).\eta(x)) && \text{par associativité de } *\\ &= \phi(x).(\psi * \eta)(x)\\ &= (\phi * (\psi * \eta))(x)\end{aligned}$$

Ceci étant vrai pour tout $x \in X$, on a bien $(\phi * \psi) * \eta = \phi * (\psi * \eta)$ comme applications.

(G2) Notons e l'application $x \mapsto 1_G$. Soit $\phi \in G^X$, alors on a pour tout $x \in X$

$$(\phi.e)(x) = \phi(x).e(x) = \phi(x).1_G = \phi(x),$$

c'est-à-dire $\phi.e = \phi$. De même $e.\phi = \phi$. Donc e est bien un élément neutre pour $(G^X, *)$.

(G3) Soit $\phi \in G^X$. Notons ψ l'application de X dans G qui à x associe $\phi(x)^{-1}$. Alors on a pour tout $x \in X$

$$(\phi * \psi)(x) = \phi(x).\psi(x) = \phi(x).\phi(x)^{-1} = 1_G = e(x),$$

c'est-à-dire $\phi * \psi = e$. De même $\psi * \phi = e$. L'application ϕ admet donc un inverse.

□

Exemple 4.4 Soit X un ensemble, alors $(\mathcal{F}(X, \mathbb{R}), +)$ est un groupe.

Si X est réduit à un élément, alors G^X est canoniquement isomorphe à G. Si $X = \{1, \ldots, n\}$ alors G^X est canoniquement isomorphe à $G^n = G \times G \times \cdots \times G$.

Soit E et F des espaces vectoriels, alors $\mathcal{L}(E, F)$ est un sous-groupe de F^E.

$(\mathcal{C}(\mathbb{R}, \mathbb{R}), +)$ est un sous-groupe de $\mathbb{R}^{\mathbb{R}}$.

4.3 Groupes d'automorphismes

Proposition 4.5
Soit G un groupe. On considère l'ensemble des automorphismes $\mathrm{Aut}(G)$ (donc des isomorphismes de groupes $G \to G$) muni de la loi de composition. Alors $(\mathrm{Aut}(G), \circ)$ est un groupe.

Démonstration : Il est plus simple de montrer que c'est un sous-groupe de $\mathrm{Bij}(G)$. Pour cela, on doit vérifier que l'inverse d'un isomorphisme de groupe est un isomorphisme de groupes, et que la composition de deux isomorphismes de groupe est un isomorphismes de groupes, ce qui est aussi déjà fait. □

Rappelons que si $x \in G$, on peut définir la conjugaison par x qui est un automorphisme de G dans G. Un tel automorphisme est appelé un automorphisme intérieur. On peut alors vérifier que $\mathrm{Inn}(G)$ est un sous-groupe de $\mathrm{Aut}(G)$.

Chapitre II

Groupes quotients, cas abélien

1 Relations d'équivalence

1.1 Définition

Définition 1.1 Soit E un ensemble. Une *relation* $\mathcal{R}$ sur E est la donnée d'un sous-ensemble de $P_{\mathcal{R}} \subset E \times E$. On notera $x\mathcal{R}y$ pour tout couple $(x, y) \in P_{\mathcal{R}}$, et on dira que x est en relation avec y.

Définition 1.2 Soit E un ensemble. Un relation $\mathcal{R}$ sur E est appelée *relation d'équivalence* si elle vérifie les propriétés suivantes :

1. $\mathcal{R}$ est *réflexive*, c'est-à-dire $x\mathcal{R}x$ pour tout $x \in E$;
2. $\mathcal{R}$ est *symétrique*, c'est-à-dire $x\mathcal{R}y$ si et seulement si $y\mathcal{R}x$;
3. $\mathcal{R}$ est *transitive*, c'est -à-dire si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.

Exemple 1.3
— L'égalité est une relation d'équivalence correspondant au sous-ensemble $\{(s, s) \mid s \in E\} \subset E \times E$.
— Soit $E = \mathbb{Z} \times \mathbb{N}^*$. La relation $(p, q)\mathcal{R}(p', q')$ si et seulement si $pq' = p'q$ est une relation d'équivalence.
— Soit $E = \mathbb{Z}$ et $p \in Z$. La relation définie par $m\mathcal{R}n$ si et seulement si $m - n$ est divisible par p est une relation d'équivalence. On note $m = n \bmod p$ ou $m = n\ [p]$.
— Soit $f : E \to E'$ une application d'ensembles. Alors on définit $x \sim y$ si et seulement si $f(x) = f(y)$. C'est une relation d'équivalence. Les 3 exemples ci-dessus sont de cette forme. Dans le premier $f = Id_E$. Dans le deuxiéme $E' = \mathbb{Q}$ et $f(p, q) = \frac{p}{q}$ et dans le troisiéme, $E' = \{0, 1, \ldots, p-1\}$ et f est l'application qui à un entier n associe le reste de la division euclidienne de n par p. on verra ensuite que toutes les relations d'équivalence sont de cette forme.

1.2 Classes d'équivalence

Définition 1.4 Soit $\mathcal{R}$ une relation d'équivalence sur E. Soit $x \in E$, la *classe d'équivalence* de x est le sous-ensemble $\{y \in E \mid x\mathcal{R}y\}$ souvent noté C_x ou $\overline{x}$.

Tous les éléments de C_x sont appelés *représentants* de la classe de x.

Exemple 1.5
— Pour l'égalité, on a $\overline{x} = \{x\}$ pour tout $x \in E$.
— $\overline{(p,q)} = \{(p',q') \in \mathbb{Z} \times \mathbb{N}^* \mid \frac{p}{q} = \frac{p'}{q'}\}$
— $\overline{m} = \{n \in \mathbb{Z} \mid m - n \in p\mathbb{Z}\} = \{m + kp \; k \in \mathbb{Z}\} = m + p\mathbb{Z}$.
Si $p = 2$ alors $C_0 = 2\mathbb{Z} = \mathcal{P}$ l'ensemble des nombres pairs, et on a

$$C_0 = C_2 = C_4 = C_{-2} = \ldots = C_{2k} \text{ pour tout } k \in \mathbb{Z}$$

De plus $C_1 = 1 + 2\mathbb{Z} = \mathcal{I}$ est l'ensemble des nombres d'impairs, et on a

$$C_1 = C_{2k+1} \text{ pour tout } k \in \mathbb{Z}$$

Lemme 1.6
Soit $\mathcal{R}$ un relation d'équivalence sur E. Alors pour tout $x \in E$ on a $x \in C_x$. De plus on a

$$x\mathcal{R}y \;\Leftrightarrow y \in C_x \;\Leftrightarrow x \in C_y \;\Leftrightarrow C_x = C_y.$$

Théorème 1.7
Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Alors on a les propriétés suivantes :

1. Pour tous x, y dans E, les classes C_x et C_y sont soit disjointes ($C_x \cap C_y = \emptyset$) soit égales.
2. L'ensemble E est l'union des classes d'équivalences pour la relation $\mathcal{R}$.

On dit que l'ensemble des classes d'équivalence de $\mathcal{R}$ forme une *partition* de E.

Démonstration :

1. Soient $x, y \in E$ tels que $C_x \cap C_y \neq \emptyset$. Alors il existe $z \in C_x$ et $z \in C_y$, autrement dit, $x\mathcal{R}z$ et $y\mathcal{R}z$. Par symétrie, $z\mathcal{R}y$, et par transitivité $x\mathcal{R}y$ donc $C_x = C_y$.
2. On a $x \in C_x$ pour tout x de E, donc $E = \bigcup_{x \in E} C_x$.

Exemple 1.8 $\mathbb{Z} = \mathcal{P} \cup \mathcal{I}$. Pour $p = 3$, on a 3 classes d'équivalences distinctes qui sont C_0, C_1 et C_2 et on a bien $\mathbb{Z} = C_0 \cup C_1 \cup C_2$.

□

2 Quotient par une relation d'équivalence

2.1 Ensemble quotient

Définition 2.1 Soit E un ensemble et $\sim$ une relation d'équivalence sur E. Le quotient de E par $\sim$ est l'ensemble des classes d'équivalence de E. Il est noté $E/\sim$.

L'application $p : E \to E/\sim$ qui à x associe C_x est appelée *projection canonique associée à* $\sim$. Elle est surjective.

Exemple 2.2
— Pour l'égalité, on a $E/== \{\{x\}, x \in E\}$, la projection canonique est une bijection entre E et $E/=$.
— On a $\mathbb{Z} \times \mathbb{N}^*/\mathcal{R}$ est en bijection avec $\mathbb{Q}$. (exercice)
— Soit $p \in \mathbb{Z}$ et la relation définie précédemment. Alors on a $\mathbb{Z}/\sim = \{C_0, C_1, \ldots, C_{p-1}\}$. Le cardinal de $\mathbb{Z}/\sim$ est p.

2.2 Théorème de factorisation

Théorème 2.3
Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$, on note $p : E \to E/\mathcal{R}$ la projection canonique. Soit $f : E \to E'$ une application d'ensemble. Alors on a les équivalences

1. il existe $\bar{f} : E/\mathcal{R} \to E'$ telle que $f = \bar{f} \circ p$;
2. $\forall x, y \in E$, $x\mathcal{R}y \Rightarrow f(x) = f(y)$.

Dans ce cas, $\bar{f}$ est unique.

Démonstration : Supposons que $f = g \circ p$ pour une certaine application $g : E/\sim \to E'$. Alors si $x \sim y$, on a $C_x = C_y$ donc $p(x) = p(y)$. D'où $f(x) = g \circ p(x) = g \circ p(y) = f(y)$.

Récirpoquement, supposons que si $x \sim y$ alors $f(x) = f(y)$. Soit $C \in E/\sim$. Alors $C = C_x$ pour un $x \in E$. On pose $g(C) := f(x)$. Il faut vérifier que c'est bien une application. En effet si $C = C_y$, alors $C_x = C_y$, donc $x \sim y$, donc par hypothése $f(x) = f(y)$, la valeur $g(C)$ est donc bien définie. □

Exercice 2.4 Soit $f : E \to F$ une application d'ensemble et soit $\mathcal{R}$ la relation d'équivalence définie par $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$. Montrer qu'il existe $\overline{f} : E/\mathcal{R} \to F$ telle que $f = \overline{f} \circ p$. Montrer que $\overline{f}$ est injective.

3 Equivalences dans les groupes

3.1 Classes à gauche

Définition 3.1 Soit G un groupe et H un sous-groupe de G. Alors on définit la relation d'équivalence sur G

$$x \sim y \;\Leftrightarrow\; x^{-1}y \in H.$$

Vérifions d'abord que c'est bien une relation d'équivalence. $x^{-1}x = e \in H$, donc $\sim$ est réflexive. Ensuite si $\sim y$ alors $x^{-1}y \in H$. Comme H est un sous-groupe, $(x^{-1}y)^{-1} = y^{-1}x \in H$, c'est-à-dire que $y \sim x$, donc $\sim$ est symétrique. Enfin si $x \sim y$ et $y \sim z$, alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ car H est stable par multiplication, donc $\sim$ est transitive.

On voit alors facilement que la classe d'un élément x pour cette relation d'équivalence est donnée par $\overline{x} = xH$. En effet,

$$\begin{aligned} y \in \overline{x} &\Leftrightarrow x^{-1}y \in H \\ &\Leftrightarrow \exists\, h \in H \text{ tel que } x^{-1}y = h \\ &\Leftrightarrow \exists\, h \in H \text{ tel que } y = xh \\ &\Leftrightarrow y \in xH. \end{aligned}$$

On appelle les classes xH, les *classes à gauche* suivant H. On note G/H l'ensemble quotient $G/\sim$.

On peut aussi définir les *classes à droite* en prenant la relation d'équivalence $x \sim y \Leftrightarrow yx^{-1} \in H$, l'ensemble quotient se note $H\backslash G$.

3.2 Théorème de Lagrange

Théorème 3.2 (Lagrange)
Soit G un groupe fini et H un sous-groupe de G. L'ordre de H divise l'ordre de G. Plus précisément on a $\sharp H.\sharp(G/H) = \sharp G$.

Démonstration : Par la section précédente, G est l'union disjointe des classes à gauches. On va montrer le lemme suivant :

Lemme 3.3
Pour tout $x \in G$, on a $|xH| = |H|$.

On a l'égalité des cardinaux car la multiplication à gauche par x donne un bijection de H dans xH (la bijection réciproque est la multiplication à gauche par x^{-1}.)

Revenons maintenant au théorème. Toutes les classes à gauche ont le même cardinal $\sharp H$ par le lemme. De plus le nombre de classe à gauche est exactement $\sharp(G/H)$. Donc on a bien $\sharp H.\sharp(G/H) = \sharp G$. □

On notera $[G : H]$ le cardinal de G/H, c'est *l'indice* de H dans G. Notons qu'il peut être fini même si G et H ne sont pas fini, par exemple $G = \mathbb{Z}$ et $H = n\mathbb{Z}$.

Corollaire 3.4
Soit x un élément d'ordre n dans un groupe fini G. Alors n divise l'ordre de G.

Si en particulier l'ordre de G est fini égal à m alors pour tout x dans G on a $x^m = 1$.

Démonstration : On a vu dans Proposition 3.15 que dans ce cas l'ordre de $\langle x \rangle$ est n. Donc on a le résultat par le théoréme précédent. □

Corollaire 3.5
Soit $G \neq \{e\}$ un groupe fini d'ordre p avec p premier. Alors G est cyclique et tout $x \neq e$ engendre G.

En particulier, tout groupe fini d'ordre p avec p premier est abélien.

Démonstration : Soit x un élément de G. Alors comme G est fini, $\langle x \rangle$ est aussi fini, donc x est d'ordre fini q par Proposition 3.15. Cet ordre q divise p qui est premier, donc on a $q = 1$ ou $q = p$. Si $q = 1$ alors $x = x^1 = e$. Sinon, $x \neq e$, et $\langle x \rangle$ est un sous-groupe de G d'ordre p. Donc on a $\langle x \rangle = G$ qui est cyclique. □

4 Quotients de groupes abéliens

Dans toute cette section, les groupes sont abéliens. On notera donc $+$ pour la loi et 0_G pour le neutre.

4.1 Construction d'une loi sur le quotient

Soit $(G, +)$ un groupe abélien et H un sous-groupe. On va définir une loi sur l'ensemble des classes à gauches G/H par

$$\forall x, y \in G \ \overline{x} + \overline{y} := \overline{x + y}.$$

Vérifions tout d'abord que cette loi est bien définie, en effet il faut vérifier que si on prend d'autres représentants de la classe $\overline{x}$ et de la classe $\overline{y}$, on obtient bien la même classe $\overline{x + y}$. Soit x' un autre représentant de $\overline{x}$ et y' un autre représentant de $\overline{y}$. Alors par définition on a $x - x' \in H$ et $y - y' \in H$. On veut vérifier que $\overline{x' + y'} = \overline{x + y}$, c'est-à-dire que $(x + y) - (x' + y') \in H$. C'est vrai car par **commutativité** de la loi $+$ de G on a

$$(x + y) - (x' + y') = \underbrace{(x - x')}_{\in H} + \underbrace{(y - y')}_{\in H} \in H$$

La loi $+$ est donc bien définie sur G/H.

Maintenant on a

$$\begin{aligned}(\overline{x}+\overline{y})+\overline{z} &= \overline{x+y}+\overline{z}\\ &= \overline{(x+y)+z}\\ &= \overline{x+(y+z)}\\ &= \overline{x}+\overline{y+z} = (\overline{x}+\overline{y})+\overline{z}\end{aligned}$$

Donc la loi est bien **associative**.

La loi est aussi **commutative** car $\overline{x}+\overline{y} = \overline{x+y} = \overline{y+x} = \overline{y}+\overline{x}$.

L'**élément neutre** est $\overline{0_G}$. En effet $\overline{x}+\overline{0_G} = \overline{x+0_G} = \overline{x}$.

L'**inverse** est donné par $-\overline{x} = \overline{-x}$ car $\overline{x}+\overline{-x} = \overline{x-x} = \overline{0_G}$.

Finalement, on a démontré le théorème suivant.

Théorème 4.1
Soit $(G,+)$ un groupe abélien, et H un sous-groupe de G. Alors $(G/H,+)$ est un groupe abélien.

Remarque 4.2 Notons qu'ici comme le groupe est abélien, on a $x+H = H+x$ c'est-à-dire que les classes à gauche sont égales aux classes à droites.

Si G n'est pas abélien, il est aussi possible de définir une loi de groupe sur G/H pour des sous-groupes H tels que les classes à gauche sont égales aux classes à droite.

Exemple 4.3 Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ a un structure de groupe. Il est commutatif et cyclique (engendré par $\overline{1}$).

4.2 Théorème de factorisation

Notons tout d'abord une propriété pour la projection.

Proposition 4.4
Soit G un groupe abélien et H un sous-groupe, alors $p : G \to G/H$ la projection canonique est un morphisme de groupes.

Démonstration : Par définition on a $p(x+y) = \overline{x+y} = \overline{x} + \overline{y} = p(x) + p(y)$, donc p est un morphisme de groupe. □

On a alors un analogue du Théorème 2.3.

Théorème 4.5
Soit G un groupe abélien et H un sous-groupe, on note $p : G \to G/H$ la projection canonique sur les classes à gauche. Soit $f : G \to G'$ un morphisme de groupe. Alors on a les équivalences

1. il existe $\bar{f} : G/H \to G'$ telle que $f = \bar{f} \circ p$;
2. $H \subset \mathrm{Ker} f$.

De plus l'application $\bar{f}$ est un morphisme de groupes qui est injectif si et seulement si $H = \mathrm{Ker} f$.

Démonstration :

Supposons qu'il existe un morphisme $g : G/H \to G'$ tel que $f = g \circ p$. Soit $x \in H$, alors $\overline{x} = \overline{0_G}$. Donc on a $f(x) = g \circ p(x) = g(\overline{x}) = g(\overline{0_G}) = e_{G'}$ car g est un morphisme de groupe. D'où $x \in \mathrm{Ker} f$.

Supposons maintenant que $H \subset \mathrm{Ker} f$. Si $x - y \in H$ alors $x - y \in Ker f$, c'est-à-dire $f(x-y) = e_{G'}$. Comme f est un morphisme, $f(x).f(y)^{-1} = e_{G'}$, donc $f(x) = f(y)$. Alors par le lemme de factorisation (Lemme **??**), il existe $g : G/H \to G'$ tel que $p \circ g = f$. Il faut vérifier que g est un morphisme de groupe. Soient $\overline{x}, \overline{y} \in G/H$. Alors

$$\begin{aligned}
g(\overline{x} + \overline{y}) &= g(p(x) + p(y)) \\
&= g \circ p(x+y) && \text{car } p \text{ est un morphisme} \\
&= f(x+y) \\
&= f(x).f(y) && \text{car } f \text{ est un morphisme} \\
&= g(p(x)).g(p(y)) \\
&= g(\overline{x}) g(\overline{y})
\end{aligned}$$

Donc g est un morphisme. □

Corollaire 4.6
Soit G un groupe abélien et $f : G \to G'$ un morphisme de groupes. Alors on a un isomorphisme $G/\mathrm{Ker}f \simeq \mathrm{Im}\, f$.

Notons que même si G' n'est pas abélien, $\mathrm{Im}\, f$ est toujours abélien si G l'est.

5 Les groupes cycliques

5.1 Groupes monogènes

Théorème 5.1
1. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$
2. Tout groupe cyclique d'ordre $n \geqslant 1$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration :

1. Soit $G = \langle x \rangle$ un groupe monogène infini. Notons $\phi : \mathbb{Z} \to G$ l'application qui à n associe x^n. C'est un morphisme de groupe car $x^{m+n} = x^m x^n$. Il est surjectif car x engendre G. Montrons qu'il est injectif. Supposons qu'on ait $x^n = x^m$ avec $n > m$, alors $x^{n-m} = 1$, et donc x est d'ordre fini, mais alors $\langle x \rangle$ est d'ordre fini ce qui est un contradiction.
2. Supposons que $G = \langle x \rangle$ ait cardinal n.
   On va montrer que l'application$\phi : \mathbb{Z} \to G$ telle que $\phi(k) = x^k$ se factorise en un isomorphisme de groupe $\mathbb{Z}/n\mathbb{Z} \to G$ en utilisant le théorème de factorisation.
   On sait que x est d'ordre n par Prop 3.15 donc $n\mathbb{Z} \subset \mathrm{Ker}f$. Maintenant si $x^m = 1$ alors n divise n (cf Prop 3.15), et donc $\mathrm{Ker}f = n\mathbb{Z}$. Comme f est surjective, on peut donc appliquer le corollaire précédent et on obtient $G \simeq \mathbb{Z}/n\mathbb{Z}$.

□

Corollaire 5.2
Si G est un groupe de cardinal p avec p premier, alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration : Soit $x \neq 1$ élément de G. Son ordre est $\neq 1$ et divise p c'est donc p. On a donc $\langle x \rangle = G$ et on conclut par le théorème précédent. □

5.2 Générateurs

Proposition 5.3
Soit $n \in \mathbb{N}^*$. Alors $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur si et seulement $x \wedge n = 1$.

Démonstration : Supposons $x \wedge n = 1$. Et notons q l'ordre de $\overline{x}$. Alors q divise n par Proposition 3.15 (3.). On a $q\overline{x} = \overline{0}$, c'est-à-dire n divise qx. Comme n est premier avec x, n divise q. Donc $n = q$.

Réciproquement supposons $x \wedge n = p > 1$. Alors $n = pq$ avec $q < n$ et $x = pq'$. Donc on a

$$qx = qpq' = nq' = 0 \text{ mod} n.$$

L'ordre de x divise donc $q < n$, donc l'ordre de x est strictement inférieur à n. □

Exemple 5.4 Les générateurs de $\mathbb{Z}/10\mathbb{Z}$ sont $1, 3, 7$ et 9. L'ordre de 6 dans $\mathbb{Z}/10\mathbb{Z}$ par exemple est 5, ce n'est donc pas un générateur.

5.3 Produits de groupes cycliques

Théorème 5.5
Soient $m, n \in \mathbb{N}^*$. Alors le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $m \wedge n = 1$. Dans ce cas $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$.

Démonstration : Commençons par démontrer le lemme suivant.

Lemme 5.6
L'ordre de $(\overline{x}, \overline{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est le ppcm de l'ordre de $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ et de l'ordre de $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$.

Démonstration : Notons $p = \text{ord}(\overline{x})$, $q = \text{ord}(\overline{y})$ et $r = \text{ord}(\overline{x}, \overline{y})$. Alors $r(\overline{x}, \overline{y}) = (\overline{rx}, \overline{ry}) = (\overline{0}, \overline{0})$, donc p et q divisent r. Donc le ppcm de p et q divise r.

Maintenant si $t = ppcm(p, q)$ alors p et q divisent tous les deux $t = pp' = qq'$, on a donc

$$t(\overline{x}, \overline{y}) = (\overline{tx}, \overline{ty}) = (\overline{p'px}, \overline{q'qy}) = (p'\overline{px}, q'\overline{qy})(\overline{0}, \overline{0}).$$

Donc r divise t. □

Notons d'abord que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un groupe fini d'ordre mn. Donc s'il est cyclique il est forcément isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ par la proposition précédente.

Supposons que $m \wedge n = 1$. Alors par le lemme, l'ordre de $(\overline{1}, \overline{1})$ est le ppcm de l'ordre de $\overline{1} \in \mathbb{Z}/m\mathbb{Z}$ et de l'ordre de $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $m \vee n$. Comme $m \wedge n = 1$, alors $m \vee n = mn$. Donc $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ a un élément d'ordre mn, comme son ordre est mn, cet élément est générateur.

Réciproquement soit $(\overline{x}, \overline{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ un générateur. On a alors $mn = p \vee q$ avec $p = \text{ord}(\overline{x})$ et $q = \text{ord}(\overline{y})$. Comme de plus $p|m$ et $q|n$, on a forcément $p = m$ et $q = n$. Alors $mn = m \vee n$ si et seulement si $m \wedge n = 1$.
□

Notons que si $n \wedge m = 1$, par le lemme précédent, (x, y) est générateur si et seulement si x et y le sont (respectivement dans $\mathbb{Z}/n\mathbb{Z}$ et dans $\mathbb{Z}/m\mathbb{Z}$. Il y a donc plusieurs isomorphismes entre $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$.

Si on prend $n = 2$ et $m = 3$, on peut par exemple envoyer $(1, 1)$ sur $1 \in \mathbb{Z}/6\mathbb{Z}$, mais aussi envoyer $(1, 1)$ sur 5.

Chapitre III

Le groupe symétrique

1 Permutations

1.1 Définition et notations

Définition 1.1 Soit E un ensemble fini. On appelle *permutation* de E, une bijection de E dans E. On note $\mathfrak{S}_E$ ou $\mathcal{S}_E$ l'ensemble des permutations de E.

Si $E = \{1, \dots, n\}$, on note $\mathfrak{S}_n$ son ensemble des permutations.

Théorème 1.2
Soit E un ensemble fini de cardinal $n \geqslant 1$. L'ensemble $\mathfrak{S}_E$ muni de la loi $\circ$ de composition est un groupe fini de cardinal $n!$.

Si de plus F est un ensemble de cardinal n, alors toute bijection de E dans F induit un isomorphisme de groupes $\mathfrak{S}_E \to \mathfrak{S}_F$.

Démonstration : On a déjà vu que $\mathfrak{S}_E$ a une structure de groupe. Si $E = \{e_1, \dots, e_n\}$, la donnée de $\sigma \in \mathfrak{S}_E$ équivaut à la donnée de $(\sigma(e_1), \dots, \sigma(e_n))$. On a n possibilités pour $\sigma(e_1)$, mais seulement $n-1$ pour $\sigma(e_2)$ car σ est une bijection, etc... donc le cardinal est bien $n!$.

Soit $\varphi : E \to F$ une bijection. Alors on définit $\Phi : \mathfrak{S}_E \to \mathfrak{S}_F$ par $\Phi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$. On vérifie facilement que c'est un isomorphisme de groupes. □

Le but de ce chapitre est de comprendre le groupe $\mathfrak{S}_n$, qu'on appelle aussi le *groupe symétrique*, et on notera $E = \{1, \dots, n\}$.

Notation : Pour $\sigma \in \mathfrak{S}_n$, on notera

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$
et $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

1.2 Support d'une permutation

Définition 1.3 Soit $\sigma \in \mathfrak{S}_n$. On définit $\mathrm{Supp}(\sigma) := \{a \in E |\ \sigma(a) \neq a\}$. C'est le *support* de σ. Les éléments $a \in E$ tel que $\sigma(a) = a$ sont appelés les *points fixes* de σ.

Proposition 1.4
Soit $\sigma \in \mathfrak{S}_n$. Alors on a les propriétés suivantes :

1. $\mathrm{Supp}(\sigma) = \emptyset \Leftrightarrow \sigma = \mathrm{Id}_E$;
2. $\mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma)$
3. $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$
4. $\mathrm{Supp}(\sigma^n) \subset \mathrm{Supp}(\sigma)\ \forall n \in \mathbb{Z}$
5. $\mathrm{Supp}(\sigma \circ \sigma') \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma')$ et si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$ alors on a égalité. On dit alors que σ et σ' sont *à supports disjoints*.

Démonstration :

1. clair
2. On a
$$\begin{aligned} a \notin \mathrm{Supp}(\sigma) &\Leftrightarrow \sigma(a) = a \\ &\Leftrightarrow a = \sigma^{-1}(a) \\ &\Leftrightarrow a \notin \mathrm{Supp}(\sigma^{-1}) \end{aligned}$$
3. Soit $b \in \sigma(\mathrm{Supp}(\sigma))$, alors $b = \sigma(a)$ avec $\sigma(a) \neq a$. Comme σ est injective, on a donc $\sigma^2(a) \neq \sigma(a)$, c'est à dire $\sigma(b) \neq b$. Et on a $\sigma(\mathrm{Supp}(\sigma)) \subset \mathrm{Supp}(\sigma)$.
De la même façon, on a donc $\sigma^{-1}(\mathrm{Supp}(\sigma^{-1})) \subset \mathrm{Supp}(\sigma^{-1})$. En appliquant σ de chaque côté on obtient $\mathrm{Supp}(\sigma^{-1}) \subset \sigma(\mathrm{Supp}(\sigma^{-1}))$, et en appliquant le point 2., on obtient $\mathrm{Supp}(\sigma) \subset \sigma(\mathrm{Supp}(\sigma))$.

4. Soit $b \notin \mathrm{Supp}(\sigma)$, alors $\sigma(b) = b$, et donc $\sigma^n(b) = b$ autrement dit $b \notin \mathrm{Supp}(\sigma^n)$.
5. Soit $a \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma')$, cela signifie $a \notin \mathrm{Supp}(\sigma)$ et $a \notin \mathrm{Supp}(\sigma')$, donc $\sigma(a) = a$ et $\sigma'(a) = a$. Donc $\sigma \circ \sigma'(a) = \sigma(a) = a$ et donc $a \notin \mathrm{Supp}(\sigma \circ \sigma')$.
   Supposons maintenant que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$. Soit $a \notin \mathrm{Supp}(\sigma \circ \sigma')$, alors $\sigma \circ \sigma'(a) = a$. Supposons $a \in \mathrm{Supp}(\sigma')$, alors $\sigma'(a) = b \neq a$, et donc $\sigma(\sigma'(a)) = \sigma(b) = a \neq b$ donc $a \in \mathrm{Supp}(\sigma)$. Ce qui est impossible car $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$. On a donc $a \notin \mathrm{Supp}(\sigma')$, autrement dit $\sigma'(a) = a$. Et comme $\sigma'(\sigma(a)) = a$, on obtient $\sigma(a) = a$, c'est-à-dire $a \notin \mathrm{Supp}(\sigma)$.

□

Lemme 1.5
Deux permutations à supports disjoints commutent.

Démonstration : Soient σ et σ' deux telles permutations.

Soit $a \in E$. Si a n'est ni dans le support de σ, ni dans celui de σ', alors on a $\sigma \circ \sigma'(a) = \sigma(a) = a$ et $\sigma' \circ \sigma(a) = \sigma'(a) = a$.

Soit $a \in \mathrm{Supp}(\sigma)$, alors par hypothèse, $a \notin \mathrm{Supp}(\sigma')$. On a donc $\sigma \circ \sigma'(a) = \sigma(a)$. De plus par le point 3. précédent, on a que $\sigma(a) \in \mathrm{Supp}(\sigma)$, et donc $\sigma(a)$ est fixé par σ'. On a donc $\sigma'(\sigma(a)) = \sigma(a)$.

De même si $a \notin \mathrm{Supp}(\sigma')$. Donc on a bien pour tout a dans E, $\sigma' \circ \sigma(a) = \sigma \circ \sigma'(a)$.

□

1.3 Orbites

Définition 1.6 Soit $\sigma \in \mathfrak{S}_n$ et $a \in E$. On définit *l'orbite* de a sous l'action de σ comme le sous-ensemble

$$\mathcal{O}_\sigma(a) := \{a, \sigma(a), \sigma^2(a), \ldots\} \subset E.$$

Remarquons que a est un point fixe de σ si et seulement si $\mathcal{O}_\sigma(a) = \{a\}$.

Lemme 1.7
On a $\mathcal{O}_\sigma(a) = \{\sigma^m(a), m \in \mathbb{Z}\}$. Et si le cardinal de $\mathcal{O}_\sigma(a)$ est p, alors p est le plus petit entier tel que $\sigma^p(a) = a$ et on a

$$\mathcal{O}_\sigma(a) := \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{p-1}(a)\}.$$

Démonstration : Notons tout d'abord que σ est d'ordre fini puisqu'élément d'un groupe fini. Donc il existe m tel que $\sigma^m(a) = a$. Notons p le plus petit entier > 0 vérifiant $\sigma^p(a) = a$.

On va montrer l'inclusion

$$\{\sigma^m(a), m \in \mathbb{Z}\} \subset \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^p(a)\},$$

et que les éléments de l'ensemble de droite sont tous distincts, ce qui montrera toutes les égalités.

Soit $n \in \mathbb{Z}$, et soit $n = pq+r$ la division euclidienne de n par p. On a alors $\sigma^n(a) = \sigma^r(a)$ donc on a l'inclusion demandée. De plus si $0 \leqslant j \leqslant k \leqslant p-1$ sont tels que $\sigma^j(a) = \sigma^k(a)$, alors $\sigma^{k-j}(a) = a$. Par minimalité de p, on en déduit $j - k = 0$, et donc les p éléments de l'ensemble de droite sont 2 à 2 distincts.

□

Exemple 1.8 Prenons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 1 & 5 \end{pmatrix}$. Alors on a $\mathcal{O}(1) = \{1, 3, 6, 5\} = \mathcal{O}(3)$ et $\mathrm{O}(2) = \mathcal{O}(4) = \{2, 4\}$.

Proposition 1.9
Soit $\sigma \in \mathfrak{S}_n$. L'ensemble des orbites sous l'action de σ forme une partition de E.

Démonstration : On définit la relation $\sim$ sur E par $a \sim b \Leftrightarrow \mathcal{O}(a) = \mathcal{O}(b)$. Il est immédiat de voir que c'est une relation d'équivalence. montrons que la classe de a est exactement $\mathcal{O}(a)$. Si $b \sim a$ alors $b \in \mathcal{O}(b) = \mathcal{O}(a)$ donc

$\mathcal{C}_a \subset \mathcal{O}(a)$. Si $b \in \mathcal{O}(a)$ alors $b = \sigma^m(a)$ pour un certain entier m. Cela implique que tout $\sigma^k(b)$ est aussi dans l'orbit de a donc $\mathcal{O}(b) \subset \mathcal{O}(a)$. Par ailleurs, $a = \sigma^{-m}(b)$ et donc $\mathcal{O}(a) \subset \mathcal{O}(b)$.

□

2 Cycles et décompositions

2.1 Cycles

Définition 2.1 Un *cycle* est une permutation ayant une unique orbite non triviale. On parle de *m-cycle* lorsque m est le cardinal de cette orbite non triviale. Un 2-cycle est aussi appelé une *transposition*.

Notation : Si σ est un m-cycle, on notera $\sigma = (a, \sigma(a), \ldots, \sigma^{m-1}(a))$, où $\mathcal{O}_\sigma(a)$ est l'orbite non triviale.

Exemple 2.2 Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}$ est un 5-cycle. On le note (13654).

La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 1 & 5 \end{pmatrix}$ n'est pas un cycle, car il a deux orbites non triviales $\mathcal{O}(1) = \{1, 3, 6, 5\}$ et $\mathcal{O}(2) = \{2, 4\}$.

Proposition 2.3
Si σ est un m-cycle, alors σ est d'ordre m et $\langle\sigma\rangle \simeq \mathbb{Z}/m\mathbb{Z}$.

Démonstration : Soit $\mathcal{O}_\sigma(a)$ l'orbite non triviale. Alors on a vu par le lemme précédent que m est le plu petit entier tel que $\sigma^m(a) = a$. Montrons que $\sigma^m(b) = b$ pour tout $b \in E$. Si $b \in \mathcal{O}_\sigma(a)$, alors $b = \sigma^k(a)$, et donc $\sigma^m(b) = \sigma^{k+m}(a) = \sigma^k(a) = b$. Si $b \notin \mathcal{O}_\sigma(a)$, alors b est un point fixe, c'est-à-dire $\sigma(b) = b$, donc $\sigma^m(b) = b$. On a donc bien $\sigma^m = \mathrm{Id}$. Par minimalité de m, c'est bien l'ordre de σ. □

2.2 Théorème de décomposition

Théorème 2.4
Toute permutation s'écrit de manière unique comme produit de cycles à supports disjoints.

Regardons d'abord sur un exemple comment on décompose une permutation en produit de cycles.

On a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 4 & 1 & 2 & 5 \end{pmatrix} = (1375) \circ (26) = (26) \circ (1375)$. On voit qu'il faut prendre les cycles correspondants aux orbites non triviales de σ.

Démonstration : Soit σ un permutation. On va donc noter $\mathcal{O}_1, \ldots, \mathcal{O}_p$ les orbites non triviales de σ. Puis on définit pour tout $i = 1, \ldots, p$ un permutation c_i par $c_i(x) = x$ si $x \notin \mathcal{O}_i$ et $c_i(x) = \sigma(x)$ si $x \in \mathcal{O}_i$.

Notons tout d'abord que si $x \in \mathcal{O}_i$, si et seulement si $c_i(x) \in \mathcal{O}_i$. Montrons maintenant que c_i est une permutation, il suffit de montrer que c'est injectif. Si $c_i(x) = c_i(y)$, alors si $x \notin \mathcal{O}_i$, on a $c_i(x) = x = c_i(y)$ n'est pas dans $\mathcal{O}_i$, donc y n'est pas dans $\mathcal{O}_i$. Et donc $c_i(y) = y$ et donc $x = y$. Si maintenant $x \in \mathcal{O}_i$, alors $c_i(x) = c_i(y)$ est aussi dans $\mathcal{O}_i$, et donc $y \in \mathcal{O}_i$. On a donc $\sigma(x) = c_i(x) = c_i(y) = \sigma(y)$, donc $x = y$.

On va maintenant montrer que c_i est un cycle dont le support est $\mathcal{O}_i$. Un récurrence immédiate montre que si $x \in \mathcal{O}_i$, alors pour tout $\ell \in \mathbb{N}$, $c_i^\ell(x) = \sigma^\ell(x)$. Pour $x \in \mathcal{O}_i$, on a donc $\mathcal{O}_{c_i}(x) = \{x, \sigma(x), \ldots\} = \mathcal{O}_\sigma(x) = \mathcal{O}_i$. Comme c_i fixe tous les éléments en dehors de $\mathcal{O}_i$, c_i n'a donc qu'une seule orbite qui est $\mathcal{O}_i$.

Comme les orbites $\mathcal{O}_i$, les c_i commutent.

Montrons maintenant que $\sigma = c_1 \circ c_2 \cdots c_p$. Soit $x \in E$. Si x n'est dans aucun des $\mathcal{O}_i$, alors x est fixé par tous les c_i, et on a donc $c_1 \cdots c_p(x) = x = \sigma(x)$. Si $x \in \mathcal{O}_i$, alors il n'est pas dans les autres $\mathcal{O}_j$ pour $j \neq i$. On a donc

$$c_1 \ldots c_p(x) = c_i \circ c_1 \ldots c_{i-1} c_{i+1} \ldots c_p(x) = c_i(x) = \sigma(x).$$

Montrons enfin l'unicité. Supposons que $\sigma = c'_1 \ldots c'_q$ à support disjoints, et notons $\mathcal{O}'_i$ l'orbite non triviale de c'_i. Alors par la proposition 1.4 5., on a $\mathrm{Supp}(\sigma) = \mathcal{O}'_1 \cup \ldots \cup \mathcal{O}'_q$, et l'union est disjointe. Montrons que chaque $\mathcal{O}'_i$ est une orbite de σ. En effet si $x \in \mathcal{O}'_i$, alors x est un point fixe pour tous les autres c'_j, et donc $\sigma(x) = c'_i(x)$. Par un récurrence immédiate on a alors que $\sigma^\ell(x) = (c'_i)^\ell(x)$, et donc $\mathcal{O}'_i = \mathcal{O}_\sigma(x)$.

□

Exemple 2.5 On a $(1243)(25617)(346) = (174256)$.

Proposition 2.6
Soit $\sigma = c_1 \dots c_p$ la décomposition de σ en produit de cycles à supports disjoints, alors

$$\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(c_1), \dots, \mathrm{ord}(c_p)).$$

Démonstration : Soit q le ppcm des ordres des c_i. Alors l'ordre de chqeu c_i divise q et donc $c_i^q = \mathrm{Id}_E$. On a donc $\sigma^q = (c_1 \dots c_p)^q = c_1^q \dots c_p^q = \mathrm{Id}_E$.

Supposons maintenant que $\sigma^m = \mathrm{Id}_E$, alors on a $c_1^m \dots c_p^m = \mathrm{Id}_E$. Le support de c_i^m est inclus dans le support de c_i, donc les supports des c_i^m sont disjoints. On a donc nécessairement $c_i^m = \mathrm{Id}_E$ pour tout i, et donc m divise le ppcm de l'ordre des c_i.

□

Exemple 2.7 On a $(123)(25164) = (1643)(25)$ est d'ordre 4.

2.3 Générateurs de $\mathfrak{S}_n$

Théorème 2.8
Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

Démonstration : Il suffit d'après le théorème pécédent de montrer que les cycles sont des produits de transpositions. Or on vérifie facilement que $(a_1 \dots a_\ell) = (a_1 a_2)(a_2 a_3) \dots (a_{\ell-1} a_\ell)$. □

Théorème 2.9

$$\begin{aligned}\mathfrak{S}_n &= \langle (i, i+1),\ i = 1, \ldots, n-1 \rangle \\ &= \langle (1i),\ i = 2, \ldots, n \rangle \\ &= \langle (12), (12 \ldots n) \rangle.\end{aligned}$$

Démonstration : On a $(i, j) = (j-1, j) \ldots (i+1, i+2)(i, i+1)(i+1, i+2) \ldots (j-1, j)$ ce qui suffit à démontrer la première égalité.

On a $(i, j) = (1, i)(1, j)(1, i)$. Ce qui montre la seconde.

Enfin notons $c = (12 \ldots n)$, alors on a $(i, i+1) = c^{i-1}(12)c^{i-1}$, ce qui montre la dernière.

□

3 Signature et groupe alterné

3.1 Signature

Définition 3.1 Soit $\sigma \in \mathfrak{S}_n$. La *signature* de σ est $\epsilon(\sigma) = (1)^{n-m}$ où m est le nombre d'orbites de σ. On dit que σ est *paire* si $\epsilon(\sigma) = 1$ et *impaire* is $\epsilon(\sigma) = -1$.

Exemple 3.2
- $\epsilon(\mathrm{Id}_E) = (-1)^{n-n} = 1$.
- Si σ est un ℓ-cycle, il a alors $1+n-\ell$ orbites. On a donc $\epsilon(\sigma) = (-1)^{\ell-1}$. En particulier la signature d'une transposition est -1.
- $\epsilon((18)(27463)) = (-1)^{9-4} = -1$

3.2 La signature comme morphisme de groupes

Lemme 3.3
Si $\sigma \in \mathfrak{S}_n$ et τ est une permutation, alors on a $\epsilon(\sigma \circ \tau) = -\epsilon(\sigma)$.

Démonstration : Notons $\sigma = c_1 \dots c_p$ la décomposition de σ en cycles à supports disjoints. On va montrer que le nombre d'orbites de $\sigma \circ \tau$ est un de plus ou un de moins que le nombre d'orbites de σ.

Notons $\tau = (ab)$. On va distinguer quatre cas selon que a, b appartiennent aux orbites des c_i.

Cas 1 : a et b n'appartiennent pas au support de σ.
Dans ce cas, $c_1 \dots c_p \tau$ est la décomposition en produit de cycles à supports disjoints. Donc son nombre d'orbites est 1 de moins que celles de σ.

Cas 2 : $a \in \mathrm{Supp}(c_i)$ et b n'appartient pas au support de σ.
Notons $c_i = (a, a_2 \dots, a_s)$. La permutation τ commute avec tous les autres c_j et on a $c_i \circ (ab) = (a, b, a_2, \dots, a_s)$. Le nombre d'orbites a donc diminué de 1.

Cas 3 : $a, b \in \mathrm{Supp}(c_i)$.
Dans ce cas τ commute avec tous les c_j sauf c_i. Notons $c_i = (a_1, \dots, a_s)$ avec $a_1 = a$ et $a_t = b$. On a alors $c_i \circ \tau = (a_1, a_{t+1}, a_{t+2}, \dots, a_s)(a_2, a_3, \dots a_t)$. Le nombre d'orbites a donc augmenté de 1.

Cas 4 : $a \in \mathrm{Supp}(c_i)$ et $b \in \mathrm{Supp}(c_j)$ pour $i \neq j$.
Notons $c_i = (a, a_2, \dots, a_s)$ et $c_j = (b, b_2, \dots, b_q)$. On a $c_i c_j \tau = (a, b_2, \dots, b_q, b, a_2, \dots, a_s)$. Le nombre d'orbites a donc diminué de 1.

□

Corollaire 3.4
L'application $\epsilon : \mathfrak{S}_n \to \{+1, -1\}$ est un morphisme de groupes.

Démonstration : En effet le lemme précédent permet de montrer par un récurrence immédiate que si $\tau_1, \dots, \tau_m$ sont des permutations, alors $\epsilon(\tau_1 \dots \tau_m) = (-1)^m$. On voit alors immédiatement que c'est un morphisme de groupes. □

Théorème 3.5
La signature est l'unique morphisme de groupes $\mathfrak{S}_n \to \mathbb{C}^*$ non trivial.

Avant de montrer ce théorème, on doit d'abord montrer le lemme suivant :

Lemme 3.6
Soient τ et τ' deux transpositions, alors il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma \circ \tau \circ \sigma = \tau'$.

Démonstration : Si $\tau = (i, j)$ et $\tau' = (k, \ell)$ tous distincts, alors on peut poser $\sigma = (ik)(j\ell)$.

Si $\tau = (ij)$ et $\tau' = (jk)$, alors on peut prendre $\sigma = (ik)$.

□

Démonstration :(*du théorème*) Soit $\phi : \mathfrak{S}_n \to \mathbb{C}^*$ un morphisme de groupes. Soit τ une transposition. Comme $\tau^2 = \mathrm{Id}_E$, on doit avoir $\phi(\tau)^2 = 1$, autrement dit $\phi(\tau) = \pm 1$.

Si $\phi(\tau) = 1$, alors d'après le lemme, pour toute autre transposition on aura

$$\phi(\tau') = \phi(\sigma \circ \tau \circ \sigma^{-1}) = \phi(\sigma)\phi(\tau)\phi(\sigma)^{-1} = \phi(\tau) = 1.$$

Comme toute permutation est produit de transpositions, on aura donc $\phi(\sigma) = 1$ pour tout σ.

Si maintenant $\phi(\tau) = -1$, par le même argument, pour toute autre transposition on aura $\phi(\tau') = -1$. Et donc si σ est un produit de m transpositions, on aura $\phi(\sigma) = (-1)^m = \epsilon(\sigma)$.

□

3.3 Le groupe $\mathfrak{A}_n$

Le noyau d'un morphisme de groupes étant un sous-groupe, il est donc naturel d'introduire la définition suivante :

Définition 3.7 Le *groupe alterné* $\mathfrak{A}_n$ est le noyau de la signature, c'est donc un sous-groupe de $\mathfrak{S}_n$. Il contient toutes les permutations de signature 1.

Exemple 3.8 On a $\mathfrak{A}_2 = \{\mathrm{Id}_E\}$.

On a $\mathfrak{A}_3 = \{\mathrm{Id}_E, (123), (132)\}$. Il est abélien isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Le groupe $\mathfrak{A}_4$ contient 12 éléments : l'identité, 3 doubles transpositions, et 8 3-cycles. Il n'est pas abélien.

Proposition 3.9
Le cardinal du groupe $\mathfrak{A}_n$ est $\dfrac{n!}{2}$.

Démonstration : Par le théorème de factorisation, la signature $\epsilon : \mathfrak{S}_n \to \{+1, -1\}$ se factorise en une application $\mathfrak{S}_n/\mathfrak{A}_n \to \{+1, -1\}$. Cette application est clairement surjective, et elle est injective. On a donc $\sharp(\mathfrak{S}_n/\mathfrak{A}_n) = 2$. On conclut par le théorème de Lagrange.

□

Théorème 3.10
Le groupe alterné est engendré par les 3-cycles.

Démonstration : Les éléments du groupe alterné sont des produits d'un nombre paire de transpositions. Il suffit de démontrer que le produit de deux transpositions est toujours un produit de 3-cycles. Or on a $(ij)(jk) = (ijk)$ et $(ij)(k\ell) = (ijk)(jk\ell)$. □

3.4 Formule explicite

Théorème 3.11
Soit $\sigma \in \mathfrak{S}_n$. Alors on a la formule

$$\epsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Démonstration : Notons $f : \mathfrak{S}_n \to \mathbb{C}^*$ la fonction donnée par cette formule. On va montrer que f est un morphisme de groupes non trivial.

Notons tout d'abord que f est à valeurs $+1$ ou -1. En effet comme σ est une bijection, on a $\prod_{i<j} |\sigma(j) - \sigma(i)| = \prod_{i<j}(j-i)$.

Soit $\tau = (k, k+1)$. Pour montrer que $f(\tau) = -1$, il suffit donc de montrer que $\prod_{i<j} \tau(j) - \tau(i)$ est négatif.

Si $i < k$ alors $\tau(j) - \tau(i) = \tau(j) - i$ est positif. Si $j > k+1$, alors $\tau(j) - \tau(i) = j - \tau(i)$ est aussi toujours positif. Il reste donc le cas où $i = k$ et $j = k+1$, dans ce cas $\tau(j) - \tau(i) = k - (k+1) = -1$. Donc finalement, le produit est négatif, et $f(\tau) = -1$.

On va maintenant montrer que f est un morphisme de groupes. On a

$$\begin{aligned} f(\sigma_1 \circ \sigma_2) &= \prod_{i<j} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)} . \frac{\sigma_2(j) - \sigma_2(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)} \prod_{i<j} \frac{\sigma_2(j) - \sigma_2(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)} f(\sigma_2) \end{aligned}$$

Par ailleurs on a

$$A = \prod_{i<j} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)} = \prod_{i<j, \sigma_2(i)<\sigma_2(j)} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)} \prod_{i<j, \sigma_2(i)>\sigma_2(j)} \frac{\sigma_1\sigma_2(j) - \sigma_1\sigma_2(i)}{\sigma_2(j) - \sigma_2(i)}$$

En effectuant le changement de variables $k = \sigma_2(i)$ et $\ell = \sigma_2(j)$ dans le premier terme et $k = \sigma_2(j)$, $\ell = \sigma_2(k)$ dans le deuxième, on obtient

$$\begin{aligned} A &= \prod_{\sigma_2^{-1}(k)<\sigma_2^{-1}(\ell), k<\ell} \frac{\sigma_1(\ell) - \sigma_1(k)}{\ell - k} \prod_{\sigma_1^{-1}(\ell)<\sigma_1^{-1}(k), k<\ell} \frac{\sigma_1(k) - \sigma_1(\ell)}{\ell - k} \\ &= \prod_{k<\ell} \frac{\sigma_1(\ell) - \sigma_1(k)}{\ell - k} \\ &= f(\sigma_1). \end{aligned}$$

On obtient donc bien $f(\sigma_1 \circ \sigma_2) = f(\sigma_1) f(\sigma_2)$.

□

Chapitre IV

Le groupe orthogonal

1 Espaces euclidiens

On commence ici par quelques rappels sur les espaces euclidiens. Dans tout ce chapitre E désignera un $\mathbb{R}$-espace vectoriel de dimension n.

1.1 Produit scalaire et isométries

Définition 1.1 Un *produit scalaire* sur E est une application bilinéaire $\langle .,. \rangle : E \times E \to \mathbb{R}$ qui est

- *symétrique*, i.e. $\forall x, y \in E, \langle x, y \rangle = \langle y, x \rangle$;
- *définie positive*, i.e. $\forall x \neq 0,\ \langle x, x \rangle > 0$.

On dit alors que $(E, \langle .,. \rangle)$ est un *espace euclidien*.

Définition 1.2 Un *isométrie vectorielle* f est un endomorphisme de E tel que

$$\forall x, y \in E\ \langle f(x), f(y) \rangle = \langle x, y \rangle.$$

Le proposition suivante est facile à vérifier

Proposition 1.3
L'ensemble des isométries vectorielles de E est un sous-groupe de $\mathrm{GL}(E)$.

On appelle *groupe orthogonal* le groupe des isométries vectorielles, et on le note $\mathrm{O}(E)$.

1.2 Le groupe $\mathrm{O}_n(\mathbb{R})$

Définition 1.4 Une base $(e_1, \ldots, e_n)$ de E est dite *orthonormale* si $\langle e_i, e_i \rangle = 1$ pour tout i et si $\langle e_i, e_j \rangle = 0$ pour $i \neq j$.

Une telle base existe toujours dans E (on peut par exemple en construire une en utilisant l'algoritme de Gram-Schmidt).

Proposition 1.5
Soit $f \in \mathcal{L}(E, E)$ et $\mathcal{B}$ une base orthonormale de E. Alors on a les équivalences

$$\begin{aligned} f \in \mathrm{O}(E) &\Leftrightarrow M = \mathrm{Mat}(f, \mathcal{B}) \text{ vérifie } M^T.M = \mathrm{I}_n \\ &\Leftrightarrow f(\mathcal{B}) \text{ est une base orthonormale} \end{aligned}$$

On notera $\mathrm{O}_n(\mathbb{R}) := \{M \in \mathrm{GL}_n(\mathbb{R}) | M^T.M = \mathrm{I}_n\}$. Une conséquence de la proposition ci-dessus est que chaque choix de base orthonormale induit un isomorphisme de groupes entre $\mathrm{O}(E)$ et $\mathrm{O}_n(\mathbb{R})$.

On note $\mathrm{SO}(E)$ (ou $\mathrm{O}^+(E)$) l'intersection $\mathrm{Ker}\det \cap \mathrm{O}(E)$ et $\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}^+(\mathbb{R}) = \mathrm{Ker}\det \cap \mathrm{O}_n(\mathbb{R})$. C'est le *groupe spécial orthogonal*, ou le groupe des *isométries directes*.

1.3 Symétries

Définition 1.6 Soit F un sous-espace vectoriel de E. On note $F^\perp := \{x \in E | \ \forall y \in F \langle x, y \rangle = 0\}$ son *orthogonal*. C'est clairement un sous-espace vectoriel de E.

On a de plus la proposition suivante

Proposition 1.7
Soit F un sous-espace de E, alors on a $F \oplus F^\perp = E$.

Ce résultat peut par exemple se démontrer en prenant une base de F qu'on complète en une base de E, et à qui on applique l'algorithme de Gram-Schmidt. On obtient alors une base orthonormale dont la première partie

engendre F, et dont la deuxième partie est dans $F^\perp$. Le fait que $F \cap F^\perp = \{0\}$ provient du fait que le produit scalaire est défini positif.

Définition 1.8 Soit F un sous-espace vectoriel de E. La *symétrie orthogonale* s_F par rapport à F est la symétrie par rapport à F parallélement à $F^\perp$.

Pour $x \in E$, si $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in F^\perp$, alors $s_F(x) = x_1 - x_2$.

On vérifie facilement que s_F est une isométrie. Par ailleurs, dans une base orthonormale adaptée à la décomposition $F \oplus F^\perp$ la matrice de s_F est de la forme

$$\mathrm{Mat}(f, \mathcal{B}) = \begin{pmatrix} \mathrm{I}_m & 0 \\ 0 & -\mathrm{I}_{n-m} \end{pmatrix}, \text{ où } m = \dim F.$$

On a par ailleurs la caractérisation suivante des symétries orthogonales.

Proposition 1.9
Soit $u \in \mathrm{O}(E)$. Alors u est une symétrie orthogonale si et seulement si $u^2 = \mathrm{Id}_E$.

Démonstration : Il est clair qu'une symétrie orthogonale vérifie $u^2 = \mathrm{Id}_E$. Supposons donc que $u^2 = \mathrm{Id}_E$. Notons $F := \mathrm{Ker}(u - \mathrm{Id}_E)$ et $G := \mathrm{Ker}(u + \mathrm{Id}_E)$.

Il est facile de voir que F et G sont en somme directe (ce sont des sous-espaces propres associés à des valeurs propres distinctes). Et par ailleurs on peut écrire

$$x = \frac{1}{2}(x + u(x)) + \frac{1}{2}(x - u(x)),$$

et on vérifie $x + u(x) \in F$ et $x - u(x) \in G$. On a donc $F \oplus G = E$. De plus si $x \in F$ et $y \in G$, on a

$$\langle x, y \rangle = \langle u(x), u(y) \rangle = \langle x, -y \rangle = -\langle x, y \rangle$$

donc $\langle x, y \rangle = 0$ et donc $G \subset F^\perp$. Par égalité des dimensions, on obtient donc $G = F^\perp$. Comme on a

$$u(x) = \frac{1}{2}(x + u(x)) - \frac{1}{2}(x - u(x)),$$

on obtient donc que u est la symétrie orthogonale par rapport à F.

□

Proposition 1.10
Soit F un sous-espace de E, et u un isométrie de E. Alors on a

$$u \circ s_F \circ u^{-1} = s_{u(F)}.$$

Démonstration : On va montrer que $u \circ s_F \circ u^{-1}$ agit comme l'identité sur $u(F)$ et comme mois l'identité sur $u(F)^\perp$.

Soit $x \in u(F)$, et notons $x = u(y)$, $y \in F$. Alors on a $u \circ s_F \circ u^{-1}(x) = u \circ s_F(y) = u(y) = x$ car $y \in F$.

Montrons maitenant que $u(F)^\perp = u(F^\perp)$. En effet on a les équivalences

$$\begin{array}{rcl} x \in (u(F))^\perp & \Leftrightarrow & \forall y \in F \ \langle u(y), x\rangle = 0 \\ & \Leftrightarrow & \forall y \in F \ \langle y, u^{-1}(x)\rangle = 0 \\ & \Leftrightarrow & u^{-1}(x) \in F^\perp \\ & \Leftrightarrow & x \in u(F^\perp) \end{array}$$

Donc si $x \in (u(F))^\perp$, on a $x = u(y)$ avec $y \in F^\perp$. Et donc $u \circ s_F \circ u^{-1}(x) = u \circ s_F(y) = u(-y) = -x$.

On a donc démontré que $u \circ s_F \circ u^{-1} = s_F$. □

2 Quelques propriétés du groupe orthogonal

2.1 Quelques propriétés

Proposition 2.1
Si $\dim_{\mathbb{R}} E \geqslant 2$, le centre de $\mathrm{O}(E)$ est $\{\pm \mathrm{Id}_E\}$.

Démonstration : Une inclusion est évidente. Supposons maintenant que u soit dans le centre, alors pour toute droite vectorielle D, u commute avec s_D et donc on a $u \circ s_D \circ u^{-1} = s_D$. Par la proprositon précédente, on obtient $s_D = s_{u(D)}$ donc $u(D) = D$. Ceci implique que tout vecteur non nul de E

est un vecteur propre de u. L'application u est donc une homothétie, et les seules homothéties de $\mathrm{O}(E)$ sont celles de rapport $+1$ ou -1. □

Le groupe $\mathrm{O}(E)$ est bien entendu infini, mais il contient des sous-groupes finis. Par exemple cette propriété fait le lien avec le chapitre précédent.

Proposition 2.2
Il existe un morphisme de groupes injectif $\Phi : \mathfrak{S}_n \to \mathrm{O}(E)$, tel que $\det \circ \Phi = \epsilon$ (la signature).

Démonstration : Notons $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthonormale de E. Soit $\sigma \in \mathfrak{S}_n$, on définit Φ_σ comme l'endomorphisme envoyant e_i sur $e_{\sigma(i)}$. C'est bien une isométrie puisque qu'il envoie la base $\mathcal{B}$ sur $\mathcal{B}$ (en permutant son ordre). On a de plus

$$\Phi_\sigma \circ \Phi_{\sigma'}(e_i) = \Phi_\sigma(e_{\sigma'(i)}) = e_{\sigma\circ\sigma'(i)} = \Phi_{\sigma\circ\sigma'}(e_i)$$

pour tout i, donc Φ est bien un morphisme de groupes.

De plus, si τ est la transposition (12), alors la matrice de $\Phi_t au$ dans la base $\mathcal{B}$ a la forme

$$\mathrm{Mat}(\Phi_\tau, \mathcal{B}) = \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & 0 & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Et donc on vérifie aisément que $\det \Phi_t au = -1$. Comme $\det \circ \Phi$ est un morphisme de groupes $\mathfrak{S}_n \to \{\pm 1\}$, on en déduit que $\det \circ \Phi = \epsilon$.

□

2.2 Générateurs

Définition 2.3 Une *réflexion* est une symétrie orthogonale par rapport à un hyperplan H.

Dans une base orthonormale $\mathcal{B}$ adaptée à la décomposition $H \oplus H^\perp$, on a donc

$$\mathrm{Mat}(s_H, \mathcal{B}) = \begin{pmatrix} \mathrm{I}_{n-1} & 0 \\ 0 & -1 \end{pmatrix}.$$

Le résultat suivant nous donne un système de générateur pour le groupe orthogonal.

Théorème 2.4
Le groupe orthogonal est engendré par les réflexions.

Avant de démontrer ce théorème, notons l'analogie avec les groupe symétrique. En effet, notons $\Phi_{(12)}$ l'isométrie échangeant les vecteurs e_1 et e_2. Alors la base $(\frac{e_1+e_2}{\sqrt{2}}, \frac{e_1-e_2}{\sqrt{2}}, e_3, \ldots, e_n)$ est encore orthonormale, et dans cette base, la matrice de $\Phi_{(12)}$ est la matrice d'une réflexion. De même chaque $\Phi_{(ij)}$ est une réflexion. On peut donc voir ce théorème comme un analogue du fait que les transpositions engendrent le groupe symétrique.

Démonstration : On va démontrer par récurrence sur p que si $u \in \mathrm{O}(E)$ avec $p = n - \mathrm{Ker}(u - \mathrm{Id}_E)$ alors u peut s'écrire comme un produit d'au plus p réflexions.

Pour $p = 0$, on a $n = \dim \mathrm{Ker}(u - \mathrm{Id}_E)$ et donc $u = \mathrm{Id}_E$ et l'assertion est vraie.

Supposons donc l'assertion vraie pour tout $i \leqslant p \in \mathbb{N}$, $p \geqslant 0$.

Soit u notons $F_u = \mathrm{Ker}(u - \mathrm{Id}_E)$ et supposons $\dim F_u = n - (p + 1)$, autrement dit supposons que $\dim F_u^\perp = p + 1$. On va construire une réflexion s telle que $u \circ s$ vérifie F_u est strictement inclus dans $F_{u\circ s}$. On pourra alors appliquer l'hypothèse de récurrence à l'isométrie $u \circ s$, et on aura le résultat.

Soit $x \in F_u^\perp$ non nul (il existe car $p + 1 \geqslant 1$), et posons $y = u(x)$. Notons d'abord que $y \neq x$ car $x \notin F_u$. Ensuite si $z \in F_u$ (donc $u(z) = z$), alors on a

$$\langle z, y\rangle = \langle u(z), u(x)\rangle = \langle z, x\rangle = 0,$$

ce qui montre que $y \in F_u^\perp$.

Notons $H = \mathrm{vect}(y - x)^\perp$. C'est bien un hyperplan car $y \neq x$. De plus, comme $H^\perp = \mathrm{vect}(y - x) \subset F_u^\perp$, on a $F_u \subset H$. On veut vérifier que $\mathrm{vect}(F_u, y) \subset F_{u\circ s_H}$ et donc que $u \circ s_H$ satisfait l'hypothèse de récurrence (en effet y n'est pas dans F_u, donc le sous-espace $\mathrm{vect}(F_u, y)$ est strictement plus grand que F_u).

Si $z \in F_u$, alors $z \in H$ donc on a $u \circ s_H(z) = u(z) = z$. Donc $F \subset \mathrm{Ker}(u \circ s_H - \mathrm{Id}_E) = F_{u\circ s_H}$.

Par ailleurs on a

$$\langle x + y, x - y\rangle = \langle x, x\rangle - \langle y, y\rangle = \langle x, x\rangle - \langle u(x), u(x)\rangle = 0,$$

donc $x+y \in \text{vect}(y-x)^\perp = H$. Alors $y = \frac{x+y}{2} + \frac{y-x}{2}$ est la décomposition de y selon $H^\perp \oplus H$. On obtient alors que

$$s_h(y) = \frac{x+y}{2} - \frac{y-x}{2} = x.$$

Finalement on obtient $u \circ s_h(y) = u(x) = y$, donc $y \in F_{u \circ s_H}$ et

$$\text{vect}(F_u, y) \subset F_{u \circ s_H},$$

ce qui finit la preuve.

□

3 Classification en dimensions 2 et 3

Nous allons maintenant nous intéresser à $\mathrm{O}_2(\mathbb{R})$ et $\mathrm{O}_3(\mathbb{R})$ et essayer de classifier leurs éléments. On commence par le cas de la dimension 2.

3.1 Rotations et symétries en dimension 2

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une matrice de $\mathrm{O}_2(\mathbb{R})$. La relation $M^T.M = \mathrm{I}_2$ nous donne les équations

$$\begin{cases} ab + cd = 0 \\ a^2 + c^2 = 1 \\ b^2 + d^2 = 1 \end{cases}$$

On en déduit donc l'existence d'uniques $\theta, theta' \in [0, 2\pi[$ tels que

$$a = \cos\theta,\ c = \sin\theta, b = \cos\theta', d = \sin\theta'.$$

L'équation $ab + cd = 0$ nous donne alors $\cos(\theta - \theta') = 0$, autrement dit $\theta - \theta' = \pm\frac{\pi}{2}$.

Cas 1 : $\theta' = \theta + \frac{\pi}{2}$. On a alors $M = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, c'est donc la matrice R_θ de rotation d'angle θ.

Cas 2 :$\theta' = \theta - \frac{\pi}{2}$. On a alors $M := S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Cette matrice est diagonalisable (avec valeurs propres 1 et -1), c'est donc une

réflexion. C'est la réflexion par rapport à la droite engendrée par le vecteur de coordonnées $(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$. Par ailleurs on vérifie immédiatement que

$$S_\theta = R_\theta . S_0 \text{ avec } S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On a donc montré le résultat suivant

Théorème 3.1

$\mathrm{SO}_2(\mathbb{R}) = \{R_\theta, \theta \in [0, 2\pi[\}$ et $\mathrm{O}_2(\mathbb{R}) = \{R_\theta, S_\varphi |\ \theta \in [0, 2\pi[, \varphi \in [0, \pi[\}$.

On a les relations $R_\theta \circ R_\varphi = R_{\theta+\varphi}$, $S_\theta \circ S\varphi = R_{\theta-\varphi}$, et $S_\varphi \circ R_\theta = R_{-\theta} \circ S_\varphi$.

Notons qu'il en découle que le groupe $\mathrm{O}_2(\mathbb{R})$ est engendré par $\mathrm{SO}_2(\mathbb{R})$ et S_0.

Il en découle aussi qu'on a un isomrophisme entre $\mathrm{SO}_2(\mathbb{R})$ et $\mathcal{U}$ le sous-groupe des racines de l'unité, donné par $R_\theta \mapsto e^{i\theta}$, et que ce groupe est abélien.

3.2 Sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$

On va voir maintenant qu'on peut totalement classifier les sous-groupes finis de $\mathrm{O}_2(\mathbb{R})$.

Théorème 3.2
Soit G un sous-groupe fini de $\mathrm{O}_2(\mathbb{R})$. Alors on a

$$G = \langle R_{\frac{2\pi}{n}} \rangle \quad \text{ou} \quad G = \langle R_{\frac{2\pi}{n}}, S_\varphi \rangle,$$

pour un certain $n \in \mathbb{N}$ et $\varphi \in [0, \pi[$.

Démonstration : Notons tout d'abord que si G est un sous-groupe fini de $\mathrm{O}_2(\mathbb{R})$, alors $G \cap \mathrm{SO}_2(\mathbb{R})$ est un sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$. Par l'isomorphisme précédent, on peut donc le voir comme un sous-groupe fini G' de $\mathcal{U}$.

Supposons que l'ordre de G' est n. Alors on a pour tout $z \in G'$, $z^n = 1$. Comme il y a exactement n-racines n-ièmes de l'unité, on obtient

$$G' = \{z \in \mathbb{C} | z^n = 1\} = \langle e^{\frac{2i\pi}{n}} \rangle.$$

Cela nous dit donc que $G \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{\frac{2\pi}{n}} \rangle$. Si G est inclus dans $\mathrm{SO}_2(\mathbb{R})$, on a donc le premier résultat. Supposons maintenant que G ne soit pas inclus dans $\mathrm{SO}_2(\mathbb{R})$. Alors il existe $\varphi \in [0, \pi[$ tel que $S_\varphi \in G$. On va montrer que $G = \langle R_{\frac{2\pi}{n}}, S_\varphi \rangle$. Soit g un élément de G. Si g est dans SO_2, alors, g est dans $G \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{\frac{2\pi}{n}} \rangle$. Si maintenant g n'est pas directe, alors $g = S_\theta$ pour un certain θ. Mais alors $S_\theta \circ S_\varphi = R_{\theta - \varphi}$ est dans $G \cap \mathrm{SO}_2(\mathbb{R}) = \langle R_{\frac{2\pi}{n}} \rangle$, donc on a

$$S_\theta \circ S_\varphi = (R_{\frac{2\pi}{n}})^k$$

autrement dit

$$S_\theta = (R_{\frac{2\pi}{n}})^k \circ S_\varphi \in \langle R_{\frac{2\pi}{n}}, S_\varphi \rangle.$$

Donc on a bien $G = \langle R_{\frac{2\pi}{n}}, S_\varphi \rangle$.

□

3.3 Le groupe diédral

Dans le théorème précédent, on comprend bien les groupes de la forme $G = \langle R_{\frac{2\pi}{n}} \rangle$ qui sont des groupes cycliques, donc abélien et isomorphes à $\mathbb{Z}/n\mathbb{Z}$. Par contre la structure d'un groupe de la forme$G = \langle R_{\frac{2\pi}{n}}, S_\varphi \rangle$. C'est l'objet de ce paragraphe de les étudier plus en détail.

Définition 3.3 Soit $\mathcal{P}_n$ le polygone régulier à n côtés de centre O. Notons $v_1, \ldots, v_n$ ses sommets (ou les vecteurs correspondants). On note $\mathbb{D}_n := \{f \in \mathrm{O}(\mathbb{R}^2) |\ f(\mathcal{P}_n) = \mathcal{P}_n)\}$. C'est un sous-groupe de $\mathrm{O}_2(\mathbb{R})$ qu'on appelle le *groupe diédral* .

Essayons de comprendre les éléments de $\mathbb{D}_n$. Un élément de $\mathbb{D}_n$ préserve le polygone $\mathcal{P}_n$, il doit donc envoyer chaque v_i sur un v_j.

Notons de plus que $f \in \mathbb{D}_n$ est entièrement déterminé par $f(v_1)$ et $f(v_2)$. En effet, (v_1, v_2) est une base, et un endomorphisme est déterminé par l'image d'une base.

Enfin si $f(v_1) = v_{\ell+1}$, alors comme f est une isométrie, on doit avoir $f(v_2) = v_\ell$ ou $f(v_2) = v_{\ell+2}$. On va donc traiter ces deux cas.

Cas 1 : $f(v_2) = v_{\ell+2}$. Dans ce cas, on voit immédiatement que f est la rotation d'angle $\dfrac{2\pi\ell}{n}$.

Cas 2 : $f(v_2) = v_\ell$. On montre alors assez facilement que $f(v_j) = v_{\ell-j}$. C'est une symétrie car si (v_1, v_2) est une base directe, alors la base $(v_{\ell+1}, v_\ell)$ est indirecte. On va alors distinguer plusieurs cas.

Si n est pair et ℓ est pair, les points $v_{\frac{\ell}{2}}$ et $v_{\frac{n+\ell}{2}}$ sont fixés par f, donc f est la symétrie par rapport à la droite passant par $v_{\frac{\ell}{2}}$ et $v_{\frac{n+\ell}{2}}$.

Si n est pair et ℓ est impair, alors f ne fixe aucun des v_j, mais il fixe les segments $[v_{\frac{\ell-1}{2}}, v_{\frac{\ell+1}{2}}]$ et $[v_{\frac{n+\ell-1}{2}}, v_{\frac{n+\ell+1}{2}}]$, donc il fixe leur milieux respectifs. C'est donc la symétrie par rapport à la droite passant par ces deux milieux.

Si n est impair, alors soit $v_{\frac{\ell}{2}}$ soit $v_{\frac{+n\ell}{2}}$ est l'unique sommet fixé. C'est donc la symétrie par rapport à la droite passant par ce sommet et le milieu du côté opposé.

Finalement, on en déduit que le groupe $\mathbb{D}_n$ a $2n$ éléments n rotations, et n symétries. Si on note r la rotation d'angle $\frac{2\pi}{n}$, et s une symétrie quelconque de $\mathbb{D}_n$, on a alors

$$\mathbb{D}_n = \langle r, s\rangle = \{r^k, sr^k, k = 0, \dots, n-1\}.$$

avec les relations $r^n = 1$, $s^2 = 1$ et $sr = r^{-1}s$.

Tous les sous-groupes finis de $\mathrm{O}(\mathbb{R}^2)$ non inclus dans $\mathrm{SO}_2(\mathbb{R})$ sont isomorphes à un groupe diédral.

3.4 Classification en dimension 3

Essayons maintenant de comprendre quelles sont les isométries de $\mathbb{R}^3$. Tout d'abord notons que si $f \in \mathrm{O}(\mathbb{R}^3)$, alors son polynôme caractéristique est un polynôme de degré 3 à coefficients réels, il admet donc au moins une racine réelle, autrement dit il admet (au moins) une valeur propre que l'on notera λ. Comme f est une isométrie, cette valeur propre λ doit être égale à 1 ou à -1. Notons e_3 un vecteur propre correspondant de norme 1, et complétons le en une base orthonormale (e_1, e_2, e_3). On a donc $V := \mathrm{vect}(e_1, e_2) = \mathrm{vect}(e_3)^\perp$. Comme $f(e_3) = \pm e_3$, on a

$$\langle f(e_1), e_3\rangle = \langle f(e_1), f(\pm e_3)\rangle = \langle e_1, \pm e_3\rangle = 0$$

et donc $f(e_1) \in V$. De même pour $f(e_2)$. On obtient donc que V est un sous-espace stable par f. De plus, on voit facilement que $f_{|_V}$ est une isométrie de V.

Autrement dit, dans la base (e_1, e_2, e_3), la matrice de f sera de la forme

$$\mathrm{Mat}(f, \mathcal{B}) = \begin{pmatrix} M' & 0 \\ 0 & \lambda \end{pmatrix} \text{ avec } M' \in \mathrm{O}_2(\mathbb{R}) \text{ et } \lambda = \pm 1$$

On va donc pouvoir se servir de la classification précédente, et on se retrouve avec a priori 4 cas à taiter :

$$\begin{pmatrix} R_\theta & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} R_\theta & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} S_\varphi & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} S_\varphi & 0 \\ 0 & -1 \end{pmatrix}$$

Le premier cas correspond à une *rotation* d'angle θ autour de l'axe $\mathrm{vect}(e_3)$. Dans le cas où $\theta = 0$ on obtient l'*identité*. Dans le cas où $\theta = \pi$, on obtient la symétrie orthogonale par rapport à l'axe $\mathrm{vect}(e_3)$. Une telle isométrie s'appelle un *retournement ou demi-tour*.

Le deuxième cas peut s'écrire

$$\begin{pmatrix} R_\theta & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} R_\theta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & \\ & & -1 \end{pmatrix},$$

il s'agit donc d'une rotation d'angle θ autour de l'axe $\mathrm{vect}(e_3)$ composée avec la symétrie orthogonale par rapport au plan $\mathrm{vect}(e_1, e_2)$ (donc orthogonal à l'axe de rotation) ce qu'on appelle parfois une *anti-rotation*. Dans le cas où $\theta = 0$, on obtient la *réflexion* par rapport au plan $\mathrm{vect}(e_1, e_2)$. Dans le cas où $\theta = \pi$, on obtient $-\mathrm{I}_3$, qui est donc la *symétrie centrale*.

Dans le troisième cas, la matrice est diagonalisable, et donc dans une base orthonormale (e'_1, e'_2, e_3) on a

$$\mathrm{Mat}(f, \mathcal{B}) = \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}$$

C'est donc la *réflexion* par rapport au plan $\mathrm{vect}(e'_1, e_3)$.

Dans le troisième cas, la matrice est aussi diagonalisable, et donc dans une base orthonormale (e'_1, e'_2, e_3) on a

$$\mathrm{Mat}(f, \mathcal{B}) = \begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$$

C'est donc la symétrie par rapport à l'axe $\mathrm{vect}(e'_1)$, autrement dit un *demi-tour*.

On a donc finalement montré le résultat suivant.

Théorème 3.4
Les isométries vectorielles directes de $\mathbb{R}^3$ sont toutes des rotations :

- l'identité (rotation d'angle 0) ;
- les demi-tours (donc les symétries orthogonales par rapport à une droite, qui sont aussi les rotations d'angle π)
- les rotations d'angle θ autour d'un certain axe.

Les isométries vectorielles indirectes de $\mathbb{R}^3$ sont

- les réflexions (donc les symétries orthogonales par rapport à un plan) ;
- la symétrie centrale (symétrie orthogonale par rapport au sous-espace $\{0\}$;
- les anti-rotations d'angle θ autour d'un certain axe.

Chapitre V

Actions de groupes

1 Définitions

Définition 1.1 Soit X un ensemble et G un groupe. On dit que G *agit* sur X s'il existe une application

$$\begin{array}{rcl} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g.x \end{array}$$

telle que

- $1_G.x = x$ pour tout $x \in X$;
- $g.(h.x) = (gh).x$ pour tous $g, h \in G$, $x \in X$

Exemple 1.2

1. Soit $X = \{1, \ldots, n\}$ et $G = \mathfrak{S}_n$, avec l'action définie par $\sigma.x := \sigma(x)$.
2. $X = \mathbb{R}^n$ et $G = \mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{O}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{R})$, avec l'action définie par $f.x := f(x)$.
3. $X = G$ avec l'action définie par la multiplication à gauche, $g.x := gx$, ou encore avec l'action par conjugaison $g.x := gxg^{-1}$.
4. On peut prendre aussi le groupe diédral $\mathbb{D}_n$ agissant sur les sommets d'un n-gone régulier centré en 0.

Proposition 1.3
Se donner une action de G sur X revient à se donner un morphisme de groupes $G \to \mathfrak{S}_X$.

Démonstration : Soit $G \times X \to X$ une action de G sur X. On définit $\Phi : G \to \mathfrak{S}_X$ par $\Phi(g)(x) = g.x$. Vérifions tout d'abord que $\Phi(g)$ est bien une bijection. En effet, on a $\Phi(g^{-1}) \circ \Phi(g)(x) = g^{-1}.(g.x) = 1_G.x = x$ et $\Phi(g) \circ \Phi(g^{-1})(x) = g.(g^{-1}.x) = 1_G.x = x$, donc $\Phi(g)$ est inversible, d'inverse $\Phi(g^{-1})$. Par ailleurs on a $\Phi(gh) = \Phi(g)\Phi(h)$ par le deuxième point de la définition. Et donc Φ est bien un morphisme de groupes. □

Notons qu'une conséquence immédiate de cette définition est que si H est un sous-groupe de G, alors H agit naturellement sur X, via la composition $H \subset G \to \mathfrak{S}_X$.

Définition 1.4 On dit que G agit *fidèlement* sur X si le morphisme $G \to \mathfrak{S}_X$ est injectif, ou autrement dit si $g.x = x$ pour tout x, alors $g = 1_G$.

On dit que G agit *transitivement* sur X si $\forall x, y \in X$ il existe $g \in G$ tel que $g.x = y$.

Exemple 1.5 Reprenons les exemples précédents.

1. Soit $X = \{1, \dots, n\}$ et $G = \mathfrak{S}_n$, avec l'action définie par $\sigma.x := \sigma(x)$. Alors l'action est fidèle et transitive.
2. $X = \mathbb{R}^n$ et $G = \mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{O}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{R})$, avec l'action définie par $f.x := f(x)$. Alors l'action est fidèle, mais pas transitive, en effet on a toujours $f(0) = 0$. Par contre, si on prend $G = \mathrm{GL}_n(\mathbb{R})$ agissant sur $\mathbb{R}^n \setminus \{0\}$, alors l'action est transitive.
3. L'action de G sur G par multiplication à gauche est fidèle et transitive. L'action par conjugaison est fidèle seulement si $Z(G) = \{1_G\}$. Elle n'est pas transitive, car 1_G est toujours envoyé sur 1_G.
4. Le groupe diédral $\mathbb{D}_n$ agit fidèlement et transitivement sur $\{1, \dots, n\}$.

Notons qu'une conséquence du fait que l'action de G sur lui même par multiplication à gauche est fidèle équivaut à dire qu'on a un morphisme de groupe injectif $G \to \mathfrak{S}_G$. Donc si G est fini, il est isomorphe à un sous-groupe d'un groupe symétrique.

2 Orbites et stabilisateurs

Définition 2.1 Soit G agissant sur X. On définit une relation sur X par

$$x \sim y \;\Leftrightarrow\; \exists\, g \in G \; g.x = y.$$

C'est la relation *d'intransitivité*.

Proposition 2.2
La relation d'intransitivité est une relation d'équivalence.

Démonstration : Exercice □

Remarquons que l'action est transitive si et seulement si la relation d'intransitivité n'a qu'une seule classe d'équivalence.

Définition 2.3 Soit G agissant sur X, et $x \in X$. L'*orbite* de x (sous l'action de G) est la classe d'équivalence de x pour la relation d'intransitivité. Autrement dit

$$\mathcal{O}_G(x) := G.x = \{g.x,\ g \in G\} \subset X.$$

Exemple 2.4

1. Soit $\sigma \in \mathfrak{S}_n$, et $a \in \{1, \ldots, n\}$. Alors on a
$$\mathcal{O}_{\langle\sigma\rangle}(a) = \{\sigma^n(a),\ n \in \mathbb{Z}\} = \mathcal{O}_\sigma(a).$$
2. $X = \mathbb{R}^n$ et $G = \mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{O}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{R})$, avec l'action définie par $f.x := f(x)$. Alors la partition de $\mathbb{R}^n$ en orbites est $\mathbb{R}^n = (\mathbb{R}^n \backslash \{0\}) \cup \{0\}$. Si $G = \mathrm{O}_n(\mathbb{R})$, alors il y a une infinité d'orbites qui sont les sphères d'un rayon donné.

Définition 2.5 Soit $x \in X$. Le *stabilisateur* de x est défini comme

$$\mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\} \subset G$$

Il est aussi appelé le *sous-groupe d'isotropie* de x.

Plus généralement, si $Y \subset X$, on note

$$\mathrm{Stab}_G(Y) := \{g \in G \mid g.y \in Y\ \forall\ y \in Y\} \subset G$$

Proposition 2.6
Le stabilisateur est un sous-groupe de G.

Démonstration : Exercice □

Exemple 2.7
1. Soit $x \in \{1, \dots, n\}$, alors le stabilisateur de x est en bijection avec $\mathfrak{S}_{n-1}$.
2. Soit $x \in \mathbb{R}^n$ et $G = \mathrm{GL}_n(\mathbb{R})$. Si x est nul, alors le stabilisateur est G. Si x est non nul, alors le stabilisateur de x est l'ensemble des $u \in \mathrm{GL}(E)$ tels que x est vecteur propre associé à la valeur propre 1 de u.
3. $\mathrm{Stab}_{\mathrm{O}_2(\mathbb{R})}(\mathcal{P}_n = \mathbb{D}_n$

3 Dénombrement

3.1 Equation aux classes

Proposition 3.1
Soit G un groupe fini agissant sur un ensemble X, alors pour tout $x \in X$ on a l'égalité

$$|\mathcal{O}_G(x)||\mathrm{Stab}_G(x)| = |G|.$$

Démonstration : Notons $H = \mathrm{Stab}_G(x)$. On considère l'application $\mathrm{ev}_x : G \to \mathcal{O}_G(x)$ envoyant g sur $g.x$. Alors on a $\mathrm{ev}_x(g) = \mathrm{ev}_x)(h)$ si et seulement si $g^{-1}h.x = x$ autrement dit si et seulement si $g^{-1}h \in H$, donc si et seulement si $gH = hH$. Par le théorème de factorisation, ev_x se factorise en une application injective $G/H \to \mathcal{O}_G(x)$. Comme elle clairement surjective, on a alors $|G/H| = |\mathcal{O}_G(x)|$, et on conclut par le Théorème de Lagrange. □

Une conséquence de cette proposition est le formule suivante reliant le cardinal de G au cardinal de X.

Théorème 3.2 (Equation aux classes)
Soit G un groupe fini, agissant sur un ensemble fini X. Soit $Y \subset X$ un sous-ensemble contenant exactement un représentant de chaque orbite. Alors on a

$$|X| = \sum_{y \in Y} |\mathcal{O}_{\mathcal{G}}(y)| = \sum_{y \in Y} \frac{|G|}{|\mathrm{Stab}_G(y)|}.$$

3.2 Applications

Définition 3.3 Soit $g \in G$, on note $\mathrm{Fix}(g) = \{x \in X \mid g.x = x\} \subset X$, c'est l'ensemble des *points fixes* de g.

Théorème 3.4 (Formule de Burnside)
Soit G fini agissant sur X fini. Notons Ω l'ensemble des orbites, alors on a la formule :

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Démonstration : Notons $\Omega = \{\mathcal{O}_1, \ldots, \mathcal{O}_\ell\}$ l'ensemble des orbites. Soit

$$A = \{(x, g) \in X \times G |\ g.x = x\}.$$

L'idée est de compter les éléments de A de deux façons différentes. D'un côté on a

$$|A| = \sum_{g \in G} |\{x \in X |\ g.x = x\}| = \sum_{g \in G} |\mathrm{Fix}(g)|.$$

D'un autre on a

$$\begin{aligned} |A| &= \sum_{x \in X} |\{g \in G |\ g.x = x\} \\ &= \sum_{x \in X} |\mathrm{Stab}_G(x)| \\ &= \sum_{x \in X} \frac{|G|}{|\mathcal{O}_G(x)|} \\ &= |G| \sum_{i=1}^{\ell} \sum_{x \in \mathcal{O}_i} \frac{1}{\mathcal{O}_i} \\ &= |G| \sum_{i=1}^{\ell} 1 = \ell |G| \end{aligned}$$

On obtient donc la formule voulue. □

L'équation aux classes permet par exemple de montrer ce résultat qui est une réciproque à une propriété des groupes finis. Notons que ce résultat ne parle pas d'action de groupes.

Théorème 3.5 (de Cauchy)
Soit G un groupe fini. Alors pour tout nombre p premier divisant $|G|$, il existe un élément de G d'ordre p.

Démonstration : Soit p un nombre premier divisant $|G|$. Notons X l'ensemble suivant

$$X = \{(x_1, \ldots, x_p) \in G^p |\ x_1 \ldots x_p = 1_G\}.$$

On va calculer le cardinal de X de deux manières différentes. D'abord notons que pour $x_1, \ldots, x_{p-1}$ éléments quelconques de G, il existe un unique x_p tel que $x_1 \ldots, x_p = 1$. Donc on a $|X| = |G|^{p-1}$.

On fait maintenant agir $\mathbb{Z}/p\mathbb{Z}$ sur G^p de la façon suivante. :

$$i.(x_1, \ldots, x_p) := (x_{i+1}, \ldots, x_{i+p})(\text{où les indices sont pris modulo } p.$$

Il est clair que c'est une action. Par ailleurs, si $x_1 \ldots x_p = 1$, alors on a

$$x_{i+1} \ldots x_{i+p} = (x_{i+1} \ldots x_p)(x_1 \ldots x_p)(x_{i+1} \ldots x_p)^{-1} = 1_G,$$

donc l'action se restreint en une action sur X.

Pour un élément $y \in X$, son stabilisateur étant un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, il est soit de cardinal 1, soit de cardinal p, autrement dit d'après la proposition son orbite est soit de cardinal 1 (et c'est un point fixe), ou de cardinal p. Parmi les ℓ orbites, il y en a donc q de cardinal 1, et $\ell - q$ de cardinal p. On obtient donc $|X| = q + p(\ell - q)$. Comme p divise $|X| = |G|^{p-1}$ par le petit Théorème de Fermat, on obtient donc que p divise q.

Par ailleurs, l'orbite d'un élément $(x_1, \ldots, x_p)$ est réduite à un point si et seulement si $x_1 = x_2 = \ldots = x_p$ avec $x_1^p = 1$. L'ensemble des points fixes sont donc en bijection avec les éléments du groupe dont l'ordre divise p. L'élément 1_G est clairement un tel élément. Donc $q \geqslant 1$ et il existe au moins $p - 1$ éléments dont l'ordre divise p (et qui ne sont pas 1_G), ils sont donc d'ordre p.

□

En considrant une autre action sur G, on peut aussi obtenir des résultats sur le cardinal du centre.

Théorème 3.6
Soit G un groupe fini. Alors il existe $N \geqslant 0$ et des sous-groupes $H_1, \ldots, H_N$ non triviaux tels que

$$|G| = |\mathrm{Z}(G) + \sum_{i=1}^{N} \frac{|G|}{|H_i|}.$$

Démonstration : On considère cette fois l'action de G sur lui même par conjugaison. Alors un élément a son orbite réduite à un point si et seulement si il est dans le centre de G.

En notant Y un ensemble de représentants des orbites, on a donc la formule

$$|G| = |\mathrm{Z}(G) + \sum_{y \in Y \setminus \mathrm{Z}(G)} \frac{|G|}{\mathrm{Stab}_G(y)}.$$

Par ailleurs, le stabilisateur de y est réduit à G si et seulement si y est un point fixe. Il n'est jamais réduit à $\{1_G\}$, en effet y commute toujours avec lui même, donc le stabilisateur de $y \neq 1_G$ contient au moins 2 éléments, 1_G et y. Donc les sous-groupes $\mathrm{Stab}_G(y)$ dans la somme précédente sont non triviaux. □

Corollaire 3.7
Soit G un groupe de cardinal p^α avec p premier. Alors le centre de G n'est pas réduit à l'élément neutre (il est même divisible par p).

Démonstration : En appliquant le résultat précédent, on voit que le deuxième terme de la somme est divisible par p, ainsi que la somme entière. On a donc que p divise l'ordre du centre de G. □

Corollaire 3.8
Tout groupe de cardinal p^2 avec p premier est abélien.

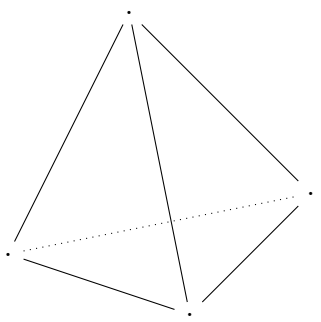
Démonstration : Par le résultat précédent, on obtient que le cardinal du centre de G est égal à p ou à p^2. Supposons qu'il soit égal à p, et prenons $x \in G \setminus \mathrm{Z}(G)$. Le stabilisateur de x contient $\mathrm{Z}(G)$, mais aussi x, il contient donc au moins $p+1$ éléments. Comme c'est un sous-groupe de G, son cardinal divise p^2, c'est donc p^2. Ceci signifie alors que x est un point fixe, et alors x est dans le centre de G. On obtient donc une contradiction. □

4 Groupe du tétraèdre

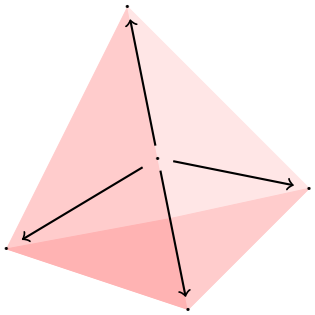
On revient maintenant aux sous-groupes d'isométries, mais cette fois dans $\mathbb{R}^3$. On a étudié le groupe diédral, comme groupes d'isométries laissant invariant un polygone régulier. On va passer maintenant en dimension 3 et étudier le sous-groupes des isométries laissant invariant un tétraèdre. régulier.

On considère un tétraèdre régulier T de centre O. Notons $\{v_1, \ldots, v_4\}$, les vecteurs correspondants de $\mathbb{R}^3$. On définit alors

$$G = \mathrm{Stab}_{\mathrm{O}_3(\mathbb{R})}(T) = \mathrm{Stab}_{\mathrm{O}_3(\mathbb{R})}(\{v_1, v_2, v_3, v_4\}).$$



Notons les v_i ont tous la même norme, que $\langle v_i, v_j \rangle = \langle v_1, v_2 \rangle$ pour tout $i \neq j$ et que $v_1 + v_2 + v_3 + v_4 = 0$.



Le but est de démontrer le théorème suivant :

Théorème 4.1
Le groupe G est isomorphe à $\mathfrak{S}_4$. De plus le groupe des isométries directes préservant le tétraèdre T est isomorphe à $\mathfrak{A}_4$.

Démonstration : On va ici utiliser les actions de groupes. Le groupe G agit naturellement sur l'ensemble $\{v_1, \dots, v_4\}$, on obtient donc un morphisme $G \to \mathfrak{S}_4$.

Ce morphisme est injectif, en effet l'action est fidèle car si $f \in G$ vérifie $f(v_i) = v_i$ pour tout i, alors comme (v_1, v_2, v_3) est une base de $\mathbb{R}^3$, on a bien $f = \mathrm{Id}$.

Montrons qu'il est surjectif. Soit $\sigma \in \mathfrak{S}_4$. On définit l'application linéaire f sur la base (v_1, v_2, v_3) par $f(v_i) = v_{\sigma(i)}$. C'est une application linéaire bijective. De plus comme $v_4 = -v_1 - v_2 - v_3$ on a bien

$$f(v_4) = -\sum_{i=1}^{3} f(v_i) = -\sum_{i=1}^{3} v_{\sigma(i)} = v_{\sigma(4)}.$$

On doit vérifier maintenant qu'elle est orthogonale (en effet ce n'est pas clair, car la base (v_1, v_2, v_3) n'est pas orthonormale). On a alors pour tout $i \neq j$,

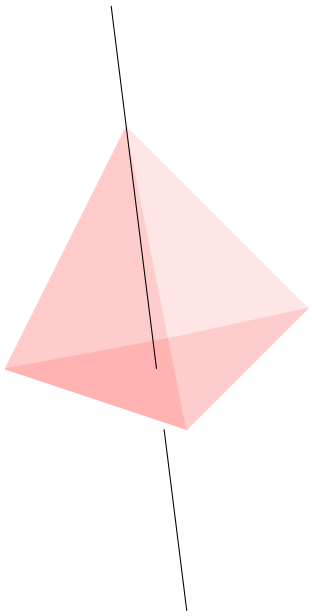
$$\langle f(v_i), f(v_j) \rangle = \langle v_{\sigma(i)}, v_{\sigma(j)} \rangle = \langle v_i, v_j \rangle,$$

f est donc une isométrie.

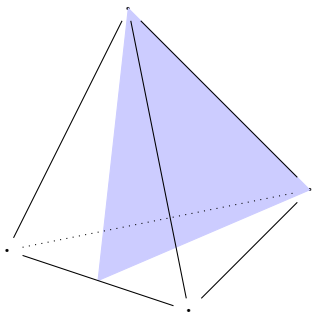
□

Donnons maintenant une description un peu plus précises de ces isométries.

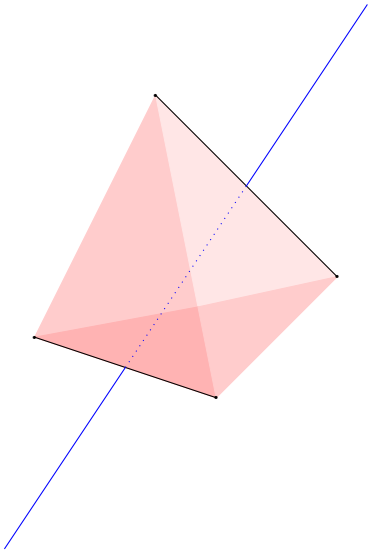
On a tout d'abord les 3-cycles, qui correspondent à une rotation d'angle $\pm\frac{2\pi}{3}$ autour d'un axe passant par un des sommets et orthogonal à la face opposée.



On a ensuite les transpositions qui correspondent à la réflexion par rapport à un plan de type $\text{vect}(v_i, v_j)$, c'est le plan passant par deux des sommets et le milieu des deux autre sommets.



On a aussi les doubles transpositions qui correspondent à un demi-tour (rotation d'angle π) autour d'un axe passant par les milieux de deux arêtes opposées.



Enfin on a les 4-cycles qui correspondent à une anti-rotation : c'est la composée de la rotation d'angle $\frac{\pi}{2}$ autour de l'axe passant par les milieux d'arêtes opposées avec la réflexion par rapport au plan orthogonal à cet axe.

Anneaux

Chapitre VI

Généralités sur les anneaux

1 Définition et premiers exemples

Définition 1.1 Un *anneau* est un ensemble A muni de deux opérations (ou lois internes) $A \times A \to A$ notées $+$ et $.$ telles que :

(A1) $(A, +)$ est un groupe abélien.

(A2) la loi $.$ est *associative* (c'est-à-dire pour tous $x, y, z \in A$, $(x.y).z = x.(y.z)$).

(A3) la loi $.$ est *distributive* par rapport à la loi $+$ (c'est-à-dire, pour tous $x, y, z \in A$, $(x+y).z = x.z + y.z$ et $z.(x+y) = zx + zy$).

(A4) La loi $.$ posséde un élément neutre noté 1_A.

Le neutre de la loi $+$ sera noté 0_A et l'inverse pour la loi $+$ d'un élément x sera noté $-x$. Comme pour les groupes, on notera $nx = \underbrace{x + x + \cdots + x}_{n \text{ fois}}$ et $x^n = \underbrace{x.x.\cdots.x}_{n \text{ fois}}$ pour $n \in \mathbb{N}$ et $nx = (-n)(-x)$ pour $n < 0$.

On dit que A est *commutatif* si la loi $.$ est commutative.

Exemple 1.2

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs.
2. $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif. On sait déjà que c'est un groupe pour la loi $+$. Vérifions que la loi $.$ est bien définie : Posons $\bar{x}.\bar{y} := \overline{x.y}$. Si $\bar{x}' = \bar{x}$ et $\bar{y} = \bar{y}'$ alors $x'y' = (x+kn)(y+\ell n) = xy + n(ky + \ell x + k\ell n)$ donc $\overline{xy} = \overline{x'y'}$.
   Voici les tables d'additions et de multiplication de $\mathbb{Z}/3\mathbb{Z}$.

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

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

Voici les tables d'additions et de multiplication de $\mathbb{Z}/4\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	0	1	2	3
$\overline{1}$	1	2	3	0
$\overline{2}$	2	3	0	1
$\overline{3}$	3	0	1	2

$.$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	0	0	0	0
$\overline{1}$	0	1	2	3
$\overline{2}$	0	2	0	2
$\overline{3}$	0	3	2	1

3. $(\mathcal{M}_n(k), +, .)$ où $k = \mathbb{R}$ ou $\mathbb{C}$ est un anneau non commutatif. De manière équivalente, si E est un k-espace vectoriel de dimension finie, alors $(\mathrm{End}(E), +, \circ)$ est un anneau.
4. $\mathbb{R}[X]$ est un anneau commutatif.

2 Règles de calcul

Proposition 2.1
Soit $(A, +, .)$ un anneau. Alors on a les propriétés suivantes :

- $\forall x \in A \quad 0_A.x = x.0_A = 0_A$
- pour tous $x, y \in A$, $(-x).y = x.(-y) = -(x.y)$.
- pour tous $x, y \in A$ et $n \in \mathbb{Z}$, $n(x.y) = (nx).y = x.(ny)$.
- pour tout $x \in A$ et $n, m \in \mathbb{Z}$, on a $(n+m)x = nx + mx$ et $(nm)x = n(mx) = (n1_A).(mx)$.

Démonstration : Laissée en exercice.

□

Remarque 2.2 Si $1_A = 0_A$ alors pour tout $x \in A$ on a $x = x.1_A = x.0_A = 0_A$. L'anneau 0_A est un anneau appelé anneau trivial. Dans tous les autres anneaux on a $1_A \neq 0_A$. Dans la suite on supposera toujours $1_A \neq 0_A$.

Proposition 2.3
Soit $(A, +, .)$ un anneau et x et y des éléments de A tels que $x.y = y.x$ (par exemple si A est commutatif). Alors pour tout $n \in \mathbb{N}$ on a la formule :

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

où $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

Démonstration :
Laissée en exercice.

□

3 Eléments inversibles et diviseurs de zéros

3.1 Le groupe des inversibles

Définition 3.1 Un élément de A ayant un inverse pour la loi . est dit *inversible*. On notera alors son inverse x^{-1}. L'ensemble des inversibles sera noté $A^\times$.

Exemple 3.2 1_A et -1_A sont toujours inversibles (mais attention on peut avoir $1_A = -1_A$).

0_A n'est jamais inversible.

Les inversibles de $\mathbb{Z}$ sont 1 et -1. On a $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$ et $\mathbb{C}^\times = \mathbb{C}^*$. Les inversibles de $\mathcal{M}_n(k)$ sont les matrices inversibles, c'est-à-dire $\mathrm{GL}_n(k)$.

Proposition 3.3
Soit $(A, +, .)$ un anneau. Alors $(A^\times, .)$ est un groupe.

Démonstration : 1_A est clairement inversible, donc dans $\mathrm{Inv}(A)$. De plus si a et b sont dans $\mathrm{Inv}(A)$, alors $a.b$ est inversible car $(a.b)^{-1} = b^{-1}.a^{-1}$. Enfin, si a est inversible, alors son inverse est aussi inversible car $(a^{-1})^{-1} = a$. □

Exemple 3.4 $(\mathrm{GL}_n(k), .)$ est un groupe.

Les éléments inversibles sont ceux qui contiennent 1 dans leur colonne et dans leur ligne dans la table de multiplication. On a donc $(\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}, \bar{2}\}$. Ce qui implique un isomorphisme $((\mathbb{Z}/3\mathbb{Z})^\times, .) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$.

On a $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$. Mais $\bar{2}$ n'est pas inversible.

Attention : $(\mathrm{Inv}(A), .)$ n'est pas stable pour la loi $+$. La somme de deux matrices inversibles n'est pas forcément inversible.

Attention, un élément x peut-être inversible à droite (c'est-à-dire il existe y tel que $xy = 1_A$) sans que $yx = 1_A$. (Exemple dans un espace vectoriel de dimension infinie.) Les inversibles sont les éléments "inversibles des deux côtés ".

Définition 3.5 Un anneau dont tous les éléments $\neq 0_A$ sont inversibles est appelé un *corps*.

Exemple 3.6 $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps mais pas $\mathbb{Z}/4\mathbb{Z}$.

3.2 Diviseurs de zéro

Définition 3.7 Si il existe $a, b \in A$ non nuls tels que $a.b = 0_A$, alors a et b sont dits *diviseurs de zéro*. Plus précisément, a est dit diviseur de zéro à gauche et b à droite.

Un élément $a \in A$ tel qu'il existe $n \in \mathbb{N}$ avec $a^n = 0_A$ est dit *nilpotent*. (Notons que c'est alors un diviseur de zéro.)

Un anneau COMMUTATIF n'ayant pas de diviseur de zéro est appelé *intègre*.

Proposition 3.8
Dans un anneau intègre, on peut SIMPLIFIER, c'est-à-dire si $x \neq 0_A$ et $xy = xz$ alors $y = z$.

Démonstration : Il suffit d'écrire $x(y - z) = 0_A$. □

Proposition 3.9
Un inversible n'est jamais diviseur de zéro, et un diviseur de zéro n'est jamais inversible.

Exemple 3.10 Un corps commutatif est toujours intègre. $\mathbb{Z}$ est intègre. $\mathbb{R}[X]$ est intègre. $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre.

$\mathcal{M}_n(k)$ n'est pas intègre (il existe des matrices nilpotentes).

4 Sous-anneaux et morphismes

4.1 Sous -anneaux

Définition 4.1 Soit $(A, +, .)$ un anneau. Un sous-ensemble $B \subset A$ est un *sous-anneau* de A si

(SA1) $(B, +)$ est un sous-groupe de $(A, +)$;
(SA2) $1_A \in B$;
(SA3) B est stable par ., c'est-à-dire $\forall\ x, y \in B,\ x.y \in B$.

Exemple 4.2 $(\mathbb{Z}, +, .)$ est un sous-anneau de $(\mathbb{R}, +, .)$. Par contre le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$. En effet, si B est un sous-anneau de $\mathbb{Z}$ alors $1 \in B$ donc $n = 1 + 1 + \cdots + 1$ est dans B ainsi que $-n$.

L'ensemble des matrices triangulaires supérieures est un sous-anneau de $\mathcal{M}_n(k)$.

4.2 Morphismes d'anneaux

Définition 4.3 Soient $(A, +, .)$ et $(B, +, .)$ deux anneaux. Une application $f : A \to B$ est un *morphisme d'anneau* s'il vérifie pour tous $x, y \in A$:

1. $f(x + y) = f(x) + f(y)$ (c'est-à-dire f est un morphisme de groupes)
2. $f(x.y) = f(x).f(y)$.
3. $f(1_A) = 1_B$.

Si $A = B$ on parle d'endomorphisme d'anneau. Si f est une bijection, on parle d'isomorphisme d'anneau. Si de plus $A = B$ on parle d'automorphisme.

Attention, la propriété (1) implique que $f(0_A) = 0_B$, mais la propriété (2) n'implique pas forcément que $f(1_A) = 1_B$, pour cela il faudrait être capable de simplifier. C'est vrai dans un anneau intègre, mais faux en général. Par exemple l'inclusion de $\mathcal{M}_n(k)$ dans $\mathcal{M}_{n+1}(k)$ est additif et multiplicatif, mais envoie 1_A sur un diviseur de zéro.

Exemple 4.4
- si B est un sous-anneau de A alors l'injection naturelle $B \to A$ est un morphisme d'anneau injectif.
- Soit E un ensemble et A un anneau. Soit $x \in E$ alors alors l'application $A^E \to A$ qui à $\phi \in A^E$ associe $\phi(x) \in A$ est un morphisme d'anneau appelé *morphisme d'évaluation* en x.
- Soit E un espace vectoriel de dimension n sur k. Alors pour toute base de E, on a un isomorphisme $\mathrm{End}(E) \simeq \mathcal{M}_n(k)$.
- La projection $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux.

— L'application $\mathbb{Z} \to A$ qui à n associe $n1_A$ est un morphisme d'anneau. C'est l'unique morphisme $\mathbb{Z} \to A$.

Remarque 4.5 Soit f un morphisme d'anneaux. On a alors $f(nx) = nf(x)$ (et $f(x^n) = f(x)^n$). L'application f est donc "$\mathbb{Z}$-linéaire".

Proposition 4.6
Soit $f : A \to B$ un morphisme d'anneau. Alors $\operatorname{Im} f$ est un sous-anneau de B. Plus généralement, si $A' \subset A$ est un sous-anneau de A, alors $f(A')$ est un sous-anneau de B.

Si $B' \subset B$ est un sous-anneau de B alors $f^{-1}(B')$ est un sous-anneau de A.

Démonstration : f est en particulier un morphisme de groupe, donc $(\operatorname{Im} f, +)$ est un sous-groupe de $(B, +)$. Comme $f(1_A) = 1_B$ alors $1_B \in \operatorname{Im} f$. Et enfin, si y_1 et y_2 sont dans $\operatorname{Im} f$ alors $y_1 = f(x_1)$ et $y_2 = f(x_2)$ donc $y_1.y_2 = f(x_1).f(x_2) = f(x_1.x_2) \in \operatorname{Im} f$.

Suite : exercice. □

Attention : $\operatorname{Ker} f$ **n'est jamais un sous-anneau. En effet** $f(1_A) = 1_B \neq 0_B$**, donc** 1_A **n'est pas dans** $\operatorname{Ker} f$**.**

5 Construction de familles d'exemples

Comme dans le chapitre sur les groupes, nous recensons ici plusieurs constructions standards permettant de construire de nouveaux exemples d'anneaux.

5.1 Anneaux produits

Proposition 5.1
Soient $(A_1, +, .)$ et $(A_2, +, .)$ deux anneaux. Alors $A_1 \times A_2$ est un anneau pour les lois :

$(x_1, x_2)+(y_1, y_2) = (x_1+y_1, x_2+y_2)$ et $(x_1, x_2).(y_1, y_2) = (x_1.y_1, x_2.y_2)$.

Les éléments neutres sont $0_{A_1 \times A_2} := (0_{A_1}, 0_{A_2})$ pour $+$ et $1_{A_1 \times A_2} := (1_{A_1}, 1_{A_2})$ pour ..

Démonstration : Exercice. □

Attention : $A_1 \times \{0\}$ est un sous-groupe de $A_1 \times A_2$ mais n'est pas un sous-anneau de $A_1 \times A_2$.

Exemple 5.2
1. $(\mathbb{C}^2, +, .)$ est un anneau. (Attention à ne pas penser aux éléments de $\mathbb{C}^2$ comme à des vecteurs).
2. L'isomorphisme de groupes $\Phi_1 : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ envoyant $(\bar{1}, \bar{1})$ sur $\bar{1}$ est un isomorphisme d'anneaux. On peut par exemple vérifier que

$$\Phi((\bar{1}, \bar{0}).(\bar{1}, \bar{2})) = \Phi((\bar{1}, \bar{0})).\Phi((\bar{1}, \bar{2}).$$

Par contre attention il existe un isomorphisme de groupes $\Phi_1 : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ envoyant $(\bar{1}, \bar{1})$ sur $\bar{5}$. Mais ce n'est pas un morphisme d'anneaux.

5.2 Anneaux de fonctions

Proposition 5.3
Soit E un ensemble et A un anneau. L'ensemble A^E des applications de E dans A est un anneau pour les lois :

$$(\phi + \psi)(x) = \phi(x) + \psi(x) \quad \text{et} \quad (\phi.\psi)(x) = \phi(x).\psi(x)$$

pour $\phi, \psi \in A^E$ et $x \in E$.

Démonstration :Exercice. □

Proposition 5.4
Soit A un anneau, E un ensemble et $x \in E$. Alors l'application $\mathrm{ev}_x : A^E \to A$ envoyant Φ sur $\Phi(x)$ est un morphisme d'anneaux. Il est appelé *morphisme d'évaluation en x*.

Exemple 5.5 L'ensemble $\mathcal{F}(\mathbb{R}, \mathbb{R})$ a une structure d'anneau. $\mathcal{C}(\mathbb{R}, \mathbb{R})$ est un sous-anneau de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

L'application naturelle $\mathbb{R}[X] \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ est un morphisme d'anneau injectif.

5.3 Anneaux de matrices

Soit A un anneau (commutatif), on peut définir $\mathcal{M}_n(A)$ comme les matrices à coefficients dans A. En effet les lois d'addition et de multiplication des matrices n'utilisent que les lois + et . de A.

Le déterminant d'une matrice à coefficient dans A a aussi du sens, car il n'y a que somme et produit dans la formule. Attention par contre les inversibles ne sont pas les matrices dont le déterminant est non nul. C sont eux dont le déterminant est un inversible de A. En effet grâce à la formule de l'inverse utilisant la transposée de la comatrice, on voit que l'unique "élément" à inverser est le déterminant. Par exemple on a $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}) | \det M = \pm 1\}$.

5.4 Anneaux de polynômes

L'idée ici est de penser à un polynôme, non pas comme une fonction d'une variable réelle, mais plutôt comme la suite de ses coefficients. Le propriété clé est donnée par le fait suivant :

Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

Définition

Cela motive ainsi la définition suivante :

Définition 5.6 Soit $(A, +, .)$ un anneau commutatif. Un *polynôme* à coefficients dans A est une suite $P = (a_k)_{k \in \mathbb{N}} = (a_0, a_1, \ldots,)$ d'éléments de

A n'ayant qu'un nombre fini de a_k différents de 0_A. Les a_k sont appelés les coefficients de P.

Si $P = (a_k)_{k\in\mathbb{N}}$ est de degré n, on le notera $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, où n est le plus grand entier tel que $a_n \neq 0$.

On note $A[X]$ l'ensemble des polynômes à coefficients dans A.

En utilisant les lois de A, on peut définir des lois d'additions et de multiplications sur l'ensemble des polynômes.

Si $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ alors $P + Q = (a_k + b_k)_{k\in\mathbb{N}}$.

Si $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ alors $P.Q = (c_k)_{k\in\mathbb{N}}$ avec $c_k = \sum_{i+j=k} a_i.b_j = \sum_{i=0}^{k} a_i b_{k-i}$.

Théorème 5.7
Muni des lois définis ci-dessus, $A[X]$ est un anneau commutatif.

Démonstration : $(A[X], +)$ est clairement un groupe abélien dont le neutre est le polynôme nul (dont tous les coefficients sont nuls).

Il est aussi clair que la loi . est commutative.

Vérifions l'associativité de la loi .. Soient $P = (a_k)$, $Q = (b_k)$ et $R = (c_k)$ des polynômes. Alors le $n$iéme coefficient de $(P.Q).R$ est donné par :

$$\begin{aligned}
\sum_{i+j=n} (\sum_{k+\ell=i} a_k b_\ell)c_j &= \sum_{i+j=n} \sum_{k+\ell=i} (a_k b_\ell)c_j \\
&= \sum_{k+\ell+j=n} (a_k b_\ell)c_j \\
&= \sum_{k+\ell+j} a_k(b_\ell c_j) \\
&= \sum_{k+p=n} \sum_{\ell+j=p} a_k(b_\ell c_j) \\
&= \sum_{k+p=n} a_k(\sum_{\ell+j=p} b_\ell c_j)
\end{aligned}$$

qui est le $n$iéme coefficient de $P.(Q.R)$.

Vérifions la distributivité. Soient $P = (a_k)$, $Q = (b_k)$ et $R = (c_k)$ des polynômes. Alors le $n$ième coefficient de $(P + Q).R$ est donné par :

$$\sum_{i+j=n}(a_i+b_i)c_j = \sum_{i+j=n} a_ic_j + b_ic_j$$
$$= \sum_{i+j=n} a_ic_j + \sum_{i+j=n} b_ic_j$$

qui est le $n$iéme coefficient de $PR+QR$.

Enfin le polynôme $U=(a_i)_{i\in\mathbb{N}}$ tel que $a_0=1_A$ et $a_i=0_A$ pour $i\geqslant 1$ est neutre pour la loi . En effet si $Q=(b_j)$ alors le $n$iéme coefficient du polynôme $U.Q$ est

$$\sum_{i+j=n} a_ib_j = a_0b_n = b_n,$$

donc $U.Q=Q$.

□

Proposition 5.8
L'application $A[X]\to\mathcal{F}(A,A)$ qui à P associe la fonction correspondante est un morphisme d'anneaux.

Attnetion, elle n'est pas toujours injective. Par exemple le polynôme $P=X^2-X$ de $\mathbb{Z}/2\mathbb{Z}[X]$, est non nul en tant que polynôme, mais on a $P(\overline{0})=P(\overline{1})=\overline{0}$, c'est un élément du noyau de ce morphisme.

Degré-valuation et intégrité

Définition 5.9 Soit A un anneau. Soit $P\in A[X]$ non nul. On définit $\deg P := \max\{n, a_n\neq 0_A\}$. C'est le *degré* de P. Par convention on pose $\deg 0=-\infty$. Si P est de dergé n, le coefficient a_n est appelé *coefficient dominant* .

De manière similaire on pose $\operatorname{val} P := \min\{n, a_n\neq 0\}$. C'est la *valuation* de P.

Proposition 5.10
Soient P et Q des polynômes. On a

$$\deg(P+Q) \leqslant \max\{\deg P, \deg Q\} \quad \text{et} \quad \deg(PQ) \leqslant \deg P + \deg Q.$$

De plus si A est intègre on a $\deg(PQ) = \deg P + \deg Q$.

Démonstration : Posons $P = a_0 + \ldots + a_n X^n$ et $Q = b_0 + \ldots + b_m X^m$ avec $a_n \neq 0$ et $b_m \neq 0$. Si $n > m$, alors le terme de plus haut degré de $P+Q$ est $a_n X^n$. Si $n = m$, alors le coefficient de degré n est $a_n + b_n$. S'il est non nul, le degré est n, s'il est nul le degré est strictement inférieur à n.

Soit $\ell \geqslant m+n+1$. Alors on a la formule $(PQ)_\ell = \sum_{i=0}^{\ell} a_i b_{\ell-i}$. Si $0 \leqslant i \leqslant n$, alors on a $m+1 \leqslant \ell - i \leqslant \ell$ donc $a_i b_{\ell-i} = 0$. Si $i \geqslant n+1$, on a aussi $a_i b_{k-i} = 0$. Donc le degré est inférieur à $m+n$. Si A est intègre, alors $(PQ)_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} = a_n b_m$. Comme a_n et b_m sont non nuls, le degré est bien égal à $m+n$.

□

Théorème 5.11
A est intègre, si et seulement si $A[X]$ est intègre.
Dans ce cas $A[X]^\times = A^\times$.

Démonstration : Si A est intègre. Par la formule précédente, on obtient que si P et Q sont non nuls, alors PQ est non nuls, car de degré $\leqslant 0$.

Si P est inversible, alors son degré est forcément égal à 0. Maintenant, il est clair qu'un polynôme constant a_0 est inversible dans $A[X]$ si et seulement si $a_0 \in A^\times$.

Réciproquement, A peut-être vu comme un sous-anneau de $A[X]$. Il sera donc intègre si $A[X]$ l'est. □

Ceci est faux si A n'est pas intègre. Par exemple si $A = \mathbb{Z}/4\mathbb{Z}$, alors on a $(\bar{2}X + 1)^2 = 1$, donc $\bar{2}X + 1$ est inversible.

Chapitre VII

Idéaux

Dans tout ce chapitre, les anneaux sont COMMUTATIFS.

1 Idéal dans un anneau commutatif

1.1 Définition

Définition 1.1 Soit $(A, +.)$ un anneau commutatif. Un sous-ensemble $I \subset A$ est appelé *idéal* si

— $(I, +)$ est un sous-groupe de $(A, +)$;
— pour tout $x \in A$ pour tout $y \in I$, xy est dans I.

Remarque 1.2 Comme A est commutatif, si I est un idéal de A, on a aussi pour tout $x \in A$ et tout $y \in I$, $y.x$ est dans I.

Il existe aussi une notion d'idéal dans les anneaux non commutatifs. On parle alors d'idéal à gauche, ou à droite, ou bilatére lorsque qu'ils sont à la fois à droite et à gauche.

Proposition 1.3
Soit A un anneau commutatif, et I un idéal. Alors on a les équivalences

$$I = A \Leftrightarrow 1_A \in I \Leftrightarrow I \text{ est un sous-anneau de } A.$$

Démonstration : Supposons que $1_A \in I$. Alors d'aprés la définition, I est un sous-anneau de A. Soit $a \in A$, alors $a = a.1_A$ avec $a \in A$ et $1_A \in I$. Donc $a \in I$, c'est-à-dire $A = I$. Les autres implications sont immédiates. □

Exemple 1.4 $\{0\}$ et A sont des idéaux de A.

Proposition 1.5
Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{Z}$.

Démonstration : Ce sont clairement des idéaux. Réciproquement, un idéal est un sous-groupe. □

1.2 Opérations sur les idéaux

Proposition 1.6
Soient I_1 et I_2 deux idéaux de A. Alors $I_1 \cap I_2$ est un idéal de A.

Plus généralement, si $(I_k)_{k\in K}$ est une famille d'idéaux de A, alors $\bigcap_{k\in K} I_k$ est un idéal de A.

Démonstration : Exercice. □

Exemple 1.7 Soient $p, q \in \mathbb{Z}$. Alors $p\mathbb{Z} \cap q\mathbb{Z} = ppcm(p, q)\mathbb{Z}$. En effet tout nombre à la fois divisible par p et q est divisible par leur ppcm. Récirpoquement, tout nombre divisible par le ppcm est donc divisible par p et par q.

Proposition 1.8
Soient I_1 et I_2 deux idéaux de A. Alors $I_1+I_2 := \{x_1+x_2, x_1 \in I_1, x_2 \in I_2\}$ est un idéal de A.

Attention dans I_1+I_2 l'écriture de $x = x_1+x_2$ n'est pas forcément unique !

Démonstration : $I_1 + I_2$ est clairement non vide. Si $x = x_1 + x_2$ et $y = y_1 + y_2$ sont des éléments de $I_1 + I_2$, alors $x - y = (x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2)$ est aussi dans $I_1 + I_2$. Donc $(I_1 + I_2, +)$ est un sous-groupe de $(A, +)$.

Maintenant, si $x = x_1 + x_2 \in I_1 + I_2$ et $y \in A$, alors $x.y = (x_1 + x_2).y = x_1.y + x_2.y$ est dans $I_1 + I_2$. Donc c'est un idéal. □

Exemple 1.9 Soient $p, q \in \mathbb{Z}$. Alors $p\mathbb{Z} + q\mathbb{Z} = pgcd(p, q)\mathbb{Z}$.

Notons ℓ le pgcd. Alors d'aprés Bezout, il existe $u, v \in \mathbb{Z}$ tels que $pu+qv = \ell$, donc $\ell \in p\mathbb{Z}+q\mathbb{Z}$. On a donc $\ell\mathbb{Z} \subset p\mathbb{Z}+q\mathbb{Z}$. Réciproquement si $m = pa+qb$ alors m est divisible par ℓ.

1.3 Idéal engendré

Proposition 1.10
Soient I_1 et I_2 deux idéaux de A. Alors $I_1 \cap I_2$ est un idéal de A.

Plus généralement, si $(I_k)_{k\in K}$ est une famille d'idéaux de A, alors $\bigcap_{k\in K} I_k$ est un idéal de A.

Démonstration : Exercice. □

Définition 1.11 Soit $X \subset A$ un sous-ensemble de A. L'*idéal engendré par X* est l'intersection de tous les idéaux de A contenant X, on le note (X). C'est le plus petit idéal de A contenant X, au sens où si J est un idéal contenant X alors $(X) \subset J$.

Si $X = \{x_1, \ldots, x_k\}$ alors on note $(X) = (x_1, \ldots, x_k)$.

Proposition 1.12
Soit $X = \{x_1, \ldots, x_k\}$ un sous-ensemble d'un anneau commutatif A. Alors $(x_1, \ldots, x_k) = \{\sum_{i=1}^{k} a_k x_k, a_i \in A\}$.

En particulier $(x_1) = x_1A = Ax_1$.

Démonstration : Pour tout $i = 1, \ldots, k$, pour tout $a_i \in A$, alors $a_i x_i \in \langle X \rangle$ puisque que $\langle X \rangle$ est un idéal. Puisque $\langle X \rangle$ est aussi un sous-groupe, alors $\sum_{i=1}^{k} a_i x_i \in \langle X \rangle$. Donc on a l'inclusion $\{\sum_{i=1}^{k} a_k x_k, a_i \in A\} \subset \langle X \rangle$.

Vérifions maintenant que $\{\sum_{i=1}^{k} a_k x_k, a_i \in A\}$ est un idéal. Il contient clairement $0_A = \sum_i 0.x_i$. Il est stable par somme, car

$$\sum_i a_i x_i + \sum_i b_i x_i = \sum_i (a_i + b_i).x_i$$

On a aussi $-(\sum_i a_i x_i) = \sum_i (-a_i).x_i$. Donc c'est un sous-groupe additif.

Enfin si $a \in A$, alors $a.(\sum_i a_i x_i) = \sum_i (a.a_i).x_i$. C'est donc bien un idéal. Il contient $x_i = 0.x_1 + 0.x_2 + \ldots + 1.x_i + 0.x_{i+1} \cdots + 0.x_k$. Il contient donc $\langle x_1, \ldots, x_k \rangle$. □

Corollaire 1.13
Soient I_1 et I_2 deux idéaux, alors $(I_1, I_2) = I_1 + I_2$. En particulier $(x_1, x_2) = (x_1) + (x_2)$.

1.4 Idéaux et morphismes

Proposition 1.14
Soit $f : A \to B$ un morphisme d'anneau. Alors Ker$f$ est un idéal de A.

Plus généralement, si I est un idéal de B alors $f^{-1}(I)$ est un idéal de A.

Démonstration : On sait déjà que (Ker$f, +$) est un sous-groupe de $(A, +)$. Soit $x \in A$ et $y \in$ Ker$f$. Alors $f(x.y) = f(x).f(y) = f(x).0_B = 0_B$ donc $x.y \in$ Ker$f$.

Suite : exercice. □

Attention : Par contre, si I est un idéal de A, $f(I)$ n'est pas en général un idéal de B.

Caractéristique d'un anneau

Soit A un anneau (non nécessairement commutatif). Le noyau de l'unique morphisme $\mathbb{Z} \to A$ est un idéal de A donc de la forme $n\mathbb{Z}$, pour $n \in \mathbb{N}$. Cet entier est appelé *caractéristique* de l'anneau A.

Par exemple, la caractéristique de $\mathbb{Z}$ est 0, celle de $\mathbb{R}[X]$ aussi, celle de $\mathbb{Z}/n\mathbb{Z}$ est n.

2 Quotient par un idéal

2.1 Structure d'anneau de A/I

Définition 2.1 Soit A un anneau commutatif, et $I \subset A$ un idéal. On définit la relation dans A

$$x \sim y \Leftrightarrow x - y \in I.$$

C'est une relation d'équivalence (c'est la même que celle pour les sous-groupes). On note A/I l'ensemble des classes d'équivalence pour cette relation.

On va définir une structure d'anneau sur l'ensemble A/I. Les lois sont données par

$$\overline{x} + \overline{y} := \overline{x+y} \quad \text{et} \quad \overline{xy} := \overline{x.y} \quad \forall x, y \in A.$$

On a déjà vu que la loi $+$ est bien définie, et que $(A/I, +)$ est un groupe.

Vérifions que la loi $.$ est bien définie. Soient $x \sim x'$ et $y \sim y'$. Alors on a

$$x.y - x'.y' = x.y - x.y' + x.y' - x'.y' = x.\underbrace{(y-y')}_{\in I} - \underbrace{(x-x')}_{\in I}.y'$$

$y - y' \in I$ donc $x.(y-y') \in I$ de même $(x-x').y' \in I$, d'où $x.(y-y') + (x-x').y' \in I$, c'est-à-dire $x.y \sim x'.y'$. Donc la loi $.$ est bien définie.

De plus on a $(\overline{x}.\overline{y}).\overline{z} = \overline{x.y}.\overline{z} = \overline{(x.y).z} = \overline{x.(y.z)} = \overline{x}.\overline{y.z} = \overline{x}.(\overline{y}.\overline{z})$. Donc $.$ est associative.

On a aussi $(\overline{x} + \overline{y}).\overline{z} = \overline{x+y}.\overline{z} = \overline{(x+y).z} = \overline{x.z + y.z} = \overline{x.z} + \overline{y.z} = \overline{x}.\overline{z} + \overline{y}; \overline{z}$ Donc $.$ est distributive par rapport à $+$.

Enfin $\overline{1_A}.\overline{x} = \overline{1_A.x} = \overline{x}$. Donc $\overline{1_A}$ est un élément neutre pour $.$

On a donc finalement montré le théorème suivant.

Théorème 2.2
Soit A un anneau commutatif et $I \subset A$ un idéal. Alors $(A/I, +, .)$ est un anneau commutatif.

On retrouve ainsi la structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$ vue précédemment.

2.2 Théorème de projection

Théorème 2.3 (de factorisation)
Soit A un anneau commutatif et $I \subset A$ un idéal. Alors la projection naturelle $p : A \to A/I$ est un morphisme d'anneau.

De plus pour tout morphisme d'anneau $f : A \to B$ tel que $I \subset \mathrm{Ker} f$, f se factorise en un morphisme d'anneau $\overline{f} : A/I \to B$.

Démonstration : Même démo que pour les groupes. Il reste à montrer que $\overline{f}(\overline{x}.\overline{y}) = \overline{f}(\overline{x.y}) = f(x.y) = f(x).f(y) = \overline{f}(\overline{x}).\overline{f}(\overline{y})$. □

Théorème 2.4
Soit $f : A \to B$ un morphisme d'anneau. Alors on a un isomorphisme d'anneau $A/\mathrm{Ker} f \simeq \mathrm{Im}\, f$.

Démonstration : Par le théorème précédent, on a un morphisme d'anneau $\overline{f} : A/\mathrm{Ker} f \to \mathrm{Im}\, f$, puisqu'on a un morphisme d'anneau $f : A \to \mathrm{Im}\, f$ de noyau $\mathrm{Ker} f$. Vérifions qu'il est surjectif : Soit $y \in \mathrm{Im}\, f$, alors $y = f(x)$ avec $x \in A$. Par définition, on a donc $\overline{f}(\overline{x}) = y$ donc $y \in \mathrm{Im}\, \overline{f}$. Le morphisme $\overline{f}$ est donc surjectif.

Vérifions qu'il est injectif. Soit $\overline{x} \in A/\mathrm{Ker} f$ tel que $\overline{f}(\overline{x}) = 0_B$. Alors $f(x) = 0_B$ par définition de $\overline{f}$. Donc $x \in \mathrm{Ker} f$, c'est-à-dire $\overline{x} = \overline{0_A}$.Donc $\overline{f}$ est injective. □

Exemple 2.5 — Soit $f : \mathbb{R}[X] \to \mathbb{R}$ définie par $f(P) = P(0) = a_0$. On vérifie aisément que c'est un morphisme d'anneaux. Son noyau est l'ensemble des polynômes dont le terme constant est nul, c'est-à-dire l'ensemble des polynômes divisibles par X. On a donc $\mathrm{Ker} f = (X)$. Il est par ailleurs claire que f est surjectif. On obtient donc un isomorphisme $\mathbb{R}[X]/(X) \simeq \mathbb{R}$.

— On peut montrer de même que $f : \mathbb{R}[X] \to \mathbb{C}$ définie par $f(P) = P(i)$ se factorise en un isomorphisme $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$. En effet si $P(i) = 0$, alors en faisant la division euclidienne de P par X^2+1, on obtient que le reste R est un polynôme de degré $\leqslant 1$ qui s'annule en i. Comme les coefficients de P sont réels, on a $P(-i) = 0$, et R s'annule aussi en $-i$, donc $R = 0$.

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

On a déjà vu que $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif.

3.1 Propriétés de $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.1
$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier ou nul.

Démonstration : On sait déjà que $\mathbb{Z} = \mathbb{Z}/0\mathbb{Z}$ est intègre. Soit $n = pq$ non premier. Alors on a $\bar{p}\bar{q} = \bar{0}$ avec $\bar{p}, \bar{q} \neq \bar{0}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. Réciproquement, si n est premier, alors $\bar{a}\bar{b} = \bar{0}$ implique n divise ab. Par le lemme d'Euclide, on aura alors n divise a ou n divise b, c'est-à-dire $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. □

Corollaire 3.2
Si A est intègre, sa caractéristique est 0 ou un nombre premier.

Démonstration : Soit A un anneau intègre, et soit n sa caractéristique. Alors par le théorème de factorisation, on a un morphisme injectif $f : \mathbb{Z}/n\mathbb{Z} \to A$. Si $\overline{a}\overline{b} = \overline{0}$ alors $f(\overline{a})f(\overline{b}) = 0_A$. Comme A est intègre, on a alors $f(\overline{a}) = 0_A$ ou $f(\overline{b}) = 0_A$. Puisque f est injective on déduit $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Autrement dit $\mathbb{Z}/n\mathbb{Z}$ est intègre. On a donc $n = 0$ ou n est premier. □

Théorème 3.3
$\mathrm{Inv}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} \text{ tels que } k \wedge n = 1\}$

Démonstration : On a les équivalences suivantes :

$$\begin{aligned}
\overline{k} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists \overline{u} \in \mathbb{Z}/n\mathbb{Z} \text{ avec } \overline{k}.\overline{u} = \overline{1} \\
&\Leftrightarrow \exists u \in \mathbb{Z} \text{ avec } \overline{ku} = \overline{1} \\
&\Leftrightarrow \exists u \in \mathbb{Z} \text{ avec } ku - 1 \text{ divisible par } n \\
&\Leftrightarrow \exists u, v \in \mathbb{Z} \text{ avec } ku - 1 = nv \\
&\Leftrightarrow k \wedge n = 1
\end{aligned}$$

□

Corollaire 3.4
$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Corollaire 3.5 (Petit théorème de Fermat)
Si p est premier, alors pour tout $x \in \mathbb{Z}$ on a $x^p = x \mod p$.

Démonstration : En effet, si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est-à-dire que $(\mathbb{Z}/p\mathbb{Z}^*, .)$ est un groupe. Son ordre est $p-1$. Donc pour tout élément $\overline{x} \in \mathbb{Z}/p\mathbb{Z}^*$ on a $\overline{x}^{p-1} = \overline{1}$ (car dans un groupe l'ordre d'un élément divise l'ordre d'un groupe (Thm Lagrange)). Autrement dit, pour tout $x \in \mathbb{Z}$ tel que $\overline{x} \neq \overline{0}$ (ou $x \notin p\mathbb{Z}$), alors $x^{p-1} = 1 \mod p$. En multipliant par x de chaque côté, on obtient $x^p = x \mod p$. Enfin si x est divisible par p, alors clairement $x^p = 0 = x \mod p$. □

3.2 Fonction indicatrice d'Euler

Définition 3.6 Soit $n \in \mathbb{Z}$, on note $\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^\times) = |\{1 \leqslant k \leqslant n | k \wedge n = 1\}|$.

Proposition 3.7
Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Alors $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Démonstration : Un nombre k n'est pas premier avec p^α si et seulement si p divise k. Les entiers $\leqslant p^\alpha$ non premiers avec p^α sont donc

$$\{p, 2p, 3p, \ldots, p^\alpha = p^{\alpha-1}p\}.$$

Il y en a $p^{\alpha-1}$ donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

3.3 Théorème des restes chinois

Théorème 3.8 (des restes chinois)
Soit $n_1, n_2, \ldots, n_k$ des entiers premiers entre eux deux à deux, et $n = n_1 n_2 \ldots n_k$ leur produit. Alors le morphisme $\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ qui à $x \in \mathbb{Z}$ associe $(x\ [n_1], \ldots, x\ [n_k])$ se favorise en un isomorphisme d'anneau

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Démonstration :Tout d'abord remarquons que ce morphisme est bien un morphisme d'anneau. Montrons ensuite la factorisation. Si $x = 0\ [n]$ alors n divise x, donc pour tout i, n_i divise x et donc l'image de x par l'application est alors nulle.

On va calculer le noyau de ce morphisme. Soit $x \in \mathbb{Z}$ tel que $x = 0\ [n_i]$ pour tout i. Donc x est divisible par le ppcm des n_i. Or comme les n_i sont premiers entre eux deux à deux, le ppcm des n_i est leur produit c'est-à-dire n. Donc $x = 0\ [n]$. Cela prouve l'injectivité du morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$.

Enfin, comme $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ ont même cardinal, le morphisme est aussi surjectif. □

On voit que la surjectivité du morphisme se déduit de la preuve. On peut aussi montrer "à la main" que c'est surjectif en utilisant l'identité de Bezout. En effet on a pour tout i, $n_i \wedge \prod_{j \neq i} n_j = n_i \wedge \frac{n}{n_i} = 1$. On peut donc trouver des entiers u_i et v_i tels que $u_i n_i + v_i \frac{n}{n_i} = 1$. Posons $e_i = v_i \frac{n}{n_i}$. On a alors $e_i = 0[n_j]$ pour $j \neq i$, et $e_i = 1[n_i]$, autrement dit $\Phi(e_i) = (0, 0, \ldots, 1, 0 \ldots)$. Les $\Phi(e_i)$ sont des générateurs du groupe $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$, cela montre donc que Φ est surjective. Cela permet aussi de construire l'application réciproque. Prenons un exemple avec $\mathbb{Z}/30\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et calculons l'image réciproque de $(\overline{1}, \overline{2}, \overline{3})$.

On a $2 \wedge 15 = 1$, donc $15 - 2.7 = 1$ donc $e_1 = 15$. On a $3 \wedge 10 = 1$, donc $10 - 3.3 = 1$ donc $e_2 = 10$. Enfin $5 \wedge 6 = 1$ donc $6 - 5 = 1$ et $e_3 = 6$. On aura donc

$$\begin{aligned}(\overline{1}, \overline{2}, \overline{3}) &= (\overline{1}, \overline{0}, \overline{0}) + 2(\overline{0}, \overline{1}, \overline{0}) + 3(\overline{0}, \overline{0}, \overline{1}) \\ &= \Phi(e_1) + 2\Phi(e_2) + 3\Phi(e_3) \\ &= \Phi(e_1 + 2e_2 + 3e_3) \\ &= \Phi(15 + 2.10 + 3.6) = \Phi(53)\end{aligned}$$

On vérifie bien que 23 est une solution.

Corollaire 3.9
Soit $n \in \mathbb{Z}$ et $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. Alors on a un isomorphisme d'anneaux :

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{s} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Corollaire 3.10
Soit $n \in \mathbb{Z}$ et $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. Alors $\phi(n) = \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1)$.

Démonstration : Le corollaire précédent donne un isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{s} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times.$$

En effet les inversibles d'un anneau produit sont $A_1^\times \times A_2^\times$. Et on applique la proposition précédente.

□

4 Idéaux premiers et maximaux

4.1 Idéal premier

Définition 4.1 Soit A un anneau commutatif. Un idéal $I \subset A$ est dit *premier* si $I \neq A$ et

$$\forall a, b \in A, \quad a.b \in I \Rightarrow a \in I \text{ ou } b \in I.$$

Exemple 4.2 Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ où p est premier et $0\mathbb{Z}$. En effet, par le lemme de Gauss, si ab est divisible par p premier, alors p divise a ou p divise b. Réciproquement, si $p\mathbb{Z}$ est premier et $p = q.r$ alors p divise q ou p divise r, ce qui montre que p est premier.

Proposition 4.3
Un idéal $I \subset A$ est premier si et seulement si A/I est un anneau intègre.

Démonstration : Supposons que I soit premier. On va montrer que A/I ne contient pas de diviseur de zéro. Soit $a, b \in A$ tels que $\overline{a}.\overline{b} = \overline{0}$. Alors $\overline{ab} = \overline{0}$ c'est-à-dire $ab \in I$. Donc par hypothèse, on a $a \in I$ ou $b \in I$, autrement dit $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, donc A/I est intègre.

Réciproquement supposons que A/I soit intègre. Soit $ab \in I$, alors $\overline{a}\overline{b} = \overline{0}$ et donc $a \in I$ ou $b \in I$. □

4.2 Idéal maximal

Définition 4.4 Un idéal $I \subset A$ est dit *maximal* si $I \neq A$ et si pour tout idéal J contenant strictement I, alors $J = A$.

Proposition 4.5
I est maximal si et seulement si A/I est un corps.

Démonstration : Soit I maximal, et $a \in A - I$ (existe car $I \neq A$), c'est-à-dire $\overline{a} \neq \overline{0}$ dans A/I. On va montrer que $\overline{a}$ est inversible. En effet l'idéal engendré par I et a $\langle I, a\rangle$ contient strictement I. Donc il est égal à A, et contient 1. Autrement dit $1 = au + b$ avec $b \in I$. Donc $\overline{1} = \overline{au} + \overline{b} = \overline{au}$ c'est-à-dire $\overline{a}$ est inversible.

Réciproquement, supposons que A/I soit un corps. Soit J un idéal contenant strictement I. Prenons $a \in J - I$. Alors $\overline{a} \neq \overline{0}$ dans A/I, donc $\overline{a}$ est inversible par définition. Ceci implique l'existence de $u \in A$ tel que $\overline{au} = \overline{1}$, c'est-à-dire $au-1 \in I$. Donc $1 = au-(au-1)$ avec $au \in J$ et $(au-1) \in I \subset J$, donc $1 \in J$, ce qui montre $A = J$. □

Exemple 4.6 Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ où p est premier. Attention, l'idéal $\{0\}$ n'est pas maximal, mais premier.

Corollaire 4.7
I maximal $\Rightarrow$ I premier.

Démonstration : I maximal $\Rightarrow$ A/I corps $\Rightarrow$ A/I intègre $\Rightarrow$ I premier. □

Corollaire 4.8
A est un corps si et seulement si ses seuls idéaux sont (0_A) et A.

Démonstration : Soit A un corps et $I \neq 0_A$ un idéal. Soit $u \in I$ avec $u \neq 0_A$, alors u est inversible, et donc $1_A = uu^{-1} \in I$ et $I = A$.

Réciproquement, si les seuls idéaux de A sont (0_A) et A, alors (0_A) est un idéal maximal. On aura donc $A = A/(0_A)$ est un corps. □

5 Aritmétique dans un anneau intègre

On suppose ici que A est intègre.

5.1 Divisibilité

Définition 5.1 On dit que $a \in A$ *divise* $b \in A$ si il existe $x \in A$ tel que $b = ax$. On dit alors que a est un diviseur de b, ou que b est un multiple de a et on note $a|b$.

Proposition 5.2
Soient $a, b \in A$.

- $a|b$ si et seulement si $(b) \subset (a)$ (c'est donc une relation d'ordre sur les éléments de A).
- $a|b$ et $b|a$ si et seulement si $a = ub$ avec u inversible. (On dit alors que a et b sont associés).

Démonstration : Supposons que $b = ax$. Soit $y \in (b)$, alors $y = bz$ avec $z \in A$. Donc $y = axz = a(xz) \in (a)$.

Réciproquement, si $(b) \subset (a)$ alors $b \in (a)$, c'est-à-dire $b = ax$ pour un certain $x \in A$.

Si $a = bx$ et $b = ay$, alors $a = bx = ayx = a(yx)$. Comme A ne contient pas de diviseur de zéro on peut simplifier pas a et on obtient $yx = 1$, c'est-à-dire que x et y sont inversibles. □

Exemple 5.3
- Dans $\mathbb{Z}$, a et b sont associés si et seulement si $a = b$ ou $a = -b$.
- Dans $A[X]$, P et Q sont associés si et seulement si il existe $a \in \mathrm{Inv}(A)$ tel que $P = aQ$. Par exemple $X + 1$ et $3X + 3$ sont associés dans $\mathbb{R}[X]$ mais pas dans $\mathbb{Z}[X]$.

— $(1+i)|2$ dans $\mathbb{Z}[i]$.

5.2 Anneau principal, pgcd, ppcm

Définition 5.4 Un anneau A est dit *principal* s'il est intègre et si tout idéal est de la forme (a).

Définition 5.5 Soient $a_1, \ldots, a_n$ des éléments de A principal.

Un élément $\delta \in A$ est appelé *pgcd* (plus grand commun diviseur) de $a_1, \ldots, a_n$ si on a $(a_1)+\cdots+(a_n) = (\delta)$. Il existe et est unique à multiplication par un inversible prés. On le note $a_1 \wedge \ldots \wedge a_n$.

Si $(a_1) + (a_2) + \ldots + (a_n) = A = (1)$ alors on dit que $a_1, a_2, \ldots, a_n$ sont premiers entre eux dans leur ensemble. (Si $n = 2$ on dit seulement que a_1 et a_2 sont premiers entre eux.)

Un élément $\mu \in A$ est appelé *ppcm* (plus petit commun multiple) de $a_1, \ldots, a_n$ si on a $(a_1)\cap\ldots\cap(a_n) = (\mu)$. Il existe et est unique à multiplication par un inversible prés. On le note $a_1 \vee \ldots \vee a_n$.

Exemple 5.6 On a déjà vu que dans $\mathbb{Z}$, $p\mathbb{Z} + q\mathbb{Z} = (p \wedge q)\mathbb{Z}$ et $p\mathbb{Z} \cap q\mathbb{Z} = (p \vee q)\mathbb{Z}$.

Corollaire 5.7 (Théorème de Bezout)
Les éléments $a_1, \ldots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si il existe des éléments v_i tels que $1_A = \sum_{i=1}^{n} a_i v_i$.

Proposition 5.8
Soit $a_1, \ldots, a_n \in A$. Notons $\delta = a_1 \wedge \ldots \wedge a_n$ et $\mu = a_1 \vee \ldots \vee a_n$.

1. δ divise tous les a_i et si d divise tous les a_i alors d divise δ.
2. Tous les a_i divisent μ et si m est divisible par tous les a_i alors μ divise m.

Démonstration : Pour tout i, $a_i \in (a_1) + \ldots + (a_n) = (\delta)$ donc δ divise a_i. De plus si d divise tous les a_i, alors $\delta = \sum_i a_i v_i = \sum_i da'iv_i = d(\sum_i a'iv_i)$ donc d divise δ.

$\mu \in (a_i)$ pour tout i donc a_i divise μ. Si a_i divise m pour tout i, alors m est dans l'intersection des (a_i) il est donc dans (μ) ce qui signifie que μ divise m.

□

Proposition 5.9
Soient a, b et c dans A. Alors on a les propriétés suivantes :

1. $a \vee b = b \vee a$ et $a \wedge b = b \wedge a$.
2. $a \vee (b \vee c) = a \vee b \vee c = (a \vee b) \vee c$ et $a \wedge (b \wedge c) = a \wedge b \wedge c = (a \wedge b) \wedge c$.
3. $ac \vee ab = a(c \vee b)$ et $ab \wedge ac = a(b \wedge c)$.
4. (Lemme de Gauss) si $a|bc$ et $a \wedge b = 1$ alors $a|c$.
5. $(a \vee b)(a \wedge b) = ab$.

Démonstration :

1. et (2) sont clairs.

(3) On a $(a(b \wedge c)) = a(b \wedge c) = a((b)+(c)) = (a(b)+a(c)) = ((ab)+(ac)) = (ab \wedge ac)$. De même pour $\vee$.

(4) On a $a|bc$ et $a|ac$ donc par la proposition précédente, a divise $ac \wedge bc$, qui est $(a \wedge b)c = c$ par (3).

(5) Notons $\delta = a \wedge b$ et $\mu = a \vee b$. On a alors $a = \delta a'$ et $b = \delta b'$, avec $a' \wedge b' = 1$. On veut montrer que $\mu = \delta a'b'$. On va montrer qu'ils se divisent l'un et l'autre. a divise $\delta a'b'$, et b aussi, donc μ divise $\delta a'b'$.
Ecrivons maintenant $\mu = ax = by = \delta a'x = \delta b'y$. Comme A est intègre, on a $a'x = b'y$. Donc a' divise $b'y$, et comme $a' \wedge b' = 1$ alors a' divise y par Gauss. On aura donc $\delta a'b'$ divise $\delta y b' = \mu$.

□

5.3 Eléments irréductibles

Définition 5.10 Un élément $a \in A$ est dit *irreductible* s'il n'est pas inversible et si ses seuls diviseurs sont les inversibles de A et les éléments associés à a.

Exemple 5.11 Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Proposition 5.12
Soit $a \in A$ non nul. Si (a) est premier, alors a est irréductible.

Démonstration : Soit $a = xy \in (a)$. Alors comme (a) est premier, on a $x \in (a)$ (ou $y \in (a)$), c'est-à-dire a divise x. Mais alors $a = xy = azy$, en simplifiant par a (A INTEGRE), on obtient que y est inversible. □

NB : la réciproque est fausse en général. Par exemple on peut montrer que 2 est irréductible dans $\mathbb{Z}[i\sqrt{3}]$, mais $4 = 2.2 = (1 + i\sqrt{3})(1 - i\sqrt{3}) \in (2)$, or $(1 + i\sqrt{3})$ n'est pas dans (2), donc (2) n'est pas premier.

Proposition 5.13
Soit A un anneau principal. Si a est irréductible, alors (a) est premier.

Démonstration : Soit a non inversible. On va montrer que (a) est maximal (il sera donc premier). D'abord $(a) \neq A$ car $a \notin A^\times$. Soit J un idéal contenant (a). Alors $J = (b)$ pour un certain $b \in A$. On a $(a) \subset (b)$ donc b divise a. Par irréductibilité de a, b est soit inversible, soit associé à a. S'il est inversible alors $J = A$, et s'il est assoccié à a alors $J = (a)$. L'idéal (a) est donc maximal.

□

Corollaire 5.14 (Lemme d'Euclide)
Soit A un anneau principal et p irréductible. Si p divise ab alors p divise a ou p divise b.

Démonstration : Par la proposition précédente, $ab \in (p)$ qui est premier, on a donc $a \in (p)$ ou $b \in (p)$. □

Chapitre VIII

Arithmétique dans les anneaux de polynômes

On supposera dorénavant que A est un anneau intègre, et donc $A[X]$ est aussi intègre.

1 Division euclidienne

1.1 Condition pour l'existence de la division

Théorème 1.1
Soit P_1 et P_2 deux polynômes de $A[X]$ (où A est intègre). On suppose que le coefficient dominant de P_2 est inversible dans A. Alors il existe des uniques polynômes Q et R tels que

$$P_1 = P_2Q + R \text{ et } \deg R < \deg P_2.$$

Démonstration :

Existence : On le démontre par récurrence sur le degré de P_1. Si $\deg P_1 < \deg P_2$ alors $Q = 0$ et $R = P_1$ conviennent. Supposons le résultat vrai pour $\deg P_1 \leqslant n$ et soit $\deg P_1 = n + 1$. Notons $P_2 = \sum_{j=0}^{m} b_j X^j$ avec $m \leqslant n + 1$. Alors le polynôme $P_1 - a_{n+1}b_m^{-1}X^{n+1-m}P_2$ est de degré $\leqslant n$. Par hypothèse de récurrence, on obtient

$$P_1 - a_{n+1}b_m^{-1}X^{n+1-m}P_2 = P_2Q + R,$$

donc

$$P_1 = (Q + a_{n+1}b_m^{-1}X^{n+1-m})P_2 + R.$$

Unicité : Si on a $P_1 = P_2Q + R = P_2S + T$, alors $P_2(Q - S) = T - R$. Le degré du terme de droite est inférieur à $\deg P_2$, tandis que celui du terme de gauche est $\deg P_2 + \deg(Q - S)$. On a donc nécessairement $Q - S = 0$, et donc $T - R = 0$.

□

Corollaire 1.2
On peut toujours faire une division euclidienne dans $k[X]$ si k est un corps.

Exemple 1.3 Faisons la division euclidienne de $\overline{2}X^2 - \overline{2}X + \overline{3}$ par $\overline{3}X - \overline{1}$ dans $\mathbb{Z}/7\mathbb{Z}[X]$. Il faut commencer par trouver l'inverse de $\overline{3}$. On peut le faire grâce à Bezout : $7 = 2.3 + 1$ donc $\overline{3}^{-1} = (-\overline{2}) = \overline{5}$. Puis on résout $\overline{3}x = \overline{2}$, ce qui donne $x = \overline{25} = \overline{3}$. On peut donc écrire

$$\begin{array}{r|l} \overline{2}X^2 - \overline{2}X + \overline{3} & \overline{3}X - \overline{1} \\ \underline{\overline{2}X^2 - \overline{3}X + 0} & ---- \\ X + \overline{3} & \overline{3}X + \overline{5} \\ \underline{X - \overline{5}} & \\ \overline{1} & \end{array}$$

Et on a $\overline{2}X^2 - \overline{2}X + \overline{3} = (\overline{3}X + \overline{5})(\overline{3}X - \overline{1}) + \overline{1}$.

1.2 Principalité d'un anneau de polynômes

La division euclidienne va nous permettre de savoir quand un anneau de polynôme est principal (ou ne l'est pas).

Théorème 1.4
$A[X]$ est principal si et seulement si A est un corps.

Démonstration : Supposons que A est un corps, et soit I un idéal de A différent de zéro. Posons $n = \min\{\deg P, P \in I \setminus \{0\}\}$, ce minimum existe car $I \neq 0$, et est atteint par un polynôme P de I. Soit S un polynôme de I. En faisant la division euclidienne de S par I, on obtient $S = QP + R$. Or $QP \in I$, donc $R = S - QP \in I$. C'est donc le polynôme nul par minimalité du degré. On a donc montré que $S \in (P)$. L'idéal I est alors principal.

Réciproquement, supposons que $A[X]$ est principal. Soit $a \in A$ non nul. Et posons $I = (X, a)$. Il existe donc un P tel que $(X, a) = (P)$. Comme P divise a, le degré de P est forcément 0, $P = b$. Maintenant b divise X, donc on peut écrire $X = (c_0 + c_1 X)b$, ce qui nous donne $c_1 b = 1$ et donc b est inversible.

Enfin $b \in (a, X)$, donc peut s'écrire $b = \lambda X + \mu a$, donc on a $b = \mu a$ et donc a est inversible. □

2 Polynômes à coefficients dans un corps

On suppose dorénavant que k est un corps.

2.1 Théorème des restes chinois

L'existence de la division euclidienne nous permet d'avoir un analogue du théorème des restes chinois dans $k[X]$ où k est un corps.

Théorème 2.1
Soit k un corps et soient P_1 et P_2 deux polynômes de $k[X]$ premiers entre eux. Alors le morphisme d'anneaux

$$\Phi : k[X] \longrightarrow k[X]/(P_1) \times k[X]/(P_2)$$

envoyant P sur ses classes modulo P_1 et P_2 se factorise en un isomorphisme d'anneaux

$$k[X]/(P_1 P_2) \simeq k[X]/(P_1) \times k[X]/(P_2).$$

Démonstration : La preuve est complétement similaire à celle pour $\mathbb{Z}$. En effet $\Phi(P) = 0$ est équivalent à dire que P_1 divise P et que P_2 divise P. Donc leur

ppcm divise P. Comme ils sont premiers entre eux, leur ppcm est P_1P_2. On a donc un morphisme d'anneau injectif $k[X]/(P_1P_2) \simeq k[X]/(P_1) \times k[X]/(P_2)$.

Pour montrer la surjectivité, on ne peut plus utiliser le cardinal. Mais par contre, on peut toujours utiliser l'algorithme de Bezout (puisque $k[X]$ est principal) pour construire l'application réciproque de Φ. Soit A et B deux polynômes. Soit $UP_1 + VP_2 = 1$ un couple de Bezout, et posons $P := BUP_1 + AVP_2$. Alors la classe de P modulo P_1 est $\overline{AVP_2} = \overline{1 - UP_1A} = \overline{A}$. De même la classe de P modulo P_2 est $\overline{B}$. On a donc montré que Φ était surjective.

□

Théorème 2.2
Soit k un corps, et P un polynôme non nul dans $k[X]$. Alors on a les équivalences

P est irréductible $\Leftrightarrow k[X]/(P)$ est un corps $\Leftrightarrow k[X]/(P)$ est intègre

Démonstration : La preuve est une conséquence du fait que $k[X]$ est principal et des propositions 5.12 et 5.13. En effet, si P est irréductible, alors (P) est maximal, et donc $k[X]/(P)$ est un corps, et donc intègre. Réciproquement, si $k[X]/(P)$ est intègre, alors (P) est premier, et donc par proposition 5.12, on a bien que P est irréductible.

□

2.2 Irréductibles dans $k[X]$

Dans cette section k est un corps.

On aimerait donc maintenant comprendre quels sont les irréductibles de $k[X]$.

Proposition 2.3
Soit $a \in k$. Alors $X - a$ est un polynôme irréductible de $k[X]$. De plus si $a \neq b$ alors $(X - a) \wedge (X - b) = 1$.

Démonstration : Si $X - a$ n'est pas irréductible, il s'écrit $X - a = P.Q$ où ni P ni Q ne sont inversibles, c'est-à-dire ni P ni Q ne sont des polynômes constants. C'est clairement impossible pour des raisons de degré.

Si $a \neq b$ alors on a $(b-a)^{-1}((X-a)-(X-b)) = 1_k$ on conclut par Bezout. □

Proposition 2.4
Soit $a \in k$ et $P \in k[X]$. Alors le reste de la division euclidienne de P par $X - a$ est $P(a)$

Démonstration : $P = (X-a)Q + R$ avec $\deg R \leqslant \deg(X-a) - 1 = 0$. Donc $R = r_0 \in k$ est un polynôme constant. Si on applique a alors on obtient $P(a) = R(a) = r_0$. □

Définition 2.5 Soit $P \in k[X]$ et $a \in k$. On dit que a est une *racine* de P si $P(a) = 0$, ou de manière équivalente si P est divisible par $X - a$.

On appelle *multiplicité* de $X - a$ dans P le grand petit entier k tel que le reste de la division euclidienne de P par $(X-a)^k$ est nul.

On dit que P est *scindé* dans $k[X]$ si il existe $a, a_1, \ldots, a_n \in k$ tels que $P = a\prod_{i=1}^{n}(X - a_i)^{r_i}$

Proposition 2.6
1. Un polynôme P non nul a au plus $\deg P$ racines distinctes.
2. Notons $r_1, \ldots, r_n$ les multiplicités respectives de $a_1, \ldots, a_n$ dans P. Alors on a $\deg P \geqslant r_1 + \cdots + r_n$.
3. Si k est infini et si $P(a) = 0$ pour tout $a \in k$ alors $P = 0$.

Démonstration :

1. Soient $a_1, \ldots, a_n$ des racines distinctes de P. Alors $X - a_1$ divise $P = (X - a_1)P_1$. Comme $a_1 \neq a_2$ on a que $(X - a_1)$ et $(X - a_2)$ sont premiers entre eux. Alors $X - a_2$ divise P_2 par Gauss. On montre ainsi par récurrence que P est divisible par $\prod_{i=1}^{n}(X - a_i)$. Son degré est donc plsu grand que n.

2. En utilisant le fait que $(X-a_1)^{r_1}$ est premier avec $\prod_{i\geqslant 2}(X-a_i)^{r_i}$ on démontre que $\prod_{i=1}^{n}(X-a_i)^{r_i}$ divise P.
3. C'est une conséquence de (1).

□

Remarque 2.7 Dans $\mathbb{Z}/p\mathbb{Z}$ le polynôme $X^p - X$ s'annule en tout point de $\mathbb{Z}/p\mathbb{Z}$ par le petit théorème de Fermat. Or il est non nul (au sens où tous ses coefficients ne sont pas nuls). Le morphisme d'anneau $k[X] \to \mathcal{F}(k,k)$ qui à un polynôme associe la fonction polynôme n'est pas toujours injectif.

2.3 Irréductibles dans $\mathbb{C}[X]$.

Ce théorème appelé théorème fondamental de l'algèbre est admis.

Théorème 2.8 (D'Alembert-Gauss)
$\mathbb{C}$ est algébriquement clos, c'est-à-dire que pour tout $P \in \mathbb{C}[X]$ non constant, il existe $a \in \mathbb{C}$ avec $P(a) = 0$.

Corollaire 2.9
Les irréductibles de $\mathbb{C}[X]$ sont de la forme $X - a$ avec $a \in \mathbb{C}$ (à multiplication par un scalaire non nul près.

Démonstration : On sait déjà que les polynômes $X - a$ sont irréductibles. Montrons qu'il n'y en a pas d'autres. En effet, soit P dans $\mathbb{C}[X]$ de degré $\geqslant 2$, alors P admet une racine a. Il est donc divisible par $X - a$. Ainsi tout polynôme de degré $\geqslant 2$ n'est pas irréductible. □

Théorème 2.10
Soit $P \in \mathbb{C}[X]$ non nul. Alors il existe $a, a_1, \dots a_r \in \mathbb{C}$ et $m_1, \dots m_r \in \mathbb{N}^*$ tels que

$$P = a \prod_{i=1}^{r} (X - a_i)^{m_i}.$$

Les a, a_i et m_i sont uniques.

Démonstration : L'existence se démontre facilement par récurrence sur le degré de P.

Montrons l'unicité par récurrence sur le degré de P. Si le degré de P est 1, alors $P = a(X - a_1) = b(X - b_1)$, on obtient donc $a = b$ et $a_1 = b_1$.

Supposons l'unicité pour P de degré $n - 1$. Alors si on a

$$P = a \prod_{i=1}^{r} (X - a_i)^{m_i} = b \prod_{j=1}^{s} (X - b_j)^{n_j},$$

$X - a_1$ divise $b \prod_{j=1}^{s} (X - b_j)^{n_j}$, et comme $X - a_1$ est irréductible, par le lemme d'Euclide, $X - a_1$ divise un des $X - b_j$. Par le proposition 2.3 il existe j tel que $b_j = a_1$. On supposera $j = 1$ quitte à réindexer les b_j. En simplifiant par $X - a_1$ ($k[X]$ est intègre), on obtient $(X - a_1)^{m_1 - 1} a \prod_{i=2}^{r} (X - a_i)^{m_i} = (X - b_1)^{n_1 - 1} b \prod_{j=2}^{s} (X - b_j)^{n_j}$, de degré $n - 1$. On conclut alors à l'aide de l'hypothèse de récurrence.

□

2.4 Irréductibles dans $\mathbb{R}[X]$.

Lemme 2.11
Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$. Notons $\bar{P}$ le polynôme $\bar{P} := \sum_{i=0}^{n} \bar{a}_i X^i \in \mathbb{C}[X]$. Alors α est racine de P si et seulement si $\bar{\alpha}$ est racine de $\bar{P}$.

Démonstration : Soit α une racine de P. Alors on a $\bar{P}(\bar{\alpha}) = \sum_{i=0}^{n} \bar{a}_i \bar{\alpha}^i = \overline{\sum_{i=0}^{n} a_i \alpha^i} = \overline{P(\alpha)} = 0$, donc $\bar{\alpha}$ est une racine de $\bar{P}$. □

Le théorème fondamental de l'algèbre nous permet de démontrer les résultat suivant.

Théorème 2.12
Les polynômes irréductibles de $\mathbb{R}[X]$ sont de la forme $X - a$ avec $a \in \mathbb{R}$ et $X^2 + bX + c$ avec $b^2 - 4c < 0$ (à multiplication par un scalaire près).

Démonstration :[Démonstration du théorème 2.12]

Notons tout d'abord que $X^2 + bX + c$ avec $b^2 - 4c < 0$ est irréductible. En effet, s'il était réductible, il s'écrirait comme le produit de deux polynômes de degré 1 à coeeficients réels. Cette égalité serait vraie dans $\mathbb{C}[X]$, et donc par unicité de la décomposition en irréductibles, on obtiendrait une contradiction.

Montrons maintenant qu'il n'y a pas d'autres irréductibles.

Soit P un irréductible dans $\mathbb{R}[X]$. Alors P est aussi dans $\mathbb{C}[X]$ et $P = \bar{P}$ car tous ses coefficients sont réels. Il a donc une racine complexe α. Si α est réelle, alors P est divisible par $X - \alpha$, donc par irréductibilité $P = a(X - \alpha)$ pour $a \in \mathbb{R}$.

Si α n'est pas réel, alors par le lemme $\bar{\alpha} \neq \alpha$ est racine de $\bar{P} = P$. Comme $X - \alpha$ et $X - \bar{\alpha}$ sont premiers entre eux, leur produit $(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha}$ divise P. Par ailleurs $X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = (X^2 + 2\mathrm{Re}(\alpha) + ||\alpha||^2)$ est dans $\mathbb{R}[X]$. Donc par irréductibilité, $P = a(X^2 + 2\mathrm{Re}(\alpha) + ||\alpha||^2)$. □

On en déduit alors le théorème suivant.

Théorème 2.13
Soit $P \in \mathbb{R}[X]$ non nul. Alors il existe $a, a_1, \ldots a_r \in \mathbb{R}$ et $m_1, \ldots m_r \in \mathbb{N}^*$, $(b_1, c_1) \neq (b_2, c_2), \ldots, (b_t, c_t) \in \mathbb{R}^2$ avec $b_j^2 - 4c_j < 0$ et $n_1, \ldots, n_t$ tels que

$$P = a \prod_{i=1}^{r} (X - a_i)^{m_i} \prod_{j=1}^{t} (X^2 + b_j X + c_j)^{n_j}.$$

Les a, a_i, m_i, b_j, c_j et n_j sont uniques.

Algèbre linéaire

Chapitre IX

Déterminant

Dans tout ce chapitre, k est un corps, et E sera un k-espace vectoriel de dimension finie.

1 Forme multilinéaires

1.1 Définition et premières propriétés

Définition 1.1 Soit $p \geqslant 1$ un entier. Une *forme p-linéaire* sur E est une application $f : E^p \to k$ telle que Pour tout $j = 1, \ldots, p$ on a

$$f(x_1, \ldots, x_j + \lambda y_j, \ldots, x_p) = f(x_1, \ldots, x_p) + \lambda f(x_1, \ldots, y_j, \ldots, x_p),$$

et ce pour tous vecteurs x_i, y_i, scalaire λ.

Exemple 1.2 Pour $p = 1$, ce sont les formes linéaires sur E noté $\mathcal{L}(E, k)$.

Pour $p = 2$, ce sont les formes bilinéaires, par exemple un produit scalaire dans E.

Pour $n = 1$ et p quelconque, l'application $k^p \to k$ qui à $(x_1, \ldots, x_p)$ associe $\prod x_i$ est p-linéaire.

Proposition 1.3
Soient f et g deux formes p-linéaires, et $\mathcal{B}$ une base de E. Alors $f = g$ si et seulement si f et g prennent les mêmes valeurs sur les vecteurs de $\mathcal{B}$.

Proposition 1.4
L'ensemble des forme p-linéaires forme un k-espace vectoriel de dimension finie.

1.2 Formes alternées

Définition 1.5
- Une forme p-linéaire est dite *symétrique* si $f(\ldots, x, \ldots, y \ldots) = f(\ldots, y, \ldots, x \ldots)$.
- Une forme p-linéaire est dite *antisymétrique* si $f(\ldots, x, \ldots, y \ldots) = -f(\ldots, y, \ldots, x \ldots)$.
- Une forme p-linéaire est dite *alternée* si $f(\ldots, x, \ldots, x \ldots) = 0$.

Proposition 1.6
Si la caractéristique de k est différente de 2, alors on a f antisymétrique $\Leftrightarrow$ f alternée.

Démonstration : Si f est antisymétrique, on a $f(\ldots, x, \ldots, x, \ldots) = -f(\ldots, x, \ldots, x, \ldots)$, donc $2f(\ldots, x, \ldots, x, \ldots) = 0$.

Si f est alternée, on a $f(\ldots, x+y, \ldots, x+y, \ldots) = 0$, en développant on obtient $f(\ldots, x, \ldots, y, \ldots) + f(\ldots, y, \ldots, x, \ldots) = 0$. □

Il est facile de voir que l'ensemble des formes p-linéaires alternées forme un sous-espace vectoriel de l'espace des formes p-linéaires.

Proposition 1.7
Si f est alternée, alors pour toute famille liée $(x_1, \ldots, x_p)$ on a $f(x_1, \ldots, x_p) = 0$.

Démonstration : C'est clair en utilisant la linéarité. □

Corollaire 1.8
Si $p \geqslant n+1$ alors il n'existe pas de forme p-linéaire alternée sur E.

2 Déterminant d'un système de vecteurs

Le but va être maintenant d'étudier l'espace des formes n-linéaires alternées sur E.

2.1 Espace vectoriel des formes n-linéaires alternées sur E

Théorème 2.1
Soit f une forme n-linéaire alternée, et soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Alors f ne dépend que de la valeur $f(e_1, \ldots, e_n)$ et on a la formule :

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \lambda_{\sigma(1),1} \cdots \lambda_{\sigma(n),n} f(e_1, \ldots, e_n),$$

où $x_j = \sum_i \lambda_{ji} e_i$. De plus pour tout $\alpha \in k$, il existe une (unique) forme n-linéaire alternée telle que $f(e_1, \ldots, e_n) = \alpha$.

Démonstration : Par n-linéarité on a

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} \lambda_{i_1,1} \lambda_{i_n,n} f(e_{i_1}, \ldots, e_{i_n}).$$

Comme f est alternée, $f(e_{i_1}, \ldots, e_{i_n}) = 0$ dès que deux des indices sont égaux, donc on peut réécrire la somme de la manière suivante :

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \lambda_{\sigma(1),1} \lambda_{\sigma(n),n} f(e_{\sigma(1)}, \ldots, e_{\sigma(n)}).$$

Soit $\sigma \in \mathfrak{S}_n$, et $\sigma = \tau_1 \cdots \tau_r$ une décomposition en produits de transpositions. En utilisant l'antisymétrie, on montre par récurrence sur r que $f(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) = (-1)^r f(e_1, \ldots, e_n)$.

Enfin, il faut de montrer que la formule

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \lambda_{\sigma(1),1} \cdots \lambda_{\sigma(n),n} \alpha$$

définit une application n-linéaire alternée :

$$\begin{aligned} f(x_1 + \mu x'_1, \ldots, x_n) &= \sum_i \sum_{\sigma, \sigma(i)=1} \epsilon(\sigma) \lambda_{\sigma(1),1} \cdots (\lambda_{i,1} + \mu \lambda'_{i,1}) \cdots \lambda_{\sigma(n),n} \alpha \\ &= \sum_i \sum_{\sigma, \sigma(i)=1} \epsilon(\sigma) \lambda_{\sigma(1),1} \cdots \lambda_{i,1} \cdots \lambda_{\sigma(n),n} \alpha \\ &+ \mu \sum_i \sum_{\sigma, \sigma(i)=1} \epsilon(\sigma) \lambda_{\sigma(1),1} \cdots \lambda'_{i,1} \cdots \lambda_{\sigma(n),n} \alpha \\ &= f(x_1, \ldots, x_n) + \mu f(x'_1, \ldots, x_n), \end{aligned}$$

f est donc n-linéaire.

Par ailleurs si f et g sont deux formes n-linéaires alternées telles que $f(e_1, \ldots, e_n) = g(e_1, \ldots, e_n)$, alors , pour toute permutation σ on a $f(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) = g(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$. Les applications f et g sont donc égales sur une base, elles sont donc égales.

□

Corollaire 2.2
Le sous-espace des formes n-linéaires alternées est un sous-espace de dimension 1.

2.2 Définition

Définition 2.3 Soit $\mathcal{B}$ une base de E. Le *déterminant dans la base* $\mathcal{B}$ est l'unique application n-linéaire alternée $\det_{\mathcal{B}}$ telle que

$$\det_{\mathcal{B}}(e_1, \ldots, e_n) = 1.$$

Proposition 2.4
Soient $\mathcal{B}$ et $\mathcal{B}'$ des base de E. Alors on a

$$\det_{\mathcal{B}'} = \det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}.$$

En particulier $\det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}(\mathcal{B}') = 1$, et donc le déterminant ne s'annule jamais sur une famille libre. On a donc la réciproque de la Proposition 1.7.

Démonstration : Ce sont deux applications n-linéaires alternées, qui prennent la même valeur sur $\mathcal{B}$. □

2.3 Formule de récurrence

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base. On note $\mathcal{B}^\ell = \mathcal{B} \setminus \{e_\ell\}$, $E_\ell = \text{vect}(\mathcal{B}^\ell)$ et $p_\ell : E \to E_\ell$ la projection sur E_ℓ parallélement à $\text{vect}(e_\ell)$.

Lemme 2.5
On a la formule $\det_{\mathcal{B}}(e_\ell, x_2, \ldots, x_n) = (-1)^{\ell+1} \det_{\mathcal{B}^\ell}(p_\ell(x_2), \ldots, p_\ell(x_n))$.

Démonstration : Les deux applications envoyant $(x_2, \ldots, x_n) \in E^{n-1}$ sur les deux termes de la formule sont $n-1$-linéaires. Elles sont de plus clairement alternées. Pour vérifier qu'elles coincident, il suffit de le vérifier sur des vecteurs de $\mathcal{B}$ (qui sont donc 2 à 2 distincts). De plus, si un des vecteurs est e_ℓ, alors le terme de gauche est nul, et celui de droite aussi car $p_\ell(e_\ell) = 0$.

Par ailleurs, si on restreint ces applications à E_ℓ^{n-1}, elles sont $n-1$-linéaires alternées sur un espace de dimension $n-1$. Il suffit donc de vérifier qu'elles coincident sur $\mathcal{B}^\ell$. Or on a $\det_{\mathcal{B}}(e_\ell, \mathcal{B}^\ell) = (-1)^{\ell+1} \det_{\mathcal{B}}(\mathcal{B}) = (-1)^{\ell+1} \det_{\mathcal{B}^\ell}(\mathcal{B}^\ell)$.

□

Corollaire 2.6
Si $x_1 = \sum_{\ell=1}^{n} \lambda_{\ell 1} e_\ell$, alors on a la formule

$$\det_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\ell=1}^{n} (-1)^{\ell+1} \lambda_{\ell 1} \det_{\mathcal{B}^\ell}(p_\ell(x_2), \ldots, p_\ell(x_n)).$$

3 Déterminant d'un endomorphisme

3.1 Définition

Soit $u \in \mathcal{L}(E)$ un endomorphisme de E. Soit $\mathcal{B}$ une base de E. Alors l'application $(x_1, \ldots, x_n) \mapsto \det_{\mathcal{B}}(u(x_1), \ldots, u(x_n))$ est n-linéaire alternée. Donc il existe un scalaire $\alpha \in k$ tel que $\det_{\mathcal{B}}(u(x_1), \ldots, u(x_n)) = \alpha \det_{\mathcal{B}}(x_1, \ldots, x_n)$.

On va montrer que ce scalaire α ne dépend pas de la base $\mathcal{B}$.

En effet, par la formule de changement de base, si $\mathcal{B}'$ est une autre base, on a

$$\begin{aligned} \det_{\mathcal{B}'}(u(x_1), \ldots, u(x_n)) &= \det_{\mathcal{B}}(u(x_1), \ldots, u(x_n)) \det_{\mathcal{B}'}(\mathcal{B}) \\ &= \alpha \det_{\mathcal{B}}(x_1, \ldots, x_n) \det_{\mathcal{B}'}(\mathcal{B}) \\ &= \alpha \det_{\mathcal{B}'}(x_1, \ldots, x_n). \end{aligned}$$

Ceci nous incite à poser la définition suivante :

Définition 3.1 Soit $u \in \mathcal{L}(E)$ un endomorphisme de E. Le *déterminant* de u est l'unique scalaire $\det u \in k$ tel que pour toute base $\mathcal{B}$ de E et toute famille de vecteurs $(x_1, \ldots, x_n)$ on ait

$$\det_{\mathcal{B}}(u(x_1), \ldots, u(x_n)) = (\det u) \det_{\mathcal{B}}(x_1, \ldots, x_n).$$

Proposition 3.2

1. Soient u et v dans $\mathcal{L}(E)$. On a l' égalité $\det(u \circ v) = \det(u) \det(v)$.
2. soit $u \in \mathcal{L}(E)$. Alors u est inversible si et seulement si $\det u \neq 0$. Dans ce cas, on a $\det(u^{-1}) = \frac{1}{\det u}$.

Démonstration : provient directement de la définition. □

3.2 Déterminant d'une matrice

Définition 3.3 Soit $A \in \mathcal{M}_n(k)$. Alors on note $\det A = \det u$ où u est défini par $A = \mathrm{Mat}(u, \mathcal{B}, \mathcal{B})$. On a alors la formule

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

On retrouve alors les formules connues pour $n = 2$ et $n = 3$.
Pour $n = 2$, on obtient

$$\det A = a_{11}a_{22} - a_{12}a_{21},$$

en effet le premier terme correspond à la permutation identité, tandis que le deuxième terme correspond à la transposition (12) dont la signature est -1.
Pour $n = 3$, on obtient

$$\det A = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{21}a_{12}a_{33} \dots$$

Le premier terme correspond à l'identité, le deuxième au 3-cycle (123), le troisième au 3-cycle (132), tous de signature 1. Le quatrième terme correspond à la tranposition (12) de signature -1.

Remarque 3.4 Notons que le propriétés du type "la valeur du déterminant ne change pas si on remplace la colonne c_i par $c_i + \sum \lambda_j c_j$" etc... se déduisent directement de la n-linéarité du déterminant.

On retrouve aussi les propriétés bien connues de déterminant.

Proposition 3.5
Soit A une matrice triangulaire, alors $\det A = \prod_{i=1}^{n} a_{ii}$.
Soit A une matrice triangulaire par bloc de la forme

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

alors on a $\det A = \det B \det C$.

Démonstration : Montrons la deuxième assertion. Notons p la taille de la matrice B. Soit $\sigma \in \mathfrak{S}_n$ telle que $a_{\sigma(1)1} \dots a_{\sigma(n),n} \neq 0$. Alors pour tout $i \leqslant p$, on a $\sigma(i) \leqslant p$. On en déduit donc que pour tout $i \geqslant p+1$, on a $\sigma(i) \geqslant p+1$. Ceci implique que l'ensemble $\{1, \dots, p\}$ est une union d'orbites de σ, et que l'ensemble $\{p+1, \dots, n\}$ aussi. Ceci veut dire que l'on peut écrire $\sigma = \sigma_1 \circ \sigma_2$ avec $\mathrm{Supp}(\sigma_1) \subset \{1, \dots, p\}$ et $\mathrm{Supp}(\sigma_2) \subset \{p+1, \dots, n\}$. Par ailleurs, l'application $\mathfrak{S}_p \times \mathfrak{S}_{n-p} \to \mathfrak{S}_n$ envoyant (σ_1, σ_2) sur $\sigma_1 \circ \sigma_2$ est injective On peut donc écrire

$$\begin{aligned}
\sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n} &= \sum_{\sigma_1 \in \mathfrak{S}_p} \sum_{\sigma_2 \in \mathfrak{S}_{n-p}} \epsilon(\sigma_1 \circ \sigma_2) \dots \\
&= \left(\sum_{\sigma_1 \in \mathfrak{S}_p} \epsilon(\sigma_1) a_{\sigma_1(1)1} \dots a_{\sigma_1(p),p} \right) \cdot \\
&\quad \left(\sum_{\sigma_2 \in \mathfrak{S}_{n-p}} \epsilon(\sigma_2) a_{\sigma_2(p+1)p+1} \dots a_{\sigma_2(n),n} \right)
\end{aligned}$$

□

4 Polynôme caractéristique

4.1 Polynôme caractéristique d'une matrice

Définition 4.1 Soit $A \in \mathcal{M}_n(k)$. Le *polynôme caractéristique* de A est défini comme

$$\chi_A(X) = \det(X\mathrm{I}_n - A)$$

Notons ici que de manière cachée, on se place dans l'anneau $\mathcal{M}_n(k[X])$. En effet, la matrice de $X\mathrm{I}_n - A$ peut-être vue comme un élément de $\mathcal{M}_n(k[X])$. Le déterminant est donc bien défini, et est un "scalaire" donc dans $k[X]$.

Proposition 4.2
Soit $A \in \mathcal{M}_n(k)$. On a la formule

$$\chi_A(X) = X^n - (\mathrm{tr}A)X^{n-1} + \dots + (-1)^n \det A.$$

Démonstration : Notons b_{ij} les coefficients de la matrice $X\mathrm{I}_n - A$ (ce sont donc des polynômes !)

Tout d'abord notons que le degré de χ_A est inférieur ou égale à n car $\deg b_{\sigma(1)1} \dots b_{\sigma(n)n} = \sum_i \deg b_{\sigma(i)i}$ et que chaque coeeficient de la matrice a degré $\leqslant 1$.

Par ailleurs si σ n'est pas l'identité, alors il existe au moins deux i tels que $b_{\sigma(i)i}$ est de degré 0, et donc le degré de $b_{\sigma(1)1} \dots b_{\sigma(n)n}$ est inférieur ou égal à $n-2$. Le coefficient devant X^n provient alors de l'unique terme $b_{11} \dots b_{nn}$. Comme $b_{ii} = X - a_{ii}$, on obtient que le coefficient devant X^n est le même que celui du polynôme $\prod_i (X - a_{ii})$. C'est donc 1. Le coefficient devant X^{n-1} du polynôme caractéristique est aussi le même que celui du polynôme $\prod_i (X - a_{ii})$, c'est donc $-\sum_i a_{ii}$.

Enfin, on a $\chi_A(0) = \det(-A) = (-1)^n \det(A)$ qui est le terme constant de χ_A.

□

4.2 Polynôme caractéristique d'un endomorphisme

Soit $\mathcal{B}$ une base de E. Alors on un isomorphisme

$$\Phi_{\mathcal{B}} := \mathcal{L}(E) \longrightarrow \mathcal{M}_n(k).$$

Soit $u \in \mathcal{L}(E)$, on peut donc calculer $\chi_{\Phi_{\mathcal{B}}(u)}$ qui a priori dépend de la base $\mathcal{B}$. La propriété suivante nous dit que ce polynôme ne dépend pas du choix de la base $\mathcal{B}$.

Proposition 4.3
Soit $A \in \mathcal{M}_n(k)$ et $P \in GL_n(k)$. Alors on a

$$\chi_{P^{-1}AP} = \chi_A.$$

Démonstration : En effet, on a

$$\chi_{P^{-1}AP}(X) = \det(X\mathrm{I}_n - P^{-1}AP) = \det(P^{-1}(X\mathrm{I}_n - A)P = \det P^{-1} \chi_A(X) \det P = \chi_A(X).$$

□

On peut donc poser la définition suivante.

Définition 4.4 Soit $u \in \mathcal{L}(E)$. Le *polynôme caractéristique* de u est défini comme

$$\chi_u(X) := \chi_A(X)$$

où A désigne la matrice de u dans une base quelconque $\mathcal{B}$ de E.

Par ailleurs, on obtient que le polynôme caractéristique est un invariant de similitude.

4.3 Matrice compagnon

On peut se demander si tout polynôme unitaire de degré n est le polynôme caractéristique est le polynôme d'une matrice. C'est clairement vrai si le polynôme est scindé, car alors une matrice diagonale (ou même triangulaire) dont les coefficients diagonaux sont les racines (avec multiplicité) de P a son polynôme caractéristique égal à P.

Il existe néanmoins une autre construction d'une telle matrice, bien utile.

Définition 4.5 Soit $P = a_0 + a_1X + \dots a_{n-1}X^{n-1} + X^n \in k[X]$. On pose

$$M(P) := \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}.$$

C'est la *matrice compagnon* du polynôme P.

Proposition 4.6
On a $\chi_{M(P)} = P$.

Démonstration : Ceci se démontre par récurrence sur n, en développant par rapport à la première ligne.

□

Chapitre X

Réduction des endomorphismes

1 Valeurs propres-vecteurs propres

1.1 Racines du polynôme caractéristique

On a vu que χ_f était un invariant de similitude. C'est donc que l'ensemble de ses racines sont aussi un invariant de similitude.

Or on a les équivalences suivantes

$$\begin{aligned}\chi_f(\lambda) = 0 &\Leftrightarrow \det(\lambda \mathrm{Id}_E - f) = 0 \\ &\Leftrightarrow \lambda \mathrm{Id}_E - f \text{ non inversible} \\ &\Leftrightarrow \mathrm{Ker}(\lambda \mathrm{Id}_E - f) \neq 0 \\ &\Leftrightarrow \exists v \neq 0_E \text{ t.q. } f(v) = \lambda v\end{aligned}$$

Ceci nous pousse à établir les définitions suivantes

Définition 1.1 Un tel λ est appelé un valeur propre de f. Un tel vecteur v est appelé un vecteur propre associé à la v.p. λ. Et on note $V_\lambda = \mathrm{Ker}(\lambda \mathrm{Id}_E - f)$, c'est le sous-espace propre associé à la v.p. λ.

Enfin on note $\mathrm{Spec}_k(f)$ l'ensemble des valeurs propres de χ_f.

Une conséquence immédiate du fait que les valeurs propres sont les racines du polynôme caractéristique est que f a au plus n valeur propres distinctes.

Avant d'étudier plus en détail les sou-espaces propres de f, faisons quelques rappels.

Définition 1.2 Des sous-espaces vectoriels $F_1, \ldots, F_m$ sont en *somme directe* si pour tout $v \in F_1 + \ldots + F_m$ l'écriture

$$v = \sum_{i=1}^{m} f_i, f_i \in F_i$$

est unique. De manière équivalente, on a

$$\sum_{i=1}^{m} f_i = 0, f_i \in F_i \Rightarrow f_i = 0 \forall i.$$

On note alors $F_1 \oplus \cdots \oplus F_m$ pour la somme des F_i.

On a la propriété suivante facile à vérifier

Proposition 1.3
Soit $\mathcal{B}^i$ une base de F_i pour $i = 1 \dots m$, alors les F_i sont en somme directe si et seulement si $\bigcup \mathcal{B}^i$ forme une base de F. En conséquence, si les espaces sont en somme directe on a

$$\dim \bigoplus F_i = \sum_i \dim F_i.$$

Proposition 1.4
Si $\mathrm{Spec}(f) = \{\lambda_1, \dots, \lambda_m\}$ alors on a

$$V_{\lambda_1} + V_{\lambda_2} + \cdots + V_{\lambda_m} = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_m}.$$

On va tout d'abord montrer

Lemme 1.5
Une famille de vecteurs propres associés à des valeurs propres distinctes est libre.

Démonstration : Soient $\lambda_1, \dots, \lambda_m$ des valeurs propres distinctes. Ceci se démontre par récurrence sur m. Pour $m = 1$ l'assertion est évidente car un vecteur propre est non nul par définition. Soient maintenant $v_1, \dots, v_m$ des

vecteurs propres associés à $\lambda_1, \ldots, \lambda_m$ respectivement. Et supposons que l'on ait des scalaires α_i tels que

$$\sum_{i=1}^{m} \alpha_i v_i = 0$$

. En appliquant f on obtient

$$0 = f(\sum_{i=1}^{m} \alpha_i v_i) = \sum_{i=1}^{m} \alpha_i \lambda_i v_i.$$

On peut donc écrire

$$0 = \lambda_m \sum_{i=1}^{m} \alpha_i v_i - \sum_{i=1}^{m} \alpha_i \lambda_i v_i = \sum_{i=}^{m-1} (\lambda_m - \lambda_i) \alpha_i v_i.$$

Par hypothèse de récurrence on obtient alors que pour tout i $(\lambda_m - \lambda_i)\alpha_i = 0$. Comme les valeurs propres sont deux à deux distinctes, on obtient bien $\alpha_i = 0$. □

Démonstration : (de la proposition) Soit pour tout i $v_i \in V_{\lambda_i}$ tels que $\sum_{i=1}^{m} v_i = 0$. Alors si certains v_i ne sont pas nuls, ils forment une famille libre ce qui est impossible. On a donc nécessairement pour tout i, $v_i = 0$, et donc les sous-espaces propres sont en somme directe.

□

1.2 Dimension des sous-espaces propres

Proposition 1.6
Les dimensions des sous-espaces propres sont des invariants de similitudes.

Démonstration : Si $g = ufu^{-1}$, et si x est un vecteur propre pour f, alors $u(x)$ est un vecteur propre de g. Donc u induit un isomorphisme de $V_\lambda(f)$ dans $V_\lambda(g)$. □

On va par ailleurs voir le lien entre dimension des sous-espaces propres et polynôme caractéristique.

Définition 1.7 Soit F un sous-espace de E. On dit que F est *stable* par f si $f(F) \subset F$. On peut alors définir $f_{|_F}$ l'*endomorphisme restreint* à F, qui est un endomorphisme de F.

Exemple 1.8 $\mathrm{Ker} f$, $\mathrm{Im}\, f$, et V_λ sont stables par f.

Proposition 1.9
Si $p = \dim V_\lambda$, alors $(X-\lambda)^p$ divise χ_f.

On utilise le lemme suivant :

Lemme 1.10
Si F est stable par f, alors $\chi_{f_{|_F}}$ divise χ_f.

Démonstration : Soit F un sous-espace stable par f. Choisissons alors une base $\mathcal{B}'$ de F que l'on compète en une base $\mathcal{B}$ de E. Dans la base $\mathcal{B}$, la matrice de f est alors triangulaire par bloc, avec le bloc en haut à gauche égal à la matrice de $f_{|_F}$ dans la base $\mathcal{B}'$. On conclut alors par la Proposition 3.5. □

Démonstration : (de la proposition) Le sous-espace propre V_λ est stable par f, et f restreint à V_λ est l'homothétie de rapport λ. Donc son polynôme caractéristique est $(X-\lambda)^p$. □

2 Polynômes d'endomorphismes

2.1 Morphisme d'évaluation

Définition 2.1 Soit $f \in \mathrm{End}(E)$ et $P = a_0 + a_1 X + \ldots + a_m X^m \in k[X]$. On définit $P(f) = a_0 \mathrm{Id}_E + a_1 f + \ldots + a_m f^m$, c'est le polynôme P évalué en f.

Proposition 2.2
L'application $\mathrm{ev_f} : k[X] \to \mathrm{End}(E)$ qui à P associe $P(f)$ est un morphisme d'algèbres (c'est-à-dire un morphisme d'anneaux et une application linéaire).

Démonstration : Le fait que ce soit une application linéaire est clair. Si $P_1 = X^m$ et $P_2 = X^p$, alors $(P_1P_2)(f) = f^{m+p} = f^m \circ f^p = P_1(f) \circ P_2(f)$.

Si P_1 et P_2 sont quelconques, on conclut par distributivité et linéarité. □

De même, on peut définir $\mathrm{ev}_A : k[X] \to \mathcal{M}_n(k)$, où $A \in \mathcal{M}_n(k)$.

Proposition 2.3
Si $A = \mathrm{Mat}(f, \mathcal{B})$, alors $P(A) = \mathrm{Mat}_n(P(f), \mathcal{B})$.

Démonstration : En effet si on note $\Phi_{\mathcal{B}} : (E) \to \mathcal{M}_n(k)$ l'application envoyant f sur $\mathrm{Mat}(f, \mathcal{B})$, $\Phi_{\mathcal{B}}$ est un isomorphisme d'algèbres. Donc si $A = \Phi_{\mathcal{B}}(f)$ et si $P(X) = a_0 + \ldots + a_nX^n$ on aura

$$\begin{aligned} a_0\mathrm{I}_n + a_1A + \ldots + a_nA^n &= a_0\Phi_{\mathcal{B}}(\mathrm{Id}_E) + a_1\Phi_{\mathcal{B}}(f) + \ldots + a_n\Phi_{\mathcal{B}}(f)^n \\ &= a_0\Phi_{\mathcal{B}}(\mathrm{Id}_E) + a_1\Phi_{\mathcal{B}}(f) + \ldots + a_n\Phi_{\mathcal{B}}(f^n) \\ &= \Phi_{\mathcal{B}}(a_0\mathrm{Id}_E + a_1f + \ldots + a_nf^n) \\ &= P(f) \end{aligned}$$

□

Proposition 2.4
Si $g = ufu^{-1}$, et si $P \in k[X]$, alors $P(g) = uP(f)u^{-1}$.

Démonstration : Cela provient du fait que $g^n = (ufu^{-1})^n = uf^nu^{-1}$, donc c'est vrai pour les monômes X^n. □

Proposition 2.5
Si $f(x) = \lambda x$ alors $P(f)(x) = P(\lambda)x$.

Démonstration : On montre tout d'abord que pour tout p, $f^p(x) = \lambda^p x$ par récurrence. Puis on conclut par linéarité. □

2.2 Polynôme minimal

Comme le morphisme d'évaluation est un morphisme d'anneaux, son noyau est un idéal de $k[X]$. Comme $k[X]$ est principal, cet idéal est de la forme (μ_f) où μ_f est un certain polynôme que l'on peut supposer unitaire. Le noyau de ev_f est l'ensemble des polynômes qui s'annulent en f. C'est donc l'unique polynôme qui vérifie :

1. μ_f unitaire ;
2. $\mu_f(f) = 0$;
3. pour tout $P \in k[X]$ tel que $P(f) = 0$, alors μ_f divise P.

Les polynômes de l'idéal (μ_f) sont appelés *polynômes annulateurs de f*, et le polynôme μ_f est appelé *polynôme minimal de f.*

Proposition 2.6
Le polynôme minimal est un invariant de similitude.

Démonstration : C'est une conséquence immédiate de Proposition 2.4. □

Définition 2.7 Soit f un endomorphisme et v un vecteur. Alors on peut montrer que l'ensemble des polynômes P tels que $P(f)(v) = 0_E$ est un idéal de $k[X]$. Il s'écrit donc $(\mu_{f,v})$, où $\mu_{f,v}$ est appelé le *polynôme minimal de f en v*.

Proposition 2.8
Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E. Alors μ_f est le ppcm des μ_{f,e_i} où $i = 1, \ldots, n$.

Démonstration : Il est clair que μ_{f,e_i} divise μ_f pour tout i, donc leur ppcm divise μ_f. Supposons maintenant que P soit divisible par tous les μ_{f,e_i}. Soit $v = \sum \lambda_i e_i$ un vecteur, alors $P(f)(v) = \sum_i \lambda_i P(f)(e_i) = 0$. Donc μ_f divise P. □

2.3 Théorème de Cayley-Hamilton

Théorème 2.9
$\chi_f(f) = 0$

Démonstration : On va montrer que pour tout $x \in E$, on a $\chi_f(f)(x) = 0_E$. C'est clair pour $x = 0_E$.

Soit donc $x \neq 0_E$. Alors il existe p tel que la famille $(x, f(x), \ldots, f^p(x))$ est libre et la famille $(x, f(x), \ldots, f^{p+1}(x))$, et on a donc $f^{p+1}(x) = \sum_{i=0}^{p} a_i f^i(x)$. Notons $F = \text{vect}(x, f(x), \ldots, f^p(x))$. Alors F est stable par f et la matrice $f_{|_F}$ dans la base $(x, f(x), \ldots, f^p(x))$ est

$$\begin{pmatrix} 0 & 0 & \ldots & a_0 \\ 1 & \ddots & & a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & a_p \end{pmatrix}$$

C'est la matrice compagnon du polynôme $P = X^{p+1} - a_p X^p \cdots - a_0$. On a donc $\chi_{f_{|_F}}(f)(x) = f^{p+1}(x) - a_p f^p(x) \cdots - a_0 x = 0$. Comme $\chi_{f_{|_F}}$ divise χ_f, on a en déduit $\chi_f(f)(x) = 0_E$.

□

Corollaire 2.10
Le polynôme minimal divise le polynôme caractéristique. En particulier le degré du polynôme minimal est toujours $\leqslant n$.

Corollaire 2.11
Les racines de μ_f sont exactement les valeurs propres de f.

Démonstration : μ_f divise χ_f, donc toute racine de μ_f est une racine de χ_f donc une valeur propre.

Réciproquement, soit λ une valeur propre et x un vecteur propre associé. Alors $0_E = \mu_f(f)(x) = \mu_f(\lambda)x$, donc $\mu_f(\lambda) = 0$. □

Corollaire 2.12
f est nilpotent si et seulement si $\chi_f = X^n$ si et seulement si $\mathrm{Spec}_{\mathbb{C}}(f) = \{0\}$.

On a finalement montré que si f est un endomorphisme , alors on peut lui associer $\{(\lambda_1, p_1, q_1, m_1), \ldots, (\lambda_s, p_s, q_s, m_s)\}$ où les$\lambda_i \in k$ sont les valeurs propres, p_i est la multiplicité de λ_i dans μ_f, $q_i = dim V_{\lambda_i}$ et m_i est la multiplicité de λ_i dans χ_f. Alors ces nombres sont des invariants de similitude.

NB : on a toujours $p_i, q_i \leqslant m_i$. Mais on peut avoir $p_i \leqslant q_i$ ou l'inverse.

3 Réduction aux sous-espaces caractéristiques

3.1 Lemme de décomposition des noyaux

Proposition 3.1
Soit $P \in k[X]$ et $f \in \mathrm{End}(E)$. Alors $\mathrm{Ker}P(f)$ est un sous-espace stable par f.

Démonstration : Cela vient du fait que $P(u) \circ u = u \circ P(u)$. □

Théorème 3.2
Soient P et Q des polynômes premiers entre eux. Alors $\mathrm{Ker}(PQ(f)) = \mathrm{Ker}(P(f)) \oplus \mathrm{Ker}(Q(f))$.

Démonstration : Montrons d'abord que les espaces sont en somme directe. Par Bezout on a $PU + QV = 1$, ce qui implique donc $U(f) \circ P(f) + V(f) \circ Q(f) = \mathrm{Id}_E$. Soit x dans l'intersection des noyaux. Alors $x = U(f) \circ P(f)(x) + V(f) \circ Q(f)(x) = 0_E$.

Soit $x \in \mathrm{Ker}PQ(f)$, et notons $x_1 = UP(f)(x)$ et $x_2 = VQ(f)(x)$. On a alors $x = x_1 + x_2$. Or $Q(f)(x_1) = UPQ(f)(x) = 0$, et de même $P(f)(x_2) = 0$. On a donc une inclusion.

Enfin $\mathrm{Ker}P(f) \subset \mathrm{Ker}PQ(f)$, et de même pour Q, donc la somme est aussi incluse.

□

Corollaire 3.3
Si $P_1, \ldots, P_s$ sont premiers entre eux deux à deux, on a $\mathrm{Ker}P(f) = \bigoplus_{i=1}^{s} \mathrm{Ker}P_i(f)$.

3.2 Sous-espaces caractéristiques

Définition 3.4 Soit f un endomorphisme de E, $\lambda \in \mathrm{Spec}(f)$, et m la multiplicité de λ dans χ_f. On définit $E_\lambda = \ker((\lambda \mathrm{Id}_E - f)^m)$, c'est le *sous-espace caractéristique* associé à la valeur propre λ.

Proposition 3.5

1. Le sous-espace propre V_λ est un sous-espace vectoriel du sous-espace caractéristique E_λ.
2. E_λ est un sous-espace stable par f.
3. Si p est la multiplicité de λ dans μ_f, alors on a $E_\lambda = \ker((\lambda \mathrm{Id}_E - f)^p)$.

Démonstration :

1. Clair.
2. Soit $x \in E_\lambda$. Alors $(\lambda \mathrm{Id}_E - f)^m(f(x)) = f \circ (\lambda \mathrm{Id}_E - f)^m(x) = 0_E$, donc E_λ est stable par f.
3. Le polynôme minimal de f restreint à E_λ divise μ_f, et il divise $(X-\lambda)^m$ qui annule $f_{|E_\lambda}$. Il divise donc leur pgcd qui est $(X-\lambda)^p$, et donc $(X-\lambda)^p$ est un polynôme annulateur de $f_{|E_\lambda}$.

□

Théorème 3.6
Soit f tel que χ_f est scindé sur k, et notons $\chi_f = \prod_{i=1}^r (X-\lambda_i)^{m_i}$, et notons f_i l'endomorphisme f restreint à E_{λ_i}. Alors on a

1. $E = E_{\lambda_1} \oplus \cdots \oplus E_{\lambda_r}$;
2. $\dim_k E_{\lambda_i} = m_i$
3. $\mu_{f_i} = (X-\lambda)^{p_i}$ et $\chi_{f_i} = (X-\lambda)^{m_i}$.

Démonstration :

1. La décomposition en somme directe vient du lemme des noyaux. Le fait que la somme soit E vient de Cayley-Hamilton.

2. On a que χ_{f_i} divise χ_f. Et par ailleurs pour tout x dans E_i, on a $(f-\lambda-i\mathrm{Id}_{E_i})^{m_i}(x)=0_E$, ce qui veut dire que $(X-\lambda_i)^{p_i}$ annule f_i. Le polynôme caractéristique de f_i a donc une unique racine qui est λ_i, il est don de la forme $(X-\lambda_i)^{t_i}$. Comme il divise χ_f, on a $t_i \leqslant m_i$, où t_i est donc la dimension de E_i. Finalement comme par le 1. on a $\sum_i t_i = n$, comme $\sum_i m_i = n$ on obtient $m_i = t_i$ pour tout i.
3. On a déjà vu $chi_{f_i} = (X-\lambda_i)^{m_i}$. Le polynôme minimal lui divise μ_f, et χ_{f_i}, il divise donc leur pgcd $(X-\lambda_i)^{p_i}$. Il est donc de la forme $(X-\lambda_i)^{s_i}$ avec $s_i \leqslant p_i$. Comme les μ_{f_i} sont premiers entre eux, le lemme des noyaux et 1. nous dit que

$$E = \bigoplus_i E_i = \bigoplus_i \mathrm{Ker}\mu_{f_i} = \mathrm{Ker}(\prod_i \mu_{f_i}).$$

Autrement dit $\prod_i \mu_{f_i}$ annule f, et donc μ_f divise $\prod_i (X-\lambda_i)^{s_i}$. D'où $s_i \geqslant p_i$.

□

Ceci implique que pour une base adaptée à la décomposition en sous-espaces caractéristiques, la matrice de f est diagonale par blocs.

3.3 Diagonalisation

Définition 3.7 Un endomorphisme est dit *diagonalisable* si il existe une base $\mathcal{B}$ telle que $\mathrm{Mat}(f,\mathcal{B})$ est diagonale, ou autrement dit s'il existe une base de vecteurs propres de f.

On a donc les équivalences

Théorème 3.8
Soit f avec $\mathrm{Spec}(f) = \{\lambda_1, \ldots, \lambda_r\}$. Les assertions suivantes sont équivalentes :

1. f est diagonalisable ;
2. il existe une base de E formée de vecteurs propres de f ;
3. $E = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r}$;
4. χ_f est scindé sur k et pour tout i on a $E_{\lambda_i} = V_{\lambda_i}$;
5. χ_f est scindé et pour tout i on a $q_i = m_i$ (c'est-à-dire $\dim_k E_{\lambda_i} = \dim_k V_{\lambda_i}$) ;
6. μ_f est scindé et pour tout i, $p_i = 1$ (autrement dit μ_f est scindé à racines simples.)

Démonstration : $1 \Leftrightarrow 2 \Leftrightarrow 3$ est clair, car on sait que les sous-espaces propres sont en somme directe.

$4 \Rightarrow 3$ vient du théorème précédent.

$3 \Rightarrow 4$ vient de fait que dans la base correspondante à la décomposition, la matrice de f est diagonale, sont polynôme caractéristique est donc scindé. Puis on utilise $V_i \subset E_i$.

$4 \Leftrightarrow 5$ vient du fait que $V_i \subset E_i$.

$3 \Leftrightarrow 6$ Notons $P = \prod_{i=1}^{r}(X - \Lambda_i)$. On a alors P divise μ_f car toutes les valeurs propres sont racines de μ_f. On a les équivalences

$$\begin{aligned} E = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r} &\Leftrightarrow \bigoplus_{i=1}^{r} \mathrm{Ker}(\lambda_i \mathrm{Id}_E - f) = E \\ &\Leftrightarrow \mathrm{Ker} P(f) = E \text{ par le lemme des noyaux} \\ &\Leftrightarrow P(f) = 0 \\ &\Leftrightarrow \mu_f \text{ divise } P \\ &\Leftrightarrow P = \mu_f \end{aligned}$$

□

3.4 Diagonalisation simultanée

Théorème 3.9
Soient f et g deux endomorphismes diagonalisables tels que $f \circ g = g \circ f$. Alors il existe une base $\mathcal{B}$ telle que les matrices de f et g dans $\mathcal{B}$ soient diagonales.

Démonstration : Soit $V = V_{\lambda_i}(f)$ un sous-espace propre de f, alors V est stable par g. En effet si $v \in V$, on a $f(g(v)) = g(f(v)) = g(\lambda_i v) = \lambda_i g(v)$, donc $g(v) \in V$. De plus $g_i := g_{|_V}$ est digonalisable (son polynôme minimal est scindé à racines simples). Soit $\mathcal{B}^i$ une base de diagonalisation de g_i. Alors $\mathcal{B} = (\mathcal{B}^1, \ldots, \mathcal{B}^s)$ est une base de diagonalisation de g, elle l'est aussi de f car elle respecte la décomposition en sous-espaces propres.

□

4 Reduction de Jordan

4.1 Trigonalisation

Définition 4.1 Un endomorphisme est *trigonalisable* s'il existe une base $\mathcal{B}$ de E dans laquelle la matrice de f est triangulaire supérieure.

Théorème 4.2
f est trigonalisable si et seulement si χ_f est scindé sur k.

Corollaire 4.3
Toute matrice est trigonalisable sur $\mathbb{C}$.

Démonstration : Le sens direct est immédiat.

On prouve par récurrence su $n = \dim E$. Pour $n = 1$ c'est clair. Soit f et λ une valeur propre de f (qui existe car χ_f est scindé) et v un vecteur propre. Complétons v en une base $(v, v_2, \ldots, v_n)$, alors la matrice de f dans cette base est triangulaire par bloc (un bloc de taille 1 et un de taille $n-1$).

$$\begin{pmatrix} \lambda & * \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$$

Par hypothèse de récurrence, il existe Q tel que $Q^{-1}BQ$ est diagonale. En posant

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ \vdots & Q & \\ 0 & & \end{pmatrix},$$

on vérifie facilement que $R^{-1}AR$ est triangulaire supérieure. □

Corollaire 4.4
Si $\chi_f = \prod (X - \lambda_i)^{m_i}$ est scindé sur k, il existe une base dans laquelle la matrice de f est de la forme

$$\begin{pmatrix} T_1 & 0 & & 0 \\ 0 & T_2 & & \\ & & \ddots & \\ 0 & & & T_s \end{pmatrix}$$

où chaque T_i est une matrice triangulaire supérieure de taille $m_i \times m_i$.

4.2 Exemple

Exemple de calcul du polynôme minimal et des sous-espaces caractéristiques, et d'une forme diagonale par bloc, où chaque bloc est triangulaire.

Etape 1 : Calculer le polynôme caractéristique, et le factoriser dans $\mathbb{C}$. Cela permet de déduire les valeur propres.

Etape 2 : Pour chaque valeur propre λ_i, on a des inclusions de sous-espaces :

$$V_{\lambda_i} = \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E) = E_i^1 \subset \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)^2 = E_i^2 \subset \cdots \subset \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)^{m_i} = E_i^{m_i} = E_{\lambda_i}.$$

On sait que la dimension de E_i^1 est $q_i \leqslant 1$, et que celle de $E_i^{m_i}$ est exactement m_i. Il existe donc un p_i tel que $E_i^{p_i} = m_i$. Ce p_i est la multiplicité de λ_i dans μ_f. Il faut donc calculer ces noyaux successifs pour chaque valeur propre.

4.3 Décomposition de Dunford

Théorème 4.5 (Décomposition de Jordan-Dunford)
Soit f tel que χ_f est scindé sur k. Alors il existe des uniques endomorphismes d et n de E tels que

1. $f = d + w$;
2. d est diagonalisable ;
3. w es nilpotent ;
4. $w \circ d = d \circ w$.

Démonstration : Soient $\lambda_1, \ldots, \lambda_s$ les valeurs propres de f et $E_1, \ldots, E_s$ les sous-espaces caractéristiques. On définit d comme l'unique endomorphisme tel que les E_i soient stables, et $d_{|_{E_i}} = \lambda_i \mathrm{Id}_{E_i}$. Il est alors clair que d est diagonalisable, en effet toute base respectant la décomposition en sous-espace caractéristique est une base de diagonalisation.

De plus pour tout x de E_i, on a $f \circ d(x) = f(\lambda_i x) = \lambda_i f(x)$. Par ailleurs $d \circ f(x) = \lambda_i f(x)$ car E_i est stable par f. Donc $d \circ f = f \circ d$ sur E_i et donc sur E. Finalement en posant $w = f - d$, on a bien que d et w commutent.

Montrons maintenant que w est nilpotent. Soit $x \in E_i$. Alors $w^{m_i}(x) = (f-d)^{m_i}(x) = (f - \lambda_i \mathrm{Id}_{E_i})^{m_i}(x) = 0_E$. En prenant le ppcm de tous les m_i on a bien que w est nilpotent.

Enfin montrons l'unicité. Supposons que $d + w = d' + w'$. On montre d'abord que les E_i sont stables par d' et w'. Si $x \in E_i$, comme d' commute à w', il commute à f et donc il commute à $(\lambda_i \mathrm{Id}_E - f)^{m_i}$. On a donc $(\lambda_i \mathrm{Id}_E - f)^{m_i} \circ d'(x) = d' \circ (\lambda_i \mathrm{Id}_E - f)^{m_i}(x) = 0_E$ donc $d'(x) \in E_i$ qui donc stable par d'.

De plus d et d' commutent sur E_i car d est une homothétie. Ils sont alors diagonalisables dans une même base. Dans cette base la matrice $d - d'$ sera diagonale. Or on a $d - d' = w' - w$, il reste à montrer que la somme de deux endomorphismes nilpotents qui commutent est encore nilpotent. Cela vient de la formule du binôme de Newton. Si on prend une puissance assez grande, tous les termes s'annulent.

□

Proposition 4.6
Dans la décomposition de Dunford, les endomorphismes d et w sont des polynômes en f.

Démonstration : Notons $P_i = (X - \lambda_i)^{p_i}$ et $Q_i = \prod_{j \neq i} P_i$.

Les polynômes P_i et Q_i sont premiers entre eux, on a donc un couple de Bezout et donc :

$$P_i U_i(f) + Q_i V_i(f) = \mathrm{Id}_E$$

On va vérifier que $g_i := Q_i V_i(f)$ est la projection sur E_i parallélement à $\bigoplus_{j \neq i} E_j$.

Si $x \in E_i$, alors $P_i U_i(f)(x) = 0$ donc on obtient $x = Q_i V_i(f)(x) = g_i(x)$. Si $x \in E_j$ avec $j \neq i$, alors $Q_i V_i(f) = 0$ c'est à dire $g_i(x) = 0$. Donc g_i est bien la projection sur E_i parallèlement à $\bigoplus_{j \neq i} E_j$.

On a donc $d = \sum_i \lambda_i g_i = (\sum_i \lambda_i Q_i V_i)(f)$ est un polynôme en f, et $w = f - d = f - \sum_i \lambda_i Q_i V_i(f) = (X - \sum_i \lambda_i Q_i V_i)(f)$ aussi.

□