

Cours d'algèbre pour la licence et le Capes

Jean-Étienne ROMBALDI

26 avril 2018

Table des matières

| | |
|--------------------------------------------------------------------------------|-----------|
| Avant-propos | ix |
| Notation | xi |
| I Notions de base | 1 |
| 1 Éléments de logique et de théorie des ensembles | 3 |
| 1.1 Quelques notions de logique | 3 |
| 1.2 Les connecteurs logiques de base | 4 |
| 1.3 Quelques méthodes de raisonnement | 8 |
| 1.4 Notions de base sur les ensembles. Quantificateurs | 10 |
| 1.5 Les symboles \sum et \prod | 12 |
| 1.6 Les théorèmes de récurrence | 14 |
| 1.7 L'algèbre des parties d'un ensemble | 24 |
| 1.8 Applications. Notions d'injectivité, surjectivité et bijectivité | 29 |
| 2 Analyse combinatoire | 39 |
| 2.1 Cardinal d'un ensemble fini | 39 |
| 2.2 Ensembles infinis dénombrables | 43 |
| 2.3 Arrangements et permutations | 44 |
| 2.4 Combinaisons | 44 |
| 2.5 Problèmes de tirage | 44 |
| 2.6 Nombres de surjections entre ensembles finis | 44 |
| 2.7 Le problème des rencontres | 44 |
| 3 Relations d'ordre et d'équivalence | 45 |
| 4 L'ensemble \mathbb{N} des entiers naturels | 47 |
| 5 L'ensemble \mathbb{Z} des entiers relatifs | 49 |
| 6 L'ensemble \mathbb{Q} des nombres rationnels | 51 |
| 7 Le corps \mathbb{C} des nombres complexes | 53 |
| 7.1 Conditions nécessaires à la construction de \mathbb{C} | 53 |
| 7.2 Construction de \mathbb{C} | 54 |
| 7.3 Conjugué et module d'un nombre complexe | 59 |
| 7.4 Les équations de degré 2 | 65 |
| 7.5 Les équations de degré 3 et 4 | 69 |

| | | |
|-----|---------------------------------------------------|----|
| 7.6 | Arguments d'un nombre complexe | 71 |
| 7.7 | Racines n -ièmes d'un nombre complexe | 85 |

II Algèbre linéaire et bilinéaire sur \mathbb{R} ou \mathbb{C} 89

| | | |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 8 | Espaces vectoriels réels ou complexes | 91 |
| 8.1 | L'espace vectoriel \mathbb{K}^n | 91 |
| 8.2 | Définition d'un espace vectoriel réel ou complexe | 92 |
| 8.3 | Sous-espaces vectoriels | 94 |
| 8.4 | Applications linéaires | 99 |
| 8.5 | La base canonique de \mathbb{K}^n et expression matricielle des applications linéaires de \mathbb{K}^n dans \mathbb{K}^m | 103 |
| 8.6 | Matrices réelles ou complexes | 105 |
| 8.6.1 | Opérations sur les matrices | 105 |
| 8.6.2 | Matrices inversibles | 109 |
| 8.6.3 | Déterminant d'une matrice d'ordre 2 | 115 |
| 8.6.4 | Transposée d'une matrice | 116 |
| 8.6.5 | Trace d'une matrice carrée | 117 |
| 8.7 | Systèmes d'équations linéaires | 118 |
| 8.8 | Sommes et sommes directes de sous-espaces vectoriels | 119 |
| 9 | Espaces vectoriels réels ou complexes de dimension finie | 123 |
| 9.1 | Systèmes libres, systèmes générateurs et bases | 123 |
| 9.2 | Espaces vectoriels de dimension finie | 127 |
| 9.3 | Rang d'un système de vecteurs ou d'une application linéaire | 134 |
| 9.4 | Expression matricielle des applications linéaires | 137 |
| 9.5 | Formules de changement de base | 140 |
| 10 | Opérations élémentaires et déterminants | 145 |
| 10.1 | Opérations élémentaires. Matrices de dilatation et de transvection | 146 |
| 10.2 | Déterminants des matrices carrées | 151 |
| 10.3 | Déterminant d'une famille de vecteurs | 163 |
| 10.4 | Déterminant d'un endomorphisme | 164 |
| 11 | Formes bilinéaires et quadratiques réelles ou complexes | 165 |
| 11.1 | Formes linéaires | 165 |
| 11.2 | Formes bilinéaires | 169 |
| 11.3 | Expression matricielle des formes bilinéaires (en dimension finie) | 170 |
| 11.4 | Formes quadratiques | 177 |
| 11.5 | Théorème de réduction de Gauss | 182 |
| 11.5.1 | Cas des espaces de dimension 2 | 182 |
| 11.5.2 | Cas des espaces de dimension $n \geq 1$ | 184 |
| 11.6 | Orthogonalité, noyau et rang | 197 |
| 11.7 | Signature d'une forme quadratique réelle en dimension finie | 207 |
| 11.8 | Quadriques dans \mathbb{R}^n ou \mathbb{C}^n | 211 |
| 11.9 | Quadriques dans \mathbb{R}^n | 214 |

| | | |
|------------|--------------------------------------------------------------------------------|------------|
| 12 | Espaces préhilbertiens | 217 |
| 12.1 | Produit scalaire | 217 |
| 12.2 | Inégalités de Cauchy-Schwarz et de Minkowski | 221 |
| 12.3 | Orthogonalité | 229 |
| 12.4 | Le procédé d'orthogonalisation de Gram-Schmidt | 231 |
| 12.5 | Projection orthogonale sur un sous-espace de dimension finie | 238 |
| 12.6 | Caractérisation des projecteurs orthogonaux dans un espace euclidien | 247 |
| 12.7 | Réduction des matrices symétriques réelles | 248 |
| 13 | Géométrie dans les espaces préhilbertiens | 249 |
| 13.1 | Mesures de l'angle non orienté de deux vecteurs non nuls | 249 |
| 13.2 | Sphères dans un espace préhilbertien | 250 |
| 13.3 | Sphères dans un espace euclidien | 252 |
| 13.4 | Hyperplans dans un espace euclidien | 255 |
| 13.5 | Hyperplan médiateur dans un espace préhilbertien | 259 |
| 13.6 | Intersection d'un hyperplan et d'une sphère dans un espace euclidien | 260 |
| 13.7 | Intersection de deux sphères dans un espace euclidien | 261 |
| 13.8 | Inversion | 264 |
| 13.9 | Symétries orthogonales dans les espaces euclidiens | 265 |
| 13.10 | Isométries | 267 |
| 13.11 | Orientation d'un espace euclidien | 274 |
| 13.12 | Produit vectoriel dans un espace euclidien | 275 |
| 13.13 | Isométries en dimension 2 | 279 |
| 13.13.1 | Isométries directes ou rotations. Angles orientés de vecteurs | 279 |
| 13.13.2 | Isométries indirectes ou réflexions | 282 |
| 13.14 | Isométries en dimension 3 | 283 |
| 13.14.1 | Isométries directes | 284 |
| 14 | Espaces préhilbertiens complexes | 289 |
| 14.1 | Produits scalaires | 289 |
| 14.2 | Inégalités de Cauchy-Schwarz et de Minkowski | 294 |
| III | Géométrie affine | 297 |
| 15 | Espaces affines | 299 |
| 15.1 | Définition d'un espace affine | 299 |
| 15.2 | Sous-espaces affines | 299 |
| 15.3 | Barycentres | 299 |
| 15.4 | Équations cartésiennes d'une droite du plan | 299 |
| 15.5 | Le triangle dans le plan affine euclidien | 301 |
| 15.5.1 | Médianes d'un triangle, centre de gravité | 301 |
| 15.5.2 | Médiatrices d'un triangle | 302 |
| 15.5.3 | Hauteurs d'un triangle | 304 |
| 16 | Espaces affines euclidiens | 307 |
| 17 | Applications affines | 309 |

| | |
|----------------------------------------------------------------------------------------------------------|------------|
| 18 Coniques | 311 |
| 18.1 Définition par directrice, foyer et excentricité | 312 |
| 18.2 Équation réduite d'une conique | 314 |
| 18.2.1 Les paraboles | 317 |
| 18.2.2 Les coniques à centres, ellipses et hyperboles | 323 |
| 18.2.3 Construction des tangentes à une conique | 332 |
| 18.3 Définition bifocale des coniques à centre | 334 |
| 18.4 Lieu orthoptique d'une conique | 338 |
| 18.4.1 Lieu orthoptique d'une ellipse | 338 |
| 18.4.2 Lieu orthoptique d'une hyperbole | 341 |
| 18.4.3 Lieu orthoptique d'une parabole | 341 |
| 18.5 Cocyclicité de 4 points sur une conique | 342 |
| 18.5.1 Cocyclicité de 4 points sur une parabole | 342 |
| 18.5.2 Cocyclicité de 4 points sur une ellipse | 343 |
| 18.6 Équations des coniques dans un repère quelconque | 343 |
| 19 Nombres complexes et géométrie euclidienne | 345 |
| 19.1 Le plan affine euclidien | 345 |
| 19.2 Le plan d'Argand-Cauchy | 345 |
| 19.3 Équations complexes des droites et cercles du plan | 347 |
| 19.3.1 Droites dans le plan complexe | 347 |
| 19.3.2 Cercles dans le plan complexe | 348 |
| 19.4 Interprétation géométrique du module d'un nombre complexe | 349 |
| 19.4.1 Module et distance euclidienne | 349 |
| 19.4.2 L'égalité du parallélogramme | 350 |
| 19.4.3 L'inégalité de Cauchy-Schwarz | 351 |
| 19.5 Lignes de niveau associées aux module | 352 |
| 19.6 Interprétation géométrique de l'argument d'un nombre complexe | 356 |
| 19.7 Lignes de niveau associées à l'argument | 359 |
| 19.8 Le triangle dans le plan complexe | 365 |
| 19.8.1 Relations trigonométriques pour un triangle | 366 |
| 19.8.2 Aire d'un triangle | 368 |
| 19.8.3 Centre de gravité d'un triangle | 370 |
| 19.8.4 Cercle circonscrit à un triangle | 371 |
| 19.8.5 Orthocentre d'un triangle | 372 |
| 19.8.6 Triangle équilatéral | 375 |
| 19.9 Interprétation géométrique des applications $z \mapsto az + b$, $z \mapsto a\bar{z} + b$ | 377 |
| IV Structures algébriques et arithmétique | 379 |
| 20 Structure de groupe | 381 |
| 20.1 Loi de composition interne | 381 |
| 20.2 Groupes | 384 |
| 20.3 Sous-groupes | 390 |
| 20.4 Sous-groupe engendré par une partie d'un groupe | 396 |
| 20.5 Groupes monogènes | 397 |
| 20.6 Groupes finis. Théorème de Lagrange | 400 |
| 20.7 Morphismes de groupes | 402 |

| | | |
|-----------|----------------------------------------------------------------------------------------------------------|------------|
| 20.8 | Sous-groupes distingués, groupes quotients | 409 |
| 20.9 | Ordre d'un élément dans un groupe | 414 |
| 20.10 | Sous-groupes des groupes cycliques | 419 |
| 21 | Structure d'anneau | 421 |
| 21.1 | Anneaux | 421 |
| 21.2 | Éléments inversibles dans un anneau unitaire | 427 |
| 21.3 | Sous-anneaux | 429 |
| 21.4 | Morphismes d'anneaux | 432 |
| 22 | Structure de corps | 435 |
| 22.1 | Corps | 435 |
| 22.2 | Morphismes de corps | 439 |
| 23 | Division euclidienne dans \mathbb{Z} | 441 |
| 23.1 | L'anneau \mathbb{Z} des entiers relatifs | 441 |
| 23.2 | Divisibilité et congruences | 442 |
| 23.3 | Le théorème de division euclidienne dans \mathbb{Z} | 444 |
| 23.4 | Les systèmes de numération | 447 |
| 23.5 | Caractéristique d'un anneau ou d'un corps commutatif | 451 |
| 23.6 | Plus grand commun diviseur | 452 |
| 23.6.1 | Plus petit commun multiple | 455 |
| 23.7 | L'algorithme d'Euclide. | 459 |
| 23.8 | Equations diophantiennes $ax + by = c$ | 462 |
| 23.9 | Equations $ax \equiv b \pmod{n}$ | 463 |
| 23.10 | Le théorème Chinois | 465 |
| 23.11 | Nombres premiers entre eux. Les théorèmes de Bézout et de Gauss | 466 |
| 24 | Nombres premiers | 473 |
| 24.1 | L'ensemble \mathcal{P} des nombres premiers | 473 |
| 24.2 | L'ensemble \mathcal{P} des nombres premiers est infini | 477 |
| 24.3 | Décomposition en facteurs premiers | 480 |
| 24.4 | Valuation p -adique | 485 |
| 24.5 | Le postulat de Bertrand | 494 |
| 24.6 | Les théorèmes de Fermat et de Wilson | 497 |
| 24.7 | Les anneaux $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ et la fonction indicatrice d'Euler | 500 |
| 25 | Les anneaux $\mathbb{Z}/n\mathbb{Z}$ | 503 |
| 25.1 | Congruences dans \mathbb{Z} . Anneaux $\mathbb{Z}/n\mathbb{Z}$ | 503 |
| 25.2 | Groupes cycliques | 504 |
| 25.3 | Fonction indicatrice d'Euler | 506 |
| 26 | Utilisation des congruences et des anneaux $\mathbb{Z}/n\mathbb{Z}$ | 511 |
| 26.1 | Équations diophantiennes $ax \equiv b \pmod{n}$ | 511 |
| 26.2 | Équations diophantiennes $x \equiv a \pmod{n}, x \equiv b \pmod{m}$ | 512 |
| 26.3 | Critères de divisibilité | 513 |

| | |
|------------------------------------------------------------------------------------------------|------------|
| V Problèmes d'algèbre | 515 |
| 27 Le théorème de d'Alembert-Gauss | 519 |
| 27.1 Énoncé | 519 |
| 27.2 Solution | 519 |
| 28 La forme quadratique $Tr(M^2)$ sur $\mathcal{M}_n(\mathbb{R})$ | 521 |
| 28.1 Énoncé | 521 |
| 28.2 Solution | 521 |
| 29 Décomposition d'un entier en carrés. Entiers de Gauss | 525 |
| 29.1 Énoncé | 525 |
| 29.2 Solution | 530 |
| 30 Nombres de Fibonacci | 543 |
| 30.1 Énoncé | 543 |
| 30.2 Solution | 545 |
| 31 Infinitude de l'ensemble des nombres premiers | 551 |
| 31.1 Énoncé | 551 |
| 31.2 Solution | 556 |
| 32 Le théorème de Fermat pour $n = 2$ et $n = 4$ | 571 |
| 32.1 Énoncé | 571 |
| 32.2 Solution | 572 |
| 33 L'anneau $\mathbb{Z}/n\mathbb{Z}$ et les nombres de Carmichael | 575 |
| 33.1 Énoncé | 575 |
| 33.2 Solution | 579 |
| 34 Sous-groupes de $\mathcal{L}(E)$ | 591 |

Avant-propos

Ce livre est en construction.

Cet ouvrage destiné aux étudiants préparant le Capes externe de Mathématiques et aux enseignants préparant l'agrégation interne fait suite au livre « Éléments d'analyse réelle pour le Capes et l'Agrégation Interne de Mathématiques ».

Notations

| | |
|-----------------|-------------------------------------------------------------------------------------------------------------|
| \mathbb{N} | ensemble des entiers naturels. |
| \mathbb{Z} | l'anneau des entiers relatifs. |
| \mathbb{Q} | corps des nombres rationnels. |
| \mathbb{R} | corps des nombres réels. |
| \mathbb{C} | corps des nombres complexes. |
| $\Re(z)$ | partie réelle du nombre complexe z . |
| $\Im(z)$ | partie imaginaire du nombre complexe z . |
| $\mathbb{K}[X]$ | algèbre des polynômes à une indéterminée à coefficients dans $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} . |
| C_n^p | coefficient binomial. |

Première partie

Notions de base

Éléments de logique et de théorie des ensembles

Pour les exemples et exercices traités dans ce chapitre les ensembles usuels de nombres entiers, rationnels réels et complexes sont supposés connus, au moins de manière intuitive comme cela se passe au Lycée. Nous reviendrons plus loin sur les constructions de ces ensembles.

1.1 Quelques notions de logique

Nous allons préciser à un premier niveau quelques notions mathématiques qui sont relativement intuitives mais nécessitent quand même des définitions rigoureuses.

L'idée étant de préciser schématiquement comment se présente une théorie mathématique ainsi que la notion essentielle de démonstration.

La première notion est celle d'assertion. De manière intuitive, une assertion est un énoncé mathématique aussi rigoureux que possible qui ne peut prendre que deux valeurs de vérité à savoir « vrai » ou « faux » mais jamais entre les deux comme dans le langage courant.

Une assertion qui est toujours vraie est une tautologie.

Par exemple les énoncés suivantes sont des assertions : $2 < 15$ (elle est vraie), $\sqrt{2}$ est un nombre rationnel (elle est fausse), $\cos(n\pi) = (-1)^n$ (vraie), ...

Deux assertions sont dites logiquement équivalentes, ou plus simplement équivalentes, si elles sont toutes deux vraies ou toutes deux fausses.

Il y a ensuite les énoncés qui se démontrent. Pour ce faire, on se donne des règles précises (que nous verrons par la pratique) qui permettent de construire de nouvelles assertions à partir d'assertions données.

Remarque 1.1 *Il ne faut pas croire que dans une théorie donnée toute assertion P soit obligatoirement démontrable. En 1931 Kurt Gödel a démontré qu'il y a des assertions non démontrables (on dit aussi qu'elles sont indécidables) : il n'est pas possible de démontrer que P est vraie ni que P est fausse.*

À la base de toute théorie mathématique, on dispose d'un petit nombre d'assertions qui sont supposés vraies a priori (c'est-à-dire avant toute expérience) et que l'on nomme axiomes ou postulats. Ces axiomes sont élaborés par abstraction à partir de l'intuition et ne sont pas déduits d'autres relations.

Par exemple, la géométrie euclidienne est basée sur une quinzaine d'axiomes. L'un de ces axiomes est le postulat numéro 15 qui affirme que par un point donné passe une et une seule droite parallèle à une droite donnée.

Une autre exemple important est donné par la construction de l'ensemble noté \mathbb{N} des entiers naturels. Cette construction peut se faire en utilisant les axiomes de Peano suivants :

- 0 est un entier naturel ;
- tout entier naturel n a un unique successeur noté $n + 1$;
- deux entiers naturels ayant même successeur sont égaux ;
- une partie P de \mathbb{N} qui contient 0 et telle que si n est dans P alors le successeur de n y est aussi, est égale à \mathbb{N} (axiome de récurrence).

Nous reviendrons au paragraphe 1.6 sur l'ensemble \mathbb{N} en partant sur une autre base.

La théorie des ensemble est basée sur le système d'axiomes de Zermelo-Fränkel.

La notion de définition nous permet de décrire un objet ou une situation précise à l'aide du langage courant.

Les énoncés qui se démontrent sont classés en fonction de leur importance dans une théorie comme suit :

- un théorème est une assertion vraie déduite d'autres assertions, il s'agit en général d'un résultat important à retenir ;
- un lemme est un résultat préliminaire utilisé pour démontrer un théorème ;
- un corollaire est une conséquence importante d'un théorème ;
- une proposition est de manière générale un résultat auquel on peut attribuer la valeur vraie ou fausse sans ambiguïté.

Pour rédiger un énoncé mathématique, on utilise le langage courant et les objets manipulés sont représentés en général par des lettres de l'alphabet latin ou grec. Usuellement, on utilise :

- les lettres minuscules a, b, c, \dots pour des objets fixés ;
- les lettres minuscules x, y, z, t, \dots pour des objets inconnus à déterminer ;
- les lettres majuscules E, F, G, H, \dots pour des ensembles ;
- des lettres de l'alphabet grecques minuscules ou majuscules $\alpha, \beta, \varepsilon, \delta, \dots \Lambda, \Gamma, \Omega, \dots$

1.2 Les connecteurs logiques de base

L'élaboration de nouvelles assertions à partir d'autres se fait en utilisant les connecteurs logiques de négation, de conjonction, de disjonction, d'implication et d'équivalence définis comme suit, où P et Q désignent des assertions.

- La négation de P , notée $\neg P$, ou non P ou \overline{P} , est l'assertion qui est vraie si P est fausse et fausse si P est vraie.

Par exemple la négation de l'assertion : « x est strictement positif » est « x est négatif ou nul ».

En théorie des ensembles on admet qu'il n'existe pas d'assertion P telle que P et \overline{P} soient toutes deux vraies. On dit que cette théorie est non contradictoire.

- La conjonction de P et Q , notée $P \wedge Q$ (lire P et Q), est l'assertion qui est vraie uniquement si P et Q sont toutes deux vraies (et donc fausse dans les trois autres cas).

Par exemple $P \wedge \overline{P}$ est toujours faux (on se place dans des théories non contradictoires).

- La disjonction de P et Q , notée $P \vee Q$ (lire P ou Q), est l'assertion qui est vraie uniquement si l'une des deux assertions P ou Q est vraie (donc fausse si P et Q sont toutes deux fausses).

Par exemple $P \vee \overline{P}$ est toujours vraie (c'est une tautologie).

Il faut remarquer que le « ou » pour « ou bien » est inclusif, c'est-à-dire que P et Q peuvent être toutes deux vrais dans le cas où $P \vee Q$ est vraie.

On peut aussi introduire le « ou exclusif », noté W , qui est vrai uniquement lorsque l'une des deux assertions, mais pas les deux simultanément, est vraie.

- L'implication, notée $P \rightarrow Q$, est l'assertion qui est fausse uniquement si P est vraie et Q fausse (donc vraie dans les trois autres cas).

On peut remarquer que si P est fausse, alors $P \rightarrow Q$ est vraie indépendamment de la valeur de vérité de Q .

L'implication est à la base du raisonnement mathématique. En partant d'une assertion P (ou de plusieurs), une démonstration aboutit à un résultat Q . Si cette démonstration est faite sans erreur, alors $P \rightarrow Q$ est vraie et on notera $P \Rightarrow Q$ (ce qui signifie que si P est vraie, alors Q est vraie). Dans ce cas, on dit que P est une condition suffisante et Q une condition nécessaire.

On peut remarquer que l'implication est transitive, c'est-à-dire que si P implique Q et Q implique R , alors P implique R .

- L'équivalence de P et Q , notée $P \leftrightarrow Q$, est l'assertion qui est vraie uniquement si $P \rightarrow Q$ et $Q \rightarrow P$ sont toutes deux vraies. Dans le cas où $P \leftrightarrow Q$ est vraie on dit que P et Q sont équivalentes et on note $P \Leftrightarrow Q$ (ce qui signifie que P et Q sont, soit toutes deux vraies, soit toutes deux fausses). Dans ce cas, on dit que Q est une condition nécessaire et suffisante de P .

On peut résumer ce qui précède, en utilisant la table de vérité suivante :

| P | Q | \overline{P} | $P \wedge Q$ | $P \vee Q$ | $P \rightarrow Q$ | $P \leftrightarrow Q$ |
|-----|-----|----------------|--------------|------------|-------------------|-----------------------|
| V | V | F | V | V | V | V |
| V | F | F | F | V | F | F |
| F | V | V | F | V | V | F |
| F | F | V | F | F | V | V |

Les tables de vérité peuvent être utilisées pour faire certaines démonstrations. On rappelle que deux assertions qui ont même table de vérité sont équivalentes.

Avec le théorème qui suit, on résume quelques règles de calcul.

Théorème 1.1 Soient P, Q, R des propositions. On a les équivalences :

1. commutativité :

$$(P \wedge Q) \Leftrightarrow (Q \wedge P)$$

$$(P \vee Q) \Leftrightarrow (Q \vee P)$$

2. associativité

$$(P \wedge (Q \wedge R)) \Leftrightarrow ((P \wedge Q) \wedge R)$$

$$(P \vee (Q \vee R)) \Leftrightarrow ((P \vee Q) \vee R)$$

3. distributivité :

$$(P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$$

$$(P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$$

4. négations :

$$(\overline{\overline{P}}) \Leftrightarrow (P)$$

$$(\overline{P \wedge Q}) \Leftrightarrow (\overline{P} \vee \overline{Q})$$

$$(\overline{P \vee Q}) \Leftrightarrow (\overline{P} \wedge \overline{Q})$$

$$(P \rightarrow Q) \Leftrightarrow (\overline{Q} \rightarrow \overline{P})$$

$$(P \rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$$

$$(\overline{P \rightarrow Q}) \Leftrightarrow (P \wedge \overline{Q})$$

Démonstration. On utilise les tables de vérité (exercices). ■

Les équivalences $(P \wedge Q) \Leftrightarrow (\overline{P \vee Q})$ et $(P \vee Q) \Leftrightarrow (\overline{P \wedge Q})$ sont appelées lois de Morgan.

Exercice 1.1 Montrer que les assertions $P \rightarrow Q$ et $\overline{P} \vee Q$ sont équivalentes.

Solution 1.1 On montre qu'elles ont même table de vérité.

| P | Q | \overline{P} | $\overline{P} \vee Q$ | $P \rightarrow Q$ |
|-----|-----|----------------|-----------------------|-------------------|
| V | V | F | V | V |
| V | F | F | F | F |
| F | V | V | V | V |
| F | F | V | V | V |

Exercice 1.2 Montrer que les assertions $\overline{P \rightarrow Q}$ et $P \wedge \overline{Q}$ sont équivalentes.

Solution 1.2 On montre qu'elles ont même table de vérité.

| P | Q | $P \wedge \overline{Q}$ | $\overline{P \rightarrow Q}$ |
|-----|-----|-------------------------|------------------------------|
| V | V | F | F |
| V | F | V | V |
| F | V | F | F |
| F | F | F | F |

Exercice 1.3 Montrer que les assertions $P \leftrightarrow P$, $(P \wedge Q) \rightarrow P$, $P \rightarrow (P \vee Q)$, $P \vee (P \rightarrow Q)$, $P \rightarrow (Q \rightarrow P)$ et $((P \rightarrow Q) \rightarrow P) \rightarrow P$ sont des tautologies (i. e. toujours vraies).

Solution 1.3 Pour $P \leftrightarrow P$, $(P \wedge Q) \rightarrow P$, $P \rightarrow (P \vee Q)$, c'est évident et pour les autres, on utilise la table de vérité :

| P | Q | $P \rightarrow Q$ | $Q \rightarrow P$ | $P \vee (P \rightarrow Q)$ | $P \rightarrow (Q \rightarrow P)$ | $((P \rightarrow Q) \rightarrow P) \rightarrow P$ |
|-----|-----|-------------------|-------------------|----------------------------|-----------------------------------|---------------------------------------------------|
| V | V | V | V | V | V | V |
| V | F | F | V | V | V | V |
| F | V | V | F | V | V | V |
| F | F | V | V | V | V | V |

Exercice 1.4 Simplifier l'expression :

$$R = (\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q}) \vee (P \wedge Q).$$

Solution 1.4 En utilisant les tables de vérité, on a :

| P | Q | $\overline{P} \wedge Q$ | $\overline{P} \wedge \overline{Q}$ | $(\overline{P} \wedge Q) \vee (\overline{P} \wedge \overline{Q})$ | $P \wedge Q$ | R |
|-----|-----|-------------------------|------------------------------------|-------------------------------------------------------------------|--------------|-----|
| V | V | F | F | F | V | V |
| V | F | F | F | F | F | F |
| F | V | V | F | V | F | V |
| F | F | F | V | V | F | V |

Donc R a la même table de vérité que $P \rightarrow Q$, ce qui signifie que R est équivalent à $P \rightarrow Q$.

Exercice 1.5 Soient P, Q, R trois assertions.

1. Écrire la négation de chacune de ces assertions : $\overline{P} \wedge Q, \overline{P} \vee Q, P \vee (Q \wedge R), P \wedge (Q \vee R), P \rightarrow \overline{Q}, P \leftrightarrow Q, \overline{P \vee Q} \rightarrow R, P \vee Q \rightarrow \overline{R}, \overline{P} \wedge Q \Rightarrow R$ et $\overline{P} \vee Q \rightarrow \overline{R}$.
2. Traduire chacune de ces assertions, ainsi sa négation, en langage courant où P correspond à « j'écris », Q à « je pense » et R à « je chante ».

Solution 1.5 On a :

$$\overline{\overline{P} \wedge Q} = P \vee \overline{Q}$$

ce qui peut se traduire par la négation de « je n'écris pas et je pense » est « j'écris ou je ne pense pas » ;

$$\overline{\overline{P} \vee Q} = P \wedge \overline{Q}$$

$$\overline{P \vee (Q \wedge R)} = \overline{P} \wedge \overline{Q \wedge R} = \overline{P} \wedge (\overline{Q} \vee \overline{R}) = (\overline{P} \wedge \overline{Q}) \vee (\overline{P} \wedge \overline{R})$$

et ainsi de suite.

Exercice 1.6 Montrer les équivalences qui suivent.

1. $(P \rightarrow (Q \rightarrow R)) \Leftrightarrow ((P \wedge Q) \rightarrow R)$
2. $((P \vee Q) \rightarrow R) \Leftrightarrow ((P \rightarrow R) \wedge (Q \rightarrow R))$
3. $((P \wedge Q) \rightarrow R) \Leftrightarrow ((P \rightarrow R) \vee (Q \rightarrow R))$
4. $(P \rightarrow (Q \wedge R)) \Leftrightarrow ((P \rightarrow Q) \wedge (P \rightarrow R))$
5. $(P \rightarrow (Q \vee R)) \Leftrightarrow ((P \rightarrow Q) \vee (P \rightarrow R))$

Solution 1.6 On peut utiliser les tables de vérité ou utiliser l'équivalence $(P \rightarrow Q) \Leftrightarrow (\overline{P} \vee Q)$. Par exemple, on a :

$$(P \rightarrow (Q \rightarrow R)) \Leftrightarrow \overline{P} \vee (\overline{Q} \vee R) \Leftrightarrow \overline{P \wedge Q} \vee R \Leftrightarrow ((P \wedge Q) \rightarrow R)$$

Exercice 1.7 Montrer que les assertions $P \vee Q$ (ou exclusif) et $(P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$ sont équivalentes.

Solution 1.7 On montre qu'elles ont même table de vérité.

| P | Q | $P \vee Q$ | $(P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$ |
|-----|-----|------------|--------------------------------------------------------|
| V | V | F | F |
| V | F | V | V |
| F | V | V | V |
| F | F | F | F |

Exercice 1.8 Soient a, b deux entiers naturels.

1. Donner un équivalent de $(a < b) \rightarrow (a = b)$
2. Donner la négation de $(a \leq b) \rightarrow (a > b)$

Solution 1.8

1. $(a < b) \rightarrow (a = b)$ est équivalent à $(a \geq b) \vee (a = b)$ encore équivalent à $a \geq b$.
2. La négation de $(a \leq b) \rightarrow (a > b)$ est $(a \leq b) \wedge (a \leq b)$, soit $(a \leq b)$.

Exercice 1.9 On dispose de 6 pièces de 1 euro dont une seule est fausse et plus lourde que les autres. Montrer qu'on peut la détecter en utilisant une balance de type Roberval en effectuant au plus deux pesées. Même question avec 8 pièces.

Solution 1.9 On numérote de 1 à 6 les pièces. On place les pièces 1, 2, 3 sur le plateau P_1 de la balance et les pièces 4, 5, 6 sur le plateau P_2 . L'un des deux plateaux, disons P_1 est plus chargé, il contient donc la fausse pièce. On isole la pièce 3 et on place la pièce 1 sur le plateau P_1 et la pièce 2 sur P_2 . Si les plateaux sont équilibrés c'est 3 qui est fausse, sinon le plateau le plus chargé contient la fausse pièce.

Pour 8 pièces, on isole les pièces 7 et 8 et on place les pièces 1, 2, 3 sur le plateau P_1 et les pièces 4, 5, 6 sur le plateau P_2 . Si les plateaux sont équilibrés, on compare 7 et 8 avec la balance et on détermine la fausse pièce, sinon l'un des deux plateaux, disons P_1 est plus chargé, il contient donc la fausse pièce et le procédé utilisé pour les 6 pièces nous permet de trouver la fausse pièce.

Exercice 1.10 Des cannibales proposent à un touriste de décider lui même de son sort en faisant une déclaration : si celle-ci est vraie, il sera rôti, sinon il sera bouilli. Quelle déclaration peut faire ce touriste (malin) pour imposer une troisième solution ?

Solution 1.10 ♠♠♠

Exercice 1.11 Les habitants d'un village sont partagés en deux clans : ceux du clan A disent toujours la vérité et ceux du clan B mentent toujours. Un touriste passant par ce village rencontre trois habitants et souhaite savoir à quel clan appartient chacun d'eux. Il n'entend pas la réponse du premier, le deuxième répète ce qu'il a entendu, selon lui, du premier et le troisième lui indique le clan du premier et du second. Le touriste a la réponse à sa question. Pouvez-vous faire de même.

Solution 1.11 ♠♠♠

On dit qu'une théorie est non contradictoire si $P \wedge \overline{P}$ est faux pour toute proposition P .

Exercice 1.12 Montrer que si dans une théorie une propriété P est contradictoire, c'est-à-dire si $P \wedge \overline{P}$ est vraie, alors $Q \wedge \overline{Q}$ est vraie pour toute propriété Q .

Solution 1.12 Nous allons montrer que s'il existe un énoncé contradictoire P , alors tout énoncé Q est vrai, donc \overline{Q} aussi et $Q \wedge \overline{Q}$ est vraie.

On vérifie tout d'abord que $R = \overline{P} \rightarrow (P \rightarrow Q)$ est une tautologie avec la table de vérité :

| P | Q | \overline{P} | $P \rightarrow Q$ | $\overline{P} \rightarrow (P \rightarrow Q)$ |
|-----|-----|----------------|-------------------|----------------------------------------------|
| V | V | F | V | V |
| V | F | F | F | V |
| F | V | V | V | V |
| F | F | V | V | V |

Comme R et \overline{P} sont vraies, $P \rightarrow Q$ est vraie et Q est vraie puisque P est vraie.

1.3 Quelques méthodes de raisonnement

En général l'énoncé d'une proposition à démontrer est formé d'une ou plusieurs hypothèses qui constituent l'assertion H et d'une ou plusieurs conclusions qui constituent l'assertion C . Il s'agit donc de montrer l'implication $H \implies C$.

Si de plus, on peut montrer que $C \implies H$, on dira alors que la réciproque de la proposition est vraie.

Les idées de base que l'on peut utiliser sont les suivantes.

- Une assertion peut toujours être remplacée par n'importe quelle assertion qui lui est équivalente.
- On peut effectuer une démonstration directe, c'est à dire de déduire logiquement C de H .
- L'implication étant transitive, on peut essayer de montrer que $C \implies C'$ sachant par ailleurs que $C' \implies H$.
- Dans le cas où une démonstration directe semble difficile, on peut essayer une démonstration par l'absurde qui consiste à étudier l'assertion $H \wedge \overline{C}$ équivalente à $\overline{H \longrightarrow C}$ et on montre qu'on aboutit à une impossibilité si cette dernière assertion est vraie (pratiquement, on suppose que la conclusion est fausse avec les hypothèses et on aboutit à une absurdité). Il en résulte alors que $\overline{H \longrightarrow C}$ est fausse, c'est à dire que $H \longrightarrow C$ est vraie, soit $H \implies C$.
- On peut aussi essayer de montrer la contraposée $\overline{C} \implies \overline{H}$ puisque les implications $H \rightarrow C$ et $\overline{C} \rightarrow \overline{H}$ sont équivalentes.
- La démonstration par contre-exemple permet de montrer qu'une implication $H \rightarrow C$, où H et C sont des propriétés portant sur des variables x , est fausse. Pour ce faire on cherche une ou des valeurs de x pour lesquels $H(x)$ est vraie et $C(x)$ est fausse.
- La démonstration par récurrence permet de montrer qu'une propriété portant sur des entiers naturels est toujours vraie. Cette méthode de démonstration est décrite au paragraphe 1.6, où elle apparaît comme un théorème basé sur le fait que l'ensemble des entiers naturels est bien ordonné. Si on accepte l'axiome de Péano, le principe de récurrence en est une conséquence immédiate.

Exercice 1.13 *En raisonnant par l'absurde, montrer que $\sqrt{2}$ est irrationnel.*

Solution 1.13 *Supposons que $\sqrt{2} = \frac{p}{q}$ avec p, q entiers naturels non nuls premiers entre eux. On a alors $p^2 = 2q^2$ qui entraîne que p est pair, soit $p = 2p'$ et $q^2 = 2p'^2$ entraîne q pair, ce qui contredit p et q premiers entre eux.*

Exercice 1.14 *En raisonnant par l'absurde, montrer que $\frac{\ln(2)}{\ln(3)}$ est irrationnel.*

Solution 1.14 *Supposons que $\frac{\ln(2)}{\ln(3)} = \frac{p}{q}$ avec p, q entiers naturels non nuls premiers entre eux. On a alors $\ln(2^q) = \ln(3^p)$ et $2^q = 3^p$, ce qui est impossible puisque 2^p est un entier pair et 3^q est un entier impair.*

Exercice 1.15 *Soit n un entier naturel non carré, c'est-à-dire ne s'écrivant pas sous la forme $n = p^2$ avec p entier. En raisonnant par l'absurde et en utilisant le théorème de Bézout, montrer que \sqrt{n} est irrationnel.*

Solution 1.15 *Si n est non carré, on a alors $n \geq 2$.*

Supposons que $\sqrt{n} = \frac{p}{q}$ avec p, q premiers entre eux dans \mathbb{N}^ . Le théorème de Bézout nous dit qu'il existe un couple (u, v) d'entiers relatifs tels que $up + vq = 1$. On a alors :*

$$1 = (up + vq)^2 = u^2p^2 + 2uvpq + v^2q^2$$

avec $u^2p^2 = u^2nq^2$. L'égalité précédente s'écrit alors $qr = 1$ avec $r = u^2nq + 2uvp + v^2q$ dans \mathbb{Z} , ce qui implique que $q = 1$ et $\sqrt{n} = p$, en contradiction avec n non carré.

Exercice 1.16 *Sachant que tout entier supérieur ou égal à 2 admet un diviseur premier, montrer que l'ensemble \mathcal{P} des nombres premiers est infini.*

Solution 1.16 *On sait déjà que \mathcal{P} est non vide (il contient 2). Supposons que \mathcal{P} soit fini avec :*

$$\mathcal{P} = \{p_1, \dots, p_r\}.$$

L'entier $n = p_1 \cdots p_r + 1$ est supérieur ou égal à 2, il admet donc un diviseur premier $p_k \in \mathcal{P}$. L'entier p_k divise alors $n = p_1 \cdots p_r + 1$ et $p_1 \cdots p_r$, il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion \mathcal{P} est infini.

Exercice 1.17 *Montrer que $x = \sqrt[3]{45 + 29\sqrt{2}} + \sqrt[3]{45 - 29\sqrt{2}}$ est un entier.*

Solution 1.17 *En posant $a = \sqrt[3]{45 + 29\sqrt{2}}$ et $b = \sqrt[3]{45 - 29\sqrt{2}}$, on a :*

$$\begin{cases} a^3 + b^3 = 90 \\ ab = \sqrt[3]{45^2 - 2 \cdot 29^2} = \sqrt[3]{343} = 7 \end{cases}$$

ce qui donne :

$$\begin{aligned} 90 &= (a + b)(a^2 - ab + b^2) \\ &= (a + b)((a + b)^2 - 3ab) = x(x^2 - 21) \end{aligned}$$

donc x est racine du polynôme :

$$P(X) = X(X^2 - 21) - 90$$

On regarde si ce polynôme a des racines entières. Comme $n^2 - 21$ est négatif pour $n \leq 4$, on cherche ces racines à partir de $n = 5$. On a $P(5) = -70$ et $P(6) = 0$. On a alors $P(X) = (X - 6)(X^2 + 6X + 15)$ et $x = 6$, puis c'est la seule racine réelle de P .

1.4 Notions de base sur les ensembles. Quantificateurs

Nous nous contenterons d'une définition intuitive de la notion d'ensemble.

Un ensemble est une collection d'objets possédant des propriétés communes, ces objets sont les éléments de l'ensemble.

On utilisera les notations suivantes, pour les ensembles de nombres usuels :

- \mathbb{N} est ensemble des entiers naturels ;
- \mathbb{Z} est l'ensemble des entiers relatifs ;
- \mathbb{Q} est l'ensemble des nombres rationnels
- \mathbb{R} est l'ensemble des nombres réels ;
- \mathbb{C} est l'ensemble des nombres complexes.

On admet l'existence d'un ensemble qui ne contient aucun élément. Cet ensemble est noté \emptyset et on dit que c'est l'ensemble vide.

Nous serons souvent amenés à décrire un ensemble en précisant les propriétés que doivent vérifier tous ses éléments, ce que nous noterons de la façon suivante :

$$E = \{\text{description des propriétés des éléments de } E\}$$

(on dit que l'ensemble E est défini en compréhension).

Cette notion d'ensemble défini en compréhension peut conduire à des paradoxes liés au problème de « l'ensemble de tous les ensembles », mais à un premier niveau, on se contente de ce point de vue intuitif. Une étude approfondie de la théorie des ensembles peut mener assez loin. Le lecteur intéressé peut consulter le volume de Bourbaki sur les ensembles, ou tout autre ouvrage spécialisé.

On peut aussi décrire un ensemble en donnant la liste finie ou infinie de tous ces éléments, quand cela est possible, ce qui se note :

$$E = \{x_1, x_2, \dots, x_n\}$$

s'il s'agit d'un ensemble fini ou :

$$E = \{x_1, x_2, \dots, x_n, \dots\}$$

s'il s'agit d'un ensemble infini pour lequel on peut numéroter les éléments (un tel ensemble est dit dénombrable). On dit alors que l'ensemble E est défini en extension.

Un singleton est un ensemble qui ne contient qu'un élément, soit $E = \{a\}$.

Si n, m sont deux entiers relatifs, l'ensemble des entiers relatifs compris entre n et m sera noté $\{n, \dots, m\}$. Dans le cas où $m < n$, il ne peut y avoir d'entiers entre n et m et cet ensemble est tout simplement l'ensemble vide. Dans le cas où $n = m$, cet ensemble est le singleton $\{n\}$. Pour $n < m$, on notera aussi $\{n, n+1, \dots, m\}$ cet ensemble.

Nous nous contentons dans un premier temps de définitions intuitives de ces notions d'ensemble fini ou dénombrable (voir les paragraphes 2.1 et 2.2 pour des définitions plus rigoureuses).

Si E est un ensemble, on notera $a \in E$ pour signifier que a est un élément de E , ce qui se lit « a appartient à E ». La négation de cette assertion est « a n'appartient pas à E » et se notera $a \notin E$.

Pour signifier qu'un ensemble F est contenu dans un ensemble E , ce qui signifie que tout élément de F est dans E , nous noterons $F \subset E$ qui se lit « F est contenu dans E ». On peut écrire de manière équivalent que $E \supset F$ pour dire que E contient F . La négation de cette assertion est notée $F \not\subset E$.

Deux ensembles E et F sont égaux si, et seulement si, ils ont les mêmes éléments, ce qui se traduit par $E \subset F$ et $F \subset E$.

On admet que si E est un ensemble, il existe un ensemble dont tous les éléments sont formés de tous les sous-ensembles (ou parties) de E . On note $\mathcal{P}(E)$ cet ensemble et on dit que c'est l'ensemble des parties de E . Ainsi $F \subset E$ est équivalent à $F \in \mathcal{P}(E)$. L'ensemble vide et E sont des éléments de $\mathcal{P}(E)$.

Par exemple pour $E = \{1, 2, 3\}$, on a :

$$\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Pour décrire des ensembles, ou faire des raisonnements, nous utiliseront les deux quantificateurs suivants.

- Le quantificateur universel « quel que soit » ou « pour tout » noté \forall utilisé pour signifier que tout élément x d'un ensemble E vérifie une propriété $P(x)$, la syntaxe étant :

$$(\forall x \in E) (P(x)). \quad (1.1)$$

- Le quantificateur existentiel « il existe » noté \exists pour signifier qu'il existe au moins un élément x de E vérifiant la propriété $P(x)$, la syntaxe étant :

$$(\exists x \in E) | (P(x)). \quad (1.2)$$

Pour signifier qu'il existe un et un seul x dans E vérifiant la propriété $P(x)$, on utilisera la syntaxe :

$$(\exists!x \in E) \mid (P(x)).$$

La négation de l'assertion 1.1 est :

$$(\exists x \in E) \mid (\overline{P(x)})$$

en utilisant le symbole \mid qui se lit « tel que » utilisé pour traduire le fait que x est tel que la propriété $\overline{P(x)}$ est vérifiée et la négation de 1.2 est :

$$(\forall x \in E) (\overline{P(x)}).$$

Nous verrons qu'il n'est pas toujours facile de traduire la négation d'une assertion en utilisant les quantificateurs.

Par exemple pour traduire le fait qu'une suite $(u_n)_{n \in \mathbb{N}}$ de nombres réels est convergente vers un réel ℓ nous écrirons :

$$(\exists \ell \in \mathbb{R}) \mid (\forall \varepsilon > 0, \exists n_0 \in \mathbb{N} \mid \forall n \geq n_0, |u_n - \ell| < \varepsilon)$$

ce qui signifie qu'il existe un réel ℓ tel que quel que soit la précision $\varepsilon > 0$ que l'on choisisse l'écart entre u_n et ℓ (soit $|u_n - \ell|$) est inférieur à ε à partir d'un certain rang n_0 .

La négation de cette assertion s'écrit :

$$(\forall \ell \in \mathbb{R}), (\exists \varepsilon > 0, \forall n_0 \in \mathbb{N}, \exists n \geq n_0 \mid |u_n - \ell| \geq \varepsilon)$$

Nous étudierons plus loin les suites réelles ou complexes.

En utilisant les quantificateurs, il faudra faire attention à l'ordre d'apparition de ces derniers. Par exemple les assertions suivantes, où f est une fonction à valeurs réelles définie sur un ensemble E :

$$\forall x \in E, \exists M > 0 \mid f(x) < M$$

et

$$\exists M > 0 \mid \forall x \in E, f(x) < M.$$

ne sont pas équivalentes. La première assertion signifie que pour tout élément x de E il existe un réel $M > 0$ qui dépend à priori de x (il faudrait donc le noter $M(x)$) tel que $f(x) < M$ (par exemple $M(x) = f(x) + 1$ convient), alors que la seconde signifie qu'il existe un réel $M > 0$, indépendant de x dans E , tel que $f(x) < M$, ce qui n'est pas la même chose.

1.5 Les symboles \sum et \prod

Si n est un entier naturel non nul et x_1, x_2, \dots, x_n des entiers, rationnels, réels ou complexes, on notera :

$$\sum_{k=1}^n x_k = x_1 + x_2 + \dots + x_n \text{ et } \prod_{k=1}^n x_k = x_1 \cdot x_2 \cdot \dots \cdot x_n$$

la somme et le produit des x_k .

Dans une telle somme ou produit l'indice est muet, c'est-à-dire que $\sum_{k=1}^n x_k = \sum_{i=1}^n x_i$ et $\prod_{k=1}^n x_k =$

$$\prod_{i=1}^n x_i.$$

La manipulation d'un produit de réels strictement positifs se ramène à une somme en utilisant la fonction logarithme :

$$\ln \left(\prod_{k=1}^n x_k \right) = \sum_{k=1}^n \ln(x_k)$$

On peut également effectuer des changements d'indice. Par exemple, en posant $i = k + 1$, on aura :

$$\sum_{k=1}^n x_k = \sum_{i=2}^{n+1} x_{i-1} = \sum_{k=2}^{n+1} x_{k-1}$$

On peut ajouter ou multiplier de telles sommes (ou produits). Par exemple, on a :

$$\begin{aligned} \sum_{k=1}^n x_k + \sum_{k=1}^n y_k &= \sum_{k=1}^n (x_k + y_k) \\ \lambda \sum_{k=1}^n x_k &= \sum_{k=1}^n \lambda x_k \\ \left(\sum_{k=1}^n x_k \right) \left(\sum_{k=1}^m y_k \right) &= \left(\sum_{j=1}^n x_j \right) \left(\sum_{k=1}^m y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k. \end{aligned}$$

Pour vérifier ce résultat, on écrit que :

$$\begin{aligned} S &= \left(\sum_{k=1}^n x_k \right) \left(\sum_{k=1}^m y_k \right) \\ &= (x_1 + x_2 + \cdots + x_n) \left(\sum_{k=1}^m y_k \right) \\ &= x_1 \sum_{k=1}^m y_k + \cdots + x_n \sum_{k=1}^m y_k \\ &= \sum_{j=1}^n x_j \left(\sum_{k=1}^m y_k \right) = \sum_{j=1}^n \left(\sum_{k=1}^m x_j y_k \right) = \sum_{\substack{1 \leq j \leq n \\ 1 \leq k \leq m}} x_j y_k. \end{aligned}$$

Exercice 1.18 Montrer que pour tout entier $n \geq 1$, on a :

$$P_n = \prod_{k=1}^n \left(1 + \frac{1}{k} \right)^k = \frac{(n+1)^n}{n!}.$$

Solution 1.18 Il revient au même de calculer $S_n = \ln(P_n)$. On a :

$$\begin{aligned} S_n &= \ln \left(\prod_{k=1}^n \left(\frac{k+1}{k} \right)^k \right) = \sum_{k=1}^n (k \ln(k+1) - k \ln(k)) \\ &= \sum_{k=1}^n k \ln(k+1) - \sum_{k=1}^n k \ln(k) \end{aligned}$$

et le changement d'indice $j = k + 1$ dans la première somme donne :

$$\begin{aligned}
 S_n &= \sum_{j=2}^{n+1} (j-1) \ln(j) - \sum_{k=1}^n k \ln(k) \\
 &= \sum_{j=2}^{n+1} j \ln(j) - \sum_{j=2}^{n+1} \ln(j) - \sum_{k=1}^n k \ln(k) \\
 &= \sum_{k=2}^{n+1} k \ln(k) - \sum_{k=2}^{n+1} \ln(k) - \sum_{k=1}^n k \ln(k) \\
 &= (n+1) \ln(n+1) - \sum_{k=2}^{n+1} \ln(k)
 \end{aligned}$$

(on a utilisé le fait que l'indice est muet dans une somme).

On a donc en définitive :

$$\begin{aligned}
 S_n &= \ln(P_n) = \ln((n+1)^{n+1}) - \sum_{k=2}^{n+1} \ln(k) \\
 &= \ln((n+1)^{n+1}) - \ln\left(\prod_{k=2}^n k\right) = \ln((n+1)^{n+1}) - \ln(n!) \\
 &= \ln\left(\frac{(n+1)^{n+1}}{n!}\right)
 \end{aligned}$$

et $P_n = \frac{(n+1)^n}{n!}$.

Une autre solution consiste à effectuer directement un changement d'indice dans le produit. Soit :

$$\begin{aligned}
 P &= \prod_{k=1}^n \left(\frac{k+1}{k}\right)^k = \frac{\prod_{k=1}^n (k+1)^k}{\prod_{k=1}^n k^k} \\
 &= \frac{\prod_{j=2}^{n+1} j^{j-1}}{\prod_{k=1}^n k^k} = \frac{\prod_{k=2}^{n+1} k^{k-1}}{\prod_{k=1}^n k^k} = \frac{2 \cdot 3^2 \cdot 4^3 \cdot \dots \cdot n^{n-1} \cdot (n+1)^n}{2^2 \cdot 3^3 \cdot 4^4 \cdot \dots \cdot (n-1)^{n-1} \cdot n^n} \\
 &= \frac{(n+1)^n}{2 \cdot 3 \cdot 4 \cdot \dots \cdot (n-1) \cdot n} = \frac{(n+1)^n}{n!}.
 \end{aligned}$$

1.6 Les théorèmes de récurrence

On désigne par \mathbb{N} l'ensemble des entiers naturels, soit :

$$\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}.$$

La construction de cet ensemble avec les opérations usuelles d'addition et de multiplication est admise.

On note \mathbb{N}^* l'ensemble \mathbb{N} privé de 0.

Notre point de départ est l'axiome du bon ordre suivant : toute partie non vide de \mathbb{N} admet un plus petit élément, ce qui signifie que si A est une partie non vide de \mathbb{N} , il existe alors un entier m tel que :

$$\begin{cases} m \in \mathbb{N}, \\ \forall n \in A, m \leq n. \end{cases}$$

Exercice 1.19 On peut montrer que $\sqrt{3}$ est irrationnel en utilisant seulement le fait que \mathbb{N} est bien ordonné. Pour ce faire on raisonne par l'absurde en supposant qu'il existe deux entiers strictement positifs a et b tels que $\sqrt{3} = \frac{a}{b}$.

On introduit l'ensemble :

$$A = \left\{ q \in \mathbb{N} - \{0\} \mid \exists p \in \mathbb{N} \mid \sqrt{3} = \frac{p}{q} \right\}.$$

1. Montrer que A a un plus petit élément q_1 . On a donc $\sqrt{3} = \frac{p_1}{q_1}$ avec $p_1 \in \mathbb{N}$.
2. Montrer que $\sqrt{3} = \frac{3q_1 - p_1}{p_1 - q_1}$ et conclure.

Solution 1.19

1. Si on suppose $\sqrt{3}$ rationnel alors l'ensemble A est non vide dans \mathbb{N} et en conséquence il admet un plus petit élément q_1 . Comme $q_1 \in A$, il existe un entier $p_1 \geq 1$ tel que $\sqrt{3} = \frac{p_1}{q_1}$.
2. On a :

$$\sqrt{3} + 1 = \frac{2}{\sqrt{3} - 1} = \frac{2q_1}{p_1 - q_1}$$

et :

$$\sqrt{3} = \frac{2q_1}{p_1 - q_1} - 1 = \frac{3q_1 - p_1}{p_1 - q_1} = \frac{p_2}{q_2}$$

où on a posé :

$$\begin{cases} p_2 = 3q_1 - p_1, \\ q_2 = p_1 - q_1. \end{cases}$$

Comme $1 < \sqrt{3} = \frac{p_1}{q_1} < 2$ (puisque $1 < 3 = \sqrt{3}^2 < 4$) on a $p_1 < 2q_1$, donc $p_2 > 0$ et $q_2 < q_1$. On a donc $\sqrt{3} = \frac{p_2}{q_2}$ avec $q_2 \in A$ et $q_2 < q_1$, ce qui contredit le fait que q_1 est le plus petit élément de A . On peut donc conclure à l'irrationalité de $\sqrt{3}$.

En fait l'exercice précédent peut se généraliser comme suit.

Exercice 1.20 Soit n un entier naturel non carré (i. e. il n'existe pas d'entier p tel que $n = p^2$). On se propose, comme dans l'exercice précédent, de montrer que \sqrt{n} est irrationnel en utilisant seulement le fait que \mathbb{N} est bien ordonné.

Pour ce faire on raisonne par l'absurde en supposant qu'il existe deux entiers strictement positifs a et b tels que $\sqrt{n} = \frac{a}{b}$.

On introduit l'ensemble :

$$A = \left\{ q \in \mathbb{N} - \{0\} \mid \exists p \in \mathbb{N} \mid \sqrt{n} = \frac{p}{q} \right\}.$$

1. Montrer que A a un plus petit élément q_1 . On a donc $\sqrt{n} = \frac{p_1}{q_1}$ avec $p_1 \in \mathbb{N}$.
2. Montrer qu'il existe un entier $m_1 \in [1, \sqrt{n}[$ tel que $\sqrt{n} = \frac{nq_1 - m_1p_1}{p_1 - m_1q_1}$ et conclure.

Solution 1.20

1. Si on suppose \sqrt{n} rationnel alors l'ensemble A est non vide dans \mathbb{N} et en conséquence il admet un plus petit élément q_1 . Comme $q_1 \in A$, il existe un entier $p_1 \geq 1$ tel que $\sqrt{n} = \frac{p_1}{q_1}$.
2. L'ensemble :

$$B = \{m \in \mathbb{N}^* \mid m^2 < n\}$$

étant non vide dans \mathbb{N}^* (1 est dans B car n non carré dans \mathbb{N} entraîne $n \geq 2$) et majoré par n admet un plus grand élément $m_1 \in \mathbb{N} \cap [1, \sqrt{n}[$ et on a :

$$m_1^2 < n < (m_1 + 1)^2$$

(m_1 est en fait la partie entière de \sqrt{n}). On a alors :

$$\sqrt{n} + m_1 = \frac{n - m_1^2}{\sqrt{n} - m_1} = \frac{(n - m_1^2) q_1}{p_1 - m_1 q_1}$$

et :

$$\sqrt{n} = \frac{(n - m_1^2) q_1}{p_1 - m_1 q_1} - m_1 = \frac{nq_1 - m_1 p_1}{p_1 - m_1 q_1} = \frac{p_2}{q_2}$$

où on a posé :

$$\begin{cases} p_2 = nq_1 - m_1 p_1, \\ q_2 = p_1 - m_1 q_1. \end{cases}$$

En tenant compte de $\sqrt{n} = \frac{p_1}{q_1}$, on a :

$$p_2 = p_1 \left(n \frac{q_1}{p_1} - m_1 \right) = p_1 (\sqrt{n} - m_1) > 0,$$

soit $p_2 \geq 1$ et $q_2 \geq 1$ puisque $\sqrt{n} = \frac{p_2}{q_2} > 0$. Ensuite de :

$$\sqrt{n} = \frac{p_1}{q_1} < m_1 + 1,$$

on déduit que :

$$q_2 = p_1 - m_1 q_1 < q_1.$$

On a donc $q_2 \in A$ et $q_2 < q_1$, ce qui contredit le fait que q_1 est le plus petit élément de A . On peut donc conclure à l'irrationalité de \sqrt{n} .

De l'axiome du bon ordre, on déduit les deux théorèmes fondamentaux qui suivent. Le premier résultat est souvent appelé théorème de récurrence faible et le second théorème de récurrence forte.

Théorème 1.2 Soient $n_0 \in \mathbb{N}$ et $\mathcal{P}(n)$ une propriété portant sur les entiers $n \geq n_0$. La propriété $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$ si et seulement si :

- (i) $\mathcal{P}(n_0)$ est vraie ;
- (ii) pour tout $n \geq n_0$ si $\mathcal{P}(n)$ est vrai alors $\mathcal{P}(n+1)$ est vraie.

Démonstration. La condition nécessaire est évidente.

En supposant les conditions (i) et (ii) vérifiées, on note A l'ensemble des entiers $n \geq n_0$ pour lesquels $\mathcal{P}(n)$ est faux. Si A est non vide il admet alors un plus petit élément $n > n_0$ (puisque $\mathcal{P}(n_0)$ est vraie). Mais alors $\mathcal{P}(n-1)$ est vraie ce qui implique, d'après (ii), que $\mathcal{P}(n)$ est vraie, soit une contradiction. En définitive A est vide et la propriété est vraie pour tout entier $n \geq n_0$. ■

Théorème 1.3 Soient $n_0 \in \mathbb{N}$ et $\mathcal{P}(n)$ une propriété portant sur les entiers $n \geq n_0$. La propriété $\mathcal{P}(n)$ est vraie pour tout entier $n \geq n_0$ si et seulement si :

- (i) $\mathcal{P}(n_0)$ est vraie ;
- (ii) pour tout $n \geq n_0$ si $\mathcal{P}(k)$ est vrai pour tout entier k compris entre n_0 et n , alors $\mathcal{P}(n+1)$ est vraie.

Démonstration. La condition nécessaire est évidente.

En supposant les conditions (i) et (ii) vérifiées, on note A l'ensemble des entiers $n \geq n_0$ pour lesquels $\mathcal{P}(n)$ est faux. Si A est non vide il admet alors un plus petit élément $n > n_0$ et $\mathcal{P}(k)$ est vraie pour tout k compris entre n_0 et $n-1$, ce qui implique que $\mathcal{P}(n)$ est vraie, soit une contradiction. En définitive A est vide et la propriété est vraie pour tout entier $n \geq n_0$. ■

Exercice 1.21 Montrer que $2^n > n^2$ pour tout entier $n \geq 5$.

Solution 1.21 Pour $n = 5$, on a $2^5 = 32 > 5^2 = 25$.

Supposant le résultat acquis au rang $n \geq 5$, on a :

$$2^{n+1} = 2 \cdot 2^n > 2n^2 > (n+1)^2$$

puisque :

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2 > 0$$

pour $n \geq 5$. Le résultat est donc vrai au rang $n+1$ et il est vrai pour tout $n \geq 5$.

Exercice 1.22 Montrer que si φ est une fonction strictement croissante de \mathbb{N} dans \mathbb{N} , on a alors $\varphi(n) \geq n$ pour tout n .

Solution 1.22 Comme φ est une fonction de \mathbb{N} dans \mathbb{N} , $\varphi(0)$ est un entier naturel et donc $\varphi(0) \geq 0$. Supposant le résultat acquis pour $n \geq 0$, sachant que φ est strictement croissante, on a $\varphi(n+1) > \varphi(n) \geq n$, donc $\varphi(n+1) > n$, ce qui équivaut à $\varphi(n+1) \geq n+1$ puisque $\varphi(n+1)$ est un entier.

Le théorème de récurrence faible peut être utilisé pour montrer quelques identités classiques comme celles qui apparaissent avec les exercices qui suivent.

Exercice 1.23 Montrer par récurrence que pour tout entier naturel non nul n , on a :

$$\begin{aligned} U_n &= \sum_{k=1}^n k = \frac{n(n+1)}{2}, \\ V_n &= \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}, \\ W_n &= \sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2} \right)^2 = U_n^2. \end{aligned}$$

Solution 1.23 Pour $n = 1$ c'est clair.

En supposant les résultats acquis pour $n \geq 1$, on a :

$$U_{n+1} = \frac{n(n+1)}{2} + n + 1 = \frac{n^2 + 3n + 2}{2} = \frac{(n+1)(n+2)}{2}$$

$$\begin{aligned} V_{n+1} &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

$$\begin{aligned} W_{n+1} &= \left(\frac{n(n+1)}{2} \right)^2 + (n+1)^3 = \frac{(n+1)^2(n^2 + 4n + 4)}{4} \\ &= \left(\frac{(n+1)(n+2)}{2} \right)^2 \end{aligned}$$

On a aussi :

$$\begin{aligned} U_n &= 1 + 2 + \cdots + (n-1) + n \\ &= n + (n-1) + \cdots + 2 + 1 \end{aligned}$$

et en additionnant terme à terme on obtient :

$$2U_n = n(n+1).$$

Le calcul de U_n peut aussi se faire en passant par V_{n+1} et en utilisant l'identité :

$$(k+1)^2 = k^2 + 2k + 1$$

Précisément, en effectuant le changement d'indice $k = j + 1$, on a :

$$V_{n+1} = \sum_{k=1}^{n+1} k^2 = \sum_{j=0}^n (j+1)^2 = \sum_{j=0}^n j^2 + 2 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit :

$$V_{n+1} = V_n + 2U_n + n + 1$$

et :

$$2U_n = V_{n+1} - V_n - (n+1) = (n+1)^2 - (n+1) = n(n+1)$$

ce qui donne bien $U_n = \frac{n(n+1)}{2}$.

De même, le calcul de V_n peut aussi se faire en passant par W_{n+1} et en utilisant l'identité :

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1$$

Précisément, en effectuant le changement d'indice $k = j + 1$, on a :

$$W_{n+1} = \sum_{k=1}^{n+1} k^3 = \sum_{j=0}^n (j+1)^3 = \sum_{j=0}^n j^3 + 3 \sum_{j=0}^n j^2 + 3 \sum_{j=0}^n j + \sum_{j=0}^n 1$$

soit :

$$W_{n+1} = W_n + 3V_n + 3U_n + n + 1$$

et :

$$\begin{aligned} 3V_n &= W_{n+1} - W_n - 3U_n - (n + 1) = (n + 1)^3 - 3\frac{n(n + 1)}{2} - (n + 1) \\ &= \frac{n(n + 1)(2n + 1)}{2} \end{aligned}$$

ce qui donne bien $V_n = \frac{n(n + 1)(2n + 1)}{6}$.

Ce procédé peut en fait se généraliser.

Exercice 1.24 Calculer, pour tout entier naturel n , la somme :

$$I_n = 1 + 3 + 5 + \cdots (2n - 1) + (2n + 1).$$

Solution 1.24 On a :

$$\begin{aligned} I_n &= \sum_{k=0}^n (2k + 1) = 2 \sum_{k=0}^n k + \sum_{k=0}^n 1 = n(n + 1) + (n + 1) \\ &= (n + 1)^2. \end{aligned}$$

Exercice 1.25 On appelle nombres triangulaires les sommes $U_n = \sum_{k=1}^n k$ et nombres pyramidaux les sommes $P_n = \sum_{k=1}^n U_k$. Montrer que :

$$P_n = \frac{n(n + 1)(n + 2)}{6}.$$

Solution 1.25 Pour $n = 1$ on a $P_1 = U_1 = 1$ et le résultat est acquis est vrai pour $n = 1$. En le supposant acquis pour $n \geq 1$, on a :

$$\begin{aligned} P_{n+1} &= \frac{n(n + 1)(n + 2)}{6} + \frac{(n + 1)(n + 2)}{2} \\ &= \frac{(n + 1)(n + 2)}{2} \left(\frac{n}{3} + 1 \right) = \frac{(n + 1)(n + 2)(n + 3)}{6}. \end{aligned}$$

Exercice 1.26 Montrer par récurrence, que pour tout entier naturel n et tout nombre complexe λ différent de 1, on a :

$$\sum_{k=0}^n \lambda^k = \frac{\lambda^{n+1} - 1}{\lambda - 1}.$$

Solution 1.26 Pour $n = 0$, c'est clair. Si c'est vrai pour $n \geq 0$, alors :

$$\sum_{k=0}^{n+1} \lambda^k = \frac{\lambda^{n+1} - 1}{\lambda - 1} + \lambda^{n+1} = \frac{\lambda^{n+2} - 1}{\lambda - 1}.$$

Plus généralement, on a l'identité (dite remarquable) suivante.

Exercice 1.27 Montrer que pour tout entier naturel n et tous nombres complexes a et b on a :

$$b^{n+1} - a^{n+1} = (b - a) \sum_{k=0}^n a^k b^{n-k}.$$

Solution 1.27 Pour $n = 0$, c'est évident. En supposant le résultat acquis au rang $n \geq 0$, on a :

$$\begin{aligned} b^{n+2} - a^{n+2} &= (b^{n+1} - a^{n+1})b + ba^{n+1} - a^{n+2} \\ &= (b - a) \sum_{k=0}^n a^k b^{n+1-k} + (b - a)a^{n+1} \\ &= (b - a)(b^{n+1} + ab^n + \dots + a^{n-1}b^2 + a^n b) + (b - a)a^{n+1} \\ &= (b - a) \sum_{k=0}^{n+1} a^k b^{n+1-k}. \end{aligned}$$

Le résultat est donc vrai pour tout $n \geq 0$.

Le théorème de récurrence nous permet de définir la fonction factorielle sur l'ensemble des entiers naturels de la façon suivante :

$$\begin{cases} 0! = 1 \\ \forall n \in \mathbb{N}, (n+1)! = (n+1)n! \end{cases}$$

De manière plus générale, c'est le théorème de récurrence qui nous assure de l'existence et de l'unicité d'une suite (réelle ou complexe) définie par :

$$\begin{cases} u_0 \text{ est un scalaire donné,} \\ \forall n \in \mathbb{N}, u_{n+1} = f(u_n) \end{cases}$$

où f est une fonction définie sur un ensemble I et à valeurs dans le même ensemble I . Une telle suite est dite définie par une relation de récurrence (d'ordre 1).

Une telle suite peut aussi se définir en donnant les premières valeurs u_0, u_1, \dots, u_p et une relation $u_{n+1} = f(u_n, \dots, u_{n-(p-1)})$ pour $n \geq p-1$. Une telle suite est dite définie par une relation de récurrence d'ordre p .

Exercice 1.28 Montrer que pour tout entier naturel n et tous nombres complexes a et b on a :

$$(a + b)^n = \sum_{k=0}^n C_n^k a^{n-k} b^k$$

où $C_n^k = \frac{n!}{k!(n-k)!}$ pour k compris entre 0 et n avec la convention $0! = 1$ (formule du binôme de Newton).

Solution 1.28 Pour $n = 0$ et $n = 1$, c'est évident. En supposant le résultat acquis au rang $n \geq 1$, on a :

$$\begin{aligned}
 (a+b)^{n+1} &= (a+b)^n (a+b) = \left(\sum_{k=0}^n C_n^k a^{n-k} b^k \right) (a+b) \\
 &= \sum_{k=0}^n C_n^k a^{n-(k-1)} b^k + \sum_{k=0}^n C_n^k a^{n-k} b^{k+1} \\
 &= \sum_{k=0}^n C_n^k a^{n-(k-1)} b^k + \sum_{k=1}^{n+1} C_n^{k-1} a^{n-(k-1)} b^k \\
 &= a^{n+1} + \sum_{k=1}^n (C_n^k + C_n^{k-1}) a^{n+1-k} b^k + b^{n+1}
 \end{aligned}$$

et tenant compte de $C_n^k + C_n^{k-1} = C_{n+1}^k$ (triangle de Pascal), cela s'écrit :

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k a^{n+1-k} b^k.$$

Le résultat est donc vrai pour tout $n \geq 0$.

Les coefficients C_n^k se notent aussi $\binom{n}{k}$.

On peut remarquer que, pour k fixé :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

est un polynôme en n de degré k , ce qui permet d'étendre cette définition à \mathbb{R} ou même \mathbb{C} .

Comme $(a+b)^n$, on a aussi :

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Exercice 1.29 Montrer par récurrence, que pour tout entier naturel non nul n et tout nombre complexe λ différent de 1, on a :

$$\sum_{k=1}^n k\lambda^k = n \frac{\lambda^{n+1}}{\lambda-1} + \lambda \frac{1-\lambda^n}{(\lambda-1)^2}.$$

Solution 1.29 Pour $n = 1$, c'est clair. Si c'est vrai pour $n \geq 1$, alors :

$$\begin{aligned}
 \sum_{k=1}^{n+1} k\lambda^k &= n \frac{\lambda^{n+1}}{\lambda-1} + \lambda \frac{1-\lambda^n}{(\lambda-1)^2} + (n+1)\lambda^{n+1} \\
 &= n \frac{\lambda^{n+1}}{\lambda-1} + \lambda \frac{1-\lambda^n}{(\lambda-1)^2} + n\lambda^{n+1} \frac{\lambda-1}{\lambda-1} + \lambda^{n+1} \frac{(\lambda-1)^2}{(\lambda-1)^2} \\
 &= \frac{n\lambda^{n+2}}{\lambda-1} + \frac{\lambda}{(\lambda-1)^2} (1 + \lambda^{n+1}(\lambda-2)) \\
 &= \frac{(n+1)\lambda^{n+2}}{\lambda-1} + \frac{\lambda}{(\lambda-1)^2} (1 - \lambda^{n+1}).
 \end{aligned}$$

Exercice 1.30 Montrer que pour tout entier $n \geq 1$, on a :

$$\sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}} = 2 \cos \left(\frac{\pi}{2^{n+1}} \right)$$

(le nombre 2 apparaissant n fois sous la racine).

Solution 1.30 Notons $x_n = \sqrt{2 + \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}}$. Pour $n = 1$, on a :

$$x_1 = \sqrt{2} = 2 \cos \left(\frac{\pi}{4} \right).$$

Supposant le résultat acquis au rang $n \geq 1$, on a :

$$x_{n+1}^2 = 2 + x_n = 2 + 2 \cos \left(\frac{\pi}{2^{n+1}} \right)$$

et utilisant la formule $\cos(2\theta) = 2 \cos^2(\theta) - 1$, il vient :

$$\cos \left(\frac{\pi}{2^{n+1}} \right) = \cos \left(2 \frac{\pi}{2^{n+2}} \right) = 2 \cos^2 \left(\frac{\pi}{2^{n+2}} \right) - 1$$

on a :

$$x_{n+1}^2 = 4 \cos^2 \left(\frac{\pi}{2^{n+2}} \right).$$

Comme x_{n+1} est positif, on en déduit que $x_{n+1} = 2 \cos \left(\frac{\pi}{2^{n+2}} \right)$.

Exercice 1.31 Soit x_1, x_2, \dots, x_n des réels dans $[0, 1]$. Montrer par récurrence que $\prod_{k=1}^n (1 - x_k) \geq 1 - \sum_{k=1}^n x_k$.

Solution 1.31 Notons :

$$u_n = \prod_{k=1}^n (1 - x_k) \text{ et } v_n = 1 - \sum_{k=1}^n x_k.$$

Pour $n = 1$, on a $u_1 = v_1$.

Supposant le résultat acquis au rang $n \geq 1$ et tenant compte de $1 - x_{n+1} \geq 0$, on a :

$$\begin{aligned} u_{n+1} &= u_n (1 - x_{n+1}) \geq \left(1 - \sum_{k=1}^n x_k \right) (1 - x_{n+1}) \\ &\geq 1 - \sum_{k=1}^n x_k - x_{n+1} + x_{n+1} \sum_{k=1}^n x_k \geq 1 - \sum_{k=1}^{n+1} x_k = v_{n+1}. \end{aligned}$$

puisque tous les x_k sont positifs.

Les théorèmes de récurrence peuvent aussi être utilisés pour montrer les résultats fondamentaux d'arithmétique suivants.

Exercice 1.32 Soit a, b deux entiers naturels avec b non nul. Montrer qu'il existe un unique couple d'entiers (q, r) tel que :

$$\begin{cases} a = bq + r, \\ 0 \leq r \leq b - 1. \end{cases}$$

Solution 1.32 On montre tout d'abord l'existence du couple (q, r) par récurrence sur l'entier $a \geq 0$.

Pour $a = 0$, le couple $(q, r) = (0, 0)$ convient.

Supposant le résultat acquis pour tous les entiers a' compris entre 0 et $a - 1$, où a est un entier naturel non nul, on distingue deux cas. Si a est compris entre 1 et $b - 1$, le couple $(q, r) = (0, a)$ convient, sinon on a $a \geq b$, donc $0 \leq a - b \leq a - 1$ et l'hypothèse de récurrence nous assure de l'existence d'un couple d'entiers (q, r) tels que $a - b = bq + r$ et $0 \leq r \leq b - 1$, ce qui nous fournit le couple d'entiers $(q', r) = (q + 1, r)$.

L'unicité se montre facilement par l'absurde.

Exercice 1.33 Soit n un entier naturel supérieur ou égal à 2. Montrer, par récurrence, que soit n est premier, soit n admet un diviseur premier $p \leq \sqrt{n}$.

Solution 1.33 Pour $n = 2$ et $n = 3$, le résultat est évident (n est premier).

Supposons le acquis pour tous les entiers strictement inférieurs à $n \geq 3$. Si n est premier, c'est terminé, sinon il existe deux entiers a et b compris entre 2 et $n - 1$ tels que $n = ab$ et comme ces deux entiers jouent des rôles symétriques, on peut supposer que $a \leq b$. L'hypothèse de récurrence nous dit que soit a est premier et c'est alors un diviseur premier de n tel que $a^2 \leq ab \leq n$, soit a admet un diviseur premier $p \leq \sqrt{a}$ et p divise aussi n avec $p \leq \sqrt{n}$.

Exercice 1.34 Montrer que tout entier naturel n supérieur ou égal à 2 se décompose de manière unique sous la forme :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

où les p_k sont des nombres premiers vérifiant :

$$2 \leq p_1 < p_2 < \cdots < p_r$$

et les α_k sont des entiers naturels non nuls (décomposition en nombres premiers).

Solution 1.34 On démontre tout d'abord l'existence d'une telle décomposition par récurrence sur $n \geq 2$.

Pour $n = 2$, on a déjà la décomposition.

Supposons que, pour $n \geq 2$, tout entier k compris entre 2 et n admet une telle décomposition. Si $n + 1$ est premier, on a déjà la décomposition, sinon on écrit $n + 1 = ab$ avec a et b compris entre 2 et n et il suffit d'utiliser l'hypothèse de récurrence pour a et b .

L'unicité d'une telle décomposition se montre également par récurrence sur $n \geq 2$. Le résultat est évident pour $n = 2$. Supposons le acquis pour tout entier k compris entre 2 et $n \geq 2$. Si $n + 1$ a deux décompositions :

$$n + 1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s},$$

où les p_j [resp. q_i] sont premiers deux à deux distincts et les α_j [resp. β_i] entiers naturels non nuls. L'entier p_1 est premier et divise le produit $q_1^{\beta_1} \cdots q_s^{\beta_s}$, il divise donc nécessairement l'un des q_k . L'entier q_k étant également premier la seule possibilité est $p_1 = q_k$. En simplifiant par p_1 on se ramène à la décomposition d'un entier inférieur ou égal à n et il suffit d'utiliser l'hypothèse de récurrence pour conclure.

Exercice 1.35 Pour tout entier naturel n supérieur ou égal à 2, on note $H_n = \sum_{k=1}^n \frac{1}{k}$.

1. Soit p un entier naturel non nul. Montrer que $H_{2p} = \frac{1}{2}H_p + \frac{a}{2b+1}$ où a, b sont des entiers naturels avec a non nul.
2. Montrer par récurrence que pour tout entier naturel non nul H_n est le quotient d'un entier impair par un entier pair et qu'en conséquence ce n'est pas un entier.

Solution 1.35

1. On a :

$$H_{2p} = \sum_{k=1}^p \frac{1}{2k} + \sum_{k=0}^{p-1} \frac{1}{2k+1} = \frac{1}{2}H_p + \frac{N}{D}$$

avec $D = \text{ppcm}(1, 3, \dots, 2p-1)$ qui est impair et N entier naturel non nul.

2. On a $H_2 = \frac{3}{2} \notin \mathbb{N}$. Supposons le résultat acquis au rang $n \geq 2$. Si $n = 2p$, on a alors :

$$\begin{aligned} H_{n+1} &= H_n + \frac{1}{2p+1} = \frac{2a+1}{2b} + \frac{1}{2p+1} \\ &= \frac{(2a+1)(2p+1) + 2b}{2b(2p+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + b + p + 2ap$ et $b' = b(2p+1)$. Si $n = 2p+1$, on a alors :

$$\begin{aligned} H_{n+1} &= H_{2(p+1)} = \frac{c}{2d+1} + \frac{1}{2}H_{p+1} \\ &= \frac{c}{2d+1} + \frac{1}{2} \frac{2a+1}{2b} = \frac{4bc + (2d+1)(2a+1)}{4b(2d+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + d + 2ad + 2bc$ et $b' = 2b(2d+1)$.

Dans tous les cas, H_n est le quotient d'un entier impair par un entier pair et en conséquence, ce n'est pas un entier.

1.7 L'algèbre des parties d'un ensemble

Nous allons définir sur l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E des opérations qui vont traduire les idées intuitives de partie complémentaire, d'intersection et de réunion.

L'ensemble E étant donné et A, B, C, \dots désignant des parties de E (donc des éléments de $\mathcal{P}(E)$), on définit les ensembles suivant.

- le complémentaire de A dans E est l'ensemble noté $C_E A$, ou $E \setminus A$ (lire E moins A) ou \overline{A} des éléments de E qui ne sont pas dans A , ce qui peut se traduire par :

$$(x \in \overline{A}) \Leftrightarrow ((x \in E) \wedge (x \notin A))$$

ou encore par :

$$\overline{A} = \{x \in E \mid x \notin A\}$$

- L'intersection de A et B , notée $A \cap B$, est l'ensemble des éléments de E qui sont dans A et dans B , soit :

$$(x \in A \cap B) \Leftrightarrow ((x \in A) \wedge (x \in B))$$

ou encore :

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$

Si $A \cap B = \emptyset$, on dit alors que A et B sont disjointes.

Par exemple A et \overline{A} sont disjointes.

- La réunion de A et B , notée $A \cup B$, est l'ensemble des éléments de E qui sont soit dans A , soit dans B (éventuellement dans A et B) soit :

$$(x \in A \cup B) \Leftrightarrow ((x \in A) \vee (x \in B))$$

ou encore :

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$

- La différence de A et B , notée $A \setminus B$, est l'ensemble des éléments de E qui sont dans A et qui ne sont pas dans B , soit :

$$(x \in A \setminus B) \Leftrightarrow ((x \in A) \wedge (x \notin B))$$

ou encore :

$$A \setminus B = \{x \in A \mid x \notin B\}$$

Ainsi $\overline{A} = E \setminus A$.

- La différence symétrique de A et B , notée $A \Delta B$, est l'ensemble des éléments de E qui sont soit dans A et pas dans B soit dans B et pas dans A (c'est-à-dire dans A ou exclusif dans B), soit :

$$(x \in A \Delta B) \Leftrightarrow ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))$$

Par exemple, on a $A \Delta \emptyset = A$, $A \Delta E = \overline{A}$.

Ces opérateurs de complémentarité, intersection, réunion et différence symétrique sont décrits à l'aide des connecteurs logiques non de négation, \wedge de conjonction, \vee de disjonction et \vee de disjonction exclusive.

Avec le théorème qui suit, on résume les résultats essentiels relatifs à ces opérateurs ensemblistes.

Théorème 1.4 Soient E un ensemble et A, B, C, \dots des sous-ensembles de E . On a :

1. commutativité :

$$A \cap B = B \cap A$$

$$A \cup B = B \cup A$$

$$A \Delta B = B \Delta A$$

2. associativité :

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

3. distributivité :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4. *différence symétrique :*

$$A \Delta A = \emptyset$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

$$A \Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$$

$$A \Delta B = (A \cup B) \setminus (A \cap B)$$

5. *négations :*

$$\overline{\overline{A}} = A$$

$$(A \subset B) \Leftrightarrow (\overline{B} \subset \overline{A})$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Démonstration. Laissée au lecteur. ■

On notera l'analogie entre ce théorème et le théorème 1.1 sur les règles de calculs avec les connecteurs logiques.

Toutes ces égalités entre ensembles se visualisent bien en utilisant les diagrammes d'Euler-Venn.

La propriété d'associativité de l'intersection et de la réunion nous permet d'écrire $A \cap B \cap C$ et $A \cup B \cup C$ l'intersection et la réunion de trois ensembles sans se soucier de parenthèses. De manière plus générale, grâce à cette associativité, on peut définir l'intersection ou la réunion de n sous-ensembles A_1, A_2, \dots, A_n de E par :

$$(x \in A_1 \cap A_2 \cap \dots \cap A_n) \Leftrightarrow ((x \in A_1) \wedge (x \in A_2) \wedge \dots \wedge (x \in A_n))$$

et :

$$(x \in A_1 \cup A_2 \cup \dots \cup A_n) \Leftrightarrow ((x \in A_1) \vee (x \in A_2) \vee \dots \vee (x \in A_n))$$

De façon condensée, on écrira $(A_k)_{1 \leq k \leq n}$ une telle famille de sous ensembles de E et :

$$\bigcap_{k=1}^n A_k = A_1 \cap A_2 \cap \dots \cap A_n$$

l'intersection et :

$$\bigcup_{k=1}^n A_k = A_1 \cup A_2 \cup \dots \cup A_n$$

la réunion.

On vérifie facilement que pour tout entier j compris entre 1 et n , on a :

$$\bigcap_{k=1}^n A_k \subset A_j \subset \bigcup_{k=1}^n A_k.$$

Définition 1.1 On dit qu'une famille $(A_k)_{1 \leq k \leq n}$ de parties d'un ensemble E forme une partition de E si les A_k sont deux à deux disjoints, c'est-à-dire que $A_k \cap A_j = \emptyset$ pour $1 \leq k \neq j \leq n$ de réunion égale à E , soit $\bigcup_{k=1}^n A_k = E$.

Dans le cas où (A_1, A_2) forme une partition de E , on a nécessairement $A_2 = \overline{A_1}$.

Exercice 1.36 Simplifier les expressions suivantes, où A et B sont des sous-ensembles d'un ensemble E :

1. $C = (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B}) \cup (A \cap B)$
2. \overline{C}
3. $D = \overline{\overline{A \cap B} \cap (\overline{A} \cap B) \cup (A \cap B) \cap (A \cap B)}$

Solution 1.36

1. Avec la distributivité de \cap sur \cup , on a :

$$\overline{A} = \overline{A} \cap E = \overline{A} \cap (B \cup \overline{B}) = (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B})$$

(on a mis \overline{A} en facteur) et avec la distributivité de \cup sur \cap , on a :

$$C = \overline{A} \cup (A \cap B) = (\overline{A} \cup A) \cap (\overline{A} \cup B) = E \cap (\overline{A} \cup B) = \overline{A} \cup B.$$

2. $\overline{C} = A \cap \overline{B}$.

3. En posant :

$$X = A \cap \overline{B}, Y = \overline{X} \cap (\overline{A} \cap B), Z = \overline{Y} \cup (A \cap B), T = \overline{Z} \cap (A \cap B)$$

on a :

$$\begin{aligned} D = \overline{T} &= Z \cup (\overline{A} \cup \overline{B}) = \overline{Y} \cup (A \cap B) \cup (\overline{A} \cup \overline{B}) \\ &= X \cup (A \cup \overline{B}) \cup (A \cap B) \cup (\overline{A} \cup \overline{B}) \end{aligned}$$

avec $(A \cup \overline{B}) \cup (\overline{A} \cup \overline{B}) = E$, donc $D = E$.

Exercice 1.37 Soient A_1, A_2, \dots, A_p des ensembles deux à deux distincts. Montrer que l'un de ces ensembles ne contient aucun des autres.

Solution 1.37 On raisonne par l'absurde, c'est-à-dire qu'on suppose que chacun des ensembles A_k contient un ensemble A_j différent de A_k . Donc A_1 contient un ensemble $A_{j_1} \neq A_1$, soit $A_{j_1} \subsetneq A_1$, A_{j_1} contient un ensemble $A_{j_2} \neq A_{j_1}$, soit $A_{j_2} \subsetneq A_{j_1}$, et on peut continuer indéfiniment, ce qui est impossible puisque la famille d'ensembles est finie.

Exercice 1.38 Que dire de deux ensembles A et B tels que $A \cap B = A \cup B$?

Solution 1.38 On a toujours $A \cap B \subset A \cup B$. Si de plus $A \cup B \subset A \cap B$, on a alors :

$$A \subset A \cup B \subset A \cap B \subset B \text{ et } B \subset A \cup B \subset A \cap B \subset A$$

ce qui donne $A = B$.

Exercice 1.39 Soient A, B, C trois ensembles. Montrer que $A \cap C = A \cup B$ si, et seulement si, $B \subset A \subset C$.

Solution 1.39 Si $A \cap C = A \cup B$, alors :

$$B \subset A \cup B = A \cap C \subset A \text{ et } A \subset A \cup B = A \cap C \subset C.$$

Réciproquement si $B \subset A \subset C$, alors :

$$A \cap C = A = A \cup B$$

Exercice 1.40 Soient A, B, C trois ensembles. Montrer que si $A \cup B \subset A \cup C$ et $A \cap B \subset A \cap C$, alors $B \subset C$.

Solution 1.40 Soit $x \in B$. Comme $A \cup B \subset A \cup C$, x est dans $A \cup C$. S'il est dans C c'est fini, sinon il est dans A , donc dans $A \cap B \subset A \cap C$, donc dans C .

Exercice 1.41 Soient A, B, C trois ensembles. Montrer que :

$$(A \cup B) \cap (B \cup C) \cap (C \cup A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$$

Solution 1.41 On a :

$$(A \cup B) \cap (B \cup C) = B \cup (A \cap C)$$

et, en notant $D = (A \cup B) \cap (B \cup C) \cap (C \cup A)$, on a :

$$D = ((B \cap C) \cup (A \cap B)) \cup (C \cap A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$$

Où alors on part de $x \in D$ et on montre que $x \in E = (A \cap B) \cup (B \cap C) \cup (C \cap A)$, puis partant de $x \in E$, on montre que $x \in D$.

La notion de produit cartésien de deux ensembles sera très souvent utilisée. Elle correspond à l'idée de couples et se généralise pour aboutir à la notion de liste.

Définition 1.2 Étant donné deux ensembles E et F , on appelle produit cartésien de E par F l'ensemble $E \times F$ des couples (x, y) formés d'un élément x de E et d'un élément y de F .

Il est à noter que les couples sont ordonnés, c'est-à-dire que $(x, y) = (y, x)$ $E \times F$ si, et seulement si $x = y$. De manière plus générale, on a $(x, y) = (x', y')$ dans $E \times F$ si, et seulement si $x = x'$ et $y = y'$.

Dans le cas où $F = E$, on note E^2 pour $E \times E$.

On peut itérer le procédé et définir le produit cartésien $E_1 \times E_2 \times \cdots \times E_n$ de n ensembles comme l'ensemble des listes (ordonnées) (x_1, x_2, \cdots, x_n) formées d'un élément x_1 de E_1 suivi d'un élément x_2 de E_2 , \cdots , suivi d'un élément x_n de E_n . On notera de façon condensé :

$$\prod_{k=1}^n E_k = E_1 \times E_2 \times \cdots \times E_n.$$

Là encore, on a $(x_1, x_2, \cdots, x_n) = (x'_1, x'_2, \cdots, x'_n)$ dans $E \times F$ si, et seulement si $x_k = x'_k$ pour tout k compris entre 1 et n .

Dans le cas où tous les E_k sont égaux à un même ensemble E , on notera E^n pour $E \times E \times \cdots \times E$ (n fois).

Exercice 1.42 Montrer que l'ensemble :

$$C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$

ne peut pas s'écrire comme produit cartésien de deux parties de \mathbb{R} .

Solution 1.42 Si $C = E \times F$, où E et F sont deux parties de \mathbb{R} , on a alors $(1, 0) \in C = E \times F$ et $(1, 0) \in C = E \times F$, donc $1 \in E \cap F$ et $(1, 1) \in E \times F = C$, ce qui est faux.

1.8 Applications. Notions d'injectivité, surjectivité et bijectivité

Les notations E, F, G désignent des ensembles.

Définition 1.3 On appelle *application*, ou *fonction*, de E dans F (ou de E vers F) toute partie Γ du produit cartésien $E \times F$ telle que :

$$\forall x \in E, \exists ! y \in F \mid (x, y) \in \Gamma.$$

En notant f une application de E dans F (c'est en réalité le triplet (E, F, Γ) avec la propriété énoncée ci-dessus), on notera pour tout $x \in E$, $f(x)$ l'unique élément de F tel que $(x, f(x)) \in \Gamma$ et on dira que $f(x)$ est l'image de x par f et x est un antécédent de y par f . Un antécédent de y par f n'est pas unique a priori.

On dira aussi que E est l'ensemble de départ (ou l'ensemble de définition), F l'ensemble d'arrivée et Γ le graphe de l'application f .

Deux applications f et g sont égales si, et seulement si, elles ont même ensemble de départ E , même ensemble d'arrivée F et même graphe Γ , c'est-à-dire que :

$$\forall x \in E, g(x) = f(x)$$

On a tout simplement précisé l'idée d'un procédé qui associe à tout élément de E un unique élément de F .

On notera :

$$\begin{array}{ccc} f : & E & \rightarrow & F \\ & x & \mapsto & f(x) \end{array}$$

une telle application (ou fonction). On utilisera aussi les notation $f : E \rightarrow F$ ou $f : x \mapsto f(x)$.

Remarque 1.2 Nous ne faisons pas la distinction ici entre fonction et application. Usuellement, on distingue ces notions en disant qu'une fonction de E dans F toute partie Γ du produit cartésien $E \times F$ telle que pour tout élément x de E , il existe au plus un élément y de F tel que $(x, y) \in \Gamma$. Le sous-ensemble D de E pour lequel il existe un unique élément y de F tel que $(x, y) \in \Gamma$ est appelé l'ensemble de définition de la fonction. Une application est donc une fonction pour laquelle tout élément de l'ensemble de départ E a une image dans F .

On notera $\mathcal{F}(E, F)$ ou F^E l'ensemble de toutes les applications de E dans F (la deuxième notation sera justifiée plus loin).

L'application qui associe à tout x d'un ensemble E le même x est l'application identique notée Id_E , où Id si l'ensemble E est fixé.

Si f est une fonction de E dans F et D un sous-ensemble non vide de E , on définit une application g de D dans F en posant :

$$\forall x \in D, g(x) = f(x)$$

et on dit que g est la restriction de f à D , ce qui se note $g = f|_D$.

Définition 1.4 Soit f une application de E dans F . Pour toute partie A de E , l'image de A par f est le sous ensemble de F noté $f(A)$ et défini par :

$$f(A) = \{f(x) \mid x \in A\}.$$

Pour toute partie B de F , l'image réciproque de B par f est le sous ensemble de E noté $f^{-1}(B)$ et défini par :

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}.$$

On a donc, pour tout $y \in F$:

$$y \in f(A) \Leftrightarrow \exists x \in A \mid y = f(x)$$

et pour tout $x \in E$:

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$

L'ensemble $f(E)$ est appelé l'image de f .

À propos de la notation $f^{-1}(B)$, on pourra lire la remarque 1.3 (qui n'engage que moi) plus loin.

Exemple 1.1 On a $f(\emptyset) = \emptyset$, $f(\{x\}) = \{f(x)\}$ pour tout $x \in E$, $f^{-1}(\emptyset) = \emptyset$ et $f^{-1}(F) = E$.

Pour tout $y \in F$, $f^{-1}\{y\}$ est l'ensemble des $x \in E$ tels que $f(x) = y$ et cet ensemble peut être vide ou formé de un ou plusieurs éléments. En fait $f^{-1}\{y\}$ est l'ensemble des solutions dans E de l'équation $f(x) = y$, où y est donné dans F et x l'inconnue dans E . Cette équation peut avoir 0 ou plusieurs solutions.

Exemple 1.2 Pour $f : x \mapsto x^2$ avec $E = F = \mathbb{R}$, on a $f^{-1}\{0\} = \{0\}$, $f^{-1}\{-1\} = \emptyset$ et $f^{-1}\{1\} = \{-1, 1\}$.

On vérifie facilement le résultat suivant.

Théorème 1.5 Soit f une application de E dans F . Pour toutes parties A, B de E et C, D de F , on a :

1. $A \subset B \Rightarrow f(A) \subset f(B)$
2. $f(A \cup B) = f(A) \cup f(B)$
3. $f(A \cap B) \subset f(A) \cap f(B)$
4. $C \subset D \Rightarrow f^{-1}(C) \subset f^{-1}(D)$
5. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
6. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
7. $f^{-1}(\overline{C}) = \overline{f^{-1}(C)}$

Démonstration. Vérification immédiate.

Par exemple, pour le point 2, on peut écrire que y est dans $f(A \cup B)$ si, et seulement si, il existe x dans $A \cup B$ tel que $y = f(x)$, ce qui implique que $y \in f(A)$ dans le cas où $x \in A$ ou $y \in f(B)$ dans le cas où $x \in B$, soit $y \in f(A) \cup f(B)$ dans tous les cas. Réciproquement si $y \in f(A) \cup f(B)$, il est dans $f(A)$ ou $f(B)$ et s'écrit donc $y = f(x)$ avec x dans A ou B , ce qui signifie que $y \in f(A \cup B)$. On a donc les inclusions $f(A \cup B) \subset f(A) \cup f(B)$ et $f(A) \cup f(B) \subset f(A \cup B)$, c'est-à-dire l'égalité souhaitée.

Pour le point 3, on a seulement une inclusion. Dire que $y \in f(A \cap B)$ équivaut à dire qu'il existe $x \in A \cap B$ tel que $y = f(x)$ et $y \in f(A) \cap f(B)$. Réciproquement, si $y \in f(A) \cap f(B)$, il existe $x_1 \in A$ et $x_2 \in B$ tels que $y = f(x_1) = f(x_2)$ et, a priori, il n'y a aucune raison pour que $x_1 = x_2$. ■

Exercice 1.43 Vérifier sur un exemple que l'égalité $f(A \cap B) = f(A) \cap f(B)$ n'est pas toujours vérifiée.

Solution 1.43 Considérer $f : x \mapsto \sin(x)$ avec $A = [-\pi, \pi]$ et $B = [0, 2\pi]$. On a :

$$f(A \cap B) = f([0, \pi]) = [0, 1] \subsetneq f(A) \cap f(B) = [-1, 1].$$

Exercice 1.44 Soit f une application de E dans F . Vérifier que :

1. pour toute partie A de E , $A \subset f^{-1}(f(A))$
2. pour toute partie B de F , $f(f^{-1}(B)) = B \cap f(E)$.

Solution 1.44 Vérification immédiate.

Exercice 1.45 Soient E un ensemble et f une application de $\mathcal{P}(E)$ dans \mathbb{R} telle que pour toutes parties disjointes de E on ait $f(A \cup B) = f(A) + f(B)$.

1. Montrer que $f(\emptyset) = 0$.
2. Montrer que pour toutes parties A, B de E , on a :

$$f(A \cup B) + f(A \cap B) = f(A) + f(B).$$

Solution 1.45

1. On a $f(\emptyset) = f(\emptyset \cup \emptyset) = f(\emptyset) + f(\emptyset)$ dans \mathbb{R} , donc $f(\emptyset) = 0$.
2. Avec les partitions $A \cup B = A \cup (B \setminus A)$ et $B = (A \cap B) \cup (B \setminus A)$, on a :

$$\begin{cases} f(A \cup B) = f(A) + f(B \setminus A) \\ f(B) = f(A \cap B) + f(B \setminus A) \end{cases}$$

et par soustraction :

$$f(A \cup B) - f(B) = f(A) - f(A \cap B)$$

qui donne le résultat.

Après avoir défini le cardinal d'un ensemble et la notion d'ensemble fini (qui est quand même intuitive), nous verrons que si E est un ensemble fini alors la fonction f qui associe à une partie A de E son cardinal (c'est-à-dire le nombre de ses éléments) vérifie l'équation fonctionnelle de l'exercice précédent.

On dispose d'une opération importante sur les fonctions, c'est la composition des fonctions qui permet de construire de nouvelles fonctions à partir de fonctions données.

Définition 1.5 Soient f une application de E dans F et g une application de F dans G . La composée de f par g est la fonction de E dans G notée $g \circ f$ et définie par :

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

Ce qui peut se schématiser par :

$$\begin{array}{ccccc} E & \xrightarrow{f} & F & \xrightarrow{g} & G \\ x & \mapsto & f(x) & \mapsto & g(f(x)) \end{array}$$

On remarquera que $f \circ g$ n'est pas définie a priori (dans la situation de la définition).

Dans le cas où f est définie de E dans F et g de F dans E , on peut définir les applications $f \circ g$ (de F dans F) et $g \circ f$ (de E dans E) et il n'y a aucune raison pour que ces applications soient égales, même si $F = E$.

Dans le cas où $E = F$, on dit que les applications f et g (définies de E dans E) commutent si $f \circ g = g \circ f$.

On vérifie facilement que la loi de composition est associative, c'est-à-dire que $f \circ (g \circ h) = (f \circ g) \circ h$, quand toutes ces composées ont un sens.

Cette propriété d'associativité permet de définir la composée de n applications $f_1 \circ f_2 \circ \dots \circ f_n$ sans se soucier de parenthèses.

Si f est une application de E dans E , on peut définir la suite de ses itérées par la relation de récurrence suivante :

$$\begin{cases} f^1 = f \\ \forall n \in \mathbb{N}^*, f^{n+1} = f^n \circ f \end{cases}$$

On convient que $f^0 = Id_E$.

On vérifie facilement que $f^p \circ f^q = f^q \circ f^p = f^{p+q}$ pour tous entiers naturels p, q .

Exercice 1.46 Soient E et F deux ensembles. Déterminer toutes les applications f de E dans E telles que $f \circ g = g \circ f$ pour toute application g de E dans E .

Solution 1.46 Soit $x \in E$ et g la fonction définie sur E par $g(y) = x$ pour tout $y \in E$ (la fonction constante égale à x). On a alors $x = g(f(x)) = f(g(x)) = f(x)$. Comme x est quelconque dans E , on déduit que $f = Id_E$.

Les notions suivantes d'injectivité et de surjectivité sont aussi très importantes.

Définition 1.6 Soient E, F deux ensembles et f une application de E dans F . On dit que f est :

1. *injective* (ou que c'est une injection) si deux éléments distincts de E ont deux images distinctes dans F , soit :

$$x_1 \neq x_2 \text{ dans } E \Rightarrow f(x_1) \neq f(x_2) \text{ dans } F \quad (1.3)$$

2. *surjective* (ou que c'est une surjection) si tout élément de F a au moins un antécédent dans E , soit :

$$\forall y \in F, \exists x \in E \mid y = f(x)$$

3. *bijjective* (ou que c'est une bijection) si elle est à la fois injective ou surjective.

Une injection peut aussi se caractériser en disant que tout élément de F a au plus un antécédent par f , encore équivalent à dire que pour tout $y \in F$ l'équation $y = f(x)$ a au plus une solution x dans E , ce qui revient à dire que si x_1 et x_2 sont deux éléments de E tels que $f(x_1) = f(x_2)$, alors $x_1 = x_2$ (contraposée de (1.3)).

Une surjection peut se caractériser en disant que pour tout $y \in F$ l'équation $y = f(x)$ a au moins une solution x dans E , encore équivalent à dire que $f(E) = F$.

Si f est une surjection de E dans F , on dit parfois que f est une surjection de E sur (pour surjection) F .

Une bijection peut se caractériser en disant que tout élément de F a un unique antécédent par f , encore équivalent à dire que pour tout $y \in F$ l'équation $y = f(x)$ a une et une seule solution x dans E , ce qui permet de définir l'application réciproque de f , notée f^{-1} , de F dans E par :

$$(y \in F \text{ et } x = f^{-1}(y)) \Leftrightarrow (x \in E \text{ et } y = f(x)).$$

Cette application f^{-1} est une bijection de F dans E .

L'application $f \circ f^{-1}$ est alors l'application identité $y \mapsto y$ de F dans F et l'application $f^{-1} \circ f$ est alors l'application identité $x \mapsto x$ de E dans E , ce qui se note $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

Définition 1.7 On appelle permutation d'un ensemble E toute bijection de E dans lui même.

On note en général $\mathfrak{S}(E)$ l'ensemble des permutations de E .

Exemple 1.3 L'application $x \mapsto x^2$ est surjective de \mathbb{R} dans \mathbb{R}^+ , mais non injective. Elle est bijective de \mathbb{R}^+ dans \mathbb{R}^+ .

Remarque 1.3 Dans le cas où f est une application de E dans F , on a noté pour toute partie B de F , $f^{-1}(B)$ l'image réciproque de B par f , sans aucune hypothèse de bijectivité pour f . Dans le cas où f est bijective, $f^{-1}(B)$ est aussi l'image directe de B par f^{-1} , mais dans le cas général, il faut bien prendre garde, malgré la notation, que f n'a aucune raison d'être bijective. Il faudrait en réalité utiliser un autre symbole que f^{-1} (par exemple $f^*(B)$, $f^{(-1)}(B)$, ou $f^{\zeta\boxtimes}(f)$), mais je préfère utiliser la notation $f^{-1}(B)$ rencontrée le plus souvent. Si l'on sait de quoi l'on parle il n'y a pas de véritable problème, il s'agit seulement d'une notation.

On peut lire dans *An introduction to the theory of numbers* de Hardy et Wright, p. 7 : « We shall very often use A as in (vi), viz. an unspecified positive constant. Different A 's have usually different values, even when they occur in the same formula; and even when definite values can be assigned to them, these values are irrelevant to the argument. » C'est peut être excessif, mais l'essentiel est toujours de savoir de quoi l'on parle, on pourra ensuite écrire les choses en toute rigueur.

Exercice 1.47 Montrer qu'une application f strictement monotone de \mathbb{R} dans \mathbb{R} est injective.

Solution 1.47 Supposons que f soit strictement croissante (au besoin on remplace f par $-f$). Si $x \neq y$, on a nécessairement $x > y$ ou $y > x$ et donc $f(x) > f(y)$ ou $f(x) < f(y)$, soit $f(x) \neq f(y)$ dans tous les cas.

Exercice 1.48 Soit m un entier naturel. Montrer que s'il existe un entier naturel n et une injection φ de $E_n = \{1, \dots, n\}$ dans $E_m = \{1, \dots, m\}$, on a alors nécessairement $n \leq m$.

Solution 1.48 On procède par récurrence sur $m \geq 0$.

Si $m = 0$, on a alors $E_m = \emptyset$ et $E_n = \emptyset$ (en effet, si $E_n \neq \emptyset$, l'ensemble $f(E_n)$ est alors non vide et contenu dans l'ensemble vide, ce qui est impossible), donc $n = 0$.

Supposons le résultat acquis pour $m \geq 0$. Soit φ une injection de E_n dans E_{m+1} . Si $n = 0$, on a bien $n \leq m + 1$. Si $n \geq 1$, on distingue alors deux cas de figure :

- soit $\varphi(n) = m + 1$ et dans ce cas φ induit une bijection de E_{n-1} dans E_m (la restriction de φ à E_{n-1}) et $n - 1 \leq m$, soit $n \leq m + 1$;
- soit $\varphi(n) \neq m + 1$ et dans ce cas, en désignant par ψ l'application de E_{m+1} dans lui-même définie par $\psi(\varphi(n)) = m + 1$, $\psi(m + 1) = \varphi(n)$ et $\psi(k) = k$ pour $k \in E_{m+1} \setminus \{\varphi(n), m + 1\}$, l'application $\psi \circ \varphi$ est injective de E_n dans E_{m+1} (composée de deux injections puisque φ est injective et ψ bijective) avec $\psi \circ \varphi(n) = m + 1$, ce qui nous ramène au cas précédent.

On déduit de l'exercice précédent que pour $n > m$ dans \mathbb{N} , il n'existe pas d'injection de $\{1, \dots, n\}$ dans $\{1, \dots, m\}$.

Exercice 1.49 Soient n, m deux entiers naturels. Montrer que s'il existe une bijection φ de $E_n = \{1, \dots, n\}$ sur $E_m = \{1, \dots, m\}$, on a alors nécessairement $n = m$.

Solution 1.49 On a $n \leq m$ puisque φ est une injection de E_n dans E_m et $m \leq n$ puisque φ^{-1} est une injection de E_m dans E_n , ce qui donne $n = m$.

Le résultat des deux exercices précédents nous seront utiles pour définir le cardinal (c'est-à-dire le nombre d'éléments) d'un ensemble fini.

Exercice 1.50 Soient E, F deux ensembles et f une bijection de E sur F . Montrer que si g [resp. h] est une application de F sur E telle que $g \circ f = Id_E$ [resp. $f \circ h = Id_F$], alors g [resp. h] est bijective et $g = f^{-1}$ [resp. $h = f^{-1}$].

Solution 1.50 Résulte de $g = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$ et $h = f^{-1} \circ (f \circ h) = f^{-1} \circ Id_F = f^{-1}$.

On vérifie facilement le résultat suivant.

Théorème 1.6 Soient E, F, G des ensembles, f une application de E dans F et g une application de F dans G .

1. Si f et g sont injectives, alors $g \circ f$ est injective (la composée de deux injections est une injection).
2. Si f et g sont surjectives, alors $g \circ f$ est surjective (la composée de deux surjections est une surjection).
3. Si f et g sont bijectives, alors $g \circ f$ est bijective (la composée de deux injections est une bijection) et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Démonstration.

1. Supposons f et g injectives. Si $g \circ f(x_1) = g \circ f(x_2)$, alors $g(f(x_1)) = g(f(x_2))$, donc $f(x_1) = f(x_2)$ puisque g est injective et $x_1 = x_2$ puisque f est injective.
2. Supposons f et g surjectives. Pour tout $z \in G$, il existe $y \in F$ tel que $z = g(y)$ puisque g est surjective et $y \in F$ s'écrit $y = f(x)$ avec $x \in E$ puisque f est surjective. On a donc $z = g \circ f(x)$ avec $x \in E$. L'application $g \circ f$ est donc surjective.

De manière plus compacte, on peut écrire que :

$$(g \circ f)(E) = g(f(E)) = g(F) = G.$$

3. Les deux premiers points nous disent que $g \circ f$ est bijective si f et g le sont. Puis avec $(f^{-1} \circ g^{-1}) \circ g \circ f = f^{-1} \circ Id_F \circ f = f^{-1} \circ f = Id_E$, on déduit que $f^{-1} \circ g^{-1}$ est l'inverse de $g \circ f$.

■

Exercice 1.51 Soient E, F, G des ensembles, f une application de E dans F et g une application de F dans G . Montrer que :

1. si $g \circ f$ est injective, alors f est injective ;
2. si $g \circ f$ est surjective, alors g est surjective ;
3. si $g \circ f$ est surjective et g injective, alors f est surjective ;
4. Si $g \circ f$ est injective et f surjective, alors g est injective.

Solution 1.51

1. Si x, x' dans E sont tels que $f(x) = f(x')$, alors $g \circ f(x) = g \circ f(x')$ et $x = x'$ puisque $g \circ f$ est injective. L'application f est donc injective.

2. Pour tout z dans G , il existe x dans E tel que $z = g \circ f(x)$ puisque $g \circ f$ est surjective et en notant $y = f(x)$, on a $y \in F$ et $z = g(y)$, ce qui prouve que g est surjective.
3. Soit $y \in F$. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $z = g(y) = (g \circ f)(x) = g(f(x))$ et $y = f(x)$ si on suppose de plus que g est injective. En conséquence, f est surjective.
4. Soient y, y' dans F tels que $g(y) = g(y')$. Comme f est surjective, il existe x, x' dans E tels que $y = f(x)$ et $y' = f(x')$, ce qui donne $g \circ f(x) = g \circ f(x')$ et $x = x'$ puisque $g \circ f$ est injective, donc $y = y'$.

Le résultat qui suit peut parfois être utile pour montrer l'injectivité, la surjectivité ou la bijectivité d'une application.

Théorème 1.7 Soient E, F deux ensembles et f une application de E dans F .

1. S'il existe une application g de F dans E telle que $g \circ f = Id_E$, alors f est injective.
2. S'il existe une application h de F dans E telle que $f \circ h = Id_F$, alors f est surjective.
3. S'il existe deux applications g et h de F dans E telles que $g \circ f = Id_E$ et $f \circ h = Id_F$, alors f est bijective et $g = h = f^{-1}$.

Démonstration.

1. Si x, x' dans E sont tels que $f(x) = f(x')$, alors $x = g \circ f(x) = g \circ f(x') = x'$ et f est injective.
2. Pour tout $y \in F$, on a $y = (f \circ h)(y) = f(h(y))$ avec $x = h(y) \in E$, donc f est surjective.
3. Les deux premiers points nous disent que f est bijective et de $g \circ f = Id_E$, on déduit que $f^{-1} = (g \circ f) \circ f^{-1} = g$. De même $h = g^{-1}$.

■

Exercice 1.52 Soient m un entier naturel non nul et E un ensemble non vide. Montrer que s'il existe une surjection φ de $E_m = \{1, \dots, m\}$ sur E , on peut alors construire une injection de E dans E_m .

Solution 1.52 Comme φ est surjective de E_m sur E , on a $\varphi^{-1}\{x\} \neq \emptyset$ pour tout $x \in E$ et chacun de ces sous-ensembles de E_m a un plus petit élément $j_x = \min \varphi^{-1}\{x\} \in E_m$, ce qui permet de définir l'application ψ de E dans E_m par :

$$\forall x \in E, \psi(x) = j_x$$

On a alors :

$$\forall x \in E, \varphi \circ \psi(x) = \varphi(j_x) = x$$

c'est-à-dire que $\varphi \circ \psi = Id_E$ et l'application ψ est injective (théorème précédent).

Exercice 1.53 Soient n, m deux entiers naturels non nuls. Montrer que s'il existe une surjection φ de $E_n = \{1, \dots, n\}$ sur $E_m = \{1, \dots, m\}$, on a alors nécessairement $n \geq m$.

Solution 1.53 En utilisant le résultat de l'exercice précédent, on peut construire une injection de E_m dans E_n et nécessairement $m \leq n$ (exercice 1.48).

Exercice 1.54 Soient E un ensemble et f une application de E dans E . Montrer que f est injective si, et seulement si, $f(A \cap B) = f(A) \cap f(B)$ pour toutes parties A et B de E .

Solution 1.54 On a toujours $f(A \cap B) \subset f(A) \cap f(B)$ pour toutes parties A et B de E , que f soit injective ou pas. En effet un élément y de $f(A \cap B)$ s'écrit $y = f(x)$ avec $x \in A \cap B$ et donc $y \in f(A) \cap f(B)$. Réciproquement si $y \in f(A) \cap f(B)$, il existe $x \in A$ et $x' \in B$ tels que $y = f(x) = f(x')$ et dans le cas où f est injective, on a nécessairement $x = x' \in A \cap B$, donc $y \in f(A \cap B)$.

On a donc $f(A \cap B) = f(A) \cap f(B)$ pour toutes parties A et B de E , si f est injective.

Réciproquement supposons que $f(A \cap B) = f(A) \cap f(B)$ pour toutes parties A et B de E . Si f n'est pas injective, il existe $x \neq x'$ dans E tels que $f(x) = f(x')$ et :

$$\emptyset = f(\emptyset) = f(\{x\} \cap \{x'\}) = f(\{x\}) \cap f(\{x'\}) = f(\{x\}) = \{f(x)\}$$

ce qui est impossible. Donc f est injective.

Exercice 1.55 Soient E un ensemble et f une application de E dans E . Montrer que f est bijective si, et seulement si, $f(\overline{A}) = \overline{f(A)}$ pour toute partie A de E .

Solution 1.55 Supposons f bijective. Un élément y de E est dans $f(\overline{A})$ si, et seulement si, il s'écrit $y = f(x)$ où x est uniquement déterminé dans \overline{A} , ce qui implique $y \notin f(A)$ (sinon $y = f(x') = f(x)$ avec $x' \in A$ et $x = x' \in A$, ce qui contredit $x \in \overline{A}$). On a donc $f(\overline{A}) \subset \overline{f(A)}$. Si $y \notin f(A)$, il s'écrit $y = f(x)$ (f est bijective) et $x \notin A$, donc $y \in \overline{f(A)}$. On a donc $\overline{f(A)} \subset f(\overline{A})$ et $f(\overline{A}) = \overline{f(A)}$.

Supposons que $f(\overline{A}) = \overline{f(A)}$ pour toute partie A de E . En particulier, on a $f(E) = f(\overline{\emptyset}) = \overline{f(\emptyset)} = \overline{\emptyset} = E$ et f est surjective. Si $x \neq x'$ dans E , en remarquant que $x' \in \overline{\{x\}}$, on a $f(x') \in f(\overline{\{x\}}) = \overline{f(\{x\})}$ et $f(x) \neq f(x')$. Donc f est injective.

Exercice 1.56 Soient E, F, G, H des ensembles, f une application de E dans F , g une application de F dans G et h une application de G dans H . Montrer que si $g \circ f$ et $h \circ g$ sont bijectives, alors f, g et h sont bijectives.

Solution 1.56 Si $g \circ f$ est bijective, elle est alors surjective et il en est de même de g (exercice 1.51). Si $h \circ g$ est bijective, elle est alors injective et il en est de même de g (exercice 1.51). Donc g est bijective. Il en résulte que $f = g^{-1} \circ (g \circ f)$ et $h = (h \circ g) \circ g^{-1}$ sont bijectives comme composées.

Exercice 1.57 On désigne par f l'application définie sur $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ par :

$$\forall (n, m) \in \mathbb{N}^2, f(n, m) = 2^n 3^m$$

Montrer que f est injective. Il résulte que \mathbb{N}^2 est en bijection avec le sous ensemble $f(\mathbb{N}^2)$ de \mathbb{N} . Ce résultat se traduit en disant que \mathbb{N}^2 est dénombrable.

Solution 1.57 L'égalité $f(n, m) = f(n', m')$ avec (n, m) et (n', m') dans \mathbb{N}^2 équivaut à $2^n 3^m = 2^{n'} 3^{m'}$ et l'unicité de la décomposition en facteurs premiers d'un entier naturel non nul nous dit que $(n, m) = (n', m')$. L'application f est donc injective de \mathbb{N}^2 dans \mathbb{N} et bijective de \mathbb{N}^2 dans $f(\mathbb{N}^2) \subset \mathbb{N}$.

Exercice 1.58 Montrer que l'application $f : (n, m) \mapsto 2^{n+m+1} + 2^m$ est injective de \mathbb{N}^2 dans \mathbb{N} .

Solution 1.58 L'égalité $f(n, m) = f(n', m')$ avec (n, m) et (n', m') dans \mathbb{N}^2 équivaut à $2^m (2^{n+1} + 1) = 2^{m'} (2^{n'+1} + 1)$. Si $m > m'$, on a alors $2^{m-m'} (2^{n+1} + 1) = 2^{n'+1} + 1$ qui est à la fois pair et impair, ce qui est impossible. De manière analogue, on voit que $m' > m$ est impossible. On a donc $m = m'$ et $2^{n+1} + 1 = 2^{n'+1} + 1$, ce qui équivaut à $n = n'$. L'application f est donc injective.

Analyse combinatoire

2.1 Cardinal d'un ensemble fini

La notion d'ensemble fini est relativement intuitive, c'est un ensemble dont on peut numéroté les éléments de 1 (ou de 0) à n où n est un entier naturel non nul (si on numérote à partir de 1). Par exemple $\{1, 2, 3, 4, 5\}$ est fini et on a envie de dire qu'il a 5 éléments.

On rappelle que si n est un entier naturel, l'ensemble $\{1, \dots, n\}$ est l'ensemble vide pour $n = 0$ et l'ensemble des entiers compris entre 1 et n pour n non nul.

De manière précise, on peut donner la définition suivante.

Définition 2.1 *On dit qu'un ensemble E est fini s'il existe un entier naturel n et une bijection φ de $\{1, \dots, n\}$ sur E .*

Un ensemble qui n'est pas fini est dit infini.

Remarque 2.1 *Si $n = 0$ dans la définition ci-dessus, on dispose alors d'une application f de E dans l'ensemble vide (la bijection réciproque φ^{-1}) et l'ensemble E est nécessairement vide. En effet si $E \neq \emptyset$, on a alors $f(E) \neq \emptyset$ qui est contenu dans l'ensemble vide, ce qui est impossible.*

Si φ est une bijection φ de $\{1, \dots, n\}$ sur E avec $n \geq 1$, on a alors $E = \varphi(\{1, \dots, n\}) = \{\varphi(1), \dots, \varphi(n)\}$ et il semble naturel de dire que n est le nombre d'éléments de E . Pour valider cette définition, on a besoin du résultat suivant qui nous assure l'unicité d'un tel entier n .

Théorème 2.1 *Si un ensemble E est en bijection avec un ensemble $\{1, \dots, n\}$ où n est un entier naturel n , alors cet entier n est unique.*

Démonstration. Si φ est une bijection de $E_n = \{1, \dots, n\}$ sur E et ψ une bijection de $E_m = \{1, \dots, m\}$ sur E , alors $\psi^{-1} \circ \varphi$ est une bijection de E_n sur E_m et $n = m$ (exercice 1.49).

■

On peut donc donner la définition suivante.

Définition 2.2 *Soit E un ensemble fini. Si φ est une bijection de $E_n = \{1, \dots, n\}$ sur E , où n est un entier naturel, on dit alors que n est le cardinal (ou le nombre d'éléments) de E et on note $n = \text{card}(E)$ (ou encore $\#(E)$).*

Une bijection φ de E_n sur un ensemble fini non vide E nous permet de numéroté les éléments de E et on peut noter :

$$E = \{x_1, x_2, \dots, x_n\}$$

où $x_k = \varphi(k)$ pour k compris entre 1 et n (ces x_k sont deux à deux distincts).

Exemple 2.1 L'ensemble vide $\emptyset = \{1, \dots, 0\}$ est de cardinal nul.

Un singleton $\{a\}$ en bijection avec $\{1\}$ est de cardinal 1.

Bien entendu l'ensemble $\{1, \dots, n\}$ est de cardinal n , pour tout entier naturel n .

De manière plus générale, l'ensemble $\{p+1, \dots, p+n\}$ des entiers compris entre $p+1$ et $p+n$, où p est un entier relatif et n un entier naturel est de cardinal n (l'application $k \mapsto k+p$ réalise une bijection de $\{1, \dots, n\}$ sur $\{p+1, \dots, p+n\}$).

Si p, q sont deux entiers relatifs avec $p \leq q$, l'ensemble $\{p, \dots, q\}$ des entiers compris entre p et q , est de cardinal $q - p + 1$.

Avec les deux théorèmes qui suivent, on donne les propriétés essentielles du cardinal d'un ensemble fini.

Théorème 2.2

1. Si E, F sont deux ensembles finis disjoints, alors $E \cup F$ est fini et :

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$$

2. Si F est une partie d'un ensemble fini E , alors :

$$\text{card}(E \setminus F) = \text{card}(E) - \text{card}(F)$$

3. Toute partie F d'un ensemble fini E est finie et $\text{card}(F) \leq \text{card}(E)$. L'égalité est réalisée si, et seulement si, $F = E$.

4. Si E, F sont deux ensembles finis, alors $E \cup F$ est fini et :

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$$

5. Si $(E_k)_{1 \leq k \leq p}$ est une famille finie d'ensembles finis et deux à deux disjoints, alors :

$$\text{card}\left(\bigcup_{k=1}^p E_k\right) = \sum_{k=1}^p \text{card}(E_k)$$

6. Si E, F sont deux ensembles finis, alors le produit cartésien $E \times F$ est fini et :

$$\text{card}(E \times F) = \text{card}(E) \text{card}(F)$$

7. Si $(E_k)_{1 \leq k \leq p}$ est une famille finie d'ensembles finis, alors le produit cartésien $\prod_{k=1}^p E_k$ est fini et :

$$\text{card}\left(\prod_{k=1}^p E_k\right) = \prod_{k=1}^p \text{card}(E_k)$$

Démonstration.

1. On désigne par n le cardinal de E et par m celui de F . On dispose donc d'une bijection f de E sur $E_n = \{1, \dots, n\}$ et d'une bijection g de F sur $E_m = \{1, \dots, m\}$. L'application h définie sur $E \cup F$ par :

$$h(x) = \begin{cases} f(x) & \text{si } x \in E \\ n + g(x) & \text{si } x \in F \end{cases}$$

réalise alors une bijection de $E \cup F$ sur $E_{n+m} = \{1, \dots, n+m\}$. En effet, elle est bien définie puisque E et F sont disjoints et pour tout $k \in E_{n+m}$ il existe un unique $x \in E \cup F$ tel que $k = h(x)$, cet élément étant $x = f^{-1}(k)$ si $1 \leq k \leq n$ ou $x = g^{-1}(k - n)$ si $n + 1 \leq k \leq n + m$. L'ensemble $E \cup F$ est donc fini de cardinal $n + m = \text{card}(E) + \text{card}(F)$.

2. Avec la partition $E = (E \setminus F) \cup F$, on déduit que $\text{card}(E) = \text{card}(F) + \text{card}(E \setminus F)$.
3. De l'égalité précédente, on déduit que $\text{card}(F) \leq \text{card}(E)$.
Supposons que $\text{card}(E) = \text{card}(F)$. Si $F \neq E$, il existe $x \in E \setminus F$ et de l'inclusion $F \cup \{x\} \subset E$ avec $F \cap \{x\} = \emptyset$, on déduit $\text{card}(F) + 1 \leq \text{card}(E)$, ce qui contredit l'égalité $\text{card}(E) = \text{card}(F)$. On a donc $F = E$. La réciproque est évidente.
4. Des partitions :

$$E \cup F = (E \setminus F) \cup F \text{ et } E = (E \setminus F) \cup (E \cap F)$$

on déduit que :

$$\text{card}(E \cup F) = \text{card}(E \setminus F) + \text{card}(F)$$

et :

$$\text{card}(E) = \text{card}(E \setminus F) + \text{card}(E \cap F)$$

ce qui donne $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$.

5. Laissée au lecteur.
6. Laissée au lecteur.
7. Laissée au lecteur.

■

Exercice 2.1 Montrer que si E, F, G sont trois ensembles finis, alors $E \cup F \cup G$ est fini et :

$$\begin{aligned} \text{card}(E \cup F \cup G) &= \text{card}(E) + \text{card}(F) + \text{card}(G) \\ &\quad - \text{card}(E \cap F) - \text{card}(E \cap G) - \text{card}(F \cap G) \\ &\quad + \text{card}(E \cap F \cap G) \end{aligned}$$

Solution 2.1 Laissée au lecteur.

Théorème 2.3 Soient E, F deux ensembles finis non vides et φ une application de E dans F .

1. Si φ est injective, alors $\text{card}(E) \leq \text{card}(F)$.
2. Si φ est surjective, alors $\text{card}(E) \geq \text{card}(F)$.
3. Si φ est bijective, alors $\text{card}(E) = \text{card}(F)$.
4. On a $\text{card}(\varphi(E)) \leq \min(\text{card}(E), \text{card}(F))$ et φ est injective si, et seulement si $\text{card}(\varphi(E)) = \text{card}(E)$, φ est surjective si, et seulement si $\text{card}(\varphi(E)) = \text{card}(F)$.
5. Si E et F sont de même cardinal, alors :

$$\varphi \text{ injective} \Leftrightarrow \varphi \text{ surjective} \Leftrightarrow \varphi \text{ bijective}$$

6. S'il existe un entier naturel non nul p tel que pour tout $y \in F$, $\varphi^{-1}\{y\}$ est de cardinal p , alors φ est surjective et $\text{card}(E) = p \text{card}(F)$ (principe des bergers).

Démonstration. On désigne par n le cardinal de E et par m celui de F . On dispose donc d'une bijection f de $E_n = \{1, \dots, n\}$ sur E et d'une bijection g de $E_m = \{1, \dots, m\}$ sur F .

1. Si $\varphi : E \rightarrow F$ est injective, alors $g^{-1} \circ \varphi \circ f$ est injective de E_n dans E_m et $n \leq m$ (exercice 1.48).
2. Si $\varphi : E \rightarrow F$ est surjective, alors $g^{-1} \circ \varphi \circ f$ est surjective de E_n dans E_m et $n \geq m$ (exercice 1.53).

3. Résulte des deux points précédents.

- (a) Comme $\varphi(E) \subset F$, on a $\text{card}(\varphi(E)) \leq \text{card}(F)$. En notant $\varphi(E) = \{y_1, \dots, y_p\}$ où les y_k , pour k compris entre 1 et p , sont deux à deux distincts, on a la partition $E = \bigcup_{k=1}^p \varphi^{-1}\{y_k\}$ et :

$$\text{card}(E) = \sum_{k=1}^p \text{card}(\varphi^{-1}\{y_k\}) \geq p = \text{card}(\varphi(E))$$

puisque les sont tous non vides.

- (b) Si φ est injective, elle induit alors une bijection de E sur $\varphi(E)$ et $\text{card}(\varphi(E)) = \text{card}(E)$.

Réciproquement si $p = \text{card}(\varphi(E)) = \text{card}(E)$ (notations du 4.a.), les $\varphi^{-1}\{y_k\}$ sont tous de cardinal égal à 1, ce qui signifie que tout élément de $\varphi(E)$ a un unique antécédent dans E , donc φ est bijective de E sur $\varphi(E)$ et injective de E dans F .

- (c) Si φ est surjective, on a alors $\varphi(E) = F$, donc $\text{card}(\varphi(E)) = \text{card}(F)$.

Réciproquement si $\text{card}(\varphi(E)) = \text{card}(F)$, on a $\varphi(E) = F$ et φ est surjective.

4. Si φ est injective, on alors $\text{card}(\varphi(E)) = \text{card}(E) = \text{card}(F)$, donc $\varphi(E) = F$ et φ est surjective.

Si φ est surjective, on a alors $\text{card}(\varphi(E)) = \text{card}(F) = \text{card}(E)$ et φ est injective, donc bijective.

Enfin si φ est bijective, elle injective.

Les trois propositions sont donc bien équivalentes.

5. Si $\varphi^{-1}\{y\}$ est de cardinal $p \geq 1$ pour tout $y \in F$, tous ces ensembles sont non vides et φ est surjective.

En notant $F = \{y_1, \dots, y_m\}$ où les y_k , pour k compris entre 1 et m , sont deux à deux distincts, on a la partition :

$$E = \varphi^{-1}(F) = \varphi^{-1}\left(\bigcup_{k=1}^m \{y_k\}\right) = \bigcup_{k=1}^m \varphi^{-1}\{y_k\}$$

et :

$$\text{card}(E) = \sum_{k=1}^m \text{card}(\varphi^{-1}\{y_k\}) = mp = p \text{card}(F).$$

■

Exercice 2.2 Montrer qu'une partie de \mathbb{N} est finie si, et seulement si, elle est majorée.

Solution 2.2 Si E est une partie majorée de \mathbb{N} , il existe alors un entier n tel que E soit contenue dans $\{1, \dots, n\}$ et E est finie de cardinal au plus égal à n .

Pour la réciproque, on procède par récurrence sur le cardinal.

Un ensemble de cardinal nul est vide et majoré par n'importe quel entier (l'assertion : $\forall x \in \emptyset, x \leq 27$ est vraie).

Supposons le résultat acquis pour les parties de \mathbb{N} de cardinal $n \geq 0$ et soit E une partie de \mathbb{N} de cardinal $n+1$. Pour $p \in E$ (E est non vide puisque de cardinal $n+1 \neq 0$) l'ensemble $E \setminus \{p\}$ est de cardinal n , donc majoré par un entier M et $M' = \max(M, p)$ est un majorant de E .

De cet exercice, on déduit que \mathbb{N} est infini (est-ce une évidence?), donc aussi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C} .

2.2 Ensembles infinis dénombrables

Définition 2.3 On dit qu'un ensemble E est infini dénombrable s'il existe une bijection de E sur \mathbb{N} .

On dira simplement dénombrable pour infini dénombrable.

Si E est un ensemble dénombrable, une bijection $n \mapsto \varphi(n)$ de \mathbb{N} sur E permet de numéroté les éléments de E :

$$E = \{\varphi(0), \varphi(1), \dots, \varphi(n), \dots\}$$

On notera plus simplement, $e_k = \varphi(k)$ où k est un entier naturel, les éléments de E .

Exercice 2.3 Montrer que l'ensemble \mathbb{Z} des entiers relatifs est dénombrable.

Solution 2.3 On peut vérifier que \mathbb{Z} est dénombrable en ordonnant les entiers relatifs comme suit :

$$\mathbb{Z} = \{0, -1, 1, -2, 2, \dots, -k, k, \dots\}$$

ce qui revient à vérifier que l'application :

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow \mathbb{N} \\ n &\mapsto \begin{cases} 2n & \text{si } n \text{ est positif ou nul} \\ -2n - 1 & \text{si } n \text{ est strictement négatif} \end{cases} \end{aligned}$$

est bijective.

Supposons que n, m soient deux entiers relatifs tels que $\varphi(n) = \varphi(m)$. Si $n \geq 0$ et $m < 0$, on a alors $2n = -2m - 1$, soit $2(n + m) = 1$ dans \mathbb{Z} , ce qui est impossible. De même $n < 0$ et $m \geq 0$ est impossible. On a donc soit $n \geq 0, m \geq 0$, donc $2n = 2m$ et $n = m$, soit $n < 0, m < 0$, donc $-2n - 1 = -2m - 1$ et $n = m$. L'application φ est donc injective.

Si k est un entier naturel, il est soit pair, donc $k = 2n = \varphi(n)$ avec $n \in \mathbb{N}$, soit impair, donc $k = 2(-n) - 1 = \varphi(n)$ avec $n \in \mathbb{Z}^*$. L'application φ est donc surjective.

On peut montrer de plusieurs façons que l'ensemble \mathbb{N}^2 est dénombrable.

Exercice 2.4 Montrer que l'application $\varphi : (n, m) \mapsto 2^n(2m + 1) - 1$ est bijective de \mathbb{N}^2 sur \mathbb{N} .

Solution 2.4 L'égalité $\varphi(n, m) = \varphi(n', m')$ avec (n, m) et (n', m') dans \mathbb{N}^2 équivaut à $2^n(2m + 1) = 2^{n'}(2m' + 1)$. Si $n > n'$, on a alors $2^{n-n'}(2m + 1) = 2m' + 1$ qui est à la fois pair et impair, ce qui est impossible. De manière analogue, on voit que $n' > n$ est impossible. On a donc $n = n'$ et $2m + 1 = 2m' + 1$, ce qui équivaut à $m = m'$. L'application φ est donc injective.

Soit $r \in \mathbb{N}$. Si $r = 0$, on a alors $r = \varphi(0, 0)$. Si $n \in \mathbb{N}^*$, alors $n + 1 \geq 2$ et cet entier se décompose en facteurs premiers, ce qui s'écrit $r + 1 = 2^n(2m + 1)$ avec (n, m) dans \mathbb{N}^2 . L'application φ est donc surjective et en définitive bijective.

Exercice 2.5 Montrer que l'application $\varphi : (n, m) \mapsto \frac{1}{2}(n + m)(n + m + 1) + m$ est bijective de \mathbb{N}^2 sur \mathbb{N} .

Solution 2.5 On remarque d'abord que pour tout $(n, m) \in \mathbb{N}^2$, les entiers $n + m$ et $n + m + 1$ sont de parités différentes, donc $\frac{1}{2}(n + m)(n + m + 1)$ est entier et φ est bien à valeurs dans \mathbb{N} .

Supposons que $\varphi(n, m) = \varphi(n', m')$ avec (n, m) et (n', m') dans \mathbb{N}^2 . En notant $N = n + m$ et $M = n' + m'$, on a $M \geq m'$ et :

$$\frac{N(N+1)}{2} \leq \varphi(n, m) = \varphi(n', m') \leq \frac{M(M+1)}{2} + M$$

ce qui entraîne

$$M^2 + 3M = \left(M + \frac{3}{2}\right)^2 - \frac{9}{4} \geq N^2 + N = \left(N + \frac{1}{2}\right)^2 - \frac{1}{4}$$

soit :

$$(2M + 3)^2 - 9 \geq (2N + 1)^2 - 1$$

ou encore :

$$(2M + 3)^2 - (2N + 1)^2 = (2(M + N) + 4)(2(M - N) + 2) \geq 8$$

c'est-à-dire :

$$(M + N + 2)(M - N + 1) \geq 2$$

et nécessairement $M \geq N$. Comme M et N jouent des rôles symétriques, on a aussi $M \leq N$ et $M = N$. De $\varphi(n, m) = \varphi(n', m')$, on déduit alors que $m = m'$ puis $n = n'$. L'application φ est donc injective.

2.3 Arrangements et permutations

2.4 Combinaisons

2.5 Problèmes de tirage

2.6 Nombres de surjections entre ensembles finis

2.7 Le problème des rencontres

3

Relations d'ordre et d'équivalence

L'ensemble \mathbb{N} des entiers naturels

L'ensemble \mathbb{N} des entiers naturels peut être construit à partir de la notion de cardinal dans le cadre de la théorie des ensembles.

L'ensemble \mathbb{Z} des entiers relatifs

Après avoir étudié la théorie des groupes, on construit à partir de l'ensemble \mathbb{N} des entiers naturels l'anneau \mathbb{Z} des entiers relatifs par un procédé de symétrisation.

6

L'ensemble \mathbb{Q} des nombres rationnels

Le corps \mathbb{Q} des nombres rationnels est construit comme le corps des fractions de \mathbb{Z} .

Le corps \mathbb{C} des nombres complexes

Les ensembles \mathbb{Z} d'entiers relatifs et \mathbb{Q} de nombres rationnels peuvent être construits à partir de problèmes analogues. Pour l'ensemble \mathbb{Z} il s'agit des équations $x + a = 0$ qui n'ont pas de solution dans \mathbb{N} pour a entier naturel non nul et pour l'ensemble \mathbb{Q} il s'agit des équations $ax = 1$ qui n'ont pas de solution dans \mathbb{Z} pour a entier relatif différent de $-1, 0$ et 1 . Le passage de l'ensemble \mathbb{Q} de nombres rationnels à l'ensemble \mathbb{R} de nombres réels est plus délicat. Les problèmes sont de nature algébrique (par exemple l'équation $x^2 = 2$ n'a pas de solution dans \mathbb{Q}) mais aussi de nature topologique : l'existence de borne supérieure pour les ensembles non vides et majorés n'est pas assurée dans \mathbb{Q} alors qu'elle l'est dans \mathbb{R} (par exemple l'ensemble $A = \{r \in \mathbb{Q} \mid r^2 \leq 2\}$ n'a pas de borne supérieure dans \mathbb{Q}). On consultera le cours d'analyse pour de plus amples détails sur la construction de l'ensemble \mathbb{R} des nombres réels.

La construction de l'ensemble des nombres complexes est motivée par le fait que certaines équations polynomiales telles que l'équation $x^2 + 1 = 0$ n'ont pas de solutions réelles.

Le but de ce chapitre est de construire un ensemble que nous noterons \mathbb{C} qui contient \mathbb{R} et qui est muni d'opérations d'addition et de multiplication ayant les mêmes propriétés que leurs analogues sur \mathbb{R} , ce qui se traduira en disant que \mathbb{C} est un corps commutatif. De plus dans cet ensemble \mathbb{C} toute équation algébrique $P(x) = 0$, où P est un polynôme non constant, a des solutions, ce qui se traduira en disant que \mathbb{C} est algébriquement clos. Dans un premier temps, on se contentera de décrire les solutions des équations de degré 2, $x^2 + bx + c = 0$. Pour les équations de degré supérieur, on dispose du théorème de d'Alembert-Gauss dit théorème fondamental de l'algèbre dont la démonstration classique nécessite des outils d'analyse réelle tels que le fait qu'une fonction continue sur un compact de \mathbb{C} est bornée et atteint ses bornes (voir le cours d'analyse et le problème du paragraphe 27). Nous verrons aussi que contrairement à \mathbb{R} , l'ensemble \mathbb{C} que nous aurons construit ne peut pas être muni d'une relation d'ordre compatible avec la multiplication, c'est-à-dire telle que si $x \leq y$ et $0 \leq z$, alors $x \cdot z \leq y \cdot z$.

7.1 Conditions nécessaires à la construction de \mathbb{C}

Supposons que nous ayons construit un ensemble \mathbb{C} contenant \mathbb{R} muni d'opérations d'addition et multiplication qui prolongent celles que nous connaissons sur les réels avec les mêmes propriétés (mises à part celle relatives à la relation d'ordre \leq sur \mathbb{R}) et tel que l'équation $x^2 + 1 = 0$ admette au moins une solution i dans \mathbb{C} .

Pour tous réels x, y , le nombre $z = x + iy$ sera alors dans \mathbb{C} et l'égalité $z = 0$ est réalisée si, et seulement si, $x = y = 0$. En effet, si $y = 0$, alors $x = 0$ et si $y \neq 0$, alors $i = -\frac{x}{y}$ est réel, ce qui n'est pas possible puisque l'équation $x^2 + 1 = 0$ n'a pas de solution réelle. Il en résulte que pour x, x', y, y' réels l'égalité $x + iy = x' + iy'$ est réalisée si, et seulement si, $x = x'$ et $y = y'$.

De plus pour l'addition et la multiplication de deux éléments $z = x + iy$ et $z' = x' + iy'$ de \mathbb{C} , on doit avoir :

$$\begin{cases} z + z' = (x + x') + i(y + y') \\ zz' = (xx' - yy') + i(xy' + yx') \end{cases}$$

7.2 Construction de \mathbb{C}

Les considérations précédentes nous conduisent à définir sur l'ensemble \mathbb{R}^2 des couples de réels les opérations d'addition et de multiplication suivantes, où $z = (x, y)$ et $z' = (x', y')$ sont deux éléments quelconques de \mathbb{R}^2 :

$$\begin{cases} z + z' = (x + x', y + y') \\ z \cdot z' = (xx' - yy', xy' + yx') \end{cases}$$

On notera \mathbb{C} l'ensemble \mathbb{R}^2 muni de ces deux opérations (ou lois de composition interne) et on l'appelle ensemble des nombres complexes.

La multiplication de deux nombres complexes z et z' sera notée $z \cdot z'$ ou plus simplement zz' .

L'égalité de deux nombres complexes $z = (x, y)$ et $z' = (x', y')$ est réalisée si, et seulement si, on a les égalités $x = x'$ et $y = y'$ (c'est ce qui se passe dans tout produit cartésien $E \times F$).

En particulier, pour $y = y' = 0$, on a $(x, 0) = (x', 0)$ si, et seulement si $x = x'$, ce qui signifie que l'application :

$$\begin{aligned} \mathbb{R} &\rightarrow \mathbb{C} \\ x &\mapsto (x, 0) \end{aligned}$$

est injective, ce qui permet de réaliser une bijection de \mathbb{R} sur le sous ensemble \mathbb{R}' de \mathbb{C} formé des couples $(x, 0)$. Cette bijection permet d'identifier \mathbb{R} à \mathbb{R}' , ce qui signifie qu'un nombre réel x est identifié à son image $(x, 0)$ dans \mathbb{C} . Cette identification $x = (x, 0)$ est bien compatible avec les opérations d'addition et de multiplication des réels dans le sens où :

$$\begin{cases} x + x' = (x, 0) + (x', 0) = (x + x', 0) = x + x' \\ xx' = (x, 0)(x', 0) = (xx', 0) = xx' \end{cases}$$

L'opération d'addition vérifie les propriétés suivantes, déduites des propriétés analogues sur \mathbb{R} :

- elle est commutative, c'est-à-dire que pour tous nombres complexes $z = (x, y)$ et $z' = (x', y')$, on a :

$$z + z' = (x + x', y + y') = (x' + x, y' + y) = z' + z$$

- elle est associative, c'est-à-dire que pour tous nombres complexes $z = (x, y)$, $z' = (x', y')$ et $z'' = (x'', y'')$, on a :

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

- le réel $0 = (0, 0)$ est un élément neutre, c'est-à-dire que pour tout nombre complexe $z = (x, y)$, on a :

$$z + 0 = 0 + z = z$$

- tout nombre complexe $z = (x, y)$ admet un opposé donné par $z' = (-x, -y)$, ce qui signifie que :

$$z + z' = z' + z = 0$$

On note $-z$ cet opposé.

Tout cela se traduit en disant que $(\mathbb{C}, +)$ est un groupe commutatif comme $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ et $(\mathbb{Z}, +)$.

La notion de groupe est étudiée plus en détails au chapitre 20.

Comme pour n'importe quel groupe, on peut vérifier que :

- l'élément neutre est unique ;
- pour tout $z \in \mathbb{C}$, l'opposé est unique ;
- tout élément de \mathbb{C} est simplifiable (ou régulier) pour l'addition, c'est-à-dire que si $z + z' = z + z''$, alors $z' = z''$.

Pour ce qui est de l'autre opération de multiplication, on a les propriétés suivantes, encore déduites des propriétés analogues sur \mathbb{R} :

- elle est commutative, c'est-à-dire que pour tous nombres complexes $z = (x, y)$ et $z' = (x', y')$, on a :

$$zz' = (xx' - yy', xy' + yx') = (x'x - y'y, y'x + x'y) = z'z$$

- elle est associative, c'est-à-dire que pour tous nombres complexes $z = (x, y)$, $z' = (x', y')$ et $z'' = (x'', y'')$, on a $z(z'z'') = (zz')z''$. En effet, on a :

$$\begin{aligned} z(z'z'') &= (x, y)(x'x'' - y'y'', x'y'' + y'x'') \\ &= (x(x'x'' - y'y'') - y(x'y'' + y'x''), x(x'y'' + y'x'') + y(x'x'' - y'y'')) \\ &= (xx'x'' - xy'y'' - yx'y'' - yy'x'', xx'y'' + xy'x'' + yx'x'' - yy'y'') \end{aligned}$$

et :

$$\begin{aligned} (zz')z'' &= (xx' - yy', xy' + yx')(x'', y'') \\ &= ((xx' - yy')x'' - (xy' + yx')y'', (xx' - yy')y'' + (xy' + yx')x'') \\ &= (xx'x'' - xy'y'' - yx'y'' - yy'x'', xx'y'' + xy'x'' + yx'x'' - yy'y'') \\ &= z(z'z'') \end{aligned}$$

On peut remarquer que seule la commutativité de l'addition des réels a été utilisée ici.

- elle est distributive par rapport à l'addition, c'est-à-dire que pour tous nombres complexes z , z' et z'' , on a $z(z' + z'') = zz' + zz''$, ce qui se vérifie encore sans problème.
- le réel $1 = (1, 0)$ est un élément neutre, c'est-à-dire que pour tout nombre complexe $z = (x, y)$, on a :

$$z \cdot 1 = 1 \cdot z = z$$

- tout nombre complexe $z = (x, y)$ différent de 0 admet un inverse donné par :

$$z' = \left(\frac{x}{x^2 + y^2}, -\frac{y}{x^2 + y^2} \right),$$

ce qui signifie que $zz' = z'z = 1$. En effet l'égalité $zz' = 1$ équivaut à :

$$\begin{cases} xx' - yy' = 1 \\ xy' + yx' = 0 \end{cases}$$

ce qui entraîne :

$$\begin{cases} x^2x' - xyy' = x \\ yxy' + y^2x' = 0 \end{cases} \quad \text{et} \quad \begin{cases} yxx' - y^2y' = y \\ x^2y' + xyx' = 0 \end{cases}$$

et en additionnant les deux premières égalités [resp. en soustrayant les deux dernières], on obtient $(x^2 + y^2)x' = x$, $(x^2 + y^2)y' = -y$, ce qui donne compte tenu de $x^2 + y^2 \neq 0$ pour $z \neq 0$, $x' = \frac{x}{x^2 + y^2}$ et $y' = -\frac{y}{x^2 + y^2}$. Réciproquement, on vérifie facilement que cette solution convient. On note z^{-1} ou $\frac{1}{z}$ cet inverse.

On peut remarquer qu'on a utilisé ici la commutativité du produit des réels.

Tout cela se traduit en disant que $(\mathbb{C}, +, \cdot)$ est un corps commutatif comme $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$.

La notion de corps est étudiée plus en détails au chapitre suivant.

Là encore le neutre et l'inverse sont uniques et tout nombre complexe non nul est simplifiable pour le produit.

On note $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ et ce qui précède nous dit que (\mathbb{C}^*, \cdot) est un groupe commutatif.

On peut remarquer que pour tout réel non nul x , on a bien :

$$\frac{1}{x} = \left(\frac{1}{x}, 0 \right) = \frac{1}{(x, 0)}$$

Ces opérations d'addition et multiplication prolongent bien celles de \mathbb{R} .

L'associativité de la multiplication permet de définir les puissances n -ièmes d'un nombre complexe z par :

$$\begin{cases} z^0 = 1 \\ \forall n \in \mathbb{N}^*, z^{n+1} = z^n \cdot z \end{cases}$$

Pour $z \neq 0$ et $n \in \mathbb{N}^*$, on a $z^n \neq 0$ et :

$$(z^n)^{-1} = \frac{1}{z^n} = (z^{-1})^n$$

On note alors $z^{-n} = \frac{1}{z^n}$.

Comme sur \mathbb{R} , on a $z^{p+q} = z^p z^q$ et $(z^p)^q = z^{pq}$ pour tous entiers relatifs p et q .

Comme sur \mathbb{R} , une égalité $zz' = 0$ équivaut à $z = 0$ ou $z' = 0$. En effet si $z \neq 0$, il admet un inverse et $0 = z^{-1} \cdot 0 = z^{-1}zz' = z'$.

En posant $i = (0, 1)$, on a :

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1$$

De cette égalité, on déduit que $\frac{1}{i} = -i$.

Le nombre complexe $-i$ est aussi solution de l'équation $x^2 + 1 = 0$ et $i, -i$ sont les seules solutions de cette équation. En effet si $\alpha^2 + 1 = 0$, on a $\alpha^2 = -1 = i^2$ et $\alpha^2 - i^2 = (\alpha - i)(\alpha + i) = 0$ de sorte que $\alpha = i$ ou $\alpha = -i$.

Théorème 7.1 *Tout nombre complexe s'écrit de manière unique $z = x + iy$, où x et y sont deux réels.*

Démonstration. Un nombre complexe s'écrit de manière unique :

$$\begin{aligned} z &= (x, y) = (x, 0) + (0, y) \\ &= (x, 0)(1, 0) + (y, 0)(0, 1) \\ &= x \cdot 1 + y \cdot i = x + iy \end{aligned}$$

■

Définition 7.1 Avec les notations du théorème qui précède, on dit que x est la partie réelle de z et y sa partie imaginaire, ce qui se note $x = \Re(z)$ et $y = \Im(z)$.

Définition 7.2 On dit qu'un nombre complexe est un imaginaire pur si sa partie réelle est nulle.

En résumé un nombre complexe s'écrit $z = x + iy$ où $i^2 = -1$ et pour $z = x + iy$, $z' = x' + iy'$ dans \mathbb{C} , on a :

$$\begin{cases} z = z' \Leftrightarrow x = x' \text{ et } y = y' \\ z \in \mathbb{R} \Leftrightarrow y = \Im(z) = 0 \\ z + z' = (x + x') + i(y + y') \\ zz' = (xx' - yy') + i(xy' + x'y) \\ \frac{1}{z} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}i \text{ si } z \neq 0 \end{cases}$$

Exercice 7.1 Écrire sous la forme $x + iy$ les nombres complexes suivants :

$$u = \left(\frac{\sqrt{3} - i}{1 + i\sqrt{3}} \right)^{27}, \left(\frac{\sqrt{3} + i}{\sqrt{3} - i} + \frac{\sqrt{3} - i}{\sqrt{3} + i} - 1 \right)^{111}, w = \frac{(1 + i\sqrt{3})^4}{(1 + i)^3}.$$

Solution 7.1 On a $\frac{\sqrt{3} - i}{1 + i\sqrt{3}} = \frac{\sqrt{3} - i}{i(\sqrt{3} - i)} = \frac{1}{i} = -i$ et $u = -i^{27} = -(i^4)^7 \frac{1}{i} = i$.

On a

$$\begin{aligned} \frac{\sqrt{3} + i}{\sqrt{3} - i} + \frac{\sqrt{3} - i}{\sqrt{3} + i} &= \frac{(\sqrt{3} + i)^2 + (\sqrt{3} - i)^2}{3 - i^2} \\ &= \frac{2(3 + i^2)}{3 - i^2} = 1 \end{aligned}$$

et $z = 0$.

On a :

$$(1 + i\sqrt{3})^4 = -8(1 + i\sqrt{3}) \text{ et } (1 + i)^3 = -2(1 - i)$$

et :

$$w = 4 \frac{1 + i\sqrt{3}}{1 - i} = 4 \frac{(1 + i\sqrt{3})(1 + i)}{(1 - i)(1 + i)} = 2(1 - \sqrt{3}) + 2i(1 + \sqrt{3})$$

Exercice 7.2 Calculer i^n pour tout entier relatif n .

Solution 7.2 Pour $n = 0$, on a $i^0 = 1$.

Tout entier relatif s'écrit $n = 4q + r$ avec $r = 0, 1, 2$ ou 3 et :

$$i^n = (i^4)^q i^r = i^r = \begin{cases} 1 & \text{si } r = 0 \\ i & \text{si } r = 1 \\ -1 & \text{si } r = 2 \\ -i & \text{si } r = 3 \end{cases}$$

Exercice 7.3 Montrer qu'il n'existe pas de relation d'ordre sur \mathbb{C} qui prolonge la relation \leq de \mathbb{R} et qui soit compatible avec la somme et le produit, c'est à dire telle que $a \leq b$ et $c \leq d$ entraîne $a + c \leq b + d$ et $a \leq b$ et $0 \leq c$ entraîne $ac \leq bc$.

Solution 7.3 Supposant qu'une telle relation existe. Si $0 \leq i$ [resp. $0 \leq -i$], alors $0 \leq i^2 \leq -1$ [resp. $0 \leq (-i)^2 = (-1)^2 i^2 = -1$] dans \mathbb{R} , ce qui est incompatible avec la relation d'ordre sur \mathbb{R} .

Exercice 7.4 Soit $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Calculer j^2 , j^3 , $1 + j + j^2$ et j^n pour tout entier relatif n .

Solution 7.4 On a $j^0 = 1$, $j^1 = j$, $j^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $j^3 = 1$ et $1 + j + j^2 = 0$. En écrivant n sous la forme $n = 3q + r$ avec $r = 0, 1$ ou 2 , on a :

$$j^n = j^r = \begin{cases} 1 & \text{si } r = 0 \\ j & \text{si } r = 1 \\ j^2 & \text{si } r = 2 \end{cases}$$

Exercice 7.5 Calculer $(1+i)^2$, $(1+i)^6$ et $(1+i)^7$. En utilisant la formule du binôme de Newton, en déduire les valeurs de $1 - C_7^2 + C_7^4 - C_7^6$ et $C_7^1 - C_7^3 + C_7^5 - 1$.

Solution 7.5 On a :

$$(1+i)^2 = 1 + 2i + i^2 = 2i$$

donc :

$$(1+i)^6 = (2i)^3 = -8i$$

et :

$$(1+i)^7 = -8i(1+i) = 8 - 8i.$$

En utilisant la formule du binôme de Newton, on a aussi :

$$(1+i)^7 = \sum_{k=0}^7 C_7^k i^k = (1 - C_7^2 + C_7^4 - C_7^6) + (C_7^1 - C_7^3 + C_7^5 - 1) i$$

ce qui nous donne $1 - C_7^2 + C_7^4 - C_7^6 = 8$ et $C_7^1 - C_7^3 + C_7^5 - 1 = -8$.

Exercice 7.6 Calculer $(1+i)^n$ pour tout entier naturel n . En déduire les valeurs des sommes $\sum_{j=0}^p C_{2p}^{2j} (-1)^j$ et $\sum_{j=0}^{p-1} C_{2p}^{2j+1} (-1)^j$ pour tout entier naturel non nul p .

Solution 7.6 On a $(1+i)^2 = 2i$, donc $(1+i)^{2p} = 2^p i^p$ pour tout $p \geq 0$ et on connaît les i^p . Pour les entiers impairs, on a :

$$(1+i)^{2p+1} = 2^p (1+i) i^p = 2^p (i^p + i^{p+1}).$$

On a donc :

$$(1+i)^{2p} = 2^p i^p = \begin{cases} 2^p & \text{si } p = 4q \\ 2^p i & \text{si } p = 4q + 1 \\ -2^p & \text{si } p = 4q + 2 \\ -2^p i & \text{si } p = 4q + 3 \end{cases}$$

et :

$$(1+i)^{2p+1} = 2^p (i^p + i^{p+1}) = \begin{cases} 2^p (1+i) & \text{si } p = 4q \\ 2^p (-1+i) & \text{si } p = 4q + 1 \\ -2^p (1+i) & \text{si } p = 4q + 2 \\ 2^p (1-i) & \text{si } p = 4q + 3 \end{cases}$$

En utilisant la formule du binôme de Newton, on a :

$$\begin{aligned}(1+i)^{2p} &= \sum_{k=0}^{2p} C_{2p}^k i^k = \sum_{j=0}^p C_{2p}^{2j} i^{2j} + \sum_{j=0}^{p-1} C_{2p}^{2j+1} i^{2j+1} \\ &= \sum_{j=0}^p C_{2p}^{2j} (-1)^j + i \sum_{j=0}^{p-1} C_{2p}^{2j+1} (-1)^j\end{aligned}$$

En identifiant les parties réelles et imaginaires, on en déduit que :

$$\begin{aligned}\sum_{j=0}^{4q} C_{8q}^{2j} (-1)^j &= 2^{4q} \text{ et } \sum_{j=0}^{4q-1} C_{8q}^{2j+1} (-1)^j = 0 \\ \sum_{j=0}^{4q+1} C_{8q+2}^{2j} (-1)^j &= 0 \text{ et } \sum_{j=0}^{4q} C_{8q+2}^{2j+1} (-1)^j = 2^{4q+1} \\ \sum_{j=0}^{4q+2} C_{8q+4}^{2j} (-1)^j &= -2^{4q+2} \text{ et } \sum_{j=0}^{4q+1} C_{8q+4}^{2j+1} (-1)^j = 0 \\ \sum_{j=0}^{4q+3} C_{8q+6}^{2j} (-1)^j &= 0 \text{ et } \sum_{j=0}^{4q+2} C_{8q+6}^{2j+1} (-1)^j = -2^{4q+3}\end{aligned}$$

Par exemple :

$$\sum_{j=0}^4 C_8^{2j} (-1)^j = C_8^4 - C_8^2 - C_8^6 + C_8^8 + 1 = 2^4 = 16$$

et :

$$\sum_{j=0}^3 C_8^{2j+1} (-1)^j = C_8^1 - C_8^3 + C_8^5 - C_8^7 = 0$$

7.3 Conjugué et module d'un nombre complexe

Définition 7.3 Le conjugué du nombre complexe $z = x + iy$ est le nombre complexe $\bar{z} = x - iy$.

On déduit immédiatement de cette définition les propriétés suivantes du conjugué.

Théorème 7.2 Pour tous nombres complexes z et z' , on a :

1. $\overline{\bar{z}} = z$.
2. $\overline{z + z'} = \bar{z} + \bar{z}'$.
3. $\overline{zz'} = \bar{z}\bar{z}'$.
4. $z + \bar{z} = 2\Re(z)$.
5. $z - \bar{z} = 2i\Im(z)$.
6. $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$.
7. z est imaginaire pur si, et seulement si, $\bar{z} = -z$.
8. $z\bar{z} = (\Re(z))^2 + (\Im(z))^2 \in \mathbb{R}^+$.

Le dernier point du théorème précédent nous permet de donner la définition suivante.

Définition 7.4 *Le module du nombre complexe $z = x + iy$ est le réel :*

$$|z| = \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$$

Dans le cas où z est réel, $|z|$ est la valeur absolue de z .

On vérifie facilement les propriétés suivantes liées au module.

Théorème 7.3 *Pour tous nombres complexes z et z' , on a :*

1. $|z| \geq 0$ et $|z| = 0$ si, et seulement si, $z = 0$;
2. $|z| = |\bar{z}|$;
3. $|zz'| = |z| |z'|$;
4. pour toute suite finie z_1, \dots, z_n de nombres complexes, on a :

$$\left| \prod_{k=1}^n z_k \right| = \prod_{k=1}^n |z_k|$$

5. si $z \neq 0$, alors $\frac{1}{z} = \frac{\bar{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}$;
6. si $z' \neq 0$, alors $\left| \frac{z}{z'} \right| = \frac{|z|}{|z'|}$;
7. $|z| = 1$ si, et seulement si, $\frac{1}{z} = \bar{z}$;
8. $|\Re(z)| \leq |z|$ et l'égalité est réalisée si, et seulement si, z est réel ;
9. $|\Im(z)| \leq |z|$ et l'égalité est réalisée si, et seulement si, z est imaginaire pur.

Du point 4. on déduit que pour tout nombre complexe z et tout entier naturel n , on a $|z^n| = |z|^n$. Cette égalité étant encore valable pour n entier relatif et z non nul.

Du point 8. on déduira l'inégalité de Cauchy-Schwarz avec son cas d'égalité.

Exercice 7.7 *Montrer que le produit de deux entiers naturels qui sont somme de deux carrés d'entiers est encore somme de deux carrés d'entiers.*

Solution 7.7 Soient $n = a^2 + b^2$ et $m = c^2 + d^2$ où a, b, c, d sont des entiers relatifs. En écrivant que $n = |u|^2$ et $m = |v|^2$ où, $u = a + ib$ et $v = c + id$, on a :

$$\begin{aligned} nm &= |uv|^2 = |(ac - bd) + (ad + bc)i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

(identité de Lagrange), c'est-à-dire que nm est somme de deux carrés d'entiers.

En utilisant la décomposition des entiers en facteurs premiers, le résultat de l'exercice précédent est utilisé pour caractériser les entiers qui sont sommes de deux carrés.

Comme pour la valeur absolue réelle, on dispose de l'inégalité triangulaire. Cette inégalité est conséquence des résultats suivants.

Théorème 7.4 *Pour tous nombres complexes z et z' , on a :*

$$|z + z'|^2 = |z|^2 + 2\Re(z\bar{z}') + |z'|^2$$

Démonstration. Il suffit d'écrire, pour $z = x + iy$, $z' = x' + iy'$:

$$\begin{aligned} |z + z'|^2 &= (x + x')^2 + (y + y')^2 \\ &= x^2 + y^2 + 2(xx' + yy') + x'^2 + y'^2 \\ &= |z|^2 + 2\Re(z\overline{z'}) + |z'|^2. \end{aligned}$$

■

Théorème 7.5 (inégalité de Cauchy-Schwarz) *Pour tous nombres complexes z et z' , on a :*

$$|\Re(z\overline{z'})| \leq |z| |z'|$$

l'égalité étant réalisée si, et seulement si, z et z' sont liées sur \mathbb{R} (i. e. $z' = 0$ ou $z \neq 0$ et $\frac{z}{z'} \in \mathbb{R}$), ce qui est encore équivalent à dire que $z\overline{z'}$ est réel.

Démonstration. On a :

$$|\Re(z\overline{z'})| \leq |z\overline{z'}| = |z| |z'|$$

et l'égalité est réalisée si, et seulement si, $z\overline{z'}$ est réel. Pour $z' = 0$, c'est le cas et pour $z' \neq 0$, il existe un réel $\lambda \in \mathbb{R}$ tel que $z = \lambda \frac{1}{\overline{z'}} = \frac{\lambda}{|z'|^2} z'$.

La réciproque est évidente.

■

Théorème 7.6 *Pour tous nombres complexes z et z' , on a :*

$$|z + z'| \leq |z| + |z'|$$

l'égalité étant réalisée si, et seulement si, z et z' sont positivement liées sur \mathbb{R} (i. e. $z = 0$ ou $z \neq 0$ et $\frac{z}{z'} \in \mathbb{R}^+$), ce qui est encore équivalent à dire que $z\overline{z'} \in \mathbb{R}^+$.

Démonstration. On a :

$$\begin{aligned} |z + z'|^2 &= |z|^2 + 2\Re(z\overline{z'}) + |z'|^2 \\ &\leq |z|^2 + 2|z||z'| + |z'|^2 = (|z| + |z'|)^2 \end{aligned}$$

ce qui équivaut à $|z + z'| \leq |z| + |z'|$. L'égalité est réalisée si, et seulement si $\Re(z\overline{z'}) = |z||z'|$, ce qui implique $|\Re(z\overline{z'})| = |z||z'|$ et z, z' sont liées sur \mathbb{R} . Pour $z' \neq 0$, on a $z = \lambda z'$ avec $\lambda \in \mathbb{R}$ et $\Re(z\overline{z'}) = \lambda |z'|^2 = |z||z'|$ impose $\lambda \geq 0$.

La réciproque est évidente.

■

Corollaire 7.1 *Pour tous nombres complexes z et z' , on a :*

$$||z| - |z'||| \leq |z - z'| \leq |z| + |z'|$$

Démonstration. Il suffit d'écrire que :

$$|z| \leq |z - z'| + |z'|$$

et :

$$|z'| \leq |z - z'| + |z|$$

■

Pour ce qui est du module d'une somme de nombres complexes, on a de manière plus générale le résultat suivant qui se montre facilement par récurrence.

Théorème 7.7 Pour toute suite finie z_1, \dots, z_n de nombres complexes non nuls avec $n \geq 2$, on a :

$$\left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$$

l'égalité étant réalisée si, et seulement si, il existe des réels $\lambda_2, \dots, \lambda_n$ tels que $z_k = \lambda_k z_1$ pour $k = 2, \dots, n$.

Démonstration. On procède par récurrence sur $n \geq 2$. Pour $n = 2$, c'est connu.

Supposons le résultat acquis au rang $n - 1 \geq 2$.

Pour z_1, \dots, z_n dans \mathbb{C} avec $n \geq 3$, en utilisant les résultats pour $n = 2$ et l'hypothèse de récurrence, on a :

$$\left| \sum_{k=1}^n z_k \right| = \left| z_1 + \sum_{k=2}^n z_k \right| \leq |z_1| + \left| \sum_{k=2}^n z_k \right| \leq \sum_{k=1}^n |z_k|.$$

Si l'égalité $\left| \sum_{k=1}^n z_k \right| = \sum_{k=1}^n |z_k|$ est réalisée, en posant $Z_2 = \sum_{k=2}^n z_k$, on a :

$$\left| \sum_{k=1}^n z_k \right| = |z_1 + Z_2| \leq |z_1| + |Z_2| \leq \sum_{k=1}^n |z_k|$$

et l'égalité $\left| \sum_{k=1}^n z_k \right| = \sum_{k=1}^n |z_k|$ nous dit que toutes les inégalités précédentes sont des égalités.

On a donc $|z_1 + Z_2| = |z_1| + |Z_2|$ et $Z_2 = \lambda_1 z_1$ avec $\lambda_1 \in \mathbb{R}^{+,*}$ ($Z_2 = 0$ entraîne $|z_1| = \sum_{k=1}^n |z_k|$,

donc $\sum_{k=2}^n |z_k| = 0$ et tous les z_k sont nuls, ce qui est contraire à l'hypothèse de départ), puis de

$|z_1| + |Z_2| = \sum_{k=1}^n |z_k|$, on déduit que $|Z_2| = \sum_{k=2}^n |z_k|$ et avec l'hypothèse de récurrence qu'il existe des réels $\lambda_k > 0$ tels que $z_k = \lambda_k z_2$ pour $k = 3, \dots, n$. On a alors :

$$Z_2 = \sum_{k=2}^n z_k = \left(1 + \sum_{k=3}^n \lambda_k \right) z_2 = \lambda_1 z_1$$

et $z_2 = \mu_2 z_1$, $z_k = \lambda_k z_2 = \mu_k z_1$ pour $k = 3, \dots, n$, tous les μ_k étant strictement positifs. ■

Exercice 7.8 Montrer que si z est un nombre complexe de module égal à 1, alors $u = i \frac{1+z}{1-z}$ est réel.

Solution 7.8 Comme z est de module 1, on a $\bar{z} = \frac{1}{z}$ et :

$$\bar{u} = -i \frac{1+\bar{z}}{1-\bar{z}} = -i \frac{1+\frac{1}{z}}{1-\frac{1}{z}} = -i \frac{z+1}{z-1} = u,$$

ce qui prouve que u est réel.

Exercice 7.9 Montrer que si z et z' sont deux nombres complexes de module égal à 1 tels que $zz' \neq -1$, alors $u = \frac{z+z'}{1+zz'}$ est réel.

Solution 7.9 Comme z et z' sont de module 1, on a :

$$\bar{u} = \frac{\bar{z} + \bar{z}'}{1 + \bar{z}z'} = \frac{\frac{1}{z} + \frac{1}{z'}}{1 + \frac{1}{zz'}} = \frac{z + z'}{1 + zz'} = u,$$

ce qui prouve que u est réel.

Exercice 7.10 Soient z, z' deux nombres complexes avec $z' \neq -1$. À quelle condition le nombre complexe $u = \frac{z + z'\bar{z}}{1 + z'}$ est-il réel ?

Solution 7.10 Dire que u est réel équivaut à dire que :

$$\bar{u} = \frac{\bar{z} + \bar{z}'z}{1 + \bar{z}'} = \frac{z + z'\bar{z}}{1 + z'}$$

ce qui est encore équivalent à :

$$(\bar{z} + \bar{z}'z)(1 + z') = (z + z'\bar{z})(1 + \bar{z}')$$

ou encore à :

$$\bar{z} + z'\bar{z}'z = z + z'\bar{z}'\bar{z}$$

soit à :

$$\bar{z}(1 - |z'|^2) = z(1 - |z'|^2).$$

En définitive, u est réel si, et seulement si, $|z'| = 1$ avec $z' \neq -1$ ou $z = \bar{z}$, ce qui signifie que z est réel.

Exercice 7.11 Soient z_1, \dots, z_n des nombres complexes non nuls deux à deux distincts et tels que $\sum_{k=1}^n z_k = 0$. Montrer qu'il existe deux indices $j \neq k$ compris entre 1 et n tels que $1 \leq \frac{|z_j|}{|z_k|} \leq 2$.

Solution 7.11 Quitte à réordonner, on peut supposer que :

$$|z_1| \leq \dots \leq |z_n|$$

En supposant que le résultat annoncé est faux, on a $\frac{|z_k|}{|z_{k-1}|} \notin [1, 2]$ pour tout k compris entre 2 et n et comme $\frac{|z_k|}{|z_{k-1}|} \geq 1$, on a nécessairement $\frac{|z_k|}{|z_{k-1}|} > 2$ pour tout k compris entre 2 et n et :

$$|z_n| > 2|z_{n-1}| > 2^2|z_{n-2}| > \dots > 2^{n-1}|z_1|.$$

Mais l'hypothèse $\sum_{k=1}^n z_k = 0$ nous donne :

$$|z_n| = \left| \sum_{k=1}^{n-1} z_k \right| \leq \sum_{k=1}^{n-1} |z_k| < |z_n| \sum_{k=1}^{n-1} \frac{1}{2^k}$$

soit :

$$\sum_{k=1}^{n-1} \frac{1}{2^k} = \frac{1}{2} \frac{1 - \frac{1}{2^{n-1}}}{1 - \frac{1}{2}} = 1 - \frac{1}{2^{n-1}} > 1$$

ce qui est impossible.

Exercice 7.12 Déterminer tous les nombres complexes a et b , tels que la fonction $f : z \mapsto az + b\bar{z}$ soit involutive (i. e. telle que $f \circ f = \text{Id}_{\mathbb{C}}$).

Solution 7.12 Dire que f est involutive équivaut à dire que pour tout nombre complexe z , on a :

$$a(az + b\bar{z}) + b(\overline{az + b\bar{z}}) = z$$

ce qui est encore équivalent à :

$$(a^2 + |b|^2 - 1)z + b(a + \bar{a})\bar{z} = 0 \quad (7.1)$$

Prenant respectivement $z = 1$ et $z = i$, on aboutit à :

$$\begin{cases} (a^2 + |b|^2 - 1) + b(a + \bar{a}) = 0 \\ (a^2 + |b|^2 - 1) - b(a + \bar{a}) = 0 \end{cases}$$

ce qui donne $a^2 + |b|^2 - 1 = 0$ par addition et $b(a + \bar{a}) = 0$ par soustraction.

Pour $b = 0$, on a $a^2 = 1$ et $a = \pm 1$.

Pour $b \neq 0$, on a $\bar{a} = -a$, ce qui signifie que a est imaginaire pur, soit $a = i\alpha$ avec α réel et $|b|^2 = 1 + \alpha^2 \geq 1$, ce qui impose $|b| \geq 1$ et $\alpha = \pm\sqrt{|b|^2 - 1}$.

Réciproquement si b est un nombre complexe de module supérieur ou égal à 1 et $a = \pm i\sqrt{|b|^2 - 1}$, on a alors $a^2 + |b|^2 = 1$ et $a + \bar{a} = 0$, ce qui entraîne (7.1) pour tout nombre complexe z .

Exercice 7.13 Déterminer l'ensemble des nombres complexes z tels que $u = (z - 1)(\bar{z} - i)$ soit réel [resp. imaginaire pur].

Solution 7.13 En écrivant $z = x + iy$, on a

$$\begin{aligned} u &= (x - 1 + iy)(x - i(y + 1)) \\ &= x^2 + y^2 + y - x + i(1 + y - x) \end{aligned}$$

et u est réel [resp. imaginaire pur] si, et seulement si, (x, y) appartient à la droite d'équation $y = x - 1$ [resp. au cercle d'équation $x^2 + y^2 + y - x = 0$].

Exercice 7.14 Déterminer l'ensemble des nombres complexes z tels que $|z - i| = |z - iz| = |z - 1|$.

Solution 7.14 On note $z = x + iy$ un nombre complexe.

L'égalité $|z - i| = |z - iz|$ équivaut à $x^2 + (y - 1)^2 = (x + y)^2 + (y - x)^2$, ou encore à :

$$x^2 - 2y + y^2 + 1 = 2x^2 + 2y^2$$

soit à :

$$x^2 + y^2 + 2y - 1 = 0. \quad (7.2)$$

L'égalité $|z - i| = |z - 1|$ équivaut à $x^2 + (y - 1)^2 = (x - 1)^2 + y^2$, encore équivalent à $x = y$. L'équation (7.2) nous dit alors que x est nécessairement solution de :

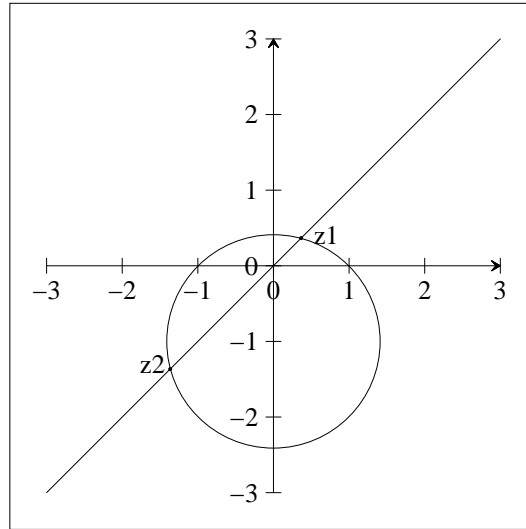
$$2x^2 + 2x - 1 = 0$$

ce qui donne deux solutions possibles :

$$z_1 = -\frac{1 + \sqrt{3}}{2}(1 + i) \quad \text{et} \quad z_2 = \frac{\sqrt{3} - 1}{2}(1 + i)$$

Réciproquement, on vérifie que ces solutions conviennent bien.

Géométriquement, l'ensemble des points cherché est l'intersection du cercle \mathcal{C} d'équation (20.24) et de la droite \mathcal{D} d'équation $y = x$ (figure 7.1).

FIGURE 7.1 – $\mathcal{C} \cap \mathcal{D}$

7.4 Les équations de degré 2

On s'intéresse ici aux équations algébriques de degré 2 à coefficients complexes, c'est-à-dire aux équations de la forme $ax^2 + bx + c = 0$ où a, b, c sont des nombres complexes avec $a \neq 0$.

Si on se place dans le cadre réel (i. e. les coefficients a, b, c sont réels et on cherche des solutions réelles), on sait qu'une telle équation n'a pas nécessairement de solution (c'est l'exemple de $x^2 + 1 = 0$ qui nous a conduit aux nombres complexes).

En divisant par a , on se ramène au cas où $a = 1$.

On remarque tout d'abord qu'une telle équation a au plus deux solutions complexes. En effet, si $z_1 \in \mathbb{C}$ est solution de $x^2 + bx + c = 0$, en désignant par z une autre solution, on a le système d'équations :

$$\begin{cases} z^2 + bz + c = 0 \\ z_1^2 + z z_1 + c = 0 \end{cases}$$

et par soustraction on aboutit à :

$$(z - z_1)(z + z_1 + b) = 0$$

qui donne $z = x_1$ ou $z = -z_1 - b$.

Il suffit donc de trouver une solution (s'il en existe) de cette équation pour avoir les deux.

Nous allons voir que sur \mathbb{C} une équation de degré 2 a toujours deux solutions, distinctes ou confondues.

Connaissant $i \in \mathbb{C}$ solution de $x^2 + 1 = 0$, on déduit que pour tout réel a non nul l'équation $x^2 + a = 0$ a exactement deux solutions distinctes. En effet si a est négatif, cette équation équivaut à $x^2 = -a$ avec $-a > 0$, et dans l'ensemble des réels, on sait que cela équivaut à dire que $x = \pm\sqrt{-a}$, ce qui fournit deux solutions réelles distinctes. Si a est positif, cette équation équivaut à $x^2 = -a = i^2(\sqrt{a})^2$, soit à $x^2 - (i\sqrt{a})^2 = 0$ ce qui équivaut à $x = \pm i\sqrt{a}$.

On a donc le résultat suivant.

Théorème 7.8 *Pour tout nombre réel non nul a l'équation $x^2 + a = 0$ a exactement deux solutions données par :*

$$\begin{cases} x_1 = -\sqrt{-a} \text{ et } x_2 = \sqrt{-a} \text{ si } a < 0 \\ x_1 = -i\sqrt{a} \text{ et } x_2 = i\sqrt{a} \text{ si } a > 0 \end{cases}$$

Pour $a = 0$, $x = 0$ est la seule solution de cette équation.

Définition 7.5 Si α est un nombre complexe, on dit que le nombre complexe u est une racine carrée de α si $u^2 = \alpha$.

Le théorème précédent nous dit que tout nombre réel non nul a a exactement deux racines carrées complexes, ce sont les réels $\pm\sqrt{a}$ pour $a > 0$ et les complexes $\pm i\sqrt{-a}$ pour $a < 0$.

Ce résultat est en fait valable pour tout nombre complexe α .

Théorème 7.9 Tout nombre complexe non nul $\alpha = a + ib$ a exactement deux racines carrées.

Démonstration. Il s'agit de résoudre l'équation $z^2 = \alpha$ et pour ce faire il nous suffit de trouver une solution.

Si $b = 0$, alors $\alpha = a$ est réel et le problème a été résolu.

On suppose donc que $b \neq 0$.

En notant $z = x + iy$, l'équation $z^2 = \alpha = a + ib$ équivaut au système de deux équations aux inconnues x, y :

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

En utilisant le module de z , le système :

$$\begin{cases} x^2 - y^2 = a \\ |z^2| = |z|^2 = x^2 + y^2 = |\alpha| \end{cases}$$

nous donne immédiatement :

$$x^2 = \frac{a + |\alpha|}{2}$$

avec

$$a + |\alpha| = a + \sqrt{a^2 + b^2} > a + \sqrt{a^2} = a + |a| \geq 0$$

et en conséquence, $x = \pm \frac{\sqrt{a + |\alpha|}}{\sqrt{2}}$, la partie imaginaire y étant déterminée par l'équation $2xy = b$ avec $b \neq 0$ (donc $x \neq 0$ et $y \neq 0$). En définitive l'équation $z^2 = \alpha$ a deux solutions complexes données par :

$$\begin{aligned} z_1 &= \sqrt{\frac{a + |\alpha|}{2}} + i \frac{b}{2\sqrt{\frac{a + |\alpha|}{2}}} = \frac{1}{\sqrt{2}} \frac{a + ib + |\alpha|}{\sqrt{a + |\alpha|}} \\ &= \frac{1}{\sqrt{2}} \frac{\alpha + |\alpha|}{\sqrt{\Re(\alpha) + |\alpha|}} = \frac{1}{\sqrt{2}} \frac{a + ib + \sqrt{a^2 + b^2}}{\sqrt{a + \sqrt{a^2 + b^2}}} \end{aligned}$$

et :

$$z_2 = -z_1$$

■

On en déduit alors le résultat suivant.

Théorème 7.10 Toute équation de degré 2, $az^2 + bz + c = 0$ ($a \neq 0$) a deux solutions complexes distinctes ou confondues.

Démonstration. En utilisant la forme réduite d'un polynôme de degré 2 :

$$az^2 + bz + c = a \left(\left(z + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right)$$

on est ramené à l'équation :

$$\left(z + \frac{b}{2a} \right)^2 = \frac{b^2 - 4ac}{4a^2}$$

qui a deux solutions distinctes (si $b^2 - 4ac \neq 0$) ou confondues (si $b^2 - 4ac = 0$). ■

Avec les notations du théorème la quantité $\delta = b^2 - 4ac$ est appelé discriminant de l'équation $ax^2 + bx + c = 0$.

Pour $\delta = 0$, $z_1 = z_2 = -\frac{b}{2a}$ est la seule solution (on dit que c'est une racine double) et pour $\delta \neq 0$, les deux solutions sont $z_1 = \frac{-b - \gamma}{2a}$ et $z_2 = \frac{-b + \gamma}{2a}$ où γ est une racine carrée de δ (i.e. $\gamma^2 = \delta$).

Dans les deux cas, on $z_1 + z_2 = -\frac{b}{a}$ et $z_1 z_2 = \frac{b^2 - \gamma^2}{4a^2} = \frac{b^2 - \delta}{4a^2} = \frac{c}{a}$.

Réciproquement si z_1, z_2 sont deux nombres complexes tels que $z_1 + z_2 = -\frac{b}{a}$ et $z_1 z_2 = \frac{c}{a}$, on a $z_2 = -\frac{b}{a} - z_1$ et $z_1 \left(-\frac{b}{a} - z_1 \right) = \frac{c}{a}$, c'est-à-dire que z_1 est solution de l'équation $z^2 + \frac{b}{a}z + \frac{c}{a} = 0$, soit de l'équation $az^2 + bz + c = 0$. Comme z_1 et z_2 jouent des rôles symétriques, z_2 est également solution de cette équation. En résumé, on a le résultat suivant.

Théorème 7.11 *Étant donnés des nombres complexes a, b, c avec $a \neq 0$, les nombres complexes z_1 et z_2 sont les racines de l'équation $az^2 + bz + c = 0$ si, et seulement si, $z_1 + z_2 = -\frac{b}{a}$ et $z_1 z_2 = \frac{c}{a}$.*

Dans le cas où les coefficients a, b, c sont réels, il en est de même de δ et on distingue trois cas de figure :

- soit $\delta = 0$ et $x_1 = -\frac{b}{2a}$ est la seule solution réelle de cette équation ;
- soit $\delta > 0$ et $x_1 = \frac{-b - \sqrt{\delta}}{2a}$, $x_2 = \frac{-b + \sqrt{\delta}}{2a}$ sont les deux solutions réelles de cette équation ;
- soit $\delta < 0$ et $x_1 = \frac{-b - i\sqrt{-\delta}}{2a}$, $x_2 = \frac{-b + i\sqrt{-\delta}}{2a}$ sont les deux solutions complexes non réelles de cette équation.

Parfois le coefficient b s'écrit naturellement sous la forme $b = 2b'$ et on a :

$$\delta = 4 \left((b')^2 - ac \right)$$

La quantité $\delta' = (b')^2 - ac$ est alors appelée discriminant réduit de l'équation $ax^2 + 2b'x + c = 0$. Dans le cas où les coefficients a, b, c sont réels, on a :

- soit $\delta' = 0$ et $x_1 = -\frac{b'}{a}$ est la seule solution réelle de cette équation ;
- soit $\delta' > 0$ et $x_1 = \frac{-b' - \sqrt{\delta'}}{a}$, $x_2 = \frac{-b' + \sqrt{\delta'}}{a}$ sont les deux solutions réelles de cette équation ;

— soit $\delta' < 0$ et $x_1 = \frac{-b' - i\sqrt{-\delta'}}{a}$, $x_2 = \frac{-b' + i\sqrt{-\delta'}}{a}$ sont les deux solutions complexes non réelles de cette équation.

De manière plus générale, on peut montrer le théorème suivant que nous admettrons.

Théorème 7.12 (d'Alembert-Gauss) *Toute équation polynomiale à coefficients complexes de degré non nul n admet n racines complexes distinctes ou confondues.*

On rappelle que si P est un polynôme non constant (i. e. de degré $n \geq 1$) à coefficients complexes [resp. réels], on dit que $\alpha \in \mathbb{C}$ [resp. $\alpha \in \mathbb{R}$] est racine de P si $P(\alpha) = 0$.

On peut donner plusieurs démonstrations du théorème de d'Alembert-Gauss mais toutes utilisent des outils d'algèbre ou d'analyse plus sophistiqués que le contenu de ce chapitre. Le problème du paragraphe 27 propose une démonstration classique qui utilise des outils d'analyse.

Il est par contre facile de montrer qu'un polynôme à coefficients complexes [resp. réels] de degré $n \geq 1$ a au plus n racines complexes [resp. réelles] distinctes ou confondues. En effet pour $n = 1$, l'unique racine du polynôme $az + b$ avec $a \neq 0$ est $z = -\frac{b}{a}$. En supposant le résultat acquis pour les polynômes de degré $n - 1 \geq 1$, on se donne un polynôme $P(z) = \sum_{k=0}^n a_k z^k$ de degré n (ce qui signifie que $a_n \neq 0$). S'il admet une racine α , on peut écrire, pour tout nombre complexe z :

$$P(z) = P(z) - P(\alpha) = \sum_{k=1}^n a_k (z^k - \alpha^k)$$

avec $z^k - \alpha^k = (z - \alpha) \sum_{j=1}^k z^{k-j} \alpha^{j-1}$ pour tout $k \geq 1$, ce qui donne $P(z) = (z - \alpha) Q(z)$, où Q est un polynôme de degré $n - 1$, il a donc au plus $n - 1$ racines et P a au plus n racines.

Une conséquence importante est que deux polynômes P et Q de degré $n \geq 1$ qui coïncident en $n + 1$ points distincts sont nécessairement égaux. En effet $P - Q$ est nul ou de degré au plus n . S'il est non constant, il est degré $p \leq n$ avec $n + 1 > p$ racines, ce qui est impossible. Il est donc constant égal à $P(\alpha) - Q(\alpha) = 0$ où α est l'une des racines communes de P et Q .

Exercice 7.15 Factoriser dans \mathbb{R} puis dans \mathbb{C} , $x^4 + 1$.

Solution 7.15 Dans \mathbb{R} on a :

$$\begin{aligned} x^4 + 1 &= (x^2 + 1)^2 - 2x^2 \\ &= (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) \end{aligned}$$

les deux polynômes $x^2 \pm \sqrt{2}x + 1$ de discriminant $\delta = -2 < 0$ étant sans racines réelles. Sur \mathbb{C} ces polynômes ont pour racines $\frac{\pm 1 \pm i1}{\sqrt{2}}$, ce qui donne :

$$x^4 + 1 = \left(x - \frac{1-i}{\sqrt{2}}\right) \left(x - \frac{1+i}{\sqrt{2}}\right) \left(x + \frac{1+i}{\sqrt{2}}\right) \left(x + \frac{1-i}{\sqrt{2}}\right)$$

Exercice 7.16 Déterminer les racines carrées complexes de $\alpha = -7 + 24i$.

Solution 7.16 En écrivant $z = x + iy$, l'équation $z^2 = \alpha$ équivaut à :

$$\begin{cases} x^2 - y^2 = -7 \\ xy = 12 \end{cases}$$

Considérant que $|z|^2 = x^2 + y^2 = |\alpha| = 25$, on déduit que $x^2 = 9$, donc $x = 3$ et $y = 4$ ou $x = -3$ et $y = -4$. Les deux racines carrées de α sont donc $\pm(3 + 4i)$.

Exercice 7.17 Résoudre dans \mathbb{C} l'équation $z^2 - (1 - 2i)z + 1 - 7i = 0$.

Solution 7.17 Cette équation est équivalente à :

$$\left(z - \frac{1 - 2i}{2}\right)^2 = \frac{(1 - 2i)^2}{4} - 1 + 7i = \frac{-7 + 24i}{4}$$

soit à $Z^2 = \alpha = -7 + 24i$, où on a posé $Z = 2z - 1 + 2i$, ce qui donne $Z = \pm(3 + 4i)$ et $z = \frac{1 - 2i}{2} \pm \frac{3 + 4i}{2}$. Les deux solutions complexes de cette équation sont donc :

$$z_1 = 2 + i, \quad z_2 = -2 - 3i.$$

7.5 Les équations de degré 3 et 4

On s'intéresse tout d'abord aux équations polynomiales de degré 3 :

$$P(z) = z^3 + az^2 + bz + c = 0$$

où a, b, c sont des nombres complexes.

Dans un premier temps, on effectue une translation en vue de supprimer le terme en z^2 de cette équation, c'est-à-dire qu'on cherche $\lambda \in \mathbb{C}$ qui permette de supprimer z^2 dans :

$$P(z - \lambda) = (z - \lambda)^3 + a(z - \lambda)^2 + b(z - \lambda) + c.$$

En développant, on a :

$$P(z - \lambda) = z^3 + (a - 3\lambda)z^2 + (\lambda^2 - 2a\lambda + b)z + (c - b\lambda + a\lambda^2 - \lambda^3).$$

Le choix de $\lambda = \frac{a}{3}$ donne :

$$P(z - \lambda) = z^3 + \left(b - \frac{a^2}{3}\right)z + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right).$$

On est donc ramené à l'équation :

$$Q(z) = z^3 + pz + q = 0$$

où on a noté $p = b - \frac{a^2}{3}$ et $q = c - \frac{ab}{3} + \frac{2a^3}{27}$. Si z est solution de $Q(z) = 0$, alors $z - \lambda$ est solution de $P(t) = 0$.

Si $p = 0$, alors les solutions de $Q(z) = 0$ sont les racines cubiques de $-q$.

Si $p \neq 0$, on cherche alors les solutions sous la forme $z = u + v$ en imposant une condition supplémentaire à u et v . En développant :

$$P(u + v) = u^3 + v^3 + (3uv + p)(u + v) + q$$

on est amené à imposer $3uv + p = 0$, ce qui donne le système de deux équations à deux inconnues :

$$\begin{cases} u^3 + v^3 = -q \\ 3uv = -p \end{cases}$$

Les nombres complexes u^3 et v^3 sont alors solutions de :

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = -\frac{p^3}{27} \end{cases}$$

ce qui revient à dire que ce sont les solutions de l'équation de degré 2 :

$$x^2 + qx - \frac{p^3}{27} = 0$$

Le discriminant de cette équation est :

$$\delta = \frac{4p^3 + 27q^2}{27}.$$

Notant ω une racine carrée de δ ($\omega^2 = \delta$), on a :

$$u^3 = \frac{-q - \omega}{2} \text{ et } v^3 = \frac{-q + \omega}{2}$$

En désignant par w une racine cubique $\frac{-q - \omega}{2}$, les deux autres sont jwt et $\bar{j}w$. Enfin la relation $3uv = -p$ avec $p \neq 0$, donne $u \neq 0$, $v \neq 0$ et $v = -\frac{p}{3u}$. On a donc ainsi trouvé trois solutions (u, v) , à savoir :

$$\left(w, -\frac{p}{3w}\right), \left(jw, -\frac{p}{3jw}\right) = \left(jw, -\frac{p\bar{j}}{3w}\right) \text{ et } \left(\bar{j}w, -\frac{p}{3\bar{j}w}\right) = \left(\bar{j}w, -\frac{pj}{3w}\right)$$

ce qui donne trois solutions pour l'équation $Q(z) = 0$:

$$z_1 = w - \frac{p}{3w}, \quad z_2 = jw - \frac{p\bar{j}}{3w}, \quad z_3 = \bar{j}w - \frac{pj}{3w}$$

et on les a toutes.

Exercice 7.18 Résoudre dans \mathbb{C} l'équation :

$$P(z) = z^3 - 3z^2 + 4z - 4 = 0$$

Solution 7.18 On élimine tout d'abord le terme en z^2 . On a :

$$\begin{aligned} P(z - \lambda) &= (z - \lambda)^3 - 3(z - \lambda)^2 + 4(z - \lambda) - 4 \\ &= z^3 - 3(\lambda + 1)z^2 + (4 + 6\lambda + 3\lambda^2)z - (\lambda^3 + 3\lambda^2 + 4\lambda + 4) \end{aligned}$$

et $\lambda = -1$ donne :

$$Q(z) = P(z + 1) = z^3 + z - 2.$$

Cherchant les solutions sous la forme $z = u + v$, on aboutit à :

$$\begin{cases} u^3 + v^3 = 2 \\ u^3 v^3 = -\frac{1}{27} \end{cases}$$

qui nous conduit à résoudre :

$$x^2 - 2x - \frac{1}{27} = 0$$

de solutions :

$$u^3 = 1 + \frac{2\sqrt{7}}{3\sqrt{3}} \text{ et } v^3 = 1 - \frac{2\sqrt{7}}{3\sqrt{3}}.$$

Ce qui donne :

$$u \in \left\{ \sqrt[3]{1 + \frac{2\sqrt{7}}{3\sqrt{3}}}, j\sqrt[3]{1 + \frac{2\sqrt{7}}{3\sqrt{3}}}, \bar{j}\sqrt[3]{1 + \frac{2\sqrt{7}}{3\sqrt{3}}} \right\}$$

et $v = -\frac{1}{3u}$ avec :

$$\frac{1}{u} = \frac{1}{\sqrt[3]{1 + \frac{2\sqrt{7}}{3\sqrt{3}}}} = \frac{\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1}}{\sqrt[3]{\frac{28}{27} - 1}} = 3\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1}.$$

D'où les solutions de $Q(z) = 0$:

$$\begin{aligned} z_1 &= \sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} + 1} - \sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1} \\ z_2 &= j\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} + 1} - \bar{j}\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1} \\ z_3 &= \bar{j}\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} + 1} - j\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1} \end{aligned}$$

Comme 1 est racine évidente de $Q(z) = 1$ et que z_1 est la seule solution réelle, on a nécessairement :

$$\sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} + 1} - \sqrt[3]{\frac{2\sqrt{7}}{3\sqrt{3}} - 1} = 1$$

ce qui peut se vérifier en élevant au carré.

Les solutions de $P(z) = 0$ sont alors :

$$z_1 + 1 = 2, \quad z_2 + 1, \quad z_3 + 1.$$

7.6 Arguments d'un nombre complexe

On suppose connues du cours d'analyse les fonctions trigonométriques \cos , \sin et \tan avec leurs principales propriétés. En particulier, les fonctions \cos et \sin sont définies sur \mathbb{R} , périodiques de période 2π , la fonction \cos est paire, la fonction \sin est impaire et on a les formules de trigonométrie suivantes valables pour tous réels a, b :

$$\begin{cases} \cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b) \\ \sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b) \end{cases}$$

desquelles on déduit les suivantes bien utiles :

$$\left\{ \begin{array}{l} \cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b) \\ \sin(a-b) = \sin(a)\cos(b) - \cos(a)\sin(b) \\ \cos(2a) = \cos^2(a) - \sin^2(a) \\ \sin(2a) = 2\sin(a)\cos(b) \\ \cos(a)\cos(b) = \frac{\cos(a+b) + \cos(a-b)}{2} \\ \sin(a)\sin(b) = \frac{\cos(a-b) - \cos(a+b)}{2} \\ \cos(a)\sin(b) = \frac{\sin(a+b) - \sin(a-b)}{2} \\ \sin(a)\cos(b) = \frac{\sin(a+b) + \sin(a-b)}{2} \end{array} \right.$$

enfin avec $\cos(0) = 1$, on déduit que :

$$\cos^2(a) + \sin^2(a) = 1.$$

La fonction \tan est définie sur $\mathbb{R} \setminus \left\{ \frac{\pi}{2} + k\pi \mid k \in \mathbb{Z} \right\}$ par $\tan(x) = \frac{\sin(x)}{\cos(x)}$ et elle est impaire et π -périodique.

La fonction \cos réalise une bijection de $[0, \pi]$ sur $[-1, 1]$, la fonction \sin une bijection de $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ sur $[-1, 1]$ et la fonction \tan une bijection de $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ sur \mathbb{R} . Les fonctions réciproques de ces fonctions trigonométriques sont notées respectivement \arccos , \arcsin et \arctan . On a donc :

$$\begin{aligned} (x \in [0, \pi] \text{ et } y = \cos(x)) &\Leftrightarrow (y \in [-1, 1] \text{ et } x = \arccos(y)) \\ (x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \text{ et } y = \sin(x)) &\Leftrightarrow (y \in [-1, 1] \text{ et } x = \arcsin(y)) \\ (x \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\text{ et } y = \tan(x)) &\Leftrightarrow (y \in \mathbb{R} \text{ et } x = \arctan(y)) \end{aligned}$$

Exercice 7.19 Montrer que pour tout réel x on a :

$$\sin\left(\frac{x}{2}\right) \left(\frac{1}{2} + \sum_{k=1}^n \cos(kx) \right) = \frac{1}{2} \sin\left(\frac{2n+1}{2}x\right).$$

Solution 7.19 Pour tout entier naturel k et pour tout réel u on a :

$$\sin\left(\frac{u}{2}\right) \cos(ku) = \frac{1}{2} \left(\sin\left(\left(k + \frac{1}{2}\right)u\right) - \sin\left(\left(k - \frac{1}{2}\right)u\right) \right),$$

on en déduit alors que pour tout réel u on a :

$$\begin{aligned} \sin\left(\frac{u}{2}\right) \left(\frac{1}{2} + \sum_{k=1}^n \cos(ku) \right) &= \frac{1}{2} \left(\sin\left(\frac{u}{2}\right) + \sum_{k=1}^n \left(\sin\left(\frac{2k+1}{2}u\right) - \sin\left(\frac{2k-1}{2}u\right) \right) \right) \\ &= \frac{1}{2} \sin\left(\frac{2n+1}{2}u\right) \end{aligned}$$

Exercice 7.20 Montrer que pour tout réel x on a :

$$\sin\left(\frac{x}{2}\right) \left(\sum_{k=0}^{n-1} \sin\left((2k+1)\frac{x}{2}\right) \right) = \sin^2\left(\frac{n}{2}x\right).$$

Solution 7.20 Pour tout entier naturel k et pour tout réel u on a :

$$\sin\left(\frac{u}{2}\right) \sin\left((2k+1)\frac{u}{2}\right) = \frac{1}{2}(\cos(ku) - \cos((k+1)u)),$$

on en déduit alors que pour tout réel u on a :

$$\begin{aligned} \sin\left(\frac{u}{2}\right) \left(\sum_{k=0}^{n-1} \sin\left((2k+1)\frac{u}{2}\right)\right) &= \frac{1}{2} \left(\sum_{k=0}^{n-1} (\cos(ku) - \cos((k+1)u))\right) \\ &= \frac{1}{2}(1 - \cos(nu)) = \sin^2\left(\frac{n}{2}u\right). \end{aligned}$$

Le résultat suivant est la base de la définition de l'argument d'un nombre complexe.

Théorème 7.13 Si z est un nombre complexe de module 1, il existe un unique réel $\theta \in [-\pi, \pi[$ tel que $z = \cos(\theta) + i \sin(\theta)$.

Démonstration. Le nombre complexe $z = x + iy$ est de module 1 si, et seulement si $x^2 + y^2 = 1$. En particulier x est dans $[-1, 1]$ et il existe un unique réel $\alpha \in [0, \pi]$ tel que $x = \cos(\alpha)$. Avec $y^2 = 1 - x^2 = \sin^2(\alpha)$, on déduit que $y = \pm \sin(\alpha)$, soit $y = \sin(\pm\alpha)$. Avec la parité de la fonction \cos , on peut écrire que $x = \cos(\pm\alpha)$ et on aboutit à $(x, y) = (\cos(\theta), \sin(\theta))$ avec $\theta \in [-\pi, \pi[$ (pour $(x, y) = (\cos(\pi), \sin(\pi)) = (-1, 0)$, on écrit $(x, y) = (\cos(-\pi), \sin(-\pi))$).

Si $\theta' \in [-\pi, \pi[$ est une autre solution, de $\cos(\theta) = \cos(\theta')$, on déduit que $\theta' = \pm\theta$. Si $\theta' = \theta$, c'est terminé, sinon $\theta' = -\theta$ et de $\sin(\theta) = \sin(\theta') = -\sin(\theta)$, on déduit que θ vaut 0 ou $-\pi$, 0 étant la seule solution puisque $\theta' = \pi \notin [-\pi, \pi[$. D'où l'unicité. ■

Corollaire 7.2 Pour tout nombre complexe non nul z , il existe un unique réel $\theta \in [-\pi, \pi[$ tel que $\frac{z}{|z|} = \cos(\theta) + i \sin(\theta)$.

Démonstration. On applique le théorème précédent à $\frac{z}{|z|}$ qui est de module égal à 1. ■

Définition 7.6 Avec les notations du corollaire qui précède, on dit que le réel $\theta \in [-\pi, \pi[$ est l'argument principal du nombre complexe non nul z .

Si $\theta \in [-\pi, \pi[$ est l'argument principal d'un nombre complexe $z \in \mathbb{C}^*$, les seuls réels θ' tels que $\frac{z}{|z|} = \cos(\theta') + i \sin(\theta')$ sont les réels $\theta' = \theta + 2k\pi$, où k est un entier relatif. En effet ces réels conviennent et les égalités $\cos(\theta) = \cos(\theta')$ et $\sin(\theta) = \sin(\theta')$ sont réalisées si, et seulement si il existe un entier relatif k tel que $\theta' = \theta + 2k\pi$ (on peut trouver un entier k tel que $\theta' - 2k\pi$ soit dans $[-\pi, \pi[$, c'est-à-dire que k est tel que $-\pi \leq \theta' - 2k\pi < \pi$, soit $k \leq \frac{\theta' + \pi}{2\pi} < k + 1$, encore équivalent à $k = \left\lfloor \frac{\theta' + \pi}{2\pi} \right\rfloor$ et $\theta' - 2k\pi$ est l'argument principal de z).

Définition 7.7 On dit qu'un réel θ est un argument du nombre complexe non nul z si $\frac{z}{|z|} = \cos(\theta) + i \sin(\theta)$.

Ce qui précède nous dit qu'un nombre complexe non nul admet une infinité d'arguments et que deux tels arguments diffèrent d'un multiple entier de 2π , on dit alors qu'ils sont égaux modulo 2π .

On notera $\theta' \equiv \theta \pmod{2\pi}$ pour signifier que les réels θ' et θ sont égaux modulo 2π .

Si θ est un argument d'un nombre complexe non nul z , on notera $\arg(z) \equiv \theta \pmod{2\pi}$. La notation $\arg(z)$ signifie qu'on a choisi un argument de z , c'est donc un réel défini modulo 2π .

Par abus de langage, on écrira $\theta = \arg(z)$ quand il n'y a pas d'ambiguïté.

Avec le théorème qui suit on donne quelques propriétés des arguments d'un nombre complexe.

Théorème 7.14 *En désignant par z et z' des nombres complexes non nuls, λ un réel non nul et n un entier relatif, on a :*

1. $\arg(\bar{z}) \equiv -\arg(z) \pmod{2\pi}$;
2. $\arg(zz') \equiv \arg(z) + \arg(z') \pmod{2\pi}$;
3. $\arg\left(\frac{z}{z'}\right) \equiv \arg(z) - \arg(z') = \arg(z\bar{z'}) \pmod{2\pi}$;
4. $\arg(z^n) \equiv n \arg(z) \pmod{2\pi}$;
5. si $\lambda > 0$, alors $\arg(\lambda z) \equiv \arg(z) \pmod{2\pi}$, si $\lambda < 0$, alors $\arg(\lambda z) \equiv \arg(z) + \pi \pmod{2\pi}$;
6. z est réel si, et seulement si $\arg(z) \equiv 0 \pmod{\pi}$ (c'est-à-dire que les arguments de z sont de la forme $k\pi$ avec $k \in \mathbb{Z}$, l'argument principal étant 0 ou $-\pi$) ;
7. z est imaginaire pur si, et seulement si $\arg(z) \equiv \frac{\pi}{2} \pmod{\pi}$ (c'est-à-dire que les arguments de z sont de la forme $\frac{\pi}{2} + k\pi$ avec $k \in \mathbb{Z}$, l'argument principal étant $-\frac{\pi}{2}$ ou $\frac{\pi}{2}$).

Démonstration. Il suffit de considérer le cas des nombres complexes de module 1 par définition des arguments.

1. Pour $z = \cos(\theta) + i \sin(\theta)$, on a :

$$\bar{z} = \cos(\theta) - i \sin(\theta) = \cos(-\theta) + i \sin(-\theta)$$

et $-\theta$ est un argument de \bar{z} , donc $\arg(\bar{z}) \equiv -\theta \pmod{2\pi}$.

2. Pour $z = \cos(\theta) + i \sin(\theta)$ et $z' = \cos(\theta') + i \sin(\theta')$, on a :

$$\begin{aligned} zz' &= (\cos(\theta) \cos(\theta') - \sin(\theta) \sin(\theta')) + i (\sin(\theta) \cos(\theta') + \cos(\theta) \sin(\theta')) \\ &= \cos(\theta + \theta') + i \sin(\theta + \theta') \end{aligned}$$

et donc $\arg(zz') \equiv \theta + \theta' \pmod{2\pi}$.

3. On a

$$\begin{aligned} \arg\left(\frac{z}{z'}\right) &\equiv \arg(z\bar{z'}) \equiv \arg(z) + \arg(\bar{z'}) \\ &\equiv \arg(z) - \arg(z') \pmod{2\pi} \end{aligned}$$

4. Se déduit de ce qui précède.

■

En désignant par ψ l'application qui associe à tout réel θ le nombre complexe $\psi(\theta) = \cos(\theta) + i \sin(\theta)$ on réalise une application surjective de \mathbb{R} sur l'ensemble Γ des nombres complexes de module 1. Cette application n'est pas injective puisque l'égalité $\psi(\theta) = \psi(\theta')$ équivaut à $\theta' \equiv \theta \pmod{2\pi}$. En restriction à $[-\pi, \pi[$ cette application ψ est bijective.

Théorème 7.15 Avec les notations qui précèdent, on a $\psi(0) = 1$ et pour tous réels θ, θ' :

$$\psi(\theta + \theta') = \psi(\theta) \psi(\theta').$$

Démonstration. On a $\psi(0) = \cos(0) + i \sin(0) = 1$ et :

$$\begin{aligned} \psi(\theta + \theta') &= \cos(\theta + \theta') + i \sin(\theta + \theta') \\ &= (\cos(\theta) \cos(\theta') - \sin(\theta) \sin(\theta')) + i (\sin(\theta) \cos(\theta') + \cos(\theta) \sin(\theta')) \\ &= (\cos(\theta) + i \sin(\theta)) (\cos(\theta') + i \sin(\theta')) \\ &= \psi(\theta) \psi(\theta') \end{aligned}$$

■

La fonction ψ vérifie donc la même équation fonctionnelle que la fonction exponentielle réelle. Cette remarque justifie la notation $\psi(\theta) = e^{i\theta}$.

Avec $1 = \psi(0) = \psi(\theta - \theta) = \psi(\theta) \psi(-\theta)$, on déduit que $\frac{1}{\psi(\theta)} = \psi(-\theta) = \overline{\psi(\theta)}$ (ce que l'on savait déjà : l'inverse d'un nombre complexe de module 1 est égal à son conjugué).

On a donc en résumé la notation :

$$\forall \theta \in \mathbb{R}, e^{i\theta} = \cos(\theta) + i \sin(\theta)$$

ce qui définit une fonction 2π -périodique surjective de \mathbb{R} sur l'ensemble Γ des nombres complexes de module 1 avec les propriétés suivantes :

$$\left\{ \begin{array}{l} e^{i \cdot 0} = e^0 = 1 \\ \forall (\theta, \theta') \in \mathbb{R}^2, e^{i(\theta + \theta')} = e^{i\theta} e^{i\theta'} \\ \forall \theta \in \mathbb{R}, \frac{1}{e^{i\theta}} = e^{-i\theta} = \overline{e^{i\theta}} \\ \forall (\theta, \theta') \in \mathbb{R}^2, (e^{i\theta} = e^{i\theta'}) \Leftrightarrow (\exists k \in \mathbb{Z} \mid \theta' = \theta + 2k\pi) \\ \forall \theta \in \mathbb{R}, \cos(\theta) = \Re(e^{i\theta}) = \frac{e^{i\theta} + e^{-i\theta}}{2} \text{ et } \sin(\theta) = \Im(e^{i\theta}) = \frac{e^{i\theta} - e^{-i\theta}}{2i} \end{array} \right.$$

Par récurrence sur $n \geq 0$, on déduit facilement que $(e^{i\theta})^n = e^{in\theta}$. Puis pour $n < 0$ on a $e^{in\theta} = \frac{1}{e^{-in\theta}} = \left(\frac{1}{e^{i\theta}}\right)^{-n} = (e^{-i\theta})^{-n} = e^{in\theta}$, c'est-à-dire que cette formule est valable pour tous les entiers relatifs. Nous verrons un peu plus loin l'intérêt de cette égalité.

On a en particulier les valeurs suivantes :

$$e^{i\pi} = -1, e^{i\frac{\pi}{2}} = i$$

les égalités $e^{i\theta} = 1$, $e^{i\theta} = -1$ et $e^{i\theta} = i$ étant réalisées respectivement si, et seulement si $\theta = 2k\pi$, $\theta = (2k+1)\pi$ et $\theta = \frac{\pi}{2} + 2k\pi$, où k est un entier relatif.

Un nombre complexe non nul peut donc s'écrire sous la forme $z = \rho e^{i\theta}$ où ρ est un réel strictement positif uniquement déterminé, c'est le module de z , et θ est un argument de z . Cette écriture est l'écriture polaire (ou trigonométrique) de z .

Exercice 7.21 Soient z, z' deux nombres complexes non nuls. Montrer que $|z + z'| = |z| + |z'|$ si, et seulement si, $\arg(z) \equiv \arg(z') \pmod{2\pi}$.

Solution 7.21 L'égalité $|z + z'| = |z| + |z'|$ est équivalente à $|z + z'|^2 = (|z| + |z'|)^2$ avec :

$$|z + z'|^2 = (z + z')(\bar{z} + \bar{z}') = |z|^2 + |z'|^2 + z\bar{z}' + \bar{z}z'.$$

On a donc $|z + z'| = |z| + |z'|$ si, et seulement si, $z\bar{z}' + \bar{z}z' = 2|z||z'|$, ce qui équivaut encore à $\Re(z\bar{z}') = |z||z'|$. En utilisant l'écriture polaire, $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$ avec $\rho > 0$, $\rho' > 0$ et θ, θ' réels, on déduit que $|z + z'| = |z| + |z'|$ si, et seulement si, $\cos(\theta - \theta') = 1$, ce qui équivaut à $\theta - \theta' \equiv 0 \pmod{2\pi}$ et signifie que $\arg(z) \equiv \arg(z') \pmod{2\pi}$.

Plus généralement, on a le résultat suivant.

Exercice 7.22 Démontrer que, pour tout entier naturel r non nul et toute famille (z_1, \dots, z_r) de complexes non nuls, l'égalité :

$$\left| \sum_{k=1}^r z_k \right| = \sum_{k=1}^r |z_k|$$

est réalisée si, et seulement si :

$$\forall k \in \mathbb{N}, (2 \leq k \leq r) \Rightarrow (\exists \lambda_k \in]0, +\infty[, z_k = \lambda_k z_1)$$

ce qui revient à dire que tous les z_k ont le même argument modulo 2π .

Solution 7.22 Chaque nombre complexe non nul z_k ($1 \leq k \leq r$) peut s'écrire $z_k = \rho_k e^{i\theta_k}$ avec $\rho_k = |z_k| > 0$ et $\theta_k \in [-\pi, \pi[$. On a alors :

$$\begin{cases} \left| \sum_{k=1}^r z_k \right|^2 = \sum_{k=1}^r |z_k|^2 + 2 \sum_{1 \leq j < k \leq r} \rho_j \rho_k \cos(\theta_j - \theta_k), \\ \left(\sum_{k=1}^r |z_k| \right)^2 = \sum_{k=1}^r |z_k|^2 + 2 \sum_{1 \leq j < k \leq r} \rho_j \rho_k \end{cases}$$

et l'égalité $\left| \sum_{k=1}^r z_k \right| = \sum_{k=1}^r |z_k|$ est équivalente à :

$$\sum_{1 \leq j < k \leq r} \rho_j \rho_k (1 - \cos(\theta_j - \theta_k)) = 0.$$

Tous les termes de cette somme étant positifs ou nuls avec $\rho_j \rho_k > 0$, on en déduit que $\cos(\theta_j - \theta_k) = 1$ avec $\theta_j - \theta_k \in]-2\pi, 2\pi[$ pour $1 \leq j < k \leq r$ (on a $-\pi \leq \theta_j < \pi$ et $-\pi \leq \theta_k < \pi$ donc $-\pi < -\theta_k \leq \pi$ et $-2\pi < \theta_j - \theta_k < 2\pi$), ce qui donne $\theta_j = \theta_k$ et en notant θ cette valeur commune on a $z_k = \rho_k e^{i\theta} = |z_k| e^{i\theta}$ pour tout entier k compris entre 1 et r ou encore :

$$z_k = \frac{|z_k|}{|z_1|} |z_1| e^{i\theta} = \lambda_k z_1 \quad (1 \leq k \leq r)$$

où on a posé $\lambda_k = \frac{|z_k|}{|z_1|}$ pour tout k compris entre 1 et r .

Réciproquement si $z_k = \lambda_k z_1$ avec $\lambda_k > 0$ pour tout k compris entre 2 et r et $\lambda_1 = 1$, on a :

$$\left| \sum_{k=1}^r z_k \right| = |z_1| \sum_{k=1}^r \lambda_k = \sum_{k=1}^r \lambda_k |z_1| = \sum_{k=1}^r |z_k|.$$

On peut aussi démontrer ce résultat par récurrence sur $r \geq 1$, le cas $r = 2$ correspondant au cas d'égalité dans l'inégalité triangulaire sur \mathbb{C} .

Exercice 7.23 Déterminer, pour tout couple de réel (θ, θ') tel que $\cos\left(\frac{\theta - \theta'}{2}\right) \neq 0$, le module et un argument de $e^{i\theta} + e^{i\theta'}$.

Solution 7.23 On a :

$$e^{i\theta} + e^{i\theta'} = e^{i\frac{\theta+\theta'}{2}} \left(e^{i\frac{\theta-\theta'}{2}} + e^{-i\frac{\theta-\theta'}{2}} \right) = 2 \cos\left(\frac{\theta - \theta'}{2}\right) e^{i\frac{\theta+\theta'}{2}}$$

donc $e^{i\theta} + e^{i\theta'} \neq 0$ si $\cos\left(\frac{\theta - \theta'}{2}\right) \neq 0$,

$$|e^{i\theta} + e^{i\theta'}| = 2 \left| \cos\left(\frac{\theta - \theta'}{2}\right) \right|$$

et :

$$\arg(e^{i\theta} + e^{i\theta'}) \equiv \begin{cases} \frac{\theta + \theta'}{2} \quad (2\pi) \text{ si } \cos\left(\frac{\theta - \theta'}{2}\right) > 0 \\ \frac{\theta + \theta'}{2} + \pi \quad (2\pi) \text{ si } \cos\left(\frac{\theta - \theta'}{2}\right) < 0 \end{cases}$$

Exercice 7.24 Pour tout réel θ , on désigne par z_θ le nombre complexe $z_\theta = 1 - e^{i\theta}$.

1. Exprimer z_θ en fonction de $\sin\left(\frac{\theta}{2}\right)$ et de $e^{i\frac{\theta}{2}}$.
2. Montrer que pour tout entier naturel n et tout réel $\theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, on a :

$$\sum_{k=0}^n e^{ik\theta} = e^{in\frac{\theta}{2}} \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)}$$

3. En déduire des expressions de $\sum_{k=0}^n \cos(k\theta)$ et de $\sum_{k=1}^n \sin(k\theta)$ pour tout entier naturel non nul n et tout réel θ .

Solution 7.24

1. On a :

$$z_\theta = e^{i\frac{\theta}{2}} \left(e^{-i\frac{\theta}{2}} - e^{i\frac{\theta}{2}} \right) = -2i \sin\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}.$$

On peut aussi écrire que :

$$\begin{aligned} z_\theta &= 1 - \cos(\theta) - i \sin(\theta) = 2 \sin^2\left(\frac{\theta}{2}\right) - 2i \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) \\ &= -2i \sin\left(\frac{\theta}{2}\right) \left(\cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \right) = -2i \sin\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}. \end{aligned}$$

2. Comme $e^{i\theta} \neq 1$ pour $\theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$, on a :

$$\begin{aligned} \sum_{k=0}^n e^{ik\theta} &= \sum_{k=0}^n (e^{i\theta})^k = \frac{1 - e^{i(n+1)\theta}}{1 - e^{i\theta}} = \frac{-2i \sin\left(\frac{n+1}{2}\theta\right) e^{i\frac{n+1}{2}\theta}}{-2i \sin\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}} \\ &= e^{in\frac{\theta}{2}} \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)}. \end{aligned}$$

3. Ce qui donne en identifiant les parties réelles et imaginaires dans l'identité précédente :

$$\sum_{k=0}^n \cos(k\theta) = \cos\left(n\frac{\theta}{2}\right) \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)}$$

et :

$$\sum_{k=1}^n \sin(k\theta) = \sin\left(n\frac{\theta}{2}\right) \frac{\sin\left(\frac{n+1}{2}\theta\right)}{\sin\left(\frac{\theta}{2}\right)}$$

pour $n \geq 1$ et $\theta \in \mathbb{R} \setminus 2\pi\mathbb{Z}$. Pour $\theta \in 2\pi\mathbb{Z}$, on a $\cos(k\theta) = 1$ et $\sin(k\theta) = 0$ pour tout k , de sorte que $\sum_{k=0}^n \cos(k\theta) = n+1$ et $\sum_{k=1}^n \sin(k\theta) = 0$.

Exercice 7.25 Pour tout réel $\theta \in]-\pi, \pi[$, on désigne par z_θ le nombre complexe $z_\theta = 1 + e^{i\theta}$.

1. Exprimer z_θ en fonction de $\cos\left(\frac{\theta}{2}\right)$ et de $e^{i\frac{\theta}{2}}$.
2. En calculant, pour n entier naturel non nul, z_θ^n de deux manières différentes, montrer que :

$$\sum_{k=0}^n C_n^k \cos(k\theta) = 2^n \cos^n\left(\frac{\theta}{2}\right) \cos\left(n\frac{\theta}{2}\right)$$

et :

$$\sum_{k=1}^n C_n^k \sin(k\theta) = 2^n \cos^n\left(\frac{\theta}{2}\right) \sin\left(n\frac{\theta}{2}\right)$$

Solution 7.25

1. On a :

$$z_\theta = e^{i\frac{\theta}{2}} \left(e^{-i\frac{\theta}{2}} + e^{i\frac{\theta}{2}} \right) = 2 \cos\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}.$$

On peut aussi écrire que :

$$\begin{aligned} z_\theta &= 1 + \cos(\theta) + i \sin(\theta) = 2 \cos^2\left(\frac{\theta}{2}\right) + 2i \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) \\ &= 2 \cos\left(\frac{\theta}{2}\right) \left(\cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \right) = 2 \cos\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}. \end{aligned}$$

2. On a d'une part :

$$z_\theta^n = 2^n \cos^n\left(\frac{\theta}{2}\right) e^{i\frac{n\theta}{2}}$$

et d'autre part, en utilisant la formule du binôme de Newton :

$$z_\theta^n = (1 + e^{i\theta})^n = \sum_{k=0}^n C_n^k e^{ik\theta}$$

ce qui donne en identifiant les parties réelles et imaginaires :

$$\sum_{k=0}^n C_n^k \cos(k\theta) = 2^n \cos^n\left(\frac{\theta}{2}\right) \cos\left(n\frac{\theta}{2}\right)$$

et :

$$\sum_{k=1}^n C_n^k \sin(k\theta) = 2^n \cos^n\left(\frac{\theta}{2}\right) \sin\left(n\frac{\theta}{2}\right)$$

Exercice 7.26 Pour tout réel $\theta \in]-\pi, \pi[$, on désigne par z_θ le nombre complexe $z_\theta = 1 + e^{i\theta}$.

1. Déterminer le module et un argument de z_θ .
2. Déterminer, pour $\theta \in]-\pi, \pi[\setminus \{0\}$, le module et un argument de $u_\theta = \frac{1 + e^{i\theta}}{1 - e^{i\theta}}$.
3. Déterminer, pour tout entier naturel $n \geq 2$, le module et un argument de z_θ^n .
4. On prend $\theta = 2\frac{\pi}{3}$ et $n = 2006$. Déterminer le module et l'argument de z_θ^n qui est dans $]-\pi, \pi[$.
5. Calculer $e^{i\frac{\pi}{12}}$.
6. On prend $\theta = \frac{\pi}{6}$ et $n = 2006$. Déterminer le module et l'argument de z_θ^n qui est dans $]-\pi, \pi[$.

Solution 7.26

1. L'exercice 7.25 nous dit que $z_\theta = 2 \cos\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}$ et tenant compte de $\cos\left(\frac{\theta}{2}\right) > 0$ pour $\theta \in]-\pi, \pi[$, on déduit que :

$$|z_\theta| = 2 \cos\left(\frac{\theta}{2}\right) \text{ et } \arg(z_\theta) \equiv \frac{\theta}{2} \pmod{2\pi}$$

2. Pour $\theta \in]-\pi, \pi[\setminus \{0\}$, on a $\sin\left(\frac{\theta}{2}\right) \neq 0$ et :

$$u_\theta = \frac{2 \cos\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}}{-2i \sin\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}}} = i \cotan\left(\frac{\theta}{2}\right)$$

(exercice 7.24), ce qui donne :

$$|u_\theta| = \left| \cotan\left(\frac{\theta}{2}\right) \right|$$

et :

$$\arg(z_\theta) \equiv \begin{cases} \frac{\pi}{2} \pmod{2\pi} & \text{si } \theta \in]0, \pi[\\ -\frac{\pi}{2} \pmod{2\pi} & \text{si } \theta \in]-\pi, 0[\end{cases}$$

3. On a $z_\theta^n = 2^n \cos^n\left(\frac{\theta}{2}\right) e^{i\frac{n\theta}{2}}$ avec $\cos\left(\frac{\theta}{2}\right) > 0$ pour $\theta \in]-\pi, \pi[$, donc :

$$|z_\theta^n| = 2^n \cos^n\left(\frac{\theta}{2}\right) \text{ et } \arg(z_\theta^n) \equiv \frac{n\theta}{2} \pmod{2\pi}$$

4. On a :

$$z_\theta = 2 \cos\left(\frac{\pi}{3}\right) e^{i\frac{\pi}{3}} = e^{i\frac{\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$2006 = 6 * 334 + 2$, de sorte que :

$$|z_\theta^n| = 1 \text{ et } \arg(z_\theta^n) \equiv \frac{n\pi}{3} \equiv \frac{2\pi}{3} \pmod{2\pi}$$

5. On a :

$$\frac{\sqrt{3}}{2} = \cos\left(\frac{\pi}{6}\right) = 2\cos^2\left(\frac{\pi}{12}\right) - 1 = 1 - 2\sin^2\left(\frac{\pi}{12}\right)$$

avec $\cos\left(\frac{\pi}{12}\right) > 0$ et $\sin\left(\frac{\pi}{12}\right) > 0$, donc :

$$\cos\left(\frac{\pi}{12}\right) = \sqrt{\frac{1}{2} + \frac{\sqrt{3}}{4}} = \frac{\sqrt{2+\sqrt{3}}}{2}$$

$$\sin\left(\frac{\pi}{12}\right) = \sqrt{\frac{1}{2} - \frac{\sqrt{3}}{4}} = \frac{\sqrt{2-\sqrt{3}}}{2}$$

6. On a

$$|z_\theta^n| = 2^n \left| \cos\left(\frac{\pi}{12}\right) \right|^n = \left(\sqrt{2+\sqrt{3}} \right)^n = (2+\sqrt{3})^{1003}$$

et $2006 = 24 * 83 + 14$ de sorte que :

$$\arg(z_\theta^n) \equiv n \frac{\pi}{12} \equiv \frac{7\pi}{6} \pmod{2\pi}$$

Exercice 7.27 Pour cet exercice, θ est un réel fixé appartenant à $]0, \pi[$.

1. Déterminer le module et un argument de $u_\theta = 1 + e^{i\theta}$.
2. Déterminer le module et un argument de $v_\theta = 1 - e^{i\theta}$.
3. Résoudre dans \mathbb{C} l'équation $z^2 - 2ze^{i\theta} + 2ie^{i\theta} \sin(\theta) = 0$.

Solution 7.27

1. On a :

$$\begin{aligned} u_\theta &= 1 + \cos(\theta) + i \sin(\theta) = 2\cos^2\left(\frac{\theta}{2}\right) + 2i \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) \\ &= 2\cos\left(\frac{\theta}{2}\right) \left(\cos\left(\frac{\theta}{2}\right) + i \sin\left(\frac{\theta}{2}\right) \right) = 2\cos\left(\frac{\theta}{2}\right) e^{i\frac{\theta}{2}} \end{aligned}$$

avec $\cos\left(\frac{\theta}{2}\right) > 0$ pour $\theta \in]0, \pi[$, donc :

$$|u_\theta| = 2\cos\left(\frac{\theta}{2}\right) \text{ et } \arg(u_\theta) \equiv \frac{\theta}{2} \pmod{2\pi}$$

2. On a :

$$\begin{aligned} v_\theta &= 1 + e^{i(\theta+\pi)} = 2\cos\left(\frac{\theta}{2} + \frac{\pi}{2}\right) e^{i(\frac{\theta}{2} + \frac{\pi}{2})} \\ &= -2\sin\left(\frac{\theta}{2}\right) e^{i(\frac{\theta}{2} + \frac{\pi}{2})} = 2\sin\left(\frac{\theta}{2}\right) e^{i(\frac{\theta}{2} + 3\frac{\pi}{2})} \end{aligned}$$

avec $\sin\left(\frac{\theta}{2}\right) > 0$ pour $\theta \in]0, \pi[$, donc :

$$|v_\theta| = 2\sin\left(\frac{\theta}{2}\right) \text{ et } \arg(v_\theta) \equiv \frac{\theta}{2} + 3\frac{\pi}{2} \equiv \frac{\theta}{2} - \frac{\pi}{2} \pmod{2\pi}$$

3. On a :

$$\begin{aligned}
 P(z) &= z^2 - 2ze^{i\theta} + 2ie^{i\theta} \sin(\theta) = (z - e^{i\theta})^2 + e^{i\theta} (2i \sin(\theta) - e^{i\theta}) \\
 &= (z - e^{i\theta})^2 + e^{i\theta} (i \sin(\theta) - \cos(\theta)) \\
 &= (z - e^{i\theta})^2 - e^{i\theta} (\cos(\theta) - i \sin(\theta)) \\
 &= (z - e^{i\theta})^2 - e^{i\theta} e^{-i\theta} = (z - e^{i\theta})^2 - 1
 \end{aligned}$$

et $P(z) = 0$ équivaut à $z = e^{i\theta} \pm 1$. Les solutions sont donc $u_\theta = 1 + e^{i\theta}$ et $-v_\theta = e^{i\theta} - 1$.

Exercice 7.28 On désigne par $D(0, 1)$ le disque unité fermé du plan complexe, soit :

$$D(0, 1) = \{z \in \mathbb{C} \mid |z| \leq 1\}$$

Montrer que l'application :

$$\begin{aligned}
 \varphi : \mathbb{C} \setminus D(0, 1) &\rightarrow \mathbb{C} \setminus [-1, 1] \\
 z &\mapsto \frac{1}{2} \left(z + \frac{1}{z} \right)
 \end{aligned}$$

est bijective.

Solution 7.28 Tout $z \in \mathbb{C} \setminus D(0, 1)$ s'écrit $z = \rho e^{i\theta}$ avec $\rho > 1$ et :

$$\begin{aligned}
 \varphi(z) &= \frac{1}{2} \left(\rho e^{i\theta} + \frac{1}{\rho} e^{-i\theta} \right) \\
 &= \frac{1}{2} \left(\left(\rho + \frac{1}{\rho} \right) \cos(\theta) + i \left(\rho - \frac{1}{\rho} \right) \sin(\theta) \right)
 \end{aligned}$$

Si $\varphi(z)$ est réel, nécessairement $\sin(\theta) = 0$, donc $\cos(\theta) = \pm 1$ et :

$$|\varphi(z)| = \frac{\rho^2 + 1}{2\rho} = \frac{(\rho - 1)^2 + 2\rho}{2\rho} > \frac{2\rho}{2\rho} = 1.$$

On a donc bien $\varphi(z) \in \mathbb{C} \setminus [-1, 1]$ pour tout $z \in \mathbb{C} \setminus D(0, 1)$.

Il s'agit maintenant de montrer que pour tout $Z \in \mathbb{C} \setminus [-1, 1]$ l'équation $\frac{1}{2} \left(z + \frac{1}{z} \right) = Z$ a une unique solution $z \in \mathbb{C} \setminus D(0, 1)$. Cette équation est équivalente à l'équation de degré 2 :

$$z^2 - 2Zz + 1 = 0$$

Le discriminant réduit de cette équation est $\delta' = Z^2 - 1 \neq 0$, ce qui donne deux solutions distinctes $z_1 = \rho_1 e^{i\theta_1}$ et $z_2 = \rho_2 e^{i\theta_2}$ dans \mathbb{C} . De $z_1 z_2 = 1$, on déduit que $\rho_1 \rho_2 e^{i(\theta_1 + \theta_2)} = 1$, donc que $e^{i(\theta_1 + \theta_2)}$ est réel positif et $\theta_1 + \theta_2 \equiv 0$ modulo 2π . On a donc $z_1 = \rho_1 e^{i\theta_1}$ et $z_2 = \frac{1}{\rho_1} e^{-i\theta_1}$. Si $\rho_1 = 1$, on a alors :

$$2Z = z_1 + z_2 = e^{i\theta_1} + e^{-i\theta_1} = 2 \cos(\theta_1)$$

et $Z = \cos(\theta_1) \in [-1, 1]$, ce qui n'est pas. On a donc $\rho_1 \neq 1$, de sorte que $z_1 \in \mathbb{C} \setminus D(0, 1)$ et $z_2 \notin \mathbb{C} \setminus D(0, 1)$ pour $\rho_1 > 1$, ou $z_2 \in \mathbb{C} \setminus D(0, 1)$ et $z_1 \notin \mathbb{C} \setminus D(0, 1)$ pour $\rho_1 < 1$. Il y a donc une unique racine dans $\mathbb{C} \setminus D(0, 1)$.

L'écriture polaire des nombres complexes non nuls peut aussi être utilisée pour résoudre des équations de la forme $a \cos(x) + b \sin(x) = 0$. Pour ce faire, on utilise le résultat suivant.

Théorème 7.16 Soient a, b des réels non tous deux nuls (c'est-à-dire que $(a, b) \neq (0, 0)$). Il existe un unique couple (ρ, θ) de réels dans $\mathbb{R}^{+,*} \times [-\pi, \pi[$ tel que :

$$\forall x \in \mathbb{R}, a \cos(x) + b \sin(x) = \rho \cos(x - \theta).$$

ρ est le module de $u = a + ib$ et θ son argument principal.

Démonstration. Comme $(a, b) \neq (0, 0)$, on a $u = a + ib \neq 0$ et ce nombre complexe s'écrit de manière unique $u = \rho e^{i\theta}$ avec $\rho = |u| = \sqrt{a^2 + b^2} > 0$ et $\theta \in [-\pi, \pi[$. Pour tout réel x , on a alors d'un part :

$$\begin{aligned} u e^{-ix} &= (a + ib) (\cos(x) - i \sin(x)) \\ &= a \cos(x) + b \sin(x) + i(b \cos(x) - a \sin(x)) \end{aligned}$$

et d'autre part :

$$u e^{-ix} = \rho e^{i(\theta-x)} = \rho \cos(\theta - x) + i \rho \sin(\theta - x)$$

ce qui donne :

$$a \cos(x) + b \sin(x) = \rho \cos(\theta - x) = \rho \cos(x - \theta)$$

et aussi :

$$a \sin(x) - b \cos(x) = \rho \sin(x - \theta).$$

Pour ce qui est de l'unicité, supposons que (ρ', θ') soit une autre solution à notre problème. On a alors, pour tout réel x :

$$\rho \cos(x - \theta) = \rho' \cos(x - \theta').$$

Prenant $x = \theta$ [resp. $x = \theta'$], on en déduit que $\rho = \rho' \cos(\theta - \theta') \leq \rho'$ [resp. $\rho' = \rho \cos(\theta' - \theta) \leq \rho$] et $\rho = \rho'$.

Prenant $x = 0$ [resp. $x = \frac{\pi}{2}$], on a $\cos(\theta) = \cos(\theta')$ [resp. $\cos(\frac{\pi}{2} - \theta) = \sin(\theta) = \cos(\frac{\pi}{2} - \theta') = \sin(\theta')$] avec θ, θ' dans $[-\pi, \pi[$, ce qui équivaut à $\theta = \theta'$. ■

Corollaire 7.3 Soient a, b des réels non tous deux nuls. Les solutions de l'équation :

$$a \cos(x) + b \sin(x) = 0 \tag{7.3}$$

sont les réels :

$$x = \theta + \frac{\pi}{2} + k\pi$$

où $\theta \in [-\pi, \pi[$ est l'argument principal de $a + ib$ et k un entier relatif.

Démonstration. Le théorème précédent nous que l'équation (7.3) est équivalente à $\cos(x - \theta) = 0$, soit à $(x - \theta) \equiv \frac{\pi}{2} \pmod{\pi}$, encore équivalent à dire que $x = \theta + \frac{\pi}{2} + k\pi$ avec $k \in \mathbb{Z}$. ■

Les formules suivantes, valables pour $\theta \in \mathbb{R}$ et $n \in \mathbb{Z}$:

$$\begin{cases} \cos(\theta) = \Re(e^{i\theta}) = \frac{e^{i\theta} + e^{-i\theta}}{2} \\ \sin(\theta) = \Im(e^{i\theta}) = \frac{e^{i\theta} - e^{-i\theta}}{2i} \end{cases}$$

(formules d'Euler) et :

$$(\cos(\theta) + i \sin(\theta))^n = (e^{i\theta})^n = e^{in\theta} = \cos(n\theta) + i \sin(n\theta)$$

(formule de Moivre) permettent d'obtenir relativement facilement des formules de trigonométrie.

En utilisant la formule du binôme de Newton, la formule de Moivre s'écrit :

$$\cos(n\theta) + i \sin(n\theta) = \sum_{k=0}^n C_n^k \cos^k(\theta) \sin^{n-k}(\theta) i^{n-k}$$

et l'identification des parties réelles et imaginaires nous permet d'exprimer $\cos(n\theta)$ et $\sin(n\theta)$ comme combinaisons linéaires de puissances de $\cos(\theta)$ et $\sin(\theta)$.

Exercice 7.29 Exprimer $\cos(4\theta)$ et $\sin(4\theta)$ comme combinaisons linéaires de puissances de $\cos(\theta)$ et $\sin(\theta)$.

Solution 7.29 On a :

$$\begin{aligned} \cos(4\theta) + i \sin(4\theta) &= e^{i4\theta} = (e^{i\theta})^4 = (\cos(\theta) + i \sin(\theta))^4 \\ &= \cos^4(\theta) + 4 \cos^3(\theta) \sin(\theta) i - 6 \cos^2(\theta) \sin^2(\theta) \\ &\quad - 4 \cos(\theta) \sin^3(\theta) i + \sin^4(\theta) \end{aligned}$$

et en conséquence :

$$\begin{aligned} \cos(4\theta) &= \cos^4(\theta) - 6 \cos^2(\theta) \sin^2(\theta) + \sin^4(\theta) \\ &= (\cos^2(\theta) + \sin^2(\theta))^2 - 8 \cos^2(\theta) \sin^2(\theta) \\ &= 1 - 8 \cos^2(\theta) \sin^2(\theta) \end{aligned}$$

et :

$$\begin{aligned} \sin(4\theta) &= 4 (\cos^3(\theta) \sin(\theta) - \cos(\theta) \sin^3(\theta)) \\ &= 4 \cos(\theta) \sin(\theta) (\cos^2(\theta) - \sin^2(\theta)) \end{aligned}$$

L'utilisation des formules d'Euler et de la formule du binôme de Newton nous permet d'exprimer des puissances $\cos(\theta)$ et $\sin(\theta)$ comme combinaisons linéaires de $\cos(p\theta)$ et $\sin(q\theta)$. On dit qu'on linéarise $\cos^n(\theta)$ ou $\sin^m(\theta)$, n et m étant des entiers naturels.

Pour ce faire, on écrit que :

$$\begin{aligned} \cos^n(\theta) &= \frac{1}{2^n} (e^{i\theta} + e^{-i\theta})^n = \frac{1}{2^n} \sum_{k=0}^n C_n^k e^{ik\theta} e^{-i(n-k)\theta} \\ &= \frac{1}{2^n} \sum_{k=0}^n C_n^k e^{i(2k-n)\theta} \\ &= \frac{1}{2^n} \sum_{k=0}^n C_n^k \cos((2k-n)\theta) + i \frac{1}{2^n} \sum_{k=0}^n C_n^k \sin((2k-n)\theta) \end{aligned}$$

et nécessairement :

$$\cos^n(\theta) = \frac{1}{2^n} \sum_{k=0}^n C_n^k \cos((2k-n)\theta). \quad (7.4)$$

On peut remarquer que l'on a aussi :

$$\sum_{k=0}^n C_n^k \sin((2k-n)\theta) = 0.$$

En réalité cette formule est évidente. Par exemple, pour $n = 2p$, le changement d'indice $k = 2p - j$ nous permet d'écrire la deuxième moitié de cette somme sous la forme :

$$\begin{aligned} \sum_{k=p+1}^{2p} C_{2p}^k \sin((2k - 2p)\theta) &= \sum_{j=0}^{p-1} C_{2p}^{2p-j} \sin((2p - 2j)\theta) \\ &= - \sum_{j=0}^p C_{2p}^j \sin((2j - 2p)\theta) \\ &= - \sum_{k=0}^p C_n^k \sin((2k - n)\theta) \end{aligned}$$

La vérification étant analogue pour n impair.

La parité de $\cos^p(\theta)$ peut aussi justifier l'absence de termes en $\sin(q\theta)$ dans la formule (7.4).

Exercice 7.30 Linéariser $\cos^4(\theta)$ et $\sin^4(\theta)$.

Solution 7.30 On a :

$$\begin{aligned} \cos^4(\theta) &= \frac{1}{16} (e^{i\theta} + e^{-i\theta})^4 \\ &= \frac{1}{16} (e^{4i\theta} + 4e^{3i\theta}e^{-i\theta} + 6e^{2i\theta}e^{-2i\theta} + 4e^{i\theta}e^{-3i\theta} + e^{-4i\theta}) \\ &= \frac{1}{16} (e^{4i\theta} + e^{-4i\theta} + 4(e^{2i\theta} + e^{-2i\theta}) + 6) \\ &= \frac{1}{8} \cos(4\theta) + \frac{1}{2} \cos(2\theta) + \frac{3}{8} \end{aligned}$$

et :

$$\begin{aligned} \sin^4(\theta) &= \frac{1}{16} (e^{i\theta} - e^{-i\theta})^4 \\ &= \frac{1}{16} (e^{4i\theta} - 4e^{3i\theta}e^{-i\theta} + 6e^{2i\theta}e^{-2i\theta} - 4e^{i\theta}e^{-3i\theta} + e^{-4i\theta}) \\ &= \frac{1}{16} (e^{4i\theta} + e^{-4i\theta} - 4(e^{2i\theta} + e^{-2i\theta}) + 6) \\ &= \frac{1}{8} \cos(4\theta) - \frac{1}{2} \cos(2\theta) + \frac{3}{8} \end{aligned}$$

On peut aussi exprimer $\tan(n\theta)$ en fonction de $\tan(\theta)$ pour tout entier naturel n .

Exercice 7.31 Exprimer $\tan(4\theta)$ en fonction de $\tan(\theta)$.

Solution 7.31 On a :

$$\tan(4\theta) = \frac{\sin(4\theta)}{\cos(4\theta)} = 4 \frac{\cos^3(\theta) \sin(\theta) - \cos(\theta) \sin^3(\theta)}{\cos^4(\theta) - 6 \cos^2(\theta) \sin^2(\theta) + \sin^4(\theta)}$$

et divisant numérateur et dénominateur par $\cos^4(\theta)$, on obtient :

$$\tan(4\theta) = 4 \tan(\theta) \frac{1 - \tan^2(\theta)}{1 - 6 \tan^2(\theta) + \tan^4(\theta)}.$$

7.7 Racines n -ièmes d'un nombre complexe

La représentation des nombres complexes nous sera très utile pour résoudre des équations de la forme $x^n = \alpha$.

On rappelle que pour tout entier naturel non nul n , la fonction $f : x \mapsto x^n$ réalise une bijection de \mathbb{R}^+ sur lui-même. L'application réciproque de f est notée $x \mapsto \sqrt[n]{x}$ ou $x \mapsto x^{\frac{1}{n}}$ et on l'appelle fonction racine n -ième. Donc pour tout réel positif a , l'unique solution de l'équation $x^n = a$ est le réel positif $\sqrt[n]{a}$.

On rappelle que si $z = re^{it}$ avec $r > 0$ et $t \in \mathbb{R}$, on a pour tout entier relatif n , $z^n = r^n e^{int}$ et pour $z' = r' e^{it'}$ avec $r' > 0$ et $t' \in \mathbb{R}$, l'égalité $z = z'$ est réalisée si, et seulement si $r = r'$ et $t \equiv t' \pmod{2\pi}$.

Dans le cas où $n = 2$ et $\alpha \neq 0$, on écrit $\alpha = \rho e^{i\theta}$ avec $\rho > 0$ et $\theta \in [-\pi, \pi[$ et on cherche $z = re^{it}$ avec $r > 0$ et $t \in [-\pi, \pi[$ tel que :

$$z^2 = r^2 e^{2it} = \rho e^{i\theta}$$

ce qui équivaut à $r^2 = \rho$ et $2t = \theta + 2k\pi$ avec $k \in \mathbb{Z}$. On a donc $r = \sqrt{\rho}$ et $t = \frac{\theta}{2} + k\pi$ avec $k \in \mathbb{Z}$, ce qui donne $z = \sqrt{\rho} e^{i\frac{\theta}{2}} e^{ik\pi}$ et α a deux racines carrées qui sont :

$$z_1 = \sqrt{\rho} e^{i\frac{\theta}{2}} \text{ et } z_2 = \sqrt{\rho} e^{i\frac{\theta}{2}} e^{i\pi} = -z_1.$$

Définition 7.8 *Étant donné un nombre complexe α et un entier naturel non nul n , on appelle racine n -ième de α tout nombre complexe z tel que $z^n = \alpha$.*

Remarque 7.1 *Si $\alpha = 0$, l'équation $z^n = \alpha$ équivaut à $z = 0$, c'est-à-dire que 0 est l'unique racine n -ième de 0.*

Si $\alpha \neq 0$, une racine n -ième de α est nécessairement non nulle.

Remarque 7.2 *Si α est un nombre complexe non nul, il s'écrit $\alpha = \rho e^{i\theta}$ avec $\rho > 0$ et $\theta \in [-\pi, \pi[$ (ou $\theta \in \mathbb{R}$ si on se contente d'un quelconque argument de α) et le nombre complexe $z_0 = \sqrt[n]{\rho} e^{i\frac{\theta}{n}}$ nous fournit une solution de l'équation $z^n = \alpha$. Pour tout autre solution z de cette équation on aura $z^n = z_0^n$, soit $\left(\frac{z}{z_0}\right)^n = 1$ et la connaissance de toutes les racines n -ièmes de 1 nous fournira toutes les racines n -ièmes de α .*

Définition 7.9 *Étant donné un entier naturel non nul n , on appelle racine n -ième de l'unité toute racine n -ième de 1.*

Théorème 7.17 *Soit n un entier naturel non nul. Il y a exactement n racines n -ièmes de l'unité qui sont données par :*

$$\omega_k = e^{\frac{2ik\pi}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) \quad (0 \leq k \leq n-1)$$

Démonstration. Si $z^n = 1$, on a alors $|z|^n = |z^n| = 1$, donc $|z| = 1$ (c'est l'unique racine n -ième réelle positive de 1) et $z = e^{i\theta}$ avec $\theta \in \mathbb{R}$. L'équation $z^n = 1$ équivaut alors à $e^{in\theta} = 1$, encore équivalent à $n\theta \equiv 0 \pmod{2\pi}$. Les racines n -ièmes de l'unité sont donc les nombres complexes $e^{\frac{2ik\pi}{n}}$ où k décrit l'ensemble \mathbb{Z} des entiers relatifs. En effectuant la division euclidienne par n , tout entier k s'écrit $k = qn + r$ avec $0 \leq r \leq n-1$ et $e^{\frac{2ik\pi}{n}} = e^{\frac{2ir\pi}{n}} = \omega_r$. De plus pour j, k entiers compris entre 0 et $n-1$, l'égalité $\omega_j = \omega_k$ est équivalente à $e^{\frac{2i(j-k)\pi}{n}} = 1$, encore

équivalent à $\frac{2(j-k)\pi}{n} \equiv 0 \text{ modulo } 2\pi$, ce qui revient à dire que $j-k$ est divisible par n , soit $j-k = qn$ et avec $|j-k| \leq n-1$ (puisque j et k sont dans l'intervalle $[0, n-1]$), on déduit que $q = 0$ est la seule possibilité, ce qui signifie que $j = k$. On a donc bien le résultat annoncé. ■

Le théorème précédent peut aussi s'énoncer comme suit.

Théorème 7.18 *Pour tout entier naturel non nul n et tout nombre complexe z , on a :*

$$z^n - 1 = \prod_{k=0}^{n-1} (z - \omega_k)$$

où les $\omega_k = e^{\frac{2ik\pi}{n}}$, pour k compris entre 0 et $n-1$, sont les racines n -ièmes de l'unité.

Démonstration. Le polynôme $P(z) = z^n - 1 - \prod_{k=0}^{n-1} (z - \omega_k)$ est nul ou de degré au plus égal à $n-1$ (le coefficient dominant de $\prod_{k=0}^{n-1} (z - \omega_k)$ est z^n) et s'annule en n points distincts (les ω_k), c'est donc le polynôme nul. ■

Exemple 7.1 *Les racines cubiques de l'unité sont :*

$$\begin{cases} \omega_0 = 1, \\ \omega_1 = e^{\frac{2i\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ \omega_2 = e^{\frac{4i\pi}{3}} = e^{-\frac{2i\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) - i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \end{cases}$$

La racine ω_1 est usuellement notée j et $\omega_2 = \bar{j}$.

Corollaire 7.4 *Soit n un entier naturel non nul. Tout nombre complexe non nul $\alpha = \rho e^{i\theta}$ a exactement n racines n -ièmes données par :*

$$u_k = u_0 \omega_k = \sqrt[n]{\rho} e^{i\frac{\theta}{n}} e^{\frac{2ik\pi}{n}} \quad (0 \leq k \leq n-1)$$

Exercice 7.32 *Résoudre dans \mathbb{C} l'équation $z^6 = (\bar{z})^2$. Combien l'équation a-t-elle de solutions ?*

Solution 7.32 *On voit que $z = 0$ est solution.*

Si $z^6 = (\bar{z})^2$ avec $z \neq 0$, alors $|z| = 1$, donc $z = e^{i\theta}$ et $e^{i8\theta} = 1$, soit $\theta = \frac{2k\pi}{8}$ avec $k \in \mathbb{Z}$, ce qui donne les 8 solutions $e^{i\frac{k\pi}{4}}$ où $k \in \{0, 1, \dots, 7\}$. Donc 9 solutions au total.

Exercice 7.33 *Résoudre dans \mathbb{C} l'équation $z^4 = (\bar{z})^4$.*

Solution 7.33 *On voit que $z = 0$ est solution.*

Pour $z \neq 0$, on écrit que $z = \rho e^{i\theta}$ avec $\rho > 0$ et $\theta \in [0, 2\pi[$ et de $z^4 = (\bar{z})^4$, on déduit que $e^{i8\theta} = 1$, soit $\theta = \frac{2k\pi}{8}$ avec $k \in \{0, 1, \dots, 7\}$. Les solutions non nulles de cette équation sont donc les nombres complexes de la forme $\rho e^{i\frac{k\pi}{4}}$ où ρ est un réel strictement positif et k est un entier compris entre 0 et 7. L'ensemble S des solutions est donc infini, c'est la réunion des quatre droites D_k d'équation polaire $\theta = k\frac{\pi}{4}$ où k est entier compris entre 0 et 3. D_0 est l'axe des x , D_1 la diagonale d'équation $y = x$, D_2 l'axe des y et D_3 la diagonale d'équation $y = -x$.

Exercice 7.34 Déterminer, pour n entier naturel non nul, toutes les racines n -ièmes de -1 .

Solution 7.34 Il s'agit de résoudre l'équation $z^n = -1 = e^{i\pi}$. Les solutions de cette équation sont les :

$$u_k = e^{(2k+1)\frac{i\pi}{n}} \quad (0 \leq k \leq n-1)$$

Exercice 7.35 En notant, pour n entier naturel non nul, $(\omega_k)_{0 \leq k \leq n-1}$ la suite de toutes les racines n -ièmes de l'unité, montrer que pour $n \geq 2$, on a $\sum_{k=0}^{n-1} \omega_k = 0$ et $\prod_{k=0}^{n-1} \omega_k = (-1)^{n-1}$.

Solution 7.35 On a :

$$\sum_{k=0}^{n-1} \omega_k = \sum_{k=0}^{n-1} \omega_1^k = \frac{1 - \omega_1^n}{1 - \omega_1} = 0$$

(pour $n \geq 2$, on a bien $\omega_1 = e^{\frac{2i\pi}{n}} \neq 1$) et :

$$\begin{aligned} \prod_{k=0}^{n-1} \omega_k &= \prod_{k=0}^{n-1} \omega_1^k = \omega_1^{\sum_{k=0}^{n-1} k} = \omega_1^{\frac{n(n-1)}{2}} \\ &= \left(e^{\frac{2i\pi}{n}} \right)^{\frac{n(n-1)}{2}} = e^{\frac{n(n-1)}{2} \frac{2i\pi}{n}} = e^{i(n-1)\pi} = (e^{i\pi})^{n-1} = (-1)^{n-1} \end{aligned}$$

($m = \frac{n(n-1)}{2}$ étant entier, on a bien $(e^{i\theta})^m = e^{im\theta}$). De la première identité, on déduit que :

$$\sum_{k=0}^{n-1} \cos\left(\frac{2k\pi}{n}\right) = \sum_{k=0}^{n-1} \sin\left(\frac{2k\pi}{n}\right) = 0.$$

Remarque 7.3 La parenthèse ($m = \frac{n(n-1)}{2}$ étant entier ...) est due à la remarque du pointilleux lecteur qui voudrait montrer que $-1 = 1$ comme suit :

$$(1 = e^{2i\pi}) \Rightarrow \left(1 = 1^{\frac{1}{2}} = (e^{2i\pi})^{\frac{1}{2}} = e^{\frac{1}{2}2i\pi} = e^{i\pi} = -1 \right)$$

Exercice 7.36 Montrer que, pour tout entier $n \geq 1$, l'ensemble des racines $2n$ -ièmes de l'unité est aussi donnée par :

$$\Gamma_{2n} = \{-1, 1\} \cup \left\{ e^{\frac{ik\pi}{n}} \mid 1 \leq k \leq n-1 \right\} \cup \left\{ e^{\frac{-ik\pi}{n}} \mid 1 \leq k \leq n-1 \right\}$$

En déduire que, pour tout nombre complexe z , on a :

$$z^{2n} - 1 = (z^2 - 1) \prod_{k=1}^{n-1} \left(z^2 - 2 \cos\left(\frac{k\pi}{n}\right) z + 1 \right).$$

Solution 7.36 Ces racines $2n$ -ièmes sont les :

$$\omega_k = e^{\frac{2ik\pi}{2n}} = e^{\frac{ik\pi}{n}} \quad (0 \leq k \leq 2n-1).$$

Pour $k = 0$, on a $\omega_0 = 1$, pour $k = n$, on a $\omega_n = e^{i\pi} = -1$ et pour $k = 2n - j$ compris entre $n+1$ et $2n-1$, on a :

$$\omega_k = e^{\frac{i\{2n-j\}\pi}{n}} = e^{\frac{-ij\pi}{n}}$$

ce qui donne le résultat attendu.

On a donc, pour tout nombre complexe z :

$$\begin{aligned} z^{2n} - 1 &= (z - 1)(z + 1) \prod_{k=1}^{n-1} \left(z - e^{i\frac{k\pi}{n}} \right) \left(z - e^{-i\frac{k\pi}{n}} \right) \\ &= (z^2 - 1) \prod_{k=1}^{n-1} \left(z^2 - \left(e^{i\frac{k\pi}{n}} + e^{-i\frac{k\pi}{n}} \right) z + 1 \right) \\ &= (z^2 - 1) \prod_{k=1}^{n-1} \left(z^2 - 2 \cos \left(\frac{k\pi}{n} \right) z + 1 \right) \end{aligned}$$

Exercice 7.37 Résoudre dans \mathbb{C} l'équation $z^8 + z^4 + 1 = 0$.

Solution 7.37 Si z est solution de cette équation, alors $t = z^4$ est solution de $t^2 + t + 1 = 0$, ce qui donne $t \neq 1$ et $\frac{t^3 - 1}{t - 1} = 0$, donc $t = j = e^{\frac{2i\pi}{3}}$ ou $t = \bar{j} = j^2$.

Il s'agit alors de calculer les racines quatrièmes de j et de \bar{j} , ces racines sont les :

$$z_k = e^{i(\frac{\pi}{6} + k\frac{\pi}{2})} \text{ et } \bar{z}_k = e^{-i(\frac{\pi}{6} + k\frac{\pi}{2})} \quad (0 \leq k \leq 3)$$

soit :

$$\begin{aligned} z_0 &= e^{i\frac{\pi}{6}} = \frac{\sqrt{3}}{2} + \frac{i}{2}, \quad z_1 = e^{2i\frac{\pi}{3}} = j = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ z_2 &= e^{7i\frac{\pi}{6}} = -z_1, \quad z_3 = e^{5i\frac{\pi}{3}} = -z_1 \end{aligned}$$

et leurs conjugués.

On peut aussi procéder comme suit. Si z est solution de cette équation, il est alors non nul et $z^4 + 1 + \frac{1}{z^4} = 0$, soit $\left(z^2 + \frac{1}{z^2}\right)^2 = 1$, donc $z^2 + \frac{1}{z^2} = \pm 1$, soit $\left(z + \frac{1}{z}\right)^2 - 2 = \pm 1$, c'est-à-dire $\left(z + \frac{1}{z}\right)^2 = 1$ ou $\left(z + \frac{1}{z}\right)^2 = 3$.

Si $\left(z + \frac{1}{z}\right)^2 = 1$, on a alors $z + \frac{1}{z} = \pm 1$, soit $z^2 \pm z + 1 = 0$ avec $z \neq \pm 1$ ou encore $\frac{z^3 \pm 1}{z \pm 1} = 0$, ce qui donne les 4 solutions, $j, \bar{j}, -j, -\bar{j}$.

Si $\left(z + \frac{1}{z}\right)^2 = 3$, on a alors $z + \frac{1}{z} = \pm\sqrt{3}$, soit $z^2 \pm \sqrt{3}z + 1 = 0$ ou encore $\left(z \pm \frac{\sqrt{3}}{2}\right)^2 = -\frac{1}{4}$,

ce qui donne les 4 autres solutions, $z_0 = \frac{\sqrt{3}}{2} + \frac{i}{2}, \bar{z}_0, -z_0, -\bar{z}_0$.

Deuxième partie

Algèbre linéaire et bilinéaire sur \mathbb{R} ou \mathbb{C}

Espaces vectoriels réels ou complexes

On notera \mathbb{K} le corps de réels ou des complexes, en précisant quand cela sera nécessaire s'il s'agit de \mathbb{R} ou \mathbb{C} . Par scalaire on entend réel ou complexe.

8.1 L'espace vectoriel \mathbb{K}^n

On peut utiliser les nombres réels $x \in \mathbb{R}$ pour représenter tous les points d'une droite, les couples de réels $(x, y) \in \mathbb{R}^2$ pour représenter tous les points d'un plan et les triplets de réels $(x, y, z) \in \mathbb{R}^3$ pour représenter tous les points d'un espace.

De manière plus générale, étant donné un entier naturel non nul n , on appelle vecteur tout élément du produit cartésien $\mathbb{K}^n = \mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}$ (répété n fois). Ces vecteurs sont des

listes ordonnées de n scalaires x_1, x_2, \dots, x_n et seront notés $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ ou plus simplement

$x = (x_i)_{1 \leq i \leq n}$ et on dit que les x_i sont les composantes du vecteur x .

La représentation sous forme de vecteurs colonnes sera justifiée plus loin par l'utilisation du calcul matriciel.

On peut naturellement munir cet ensemble d'une opération interne d'addition notée $+$ et définie par :

$$\forall x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n, \forall y = (y_i)_{1 \leq i \leq n} \in \mathbb{K}^n, x + y = (x_i + y_i)_{1 \leq i \leq n}$$

On dit que cette opération est interne car elle associe à deux éléments x et y de \mathbb{K}^n un élément $x + y$ de \mathbb{K}^n .

Des propriétés de l'addition des scalaires, on déduit facilement que cette opération d'addition vérifie les propriétés suivantes :

- (i) elle est commutative, ce qui signifie que pour tous vecteurs x et y , on a $x + y = y + x$;
- (ii) elle est associative, ce qui signifie que pour tous vecteurs x, y et z , on a $x + (y + z) = (x + y) + z$;

- (iii) le vecteur nul $0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ est un élément neutre pour cette addition, ce qui signifie que pour tout vecteur x on a $x + 0 = 0 + x = x$;

(iv) pour tout vecteur $x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n$, le vecteur $x' = (-x_i)_{1 \leq i \leq n}$ est tel que $x + x' = x' + x = 0$, on dit que x' est un opposé de x et on le note $-x$.

Tout cela se résume en disant que l'ensemble \mathbb{K}^n muni de l'addition, que l'on note $(\mathbb{K}^n, +)$, est un groupe commutatif (voir le chapitre 20).

De même, on peut naturellement munir \mathbb{K}^n d'une multiplication externe définie par :

$$\forall \lambda \in \mathbb{K}, \forall x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n, \lambda \cdot x = (\lambda \cdot x_i)_{1 \leq i \leq n}$$

On dit que cette opération est externe car elle associe à un scalaire λ (en dehors de \mathbb{K}^n) et à un élément x de \mathbb{K}^n un élément $\lambda \cdot x$ de \mathbb{K}^n .

On écrira plus simplement λx pour $\lambda \cdot x$.

Là encore des propriétés de l'addition et de la multiplication des scalaires, on déduit que cette opération externe vérifie les propriétés suivantes :

- (v) pour tout scalaire λ et tous vecteurs x et y , on a $\lambda(x + y) = \lambda x + \lambda y$;
- (vi) pour tous scalaires λ, μ et tout vecteur x , on a $(\lambda + \mu)x = \lambda x + \mu x$;
- (vii) pour tous scalaires λ, μ et tout vecteur x , on a $\lambda(\mu x) = (\lambda\mu)x$;
- (viii) pour tout vecteur x , on a $1 \cdot x = x$.

Tout cela se résume en disant que l'ensemble \mathbb{K}^n muni de cette addition interne et de cette multiplication externe, que l'on note $(\mathbb{K}^n, +, \cdot)$, est un \mathbb{K} -espace vectoriel, ou simplement un espace vectoriel, le corps \mathbb{K} étant sous-entendu.

8.2 Définition d'un espace vectoriel réel ou complexe

De manière plus générale, on donne la définition suivante.

Définition 8.1 On appelle \mathbb{K} -espace vectoriel tout ensemble non vide E muni d'une addition interne $(x, y) \in E \times E \mapsto x + y \in E$ et d'une multiplication externe $(\lambda, x) \in \mathbb{K} \times E \mapsto \lambda x \in E$ vérifiant les propriétés (i) à (viii) précédentes.

Pour simplifier, on dira espace vectoriel pour \mathbb{K} -espace vectoriel. Quand cela sera nécessaire, on précisera espace vectoriel réel (i. e. pour $\mathbb{K} = \mathbb{R}$) ou espace vectoriel complexe (i. e. pour $\mathbb{K} = \mathbb{C}$).

Les éléments d'un espace vectoriel sont appelés vecteurs.

Dans un espace vectoriel l'élément neutre pour l'addition est noté 0 et on dit que c'est le vecteur nul et le symétrique d'un vecteur x est noté $-x$ et on dit que c'est l'opposé de x .

On vérifie facilement que le neutre 0 est unique, c'est-à-dire que c'est l'unique élément e de E tel que $x + e = e + x = x$ pour tout $x \in E$ (on a $e = e + 0$ puisque 0 est neutre et $e + 0 = 0$ puisque e est neutre, donc $e = 0$), que pour tout $x \in E$ l'opposé $-x$ est unique (si x' est un autre opposé, de $x + x' = 0$, on déduit que $(-x) + (x + x') = x' = (-x) + 0 = -x$) et que tout élément de E est simplifiable, c'est-à-dire que pour tous x, y, z dans E l'égalité $x + y = x + z$ équivaut à $y = z$ (il suffit d'ajouter $-x$ aux deux membres de cette égalité).

Pour x, y dans E , la somme $x + (-y)$ est simplement notée $x - y$.

Exemple 8.1 L'ensemble \mathbb{C} des nombres complexes est un espace vectoriel réel et aussi un espace vectoriel complexe.

Exemple 8.2 On rappelle qu'une suite réelle est une application u définie sur \mathbb{N} et à valeurs réelles. L'ensemble de toutes les suites réelles est un espace vectoriel réel.

Exemple 8.3 Plus généralement, étant donné une partie I non vide de \mathbb{R} , l'ensemble E de toutes les applications de I dans \mathbb{R} (resp. dans \mathbb{C}) est un espace vectoriel réel (resp. complexe).

Exemple 8.4 L'ensemble noté $\mathbb{R}[x]$ des fonctions polynomiales réelles (on dira plus simplement polynômes réel), c'est-à-dire l'ensemble des fonctions P définies par $P(x) = \sum_{k=0}^n a_k x^k$ pour tout réel x , où les coefficients a_k sont réels, est un espace vectoriel réel. Même chose sur \mathbb{C} .

Exemple 8.5 L'ensemble \mathcal{F} des polynômes trigonométriques, c'est-à-dire l'ensemble des fonctions P définies par $P(x) = \sum_{k=0}^n (a_k \cos(kx) + b_k \sin(kx))$ pour tout réel x , où les coefficients a_k et b_k sont réels, est un espace vectoriel réel.

Exercice 8.1 Montrer que dans un espace vectoriel E , l'égalité $\lambda x = 0$ où λ est un scalaire et x un vecteur est équivalente à $\lambda = 0$ ou $x = 0$.

Solution 8.1 Pour tout vecteur x , on a :

$$0 \cdot x + x = 0 \cdot x + 1 \cdot x = (0 + 1)x = 1 \cdot x = x$$

et simplifiant par x (ce qui revient à ajouter $-x$ aux deux membres de cette égalité), on aboutit à $0 \cdot x = 0$.

De même, pour tout scalaire λ , on a :

$$\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$$

et simplifiant par $\lambda \cdot 0$, on aboutit à $\lambda \cdot 0 = 0$.

Supposons que $\lambda x = 0$. Si $\lambda = 0$ c'est terminé, sinon λ est inversible dans \mathbb{K} et :

$$x = 1 \cdot x = \left(\frac{1}{\lambda}\lambda\right)x = \frac{1}{\lambda}(\lambda x) = \frac{1}{\lambda}0 = 0.$$

Exercice 8.2 Montrer que dans un espace vectoriel E , on a $(-1)x = -x$ pour tout vecteur x .

Solution 8.2 Pour tout vecteur x , on a :

$$x + (-1)x = 1 \cdot x + (-1)x = (1 - 1)x = 0 \cdot x = 0$$

et $(-1)x = -x$ puisque l'opposé de x est unique.

Définition 8.2 Soient E un espace vectoriel, n un entier naturel non nul et x, y, x_1, \dots, x_n des éléments de E .

On dit que y est colinéaire à x s'il existe un scalaire λ tel que $y = \lambda x$.

Plus généralement, on dit que y est combinaison linéaire de x_1, \dots, x_n s'il existe des scalaires $\lambda_1, \dots, \lambda_n$ tels que $y = \sum_{k=1}^n \lambda_k x_k$.

On peut remarquer que, par définition, un espace vectoriel est stable par combinaison linéaire, c'est-à-dire que si x_1, \dots, x_n sont dans E et $\lambda_1, \dots, \lambda_n$ dans \mathbb{K} , alors la combinaison linéaire $\sum_{k=1}^n \lambda_k x_k$ est encore dans E .

En s'inspirant de la construction l'espace vectoriel \mathbb{K}^n comme produit cartésien de p exemplaires de l'espace vectoriel \mathbb{K} , on vérifie facilement que le produit cartésien $F = F_1 \times \dots \times F_p$ de p espaces vectoriels F_1, \dots, F_p est naturellement muni d'une structure d'espace vectoriel avec les lois définies par :

$$\begin{cases} x + y = (x_1 + y_1, \dots, x_p + y_p) \\ \lambda x = (\lambda x_1, \dots, \lambda x_p) \end{cases}$$

où $x = (x_1, \dots, x_p)$, $y = (y_1, \dots, y_p)$ sont deux éléments de F et λ un scalaire.

8.3 Sous-espaces vectoriels

Définition 8.3 Soit E un espace vectoriel. On dit qu'une partie F de E est un sous-espace vectoriel de E si :

1. le vecteur 0 est dans F ;
2. pour tous vecteurs x, y dans F et tout scalaire λ , les vecteurs $x + y$ et λx sont dans F .

L'appellation sous-espace vectoriel est justifiée par le résultat suivant.

Théorème 8.1 Tout sous-espace vectoriel d'un espace vectoriel est un espace vectoriel.

Démonstration. Soit F un sous-espace vectoriel d'un espace vectoriel E .

Comme F contient 0 , il est non vide.

Le deuxième point de la définition nous dit que l'addition des vecteurs et la multiplication d'un vecteur par un scalaire restreintes à F y définissent bien respectivement une opération interne et externe.

L'addition des vecteurs qui est commutative sur E l'est en particulier sur F .

L'élément neutre 0 pour l'addition est bien dans F .

Tout vecteur $x \in F$ admet un opposé $-x \in E$ et en écrivant que $-x = (-1)x$, on voit que $-x$ est bien dans F .

Les propriétés (v) à (viii) vérifiées dans E le sont en particulier dans F . ■

De manière équivalente, on peut dire qu'une partie F d'un espace vectoriel E est un sous-espace vectoriel si, et seulement si, F est non vide et pour tous vecteurs x, y dans F , tous scalaires λ, μ , le vecteur $\lambda x + \mu y$ est dans F .

Exercice 8.3 Justifier l'affirmation précédente.

Solution 8.3 Laissée au lecteur.

De manière plus générale, un sous-espace vectoriel d'un espace vectoriel est une partie non vide stable par combinaison linéaire.

Exercice 8.4 Justifier l'affirmation précédente.

Solution 8.4 Laissée au lecteur.

Exemple 8.6 Si E un espace vectoriel, alors $\{0\}$ et E sont des sous-espaces vectoriels de E .

Exemple 8.7 \mathbb{R} et l'ensemble des imaginaires purs sont des sous-espaces vectoriels réels de \mathbb{C} .

Exercice 8.5 Montrer que l'intersection de deux sous-espaces vectoriels d'un espace vectoriel E est un sous-espace vectoriel. Qu'en est-il de la réunion ?

Solution 8.5 Soient F, G deux sous-espaces vectoriels de E . L'intersection $H = F \cap G$ contient 0 puisqu'ils sont dans F et G et pour tous x, y dans H , λ, μ dans \mathbb{K} , le vecteur $\lambda x + \mu y$ est dans F et G , donc dans H . En définitive, H est un sous-espace vectoriel de E .

En général la réunion de deux sous-espaces vectoriels de E n'est pas un sous-espace vectoriel.

Par exemple dans \mathbb{R}^2 , les ensembles F et G définis par $F = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \mid x \in \mathbb{R} \right\}$ (l'axe des x) et

$G = \left\{ \begin{pmatrix} 0 \\ y \end{pmatrix} \mid y \in \mathbb{R} \right\}$ (l'axe des y) sont des sous-espaces vectoriels, mais pas $F \cup G$ puisque $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ sont dans cette réunion, mais pas leur somme $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Exercice 8.6 Soient F, G deux sous-espaces vectoriels de E . Montrer que $F \cup G$ est un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

Solution 8.6 Si $F \subset G$ [resp. $G \subset F$], on a alors $F \cup G = G$ [resp. $F \cup G = F$] et c'est un sous-espace vectoriel de E .

Réciproquement supposons que $F \cup G$ soit un sous-espace vectoriel de E . Si $F \not\subset G$ et $G \not\subset F$, il existe alors $x \in F \setminus G$ et $y \in G \setminus F$, donc comme x et y sont dans $F \cup G$, il en est de même de $x + y$, mais $x + y \in F$ entraîne $y = (x + y) - x \in F$, ce qui n'est pas et $x + y \in G$ entraîne $x = (x + y) - y \in G$, ce qui n'est pas, il y a donc une impossibilité et on a nécessairement $F \subset G$ ou $G \subset F$.

Exercice 8.7 On désigne par \mathcal{F} l'espace vectoriel des fonctions de \mathbb{R} dans \mathbb{R} et par \mathcal{P} [resp. \mathcal{I}] le sous-ensemble de \mathcal{F} formés de toutes les fonctions paires [resp. impaires] de \mathbb{R} dans \mathbb{R} .

1. Montrer que \mathcal{P} et \mathcal{I} sont des sous-espaces vectoriels de \mathcal{F} .
2. Calculer $\mathcal{P} \cap \mathcal{I}$.
3. Montrer que toute fonction $f \in \mathcal{F}$, s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire. Ce résultat se traduit en disant que \mathcal{F} est somme directe des sous-espaces \mathcal{P} et \mathcal{I} et on note $\mathcal{F} = \mathcal{P} \oplus \mathcal{I}$.

Solution 8.7

1. La fonction nulle est à la fois paire et impaire donc dans \mathcal{P} et dans \mathcal{I} . Si f, g sont deux fonctions paires [resp. impaires], il en est alors de même de $f + g$ et de λf pour tout réel λ . Les ensembles \mathcal{P} et \mathcal{I} sont donc bien des sous-espaces vectoriels de \mathcal{F} .
2. Dire qu'une fonction f est dans $\mathcal{P} \cap \mathcal{I}$ signifie qu'elle est à la fois paire et impaire et donc que pour tout réel x , on a :

$$f(x) = f(-x) = -f(x)$$

ce qui revient à dire que $f(x) = 0$. On a donc $\mathcal{P} \cap \mathcal{I} = \{0\}$.

3. Pour toute fonction $f \in \mathcal{F}$, la fonction g [resp. h] définie sur \mathbb{R} par :

$$g(x) = \frac{f(x) + f(-x)}{2} \text{ [resp. } h(x) = \frac{f(x) - f(-x)}{2}]$$

est paire [resp. impaire] et $f = g + h$. Si (g', h') est un autre couple dans $\mathcal{P} \times \mathcal{I}$ tel que $f = g' + h'$, la fonction $g - g' = h' - h$ est dans $\mathcal{P} \cap \mathcal{I}$ donc nulle et $g = g'$, $h = h'$. Une telle écriture est donc unique.

Par exemple si f est la fonction \exp , les fonctions g et h sont les fonctions hyperboliques ch et sh définies par $\text{ch}(x) = \frac{e^x + e^{-x}}{2}$ et $\text{sh}(x) = \frac{e^x - e^{-x}}{2}$.

Définition 8.4 Dans l'espace \mathbb{K}^n , où n est un entier naturel non nul, on appelle droite vectorielle tout sous-ensemble de la forme :

$$D = \{\lambda a \mid \lambda \in \mathbb{K}\}$$

où a est un vecteur non nul donné.

On notera $D = \mathbb{K}a$ une telle droite.

On a donc, en notant $a = (a_k)_{1 \leq k \leq n}$, pour tout $x = (x_k)_{1 \leq k \leq n} \in \mathbb{K}^n$:

$$(x \in D) \Leftrightarrow (\exists \lambda \in \mathbb{K} \mid \forall k \in \{1, 2, \dots, n\}, x_k = \lambda a_k)$$

Une telle représentation est appelée représentation paramétrique de la droite D .

Cette définition correspond bien à la notion de droite vectorielle du plan \mathbb{R}^2 ou de l'espace \mathbb{R}^3 étudiée en Lycée.

On vérifie facilement qu'une droite de \mathbb{K}^n est un sous-espace vectoriel.

Pour $n = 1$, $D = \mathbb{K}$ est la seule droite vectorielle puisque, pour tout $a \neq 0$, tout scalaire x peut s'écrire $x = \frac{x}{a}a = \lambda a$, donc $\mathbb{K} \subset \mathbb{K}a \subset \mathbb{K}$ et $\mathbb{K} = \mathbb{K}a$.

Définition 8.5 Dans l'espace \mathbb{K}^n , où $n \geq 2$, on appelle plan vectoriel tout sous-ensemble de la forme :

$$P = \{\lambda a + \mu b \mid (\lambda, \mu) \in \mathbb{K}^2\}$$

où a et b sont deux vecteurs non colinéaires donnés.

On notera $P = \mathbb{K}a \oplus \mathbb{K}b$ un tel plan.

On a donc, en notant $a = (a_k)_{1 \leq k \leq n}$ et $b = (b_k)_{1 \leq k \leq n}$, pour tout $x = (x_k)_{1 \leq k \leq n} \in \mathbb{K}^n$:

$$(x \in P) \Leftrightarrow (\exists (\lambda, \mu) \in \mathbb{K}^2 \mid \forall k \in \{1, 2, \dots, n\}, x_k = \lambda a_k + \mu b_k)$$

Une telle représentation est appelée représentation paramétrique du plan P .

Là encore cette définition correspond bien à la notion de plan vectoriel de l'espace \mathbb{R}^3 étudiée en Lycée.

On vérifie facilement qu'un plan de \mathbb{K}^n est un sous-espace vectoriel.

Une partie finie d'un espace vectoriel E distincte de $\{0\}$ n'est pas un sous-espace vectoriel, mais à partir d'une partie finie de vecteurs de E , on peut engendrer un sous-espace vectoriel en s'inspirant des définitions de droites et plans.

Théorème 8.2 Soient E un espace vectoriel et x_1, \dots, x_n des éléments de E . L'ensemble F de toutes les combinaisons linéaires de x_1, \dots, x_n est un sous-espace vectoriel de E .

Démonstration. L'ensemble F contient $0 = \sum_{k=1}^n 0 \cdot x_k$ et pour $x = \sum_{k=1}^n \lambda_k x_k$, $y = \sum_{k=1}^n \mu_k x_k$ dans F et λ, μ dans \mathbb{K} , on a :

$$\lambda x + \mu y = \sum_{k=1}^n (\lambda \lambda_k + \mu \mu_k) x_k \in F$$

donc F est bien un sous-espace vectoriel de E . ■

Définition 8.6 Avec les notations du théorème précédent, on dit que F est le sous-espace vectoriel de E engendré par x_1, \dots, x_n et on le note $F = \langle x_1, \dots, x_n \rangle$, ou $F = \text{Vect} \{x_1, \dots, x_n\}$ ou encore $F = \sum_{k=1}^n \mathbb{K}x_k$.

Remarque 8.1 Si tous les x_k sont nuls, alors $F = \{0\}$.

Exemple 8.8 Dans l'espace $\mathbb{K}[x]$ des fonctions polynomiales, pour tout entier naturel non nul n , le sous-espace vectoriel engendré par $1, x, \dots, x^n$ est formé de l'ensemble des polynômes de degré au plus égal à n , on le note $\mathbb{K}_n[x]$ ou $\mathbb{K}[x]_n$ (le cas $n = 0$ correspond aux polynômes constants).

De manière un peu plus générale, on peut définir le sous-espace vectoriel d'un espace vectoriel E engendré par une famille X non vide de E (non nécessairement finie) comme l'ensemble $F = \text{Vect}(X)$ (ou $F = \langle X \rangle$) de toutes les combinaisons linéaires d'éléments de X . Un vecteur x de E est donc dans $\text{Vect}(X)$ si, et seulement si, il existe un entier $p \geq 1$, des vecteurs x_1, \dots, x_p dans X et des scalaires $\lambda_1, \dots, \lambda_p$ tels que $x = \sum_{k=1}^p \lambda_k x_k$.

Le théorème qui suit nous donne deux définitions équivalentes de $\text{Vect}(X)$.

Théorème 8.3 *Si X est une partie non vide d'un espace vectoriel E , $\text{Vect}(X)$ est l'intersection de tous les sous-espaces vectoriels de E qui contiennent X . C'est aussi le plus petit (pour l'ordre défini par l'inclusion) sous-espace vectoriel de E qui contient X , c'est-à-dire que $\text{Vect}(X)$ contient X et est contenu dans tout sous-espace vectoriel de E qui contient X .*

On peut aussi définir des sous-espaces vectoriels de \mathbb{K}^n en utilisant des équations linéaires (on verra plus loin, avec la notion de base, que cela est encore possible pour n'importe quel espace vectoriel).

Théorème 8.4 *Étant donné un entier naturel non nul n et n scalaires non tous nuls a_1, \dots, a_n , l'ensemble :*

$$F = \left\{ x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n \mid \sum_{k=1}^n a_k x_k = 0 \right\}$$

est un sous-espace vectoriel de \mathbb{K}^n .

Démonstration. Il suffit de vérifier. ■

Remarque 8.2 *En fait si tous les a_k sont nuls, F est encore défini et c'est \mathbb{K}^n tout entier.*

Pour $n = 1$, on a $a_1 \neq 0$ et cet espace F est réduit à $\{0\}$.

Pour $n = 2$, on a $(a_1, a_2) \neq (0, 0)$ et supposant par exemple que $a_2 \neq 0$, l'équation $a_1 x_1 + a_2 x_2 = 0$ équivaut à $x_2 = -\frac{a_1}{a_2} x_1$, ce qui signifie que F est l'ensemble des vecteurs de la forme :

$$x = x_1 \begin{pmatrix} 1 \\ -\frac{a_1}{a_2} \end{pmatrix}$$

où x_1 décrit \mathbb{K} , ce qui équivaut encore à dire que F est l'ensemble des vecteurs de la forme :

$$x = \frac{x_1}{a_2} \begin{pmatrix} a_2 \\ -a_1 \end{pmatrix} = \lambda \begin{pmatrix} a_2 \\ -a_1 \end{pmatrix}$$

où λ décrit \mathbb{K} . En définitive F est la droite engendrée par $\begin{pmatrix} a_2 \\ -a_1 \end{pmatrix}$.

Pour $n = 3$, on a $(a_1, a_2, a_3) \neq (0, 0, 0)$ et supposant par exemple que $a_3 \neq 0$, l'équation $a_1 x_1 + a_2 x_2 + a_3 x_3 = 0$ équivaut à $x_3 = -\frac{a_1}{a_3} x_1 - \frac{a_2}{a_3} x_2$, ce qui signifie que F est l'ensemble des vecteurs de la forme :

$$x = x_1 \begin{pmatrix} 1 \\ 0 \\ -\frac{a_1}{a_3} \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ -\frac{a_2}{a_3} \end{pmatrix}$$

où (x_1, x_2) décrit \mathbb{K}^2 , ce qui équivaut encore à dire que F est l'ensemble des vecteurs de la forme :

$$x = \frac{x_1}{a_3} \begin{pmatrix} a_3 \\ 0 \\ -a_1 \end{pmatrix} + \frac{x_2}{a_3} \begin{pmatrix} 0 \\ a_3 \\ -a_2 \end{pmatrix} = \lambda \begin{pmatrix} a_3 \\ 0 \\ -a_1 \end{pmatrix} + \mu \begin{pmatrix} 0 \\ a_3 \\ -a_3 \end{pmatrix}$$

où (λ, μ) décrit \mathbb{K}^2 , les vecteurs $\begin{pmatrix} a_3 \\ 0 \\ -a_1 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ a_3 \\ -a_3 \end{pmatrix}$ étant non colinéaires puisque $a_3 \neq 0$.

En définitive F est le plan engendré par $\begin{pmatrix} a_3 \\ 0 \\ -a_1 \end{pmatrix}$ et $\begin{pmatrix} 0 \\ a_3 \\ -a_3 \end{pmatrix}$.

De manière générale, on donne la définition suivante.

Définition 8.7 *Étant donné un entier naturel non nul n , on appelle hyperplan vectoriel de \mathbb{K}^n tout sous-espace vectoriel de la forme :*

$$H = \left\{ x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n \mid \sum_{k=1}^n a_k x_k = 0 \right\}$$

où les scalaires a_1, \dots, a_n ne sont pas tous nuls.

On dit aussi que H est l'hyperplan d'équation $\sum_{k=1}^n a_k x_k = 0$.

De manière un peu plus générale, on appelle hyperplan affine de \mathbb{K}^n tout sous-ensemble de \mathbb{K}^n de la forme :

$$H = \left\{ x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n \mid \sum_{k=1}^n a_k x_k = \lambda \right\}$$

où λ est un scalaire et les scalaires a_1, \dots, a_n ne sont pas tous nuls.

On dit aussi que H est l'hyperplan d'équation $\sum_{k=1}^n a_k x_k = \lambda$.

Pour $n = 2$, un hyperplan est une droite affine et pour $n = 3$, un hyperplan est un plan affine.

Dans l'espace \mathbb{R}^3 l'intersection de deux plans vectoriels distincts est une droite.

Plus généralement, on a le résultat suivant.

Théorème 8.5 *Étant donnés deux entiers naturels non nuls n et p , des scalaires $a_{1,1}, \dots, a_{1,n}, \dots, a_{p,1}, \dots, a_{p,n}$, l'ensemble :*

$$F = \left\{ x = (x_i)_{1 \leq i \leq n} \in \mathbb{K}^n \mid \sum_{k=1}^n a_{i,k} x_k = 0 \quad (1 \leq i \leq p) \right\}$$

est un sous-espace vectoriel de \mathbb{K}^n .

On dit que F est le sous-espace vectoriels de \mathbb{K}^n d'équations linéaires :

$$\begin{cases} \sum_{k=1}^n a_{1,k} x_k = 0 \\ \vdots \\ \sum_{k=1}^n a_{p,k} x_k = 0 \end{cases}$$

8.4 Applications linéaires

Pour ce paragraphe, on désigne par E et F deux espaces vectoriels. On note 0 le vecteur nul de E et aussi celui de F . En toute rigueur il faudrait noter 0_E et 0_F ces vecteurs nuls, mais en fonction du contexte on sait en général de quel vecteur nul il s'agit.

Définition 8.8 *On dit qu'une application u de E dans F est linéaire (ou que c'est un morphisme d'espaces vectoriels) si pour tous vecteurs x, y de E et tout scalaire λ , on a :*

$$\begin{cases} u(x + y) = u(x) + u(y) \\ u(\lambda x) = \lambda u(x) \end{cases}$$

Remarque 8.3 *Une application linéaire u de E dans F transforme 0_E en 0_F et l'opposé de x dans E en l'opposé de $u(x)$ dans F . En effet, on a :*

$$u(0) = u(0 + 0) = u(0) + u(0)$$

donc $u(0) = 0$ et :

$$0 = u(0) = u(x + (-x)) = u(x) + u(-x)$$

et donc $u(-x) = -u(x)$.

Exemple 8.9 *Pour tout scalaire λ , l'application $u : x \mapsto \lambda x$ est linéaire de E dans E . On dit que c'est l'homothétie de rapport λ . Pour $\lambda = 1$, cette application est l'application identité et on la note Id_E ou Id .*

Exemple 8.10 *Pour tout entier j compris entre 1 et n , l'application u définie sur \mathbb{K}^n par $u(x) = x_j$, si $x = (x_i)_{1 \leq i \leq n}$ est linéaire de E dans \mathbb{K} . On dit que c'est la j -ième projection canonique.*

Exemple 8.11 *Une translation de vecteur non nul $x \mapsto x + a$, définie de E dans E , n'est pas linéaire.*

Exemple 8.12 *Étant donné un intervalle réel I , la dérivation $f \mapsto f'$ est linéaire de l'espace vectoriel des fonctions dérivables de I dans \mathbb{R} dans l'espace vectoriel des fonctions de I dans \mathbb{R} .*

On notera $\mathcal{L}(E, F)$ (ou plus précisément $\mathcal{L}_{\mathbb{K}}(E, F)$) l'ensemble de toutes les applications linéaires de E dans F .

Si u et v sont deux applications linéaires de E dans F , $u + v$ est l'application définie sur E par :

$$\forall x \in E, (u + v)(x) = u(x) + v(x)$$

et pour tout scalaire λ , λu est l'application définie sur E par :

$$\forall x \in E, (\lambda u)(x) = \lambda u(x).$$

Il est facile de vérifier que $u + v$ et λu sont aussi des application linéaires de E dans F . On a donc ainsi défini une addition interne sur $\mathcal{L}(E, F)$ et une multiplication externe. Le résultat qui suit se démontre alors facilement.

Théorème 8.6 *L'ensemble $\mathcal{L}(E, F)$ de toutes les applications linéaires de E dans F muni de ces deux opérations est un espace vectoriel.*

Dans le cas où $F = E$, on note plus simplement $\mathcal{L}(E)$ pour $\mathcal{L}(E, F)$.

Les éléments de $\mathcal{L}(E)$ sont aussi appelés endomorphismes de E .

La composition des applications permet aussi de construire des applications linéaires à partir d'applications linéaires données.

Théorème 8.7 *Soient E, F, G des espaces vectoriels, u une application linéaire de E dans F et v une application linéaire de F dans G . La composée $v \circ u$ est alors une application linéaire de E dans G .*

Démonstration. Il suffit de vérifier. ■

Théorème 8.8 *Si u est une application linéaire de E dans F , on a alors pour tout entier naturel non nul n , tous vecteurs x_1, \dots, x_n de E et tous scalaires $\lambda_1, \dots, \lambda_n$:*

$$u\left(\sum_{k=1}^n \lambda_k x_k\right) = \sum_{k=1}^n \lambda_k u(x_k).$$

Démonstration. On procède par récurrence pour $n \geq 1$. Pour $n = 1$, on a bien $u(\lambda x) = \lambda u(x)$ pour tout scalaire λ et tout vecteur x par définition d'une application linéaire.

Pour $n = 2$, toujours par définition d'une application linéaire, on a pour tous vecteurs x, y et tous scalaires λ, μ :

$$u(\lambda x + \mu y) = u(\lambda x) + u(\mu y) = \lambda u(x) + \mu u(y).$$

Supposant le résultat acquis au rang $n \geq 2$, on se donne $n + 1$ vecteurs x_1, \dots, x_n, x_{n+1} et $n + 1$ scalaires $\lambda_1, \dots, \lambda_n, \lambda_{n+1}$ et on a :

$$\begin{aligned} u\left(\sum_{k=1}^{n+1} \lambda_k x_k\right) &= u\left(\sum_{k=1}^n \lambda_k x_k\right) + u(\lambda_{n+1} x_{n+1}) \\ &= \sum_{k=1}^n \lambda_k u(x_k) + \lambda_{n+1} u(x_{n+1}) \\ &= \sum_{k=1}^{n+1} \lambda_k u(x_k) \end{aligned}$$

■

Définition 8.9 *Soit u une application linéaire de E dans F .*

Le noyau de u est l'ensemble :

$$\ker(u) = \{x \in E \mid u(x) = 0\}$$

et l'image de u l'ensemble :

$$\operatorname{Im}(u) = \{u(x) \mid x \in E\}.$$

Théorème 8.9 *Le noyau d'une application linéaire u de E dans F est un sous-espace vectoriel de E et son image un sous-espace vectoriel de F .*

Démonstration. On a vu que $\ker(u)$ contient 0 et pour x, y dans $\ker(u)$, λ, μ dans \mathbb{K} , on a :

$$u(\lambda x + \mu y) = \lambda u(x) + \mu u(y) = 0$$

ce qui signifie que $\lambda x + \mu y \in \ker(u)$. Donc $\ker(u)$ est bien un sous-espace vectoriel de E .

De manière analogue, en utilisant la linéarité de u , on montre que $\operatorname{Im}(u)$ est un sous-espace vectoriel de F . ■

Théorème 8.10 Soit u une application linéaire de E dans F .

1. L'application u est injective si, et seulement si, $\ker(u)$ est réduit à $\{0\}$.
2. L'application u est surjective si, et seulement si, $\operatorname{Im}(u) = F$.

Démonstration.

1. Supposons u injective. Pour tout $x \in \ker(u)$, on a $u(x) = u(0)$ et nécessairement $x = 0$ puisque u est injective. Donc $\ker(u) = \{0\}$.
Réciproquement, supposons que $\ker(u) = \{0\}$. Si x, y dans E sont tels que $u(x) = u(y)$, on a alors $u(x - y) = u(x) - u(y) = 0$, c'est-à-dire que $x - y \in \ker(u)$ et donc $x = y$.
2. Ce résultat est en fait valable pour toute application de E dans F (la linéarité de u n'intervient pas ici). ■

Les applications linéaires de E dans \mathbb{K} ont un statut particulier.

Définition 8.10 On appelle forme linéaire sur E toute application linéaire de E dans \mathbb{K} .

Exemple 8.13 Étant donné un segment $I = [a, b]$ non réduit à un point, l'application $f \mapsto \int_a^b f(x) dx$ est une forme linéaire sur l'espace vectoriel des fonctions continues de I dans \mathbb{R} .

Exercice 8.8 Montrer qu'une forme linéaire φ sur E non identiquement nulle est surjective.

Solution 8.8 Dire que $\varphi \neq 0$ signifie qu'il existe un vecteur $x_0 \in E$ tel que $\lambda = \varphi(x_0) \neq 0$. Pour tout scalaire y , on peut alors écrire :

$$y = \frac{y}{\lambda} \lambda = \frac{y}{\lambda} \varphi(x_0) = \varphi\left(\frac{y}{\lambda} x_0\right)$$

soit $y = \varphi(x)$ avec $x = \frac{y}{\lambda} x_0 \in E$, ce qui signifie que φ est surjective.

Exercice 8.9 On se donne un intervalle réel I non réduit à un point et on désigne par E l'ensemble de toutes les fonctions dérivables de I dans \mathbb{R} et par F l'ensemble de toutes les fonctions de I dans \mathbb{R} .

1. Montrer que E est un espace vectoriel.
2. Déterminer le noyau de l'application linéaire $u : f \mapsto f'$ où f' est la fonction dérivée de f .

Solution 8.9 Laissée au lecteur.

Exercice 8.10 Soit u une application linéaire de E dans E (i. e. un endomorphisme de E). Montrer que :

$$\operatorname{Im}(u) \subset \ker(u) \Leftrightarrow u \circ u = 0.$$

Solution 8.10 Si $\text{Im}(u) \subset \ker(u)$, on a alors $u(x) \in \ker(u)$ pour tout $x \in E$ et $u(u(x)) = 0$, ce qui signifie que $u \circ u = 0$.

Réciproquement si $u \circ u = 0$, pour tout $y = u(x) \in \text{Im}(u)$, on a $u(y) = u(u(x)) = u \circ u(x) = 0$, ce qui signifie que $y \in \ker(u)$ et $\text{Im}(u) \subset \ker(u)$.

Exercice 8.11 On appelle projecteur de E tout endomorphisme p de E tel que $p \circ p = p$.

1. Montrer que $\text{Im}(p)$ est l'ensemble des vecteurs invariants de p .
2. Montrer que $\text{Im}(p) \cap \ker(p) = \{0\}$.
3. Montrer que tout vecteur $x \in E$ s'écrit de manière unique comme somme d'un vecteur de $\ker(p)$ et d'un vecteur de $\text{Im}(p)$ (on dit que E est somme directe de $\ker(p)$ et $\text{Im}(p)$, ce qui se note $E = \ker(p) \oplus \text{Im}(p)$).
4. Montrer que si p est un projecteur, il en est alors de même de $q = Id_E - p$ et on a $\ker(q) = \text{Im}(p)$ et $\text{Im}(q) = \ker(p)$.

Solution 8.11 *Laissée au lecteur.*

On rappelle que si u est une bijection de E sur F , elle admet alors une application réciproque notée u^{-1} et définie par :

$$(y \in F \text{ et } x = u^{-1}(y)) \Leftrightarrow (x \in E \text{ et } y = u(x)).$$

Cette application u^{-1} est aussi l'unique application de F dans E telle que $u \circ u^{-1} = Id_F$ et $u^{-1} \circ u = Id_E$.

Dans le cas où u est linéaire, il en est de même de u^{-1} . En effet si y, y' sont deux éléments de F , ils s'écrivent de manière unique $y = u(x)$, $y' = u(x')$ et on a :

$$\begin{aligned} u^{-1}(y + y') &= u^{-1}(u(x) + u(x')) \\ &= u^{-1}(u(x + x')) = x + x' = u^{-1}(y) + u^{-1}(y') \end{aligned}$$

et pour tout scalaire λ :

$$u^{-1}(\lambda y) = u^{-1}(\lambda u(x)) = u^{-1}(u(\lambda x)) = \lambda x = \lambda u^{-1}(y).$$

Définition 8.11 On appelle isomorphisme de E sur F toute application linéaire bijective de E sur F .

Dans le cas où $E = F$, un isomorphisme de E sur E est appelé automorphisme de E .

On note $GL(E)$ l'ensemble de tous les automorphismes de E et on dit que $GL(E)$ est le groupe linéaire de E (l'appellation groupe sera justifiée plus loin).

Exercice 8.12 L'ensemble $GL(E)$ est-il un espace vectoriel ?

Solution 8.12 Non, sauf dans le cas où $E = \{0\}$.

8.5 La base canonique de \mathbb{K}^n et expression matricielle des applications linéaires de \mathbb{K}^n dans \mathbb{K}^m

Tout vecteur $x = (x_i)_{1 \leq i \leq n}$ de \mathbb{K}^n s'écrit $\sum_{k=1}^n x_k e_k$, où on a noté, pour tout entier k compris entre 1 et n , e_k le vecteur dont toutes les composantes sont nulles sauf la k -ième qui vaut 1. L'espace vectoriel \mathbb{K}^n est donc engendré par les vecteurs e_1, e_2, \dots, e_n . On dit que le système (e_1, e_2, \dots, e_n) , que l'on note plus simplement $(e_k)_{1 \leq k \leq n}$, est un système générateur de \mathbb{K}^n . De plus par définition du produit cartésien \mathbb{K}^n une telle écriture est unique, ce qui se traduit en disant que le système $(e_k)_{1 \leq k \leq n}$ est un système libre.

On dit que $(e_k)_{1 \leq k \leq n}$ est la base canonique de \mathbb{K}^n . Nous définirons plus loin la notion de base d'un espace vectoriel.

Si m est un autre entier naturel non nul, on note $(f_k)_{1 \leq k \leq m}$ la base canonique de \mathbb{K}^m .

Étant donnée une application linéaire u de E dans F , on a pour tout vecteur $x = \sum_{j=1}^n x_j e_j$ de \mathbb{K}^n :

$$u(x) = u\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j u(e_j)$$

et chacun des vecteurs $u(e_j)$, pour j compris entre 1 et n , étant dans \mathbb{K}^m , il s'écrit :

$$u(e_j) = \sum_{i=1}^m a_{ij} f_i$$

On a donc en définitive :

$$u(x) = \sum_{j=1}^n x_j \sum_{i=1}^m a_{ij} f_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} x_j \right) f_i$$

ce qui signifie que les composantes du vecteurs $u(x)$ sont données par :

$$y_i = \sum_{j=1}^n a_{ij} x_j \quad (1 \leq i \leq m) \quad (8.1)$$

Par exemple pour $n = m = 2$, on a :

$$\begin{cases} u(e_1) = a_{11}f_1 + a_{21}f_2 \\ u(e_2) = a_{12}f_1 + a_{22}f_2 \end{cases}$$

et :

$$u(x) = y_1 f_1 + y_2 f_2$$

avec :

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 \\ y_2 = a_{21}x_1 + a_{22}x_2 \end{cases} \quad (8.2)$$

L'application linéaire u est donc uniquement déterminée par les 4 scalaires a_{11}, a_{12}, a_{21} et a_{22} . On stocke ces scalaires dans un tableau à 2 lignes et 2 colonnes :

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

où la première colonne $\begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}$ est le vecteur $u(e_1)$ et la deuxième colonne $\begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}$ le vecteur $u(e_2)$. Un tel tableau est appelé matrice à 2 lignes et 2 colonnes ou plus simplement matrice 2×2 .

On traduit les deux égalités de (8.2) en utilisant le produit matriciel :

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

De manière générale, une application linéaire u de \mathbb{K}^n dans \mathbb{K}^m est donc uniquement déterminée par la matrice A à m lignes et n colonnes :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

où la colonne numéro j , pour j compris entre 1 et n , est le vecteur :

$$u(e_j) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

Les égalités (8.1) se traduisent alors par le produit matriciel :

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$$

qui s'effectue comme suit :

$$y_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \sum_{j=1}^n a_{ij} x_j$$

pour tout i compris entre 1 et m .

Tout cela est compacté en :

$$y = u(x) \Leftrightarrow y = Ax$$

et on dit que A est la matrice de u dans les bases canoniques de \mathbb{K}^n et \mathbb{K}^m . Si $n = m$, on dit simplement que A est la matrice de $u \in \mathcal{L}(\mathbb{K}^n)$ dans la base canonique de \mathbb{K}^n .

Exercice 8.13 Soit $u \in \mathcal{L}(\mathbb{K}^3)$ de matrice $A = \begin{pmatrix} 4 & 2 & -4 \\ -6 & -4 & 6 \\ -1 & -1 & 1 \end{pmatrix}$ dans la base canonique (e_1, e_2, e_3) . Déterminer le noyau u .

Solution 8.13 L'image du vecteur $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ est le vecteur :

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 4 & 2 & -4 \\ -6 & -4 & 6 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4x_1 + 2x_2 - 4x_3 \\ -6x_1 - 4x_2 + 6x_3 \\ -x_1 - x_2 + x_3 \end{pmatrix}$$

Dire que $x \in \mathbb{K}^3$ est dans le noyau de u équivaut à dire que ses composantes sont solutions du système linéaire de 3 équations à 3 inconnues :

$$\begin{cases} 4x_1 + 2x_2 - 4x_3 = 0 \\ -6x_1 - 4x_2 + 6x_3 = 0 \\ -x_1 - x_2 + x_3 = 0 \end{cases}$$

L'équation (3) donne $x_3 = x_1 + x_2$ qui reporté dans la première donne $x_2 = 0$ et $x_1 = x_3$. Réciproquement tout vecteur vérifiant ces conditions est solution du système linéaire. Le noyau de u est donc :

$$\ker(u) = \left\{ \begin{pmatrix} x_1 \\ 0 \\ x_1 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = x_1 (e_1 + e_3) \mid x \in \mathbb{K} \right\}$$

c'est donc la droite vectorielle engendré par le vecteur $e_1 + e_3$.

8.6 Matrices réelles ou complexes

On note $\mathcal{M}_{m,n}(\mathbb{K})$ l'ensemble de toutes les matrices à m lignes et n colonnes et à coefficients dans \mathbb{K} .

Une matrice $\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$ dans $\mathcal{M}_{m,n}(\mathbb{K})$ sera notée $A = ((a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, le pre-

mier indice i étant le numéro de ligne et le deuxième j , le numéro de colonne.

Pour $n = m$, on note $\mathcal{M}_n(\mathbb{K})$ l'ensemble $\mathcal{M}_{n,n}(\mathbb{K})$ et dit que c'est l'ensemble des matrices carrées d'ordre n à coefficients dans \mathbb{K} .

8.6.1 Opérations sur les matrices

Théorème 8.11 Si u et v sont deux applications linéaires de \mathbb{K}^n dans \mathbb{K}^m ayant pour matrices respectives $A = ((a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ et $B = ((b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ dans les bases canoniques, alors l'application linéaire $u + v$ a pour matrice dans ces bases canoniques, la matrice $((a_{i,j} + b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$. Et pour tout scalaire λ , la matrice de λu dans les bases canoniques est la matrice $((\lambda a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$.

Démonstration. Résulte de :

$$\begin{aligned} (u + v)(e_j) &= u(e_j) + v(e_j) \\ &= \sum_{i=1}^m a_{ij} f_i + \sum_{i=1}^m b_{ij} f_i \\ &= \sum_{i=1}^m (a_{ij} + b_{ij}) f_i \quad (1 \leq j \leq n) \end{aligned}$$

et de :

$$(\lambda u)(e_j) = \lambda u(e_j) = \lambda \sum_{i=1}^m a_{ij} f_i = \sum_{i=1}^m \lambda a_{ij} f_i \quad (1 \leq j \leq n)$$

■

On définit donc naturellement la somme de deux matrices $n \times m$ et le produit d'une telle matrice par un scalaire par :

$$A + B = ((a_{i,j} + b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \text{ et } \lambda A = ((\lambda a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

en utilisant les notations précédentes.

On vérifie alors facilement le résultat suivant.

Théorème 8.12 *L'ensemble $\mathcal{M}_{m,n}(\mathbb{K})$ des matrices à m lignes et n colonnes est un espace vectoriel.*

On note 0 la matrice nulle, c'est-à-dire l'élément de $\mathcal{M}_{m,n}(\mathbb{K})$ dont toutes les composantes sont nulles et pour toute matrice $A = ((a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, on note $-A = ((-a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ l'opposé de A .

En explicitant la matrice d'une composée de deux applications linéaires on définira le produit de deux matrices.

On se donne donc une application linéaire v de \mathbb{K}^n dans \mathbb{K}^m et une application linéaire u de \mathbb{K}^m dans \mathbb{K}^r de matrices respectives $B = ((b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ dans $\mathcal{M}_{m,n}(\mathbb{K})$ et $A = ((a_{i,j}))_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m}}$ dans $\mathcal{M}_{r,m}(\mathbb{K})$.

On note toujours $(e_k)_{1 \leq k \leq n}$ la base canonique de \mathbb{K}^n , $(f_k)_{1 \leq k \leq m}$ celle de \mathbb{K}^m et $(g_k)_{1 \leq k \leq r}$ est celle de \mathbb{K}^r .

La matrice $C = ((c_{i,j}))_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}} \in \mathcal{M}_{r,n}(\mathbb{K})$ de $u \circ v \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^r)$ est obtenu en calculant les composantes des vecteurs $u \circ v(e_j)$, pour j compris entre 1 et n , dans la base $(g_k)_{1 \leq k \leq r}$.

On a :

$$u \circ v(e_j) = u(v(e_j)) = u\left(\sum_{k=1}^m b_{kj} f_k\right) = \sum_{k=1}^m b_{kj} u(f_k)$$

avec, pour k compris entre 1 et m :

$$u(f_k) = \sum_{i=1}^r a_{ik} g_i$$

ce qui donne :

$$u \circ v(e_j) = \sum_{k=1}^m b_{kj} \left(\sum_{i=1}^r a_{ik} g_i \right) = \sum_{i=1}^r \left(\sum_{k=1}^m a_{ik} b_{kj} \right) g_i$$

et signifie que les coefficients de la matrice C sont donnés par :

$$c_{ij} = \sum_{k=1}^m a_{ik} b_{kj} \quad (1 \leq i \leq r, \quad 1 \leq j \leq n).$$

Au vu de ce résultat, on donne la définition suivante.

Définition 8.12 Étant données une matrice $A = ((a_{i,j}))_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m}} \in \mathcal{M}_{r,m}(\mathbb{K})$ et une matrice $B = ((b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{m,n}(\mathbb{K})$, le produit AB de A par B est la matrice $C = ((c_{i,j}))_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$ de $\mathcal{M}_{r,n}(\mathbb{K})$ définie par :

$$c_{ij} = \sum_{k=1}^m a_{ik} b_{kj} \quad (1 \leq i \leq r, \quad 1 \leq j \leq n).$$

Et nous venons de montrer le résultat suivant.

Théorème 8.13 Si v est une application linéaire de \mathbb{K}^n dans \mathbb{K}^m de matrice $B = ((b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ dans $\mathcal{M}_{m,n}(\mathbb{K})$ et u une application linéaire de \mathbb{K}^m dans \mathbb{K}^r de matrice $A = ((a_{i,j}))_{\substack{1 \leq i \leq r \\ 1 \leq j \leq m}}$ dans $\mathcal{M}_{r,m}(\mathbb{K})$ dans les bases canoniques, alors la matrice dans les bases canoniques de l'application linéaire $u \circ v$ de \mathbb{K}^n dans \mathbb{K}^r est la matrice produit $C = AB$.

Il est important de remarquer que l'on ne peut définir le produit AB que si le nombre de colonnes de la matrice A est égal au nombre de lignes de la matrice B , ce produit est donc défini de $\mathcal{M}_{r,m}(\mathbb{K}) \times \mathcal{M}_{m,n}(\mathbb{K})$ dans $\mathcal{M}_{r,n}(\mathbb{K})$.

Exercice 8.14 Soient $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 2 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -1 \\ 0 & 2 \\ 2 & 3 \end{pmatrix}$. Calculer AB et BA .

Solution 8.14 On a : $AB = \begin{pmatrix} 7 & 12 \\ 1 & 8 \end{pmatrix}$ et $BA = \begin{pmatrix} 2 & 0 & 2 \\ -2 & 4 & 2 \\ -1 & 10 & 9 \end{pmatrix}$.

Exercice 8.15 Pour tout réel θ , on désigne par M_θ la matrice réelle :

$$M_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Montrer que pour tous réels θ et θ' , on a $M_\theta M_{\theta'} = M_{\theta'} M_\theta = M_{\theta+\theta'}$.

Solution 8.15 Laissée au lecteur.

Exercice 8.16 On se place dans l'espace $\mathcal{M}_2(\mathbb{K})$ des matrices carrées d'ordre 2 où on note $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ la matrice identité d'ordre 2.

1. Donner des exemples de matrices A et B telles que $AB = 0$ et $BA \neq 0$.
2. Montrer que si $AB = I_2$, alors $BA = I_2$.

Solution 8.16 Laissée au lecteur.

Exercice 8.17 Déterminer dans la base canonique (e_1, e_2) de \mathbb{R}^2 la matrice de l'endomorphisme u (s'il existe) tel que $u(e_1) = ae_1 - e_2$ et $u \circ u = u$ où a est un réel donné.

Solution 8.17 Laissée au lecteur.

Exercice 8.18 Donner une condition nécessaire et suffisante portant sur les réels a et b pour que l'endomorphisme u de \mathbb{R}^2 de matrice $A = \begin{pmatrix} a+1 & a \\ b & b+1 \end{pmatrix}$ soit un automorphisme.

Solution 8.18 *Laissée au lecteur.*

Exercice 8.19 *Déterminer, par leur matrice dans la base canonique, tous les endomorphismes non nuls de \mathbb{K}^2 tels que $\text{Im}(u) \subset \ker(u)$. Si u est un tel endomorphisme donner la matrice de $v = \text{Id}_E + u$ et montrer que c'est un automorphisme de E .*

Solution 8.19 *Laissée au lecteur.*

L'opération de multiplication des matrices est une opération interne sur l'espace $\mathcal{M}_n(\mathbb{K})$ des matrices carrées d'ordre n vérifiant les propriétés suivantes :

- elle est associative, c'est-à-dire que pour toutes matrices A, B, C dans $\mathcal{M}_n(\mathbb{K})$, on a $A(BC) = (AB)C$;
- elle est distributive par rapport à l'addition, c'est-à-dire que pour toutes matrices A, B, C dans $\mathcal{M}_n(\mathbb{K})$, on a $A(B + C) = AB + AC$;
- la matrice

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

est l'élément neutre pour ce produit, c'est-à-dire que $A \cdot I_n = I_n \cdot A = A$ pour toute matrice A dans $\mathcal{M}_n(\mathbb{K})$.

Ces propriétés ajoutées à celle de l'addition des matrices se traduisent en disant que $(\mathcal{M}_n(\mathbb{K}), +, \cdot)$ est un anneau unitaire.

L'associativité du produit matriciel dans $\mathcal{M}_n(\mathbb{K})$ permet de définir les puissances successives d'une matrice A par la relation de récurrence :

$$\begin{cases} A^0 = I_n \\ \forall p \in \mathbb{N}, A^{p+1} = A^p A = A A^p. \end{cases}$$

Exercice 8.20 *Calculer A^n pour tout entier naturel n , où $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.*

Solution 8.20 On a $A^0 = I_3$, $A^1 = A$ et :

$$A^2 = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}.$$

En supposant que, pour $n \geq 1$, on a $A^n = \begin{pmatrix} 1 & n & a_n \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$, où a_n est un entier à déterminer, on a :

$$\begin{aligned} A^{n+1} &= \begin{pmatrix} 1 & n & a_n \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n+1 & n+a_n+1 \\ 0 & 1 & n+1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n & a_{n+1} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

avec :

$$a_{n+1} = a_n + n + 1.$$

La suite $(a_n)_{n \geq 1}$ est donc définie par la relation de récurrence :

$$\begin{cases} a_1 = 1 \\ \forall n \geq 1, a_{n+1} = a_n + n + 1 \end{cases}$$

ce qui donne :

$$a_n = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

(vérification par récurrence sur $n \geq 1$). On a donc, pour tout $n \geq 0$:

$$A^n = \begin{pmatrix} 1 & n & \frac{n(n+1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$$

Remarque 8.4 Le produit des matrices dans $\mathcal{M}_n(\mathbb{K})$ n'est pas commutatif. Par exemple pour

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$, on a :

$$AB = \begin{pmatrix} 5 & 11 \\ 11 & 25 \end{pmatrix} \neq BA = \begin{pmatrix} 10 & 14 \\ 14 & 20 \end{pmatrix}.$$

On dira que deux matrices A et B dans $\mathcal{M}_n(\mathbb{K})$ commutent si $AB = BA$.

8.6.2 Matrices inversibles

Définition 8.13 On dit qu'une matrice A dans $\mathcal{M}_n(\mathbb{K})$ est inversible s'il existe une matrice A' dans $\mathcal{M}_n(\mathbb{K})$ telle que $AA' = A'A = I_n$. On dit alors que A' est un inverse de A .

Si une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible son inverse est alors unique. En effet si A'' est un autre inverse de A , on a :

$$A'' = A''I_n = A''(AA') = (A''A)A' = I_nA' = A'.$$

On note A^{-1} l'inverse de A quand il existe.

On peut aussi remarquer qu'une matrice inversible A n'est jamais nulle puisque $AA^{-1} = I_n \neq 0$.

Exercice 8.21 Montrer que si la matrice $A \in \mathcal{M}_n(\mathbb{K})$ a une colonne [resp. une ligne] nulle, alors elle n'est pas inversible.

Solution 8.21 En notant C_1, \dots, C_n [resp. L_1, \dots, L_n] les colonne [resp. lignes] de A , on a pour toute matrice $A' \in \mathcal{M}_n(\mathbb{K})$:

$$A'A = (A'C_1, \dots, A'C_n)$$

et pour $C_j = 0$, la colonne j de $A'A$ est nulle, ce qui interdit l'égalité $A'A = I_n$.

Pour ce qui est des lignes, on écrit que :

$$AA' = \begin{pmatrix} L_1A' \\ \vdots \\ L_nA' \end{pmatrix}.$$

Exercice 8.22 Montrer que pour tout réel θ , la matrice $M_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ est inversible d'inverse $M_{-\theta}$.

Solution 8.22 *Laissée au lecteur.*

Théorème 8.14 Si $A \in \mathcal{M}_n(\mathbb{K})$ est inversible, alors A^{-1} est aussi inversible et $(A^{-1})^{-1} = A$. Le produit de deux matrices inversibles A et B est inversible et $(AB)^{-1} = B^{-1}A^{-1}$.

Démonstration. Le premier point résulte de la définition et le deuxième de :

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

et :

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n.$$

■

Par récurrence, on déduit que le produit de p matrices inversibles A_1, \dots, A_p est inversible avec $(A_1 \cdots A_p)^{-1} = A_p^{-1} \cdots A_1^{-1}$.

Exercice 8.23 Soit $P \in \mathcal{M}_n(\mathbb{K})$ inversible. Montrer que $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si, et seulement si, AP [resp. PA] est inversible.

Solution 8.23 Le théorème précédent nous dit que la condition est nécessaire.

Réciproquement si AP [resp. PA] est inversible, alors $A = (AP)P^{-1}$ [resp. $A = P^{-1}(PA)$] est inversible.

Théorème 8.15 Un endomorphisme u de \mathbb{K}^n est bijectif si, et seulement si, sa matrice A dans la base canonique est inversible et dans ce cas A^{-1} est la matrice de u^{-1} dans la base canonique.

Démonstration. Supposons u bijectif et notons A' la matrice de u^{-1} dans la base canonique de \mathbb{K}^n . De $u \circ u^{-1} = u^{-1} \circ u = Id$, on déduit que $AA' = A'A = I_n$, ce qui signifie que A est inversible d'inverse A' .

Réciproquement supposons A inversible et désignons par u' l'endomorphisme de \mathbb{K}^n de matrice A^{-1} dans la base canonique. La matrice de $u \circ u'$ [resp. de $u' \circ u$] est $AA^{-1} = I_n$ [resp. $A^{-1}A = I_n$], donc $u \circ u' = Id$ [resp. de $u' \circ u = Id$] et u est surjective [resp. injective]. L'endomorphisme u est donc bijectif. ■

Exercice 8.24 On désigne par $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{K}^n avec $n \geq 2$ et pour tout entier j compris entre 1 et n , par M_j la matrice :

$$M_j = (0, \dots, 0, e_1, 0, \dots, 0)$$

la colonne e_1 étant en position j .

Montrer que pour tout scalaire λ et tout entier j compris entre 2 et n , la matrice :

$$P_j(\lambda) = I_n + \lambda M_j$$

est inversible et déterminer son inverse.

Solution 8.24 Soit, pour j et λ fixés, u l'endomorphisme de \mathbb{K}^n canoniquement associé à $P_j(\lambda)$. Il est défini par :

$$u(e_k) = \begin{cases} \lambda e_1 + e_j & \text{si } k = j \\ e_k & \text{si } k \neq j \end{cases}$$

Cet endomorphisme est inversible d'inverse u' défini par :

$$u'(e_k) = \begin{cases} -\lambda e_1 + e_j & \text{si } k = j \\ e_k & \text{si } k \neq j \end{cases}$$

donc $P_j(\lambda)$ est inversible d'inverse $P_j(-\lambda)$.

Les matrices $P_j(\lambda)$ sont des matrices de transvection (paragraphe 10.1). On peut vérifier que la multiplication à gauche par une matrice de transvection $P_j(\lambda)$ a pour effet de remplacer la ligne L_1 de A par $L_1 + \lambda L_j$, les autres lignes étant inchangées et la multiplication à droite par une matrice de transvection $P_j(\lambda)$ a pour effet de remplacer la colonne C_j par $C_j + \lambda C_1$, les autres colonnes étant inchangées (théorème 10.1).

Théorème 8.16 Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si, et seulement si, l'unique solution du système linéaire $Ax = 0$ est $x = 0$.

Démonstration. Si A est inversible et x est solution de $Ax = 0$, on a alors $A^{-1}Ax = x = 0$, donc 0 est l'unique solution de $Ax = 0$.

Pour la réciproque, on procède par récurrence sur $n \geq 1$.

On désigne par $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{K}^n .

Pour $n = 1$, $A = (a)$ est inversible si, et seulement si, $a \neq 0$ et le résultat est évident.

Supposons le résultat acquis pour $n - 1 \geq 1$ et soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que $x = 0$ soit l'unique solution du système linéaire $Ax = 0$.

La première colonne de A n'est pas nulle puisque c'est $C_1 = Ae_1$ avec $e_1 \neq 0$, il existe donc un indice j tel que $a_{j1} \neq 0$. Montrer que A est inversible équivaut à montrer que $\frac{1}{a_{j1}}A$ est inversible, ce qui nous ramène à $a_{j1} = 1$. Si $a_{11} = 0$, alors $j \geq 2$ et il est équivalent de montrer que la matrice $P_j(1)A$ (notations de l'exercice 8.24) est inversible, ce qui nous ramène à $a_{11} = 1$ ($P_j(1)A$ se déduit de A en ajoutant la ligne j à la ligne 1). Il est encore équivalent de montrer que $AP_2(-a_{12})$ est inversible, ce qui ramène à $a_{12} = 0$ et multipliant à droite par $P_j(-a_{1j})$ pour $2 \leq j \leq n$, on se ramène à $a_{1j} = 0$. En résumé, il suffit de considérer le cas où :

$$A = \begin{pmatrix} 1 & 0 \\ c & B \end{pmatrix}$$

avec $0 \in \mathcal{M}_{1,n-1}(\mathbb{K})$, $c \in \mathcal{M}_{n-1,1}(\mathbb{K})$ et $B \in \mathcal{M}_{n-1}(\mathbb{K})$. Si $x' \in \mathbb{K}^{n-1} \setminus \{0\}$ est solution de $Bx' = 0$, alors $x = \begin{pmatrix} 0 \\ x' \end{pmatrix} \in \mathbb{K}^n \setminus \{0\}$ est solution de $Ax = 0$, ce qui contredit l'hypothèse de départ. Donc $x' = 0$ est l'unique solution de $Bx' = 0$ et B est inversible. En posant $A' = \begin{pmatrix} 1 & 0 \\ d & B^{-1} \end{pmatrix}$ où $d \in \mathcal{M}_{n-1,1}(\mathbb{K})$ est à préciser, on a :

$$AA' = \begin{pmatrix} 1 & 0 \\ c & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d & B^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c + Bd & I_{n-1} \end{pmatrix}$$

et :

$$A'A = \begin{pmatrix} 1 & 0 \\ d & B^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & B \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ d + B^{-1}c & I_{n-1} \end{pmatrix}$$

soit $AA' = A'A = I_n$ en prenant $d = -B^{-1}c$. La matrice A est donc inversible. ■

Corollaire 8.1 *Un endomorphisme u de \mathbb{K}^n est bijectif si, et seulement si, son noyau est réduit à $\{0\}$.*

Démonstration. Si A est la matrice canoniquement associée à u , on a $u(x) = Ax$ et $\ker(u) = \{0\}$ équivaut à dire que 0 est l'unique solution de $Ax = 0$, ce qui équivaut à A inversible encore équivalent à dire que u est un isomorphisme. ■

Corollaire 8.2 *Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible d'inverse $A' \in \mathcal{M}_n(\mathbb{K})$ si, et seulement si, $A'A = I_n$ [resp. $AA' = I_n$].*

Démonstration. Supposons que $A'A = I_n$. Si x est solution de $Ax = 0$, on a alors $x = I_n x = A'(Ax) = A'0 = 0$ et A est inversible avec $A^{-1} = (A'A)A^{-1} = A'$.

Si $AA' = I_n$, la matrice A' est alors inversible d'inverse A , donc $A = (A')^{-1}$ est inversible d'inverse A' . ■

Exercice 8.25 *Montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ a une colonne [resp. une ligne] nulle, alors elle n'est pas inversible.*

Solution 8.25 *Si la colonne j [resp. la ligne i] de A est nulle, alors pour toute matrice $A' \in \mathcal{M}_n(\mathbb{K})$, la matrice $A'A$ [resp. AA'] a sa colonne j [resp. sa ligne i] nulle. En conséquence il ne peut exister de matrice $A' \in \mathcal{M}_n(\mathbb{K})$ telle que $A'A = I_n$ [resp. $AA' = I_n$], ce qui signifie que A n'est pas inversible.*

Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible et calculer son inverse revient à montrer que pour tout vecteur $y \in \mathbb{K}^n$ le système linéaire de n équation à n inconnues $Ax = y$ a une unique solution et à exprimer cette solution x en fonction de y . Nous verrons plus loin comment l'algorithme de Gauss nous permet d'effectuer une telle résolution.

Exercice 8.26 *Montrer que la matrice $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ est inversible et déterminer son inverse.*

Solution 8.26 *Il s'agit de résoudre, pour $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ donné dans \mathbb{K}^2 , le système :*

$$\begin{cases} x_1 + 2x_2 = y_1 \\ 3x_1 + 4x_2 = y_2 \end{cases}$$

Multipliant la première équation par 3 et retranchant la deuxième équation au résultat obtenu, on a $2x_2 = 3y_1 - y_2$, soit $x_2 = \frac{3}{2}y_1 - \frac{1}{2}y_2$ qui reporté dans la première équation donne $x_1 = -y_1 + y_2$. On a donc :

$$\begin{cases} x_1 = -y_1 + y_2 \\ x_2 = \frac{3}{2}y_1 - \frac{1}{2}y_2 \end{cases}$$

ce qui signifie que A est inversible et que :

$$A^{-1} = \frac{1}{2} \begin{pmatrix} -4 & 2 \\ 3 & -1 \end{pmatrix}.$$

De manière plus générale, on a le résultat suivant.

Théorème 8.17 Une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$ est inversible si, et seulement si, $ad - bc \neq 0$ et dans ce cas son inverse est donné par :

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

Démonstration. Pour tous scalaires a, b, c, d , on a :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (ad - bc) I_2$$

Si $ad - bc \neq 0$, cela s'écrit $AA' = I_2$ avec $A' = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, ce qui signifie que A est inversible d'inverse A' . Réciproquement si A est inversible, on a :

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = A^{-1} \left(A \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right) = (ad - bc) A^{-1}$$

donc $ad - bc \neq 0$ (puisque $A \neq 0$) et $A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. ■

Exercice 8.27 Soit $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Pour tout entier $n \geq 1$, on désigne par A^n la matrice $A \cdot A \cdots A$, ce produit ayant n termes. On note $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et par convention $A^0 = I_2$.

1. Calculer A^2 et A^3 .
2. Montrer que pour tout entier $n \geq 1$, la matrice A^n est de la forme :

$$A^n = \begin{pmatrix} a_n + (-1)^n & a_n \\ a_n & a_n + (-1)^n \end{pmatrix}$$

où a_n est un entier.

3. Calculer $A^2 - 2A - 3I_2$.
4. Montrer que A est inversible et calculer A^{-1} .
5. Montrer que pour tout entier $n \geq 2$, il existe un polynôme Q_n et deux entiers α_n et β_n tels que :

$$X^n = Q_n(X) (X^2 - 2X - 3) + \alpha_n X + \beta_n. \quad (8.3)$$

6. En évaluant (8.3) en -1 et 3 déterminer α_n et β_n .
7. En déduire A^n pour tout $n \geq 2$.

Solution 8.27

1. On a :

$$A^2 = \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 13 & 14 \\ 14 & 13 \end{pmatrix}$$

2. C'est vrai pour $n = 1$ avec $a_1 = 2$ et en supposant le résultat acquis pour n , on a :

$$\begin{aligned} A^{n+1} &= \begin{pmatrix} a_n + (-1)^n & a_n \\ a_n & a_n + (-1)^n \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3a_n + (-1)^n & 3a_n + 2(-1)^n \\ 3a_n + 2(-1)^n & 3a_n + (-1)^n \end{pmatrix} \\ &= \begin{pmatrix} 3a_n + 2(-1)^n + (-1)^{n+1} & 3a_n + 2(-1)^n \\ 3a_n + 2(-1)^n & 3a_n + 2(-1)^n + (-1)^{n+1} \end{pmatrix} \end{aligned}$$

puisque :

$$2(-1)^n + (-1)^{n+1} = (-1)^n (2 - 1) = (-1)^n$$

3. On a $A^2 - 2A - 3I_2 = 0$.

4. On a :

$$A^{-1} = \frac{1}{3} \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}$$

par calcul direct ou avec la question précédente :

$$A^{-1} = \frac{1}{3} (A - 2I_2).$$

5. Pour $n = 2$, on a :

$$X^2 = (X^2 - 2X - 3) + 2X + 3$$

donc $Q_2 = 1$ et $(\alpha_2, \beta_2) = (2, 3)$. Supposant le résultat acquis pour $n \geq 2$, on a :

$$\begin{aligned} X^{n+1} &= XQ_n(X) (X^2 - 2X - 3) + \alpha_n X^2 + \beta_n X \\ &= XQ_n(X) (X^2 - 2X - 3) + \alpha_n ((X^2 - 2X - 3) + 2X + 3) + \beta_n X \\ &= (\alpha_n + XQ_n(X)) (X^2 - 2X - 3) + (2\alpha_n + \beta_n) X + 3\alpha_n \end{aligned}$$

soit le résultat au rang $n + 1$.

6. -1 et 3 sont les racines de $X^2 - 2X - 3$, donc :

$$\begin{cases} -\alpha_n + \beta_n = (-1)^n \\ 3\alpha_n + \beta_n = 3^n \end{cases}$$

et résolvant le système :

$$\begin{cases} \alpha_n = \frac{3^n - (-1)^n}{4} \\ \beta_n = \frac{3^n + 3(-1)^n}{4} \end{cases}$$

7. On a :

$$\begin{aligned} A^n &= \alpha_n A + \beta_n I_2 = \frac{1}{4} ((3^n - (-1)^n) A + (3^n + 3(-1)^n) I_2) \\ &= \frac{1}{4} \begin{pmatrix} 3^n - (-1)^n + 3^n + 3(-1)^n & 2(3^n - (-1)^n) \\ 2(3^n - (-1)^n) & 3^n - (-1)^n + 3^n + 3(-1)^n \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 3^n + (-1)^n & 3^n - (-1)^n \\ 3^n - (-1)^n & 3^n + (-1)^n \end{pmatrix} = \begin{pmatrix} a_n + (-1)^n & a_n \\ a_n & a_n + (-1)^n \end{pmatrix} \end{aligned}$$

avec :

$$a_n = \frac{3^n - (-1)^n}{2} \text{ et } a_n + (-1)^n = \frac{3^n + (-1)^n}{2}.$$

8.6.3 Déterminant d'une matrice d'ordre 2

Définition 8.14 Le déterminant d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$ est le scalaire :

$$\det(A) = ad - bc.$$

Ce déterminant est aussi noté :

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

Le théorème 8.17 nous dit qu'une matrice $A \in \mathcal{M}_2(\mathbb{K})$ est inversible si, et seulement si, son déterminant est non nul. Nous généraliserons plus loin cette définition du déterminant.

Avec le théorème qui suit on résume les propriétés fondamentales du déterminant des matrices d'ordre 2.

Théorème 8.18 On désigne par A, B des matrices d'ordre 2.

1. $\det(I_2) = 1$.
2. Pour tout scalaire λ , on a, $\det(\lambda A) = \lambda^2 \det(A)$.
3. $\det(AB) = \det(A) \det(B)$.
4. Si A est inversible, alors $\det(A^{-1}) = \frac{1}{\det(A)}$.
5. Si l'une des lignes [resp. des colonnes] de A est nulle, alors $\det(A) = 0$.
6. Si A' est la matrice déduite de A en permutant les deux lignes [resp. les deux colonnes], alors $\det(A') = -\det(A)$.

Démonstration. On note $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$.

1. Il suffit de vérifier.
2. On a $\lambda A = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$ et :

$$\det(\lambda A) = \lambda^2 ad - bc = \lambda^2 \det(A).$$

3. On a :

$$AB = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

et :

$$\begin{aligned} \det(AB) &= (aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') \\ &= aa'cb' + aa'dd' + bc'cb' + bc'dd' - ab'ca' - ab'dc' - bd'ca' - bd'dc' \\ &= aa'dd' + bc'cb' - ab'dc' - bd'ca' \\ &= ad(a'd' - b'c') - bc(a'd' - b'c') \\ &= (ad - bc)(a'd' - b'c') = \det(A) \det(B). \end{aligned}$$

4. Dans le cas où A est inversible, on $AA^{-1} = I_2$ et :

$$\det(A) \det(A^{-1}) = \det(AA^{-1}) = \det(I_2) = 1,$$

ce qui donne $\det(A^{-1}) = \frac{1}{\det(A)}$.

5. Résulte de la définition.

6. On a $A' = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$ [resp. $A' = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$] et :

$$\det(A') = cb - ad = -\det(A).$$

■

8.6.4 Transposée d'une matrice

Définition 8.15 Si $A = ((a_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ est une matrice à n lignes et m colonnes, la transposée de A est la matrice à m lignes et n colonnes ${}^tA = ((a'_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ où $a'_{ij} = a_{ji}$.

La transposée d'un vecteur colonne $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ est le vecteur ligne ${}^tX = (x_1, x_2, \dots, x_n)$.

En représentant $A = ((a_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ sous forme de lignes $A = \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{pmatrix}$ [resp. de colonnes

$M = (C_1, C_2, \dots, C_m)$] où :

$$L_i = (a_{i1}, a_{i2}, \dots, a_{im}) \text{ [resp. } C_j = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{n,j} \end{pmatrix}]$$

est la ligne numéro i [resp. la colonne numéro j] de M , on a :

$${}^tA = ({}^tL_1, {}^tL_2, \dots, {}^tL_n) \text{ [resp. } {}^tA = \begin{pmatrix} {}^tC_1 \\ {}^tC_2 \\ \vdots \\ {}^tC_m \end{pmatrix}]$$

Exemple 8.14 La transposée d'une matrice carrée triangulaire supérieure [resp. inférieure] est triangulaire inférieure [resp. supérieure].

Définition 8.16 On dit qu'une matrice carrée $A = ((a_{ij}))_{1 \leq i, j \leq n}$ est symétrique si elle est égale à sa transposée, ce qui revient à dire que $a_{ij} = a_{ji}$ pour tous i, j compris entre 1 et n .

Définition 8.17 On dit qu'une matrice carrée $A = ((a_{ij}))_{1 \leq i, j \leq n}$ est anti-symétrique si ${}^tA = -A$, ce qui revient à dire que $a_{ij} = -a_{ji}$ pour tous i, j compris entre 1 et n .

Remarque 8.5 Une matrice anti-symétrique a tous ses termes diagonaux nuls. En effet, pour tout i compris entre 1 et n , on $a_{ii} = -a_{ii}$ et en conséquence, $a_{ii} = 0$.

Théorème 8.19 Pour toutes matrices $A = ((a_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ et $B = ((b_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ dans $\mathcal{M}_{n,m}(\mathbb{K})$ et tout scalaire λ , on a :

$${}^t({}^tA) = A, {}^t(A+B) = {}^tA + {}^tB, {}^t(\lambda A) = \lambda {}^tA$$

Pour toutes matrices $A = ((a_{ij}))_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$ dans $\mathcal{M}_{p,n}(\mathbb{K})$ et $B = ((b_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ dans $\mathcal{M}_{n,m}(\mathbb{K})$:

$${}^t(AB) = {}^tB {}^tA$$

Si $A \in \mathcal{M}_n(\mathbb{K})$ est inversible, alors tA est aussi inversible et :

$$({}^tA)^{-1} = {}^t(A^{-1})$$

Démonstration. On a ${}^tA = ((a'_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ avec $a'_{ij} = a_{ji}$ et ${}^t({}^tA) = {}^tA' = ((a''_{ij}))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ avec $a''_{ij} = a'_{ji} = a_{ij}$. Donc ${}^t({}^tA) = A$.

Les résultats sur les combinaisons linéaires de matrices sont évidents.

Les coefficients de $C = AB$ sont les $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ et ceux de tC les :

$$c'_{ij} = c_{ji} = \sum_{k=1}^n a_{jk}b_{ki} = \sum_{k=1}^n b'_{ik}a'_{kj}$$

et on reconnaît là les coefficients de ${}^tB {}^tA$.

Si $A \in \mathcal{M}_n(\mathbb{K})$ est inversible, on a :

$$I_n = {}^tI_n = {}^t(AA^{-1}) = {}^t(A^{-1}) {}^tA$$

ce qui signifie que tA est inversible avec $({}^tA)^{-1} = {}^t(A^{-1})$. ■

Cette notion de matrice transposée nous sera utile lors de l'étude des formes bilinéaires et quadratiques.

8.6.5 Trace d'une matrice carrée

Définition 8.18 La trace d'une matrice carrée $A = ((a_{ij}))_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$ est le scalaire :

$$\text{Tr}(A) = \sum_{i=1}^n a_{ii}$$

(somme des termes diagonaux).

Exemple 8.15 La trace de la matrice identité I_n est $\text{Tr}(I_n) = n$.

Théorème 8.20 L'application trace est linéaire de $\mathcal{M}_n(\mathbb{K})$ dans \mathbb{K} (on dit que c'est une forme linéaire) et pour toutes matrices A, B dans $\mathcal{M}_n(\mathbb{K})$, on a $\text{Tr}(AB) = \text{Tr}(BA)$.

Exercice 8.28 Montrer qu'une matrice et sa transposée ont même trace.

Exercice 8.29 Calculer $\text{Tr}({}^tAA)$ pour $A = ((a_{ij}))_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$.

8.7 Systèmes d'équations linéaires

On se donne une matrice $A = ((a_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ dans $\mathcal{M}_{m,n}(\mathbb{K})$, un vecteur $b = (b_i)_{1 \leq i \leq m}$ dans \mathbb{K}^m et on s'intéresse au système linéaire $Ax = b$ d'inconnue $x = (x_i)_{1 \leq i \leq n}$ dans \mathbb{K}^n . Un tel système s'écrit :

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Pour $b = 0$, un tel système a au moins $x = 0$ comme solution. Le système $Ax = 0$ est le système homogène associé au système $Ax = b$.

En notant, pour j compris entre 1 et n , $C_j = (a_{ij})_{1 \leq i \leq m}$ la colonne numéro j de la matrice A , résoudre le système $Ax = b$ revient à trouver tous les scalaires x_1, \dots, x_n tels que :

$$x_1C_1 + x_2C_2 + \cdots + x_nC_n = b$$

Dans le cas où le nombre d'inconnues n est strictement supérieur au nombre d'équations m , le système homogène $Ax = 0$ a une infinité de solutions.

Théorème 8.21 *Pour toute matrice $A = ((a_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{m,n}(\mathbb{K})$ avec $n > m$, le système homogène $Ax = 0$ a une infinité de solutions.*

Démonstration. On sait déjà que $x = 0$ est solution.

On désigne par $B = \begin{pmatrix} A \\ 0_{n-m,n} \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$ la matrice carrée d'ordre n ayant pour m premières lignes celles de A , les suivantes étant nulles. Pour toute matrice $B' \in \mathcal{M}_n(\mathbb{K})$ la matrice BB' a sa dernière ligne nulle et ne peut donc égaler I_n , ce qui signifie que la matrice B n'est pas inversible. Il existe donc $x \in \mathbb{K}^n \setminus \{0\}$ tel que $Bx = \begin{pmatrix} Ax \\ 0_{n-m,n} \end{pmatrix} = 0$ (théorème 8.16). Le vecteur x est donc solution non nulle de $Ax = 0$ et la droite dirigée par x nous donne une infinité de solutions de ce système linéaire. ■

Exercice 8.30 *Résoudre le système linéaire :*

$$\begin{cases} 2x + y - z = 0 & (1) \\ x + y + z = 0 & (2) \end{cases}$$

Solution 8.28 *On élimine l'inconnue z en additionnant les deux équations, ce qui donne $3x + 2y = 0$, soit $y = -\frac{3}{2}x$ qui reporté dans (1) nous donne $z = \frac{1}{2}x$. Une solution de ce système est*

donc de la forme $X = \frac{x}{2}u$ où u est le vecteur $u = \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}$ et x un scalaire. Réciproquement

l'égalité $Au = 0$ nous dit que tout vecteur X colinéaire à u est solution du système.

En définitive l'ensemble des solutions de ce système est la droite $D = \mathbb{K}u$ dirigée par u .

Théorème 8.22 *Soit A dans $\mathcal{M}_n(\mathbb{K})$. Le système $Ax = b$ a une unique solution dans \mathbb{K}^n pour tout vecteur b , si et seulement si, la matrice A est inversible.*

Démonstration. Supposons A inversible. Le vecteur $A^{-1}b$ est solution de $Ax = b$ et si x est solution de ce système, on a alors $A^{-1}(Ax) = A^{-1}b$, soit $x = A^{-1}b$. Notre système a bien une unique solution.

Réciproquement, supposons que, pour tout $b \in \mathbb{K}^n$ le système $Ax = b$ a unique solution. En désignant par $(e_j)_{1 \leq j \leq n}$ la base canonique de \mathbb{K}^n et, pour tout j compris entre 1 et n , par C_j la solution de $Ax = e_j$, la matrice $A' = (C_1, \dots, C_n)$ est telle que :

$$AA' = (AC_1, \dots, AC_n) = (e_1, \dots, e_n) = I_n$$

ce qui signifie que A est inversible d'inverse A' . ■

La méthode des pivots de Gauss peut être utilisée pour résoudre un tel système. Nous décrivons dans un premier temps cette méthode sur un exemple avec l'exercice qui suit.

Exercice 8.31 Résoudre le système linéaire :

$$\begin{cases} x + y + z = 3 & (1) \\ 2x + y + z = 4 & (2) \\ x - y + z = 1 & (3) \end{cases}$$

Solution 8.29 La première étape consiste à éliminer x dans les équations (2) et (3). Pour ce faire on remplace l'équation (2) par $(2) - 2(1)$ et l'équation (3) par $(3) - (1)$, ce qui donne le système :

$$\begin{cases} x + y + z = 3 & (1) \\ -y - z = -2 & (2) \\ -2y = -2 & (3) \end{cases}$$

La deuxième étape consiste à éliminer y dans l'équation (3) en remplaçant cette équation par $(3) - 2(2)$, ce qui donne :

$$\begin{cases} x + y + z = 3 & (1) \\ -y - z = -2 & (2) \\ 2z = 2 & (3) \end{cases}$$

Le système obtenue est alors un système triangulaire et il se résout en remontant les équations, ce qui donne :

$$\begin{cases} z = 1 \\ y = 2 - z = 1 \\ x = 3 - y - z = 1 \end{cases}$$

8.8 Sommes et sommes directes de sous-espaces vectoriels

On se donne pour ce paragraphe un espace vectoriel E .

Définition 8.19 Soient F et G deux sous-espaces vectoriels de E . On dit que E est somme des espaces F et G si l'application :

$$\begin{aligned} \varphi \quad F \times G &\rightarrow E \\ (x, y) &\mapsto x + y \end{aligned}$$

est surjective et on note alors $E = F + G$.

Si cette application est bijective, on dit que E est somme directe des espaces F et G et on note $E = F \oplus G$.

Dire que $E = F + G$ signifie donc que l'on peut écrire tout vecteur $x \in E$ sous la forme $x = y + z$, où $y \in F$ et $z \in G$ et dire que $E = F \oplus G$ signifie donc que l'on peut écrire de manière unique tout vecteur $x \in E$ sous la forme $x = y + z$, où $y \in F$ et $z \in G$.

Théorème 8.23 Soient F et G deux sous-espaces vectoriels de E . On a $E = F \oplus G$ si, et seulement si, $E = F + G$ et $F \cap G = \{0\}$.

Démonstration. Supposons que $E = F \oplus G$, on a alors $E = F + G$ et tout $x \in F \cap G$ s'écrit $x = x + 0 = 0 + x$ avec $(x, 0)$ et $(0, x)$ dans $F \times G$, ce qui impose $x = 0$ puisque φ est bijective.

Réciproquement supposons que $E = F + G$ et $F \cap G = \{0\}$. Si $x \in E$ s'écrit $x = y + z = y' + z'$, avec y, y' dans F et z, z' dans G , on a alors $y - y' = z' - z \in F \cap G$, donc $y - y' = z - z' = 0$ et $(y, z) = (y', z')$. La somme est donc directe. ■

Définition 8.20 On dit que deux sous-espaces vectoriels F et G de E sont supplémentaires, si $E = F \oplus G$. On dit aussi que F est un supplémentaire de G ou que G est un supplémentaire de F dans E .

Remarque 8.6 E est l'unique supplémentaire de $\{0\}$, mais un sous-espace vectoriel F de E distinct de $\{0\}$ et de E admet une infinité de supplémentaires. Il suffit de considérer deux droites de \mathbb{R}^2 dirigées par deux vecteurs non colinéaires pour s'en convaincre.

On peut définir la somme ou la somme directe de p sous-espaces de E comme suit.

Définition 8.21 Soient $p \geq 2$ un entier et F_1, \dots, F_p des sous-espaces vectoriels de E . On dit que E est somme des espaces F_1, \dots, F_p si l'application :

$$\begin{aligned} \varphi : F_1 \times \dots \times F_p &\rightarrow E \\ (x_1, \dots, x_p) &\mapsto x_1 + \dots + x_p \end{aligned}$$

est surjective et on note alors $E = F_1 + \dots + F_p$ ou de manière plus compacte $E = \sum_{k=1}^p F_k$.

Si cette application est bijective, on dit que E est somme directe des espaces F_1, \dots, F_p et on note $E = F_1 \oplus \dots \oplus F_p$ ou $E = \bigoplus_{k=1}^p F_k$.

En fait la somme de deux sous-espaces vectoriels F et G peut se définir par :

$$F + G = \{y + z \mid y \in F \text{ et } z \in G\}.$$

Il est facile de vérifier que $F + G$ est un sous-espace vectoriel de E . Ce sous-espace n'est en général pas égal à E .

On peut aussi définir $F + G$ comme le sous-espace vectoriel de E engendré par la réunion $F \cup G$ (qui en général n'est pas un espace vectoriel).

Théorème 8.24 Si F, G sont deux sous-espaces vectoriels de E , alors la somme $F + G$ est le sous-espace vectoriel de E engendré par $F \cup G$.

Démonstration. Dire que $x \in \text{Vect}(F \cup G)$ équivaut à dire qu'il s'écrit $x = \sum_{k=1}^p \lambda_k x_k$ où les x_k sont des éléments de $F \cup G$ et les λ_k des scalaires. En séparant les x_k qui sont dans F de ceux qui sont dans G , cette somme peut s'écrire $x = y + z$ avec $y \in F$ et $z \in G$, ce qui signifie que $x \in F + G$.

Réciproquement $x \in F + G$ s'écrit $x = y + z$ avec $(y, z) \in F \times G$ et il est bien dans $\text{Vect}(F \cup G)$. ■

De manière un peu plus générale, on a le résultat suivant.

Théorème 8.25 Si F_1, \dots, F_p sont des sous-espaces vectoriels de E , alors la somme $\sum_{k=1}^p F_k$ est le sous-espace vectoriel de E engendré par $\bigcup_{k=1}^p F_k$.

Exercice 8.32 Montrer que si φ est une forme linéaire non nulle sur E , il existe alors un vecteur non nul a dans E tel que :

$$E = \ker(\varphi) \oplus \mathbb{K}a.$$

Solution 8.30 La forme linéaire φ étant non nulle, on peut trouver un vecteur a dans E tel que $\varphi(a) \neq 0$. Ce vecteur a est nécessairement non nul. Pour tout vecteur x dans E , le vecteur $h = x - \frac{\varphi(x)}{\varphi(a)}a$ est dans le noyau de φ et en écrivant que $x = h + \frac{\varphi(x)}{\varphi(a)}a$ on déduit que $E = \ker(\varphi) + \mathbb{K}a$. Si x est dans $\ker(\varphi) \cap \mathbb{K}a$ on a alors $x = \lambda a$ et $\lambda\varphi(a) = \varphi(x) = 0$ avec $\varphi(a) \neq 0$ ce qui entraîne $\lambda = 0$ et $x = 0$. On a donc $\ker(\varphi) \cap \mathbb{K}a = \{0\}$ et $E = \ker(\varphi) \oplus \mathbb{K}a$.

Espaces vectoriels réels ou complexes de dimension finie

On note toujours \mathbb{K} le corps de réels ou des complexes.

9.1 Systèmes libres, systèmes générateurs et bases

Nous avons déjà rencontré et utilisé la base canonique de \mathbb{K}^n . Nous allons donner une définition précise de cette notion dans le cadre des espaces vectoriels réels ou complexes, ce qui nous mènera à la notion de dimension.

On se donne un espace vectoriel E .

Définition 9.1 Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une famille (ou un système) de n vecteurs de E , où n est un entier naturel non nul. On dit que \mathcal{B} est :

- une famille libre, ou que les vecteurs e_1, \dots, e_n sont linéairement indépendants, si pour toute famille $(\lambda_i)_{1 \leq i \leq n}$ l'égalité $\sum_{i=1}^n \lambda_i e_i = 0$ est réalisée si, et seulement si, tous les λ_i sont nuls ;
- une famille liée, si ce n'est pas une famille libre (i. e. il existe des scalaires $\lambda_1, \dots, \lambda_n$ non tous nuls tels que $\sum_{i=1}^n \lambda_i e_i = 0$) ;
- une famille génératrice si pour tout vecteur $x \in E$, il existe des scalaires $\lambda_1, \dots, \lambda_n$ tels que $x = \sum_{i=1}^n \lambda_i e_i$;
- une base de E si elle est libre et génératrice.

Remarque 9.1 Dire que $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une famille génératrice de E équivaut à dire que $E = \text{vect}(\mathcal{B})$ (l'espace vectoriel engendré par \mathcal{B}).

Avec le théorème qui suit, on résume quelques propriétés des familles libres ou liées.

Théorème 9.1 Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une famille de n vecteurs de E , où n est un entier naturel non nul.

1. Si $n = 1$, dire que \mathcal{B} est libre [resp. liée] signifie que $e_1 \neq 0$ [resp. $e_1 = 0$].
2. Si \mathcal{B} est libre, alors tous les vecteurs e_i sont non nuls.
3. Si l'un des e_i est nul, alors \mathcal{B} est liée.
4. Si \mathcal{B} contient une famille liée, elle est elle-même liée.

5. Si \mathcal{B} est contenue dans une partie libre, elle est elle-même libre.
6. Si \mathcal{B} est liée, l'un des vecteurs e_j est combinaison linéaire des autres.
7. Si \mathcal{B} est une base de E , alors tout vecteur x de E s'écrit de manière unique comme combinaison linéaire des vecteurs e_1, \dots, e_n .

Démonstration. Résultent des définitions. ■

L'utilisation des déterminants, définis pour l'instant dans le seul cas des matrices d'ordre 2, nous donne un moyen élémentaire de vérifier que deux vecteurs de \mathbb{K}^2 sont linéairement indépendants.

Théorème 9.2 Les vecteurs $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ sont linéairement indépendants si, et seulement si :

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \neq 0.$$

Démonstration. Il revient au même de montrer que x et y sont liés si, et seulement si, $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = 0$.

Supposons le système (x, y) lié. On a alors $y = \lambda x$ ou $x = \lambda y$ pour un scalaire λ et, par exemple dans le premier cas :

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = \begin{vmatrix} x_1 & \lambda x_1 \\ x_2 & \lambda x_2 \end{vmatrix} = \lambda(x_1 x_2 - x_1 x_2) = 0.$$

Réciproquement, on suppose que $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = 0$.

Si $x = 0$ ou $y = 0$, le système (x, y) est alors lié.

Si x et y sont non nuls, en supposant que y_2 est non nul, l'égalité $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1 y_2 - y_1 x_2 = 0$ entraîne (c'est même équivalent) :

$$y_2 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - x_2 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

avec $(y_2, -x_2) \neq (0, 0)$, ce qui signifie que x et y sont liés. Si $y_2 = 0$, on a alors $y_1 \neq 0$ et on écrit que l'égalité $x_1 y_2 - x_2 y_1 = 0$ entraîne :

$$x_1 \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} - y_1 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

avec $(x_1, -y_1) \neq (0, 0)$. ■

Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base de E , alors tout vecteur $x \in E$ s'écrit $x = \sum_{i=1}^n \lambda_i e_i$ et les scalaires λ_i qui sont uniquement déterminés sont appelés les composantes ou coordonnées de x dans la base \mathcal{B} . Réciproquement une telle famille \mathcal{B} vérifiant cette propriété est une base de E .

La base canonique de \mathbb{K}^n est bien une base au sens de la définition qu'on a donné.

Exemple 9.1 Dans l'espace $\mathbb{R}_n[x]$ [resp. $\mathbb{C}_n[x]$] des fonctions polynomiales réelles [resp. complexes] de degré au plus égal à n , la famille de polynômes $(1, x, \dots, x^n)$ est une base puisque tout polynôme dans $\mathbb{R}_n[x]$ [resp. $\mathbb{C}_n[x]$] s'écrit sous la forme $P = \sum_{k=0}^n a_k x^k$, les réels [resp. complexes] a_k étant uniquement déterminés. On dit que cette base est la base canonique de $\mathbb{R}_n[x]$ [resp. $\mathbb{C}_n[x]$]

Le résultat de l'exercice qui suit est à retenir.

Exercice 9.1 Soient n un entier naturel et $\mathcal{B} = (P_0, P_1, \dots, P_n)$ une famille de polynômes dans $\mathbb{K}_n[x]$ telle que P_k soit de degré k , pour tout k compris entre 0 et n (P_0 est constant non nul). On dit qu'une telle famille de polynômes est échelonnée en degrés. Montrer que \mathcal{B} est une base de $\mathbb{K}_n[x]$.

Solution 9.1 Notons, pour k compris entre 0 et n :

$$P_k(x) = a_{k,0} + a_{k,1}x + \dots + a_{k,k}x^k = \sum_{j=0}^k a_{k,j}x^j$$

où le coefficient $a_{k,k}$ est non nul.

Nous allons montrer le résultat par récurrence sur $n \geq 0$.

Pour $n = 0$, $\mathbb{K}_0[x]$ est l'espace des fonctions (ou polynômes) constantes sur \mathbb{K} et P_0 est non nul dans cet espace, donc libre, et en écrivant tout polynôme constant sous la forme :

$$P(x) = a = \frac{a}{P_0}P_0 = \lambda P_0,$$

on voit que P_0 engendre $\mathbb{K}_0[x]$. Donc (P_0) est une base de $\mathbb{K}_0[x]$.

Supposons le résultat acquis au rang $n \geq 0$ et soit $\mathcal{B} = (P_0, P_1, \dots, P_{n+1})$ une famille de polynômes échelonnée en degrés dans $\mathbb{K}_{n+1}[x]$. La famille (P_0, P_1, \dots, P_n) est alors échelonnée en degrés dans $\mathbb{K}_n[x]$ et l'hypothèse de récurrence nous dit qu'elle forme une base de $\mathbb{K}_n[x]$. On se donne un polynôme P dans $\mathbb{K}_{n+1}[x]$. Si P est de degré inférieur ou égal à n , il est dans $\mathbb{K}_n[x]$ et s'écrit comme combinaison linéaire de P_0, P_1, \dots, P_n , sinon il est de la forme $P(x) = Q(x) + a_{n+1}x^{n+1}$ avec Q dans $\mathbb{K}_n[x]$ et $a_{n+1} \neq 0$. En écrivant que :

$$x^{n+1} = \frac{1}{a_{n+1,n+1}}P_{n+1}(x) - \sum_{j=0}^n \frac{a_{n+1,j}}{a_{n+1,n+1}}x^j,$$

on déduit que $P(x) = R(x) + \frac{a_{n+1}}{a_{n+1,n+1}}P_{n+1}(x)$ avec R dans $\mathbb{K}_n[x]$, donc combinaison linéaire de P_0, P_1, \dots, P_n et P est combinaison linéaire de P_0, P_1, \dots, P_{n+1} . Le système \mathcal{B} est donc générateur de $\mathbb{K}_{n+1}[x]$.

Si on a l'égalité $\sum_{j=0}^{n+1} \lambda_j P_j = 0$, alors $\lambda_{n+1}P_{n+1} = -\sum_{j=0}^n \lambda_j P_j$ est dans $\mathbb{K}_n[x]$ et λ_{n+1} est nécessairement nul puisque P_{n+1} qui est de degré $n+1$ n'est pas dans $\mathbb{K}_n[x]$. On a alors $\sum_{j=0}^n \lambda_j P_j$ et tous les λ_j sont nuls puisque (P_0, P_1, \dots, P_n) une base de $\mathbb{K}_n[x]$. Le système \mathcal{B} est donc libre et c'est une base de $\mathbb{K}_{n+1}[x]$.

Exercice 9.2 Montrer que la famille $\mathcal{B} = (L_0, L_1, L_2)$ de polynômes de $\mathbb{K}_2[x]$ définie par :

$$\begin{cases} L_0(x) = (x-1)(x-2) \\ L_1(x) = x(x-2) \\ L_2(x) = x(x-1) \end{cases}$$

forme une base de $\mathbb{K}_2[x]$. En déduire que pour tout polynôme P dans $\mathbb{K}_2[x]$ on a :

$$\int_0^2 P(t) dt = \frac{P(0) + 4P(1) + P(2)}{3}$$

(formule des trois niveaux).

Solution 9.2 Supposons que $\lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2 = 0$. Prenant les valeurs successives $x = 0, 1, 2$, on déduit que $\lambda_0 = \lambda_1 = \lambda_2 = 0$. Le système \mathcal{B} est donc libre. Étant donné $P = ax^2 + bx + c$, on cherche des scalaires $\lambda_0, \lambda_1, \lambda_2$ tels que :

$$ax^2 + bx + c = \lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2.$$

Là encore les valeurs $x = 0, 1, 2$ nous donne :

$$\begin{cases} 2\lambda_0 = c \\ -\lambda_1 = a + b + c \\ 2\lambda_2 = 4a + 2b + c \end{cases}$$

ce qui détermine de manière unique les scalaires $\lambda_0, \lambda_1, \lambda_2$. Le système \mathcal{B} est donc générateur et c'est une base de $\mathbb{K}_2[x]$.

Tout polynôme P dans $\mathbb{K}_2[x]$ s'écrit donc de manière unique $P = \lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2$ avec $\lambda_0 = \frac{P(0)}{2}$, $\lambda_1 = -P(1)$ et $\lambda_2 = \frac{P(2)}{2}$. On a alors :

$$\begin{aligned} \int_0^2 P(t) dt &= \frac{P(0)}{2} \int_0^2 L_0(t) dt - P(1) \int_0^2 L_1(t) dt + \frac{P(2)}{2} \int_0^2 L_2(t) dt \\ &= \frac{P(0) + 4P(1) + P(2)}{3} \end{aligned}$$

On se limitera dans ce chapitre aux familles libres ou génératrices qui sont finies. Mais en réalité, on est rapidement amené à considérer des familles qui peuvent être infinies. On donne donc les définitions suivantes (qui ne seront pas utilisées au niveau élémentaire où se situe ce cours).

Définition 9.2 Soit $\mathcal{B} = (e_i)_{i \in I}$ une famille de vecteurs de E , où I est un ensemble non vide quelconque (fini ou infini) d'indices. On dit que \mathcal{B} est :

- une famille libre, ou que les vecteurs e_i , pour $i \in I$ sont linéairement indépendants, si toute sous-famille finie de \mathcal{B} est libre, ce qui signifie que pour tout sous-ensemble non vide et fini J de I , une combinaison linéaire $\sum_{j \in J} \lambda_j e_j$, où les λ_j pour $j \in J$ sont des scalaires, est nulle si, et seulement si, tous ces λ_j sont nuls ;
- une famille liée, si ce n'est pas une famille libre (i. e. il existe une partie finie J de I et des scalaires λ_j où j décrit J qui sont non tous nuls tels que $\sum_{j \in J} \lambda_j e_j = 0$) ;
- une famille génératrice si l'espace vectoriel engendré par \mathcal{B} est l'espace E tout entier, ce qui signifie que pour tout vecteur $x \in E$, il existe une partie finie J de I et des scalaires λ_j où j décrit J tels que $x = \sum_{j \in J} \lambda_j e_j$;
- une base de E si elle est libre et génératrice.

Exercice 9.3 On désigne par E l'espace vectoriel des applications de \mathbb{R} dans \mathbb{R} et pour tout entier $k \geq 1$ par f_k la fonction définie sur \mathbb{R} par :

$$\forall x \in \mathbb{R}, f_k(x) = \sin(kx).$$

Montrer que la famille (f_1, f_2, f_3) est libre dans E .

Solution 9.3 Soient $\lambda_1, \lambda_2, \lambda_3$ des réels tels que :

$$\forall x \in \mathbb{R}, \lambda_1 \sin(x) + \lambda_2 \sin(2x) + \lambda_3 \sin(3x) = 0.$$

En dérivant deux fois, on a :

$$\forall x \in \mathbb{R}, \lambda_1 \sin(x) + 4\lambda_2 \sin(2x) + 9\lambda_3 \sin(3x) = 0.$$

et retranchant ces deux équations, on a :

$$\forall x \in \mathbb{R}, 3\lambda_2 \sin(2x) + 8\lambda_3 \sin(3x) = 0.$$

Prenant $x = \frac{\pi}{2}$ dans cette troisième équation on obtient $\lambda_3 = 0$ et la première donne $\lambda_1 = \lambda_3 = 0$. Il reste donc $\lambda_2 \sin(2x) = 0$ et $\lambda_2 = 0$. La famille (f_1, f_2, f_3) est donc libre dans E .

Un peu plus généralement, on a le résultat suivant.

Exercice 9.4 On désigne par E l'espace vectoriel des applications de \mathbb{R} dans \mathbb{R} . Montrer, pour tous réels $0 < a_1 < a_2 < \dots < a_n$, la famille :

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

est libre dans E (ce qui peut se traduire en disant que la famille de fonctions $\{f_a : x \mapsto \sin(ax) \mid a \in \mathbb{R}^{+,*}\}$ est libre dans E).

Solution 9.4 On procède par récurrence sur $n \geq 1$.

Pour $n = 1$, la fonction $f_a : x \mapsto \sin(ax)$ n'est pas la fonction nulle, donc (f_a) est libre dans E .

Supposons le résultat acquis au rang $n - 1 \geq 1$ et soient $0 < a_1 < a_2 < \dots < a_n$, $\lambda_1, \lambda_2, \dots, \lambda_n$ des réels tels que :

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

En dérivant deux fois, on a :

$$\forall x \in \mathbb{R}, \sum_{k=1}^n \lambda_k a_k^2 \sin(a_k x) = 0.$$

Il en résulte que :

$$\forall x \in \mathbb{R}, \sum_{k=1}^{n-1} \lambda_k (a_k^2 - a_n^2) \sin(a_k x) = 0.$$

et l'hypothèse de récurrence nous dit que $\lambda_k (a_k^2 - a_n^2) = 0$ pour tout k compris entre 1 et $n - 1$, ce qui équivaut à dire que $\lambda_k = 0$ pour tout k compris entre 1 et $n - 1$ puisque $a_k^2 \neq a_n^2$ pour $k \neq n$. Il reste alors $\lambda_n f_{a_n} = 0$ dans E et $\lambda_n = 0$. On a donc ainsi montré que la famille $(f_{a_k})_{1 \leq k \leq n}$ est libre dans E .

9.2 Espaces vectoriels de dimension finie

Le théorème qui suit est essentiel pour définir la notion de dimension finie.

Théorème 9.3 Si un espace vectoriel E admet une famille génératrice \mathcal{B} formée de $n \geq 1$ éléments, alors toute famille libre dans E a au plus n éléments (ce qui équivaut à dire qu'un système de plus de $n + 1$ vecteurs est lié).

Démonstration. On procède par récurrence sur n .

Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une famille génératrice de E .

Si $n = 1$, alors pour tout couple (x, y) de vecteurs non nuls de E on peut trouver deux scalaires non nuls λ et μ tels que $x = \lambda e_1$ et $y = \mu e_1$ et on a la combinaison linéaire nulle $\mu x - \lambda y = 0$ avec μ et $-\lambda$ non nuls, ce qui signifie que le système (x, y) est lié. Il ne peut donc exister de famille libre à 2 éléments dans E et a fortiori il ne peut en exister à plus de 2 éléments.

Supposons le résultat acquis au rang $n - 1 \geq 1$, c'est-à-dire que dans tout espace vectoriel F admettant un système générateur de $n - 1$ vecteurs une famille de plus de n vecteurs est liée. Supposons que E soit un espace vectoriel admettant une famille génératrice à n éléments. Supposons qu'il existe une famille libre ayant $m \geq n + 1$ éléments. On peut extraire de cette famille une famille libre à $n + 1$ éléments puisque toute sous-famille d'une famille libre est libre. Soit $\mathcal{L} = (f_i)_{1 \leq i \leq n+1}$ une telle famille. Comme $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est génératrice, il existe des scalaires a_{ij} tels que :

$$\begin{cases} f_1 = a_{11}e_1 + \cdots + a_{1n}e_n \\ \vdots \\ f_{n+1} = a_{n+1,1}e_1 + \cdots + a_{n+1,n}e_n \end{cases}$$

Si tous les $a_{i,n}$ sont nuls alors les f_i sont dans l'espace vectoriel F engendré par les $n - 1$ vecteurs e_1, \dots, e_{n-1} et en conséquence liés (hypothèse de récurrence), en contradiction avec \mathcal{L} libre. Il existe donc un indice i compris entre 1 et $n + 1$ tel que $a_{i,n} \neq 0$ et en changeant au besoin la numérotation des éléments de \mathcal{L} on peut supposer que $i = n + 1$. Les n vecteurs :

$$\begin{cases} g_1 = a_{n+1,n}f_1 - a_{1n}f_{n+1} \\ \vdots \\ g_n = a_{n+1,n}f_1 - a_{nn}f_{n+1} \end{cases}$$

sont dans l'espace vectoriel F engendré par les $n - 1$ vecteurs e_1, \dots, e_{n-1} (on a annulé les composantes en e_{n+1}) et en conséquence liés (hypothèse de récurrence), c'est-à-dire qu'il existe des scalaires $\lambda_1, \dots, \lambda_n$ non tous nuls tels que :

$$\lambda_1 g_1 + \cdots + \lambda_n g_n = 0$$

ce qui entraîne :

$$a_{n+1,n}(\lambda_1 f_1 + \cdots + \lambda_n f_n) - (\lambda_1 a_{1n} + \cdots + \lambda_n a_{nn}) f_{n+1} = 0$$

les scalaires $a_{n+1,n}\lambda_1, \dots, a_{n+1,n}\lambda_n$ n'étant pas tous nuls. Ce qui nous dit encore que les f_i sont liés et est en contradiction avec \mathcal{L} libre. Il est donc impossible de trouver un tel système \mathcal{L} libre. ■

Définition 9.3 On dit qu'un espace vectoriel est de dimension finie s'il est réduit à $\{0\}$ ou s'il est différent de $\{0\}$ et admet une base formée d'un nombre fini de vecteurs. Dans le cas contraire, on dit qu'il est de dimension infinie.

On déduit alors du théorème précédent le suivant.

Théorème 9.4 Si E un espace vectoriel non réduit à $\{0\}$ et de dimension finie, alors toutes les bases ont le même nombre d'éléments.

Démonstration. Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n'}$ sont deux bases de l'espace vectoriel E , ce sont alors deux familles génératrices et libres et le théorème précédent nous dit que $n' \leq n$ et $n \leq n'$, soit $n = n'$. ■

On peut alors donner la définition suivante.

Définition 9.4 Si E est un espace vectoriel non réduit à $\{0\}$ et de dimension finie, alors sa dimension est le nombre de l'une quelconque de ses bases. On note $\dim_{\mathbb{K}}(E)$ (ou simplement $\dim(E)$) cette dimension.

Par convention, on dira que l'espace vectoriel $\{0\}$ est de dimension 0.

Un espace vectoriel E est donc de dimension 0 si, et seulement si, il est réduit à $\{0\}$.

Dans le cas général on peut montrer, mais cela dépasse le niveau de ce cours d'introduction, que tout espace vectoriel admet une base (finie ou infinie).

On appelle droite tout espace vectoriel de dimension 1 et plan tout espace vectoriel de dimension 2.

Exemple 9.2 Bien entendu l'espace \mathbb{K}^n est de dimension n .

Exemple 9.3 L'ensemble \mathbb{C} des nombres complexes est un espace vectoriel réel de dimension 2 et un espace vectoriel complexe de dimension 1, soit $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ et $\dim_{\mathbb{C}}(\mathbb{C}) = 1$.

Exemple 9.4 Pour tout entier naturel n , l'espace $\mathbb{K}_n[x]$ des fonctions polynomiales de degré au plus égal à n est de dimension $n + 1$.

Exemple 9.5 Pour tous entiers naturels non nuls n et m , l'espace $\mathcal{M}_{m,n}(\mathbb{K})$ des matrices à m lignes et n colonnes est un espace vectoriel de dimension $m \cdot n$. En particulier l'espace $\mathcal{M}_n(\mathbb{K})$ des matrices carrées d'ordre n est de dimension n^2 .

La base canonique de $\mathcal{M}_{m,n}(\mathbb{K})$ est $(E_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ où $E_{i,j}$ est la matrice dont tous les coefficients sont nuls sauf celui en position (i, j) .

Exemple 9.6 L'espace des fonctions définies sur un intervalle réel I et à valeurs réelles est de dimension infinie (l'exercice 9.4 nous montre qu'on peut trouver des familles libres ayant une infinité d'éléments). Il admet des bases, mais il n'est pas possible d'en expliciter une.

Exercice 9.5 Montrer que la dimension de l'espace des matrices carrées A d'ordre n qui sont symétriques (i. e. telles que ${}^t A = A$) est égale à $\frac{n(n+1)}{2}$ et que la dimension de l'espace des matrices carrées A d'ordre n qui sont anti-symétriques (i. e. telles que ${}^t A = -A$) est égale à $\frac{n(n-1)}{2}$.

Solution 9.5 Laissée au lecteur.

Remarque 9.2 Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base E , on a alors $E = \text{vect}(\mathcal{B})$.

Le théorème qui suit explique l'importance de l'espace vectoriel \mathbb{K}^n .

Théorème 9.5 Un espace vectoriel de dimension n est isomorphe à \mathbb{K}^n .

Démonstration. C'est le choix d'une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E qui nous permet de définir un isomorphisme de E sur \mathbb{K}^n . En effet l'unicité de l'écriture de tout vecteur x de E sous la forme $x = \sum_{k=1}^n \lambda_k e_k$ se traduit en disant que l'application :

$$\begin{aligned} E &\rightarrow \mathbb{K}^n \\ x = \sum_{k=1}^n \lambda_k e_k &\mapsto (\lambda_1, \lambda_2, \dots, \lambda_n) \end{aligned}$$

est bijective et il est facile de vérifier que cette application est linéaire. ■

Théorème 9.6 Soit E un espace vectoriel de dimension $n \geq 1$.

1. Une famille libre dans E a au plus n élément et c'est une base si, et seulement si, elle a exactement n éléments.
2. Une famille génératrice dans E a au moins n élément et c'est une base si, et seulement si, elle a exactement n éléments.

Démonstration. Le cas $n = 1$ est laissé au lecteur et on suppose que $n \geq 2$.

1. Le théorème 9.3 nous dit qu'une famille libre dans E a au plus n élément et si c'est une base, elle a obligatoirement n éléments. Il reste à montrer qu'une famille libre de n éléments est une base. Pour ce faire il suffit de montrer qu'elle est génératrice. Notons $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une telle famille libre. Pour tout vecteur $x \in E$ la famille $\mathcal{B} \cup \{x\}$ est liée puisque formée de $n + 1$ éléments, il existe donc des scalaires $\lambda, \lambda_1, \dots, \lambda_n$ non tous nuls tels que $\lambda x + \sum_{i=1}^n \lambda_i e_i = 0$. Si $\lambda = 0$, on a alors $\sum_{i=1}^n \lambda_i e_i = 0$ et tous les λ_i sont nuls puisque \mathcal{B} est libre, ce qui n'est pas possible. On a donc $\lambda \neq 0$ et $x = -\sum_{i=1}^n \frac{\lambda_i}{\lambda} e_i$. On a donc ainsi montré que \mathcal{B} est génératrice et que c'est une base.
2. Le théorème 9.3 nous dit qu'une famille génératrice dans E a au moins n élément et si c'est une base, elle a obligatoirement n éléments. Il reste à montrer qu'une famille génératrice de n éléments est une base. Pour ce faire il suffit de montrer qu'elle est libre. Notons $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une telle famille génératrice. Si cette famille est liée, l'un des e_i , disons e_n , est combinaison linéaire des autres et la famille $(e_i)_{1 \leq i \leq n-1}$ est génératrice, ce qui est en contradiction avec le théorème 9.3. La famille \mathcal{B} est donc génératrice et c'est une base de E . ■

On retient de ces résultats que pour montrer qu'une famille finie \mathcal{B} de vecteurs est une base de E , on peut procéder comme suit :

- si on ne connaît pas la dimension de E , on montre que \mathcal{B} est génératrice et libre ;
- si on sait que E est de dimension n , on vérifie que \mathcal{B} a exactement n éléments et on montre que \mathcal{B} est libre ou qu'elle est génératrice (il est inutile de montrer les deux points).

On a défini un espace vectoriel de dimension finie comme un espace vectoriel admettant une base finie. Le théorème qui suit nous dit qu'on peut aussi définir un espace vectoriel de dimension finie comme un espace vectoriel admettant une famille génératrice finie.

Théorème 9.7 Soit E un espace vectoriel admettant une famille génératrice finie. De cette famille on peut extraire une base et E est de dimension finie.

Démonstration. Soit $\mathcal{G} = (u_i)_{1 \leq i \leq p}$ une famille génératrice de E . Si cette famille est libre, elle constitue alors une base de E et E est de dimension p . Sinon, cette famille est liée et l'un de ses éléments, disons u_p est combinaison linéaire des autres (en changeant la numérotation des éléments de G on peut toujours se ramener à ce cas de figure), ce qui implique que la famille $\mathcal{G}' = (u_i)_{1 \leq i \leq p-1}$ est encore génératrice. Si cette famille est libre, c'est alors une base et E est de dimension finie, sinon on recommence. En un nombre fini de telles opérations on construit ainsi une base de E formée de $n \leq p$ éléments. ■

Théorème 9.8 (base incomplète) *Soit E un espace vectoriel de dimension $n \geq 1$. Toute famille libre à p éléments dans E (nécessairement $1 \leq p \leq n$) peut se compléter en une base.*

Démonstration. Soient $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E et $\mathcal{L} = (u_i)_{1 \leq i \leq p}$ une famille libre dans E . On sait déjà que $p \leq n$. Si $p = n$, \mathcal{L} est alors une base.

Supposons que $p < n$. Il existe alors un vecteur e_k dans \mathcal{B} tel que $\mathcal{L}' = \mathcal{L} \cup \{e_k\}$ soit libre. En effet si un tel système est lié pour tout entier k compris entre 1 et n , il existe alors, pour chaque entier k , des scalaires $\lambda_1, \dots, \lambda_p, \lambda_{p+1}$ non tous nuls tels que $\sum_{i=1}^p \lambda_i u_i + \lambda_{p+1} e_k = 0$. Si

$\lambda_{p+1} = 0$, on a alors $\sum_{i=1}^p \lambda_i u_i = 0$ et tous les λ_i sont nuls puisque \mathcal{L} est libre. On a donc $\lambda_{p+1} \neq 0$

et $e_k = -\sum_{i=1}^p \frac{\lambda_i}{\lambda_{p+1}} u_i$. En conséquence, tous les vecteurs de la base \mathcal{B} sont combinaisons linéaires des éléments de \mathcal{L} et \mathcal{L} est alors générateur de E , ce qui est impossible pour $p < n$. Le système \mathcal{L}' est donc libre. Si $p+1 = n$, c'est une base et sinon on recommence. On arrive ainsi à compléter \mathcal{L} en une base de E au bout d'un nombre fini d'opérations. ■

Les deux corollaires qui suivent sont des résultats importants à retenir.

Corollaire 9.1 *Soit E un espace vectoriel de dimension n . Tout sous-espace vectoriel F de E est de dimension finie $m \leq n$ et $m = n$ si, et seulement si, $F = E$.*

Démonstration. Si $F = \{0\}$, il est alors de dimension $0 \leq n$ et $n = 0$ équivaut à $F = E$.

On suppose que $F \neq \{0\}$ (donc $n \geq 1$).

Montrons tout d'abord que F est de dimension finie. Comme $n+1$ vecteurs de F sont nécessairement liés, on peut définir l'entier m comme le plus grand entier pour lequel on peut trouver m vecteurs de F linéairement indépendants. On a $m \geq 1$ puisque $F \neq \{0\}$ et $m \leq n$ d'après le théorème 9.3. Soient donc $(f_i)_{1 \leq i \leq m}$ une famille libre dans F . Pour tout vecteur $x \in F$, la famille (f_1, \dots, f_m, x) est liée et x est combinaison linéaire des f_i puisque $(f_i)_{1 \leq i \leq m}$ est libre. La famille $(f_i)_{1 \leq i \leq m}$ est donc une base de F et cet espace est de dimension finie $m \leq n$.

Si $m = n$, une base de F est aussi une base de E et $F = E$. La réciproque est évidente. ■

Corollaire 9.2 *Tout sous-espace-vectoriel F d'un espace vectoriel E de dimension finie admet des supplémentaires et pour tout supplémentaire G de F dans E , on :*

$$\dim(E) = \dim(F) + \dim(G). \quad (9.1)$$

Démonstration. On suppose que F est un sous-espace vectoriel strict de E , c'est-à-dire que $F \neq \{0\}$ et $F \neq E$. On a alors $1 \leq p = \dim(F) \leq n-1$.

Une base $\mathcal{L} = (u_i)_{1 \leq i \leq p}$ de F se complète en une base $\mathcal{B} = (u_i)_{1 \leq i \leq n}$ et on vérifie facilement que le sous-espace vectoriel G de E engendré par $\mathcal{L}' = (u_i)_{p+1 \leq i \leq n}$ est un supplémentaire de F . Pour cet espace G , on a $\dim(G) = n - p = \dim(E) - \dim(F)$.

Réciproquement si $E = F \oplus G$, on vérifie facilement que la réunion d'une base de F et d'une base de G nous fournit une base de E , ce qui implique que $\dim(E) = \dim(F) + \dim(G)$. ■

De manière plus générale, on peut montrer que si E est un espace vectoriel de dimension finie ou non, alors tout sous-espace vectoriel de E admet une supplémentaire dans E .

L'égalité (9.1) pour $E = F \oplus G$ peut se généraliser.

Théorème 9.9 *Soit E un espace vectoriel de dimension n . Si E est somme directe de $p \geq 2$ sous espaces stricts F_1, \dots, F_p , soit $E = \bigoplus_{k=1}^p F_k$, alors en désignant, pour tout k compris entre 1 et p , par \mathcal{B}_k une base de F_k , la famille $\mathcal{B} = \bigcup_{k=1}^p \mathcal{B}_k$ est une base de E et :*

$$\dim(E) = \sum_{k=1}^p \dim(F_k).$$

Démonstration. On vient de voir que le résultat est vrai pour $p = 2$ et une récurrence nous montre qu'il est vrai pour tout $p \geq 2$. ■

Dans le cas de la somme, non nécessairement directe, de deux sous-espaces d'un espace de dimension finie, on a le résultat suivant.

Théorème 9.10 *Soient E un espace vectoriel de dimension finie et F, G deux sous espaces vectoriels de E . On a :*

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

Démonstration. Comme $F \cap G$ est un sous-espace de G , il admet un supplémentaire H dans G :

$$G = (F \cap G) \oplus H$$

Ce sous-espace H de G est aussi un sous-espace de $F + G$.

En fait H est un supplémentaire de F dans $F + G$.

En effet, on a $F + H \subset F + G$ puisque $H \subset G$ et tout $x \in F + G$ s'écrit $x = y + z$ avec $y \in F$ et $z \in G = (F \cap G) \oplus H$, donc $z = z_1 + z_2$ avec $z_1 \in F \cap G \subset F$ et $z_2 \in H$, ce qui donne $x = (y + z_1) + z_2 \in F + H$. On a donc $F + G \subset F + H$ et l'égalité $F + G = F + H$.

Si maintenant x est dans $F \cap H$, il est dans $F \cap G$ puisque $H \subset G$, donc dans $(F \cap G) \cap H = \{0\}$. On a donc $F \cap H = \{0\}$ et $F + G = F \oplus H$.

Il en résulte que :

$$\begin{aligned} \dim(F + G) &= \dim(F) + \dim(H) \\ &= \dim(F) + \dim(G) - \dim(F \cap G). \end{aligned}$$

■

Ce résultat a pour conséquence le résultat suivant très utile pour montrer qu'un espace est somme directe de deux sous-espaces.

Théorème 9.11 *Soient E un espace vectoriel de dimension finie et F, G deux sous espaces vectoriels de E . On a :*

$$\begin{aligned} (E = F \oplus G) &\Leftrightarrow E = F + G \text{ et } \dim(E) = \dim(F) + \dim(G) \\ &\Leftrightarrow F \cap G = \{0\} \text{ et } \dim(E) = \dim(F) + \dim(G) \end{aligned}$$

Démonstration. On sait déjà que si $E = F \oplus G$, alors $E = F + G$, $F \cap G = \{0\}$ et $\dim(E) = \dim(F) + \dim(G)$.

Supposons que $E = F + G$ et $\dim(E) = \dim(F) + \dim(G)$. Le théorème précédent nous dit alors que $\dim(F \cap G) = 0$, soit que $F \cap G = \{0\}$ et on a $E = F \oplus G$.

De même si $F \cap G = \{0\}$ et $\dim(E) = \dim(F) + \dim(G)$, on a alors $F + G = F \oplus G$ et cet espace a même dimension que E , donc $E = F \oplus G$. ■

Les propriétés des applications linéaires injectives, surjectives ou bijectives décrites par le théorème qui suit sont importantes.

Théorème 9.12 Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F .

1. Si u est injective, elle transforme alors tout système libre de E en un système libre de F et $\dim(E) \leq \dim(F)$.
2. Si u est surjective, elle transforme alors tout système générateur de E en un système générateur de F et $\dim(F) \leq \dim(E)$.
3. Si u est bijective, elle transforme alors toute base de E en une base de F et $\dim(E) = \dim(F)$ (deux espaces vectoriels de dimension finie isomorphes ont la même dimension).
4. Si $\dim(E) = \dim(F)$, alors :

$$u \text{ bijective} \Leftrightarrow u \text{ injective} \Leftrightarrow u \text{ surjective}.$$

Démonstration.

1. Soit $\mathcal{L} = (x_i)_{1 \leq i \leq p}$ un système libre dans E . Si $\sum_{i=1}^p \lambda_i u(x_i) = 0$, on a alors du fait de la linéarité de u , $u\left(\sum_{i=1}^p \lambda_i x_i\right) = 0$, ce qui signifie que $\sum_{i=1}^p \lambda_i x_i$ est dans le noyau de u , donc nul puisque u est injective, ce qui équivaut à la nullité de tous les coefficients λ_i puisque \mathcal{L} est libre. La famille $u(\mathcal{L})$ est donc libre.
Prenant pour \mathcal{L} une base de E , elle est formée de $n = \dim(E)$ éléments et $u(\mathcal{L})$ est libre à n éléments dans F , donc $n \leq m = \dim(F)$.
2. Soit $\mathcal{L} = (x_i)_{1 \leq i \leq p}$ un système générateur de E . Comme u est surjective tout vecteur y de F s'écrit $y = u(x)$ avec x dans E qui s'écrit $x = \sum_{i=1}^p \lambda_i x_i$, ce qui donne $y = \sum_{i=1}^p \lambda_i u(x_i)$.
Le système $u(\mathcal{L})$ est donc générateur de F .
Prenant pour \mathcal{L} une base de E , elle est formée de n éléments et $u(\mathcal{L})$ est générateur de F à n éléments, donc $n \geq m$.
3. et 4. Résultent des deux points précédents.

■

Le théorème 9.5 et le point 3. du théorème précédent nous disent que deux espaces vectoriels de dimension finie ont même dimension si, et seulement si, ils sont isomorphes.

En vue de généraliser le théorème 9.11, on utilisera le résultat suivant.

Lemme 9.1 Si F_1, \dots, F_p sont des espaces vectoriels de dimension finie, il en est de même de l'espace produit $F = F_1 \times \dots \times F_p$ et on a :

$$\dim(F) = \sum_{k=1}^p \dim(F_k).$$

Démonstration. Pour $p = 1$, il n'y a rien à montrer.

En procédant par récurrence sur $p \geq 2$, il suffit de montrer le résultat pour $p = 2$.

Pour ce faire, on vérifie que si $\mathcal{B}_1 = (e_i)_{1 \leq i \leq n}$ est une base de F_1 et $\mathcal{B}_2 = (f_j)_{1 \leq j \leq m}$ une base de F_2 , alors la famille :

$$\mathcal{B} = \{(e_i, 0) \mid 1 \leq i \leq n\} \cup \{(0, f_j) \mid 1 \leq j \leq m\}$$

est une base de $F = F_1 \times F_2$. En effet tout vecteur $z = (x, y)$ dans F s'écrit :

$$z = \left(\sum_{i=1}^n \lambda_i e_i, \sum_{j=1}^m \mu_j f_j \right) = \sum_{i=1}^n \lambda_i (e_i, 0) + \sum_{j=1}^m \mu_j (0, f_j)$$

donc \mathcal{B} engendre F et l'égalité :

$$\sum_{i=1}^n \lambda_i (e_i, 0) + \sum_{j=1}^m \mu_j (0, f_j) = 0$$

est équivalente à :

$$\left(\sum_{i=1}^n \lambda_i e_i, \sum_{j=1}^m \mu_j f_j \right) = (0, 0)$$

soit à $\sum_{i=1}^n \lambda_i e_i = 0$ et $\sum_{j=1}^m \mu_j f_j = 0$ qui impose $\lambda_i = 0$ pour tout i compris entre 1 et n et $\mu_j = 0$ pour tout j compris entre 1 et m . La famille \mathcal{B} est donc libre et c'est une base de F . L'espace F est donc de dimension finie égale au nombre d'éléments de \mathcal{B} , soit à $n + m$. ■

Théorème 9.13 Si F_1, \dots, F_p sont des sous-espaces vectoriels d'un espace vectoriel E de dimension finie, on a alors $E = \bigoplus_{k=1}^n F_k$ si, et seulement si, $E = \sum_{k=1}^p F_k$ et $\dim(E) = \sum_{k=1}^p \dim(F_k)$.

Démonstration. On sait déjà que la condition est nécessaire.

Dire que $E = \sum_{k=1}^p F_k$, équivaut à dire que l'application linéaire :

$$\begin{array}{ccc} \varphi & F = F_1 \times \dots \times F_p & \rightarrow & E \\ & (x_1, \dots, x_p) & \mapsto & x_1 + \dots + x_p \end{array}$$

est surjective et si de plus $\dim(F) = \dim(E)$, cette application est en fait une bijection ce qui signifie que $E = \bigoplus_{k=1}^n F_k$. ■

Exercice 9.6 Montrer que l'ensemble des matrices carrées d'ordre n de trace nulle est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ et calculer sa dimension.

9.3 Rang d'un système de vecteurs ou d'une application linéaire

On désigne par E un espace vectoriel de dimension finie.

On rappelle que le sous-espace vectoriel $F = \text{Vect}\{x_1, \dots, x_p\}$ de E engendré par des vecteurs x_1, \dots, x_p de E est l'ensemble de toutes les combinaisons linéaires de ces vecteurs, soit :

$$F = \left\{ x = \sum_{k=1}^p \lambda_k x_k \mid (\lambda_1, \lambda_2, \dots, \lambda_p) \in \mathbb{K}^p \right\}.$$

Définition 9.5 Le rang de la famille $\{x_1, \dots, x_p\}$ de vecteurs de E est la dimension de l'espace vectoriel engendré par ces vecteurs. On le note $\text{rg}(x_1, \dots, x_p)$.

Théorème 9.14 Le rang d'une famille $\{x_1, \dots, x_p\}$ de p vecteurs de E est au maximum égal à p et ce rang vaut p si, et seulement si, cette famille est libre.

Démonstration. Si le système $\mathcal{L} = \{x_1, \dots, x_p\}$ est libre, il constitue une base de $F = \text{Vect}(\mathcal{L})$ et $\text{rg}(\mathcal{L}) = \dim(F) = p$. Réciproquement si le rang vaut p , la famille \mathcal{L} est génératrice de F avec p éléments, c'est donc une base de F et en conséquence une famille libre. ■

Remarque 9.3 Si E est de dimension n , le rang d'une famille de vecteurs de E est au plus égal à n . Si ce rang vaut n , on a alors $\text{Vect}\{x_1, \dots, x_p\} = E$ et $\{x_1, \dots, x_p\}$ est un système générateur de E . Dans le cas où $p = n$, c'est une base.

Définition 9.6 Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F . Le rang de u est la dimension de $\text{Im}(u)$. On le note $\text{rg}(u)$.

En désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E , l'image de u est le sous-espace vectoriel de F engendré par $\{u(e_1), \dots, u(e_n)\}$ et :

$$\text{rg}(u) = \text{rg}(u(e_1), \dots, u(e_n)).$$

Remarque 9.4 Comme $\text{Im}(u)$ est un sous-espace vectoriel de F , on a $\text{rg}(u) \leq \dim(F)$ et comme $\text{rg}(u) = \text{rg}(u(e_1), \dots, u(e_n))$, on a aussi $\text{rg}(u) \leq \dim(E)$. Donc :

$$\text{rg}(u) \leq \min(\dim(E), \dim(F))$$

Plus précisément, on a les résultats suivants.

Théorème 9.15 Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F . On a $\text{rg}(u) = \dim(F)$ si, et seulement si, u est surjective.

Démonstration. Dire que u est surjective équivaut à dire que $\text{Im}(u) = F$, ce qui est encore équivalent à $\text{rg}(u) = \dim(\text{Im}(u)) = \dim(F)$ puisque $\text{Im}(u)$ est un sous-espace vectoriel de F . ■

Théorème 9.16 (du rang) Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F . On a :

$$\dim(E) = \dim(\ker(u)) + \text{rg}(u).$$

Démonstration. Soit H un supplémentaire de $\ker(u)$ dans E et v la restriction de u à H , c'est-à-dire l'application v définie sur H par :

$$\forall x \in H, v(x) = u(x).$$

Le noyau de cette application est :

$$\ker(v) = H \cap \ker(u) = \{0\}$$

ce qui signifie que v est injective de H dans F et réalise une bijection de H dans $\text{Im}(v)$.

En écrivant tout vecteur y de $\text{Im}(u)$ sous la forme $y = u(x)$ avec $x \in E$ qui s'écrit $x = x_1 + x_2$ où $x_1 \in \ker(u)$ et $x_2 \in H$, on a $y = u(x_1) + u(x_2) = v(x_2)$, c'est-à-dire que y est dans $\text{Im}(v)$. On a donc $\text{Im}(u) \subset \text{Im}(v)$ et comme $\text{Im}(v) \subset \text{Im}(u)$, on a en fait $\text{Im}(v) = \text{Im}(u)$ et v réalise un isomorphisme de H sur $\text{Im}(u)$. Il en résulte que :

$$\text{rg}(u) = \dim(\text{Im}(u)) = \dim(H) = \dim(E) - \dim(\ker(u)).$$

■

Remarque 9.5 En montrant le théorème du rang, on a en fait montré que $\text{Im}(u)$ est isomorphe à un supplémentaire de $\ker(u)$ dans E .

Corollaire 9.3 Soient E, F deux espaces vectoriels de dimension finie et u une application linéaire de E dans F . On a :

1. $\text{rg}(u) \leq \min(\dim(E), \dim(F))$;
2. $\text{rg}(u) = \dim(E)$ si, et seulement si, u est injective.

Démonstration.

1. De la formule du rang, on déduit que $\text{rg}(u) \leq \dim(E)$ et $\text{rg}(u) \leq \dim(F)$ par définition.
2. Si $\text{rg}(u) = \dim(E)$, la formule du rang nous dit que $\dim(\ker(u)) = 0$, soit que $\ker(u) = \{0\}$ et u est injective. Réciproquement si u est injective, on a $\ker(u) = \{0\}$ et $\text{rg}(u) = \dim(E)$.

■

Exercice 9.7 Soit E un espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$.

1. Montrer que :

$$\text{Im}(u) = \text{Im}(u^2) \Leftrightarrow \ker(u) = \ker(u^2)$$

où $u^2 = u \circ u$.

2. Montrer que :

$$\text{Im}(u) = \text{Im}(u^2) \Leftrightarrow E = \ker(u) \oplus \text{Im}(u) \Leftrightarrow \ker(u) = \ker(u^2)$$

Solution 9.6

1. On a toujours :

$$\text{Im}(u^2) \subset \text{Im}(u), \ker(u) \subset \ker(u^2)$$

donc :

$$\text{Im}(u) = \text{Im}(u^2) \Leftrightarrow \text{rg}(u) = \text{rg}(u^2)$$

et :

$$\ker(u) = \ker(u^2) \Leftrightarrow \dim(\ker(u)) = \dim(\ker(u^2))$$

D'autre part, le théorème du rang nous dit que :

$$\dim(E) = \dim(\ker(u)) + \text{rg}(u) = \dim(\ker(u^2)) + \text{rg}(u^2)$$

ce qui permet de déduire que :

$$\text{Im}(u) = \text{Im}(u^2) \Leftrightarrow \ker(u) = \ker(u^2)$$

2. Il suffit de montrer que :

$$\text{Im}(u) = \text{Im}(u^2) \Leftrightarrow E = \ker(u) \oplus \text{Im}(u)$$

Si $\text{Im}(u) = \text{Im}(u^2)$, alors pour tout x dans E , il existe y dans E tel que $u(x) = u^2(y)$, donc $x - u(y) \in \ker(u)$ et $x = (x - u(y)) + u(y) \in \ker(u) + \text{Im}(u)$. On a donc $E = \ker(u) + \text{Im}(u)$ et avec le théorème du rang, on déduit que $E = \ker(u) \oplus \text{Im}(u)$.

Si $E = \ker(u) \oplus \text{Im}(u)$ alors tout $x \in \ker(u^2)$ s'écrit $x = x_1 + u(x_2)$ avec $u(x_1) = 0$ et $0 = u^2(x) = u^3(x_2)$ entraîne que $u^2(x_2) \in \ker(u) \cap \text{Im}(u) = \{0\}$, donc $u(x_2) \in \ker(u) \cap \text{Im}(u) = \{0\}$ et $x = x_1 \in \ker(u)$. On a donc $\ker(u^2) \subset \ker(u)$ et $\ker(u) = \ker(u^2)$, ce qui équivaut à $\text{Im}(u) = \text{Im}(u^2)$.

9.4 Expression matricielle des applications linéaires

Nous avons déjà introduit les matrices en utilisant les bases canoniques de \mathbb{K}^n et \mathbb{K}^m . En fait tout peut être repris dans le cadre des espaces vectoriels de dimension fini en utilisant des bases de ces espaces, les démonstrations étant identiques à celles du paragraphe 8.5.

On se donne un espace vectoriel E de dimension n , une base $\mathcal{B} = (e_k)_{1 \leq k \leq n}$ de E , un espace vectoriel F de dimension m , une base $\mathcal{B}' = (f_k)_{1 \leq k \leq m}$ de F et une application linéaire u de E dans F .

Pour tout entier j compris entre 1 et n , il existe des scalaires a_{ij} tels que :

$$u(e_j) = \sum_{i=1}^m a_{ij} f_i$$

et pour tout vecteur $x = \sum_{j=1}^n x_j e_j$ dans E , on a :

$$u(x) = \sum_{j=1}^n x_j \sum_{i=1}^m a_{ij} f_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} x_j \right) f_i$$

c'est-à-dire que les composantes dans la base \mathcal{B}' de $u(x)$ sont les :

$$y_i = \sum_{j=1}^n a_{ij} x_j \quad (1 \leq i \leq m)$$

Définition 9.7 Avec les notations qui précèdent, on dit que la matrice :

$$A = ((a_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

est la matrice de u dans les bases \mathcal{B} et \mathcal{B}' .

Dans le cas où $E = F$ et $\mathcal{B} = \mathcal{B}'$, on dira simplement que A est la matrice de u dans la base \mathcal{B} .

Pour tout j compris entre 1 et n , la colonne numéro j de la matrice A est le vecteur :

$$C_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

formé des composantes de $u(e_j)$ dans la base \mathcal{B}' .

L'égalité $y = u(x)$ se traduit alors par le produit matriciel :

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = AX$$

où les x_j , pour j compris entre 1 et n sont les composantes de x dans la base \mathcal{B} et les y_i , pour i compris entre 1 et m celles de $u(x)$ dans la base \mathcal{B}' .

Exercice 9.8 Pour tout entier naturel non nul n , on désigne par $\mathbb{R}_n[x]$ l'espace vectoriel des fonctions polynomiales à coefficients réels et de degré au plus égal à n . Pour $n \geq 1$, on considère l'application :

$$\begin{array}{ccc} u : \mathbb{R}_n[x] & \rightarrow & \mathbb{R}_n[x] \\ P & \mapsto & xP' \end{array}$$

où on a noté, pour toute fonction polynomiale $P \in \mathbb{R}_n[x]$, P' le polynôme dérivé de P .

1. Montrer que u est une application linéaire de E dans E .
2. Donner la matrice de u dans la base canonique $\mathcal{B} = (1, x, x^2, \dots, x^n)$ de E .
3. L'application u est-elle injective ?
4. L'application u est-elle surjective ?
5. Calculer le noyau, l'image et le rang de u .
6. Soit F le sous-espace-vectoriel de E engendré par (x, x^2, \dots, x^n) . Montrer que l'application u est bijective de F sur F .

Solution 9.7

1. Pour $P \in E$, on a $P' \in \mathbb{R}_{n-1}[x]$ et $xP' \in \mathbb{R}_n[x] = E$, donc u va bien de E dans E .
Pour P, Q dans E et λ, μ dans \mathbb{R} , on a :

$$\begin{aligned} u(\lambda P + \mu Q) &= x(\lambda P + \mu Q)' = \lambda(xP') + \mu(xQ') \\ &= \lambda u(P) + \mu u(Q) \end{aligned}$$

donc u est linéaire.

2. On a $u(1) = 0$ et pour k entier compris entre 1 et n :

$$u(x^k) = kx^{k-1}.$$

La matrice de u dans \mathcal{B} est donc :

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n-1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & n \end{pmatrix}$$

3. On a $u(1) = 0$ avec $1 \neq 0$, donc u non injective.
4. Pour tout polynôme $P \in E$, on a $u(P)(0) = 0$ car $u(P) = xP'$, donc 1 n'est pas dans l'image de u et u est non surjective.
5. On a $P \in \ker(u)$ si, et seulement si, $xP' = 0$, ce qui équivaut encore à $P' = 0$, soit P constant. Donc $\ker(u)$ est la droite dirigée par le polynôme constant 1.
En utilisant le théorème du rang, on déduit que

$$\text{rg}(u) = \dim(E) - 1 = n.$$

L'image de u est contenu dans l'espace $x\mathbb{R}_{n-1}[x]$ des polynômes de $\mathbb{R}_n[x]$ multiples de x . Réciproquement tout polynôme dans $x\mathbb{R}_{n-1}[x]$ s'écrit xQ avec $Q \in \mathbb{R}_{n-1}[x]$ et désignant par $P \in \mathbb{R}_n[x]$ une primitive de Q , on a $xQ = xP' = u(P)$. Donc $\text{Im}(u) = x\mathbb{R}_{n-1}[x]$. On retrouve le rang de u :

$$\text{rg}(u) = \dim(x\mathbb{R}_{n-1}[x]) = \dim(\mathbb{R}_{n-1}[x]) = n.$$

6. On remarque que $F = x\mathbb{R}_{n-1}[x] = \text{Im}(u)$. Donc la restriction v de u à F est un endomorphisme de F . Son noyau est :

$$\ker(v) = F \cap \ker(u) = \{0\}$$

il en résulte que u est un isomorphisme.

Comme dans le cas de \mathbb{K}^n et \mathbb{K}^m , on a le résultat suivant.

Théorème 9.17 Si u et v sont deux applications linéaires de E dans F de matrices respectives $A = ((a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ et $B = ((b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ dans les bases \mathcal{B} et \mathcal{B}' alors, pour tous scalaires λ, μ , l'application linéaire $\lambda u + \mu v$ a pour matrice dans ces bases la matrice $\lambda A + \mu B = ((\lambda a_{i,j} + \mu b_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$.

Ce résultat peut se traduire en disant que l'application qui associe à toute application linéaire $u \in \mathcal{L}(E, F)$ sa matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ dans les bases \mathcal{B} et \mathcal{B}' est linéaire. Plus précisément, on a le résultat suivant.

Théorème 9.18 Étant données une base $\mathcal{B} = (e_k)_{1 \leq k \leq n}$ de E et une base $\mathcal{B}' = (f_k)_{1 \leq k \leq m}$ de F , l'application φ qui associe à toute application linéaire $u \in \mathcal{L}(E, F)$ sa matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ dans les bases \mathcal{B} et \mathcal{B}' est un isomorphisme de $\mathcal{L}(E, F)$ sur $\mathcal{M}_{m,n}(\mathbb{K})$.

Démonstration. On vient de voir que φ est linéaire et cette application est bijective du fait qu'une application linéaire $u \in \mathcal{L}(E, F)$ est uniquement déterminée par sa matrice dans les bases \mathcal{B} et \mathcal{B}' . ■

En particulier, pour toute matrice $A \in \mathcal{M}_{m,n}(\mathbb{K})$ il existe une unique application linéaire $u \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^m)$ ayant pour matrice A dans les bases canoniques de \mathbb{K}^n et \mathbb{K}^m . On dira que u est l'application linéaire canoniquement associée à la matrice A .

Pour ce qui est de la matrice d'une composée d'applications linéaires nous avons le résultat suivant où G est un espace vectoriel de dimension r et $\mathcal{B}'' = (g_k)_{1 \leq k \leq r}$ une base de G .

Théorème 9.19 Si v est une application linéaire de E dans F de matrice $B \in \mathcal{M}_{m,n}(\mathbb{K})$ dans les bases \mathcal{B} et \mathcal{B}' et u une application linéaire de F dans G de matrice $A \in \mathcal{M}_{r,m}(\mathbb{K})$ dans les bases \mathcal{B}' et \mathcal{B}'' , alors la matrice dans les bases \mathcal{B} et \mathcal{B}'' de l'application linéaire $u \circ v$ de E dans G est la matrice produit $C = AB \in \mathcal{M}_{r,n}(\mathbb{K})$.

On en déduit le résultat suivant, où \mathcal{B} et \mathcal{B}' sont deux bases de E .

Théorème 9.20 Un endomorphisme u de E est bijectif si, et seulement si, sa matrice A dans les bases \mathcal{B} et \mathcal{B}' est inversible et dans ce cas A^{-1} est la matrice de u^{-1} dans les bases \mathcal{B}' et \mathcal{B} .

En regardant une matrice comme un ensemble de vecteurs colonnes, on peut donner la définition suivante.

Définition 9.8 Soit $A = ((a_{i,j}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ une matrice dans $\mathcal{M}_{m,n}(\mathbb{K})$. En désignant, pour tout j compris entre 1 et n , par $C_j = (a_{i,j})_{1 \leq i \leq m}$ le vecteur de \mathbb{K}^m représentant la colonne numéro j de A , le rang de A est le rang de la famille (C_1, C_2, \dots, C_n) de vecteurs de \mathbb{K}^m .

Théorème 9.21 Le rang d'une matrice $A \in \mathcal{M}_{r,m}(\mathbb{K})$ est égal au rang de l'application linéaire $u \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^r)$ canoniquement associée à la matrice A .

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

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

■

Théorème 9.22 Si $u \in \mathcal{L}(E, F)$ a pour matrice $A \in \mathcal{M}_{r,m}(\mathbb{K})$ dans les bases \mathcal{B} et \mathcal{B}' (toujours avec les notations du début de ce paragraphe), alors le rang de u est égal au rang de A .

Démonstration. On utilise la formule du rang.

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

9.5 Formules de changement de base

On se donne un espace vectoriel E de dimension n et deux bases de E , $\mathcal{B}_1 = (e_k)_{1 \leq k \leq n}$ et $\mathcal{B}_2 = (e'_k)_{1 \leq k \leq n}$. Une question naturelle est de savoir comment passer des composantes d'un vecteur de E d'une base à l'autre.

Pour tout vecteur $x = \sum_{j=1}^n x_j e_j = \sum_{j=1}^n x'_j e'_j$ dans E , on note $X = (x_j)_{1 \leq j \leq n}$ et $X' = (x'_j)_{1 \leq j \leq n}$ les vecteurs de \mathbb{K}^n respectivement formés des composantes de x dans les bases \mathcal{B}_1 et \mathcal{B}_2 .

Comme, pour j compris entre 1 et n le vecteur e'_j est dans E , il s'écrit :

$$e'_j = \sum_{i=1}^n p_{ij} e_i$$

où les p_{ij} sont des scalaires uniquement déterminés. On a alors :

$$\begin{aligned} x &= \sum_{i=1}^n x_i e_i = \sum_{j=1}^n x'_j e'_j = \sum_{j=1}^n x'_j \left(\sum_{i=1}^n p_{ij} e_i \right) \\ &= \sum_{i=1}^n \left(\sum_{j=1}^n p_{ij} x'_j \right) e_i \end{aligned}$$

et avec l'unicité de l'écriture de x dans la base \mathcal{B}_1 , on déduit que :

$$x_i = \sum_{j=1}^n p_{ij} x'_j \quad (1 \leq i \leq n)$$

ce qui peut se traduire par l'égalité matricielle :

$$X = PX'$$

où P est la matrice :

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix}$$

ayant pour colonne j le vecteur de \mathbb{K}^n formé des composantes de e'_j dans la bases \mathcal{B}_1 .

On peut retenir cette formule sous la forme :

$$X_{\mathcal{B}_1} = P_{\mathcal{B}_1 \rightarrow \mathcal{B}_2} X_{\mathcal{B}_2}$$

avec des notations évidentes.

Définition 9.9 Avec les notations qui précèdent, on dit que P est la matrice de passage de la base \mathcal{B}_1 à la base \mathcal{B}_2 .

Théorème 9.23 Avec les notations qui précèdent, la matrice de passage P de \mathcal{B}_1 à \mathcal{B}_2 est inversible et son inverse est la matrice de passage de \mathcal{B}_2 à \mathcal{B}_1 .

Démonstration. Il suffit de remarquer que la matrice P de \mathcal{B}_1 à \mathcal{B}_2 est la matrice dans les bases \mathcal{B}_2 et \mathcal{B}_1 de l'identité de E . En effet, pour tout j compris entre 1 et n on a :

$$Id_E(e'_j) = e'_j = \sum_{i=1}^n p_{ij} e_i.$$

Cette matrice est donc inversible et son inverse est la matrice dans les bases \mathcal{B}_1 et \mathcal{B}_2 de $(Id_E)^{-1} = Id_E$ c'est-à-dire la matrice de passage de \mathcal{B}_2 à \mathcal{B}_1 . ■

On a donc :

$$(P_{\mathcal{B}_1 \rightarrow \mathcal{B}_2})^{-1} = P_{\mathcal{B}_2 \rightarrow \mathcal{B}_1}.$$

Le calcul de l'inverse de la matrice de passage P de \mathcal{B}_1 à \mathcal{B}_2 peut se calculer en résolvant le système linéaire aux inconnues e_i :

$$e'_j = \sum_{i=1}^n p_{ij} e_i \quad (1 \leq i \leq n)$$

Exercice 9.9 On désigne par $\mathcal{B}_1 = (e_1, e_2, e_3)$ la base canonique de \mathbb{K}^3 .

1. Montrer que $\mathcal{B}_2 = (e'_1 = e_1 - e_2, e'_2 = 2e_2 + e_3, e'_3 = e_1 + e_3)$ est une base de \mathbb{K}^3 .
2. Calculer l'inverse de la matrice de passage P de \mathcal{B}_1 à \mathcal{B}_2 .

Solution 9.8

1. L'égalité $\lambda_1 e'_1 + \lambda_2 e'_2 + \lambda_3 e'_3 = 0$ équivaut à :

$$\begin{cases} \lambda_1 + \lambda_3 = 0 \\ -\lambda_1 + 2\lambda_2 = 0 \\ \lambda_2 + \lambda_3 = 0 \end{cases}$$

En additionnant les deux premières équations, on a $\lambda_3 + 2\lambda_2 = 0$ qui reporté dans la troisième donne $\lambda_2 = 0$. Les équations 2 et 3 donnent alors $\lambda_1 = \lambda_3 = 0$. La famille \mathcal{B}_2 est donc libre dans \mathbb{K}^3 et c'est une base puisqu'elle a trois éléments.

2. La matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 est la matrice :

$$P = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Avec :

$$\begin{cases} e'_1 = e_1 - e_2 \\ e'_2 = 2e_2 + e_3 \\ e'_3 = e_1 + e_3 \end{cases}$$

on déduit que :

$$\begin{cases} e_1 = 2e'_1 + e'_2 - e'_3 \\ e_2 = e'_1 + e'_2 - e'_3 \\ e_3 = -2e'_1 - e'_2 + 2e'_3 \end{cases}$$

ce qui signifie que :

$$P^{-1} = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 1 & -1 \\ -1 & -1 & 2 \end{pmatrix}$$

On est maintenant en mesure d'exprimer la matrice d'un endomorphisme u de E dans la base \mathcal{B}_2 en fonction de sa matrice dans la base \mathcal{B}_1 .

Théorème 9.24 Si u est un endomorphisme de E de matrice $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans la base \mathcal{B}_1 et de matrice $A' = ((a'_{ij}))_{1 \leq i, j \leq n}$ dans la base \mathcal{B}_2 , on a alors $A' = P^{-1}AP$, où P est la matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 .

Démonstration. PA' est la matrice de $Id_E \circ u = u$ dans les bases \mathcal{B}_2 et \mathcal{B}_1 et AP est aussi la matrice de $u \circ Id_E = u$ dans les bases \mathcal{B}_2 et \mathcal{B}_1 . On a donc $PA' = AP$, ce qui équivaut à $A' = P^{-1}AP$. ■

Cette formule de changement de base peut se retenir sous la forme :

$$A_{\mathcal{B}_2} = P_{\mathcal{B}_2 \rightarrow \mathcal{B}_1} A_{\mathcal{B}_1} P_{\mathcal{B}_1 \rightarrow \mathcal{B}_2}.$$

Dans le cas où la matrice A' de u dans la base \mathcal{B}_2 a une forme plus simple que celle de A , on peut l'utiliser pour calculer les puissances de u ou de A . L'idée étant que l'égalité $A' = P^{-1}AP$ entraîne pour tout entier naturel p , on a $(A')^p = P^{-1}A^pP$ ou encore $A^p = P(A')^pP^{-1}$. La vérification étant immédiate par récurrence sur $p \geq 0$ (toujours avec la convention $A^0 = I_n$).

Si par exemple, la matrice A' est diagonale, c'est-à-dire de la forme :

$$A' = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

on a alors, pour tout $p \geq 0$:

$$(A')^p = \begin{pmatrix} \lambda_1^p & 0 & \cdots & 0 \\ 0 & \lambda_2^p & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n^p \end{pmatrix}$$

Pour $p \geq 1$, l'endomorphisme u^p est défini par la formule de récurrence $u^p = u^{p-1} \circ u$ avec $u^0 = Id_E$. Si A est la matrice de u dans la base \mathcal{B}_1 , alors celle de A^p dans cette même base est A^p .

Exercice 9.10 On désigne par \mathcal{B}_1 et \mathcal{B}_2 les bases de \mathbb{K}^3 de l'exercice 9.9 et par u l'endomorphisme de \mathbb{K}^3 de matrice $A = \begin{pmatrix} 4 & 2 & -4 \\ -6 & -4 & 6 \\ -1 & -1 & 1 \end{pmatrix}$ dans la base canonique \mathcal{B}_1 .

1. Déterminer la matrice de u dans la base \mathcal{B}_2 .
2. Calculer, pour tout $p \in \mathbb{N}$, la matrice de u^p dans la base canonique de \mathbb{K}^3 .

Solution 9.9

1. La matrice de u dans la base \mathcal{B}_2 est :

$$\begin{aligned} A' = P^{-1}AP &= \begin{pmatrix} 2 & 1 & -2 \\ 1 & 1 & -1 \\ -1 & -1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 2 & -4 \\ -6 & -4 & 6 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

2. La matrice de u^p dans la base \mathcal{B}_2 est :

$$(A')^p = \begin{pmatrix} 2^p & 0 & 0 \\ 0 & (-1)^p & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et dans la base \mathcal{B}_1 c'est :

$$\begin{aligned} A^p = P(A')^p P^{-1} &= \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2^p & 0 & 0 \\ 0 & (-1)^p & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 & -2 \\ 1 & 1 & -1 \\ -1 & -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2^{p+1} & 2^p & -2^{p+1} \\ 2(-1)^p - 2^{p+1} & 2(-1)^p - 2^p & 2^{p+1} - 2(-1)^p \\ (-1)^p & (-1)^p & (-1)^{p+1} \end{pmatrix} \end{aligned}$$

Exercice 9.11 Soit $u \in \mathcal{L}(\mathbb{K}^3)$ de matrice $A = \begin{pmatrix} -5 & 3 & 3 \\ -8 & 6 & 4 \\ -1 & 1 & 3 \end{pmatrix}$ dans la base canonique $\mathcal{B}_1 = (e_1, e_2, e_3)$.

1. Déterminer les images par u des vecteurs $e'_1 = e_1 + e_2$, $e'_2 = e_2 - e_3$, $e'_3 = e_1 + 2e_2 + e_3$.
2. Montrer que $\mathcal{B}_2 = (e'_1, e'_2, e'_3)$ est une base de \mathbb{K}^3 et donner la matrice de u dans cette base.
3. Calculer, pour tout $p \in \mathbb{N}$, la matrice de u^p dans la base canonique de \mathbb{K}^3 .

Solution 9.10 Laissée au lecteur.

Opérations élémentaires et déterminants

On note toujours \mathbb{K} le corps de réels ou des complexes.

On se donne un entier $n \geq 1$ et $\mathcal{M}_n(\mathbb{K})$ désigne l'espace vectoriel des matrices carrées d'ordre n à coefficients dans \mathbb{K} .

Pour i, j entiers compris entre 1 et n , on note E_{ij} la matrice dont tous les coefficients sont nuls sauf celui d'indice (i, j) (ligne i et colonne j) qui vaut 1.

On rappelle que la famille $(E_{ij})_{1 \leq i, j \leq n}$ est une base de $\mathcal{M}_n(\mathbb{K})$ qui est donc de dimension n^2 .

Pour toute matrice $A = ((a_{ij}))_{1 \leq i, j \leq n} \in \mathcal{M}_n(\mathbb{K})$, on note pour tout entier i compris entre 1 et n :

$$L_i = (a_{i1}, a_{i2}, \dots, a_{in})$$

sa ligne numéro i (c'est une matrice à une ligne et n colonnes) et pour tout entier j compris entre 1 et n :

$$C_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$$

sa colonne numéro j (c'est une matrice à n lignes et une colonne).

On écrira :

$$A = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \text{ ou } A = (C_1 \quad \dots \quad C_n).$$

Définition 10.1 On dit qu'une matrice $A = ((a_{ij}))_{1 \leq i, j \leq n} \in \mathcal{M}_n(\mathbb{K})$ est triangulaire inférieure [resp. supérieure] si $a_{ij} = 0$ pour $1 \leq i < j \leq n$ [resp. pour $1 \leq j < i \leq n$].

Une matrice triangulaire inférieure est donc de la forme :

$$A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

et une matrice triangulaire supérieure de la forme :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

Définition 10.2 Une matrice diagonale est une matrice triangulaire inférieure et supérieure.

Une matrice diagonale est donc de la forme :

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

10.1 Opérations élémentaires. Matrices de dilatation et de transvection

On suppose que $n \geq 2$.

On appelle matrice déduite de A par opération élémentaire sur les lignes de A toute matrice de la forme :

$$A_i(\lambda) = \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ \lambda L_i \\ L_{i+1} \\ \vdots \\ L_n \end{pmatrix},$$

avec $1 \leq i \leq n$ et $\lambda \in \mathbb{K}^*$, c'est-à-dire que la matrice $A_i(\lambda)$ est déduite de la matrice A en multipliant sa ligne numéro i par λ ou de la forme :

$$A_{ij}(\lambda) = \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ L_i + \lambda L_j \\ L_{i+1} \\ \vdots \\ L_n \end{pmatrix}$$

$1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$, c'est-à-dire que la matrice $A_{ij}(\lambda)$ est déduite de la matrice A en ajoutant à la ligne numéro i la ligne numéro j multipliée par λ .

On appelle matrice déduite de A par opération élémentaire sur les colonnes de A toute matrice de la forme :

$$A'_j(\lambda) = (C_1 \cdots C_{j-1} \quad \lambda C_j \quad C_{j+1} \cdots C_n),$$

avec $1 \leq j \leq n$ et $\lambda \in \mathbb{K}^*$, c'est-à-dire que la matrice $A'_i(\lambda)$ est déduite de la matrice A en multipliant sa colonne numéro j par λ ou de la forme :

$$A'_{ij}(\lambda) = \begin{pmatrix} C_1 & \cdots & C_{j-1} & C_j + \lambda C_i & C_{j+1} & \cdots & C_n \end{pmatrix}$$

$1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$, c'est-à-dire que la matrice $A'_{ij}(\lambda)$ est déduite de la matrice A en ajoutant à la colonne numéro j la colonne numéro i multipliée par λ .

Définition 10.3 On appelle matrice de transvection toute matrice de la forme :

$$T_{ij}(\lambda) = I_n + \lambda E_{ij},$$

avec $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$.

Une matrice de transvection $T_{ij}(\lambda)$ est donc une matrice triangulaire dont tous les termes diagonaux valent 1 et de termes hors de la diagonale tous nuls sauf celui d'indice (i, j) (i. e. en ligne i et colonne j) qui vaut λ .

Définition 10.4 On appelle matrice de dilatation toute matrice de la forme :

$$D_i(\lambda) = I_n + (\lambda - 1) E_{ii},$$

avec $1 \leq i \leq n$ et $\lambda \in \mathbb{K}^*$.

Une matrice de dilatation $D_i(\lambda)$ est donc diagonale de termes diagonaux tous égaux à 1 sauf le numéro i qui vaut λ .

Théorème 10.1 Avec les notations qui précèdent on a :

$$\begin{aligned} A_i(\lambda) &= D_i(\lambda) A, \quad A_{ij}(\lambda) = T_{ij}(\lambda) A, \\ A'_j(\lambda) &= A D_j(\lambda), \quad A'_{ij}(\lambda) = A T_{ij}(\lambda). \end{aligned}$$

C'est-à-dire que :

1. la multiplication à gauche par une matrice de dilatation $D_i(\lambda)$ a pour effet de multiplier la ligne i par λ ;
2. la multiplication à droite par une matrice de dilatation $D_j(\lambda)$ a pour effet de multiplier la colonne j par λ ;
3. la multiplication à gauche par une matrice de transvection $T_{ij}(\lambda)$ a pour effet de remplacer la ligne L_i par $L_i + \lambda L_j$;
4. la multiplication à droite par une matrice de transvection $T_{ij}(\lambda)$ a pour effet de remplacer la colonne C_j par $C_j + \lambda C_i$.

Démonstration. Le coefficient d'indice (p, q) du produit de matrices $D_i(\lambda) A$ est obtenu en faisant le produit de la ligne p de $D_i(\lambda)$ par la colonne q de A , ce qui donne en notant $\alpha_{p,q}$ ce coefficient :

$$\alpha_{p,q} = \begin{cases} a_{p,q} & \text{si } 1 \leq p \neq i \leq n, \quad 1 \leq q \leq n, \\ \lambda a_{iq} & \text{si } p = i, \quad 1 \leq q \leq n. \end{cases}$$

On a donc bien $A_i(\lambda) = D_i(\lambda) A$.

Les autres égalités se montrent de façon analogue. ■

Ce résultat justifie la définition suivante.

Définition 10.5 On appelle *matrice élémentaire* une *matrice de dilatation* ou de *transvection*.

Lemme 10.1 Une *matrice élémentaire* est *inversible* avec :

$$T_{ij}(\lambda)^{-1} = T_{ij}(-\lambda),$$

pour une *matrice de transvection* et :

$$D_i(\lambda)^{-1} = D_i\left(\frac{1}{\lambda}\right),$$

pour une *matrice de dilatation*.

Démonstration. Pour λ, μ dans \mathbb{K} et $i \neq j$ compris entre 1 et n , la matrice $T_{ij}(\lambda)T_{ij}(\mu)$ se déduit de $T_{ij}(\mu)$ en ajoutant à sa ligne i sa ligne j multipliée par λ , ce qui donne la matrice $T_{ij}(\lambda + \mu)$.

Prenant $\mu = -\lambda$, on a $T_{ij}(\lambda)T_{ij}(-\lambda) = T_0 = I_n$, ce qui signifie que $T_{ij}(\lambda)$ est inversible d'inverse $T_{ij}(-\lambda)$.

Le deuxième résultat est évident. ■

Avec l'exercice qui suit, on vérifie que toute matrice inversible d'ordre 2 est produit de matrices élémentaires. Ce résultat est en fait vrai pour les matrices inversibles d'ordre $n \geq 2$.

Exercice 10.1 Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une *matrice inversible*.

1. On suppose que $c \neq 0$.

(a) Déterminer un scalaire λ_1 tel que :

$$A_1 = T_{12}(\lambda_1)A = \begin{pmatrix} 1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

(b) Déterminer un scalaire λ_2 tel que :

$$A_2 = T_{21}(\lambda_2)A_1 = \begin{pmatrix} 1 & b_2 \\ 0 & d_2 \end{pmatrix}$$

(c) Déterminer un scalaire λ_3 tel que :

$$A_3 = A_2T_{12}(\lambda_3) = \begin{pmatrix} 1 & 0 \\ 0 & d_1 \end{pmatrix}$$

(d) En déduire qu'il existe des matrices de transvection P_1, P_2, Q_1 et une matrice de dilatation D telles que :

$$A = P_1P_2DQ_1$$

2. Donner un résultat analogue dans le cas où $c = 0$.

Solution 10.1

1.

(a) Pour tout scalaire λ_1 , on a :

$$T_{12}(\lambda_1) A = \begin{pmatrix} 1 & \lambda_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + c\lambda_1 & b + d\lambda_1 \\ c & d \end{pmatrix}$$

et prenant λ_1 tel que $a + c\lambda_1 = 1$, soit $\lambda_1 = \frac{1-a}{c}$, on a :

$$T_{12}(\lambda_1) A = \begin{pmatrix} 1 & \frac{d - \det(A)}{c} \\ c & d \end{pmatrix}$$

(b) Pour tout scalaire λ_2 , on a :

$$T_{21}(\lambda_2) A_1 = \begin{pmatrix} 1 & 0 \\ \lambda_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_1 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & b_1 \\ c + \lambda_2 & d + b_1\lambda_2 \end{pmatrix}$$

et prenant $\lambda_2 = -c$, on a :

$$T_{21}(\lambda_2) A_1 = \begin{pmatrix} 1 & b_1 \\ 0 & d - cb_1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{d - \det(A)}{c} \\ 0 & \det(A) \end{pmatrix}$$

(c) Pour tout scalaire λ_3 , on a :

$$A_2 T_{12}(\lambda_3) = \begin{pmatrix} 1 & b_2 \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} 1 & \lambda_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_2 + \lambda_3 \\ 0 & d_2 \end{pmatrix}$$

et prenant $\lambda_3 = -b_2$, on a :

$$A_2 T_{12}(\lambda_3) = \begin{pmatrix} 1 & 0 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \det(A) \end{pmatrix}$$

(d) On a donc en définitive :

$$T_{21}(\lambda_2) T_{12}(\lambda_1) A T_{12}(\lambda_3) = D(\det(A))$$

et utilisant le fait que les matrices de transvections sont inversibles, on déduit que :

$$A = T_{12}(-\lambda_1) T_{21}(-\lambda_2) D(\det(A)) T_{12}(-\lambda_3)$$

$$\text{où } \lambda_1 = \frac{1-a}{c}, \lambda_2 = -c \text{ et } \lambda_3 = \frac{\det(A) - d}{c}.$$

2. Si $c = 0$, on a nécessairement $a \neq 0$ puisque A est inversible et :

$$T_{21}(1) A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ a & b + d \end{pmatrix}$$

ce qui nous ramène au cas précédent et donne :

$$T_{21}(1) A = P_1 P_2 D Q_1$$

soit :

$$A = T_{21}(-1) P_1 P_2 D Q_1.$$

De manière plus générale, on a le résultat suivant.

Théorème 10.2 Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ (où $n \geq 2$) est inversible si, et seulement si, elle est produit de matrices élémentaires. Précisément si $A \in \mathcal{M}_n(\mathbb{K})$ est inversible, il existe alors des matrices de transvection P_1, \dots, P_r et Q_1, \dots, Q_s et une matrice de dilatation $D_n(\lambda)$ telles que :

$$A = P_1 \cdots P_r D_n(\lambda) Q_1 \cdots Q_s.$$

Démonstration. On procède par récurrence sur $n \geq 2$.

Le cas $n = 2$ a été traité avec l'exercice précédent.

On le suppose vrai pour toutes les matrices inversibles d'ordre $n - 1 \geq 2$ et on se donne une matrice inversible A d'ordre n .

On se ramène tout d'abord par opération élémentaire au cas où $a_{21} \neq 0$. Si $a_{21} = 0$, comme A est inversible, sa colonne 1 n'est pas nulle (cette colonne est Ae_1 où e_1 est le premier vecteur de base canonique et $x = 0$ est l'unique solution de $Ax = 0$), il existe donc un indice $i \in \{1, 3, \dots, n\}$ tel que $a_{i1} \neq 0$ et la matrice $T_{2i}(1)A$ (déduite de A en ajoutant la ligne i à la ligne 2) est telle que son coefficient d'indice $(2, 1)$ est non nul.

Une fois ramené à $a_{21} \neq 0$, on se ramène à $a_{11} = 1$ en remplaçant la première ligne L_1 par $L_1 + \lambda L_2$ (multiplication à gauche par $T_{12}(\lambda)$) où le scalaire λ est choisi tel que $a_{11} + \lambda a_{21} = 1$.

Ensuite, pour tout $i \in \{2, 3, \dots, n\}$, en remplaçant la ligne L_i par $L_i - a_{i1}L_1$ (multiplication à gauche par $T_{i1}(-a_{i1})$), on annule le coefficient d'indice $(i, 1)$.

On peut donc trouver des matrices de transvection P_1, \dots, P_k telles que :

$$P_k \cdots P_1 A = \begin{pmatrix} 1 & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}.$$

De manière analogue, en multipliant à droite par des matrices de transvection, Q_1, \dots, Q_m , on obtient :

$$P_k \cdots P_1 A Q_1 \cdots Q_m = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \beta_{n2} & \cdots & \beta_{nn} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & B & & \\ 0 & & & \end{pmatrix}$$

On peut alors conclure en appliquant l'hypothèse de récurrence à la matrice B qui est d'ordre $n - 1$ et inversible. En effet, si B n'est pas inversible, il existe $x' \neq 0$ dans \mathbb{K}^{n-1} tel que $Bx' = 0$, donc $x = \begin{pmatrix} 0 \\ x' \end{pmatrix} \in \mathbb{K}^n$ est non nul solution de $P_k \cdots P_1 A Q_1 \cdots Q_m x = 0$ qui équivaut à $Ay = 0$ avec $y = Q_1 \cdots Q_m x \neq 0$ puisque les matrices P_i et Q_j sont inversibles, en contradiction avec A inversible. ■

Nous verrons plus loin (paragraphe 10) que, comme dans le cas $n = 2$, le scalaire λ qui intervient dans le théorème précédent est uniquement déterminé par la matrice A , c'est son déterminant.

Pour $n = 1$, le résultat est encore vrai avec $A = (a) = D(a)$.

10.2 Déterminants des matrices carrées

Nous avons déjà défini le déterminant d'une matrice d'ordre deux, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par :

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

(définition 8.14).

Une matrice d'ordre 1 étant tout simplement un réel ou un complexe, son déterminant est lui même.

Le déterminant d'une matrice carrée $A = ((a_{ij}))_{1 \leq i, j \leq n}$ d'ordre $n \geq 3$ peut se définir par récurrence comme suit :

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

où $A_{i,1}$ est, pour i compris entre 1 et n , la matrice d'ordre $n-1$ déduite de A en supprimant la première colonne et la ligne numéro i .

Dans cette expression, on dit qu'on développe le déterminant suivant la première colonne.

On note :

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

Les lignes d'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ étant notées L_1, L_2, \dots, L_n , on écrira aussi :

$$\det(A) = \det \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{pmatrix}.$$

Exemple 10.1 Pour $n = 3$ et $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$, on a :

$$\det(A) = \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 4 \begin{vmatrix} 2 & 3 \\ 8 & 9 \end{vmatrix} + 7 \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = 0$$

Exercice 10.2 Soient $\alpha_1, \alpha_2, \alpha_3$ des réels ou des complexes. Calculer le déterminant de la matrice :

$$V(\alpha_1, \alpha_2, \alpha_3) = \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}$$

Une telle matrice est dite de Vandermonde.

Solution 10.2 On a :

$$\begin{aligned}
 \det(V(\alpha_1, \alpha_2, \alpha_3)) &= \begin{vmatrix} \alpha_2 & \alpha_3 \\ \alpha_2^2 & \alpha_3^2 \end{vmatrix} - \alpha_1 \begin{vmatrix} 1 & 1 \\ \alpha_2^2 & \alpha_3^2 \end{vmatrix} + \alpha_1^2 \begin{vmatrix} 1 & 1 \\ \alpha_2 & \alpha_3 \end{vmatrix} \\
 &= \alpha_2 \alpha_3^2 - \alpha_2^2 \alpha_3 - \alpha_1 (\alpha_3^2 - \alpha_2^2) + \alpha_1^2 (\alpha_3 - \alpha_2) \\
 &= \alpha_2 \alpha_3 (\alpha_3 - \alpha_2) - \alpha_1 (\alpha_3 - \alpha_2) (\alpha_3 + \alpha_2) + \alpha_1^2 (\alpha_3 - \alpha_2) \\
 &= (\alpha_3 - \alpha_2) (\alpha_2 \alpha_3 - \alpha_1 (\alpha_3 + \alpha_2) + \alpha_1^2) \\
 &= (\alpha_3 - \alpha_2) (\alpha_2 (\alpha_3 - \alpha_1) - \alpha_1 (\alpha_3 - \alpha_1)) \\
 &= (\alpha_3 - \alpha_2) (\alpha_3 - \alpha_1) (\alpha_2 - \alpha_1)
 \end{aligned}$$

Exercice 10.3 Calculer le déterminant de la matrice :

$$A = \begin{pmatrix} 5 & 4 & 2 & 1 \\ 2 & 3 & 1 & -2 \\ -5 & -7 & -3 & 9 \\ 1 & -2 & -1 & 4 \end{pmatrix}.$$

Solution 10.3 On a $\det(A) = 38$.

Théorème 10.3 Si $A_i(\lambda)$ est la matrice déduite de $A \in \mathcal{M}_n(\mathbb{K})$ en multipliant sa ligne i par un scalaire λ , on a alors $\det(A_i(\lambda)) = \lambda \det(A)$, soit :

$$\det \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ \lambda L_i \\ L_{i+1} \\ \vdots \\ L_n \end{pmatrix} = \lambda \det \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ L_i \\ L_{i+1} \\ \vdots \\ L_n \end{pmatrix}$$

Démonstration. On procède par récurrence sur $n \geq 1$.

Pour $n = 1$ c'est clair et pour $n = 2$, on a :

$$\begin{vmatrix} \lambda a & \lambda b \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ \lambda c & \lambda d \end{vmatrix} = \lambda(ad - bc) = \lambda \det(A).$$

Supposons le résultat acquis pour les matrices d'ordre $n - 1 \geq 2$. Soient A d'ordre n et $A' = A_i(\lambda)$ déduite de A en multipliant sa ligne i par λ . On a alors :

$$\det(A') = (-1)^{i+1} \lambda a_{i,1} \det(A_{i,1}) + \sum_{\substack{k=1 \\ k \neq i}}^n (-1)^{k+1} a_{k,1} \det(A'_{k1})$$

la matrice $A'_{k,1}$, pour $k \neq i$, étant déduite de $A_{k,1}$ en multipliant sa ligne i par λ . On a donc $\det(A'_{k,1}) = \lambda \det(A_{k,1})$ pour $k \neq i$ et $\det(A') = \lambda \det(A)$. ■

Corollaire 10.1 Si $A \in \mathcal{M}_n(\mathbb{K})$ a une ligne nulle, alors $\det(A) = 0$.

Démonstration. Supposons que la ligne i de A soit nulle. En désignant par $A' = A_i(\lambda)$ la matrice déduite de A en multipliant sa ligne i par $\lambda = 0$, on a $A' = A$ et $\det(A) = \det(A') = 0 \det(A) = 0$. ■

Corollaire 10.2 Pour tout $A \in \mathcal{M}_n(\mathbb{K})$ et tout scalaire λ , on a $\det(\lambda A) = \lambda^n \det(A)$.

Démonstration. En utilisant n fois le théorème précédent, on a :

$$\begin{aligned} \det(\lambda A) &= \det \begin{pmatrix} \lambda L_1 \\ \lambda L_2 \\ \vdots \\ \lambda L_n \end{pmatrix} = \lambda \det \begin{pmatrix} L_1 \\ \lambda L_2 \\ \vdots \\ \lambda L_n \end{pmatrix} \\ &= \dots = \lambda^n \det \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_n \end{pmatrix}. \end{aligned}$$

■

Théorème 10.4 Le déterminant d'une matrice triangulaire est égale au produit de ses termes diagonaux, soit :

$$\det(A) = \prod_{i=1}^n a_{ii}$$

Démonstration. Considérons tout d'abord le cas des matrices triangulaires inférieures.

On procède par récurrence sur $n \geq 1$.

Pour $n = 1$ c'est clair et pour $n = 2$, on a :

$$\begin{vmatrix} a & 0 \\ c & d \end{vmatrix} = ad - 0 \cdot c = ad.$$

Supposons le résultat acquis pour les matrices triangulaires inférieures d'ordre $n - 1 \geq 2$ et soit A triangulaire inférieure d'ordre n . La matrice A_{11} est triangulaire inférieure de diagonale a_{22}, \dots, a_{nn} et pour i compris entre 2 et n , la matrice A_{i1} est telle que sa première ligne est nulle, elle est donc de déterminant nul et :

$$\det(A) = a_{1,1} \det(A_{1,1}) = \prod_{i=1}^n a_{ii}.$$

Pour le cas des matrices triangulaires supérieures, le cas $n = 1$ est encore évident et le cas $n = 2$ se vérifie par le calcul. Supposant le résultat acquis au rang $n - 1 \geq 2$, pour A triangulaire supérieure d'ordre n , La matrice A_{11} est triangulaire supérieure de diagonale a_{22}, \dots, a_{nn} et pour i compris entre 2 et n , les coefficients a_{i1} sont nuls de sorte que :

$$\det(A) = a_{1,1} \det(A_{1,1}) = \prod_{i=1}^n a_{ii}.$$

■

Exemple 10.2 Si $A = I_n$ est la matrice identité, on a alors $\det(I_n) = 1$.

Exemple 10.3 Si $A = D_i(\lambda)$ est une matrice de dilatation, on a alors $\det(D_i(\lambda)) = \lambda$.

Exemple 10.4 Si $A = T_{ij}(\lambda)$ est une matrice de transvection, on a alors $\det(T_{ij}(\lambda)) = 1$.

Théorème 10.5 Soient A, A', A'' des matrices de lignes respectives L_i, L'_i, L''_i (pour i compris entre 1 et n) telles que $L_i = L'_i = L''_i$ pour $i \neq k$ et $L''_k = L_k + L'_k$ où k est un indice compris entre 1 et n . On a :

$$\det(A'') = \det(A) + \det(A')$$

soit :

$$\det \begin{pmatrix} L_1 \\ \vdots \\ L_{k-1} \\ L_k + L'_k \\ L_{k+1} \\ \vdots \\ L_n \end{pmatrix} = \det \begin{pmatrix} L_1 \\ \vdots \\ L_{k-1} \\ L_k \\ L_{k+1} \\ \vdots \\ L_n \end{pmatrix} + \det \begin{pmatrix} L_1 \\ \vdots \\ L_{k-1} \\ L'_k \\ L_{k+1} \\ \vdots \\ L_n \end{pmatrix}$$

Démonstration. On procède par récurrence sur $n \geq 1$.

Pour $n = 1$ c'est clair et pour $n = 2$, il suffit de calculer.

Supposons le résultat acquis pour les matrices d'ordre $n - 1 \geq 2$. Soient A, A', A'' d'ordre n vérifiant les conditions du théorème. On a alors :

$$\det(A'') = (-1)^{k+1} (a_{k,1} + a'_{k,1}) \det(A''_{k,1}) + \sum_{\substack{i=1 \\ i \neq k}}^n (-1)^{i+1} a_{i,1} \det(A''_{i,1})$$

avec $A''_{k,1} = A_{k,1} = A'_{k,1}$ et pour $i \neq k$, les matrices $A_{i,1}, A'_{i,1}, A''_{i,1}$ vérifiant les hypothèses du théorème au rang $n - 1$ (avec des notations évidentes), donc :

$$\begin{aligned} \det(A'') &= (-1)^{k+1} (a_{k,1} \det(A_{k,1}) + a'_{k,1} \det(A'_{k,1})) \\ &+ \sum_{\substack{i=1 \\ i \neq k}}^n (-1)^{i+1} a_{i,1} \det(A_{i,1}) + \sum_{\substack{i=1 \\ i \neq k}}^n (-1)^{i+1} a'_{i,1} \det(A'_{i,1}) \\ &= \det(A) + \det(A'). \end{aligned}$$

■

Les théorèmes 10.3 et 10.5 se traduisent en disant que le déterminant est linéaire par rapport à chaque ligne.

Théorème 10.6 Si A' est la matrice déduite de $A \in \mathcal{M}_n(\mathbb{K})$ en permutant deux lignes, on a alors $\det(A') = -\det(A)$, soit :

$$\det \begin{pmatrix} \vdots \\ L_i \\ \vdots \\ L_j \\ \vdots \end{pmatrix} = -\det \begin{pmatrix} \vdots \\ L_j \\ \vdots \\ L_i \\ \vdots \end{pmatrix}$$

où les pointillés indiquent les lignes inchangées.

Démonstration. On procède par récurrence sur $n \geq 2$.

Pour $n = 2$, il suffit de calculer.

Supposons le résultat acquis pour les matrices d'ordre $n - 1 \geq 2$.

La permutation de deux lignes se faisant avec un nombre impair de permutations de deux lignes successives (par exemple la permutation $(2, 4)$ se fait par les trois permutations $(2, 3, 4) \rightarrow (3, 2, 4) \rightarrow (3, 4, 2) \rightarrow (4, 3, 2)$), il suffit de considérer le cas où $j = i + 1$ (montrer ce point rigoureusement). On se donne donc A d'ordre n et A' est déduite de $A \in \mathcal{M}_n(\mathbb{K})$ en permutant les lignes i et $i + 1$. Pour $k \neq i$ et $k \neq i + 1$, on a $a'_{k1} = a_{k,1}$ et $\det(A'_{k,1}) = -\det(A_{k,1})$ par hypothèse de récurrence, et avec $a'_{i,1} = a_{(i+1),1}$, $a'_{(i+1),1} = a_{i,1}$, $A'_{i,1} = A_{(i+1),1}$, $A'_{(i+1),1} = A_{i,1}$, on déduit que :

$$\begin{aligned} \det(A') &= (-1)^{i+1} a_{(i+1),1} \det(A_{(i+1),1}) + (-1)^i a_{i,1} \det(A_{i,1}) \\ &\quad - \sum_{\substack{k=1 \\ k \neq i, k \neq i+1}}^n (-1)^{k+1} a_{k,1} \det(A_{k,1}) = -\det(A). \end{aligned}$$

■

Le résultat précédent se traduit en disant que le déterminant est une forme alternée sur les lignes.

Corollaire 10.3 Si la matrice $A \in \mathcal{M}_n(\mathbb{K})$ a deux lignes identiques, alors $\det(A) = 0$.

Démonstration. Si $L_i = L_j$ avec $i \neq j$, alors matrice A' déduite de A en permutant ces deux lignes est égale à A et $\det(A) = -\det(A)$, donc $\det(A) = 0$. ■

Corollaire 10.4 On ne change pas la valeur d'un déterminant si on ajoute à une ligne une combinaison linéaire des autres lignes.

Démonstration. Il suffit de montrer le résultat quand on ajoute à la ligne L_i la ligne L_j multipliée par un scalaire λ où $i \neq j$. Dans ce cas, on a :

$$\det \begin{pmatrix} \vdots \\ L_i + \lambda L_j \\ \vdots \\ L_j \\ \vdots \end{pmatrix} = \det \begin{pmatrix} \vdots \\ L_j \\ \vdots \\ L_j \\ \vdots \end{pmatrix} + \lambda \det \begin{pmatrix} \vdots \\ L_j \\ \vdots \\ L_j \\ \vdots \end{pmatrix} = \det \begin{pmatrix} \vdots \\ L_j \\ \vdots \\ L_j \\ \vdots \end{pmatrix}$$

où les pointillés indiquent les lignes inchangées. ■

En effectuant des opérations élémentaires sur les lignes d'une matrice A , on peut se ramener à une matrice triangulaire supérieure de même déterminant que celui de A .

Exercice 10.4 Calculer le déterminant de la matrice :

$$A = \begin{pmatrix} 5 & 4 & 2 & 1 \\ 2 & 3 & 1 & -2 \\ -5 & -7 & -3 & 9 \\ 1 & -2 & -1 & 4 \end{pmatrix}$$

de l'exercice 10.3 en effectuant des opérations élémentaires.

Solution 10.4 Les opérations $L_2 \rightarrow L_2 - \frac{2}{5}L_1$, $L_3 \rightarrow L_3 + L_1$, $L_4 \rightarrow L_4 - \frac{1}{5}L_1$ donnent :

$$\begin{aligned} \det(A) &= \begin{vmatrix} 5 & 4 & 2 & 1 \\ 0 & \frac{7}{5} & \frac{1}{5} & -\frac{12}{5} \\ 0 & -3 & -1 & 10 \\ 0 & -\frac{14}{5} & -\frac{7}{5} & \frac{19}{5} \end{vmatrix} = 5 \begin{vmatrix} 7 & 1 & -12 \\ \frac{7}{5} & \frac{1}{5} & -\frac{12}{5} \\ -3 & -1 & 10 \\ -\frac{14}{5} & -\frac{7}{5} & \frac{19}{5} \end{vmatrix} \\ &= 5 \frac{1}{5} \frac{1}{5} \begin{vmatrix} 7 & 1 & -12 \\ -3 & -1 & 10 \\ -14 & -7 & 19 \end{vmatrix} = \frac{1}{5} \begin{vmatrix} 7 & 1 & -12 \\ -3 & -1 & 10 \\ -14 & -7 & 19 \end{vmatrix} \end{aligned}$$

Puis les opérations $L_2 \rightarrow L_2 + \frac{3}{7}L_1$, $L_3 \rightarrow L_3 + \frac{14}{7}L_1 = L_3 + 2L_1$ donnent :

$$\begin{aligned} \det(A) &= \frac{1}{5} \begin{vmatrix} 7 & 1 & -12 \\ 0 & -\frac{4}{7} & \frac{34}{7} \\ 0 & -5 & -5 \end{vmatrix} = \frac{1}{5} \cdot 7 \cdot \frac{2}{7} \cdot 5 \begin{vmatrix} -2 & 17 \\ -1 & -1 \end{vmatrix} \\ &= 2 \cdot 19 = 38 \end{aligned}$$

Exercice 10.5 Développer le déterminant de la matrice suivante sous la forme d'un produit de facteurs linéaires en x :

$$A(x) = \begin{pmatrix} x+2 & 2x+3 & 3x+4 \\ 2x+3 & 3x+4 & 4x+5 \\ 3x+5 & 5x+8 & 10x+17 \end{pmatrix}.$$

Solution 10.5 Les opérations $L_3 \rightarrow L_3 - L_2$, $L_2 \rightarrow L_2 - L_1$ (dans l'ordre indiqué) donnent :

$$\begin{aligned} \det(A(x)) &= \begin{vmatrix} x+2 & 2x+3 & 3x+4 \\ x+1 & x+1 & x+1 \\ x+2 & 2x+4 & 6x+12 \end{vmatrix} \\ &= (x+1)(x+2) \begin{vmatrix} x+2 & 2x+3 & 3x+4 \\ 1 & 1 & 1 \\ 1 & 2 & 6 \end{vmatrix} \end{aligned}$$

puis $L_3 \rightarrow L_3 - L_2$ donne :

$$\begin{aligned} \det(A(x)) &= (x+1)(x+2) \begin{vmatrix} x+2 & 2x+3 & 3x+4 \\ 1 & 1 & 1 \\ 0 & 1 & 5 \end{vmatrix} \\ &= (x+1)(x+2) \left((x+2) \begin{vmatrix} 1 & 1 \\ 1 & 5 \end{vmatrix} - \begin{vmatrix} 2x+3 & 3x+4 \\ 1 & 5 \end{vmatrix} \right) \\ &= (x+1)(x+2)(4(x+2) - (7x+11)) \\ &= -(x+1)(x+2)(3x+3) = -3(x+1)^2(x+2) \end{aligned}$$

Exercice 10.6 Soient α, β deux scalaires et $A(\alpha, \beta) = ((a_{ij}))_{1 \leq i, j \leq n}$ la matrice d'ordre $n \geq 3$ définie par :

$$\forall i \in \{1, 2, \dots, n\}, \quad \begin{cases} a_{ii} = \beta, \\ a_{ij} = \alpha \text{ si } j \in \{1, 2, \dots, n\} - \{i\}. \end{cases}$$

Calculer $\Delta(\alpha, \beta) = \det(A(\alpha, \beta))$.

Solution 10.6 La matrice $A(\alpha, \beta)$ est de la forme :

$$A(\alpha, \beta) = \begin{pmatrix} \beta & \alpha & \alpha & \cdots & \alpha \\ \alpha & \beta & \alpha & \cdots & \alpha \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \alpha & \cdots & \alpha & \beta & \alpha \\ \alpha & \cdots & \alpha & \alpha & \beta \end{pmatrix}.$$

Si $\alpha = 0$, la matrice est diagonale et :

$$\Delta(0, \beta) = \beta^n.$$

On suppose que $\alpha \neq 0$.

En ajoutant les lignes 2 à n à la première ligne on a :

$$\Delta(\alpha, \beta) = (\beta + (n-1)\alpha) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \beta & \alpha & \cdots & \alpha \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \alpha & \cdots & \alpha & \beta & \alpha \\ \alpha & \cdots & \alpha & \alpha & \beta \end{vmatrix}.$$

Puis en retranchant la première ligne multipliée par α aux lignes 2 à n on obtient :

$$\begin{aligned} \Delta(\alpha, \beta) &= (\beta + (n-1)\alpha) \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & \beta - \alpha & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \beta - \alpha & 0 \\ 0 & \cdots & 0 & 0 & \beta - \alpha \end{vmatrix} \\ &= (\beta + (n-1)\alpha) (\beta - \alpha)^{n-1}. \end{aligned}$$

Exercice 10.7 En admettant que 1700, 1020, 1122 et 1309 sont tous divisibles par 17, montrer sans le calculer que le déterminant :

$$D = \begin{vmatrix} 1 & 7 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 \\ 1 & 3 & 0 & 9 \end{vmatrix}$$

est divisible par 17.

Solution 10.7 On ne change pas la valeur de ce déterminant si on remplace la colonne 4 par $C_4 + 10C_3 + 10^2C_2 + 10^3C_1$, ce qui donne :

$$D = \begin{vmatrix} 1 & 7 & 0 & 1700 \\ 1 & 0 & 2 & 1020 \\ 1 & 1 & 2 & 1122 \\ 1 & 3 & 0 & 1309 \end{vmatrix} = 17 \begin{vmatrix} 1 & 7 & 0 & 100 \\ 1 & 0 & 2 & 60 \\ 1 & 1 & 2 & 66 \\ 1 & 3 & 0 & 77 \end{vmatrix} = 17q$$

avec q entier puisque tous les coefficients du déterminant sont entiers.

Les théorèmes 10.3, 10.5 et le corollaire 10.1 se traduisent aussi par le résultat suivant.

Corollaire 10.5 Pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, toute matrice de dilatation $D_i(\lambda)$ et toute matrice de transvection $T_{ij}(\lambda)$, on a :

$$\begin{cases} \det(D_i(\lambda)A) = \det(D_i(\lambda)) \det(A) = \lambda \det(A) \\ \det(T_{ij}(\lambda)A) = \det(T_{ij}(\lambda)) \det(A) = \det(A) \end{cases}$$

En utilisant le théorème 10.2, on obtient le résultat suivant.

Théorème 10.7 Pour toute matrice inversible A et toute matrice B dans $\mathcal{M}_n(\mathbb{K})$, on a $\det(AB) = \det(A) \det(B)$.

Démonstration. La matrice A étant inversible s'écrit $A = P_1 \cdots P_r D_n(\lambda) Q_1 \cdots Q_s$, où les matrices P_i et Q_j sont des matrices de transvection et la matrice $D_n(\lambda)$ une matrice de dilatation (théorème 10.2). Une utilisation répétée du corollaire précédent nous donne :

$$\det(A) = \det(D_n(\lambda)) = \lambda$$

et pour toute matrice B :

$$\det(AB) = \det(D_n(\lambda)) \det(B) = \det(A) \det(B).$$

■

Le résultat précédent est en fait valable pour toutes matrices A et B . Le cas où la matrice A n'est pas inversible se traite en utilisant le résultat suivant.

Théorème 10.8 Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible si, et seulement si, son déterminant est non nul et dans ce cas, on a $\det(A^{-1}) = \frac{1}{\det(A)}$.

Démonstration. Si A est inversible d'inverse A^{-1} , on $AA^{-1} = I_n$ et le théorème précédent nous dit que $\det(A) \det(A^{-1}) = \det(I_n) = 1$, donc $\det(A) \neq 0$ et $\det(A^{-1}) = \frac{1}{\det(A)}$.

La réciproque se démontre par récurrence sur $n \geq 1$.

Pour $n = 1$, le résultat est évident car $\det(a) = a$ pour tout scalaire a .

Supposons le résultat acquis pour les matrices d'ordre $n - 1 \geq 1$ et soit A d'ordre n telle que $\det(A) \neq 0$. La première colonne de A est nécessairement non nulle (définition du déterminant) et on peut reprendre la démonstration du théorème 10.2 pour trouver des matrices de transvection P_1, \dots, P_k telles que :

$$P_k \cdots P_1 A = \begin{pmatrix} 1 & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & B \end{pmatrix}$$

où α est un vecteur ligne à $n - 1$ composantes et B une matrice carrée d'ordre $n - 1$.

Comme les matrices P_k sont inversibles, on a :

$$\det(A) = \det(P_k \cdots P_1 A) = \det(B)$$

et $\det(B) \neq 0$. La matrice B est donc inversible, ce qui implique que A est aussi inversible. En effet si $Ax = 0$, en notant $x = \begin{pmatrix} x_1 \\ x' \end{pmatrix}$ avec $x_1 \in \mathbb{K}$ et $x' \in \mathbb{K}^{n-1}$, on a :

$$\begin{cases} x_1 + \alpha x' = 0 \\ Bx' = 0 \end{cases}$$

ce qui entraîne $x' = 0$ et $x_1 = 0$, soit $x = 0$. La matrice A est donc inversible. ■

Théorème 10.9 Pour toutes matrices A et B dans $\mathcal{M}_n(\mathbb{K})$, on a :

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

Démonstration. Il reste à traiter le cas où la matrice A n'est pas inversible. Dans ce cas la matrice AB ne peut être inversible (sinon, en notant C l'inverse de AB , on a $(AB)C = I_n$, soit $A(BC) = I_n$ et A est inversible) et on a :

$$0 = \det(AB) = \det(A) \det(B) = 0 \cdot \det(B).$$

L'égalité $\det(BA) = \det(B) \det(A)$ donne $\det(AB) = \det(BA)$. ■

On peut remarquer que $\det(AB) = \det(BA)$ alors qu'en général $AB \neq BA$.

La multiplication à droite par une matrice élémentaire se traduisant par une action particulière sur les colonnes, on déduit de ce théorème et du théorème 10.1 les propriétés suivantes du déterminant.

Corollaire 10.6 Si $A'_j(\lambda)$ est la matrice déduite de $A \in \mathcal{M}_n(\mathbb{K})$ en multipliant sa colonne j par un scalaire λ , on a alors $\det(A'_j(\lambda)) = \lambda \det(A)$.
Si $A \in \mathcal{M}_n(\mathbb{K})$ a une colonne nulle, alors $\det(A) = 0$.

Pour l'instant, le déterminant d'une matrice se calcule en utilisant la première colonne de cette dernière. En réalité, on peut aussi utiliser la première ligne et nous en déduirons que cette première ligne ou colonne peut être remplacée par n'importe quelle autre. Précisément, on a les résultats suivants.

Théorème 10.10 Pour toute matrice A dans $\mathcal{M}_n(\mathbb{K})$, on a $\det({}^t A) = \det(A)$.

Démonstration. Comme d'habitude c'est trivial pour $n = 1$. On suppose donc que $n \geq 2$.

Si A n'est pas inversible, il en est de même de sa transposée (en effet si ${}^t A$ est inversible, il en est de même de $A = {}^t({}^t A)$ – théorème 8.19 –) et on a alors $\det({}^t A) = \det(A) = 0$.

Si A est inversible, elle s'écrit :

$$A = P_1 \cdots P_r D_n(\lambda) Q_1 \cdots Q_s$$

où les P_i, Q_j sont des matrices de transvection et $\lambda = \det(A)$, ce qui donne :

$${}^t A = {}^t Q_s \cdots {}^t Q_1 {}^t D_n(\lambda) {}^t P_r \cdots {}^t P_1$$

les transposées de matrices élémentaires étant des matrices élémentaires de même type avec ${}^t D_n(\lambda) = D_n(\lambda)$, ce qui donne :

$$\det({}^t A) = \det(D_n(\lambda)) = \lambda = \det(A).$$

■

De ce résultat, on déduit le développement du déterminant suivant la première ligne (pour $n \geq 2$) :

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

où $A_{1,j}$ est la matrice carrée d'ordre $n - 1$ déduite de A en supprimant la ligne 1 et la colonne j .

On en déduit alors les propriétés suivantes relatives aux colonnes, ces propriétés étant analogues à celles obtenues pour les lignes.

Corollaire 10.7 Si A' est la matrice déduite de $A \in \mathcal{M}_n(\mathbb{K})$ en permutant deux colonnes, on a alors $\det(A') = -\det(A)$.

Soient A, A', A'' des matrices de lignes respectives C_j, C'_j, C''_j (pour j compris entre 1 et n) telles que $C_j = C'_j = C''_j$ pour $j \neq k$ et $C''_k = C_k + C'_k$ où k est un indice compris entre 1 et n . On a :

$$\det(A'') = \det(A) + \det(A').$$

On ne change pas la valeur d'un déterminant si on ajoute à une ligne une combinaison linéaire des autres lignes.

Ce corollaire se traduit en disant que le déterminant est linéaire par rapport à chaque colonne et que c'est une forme alternée sur les colonnes.

En général, pour calculer un déterminant, on essayera d'effectuer des opérations élémentaires sur les lignes ou les colonnes dans le but de faire apparaître un maximum de coefficients nuls, ce qui facilitera le calcul du déterminant de la matrice obtenue.

De tout ce qui précède, on déduit les différentes formes de développement d'un déterminant suivant une ligne ou une colonne (pour $n \geq 2$).

Théorème 10.11 Pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, on a :

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

(développement suivant la colonne j) et

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

(développement suivant la ligne i) où $A_{i,j}$ est la matrice carrée d'ordre $n-1$ déduite de A en supprimant la ligne i et la colonne j .

Démonstration. Pour $j = 1$, c'est la définition première du déterminant et pour $i = 1$ c'est une conséquence immédiate de $\det({}^t A) = \det(A)$.

Fixons la colonne $j \geq 2$ et notons $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{K}^n .

La colonne C_j s'écrit $C_j = \sum_{i=1}^n a_{i,j} e_i$ et en utilisant la linéarité du déterminant par rapport à la j -ième colonne, on a :

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

où $B_{i,j}$ est la matrice déduite de A en remplaçant C_j par e_i . En permutant la colonne j avec la colonne $j-1$, puis $j-1$ avec $j-2, \dots, 2$ avec 1 et ensuite la ligne i avec la ligne $i-1, i-1$ avec $i-2, \dots, 2$ avec 1 (on fait rien pour $i = 1$) on aboutit à :

$$\begin{aligned} \det(B_{i,j}) &= (-1)^{i+j} \begin{vmatrix} 1 & a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ 0 & a_{21} & \cdots & a_{2,j-1} & a_{2,j+1} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ 0 & a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & a_{n,1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{n,n} \end{vmatrix} \\ &= (-1)^{i+j} \det(A_{i,j}) \end{aligned}$$

et on a le résultat annoncé.

On procède de manière analogue pour la deuxième formule. ■

Avec les notations du théorème, on dit que $\det(A_{i,j})$ est le mineur d'indice (i, j) de la matrice A et que $(-1)^{i+j} \det(A_{i,j})$ est le cofacteur d'indice (i, j) de A .

Exercice 10.8 Soient $n \geq 2$ un entier et $\alpha_1, \alpha_2, \dots, \alpha_n$ des scalaires.

1. Calculer le déterminant $\Delta(\alpha_1, \dots, \alpha_n)$ de la matrice :

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

Une telle matrice est dite de Vandermonde.

2. À quelle condition une telle matrice est-elle inversible ?

Solution 10.8 Pour $n = 2$, on a $\Delta(\alpha_1, \alpha_2) = \alpha_2 - \alpha_1$ et pour $n = 3$, on a fait le calcul avec l'exercice 10.2.

1. Le calcul de $\Delta(\alpha_1, \dots, \alpha_n)$ se fait par récurrence sur $n \geq 2$.

En retranchant, pour $i = n, n-1, \dots, 2$ à la ligne i la ligne $i-1$ multipliée par α_1 , on obtient :

$$\begin{aligned} \Delta(\alpha_1, \dots, \alpha_n) &= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & \alpha_2 - \alpha_1 & \cdots & \alpha_n - \alpha_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_2^{n-2}(\alpha_2 - \alpha_1) & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} \\ &= \begin{vmatrix} \alpha_2 - \alpha_1 & \alpha_3 - \alpha_1 & \cdots & \alpha_n - \alpha_1 \\ \alpha_2(\alpha_2 - \alpha_1) & \alpha_3(\alpha_3 - \alpha_1) & \cdots & \alpha_n(\alpha_n - \alpha_1) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_2^{n-2}(\alpha_2 - \alpha_1) & \alpha_3^{n-2}(\alpha_3 - \alpha_1) & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} \end{aligned}$$

soit :

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

et par récurrence :

$$\begin{aligned} \det(A_n) &= \prod_{k=2}^n (\alpha_k - \alpha_1) \prod_{2 \leq i < j \leq n} (\alpha_j - \alpha_i) \\ &= \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i). \end{aligned}$$

2. Cette matrice est inversible si, et seulement si, les α_i sont deux à deux distincts.

Exercice 10.9 Calculer le déterminant de la matrice :

$$A_n = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2^2 & \cdots & 2^n \\ \vdots & \vdots & \ddots & \vdots \\ n & n^2 & \cdots & n^n \end{pmatrix}.$$

Solution 10.9 On a :

$$\begin{aligned} \det(A_n) &= n! \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n & \cdots & n^{n-1} \end{vmatrix} = n! \Delta(1, 2, \dots, n) \\ &= n! \prod_{1 \leq j < i \leq n} (i - j) = n! \prod_{i=2}^n (i-1)! = \prod_{i=2}^n i!. \end{aligned}$$

Exercice 10.10 Soit

$$A_n = \begin{pmatrix} a_1 & c_1 & 0 & \cdots & 0 \\ b_2 & a_2 & c_2 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & b_{n-1} & a_{n-1} & c_{n-1} \\ 0 & \cdots & 0 & b_n & a_n \end{pmatrix},$$

une matrice tridiagonale d'ordre $n \geq 3$ à coefficients réels ou complexes.

Pour tout entier k compris entre 1 et n , on désigne par D_k le déterminant de la matrice d'ordre k formée des k premières lignes et k premières colonnes de A_n (les D_k sont les déterminants extraits principaux de A_n).

1. Exprimer, pour tout k compris entre 3 et n , D_k en fonction de D_{k-1} et D_{k-2} .
2. Calculer le déterminant de :

$$A_n = \begin{pmatrix} 2 & 1 & 0 & \cdots & 0 \\ 2^2 & 5 & 1 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & (n-1)^2 & 2n-1 & 1 \\ 0 & \cdots & 0 & n^2 & 2n+1 \end{pmatrix}$$

Solution 10.10

1. En développant D_k suivant la dernière ligne on a :

$$\begin{aligned} D_k &= a_k \begin{vmatrix} a_1 & c_1 & 0 & \cdots & 0 \\ b_2 & a_2 & c_2 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & b_{k-2} & a_{k-2} & c_{k-2} \\ 0 & \cdots & 0 & b_{k-1} & a_{k-1} \end{vmatrix} - b_k \begin{vmatrix} a_1 & c_1 & 0 & \cdots & 0 \\ b_2 & a_2 & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & c_{k-3} & 0 \\ \vdots & \ddots & b_{k-2} & a_{k-2} & 0 \\ 0 & \cdots & 0 & b_{k-1} & c_{k-1} \end{vmatrix} \\ &= a_k D_{k-1} - b_k c_{k-1} D_{k-2}. \end{aligned}$$

Ce qui donne, avec les valeurs initiales $D_1 = a_1$ et $D_2 = a_1 a_2 - b_2 c_1$, un algorithme de calcul de D_n .

2. On a :

$$D_n = (2n + 1) D_{n-1} - n^2 D_{n-2}$$

avec les valeurs initiales $D_1 = 2$, $D_2 = 6$. En calculant D_3 et D_4 on conjecture que $D_n = (n + 1)!$ Ce qui se montre par récurrence sur $n \geq 2$. C'est vrai pour $n = 2$ et le supposant acquis jusqu'au rang $n - 1 \geq 2$, on a :

$$D_n = (2n + 1) n! - n^2 (n - 1)! = (n + 1)!$$

10.3 Déterminant d'une famille de vecteurs

Étant donnée une famille $(x_j)_{1 \leq j \leq n}$ de n vecteurs de \mathbb{K}^n , on définit le déterminant de cette famille comme le déterminant de la matrice A dont les colonnes sont formées de ces vecteurs. En notant, pour j compris entre 1 et n , $x_j = (x_{i,j})_{1 \leq i \leq n}$ (vecteur colonne), on a donc :

$$\det(x_1, \dots, x_n) = \det((x_{i,j}))_{1 \leq i,j \leq n}.$$

Du théorème 10.8 on déduit le résultat suivant bien utile pour vérifier qu'un système de n vecteurs dans \mathbb{K}^n est libre et donc forme une base.

Théorème 10.12 Une famille $(x_j)_{1 \leq j \leq n}$ de n vecteurs de \mathbb{K}^n est libre si, et seulement si, son déterminant est non nul.

Démonstration. En utilisant les notations qui précèdent, on note $P = ((x_{i,j}))_{1 \leq i,j \leq n}$.

Dire que le système $(x_j)_{1 \leq j \leq n}$ est libre équivaut à dire que l'unique solution $\lambda \in \mathbb{K}^n$ du système linéaire $\sum_{j=1}^n \lambda_j x_j$ est $\lambda = 0$, ce système s'écrivant aussi $P\lambda = 0$, cela revient à dire que la matrice P est inversible, ce qui est encore équivalent à $\det(P) \neq 0$. ■

Si E un espace vectoriel réel ou complexe de dimension $n \geq 1$ et \mathcal{B} une base E , en notant pour tout vecteur $x \in E$, X le vecteur colonne de \mathbb{K}^n formé des composantes de x dans la base \mathcal{B} , on définit le déterminant d'une famille $(x_j)_{1 \leq j \leq n}$ de n vecteurs de E dans la base \mathcal{B} par :

$$\det_{\mathcal{B}}(x_1, \dots, x_n) = \det(X_1, \dots, X_n).$$

Ce déterminant dépend du choix d'une base de E .

Théorème 10.13 Si \mathcal{B} et \mathcal{B}' sont deux bases de E , alors pour tout n -uplet (x_1, x_2, \dots, x_n) de vecteurs de E , on a :

$$\det_{\mathcal{B}}(x_1, x_2, \dots, x_n) = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(x_1, x_2, \dots, x_n)$$

Démonstration. En désignant pour tout vecteur x de E par X [resp. X'] le vecteur colonne de \mathbb{K}^n formé des composantes de x dans la base \mathcal{B} [resp. \mathcal{B}'] et par P la matrice de passage de \mathcal{B} à \mathcal{B}' , on a $X = PX'$ et :

$$\begin{aligned} \det_{\mathcal{B}}(x_1, x_2, \dots, x_n) &= \det(X_1, X_2, \dots, X_n) = \det(PX'_1, PX'_2, \dots, PX'_n) \\ &= \det(P \cdot (X'_1, X'_2, \dots, X'_n)) = \det(P) \det((X'_1, X'_2, \dots, X'_n)) \\ &= \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(x_1, x_2, \dots, x_n) \end{aligned}$$

■

10.4 Déterminant d'un endomorphisme

On désigne par E un espace vectoriel réel ou complexe de dimension $n \geq 1$.

Si \mathcal{B}_1 et \mathcal{B}_2 sont deux bases de E , u un endomorphisme de E , A_1 la matrice de u dans la base \mathcal{B}_1 et A_2 sa matrice dans la base \mathcal{B}_2 , on sait alors que $A_2 = P^{-1}AP$ où P est la matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 . Il en résulte alors que :

$$\begin{aligned} \det(A_2) &= \det(P^{-1}AP) = \det(P^{-1}) \det(A_1) \det(P) \\ &= \frac{1}{\det(P)} \det(A_1) \det(P) = \det(A_1). \end{aligned}$$

C'est-à-dire que ces déterminants ne dépendent pas du choix d'une base.

On peut alors donner la définition suivante.

Définition 10.6 *Le déterminant d'un endomorphisme u de E est le déterminant de la matrice de u dans une base de E .*

Du théorème 9.19, on déduit le résultat suivant.

Théorème 10.14 *Si u, v sont deux endomorphismes de E , alors :*

$$\det(u \circ v) = \det(v \circ u) = \det(u) \det(v).$$

Et du théorème 9.20, on déduit le résultat suivant.

Théorème 10.15 *Un endomorphisme u de E est inversible si, et seulement si, son déterminant est non nul.*

Formes bilinéaires et quadratiques réelles ou complexes

On se limite pour ce chapitre à l'étude des formes bilinéaires et quadratiques définies sur un espace vectoriel réel ou complexe.

On désigne pour ce chapitre par E un espace vectoriel réel ou complexe de dimension finie ou non et non réduit à $\{0\}$.

On notera \mathbb{K} le corps de réels ou des complexes, en précisant quand cela sera nécessaire s'il s'agit de \mathbb{R} ou \mathbb{C} . Par scalaire on entend réel ou complexe.

L'étude des formes quadratiques sur un corps quelconque de caractéristique différente de 2 sera reprise plus loin.

11.1 Formes linéaires

On rappelle la définition suivante déjà donnée au paragraphe 8.4.

Définition 11.1 Une forme linéaire sur E est une application linéaire de E dans \mathbb{K} .

Exemple 11.1 Si E est un espace vectoriel de dimension n et $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ une base de E , alors la j -ième projection :

$$p_j : x = \sum_{i=1}^n x_i e_i \mapsto x_j$$

où j est un entier compris entre 1 et n , est une forme linéaire sur E .

Exemple 11.2 Si E est un espace vectoriel de dimension n , $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ une base de E et $\alpha_1, \alpha_2, \dots, \alpha_n$ des scalaires, alors l'application :

$$\ell : x = \sum_{i=1}^n x_i e_i \mapsto \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$$

est une forme linéaire sur E .

En fait toutes les formes linéaires sur E de dimension n sont de la forme précédente. En effet, tout vecteur x de E s'écrit $x = \sum_{j=1}^n x_j e_j$ et pour tout forme linéaire ℓ sur E , on a :

$$\ell(x) = \ell\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j \ell(e_j) = \sum_{j=1}^n \alpha_j x_j$$

en notant $\alpha_j = \ell(e_j)$ pour tout entier j compris entre 1 et n .

La matrice ligne :

$$L = (\alpha_1, \alpha_2, \dots, \alpha_n) = (\ell(e_1), \ell(e_2), \dots, \ell(e_n))$$

est tout simplement la matrice de ℓ dans la base $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ de E et on a :

$$\forall x \in E, \ell(x) = L \cdot x = (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{j=1}^n \alpha_j x_j.$$

Ce résultat peut aussi s'exprimer sous la forme :

$$\forall x \in E, \ell(x) = \sum_{j=1}^n \alpha_j p_j(x) = \left(\sum_{j=1}^n \alpha_j p_j \right) (x)$$

où p_j désigne, pour j compris entre 1 et n , la projection $x \mapsto x_j$.

On peut donc écrire, une base \mathcal{B} de E étant donnée, toute forme linéaire ℓ sur E sous la forme :

$$\ell = \sum_{j=1}^n \alpha_j p_j$$

où les $\alpha_j \in \mathbb{K}$ sont uniquement déterminés par $\alpha_j = \ell(e_j)$ pour tout entier j compris entre 1 et n .

Nous avons donc montré le résultat suivant.

Théorème 11.1 *Si E est un espace vectoriel de dimension n et $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ une base de E , alors l'ensemble de toutes les formes linéaires sur E est un espace vectoriel de dimension n de base (p_1, \dots, p_n) .*

On rappelle que si on dispose d'une base \mathcal{B} d'un espace vectoriel E dire qu'une famille (v_1, \dots, v_p) d'éléments de E est libre (ou que ces éléments sont linéairement indépendants) équivaut à dire que les vecteurs colonnes X_1, \dots, X_p formés des composantes de ces vecteurs dans la base \mathcal{B} sont linéairement indépendants dans \mathbb{K}^n . On peut donc parler de formes linéaires linéairement indépendantes.

On rappelle également que pour montrer que le système (X_1, \dots, X_p) est libre dans \mathbb{K}^n , il suffit d'extraire de la matrice (X_1, \dots, X_p) un déterminant d'ordre p non nul (ce qui impose bien sur que $p \leq n$).

Dire que le système (X_1, \dots, X_p) est libre dans \mathbb{K}^n équivaut aussi à dire que la matrice (X_1, \dots, X_p) est de rang p . Comme une matrice et sa transposée ont même rang, il revient au

même de calculer le rang de la matrice transposée $\begin{pmatrix} {}^t X_1 \\ \vdots \\ {}^t X_p \end{pmatrix}$.

On retiendra que des formes linéaires ℓ_1, \dots, ℓ_p définies sur E , de base $\mathcal{B} = (e_j)_{1 \leq j \leq n}$, par :

$$\forall x \in E, \ell_i(x) = \sum_{j=1}^n \alpha_{i,j} x_j \quad (1 \leq i \leq p)$$

sont linéairement indépendantes si, et seulement si la matrice :

$$A = \begin{pmatrix} L_1 \\ \vdots \\ L_p \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & & \ddots & \vdots \\ \alpha_{p1} & \alpha_{p2} & \cdots & \alpha_{pn} \end{pmatrix}$$

est de rang p (L_i est la matrice de ℓ_i dans la base \mathcal{B} de E), ce qui revient à dire qu'on peut en extraire un déterminant d'ordre p non nul.

Exercice 11.1 Montrer que les formes linéaires $(\ell_j)_{1 \leq j \leq 3}$ définies sur \mathbb{K}^5 par :

$$\begin{cases} \ell_1(x) = x_1 + x_2 + x_3 + x_4 + x_5 \\ \ell_2(x) = 3x_1 - 2x_3 + 2x_4 + x_5 \\ \ell_3(x) = 3x_2 + x_3 + 3x_4 \end{cases}$$

sont linéairement indépendantes.

Solution 11.1 Il s'agit de vérifier que la matrice :

$$A = \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 0 & -2 & 2 & 1 \\ 0 & 3 & 1 & 3 & 0 \end{pmatrix}$$

est de rang 3, ce qui résulte de :

$$\begin{vmatrix} 1 & 1 & 1 \\ 3 & 0 & -2 \\ 0 & 3 & 1 \end{vmatrix} = 12 \neq 0.$$

Remarque 11.1 La somme de deux formes linéaires sur E est une forme linéaire, mais en général le produit de deux formes linéaires sur E n'est pas une forme linéaire.

Exercice 11.2 Soient ℓ_1 et ℓ_2 deux formes linéaires sur E . Montrer que l'application $\ell_1\ell_2$ est une forme linéaire sur E si, et seulement si, l'une de ces deux formes est l'application nulle.

Solution 11.2 Il est clair que si l'une de ces deux formes est l'application nulle, alors $\ell_1\ell_2$ est une forme linéaire sur E .

Réciproquement supposons que $\ell_1\ell_2$ soit linéaire. On a alors pour tout scalaire λ et tous vecteurs x, y dans E :

$$\begin{aligned} \ell_1(x)\ell_2(x) + \lambda\ell_1(y)\ell_2(y) &= (\ell_1\ell_2)(x) + \lambda(\ell_1\ell_2)(y) \\ &= (\ell_1\ell_2)(x + \lambda y) = \ell_1(x + \lambda y)\ell_2(x + \lambda y) \\ &= (\ell_1(x) + \lambda\ell_1(y))(\ell_2(x) + \lambda\ell_2(y)) \\ &= \ell_1(x)\ell_2(x) + \lambda(\ell_1(x)\ell_2(y) + \ell_1(y)\ell_2(x)) + \lambda^2\ell_1(y)\ell_2(y) \end{aligned}$$

et le polynôme :

$$\ell_1(y)\ell_2(y)\lambda^2 + (\ell_1(x)\ell_2(y) + \ell_1(y)\ell_2(x) - \ell_1(y)\ell_2(y))\lambda$$

est identiquement nul, ce qui équivaut à :

$$\ell_1(y)\ell_2(y) = 0 \text{ et } \ell_1(x)\ell_2(y) + \ell_1(y)\ell_2(x) - \ell_1(y)\ell_2(y) = 0$$

ou encore à :

$$\ell_1(y) \ell_2(y) = 0 \text{ et } \ell_1(x) \ell_2(y) + \ell_1(y) \ell_2(x) = 0$$

pour tous x, y dans E .

Si $\ell_1 \neq 0$, il existe alors $y \in E$ tel que $\ell_1(y) \neq 0$, donc $\ell_2(y) = 0$ et $\ell_1(y) \ell_2(x) = 0$ pour tout $x \in E$, ce qui équivaut à $\ell_2 = 0$.

Exercice 11.3 Déterminer le noyau de la forme linéaire définie sur l'espace \mathbb{K}^3 par :

$$\ell : v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto x - y$$

Solution 11.3 Ce noyau est :

$$\begin{aligned} \ker(\ell) &= \{v \in \mathbb{K}^3 \mid x = y\} \\ &= \left\{ v = \begin{pmatrix} x \\ x \\ z \end{pmatrix} = xv_1 + zv_2 \mid (x, y) \in \mathbb{K}^2 \right\} \end{aligned}$$

où on a noté $v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ et $v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Les vecteurs v_1 et v_2 étant linéairement indépendants, ce noyau est le plan vectoriel engendré par v_1 et v_2 .

De manière plus générale, on donne la définition suivante.

Définition 11.2 On appelle hyperplan vectoriel de E , le noyau d'une forme linéaire non nulle sur E .

De manière un peu plus générale, un hyperplan affine de E est un sous-ensemble de E de la forme :

$$H = \{x \in E \mid \ell(x) = \lambda\}$$

où ℓ est une forme linéaire non nulle et λ un réel.

Sur E , de base $\mathcal{B} = (e_j)_{1 \leq j \leq n}$, un hyperplan et donc l'ensemble des vecteurs $x = \sum_{j=1}^n x_j e_j$ tels que :

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$$

où les scalaires α_j ne sont pas tous nuls.

De plus une forme linéaire non nulle ℓ étant surjective (exercice 8.8), le théorème du rang nous dit que, pour E de dimension n , on a :

$$\dim(\ker(\ell)) = n - 1.$$

Réciproquement si H est un sous-espace de dimension $n - 1$ dans E de dimension n , il admet une base $(e_i)_{1 \leq i \leq n-1}$ qui peut se compléter en une base $(e_i)_{1 \leq i \leq n}$ de E et H est le noyau de la n -ième projection :

$$p_n : x = \sum_{j=1}^n x_j e_j \mapsto x_n.$$

Nous avons donc montré le résultat suivant.

Théorème 11.2 *Sur un espace vectoriel E de dimension n un hyperplan est un sous-espace de E de dimension $n - 1$.*

Les supplémentaires d'un hyperplan dans E de dimension finie sont donc des droites. En fait ce résultat est général.

Théorème 11.3 *Si H est un hyperplan d'un espace vectoriel E , il existe alors une droite D telle que $E = H \oplus D$.*

Démonstration. On a $H = \ker(\ell)$ où ℓ est une forme linéaire non nulle sur E . Il existe donc un vecteur non nul a dans E tel que $\ell(a) \neq 0$. En désignant par $D = \mathbb{K}a$ la droite dirigée par a , on a alors $E = H \oplus D$. En effet, si $x \in H \cap D$, il existe un scalaire λ tel que $x = \lambda a$ et $\ell(x) = \lambda \ell(a) = 0$ nous donne $\lambda = 0$. On a donc $H \cap D = \{0\}$. De plus pour tout vecteur $x \in E$, le vecteur $y = x - \frac{\ell(x)}{\ell(a)}a$ est dans $H = \ker(\ell)$ et avec $x = y + \frac{\ell(x)}{\ell(a)}a$, on déduit que $x \in H + D$. On a donc $E = H + D$ et $E = H \oplus D$. ■

Réciproquement un sous-espace vectoriel H de E supplémentaire d'une droite D est le noyau de la forme linéaire ℓ qui associe à tout vecteur x de E sa projection sur D , c'est donc un hyperplan.

On a donc le résultat suivant.

Théorème 11.4 *Un hyperplan de E est un sous-espace de E supplémentaire d'une droite.*

11.2 Formes bilinéaires

Définition 11.3 *Une forme bilinéaire sur E est une application :*

$$\begin{aligned} \varphi : E \times E &\rightarrow \mathbb{K} \\ (x, y) &\mapsto \varphi(x, y) \end{aligned}$$

telle que pour tout x dans E l'application $y \mapsto \varphi(x, y)$ est linéaire et pour tout y dans E l'application $x \mapsto \varphi(x, y)$ est linéaire.

Définition 11.4 *On dit qu'une forme bilinéaire φ sur E est symétrique si $\varphi(y, x) = \varphi(x, y)$ pour tous x, y dans E .*

Définition 11.5 *On dit qu'une forme bilinéaire φ sur E est anti-symétrique (ou alternée) si $\varphi(y, x) = -\varphi(x, y)$ pour tous x, y dans E .*

Remarque 11.2 *Une application symétrique φ de E^2 dans \mathbb{K} est bilinéaire si, et seulement si, l'une des deux applications $y \mapsto \varphi(x, y)$ (pour tout x dans E) ou $x \mapsto \varphi(x, y)$ (pour tout y dans E) est linéaire.*

Exemple 11.3 *Si ℓ_1 et ℓ_2 sont deux formes linéaires sur E , alors l'application :*

$$(x, y) \mapsto \ell_1(x) \ell_2(y)$$

est une forme bilinéaire sur E .

Exemple 11.4 Si E est l'espace $\mathcal{C}^0([a, b], \mathbb{R})$ des fonctions continues de $[a, b]$ dans \mathbb{R} , alors l'application :

$$\varphi : (f, g) \mapsto \int_a^b f(t) g(t) dt$$

est une forme bilinéaire.

Exemple 11.5 Si ℓ_1, \dots, ℓ_p sont des formes linéaires sur E et $(\alpha_{ij})_{1 \leq i, j \leq p}$ une famille de scalaires, alors l'application :

$$(x, y) \mapsto \sum_{1 \leq i, j \leq p} \alpha_{ij} \ell_i(x) \ell_j(y)$$

est une forme bilinéaire.

Nous verrons un peu plus loin que, sur un espace de dimension n , toutes les formes bilinéaires sont de la forme précédente.

On notera $Bil(E)$ l'ensemble de toutes les formes bilinéaires sur E .

On vérifie facilement que $Bil(E)$ est un espace vectoriel.

Exercice 11.4 Montrer que toute forme bilinéaire φ sur E s'écrit de manière unique comme somme d'une forme bilinéaire symétrique et d'une forme bilinéaire alternée.

Solution 11.4 Soit φ une forme bilinéaire sur E . Les applications φ_1 et φ_2 définies sur E^2 par :

$$\begin{cases} \varphi_1(x, y) = \frac{1}{2}(\varphi(x, y) + \varphi(y, x)) \\ \varphi_2(x, y) = \frac{1}{2}(\varphi(x, y) - \varphi(y, x)) \end{cases}$$

sont bilinéaires, la forme φ_1 étant symétrique et φ_2 étant alternée. Et on a bien $\varphi = \varphi_1 + \varphi_2$. Réciproquement si $\varphi = \varphi_1 + \varphi_2$ avec φ_1 bilinéaire symétrique et φ_2 bilinéaire alternée, on a alors :

$$\begin{cases} \varphi(x, y) = \varphi_1(x, y) + \varphi_2(x, y) \\ \varphi(y, x) = \varphi_1(y, x) + \varphi_2(y, x) = \varphi_1(x, y) - \varphi_2(x, y) \end{cases}$$

et $\varphi(x, y) + \varphi(y, x) = 2\varphi_1(x, y)$, $\varphi(x, y) - \varphi(y, x) = \varphi_2(x, y)$, ce qui prouve l'unicité de φ_1 et φ_2 .

En désignant par $Bil_s(E)$ [resp. $Bil_a(E)$] le sous-ensemble de $Bil(E)$ constitué des formes bilinéaires symétriques [resp. alternées] sur E , on vérifie facilement que $Bil_s(E)$ et $Bil_a(E)$ sont des sous-espaces vectoriels de $Bil(E)$ et l'exercice précédant nous dit que $Bil(E)$ est somme directe de $Bil_s(E)$ et $Bil_a(E)$, soit :

$$Bil(E) = Bil_s(E) \oplus Bil_a(E)$$

11.3 Expression matricielle des formes bilinéaires (en dimension finie)

Comme pour les applications linéaires, les matrices nous serviront à décrire une forme bilinéaire dans le cas des espaces de dimension finie.

Pour ce paragraphe E est un espace vectoriel de dimension n et on désigne par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E .

Tout vecteur $x \in E$ s'écrit de manière unique sous la forme $x = \sum_{j=1}^n x_j e_j$. On associe à un tel

x le vecteur colonne $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ de \mathbb{K}^n .

Plaçons nous tout d'abord sur $E = \mathbb{R}^2$ (ou \mathbb{C}^2) muni de sa base canonique (e_1, e_2) . Si φ est une forme bilinéaire sur E , on a alors pour tous vecteurs $x = x_1 e_1 + x_2 e_2$ et $y = y_1 e_1 + y_2 e_2$ dans E :

$$\begin{aligned} \varphi(x, y) &= \varphi(x_1 e_1 + x_2 e_2, y) \\ &= x_1 \varphi(e_1, y) + x_2 \varphi(e_2, y) \\ &= x_1 \varphi(e_1, y_1 e_1 + y_2 e_2) + x_2 \varphi(e_2, y_1 e_1 + y_2 e_2) \\ &= x_1 (y_1 \varphi(e_1, e_1) + y_2 \varphi(e_1, e_2)) + x_2 (y_1 \varphi(e_2, e_1) + y_2 \varphi(e_2, e_2)) \end{aligned}$$

En désignant par A la matrice :

$$A = \begin{pmatrix} \varphi(e_1, e_1) & \varphi(e_1, e_2) \\ \varphi(e_2, e_1) & \varphi(e_2, e_2) \end{pmatrix}$$

on remarque que :

$$\begin{aligned} AY &= \begin{pmatrix} \varphi(e_1, e_1) & \varphi(e_1, e_2) \\ \varphi(e_2, e_1) & \varphi(e_2, e_2) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} y_1 \varphi(e_1, e_1) + y_2 \varphi(e_1, e_2) \\ y_1 \varphi(e_2, e_1) + y_2 \varphi(e_2, e_2) \end{pmatrix} \end{aligned}$$

et :

$$\begin{aligned} {}^t X (AY) &= (x_1, x_2) \begin{pmatrix} y_1 \varphi(e_1, e_1) + y_2 \varphi(e_1, e_2) \\ y_1 \varphi(e_2, e_1) + y_2 \varphi(e_2, e_2) \end{pmatrix} \\ &= \varphi(x, y). \end{aligned}$$

Le produit des matrices étant associatif, cela s'écrit :

$$\varphi(x, y) = {}^t X A Y$$

Le cas d'une forme bilinéaire sur un espace de dimension n se traite de manière analogue.

Définition 11.6 La matrice d'une forme bilinéaire φ dans la base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E est la matrice carrée d'ordre n :

$$A = ((\varphi(e_i, e_j)))_{1 \leq i, j \leq n}.$$

Théorème 11.5 Soit φ une forme bilinéaire sur E et A la matrice de φ dans la base \mathcal{B} . Pour tous vecteurs x, y dans E , on a :

$$\varphi(x, y) = {}^t X A Y$$

Démonstration. En utilisant la bilinéarité de φ , on a :

$$\begin{aligned} \varphi(x, y) &= \varphi\left(\sum_{i=1}^n x_i e_i, y\right) = \sum_{i=1}^n x_i \varphi(e_i, y) \\ &= \sum_{i=1}^n x_i \varphi\left(e_i, \sum_{j=1}^n y_j e_j\right) = \sum_{i=1}^n x_i \sum_{j=1}^n y_j \varphi(e_i, e_j) \end{aligned}$$

et avec :

$$AY = \left(\sum_{j=1}^n y_j \varphi(e_i, e_j) \right)_{1 \leq i \leq n}$$

$${}^t XAY = {}^t X(AY) = \sum_{i=1}^n x_i \sum_{j=1}^n y_j \varphi(e_i, e_j)$$

on a le résultat annoncé. ■

On retiendra que l'expression d'une forme bilinéaire φ dans une base est :

$$\varphi(x, y) = {}^t XAY = \sum_{i=1}^n x_i \sum_{j=1}^n a_{ij} y_j = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j$$

où on a posé $a_{ij} = \varphi(e_i, e_j)$ pour i, j compris entre 1 et n .

Réciproquement une telle fonction sur E^2 définit bien une forme bilinéaire sur E .

Ce résultat peut aussi s'exprimer comme suit.

Théorème 11.6 *Une application φ de $E \times E$ dans \mathbb{K} est une forme bilinéaire sur E si, et seulement si, et seulement si, il existe une matrice $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans $\mathcal{M}_n(\mathbb{K})$ et des formes linéaires ℓ_1, \dots, ℓ_n linéairement indépendantes telles que :*

$$\forall (x, y) \in E \times E, \varphi(x, y) = \sum_{1 \leq i, j \leq n} a_{ij} \ell_i(x) \ell_j(y).$$

Démonstration. Si φ est bilinéaire, on a dans une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E , pour tous x, y dans E :

$$\varphi(x, y) = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j = \sum_{1 \leq i, j \leq n} a_{ij} \ell_i(x) \ell_j(y)$$

où $(\ell_i)_{1 \leq i \leq n}$ est la base duale de \mathcal{B} .

Et la réciproque est claire. ■

L'application qui associe à une forme bilinéaire φ sur un espace vectoriel E de dimension n sa matrice dans une base donnée de E réalise un isomorphisme de $\text{Bil}(E)$ sur l'espace $\mathcal{M}_n(\mathbb{K})$ des matrices carrées d'ordre n . Cet espace étant de dimension n^2 , on en déduit que :

$$\dim_{\mathbb{K}}(\text{Bil}(E)) = n^2.$$

Théorème 11.7 *Une forme bilinéaire φ sur E est symétrique [resp. alternée] si, et seulement si, sa matrice A dans une quelconque base \mathcal{B} de E est symétrique [resp. alternée].*

Démonstration. Si φ est symétrique [resp. alternée], on a en particulier $\varphi(e_i, e_j) = \varphi(e_j, e_i)$ [resp. $\varphi(e_i, e_j) = -\varphi(e_j, e_i)$] pour tous i, j compris entre 1 et n , ce qui signifie que la matrice A de φ dans \mathcal{B} est symétrique [resp. alternée].

Réciproquement si cette matrice est symétrique [resp. alternée], on a alors pour tous x, y dans E :

$$\varphi(y, x) = {}^t YAX = {}^t ({}^t YAX) = {}^t X {}^t AY = {}^t XAY = \varphi(x, y)$$

$$\text{resp. } \varphi(y, x) = {}^t YAX = {}^t ({}^t YAX) = {}^t X {}^t AY = -{}^t XAY = -\varphi(x, y)$$

(le produit matriciel $T = {}^t YAX$ étant un scalaire, on a bien ${}^t T = T$). ■

Le sous-espace $Bil_s(E)$ de $Bil(E)$ formé des formes bilinéaires symétriques sur E est donc isomorphe au sous-espace de $\mathcal{M}_n(\mathbb{K})$ formé des matrices symétriques, cet espace étant de dimension $\frac{n(n+1)}{2}$, il en résulte que :

$$\dim(Bil_s(E)) = \frac{n(n+1)}{2}.$$

Avec $Bil(E) = Bil_s(E) \oplus Bil_a(E)$, on déduit que :

$$\dim(Bil_a(E)) = n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2}$$

Exercice 11.5 Montrer que chacune des applications φ qui suivent est bilinéaire et calculer sa matrice dans la base canonique de \mathbb{R}^n .

1. $n = 2$, $\varphi(x, y) = x_1y_1 - 2x_2y_2$.
2. $n = 3$, $\varphi(x, y) = x_1y_1 - x_1y_2 - x_2y_2 - 2x_2y_3 - x_3y_1 - 2x_3y_3$.
3. $n = 3$, $\varphi(x, y) = 2x_1y_1 - 3x_2y_2 - x_3y_3$.

Solution 11.5 La bilinéarité de chacune de ces applications est évidente. Les matrices respectives dans les bases canoniques sont :

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & -2 \\ -1 & 0 & -2 \end{pmatrix}, A_3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

La première et la troisième sont symétriques, mais pas la deuxième.

Exercice 11.6 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$. Déterminer la forme bilinéaire φ sur \mathbb{R}^3 de matrice A dans la base canonique.

Solution 11.6 On a :

$$\begin{aligned} \varphi(x, y) &= {}^tXAY = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \\ &= x_1(y_1 + 2y_2 + 3y_3) + x_2(2y_1 + 3y_2 + 4y_3) + x_3(3y_1 + 4y_2 + 5y_3) \end{aligned}$$

Exercice 11.7 Déterminer dans la base canonique $\mathcal{B} = (e_1, e_2, e_3)$ de \mathbb{R}^3 la matrice de la forme bilinéaire symétrique φ telle que pour $v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, on ait :

$$\begin{aligned} \varphi(v_1, v_1) &= 5, \quad \varphi(v_1, v_2) = 0, \quad \varphi(v_1, v_3) = -1, \\ \varphi(v_2, v_2) &= 1, \quad \varphi(v_2, v_3) = 4, \quad \varphi(v_3, v_3) = 0. \end{aligned}$$

Solution 11.7 Comme :

$$\det(v_1, v_2, v_3) = \begin{vmatrix} 1 & -1 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \end{vmatrix} = 2 \neq 0$$

$\mathcal{B}' = (v_1, v_2, v_3)$ est une base de \mathbb{R}^3 .

En désignant, pour tous vecteurs x, y dans \mathbb{R}^3 , par $(x'_j)_{1 \leq j \leq 3}$ et $(y'_j)_{1 \leq j \leq 3}$ les coordonnées de ces vecteurs dans la base \mathcal{B}' , on a (en supposant que φ existe) :

$$\begin{aligned}\varphi(x, y) &= \varphi(x'_1 v_1 + x'_2 v_2 + x'_3 v_3, y'_1 v_1 + y'_2 v_2 + y'_3 v_3) \\ &= x'_1 y'_1 \varphi(v_1, v_1) + x'_2 y'_2 \varphi(v_2, v_2) + x'_3 y'_3 \varphi(v_3, v_3) \\ &\quad + (x'_1 y'_2 + x'_2 y'_1) \varphi(v_1, v_2) + (x'_1 y'_3 + x'_3 y'_1) \varphi(v_1, v_3) \\ &\quad + (x'_2 y'_3 + x'_3 y'_2) \varphi(v_2, v_3) \\ &= 5x'_1 y'_1 + x'_2 y'_2 - (x'_1 y'_3 + x'_3 y'_1) + 4(x'_2 y'_3 + x'_3 y'_2)\end{aligned}$$

Par ailleurs, avec :

$$\begin{cases} v_1 = e_1 + 2e_2 + e_3 \\ v_2 = -e_1 + 2e_2 \\ v_3 = e_1 + e_3 \end{cases}$$

on déduit que :

$$\begin{cases} e_1 = v_1 - v_2 - v_3 \\ e_2 = \frac{1}{2}(v_1 - v_3) \\ e_3 = -v_1 + v_2 + 2v_3 \end{cases}$$

et :

$$\begin{aligned}\varphi(e_1, e_1) &= 16, \quad \varphi(e_2, e_2) = \frac{7}{4}, \quad \varphi(e_3, e_3) = 26, \\ \varphi(e_1, e_2) &= \frac{11}{2}, \quad \varphi(e_1, e_3) = -21, \quad \varphi(e_2, e_3) = -6\end{aligned}$$

ce qui permet de définir φ dans la base canonique et montre l'unicité d'une telle forme. Réciproquement, on vérifie que cette application bilinéaire convient.

L'exercice précédent peut se résoudre de façon plus efficace en utilisant la formule de changement de base donnée par le résultat qui suit.

Théorème 11.8 Soient \mathcal{B}_1 et \mathcal{B}_2 deux bases de E et P la matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 . Si A_1 et A_2 sont les matrices d'une forme bilinéaire φ sur E dans les bases \mathcal{B}_1 et \mathcal{B}_2 respectivement, on a alors :

$$A_2 = {}^t P A_1 P.$$

Démonstration. Pour $x \in E$, on note respectivement X_1 et X_2 les vecteurs colonnes formés des composantes de x dans les bases \mathcal{B}_1 et \mathcal{B}_2 respectivement. Pour tous vecteurs x, y dans E , on a alors :

$$\begin{aligned}\varphi(x, y) &= {}^t X_1 A_1 Y_1 = {}^t (P X_2) A_1 (P Y_2) \\ &= {}^t X_2 ({}^t P A_1 P) Y_2\end{aligned}$$

ce qui signifie exactement que $A_2 = {}^t P A_1 P$ du fait de l'unicité de la matrice de φ dans la base \mathcal{B}_2 . ■

Exercice 11.8 Reprendre l'exercice 11.7 en utilisant le théorème précédent.

Solution 11.8 La matrice de passage de \mathcal{B} à \mathcal{B}' est :

$$P = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

et la matrice de φ dans \mathcal{B}' :

$$A' = \begin{pmatrix} \varphi(v_1, v_1) & \varphi(v_1, v_2) & \varphi(v_1, v_3) \\ \varphi(v_2, v_1) & \varphi(v_2, v_2) & \varphi(v_2, v_3) \\ \varphi(v_3, v_1) & \varphi(v_3, v_2) & \varphi(v_3, v_3) \end{pmatrix} = \begin{pmatrix} 5 & 0 & -1 \\ 0 & 1 & 4 \\ -1 & 4 & 0 \end{pmatrix}$$

Il en résulte que la matrice de φ dans \mathcal{B} est :

$$A = {}^t P^{-1} A' P^{-1}$$

avec :

$$P^{-1} = \begin{pmatrix} 1 & \frac{1}{2} & -1 \\ -1 & 0 & 1 \\ -1 & -\frac{1}{2} & 2 \end{pmatrix}$$

ce qui donne :

$$\begin{aligned} A &= \begin{pmatrix} 1 & -1 & -1 \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ -1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 5 & 0 & -1 \\ 0 & 1 & 4 \\ -1 & 4 & 0 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} & -1 \\ -1 & 0 & 1 \\ -1 & -\frac{1}{2} & 2 \end{pmatrix} \\ &= \begin{pmatrix} 16 & \frac{11}{2} & -21 \\ \frac{11}{2} & \frac{7}{4} & -6 \\ -21 & -6 & 26 \end{pmatrix}. \end{aligned}$$

Définition 11.7 Le discriminant dans une base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ de E d'une forme bilinéaire φ est le déterminant de la matrice $A = ((\varphi(e_i, e_j)))_{1 \leq i, j \leq n}$ de φ dans cette base. On le note $\Delta_{\mathcal{B}}(\varphi)$.

En utilisant le théorème 11.8, on déduit que si \mathcal{B}_1 et \mathcal{B}_2 sont deux bases de E et P la matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 , on a alors pour toute forme bilinéaire φ sur E :

$$\Delta_{\mathcal{B}_2}(\varphi) = (\det(P))^2 \Delta_{\mathcal{B}_1}(\varphi)$$

Exercice 11.9 Soient E, F deux espaces vectoriels, u une application linéaire de E dans F et φ une forme bilinéaire sur F .

1. Montrer que l'application ψ définie sur E^2 par :

$$\forall (x, y) \in E^2, \psi(x, y) = \varphi(u(x), u(y))$$

est bilinéaire.

2. En supposant E et F de dimension finie et en désignant par \mathcal{B}_1 une base de E , \mathcal{B}_2 une base de F , A la matrice de u dans les bases \mathcal{B}_1 et \mathcal{B}_2 et par B la matrice de φ dans la base \mathcal{B}_2 , déterminer la matrice de ψ dans la base \mathcal{B}_1 .

3. On suppose ici que E est de dimension $n \geq 1$ et que φ est une forme bilinéaire sur E . On appelle matrice de Gram d'une famille $(x_i)_{1 \leq i \leq n}$ de vecteurs de E , la matrice :

$$G(x_1, \dots, x_n) = ((\varphi(x_i, x_j)))_{1 \leq i, j \leq n}$$

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

- (a) En désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E , montrer que :

$$g(x_1, \dots, x_n) = (\det_{\mathcal{B}}(x_1, \dots, x_n))^2 \Delta_{\mathcal{B}}(\varphi)$$

- (b) Montrer que pour tout endomorphisme u de E , on a :

$$g(u(x_1), \dots, u(x_n)) = (\det(u))^2 g(x_1, \dots, x_n)$$

Solution 11.9

1. Pour x [resp. y] fixé dans E , l'application $y \mapsto \varphi(u(x), u(y))$ [resp. $x \mapsto \varphi(u(x), u(y))$] est linéaire comme composée de deux applications linéaires. L'application ψ est donc bilinéaire sur E .
2. On note, pour tout vecteur x de E , X le vecteur colonne formé des composantes de x dans la base \mathcal{B}_1 . Pour x, y dans E , on a :

$$\varphi(u(x), u(y)) = {}^t(AX) B (AY) = {}^tX ({}^tABA) Y$$

et en conséquence tABA est la matrice de ψ dans la base \mathcal{B}_1 .

3.

- (a) Soient $u \in \mathcal{L}(E)$ défini par $u(e_i) = x_i$ pour tout i compris entre 1 et n et ψ la forme bilinéaire définie sur E^2 par :

$$\forall (x, y) \in E^2, \psi(x, y) = \varphi(u(x), u(y))$$

On a :

$$\begin{aligned} \Delta_{\mathcal{B}}(\psi) &= \det \left(((\psi(e_i, e_j)))_{1 \leq i, j \leq n} \right) \\ &= \det \left(((\varphi(u(e_i), u(e_j))))_{1 \leq i, j \leq n} \right) \\ &= \det \left(((\varphi(x_i, x_j)))_{1 \leq i, j \leq n} \right) \\ &= g(x_1, \dots, x_n) \end{aligned}$$

et avec la question 2. on a aussi :

$$\begin{aligned} \Delta_{\mathcal{B}}(\psi) &= \det({}^tABA) = (\det(A))^2 \det(B) \\ &= (\det_{\mathcal{B}}(x_1, \dots, x_n))^2 \Delta_{\mathcal{B}}(\varphi) \end{aligned}$$

- (b) On a :

$$g(u(x_1), \dots, u(x_n)) = (\det_{\mathcal{B}}(u(x_1), \dots, u(x_n)))^2 \Delta_{\mathcal{B}}(\varphi)$$

avec :

$$\det_{\mathcal{B}}(u(x_1), \dots, u(x_n)) = \det(u) \det_{\mathcal{B}}(x_1, \dots, x_n)$$

ce qui donne :

$$\begin{aligned} g(u(x_1), \dots, u(x_n)) &= (\det(u))^2 (\det_{\mathcal{B}}(x_1, \dots, x_n))^2 \Delta_{\mathcal{B}}(\varphi) \\ &= (\det(u))^2 g(x_1, \dots, x_n) \end{aligned}$$

11.4 Formes quadratiques

Définition 11.8 On appelle forme quadratique sur E une application q définie de E dans \mathbb{K} par :

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

où φ est une forme bilinéaire.

Remarque 11.3 Il est facile de vérifier que l'ensemble $Q(E)$ des formes quadratiques sur E est un espace vectoriel.

Remarque 11.4 A priori, il n'y a pas unicité des formes bilinéaires associées à une forme quadratique. Par exemple sur \mathbb{R}^2 , les formes bilinéaires φ et ψ définies par :

$$\begin{cases} \varphi(x, y) = x_1 y_1 + x_2 y_2 \\ \psi(x, y) = x_1 y_1 + x_1 y_2 - x_2 y_1 + x_2 y_2 \end{cases}$$

définissent la même forme quadratique :

$$\begin{aligned} q(x) &= \varphi(x, x) = x_1^2 + x_2^2 \\ &= \psi(x, x) = x_1^2 + x_1 x_2 - x_2 x_1 + x_2^2 \end{aligned}$$

L'unicité de φ est assurée par le résultat suivant.

Théorème 11.9 Si q est une forme quadratique sur E , il existe alors une unique forme bilinéaire symétrique φ telle que $q(x) = \varphi(x, x)$ pour tout $x \in E$.

Démonstration. La forme quadratique q est définie par $q(x) = \varphi_0(x, x)$ pour tout $x \in E$, où φ_0 est une forme bilinéaire sur E . L'application φ définie sur $E \times E$ par :

$$\varphi(x, y) = \frac{1}{2} (\varphi_0(x, y) + \varphi_0(y, x))$$

est bilinéaire et symétrique avec $\varphi(x, x) = q(x)$ pour tout $x \in E$, ce qui prouve l'existence de φ .

Comme φ est bilinéaire et symétrique, on a pour x, y dans E :

$$\begin{aligned} q(x + y) &= \varphi(x + y, x + y) = \varphi(x, x) + 2\varphi(x, y) + \varphi(y, y) \\ &= q(x) + 2\varphi(x, y) + q(y) \end{aligned}$$

de sorte que :

$$\varphi(x, y) = \frac{1}{2} (q(x + y) - q(x) - q(y))$$

ce qui prouve l'unicité de φ . ■

Définition 11.9 Avec les notations du théorème qui précède, on dit que φ est la forme polaire de la forme quadratique q .

On retiendra l'expression de cette forme polaire :

$$\forall (x, y) \in E^2, \varphi(x, y) = \frac{1}{2} (q(x + y) - q(x) - q(y))$$

En écrivant que :

$$\begin{cases} q(x+y) = q(x) + 2\varphi(x, y) + q(y) \\ q(x-y) = q(x) - 2\varphi(x, y) + q(y) \end{cases}$$

on déduit que cette forme polaire est aussi définie par :

$$\forall (x, y) \in E^2, \varphi(x, y) = \frac{1}{4}(q(x+y) - q(x-y))$$

On notera aussi que pour tout scalaire λ et tout vecteur x , on a :

$$q(\lambda x) = \varphi(\lambda x, \lambda x) = \lambda^2 \varphi(x, x) = \lambda^2 q(x)$$

ce qui se traduit en disant que q est une fonction homogène de degré 2.

Remarque 11.5 *L'application qui associe à une forme quadratique q sa forme polaire φ réalise un isomorphisme d'espaces vectoriels de $Q(E)$ sur l'espace $Bil_s(E)$ des formes bilinéaires symétriques sur E . Pour E de dimension n , $Q(E)$ est de dimension $\frac{n(n+1)}{2}$.*

Remarque 11.6 *De cet isomorphisme, on déduit aussi que deux formes bilinéaires symétriques φ_1 et φ_2 sur E sont égales si, et seulement si, $\varphi_1(x, x) = \varphi_2(x, x)$ pour tout $x \in E$.*

Dans le cas des espaces vectoriels de dimension finie on peut utiliser les matrices pour définir les formes quadratiques.

Définition 11.10 *Soit E un espace vectoriel de dimension n et \mathcal{B} une base de E . Si q est une forme quadratique sur E de forme polaire φ , on dit alors que la matrice de φ dans la base \mathcal{B} est la matrice de q dans cette base.*

En reprenant les notations du paragraphe 11.3, une forme quadratique est définie sur E de base \mathcal{B} par :

$$q(x) = \varphi(x, x) = {}^t X A X = \sum_{1 \leq i, j \leq n} a_{ij} x_i x_j$$

et comme $a_{ij} = a_{ji}$, cela peut s'écrire :

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

Réciproquement une fonction q ainsi définie est une forme quadratique sur E de matrice $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans la base \mathcal{B} .

Le choix d'une base de E permet donc de réaliser un isomorphisme d'espaces vectoriels de $Q(E)$ sur l'espace des polynômes homogènes de degré 2 à n variables.

Exercice 11.10 *Déterminer la matrice et la forme polaire de la forme quadratique q définie dans la base canonique de \mathbb{K}^3 par :*

$$q(x) = x_1^2 + 3x_2^2 + 5x_3^2 + 4x_1x_2 + 6x_1x_3 + 2x_2x_3.$$

Solution 11.10 La matrice de q dans la base canonique est :

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix}$$

et sa forme polaire est définie par :

$$\begin{aligned} \varphi(x, y) &= {}^t X A Y = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \\ &= x_1 y_1 + 3x_2 y_2 + 5x_3 y_3 + 2(x_1 y_2 + x_2 y_1) + 3(x_1 y_3 + y_1 x_3) + x_2 y_3 + x_3 y_2 \end{aligned}$$

Exercice 11.11 Soient ℓ_1, ℓ_2 deux formes linéaires indépendantes sur E .

1. Montrer que l'application q définie sur E par :

$$\forall x \in E, q(x) = \ell_1(x) \ell_2(x)$$

est une forme quadratique et déterminer sa forme polaire.

2. Montrer que q peut s'écrire comme différence de deux carrés de formes linéaires indépendantes.

3. On suppose que $E = \mathbb{K}^n$. Donner la matrice de q dans la base canonique de E .

Solution 11.11

1. L'application φ définie sur E^2 par :

$$\forall x, y \in E, \varphi(x, y) = \frac{1}{2} \ell_1(x) \ell_2(y) + \frac{1}{2} \ell_1(y) \ell_2(x)$$

est bilinéaire symétrique et $q(x) = \varphi(x, x)$ pour tout $x \in E$. Donc q est une forme quadratique de forme polaire φ .

2. On a :

$$q(x) = \frac{1}{4} (\ell_1(x) + \ell_2(x))^2 - \frac{1}{4} (\ell_1(x) - \ell_2(x))^2$$

les formes linéaires $\ell'_1 = \frac{1}{2}(\ell_1 + \ell_2)$ et $\ell'_2 = \frac{1}{2}(\ell_1 - \ell_2)$ étant indépendantes puisque ℓ_1, ℓ_2 le sont. En effet si $\alpha \ell'_1 + \beta \ell'_2 = 0$, on a alors $(\alpha + \beta) \ell_1 + (\alpha - \beta) \ell_2 = 0$, donc $\alpha + \beta = \alpha - \beta = 0$ et $\alpha = \beta = 0$.

3. Pour $E = \mathbb{K}^n$, notons dans la base canonique :

$$\begin{cases} \ell_1(x) = \sum_{j=1}^n \alpha_j x_j \\ \ell_2(x) = \sum_{j=1}^n \beta_j x_j \end{cases}$$

On a alors :

$$\begin{aligned} q(x) &= \left(\sum_{j=1}^n \alpha_j x_j \right) \left(\sum_{j=1}^n \beta_j x_j \right) \\ &= \sum_{1 \leq i, j \leq n} \alpha_i \beta_j x_i x_j = \sum_{i=1}^n \alpha_i \beta_i x_i^2 + \sum_{1 \leq i < j \leq n} (\alpha_i \beta_j + \alpha_j \beta_i) x_i x_j \end{aligned}$$

ce qui signifie que la matrice de q est :

$$A = \frac{1}{2} ((\alpha_i \beta_j + \alpha_j \beta_i))_{1 \leq i, j \leq n} = \frac{1}{2} ({}^t L_1 L_2 + {}^t L_2 L_1)$$

où $L_1 = (\alpha_1 \cdots \alpha_n)$ et $L_2 = (\beta_1 \cdots \beta_n)$ sont les matrices de ℓ_1, ℓ_2 dans la base canonique de \mathbb{K}^n .

On peut aussi écrire, en remarquant que ${}^t(\alpha) = (\alpha)$ pour α réel ou complexe, que :

$$\begin{aligned} \varphi(x, y) &= \frac{1}{2} (\ell_1(x) \ell_2(y) + \ell_1(y) \ell_2(x)) \\ &= \frac{1}{2} ((L_1 X)(L_2 Y) + (L_1 Y)(L_2 X)) \\ &= \frac{1}{2} ({}^t(L_1 X)(L_2 Y) + {}^t(L_2 X)(L_1 Y)) \\ &= \frac{1}{2} (({}^t X {}^t L_1)(L_2 Y) + ({}^t X {}^t L_2)(L_1 Y)) \\ &= \frac{1}{2} ({}^t X ({}^t L_1 L_2 + {}^t L_2 L_1) Y) \end{aligned}$$

et la matrice A de φ , ou de q , est :

$$A = \frac{1}{2} ({}^t L_1 L_2 + {}^t L_2 L_1).$$

Ou encore revenir à la définition de la matrice $A = ((a_{ij}))_{1 \leq i, j \leq n}$ de q dans la base canonique $(e_i)_{1 \leq i \leq n}$:

$$\begin{aligned} a_{ij} = \varphi(e_i, e_j) &= \frac{1}{2} (\ell_1(e_i) \ell_2(e_j) + \ell_1(e_j) \ell_2(e_i)) \\ &= \frac{1}{2} (\alpha_i \beta_j + \alpha_j \beta_i) \end{aligned}$$

Exercice 11.12 Soit L une matrice ligne à n colonnes. Montrer que la matrice $A = {}^t L L$ est une matrice carrée symétrique et que la forme quadratique q de matrice A dans la base canonique de \mathbb{K}^n est le carré d'une forme linéaire.

Solution 11.12 Si $L = (\alpha_1 \ \alpha_2 \ \cdots \ \alpha_n)$, on a alors :

$$A = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} (\alpha_1 \ \alpha_2 \ \cdots \ \alpha_n) = ((\alpha_i \alpha_j))_{1 \leq i, j \leq n}$$

ce qui définit bien une matrice symétrique d'ordre n .

La forme quadratique q de matrice A est alors définie par :

$$q(x) = {}^t X A X = {}^t X ({}^t L L) X = {}^t (L X) (L X) = (L X)^2$$

avec $L X = \ell(x)$ où ℓ est la forme linéaire de matrice L dans la base canonique de \mathbb{K}^n . On a donc $q = \ell^2$.

Exercice 11.13 Soient p un entier naturel non nul, ℓ_1, \dots, ℓ_p des formes linéaires sur E et $\lambda_1, \dots, \lambda_p$ des scalaires. Montrer que l'application q définie sur E par :

$$\forall x \in E, q(x) = \sum_{j=1}^p \alpha_j \ell_j^2(x)$$

est une forme quadratique et déterminer sa forme polaire.

Solution 11.13 L'application φ définie sur E^2 par :

$$\forall x \in E^2, \varphi(x, y) = \sum_{j=1}^p \alpha_j \ell_j(x) \ell_j(y)$$

est bilinéaire symétrique et $q(x) = \varphi(x, x)$ pour tout $x \in E$.

Nous allons voir que sur un espace de dimension finie toute forme quadratique peut se mettre sous la forme indiquée par l'exercice précédent.

L'utilisation des dérivées partielles peut être intéressante pour déterminer rapidement la forme polaire d'une forme quadratique sur \mathbb{R}^n .

Exercice 11.14 Montrer que si q est une forme quadratique sur \mathbb{R}^n , alors sa forme polaire φ est donnée par :

$$\varphi(x, y) = \frac{1}{2} \sum_{j=1}^n \frac{\partial q}{\partial x_j}(x) y_j = \frac{1}{2} \sum_{i=1}^n \frac{\partial q}{\partial y_i}(y) x_i$$

Solution 11.14 En notant $A = ((a_{ij}))_{1 \leq i, j \leq n}$ la matrice de q dans la base canonique, on a :

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

et la forme polaire de q est définie par :

$$\varphi(x, y) = \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j.$$

Pour tout entier k compris entre 1 et n , on a alors :

$$\begin{aligned} \frac{\partial q}{\partial x_k}(x) &= \frac{\partial}{\partial x_k} \left(\sum_{i=1}^n x_i \sum_{j=1}^n a_{ij} x_j \right) = \sum_{i=1}^n \frac{\partial}{\partial x_k} \left(x_i \sum_{j=1}^n a_{ij} x_j \right) \\ &= \frac{\partial}{\partial x_k} \left(x_k \sum_{j=1}^n a_{kj} x_j \right) + \sum_{\substack{i=1 \\ i \neq k}}^n \frac{\partial}{\partial x_k} \left(x_i \sum_{j=1}^n a_{ij} x_j \right) \\ &= \sum_{j=1}^n a_{kj} x_j + x_k a_{kk} + \sum_{\substack{i=1 \\ i \neq k}}^n x_i a_{ik} = \sum_{j=1}^n a_{kj} x_j + \sum_{i=1}^n a_{ik} x_i \\ &= \sum_{j=1}^n a_{jk} x_j + \sum_{i=1}^n a_{ki} x_i = 2 \sum_{i=1}^n a_{ik} x_i \end{aligned}$$

(les égalités $a_{kj} = a_{jk}$ sont justifiées par la symétrie de la matrice A). On en déduit alors que :

$$\begin{aligned}\varphi(x, y) &= \sum_{1 \leq i, j \leq n} a_{ij} x_i y_j = \sum_{j=1}^n \left(\sum_{i=1}^n a_{ij} x_i \right) y_j \\ &= \frac{1}{2} \sum_{j=1}^n \frac{\partial q}{\partial x_j}(x) y_j\end{aligned}$$

Par symétrie, on a la deuxième formule.

Par exemple, la forme polaire de la forme quadratique q définie dans la base canonique de \mathbb{R}^3 par :

$$q(x) = x_1^2 + 3x_2^2 + 5x_3^2 + 4x_1x_2 + 6x_1x_3 + 2x_2x_3.$$

est donnée par :

$$\begin{aligned}\varphi(x, y) &= \frac{1}{2} ((2x_1 + 4x_2 + 6x_3) y_1 + (4x_1 + 6x_2 + 2x_3) y_2 + (10x_3 + 6x_1 + 2x_2) y_3) \\ &= (x_1 + 2x_2 + 3x_3) y_1 + (2x_1 + 3x_2 + x_3) y_2 + (5x_3 + 3x_1 + x_2) y_3\end{aligned}$$

qui est bien le résultat obtenu à l'exercice 11.10.

11.5 Théorème de réduction de Gauss

11.5.1 Cas des espaces de dimension 2

On désigne par E un \mathbb{K} -espace vectoriel de dimension 2, $\mathcal{B} = (e_1, e_2)$ une base de E et pour tout vecteur v de E , on note x, y les coordonnées de v dans cette base, soit $v = xe_1 + ye_2$.

Dans cette base, une forme quadratique q s'écrit sous la forme :

$$q(v) = ax^2 + 2bxy + cy^2$$

La matrice de cette forme quadratique dans la base \mathcal{B} est donc :

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

On suppose que $q \neq 0$, soit $(a, bc) \neq (0, 0, 0)$.

— Si $a \neq 0$, on a :

$$q(v) = a \left(x + \frac{b}{a} y \right)^2 + \frac{\delta}{a} y^2$$

où $\delta = ac - b^2$ est le déterminant de A . Il y a alors deux possibilités :

— soit $\delta = 0$ et :

$$q(v) = a \left(x + \frac{b}{a} y \right)^2 = a \ell_1^2(v)$$

où $\ell_1 : v \mapsto x + \frac{b}{a} y$ est une forme linéaire non nulle

— soit $\delta \neq 0$ et :

$$q(v) = a \left(x + \frac{b}{a} y \right)^2 + \frac{\delta}{a} y^2 = a \ell_1^2(v) + \frac{\delta}{a} \ell_2^2(v)$$

où $\ell_1 : v \mapsto x + \frac{b}{a} y$ et $\ell_2 : v \mapsto y$ sont deux formes linéaires indépendantes puisque

$$\begin{vmatrix} 1 & 0 \\ \frac{b}{a} & 1 \end{vmatrix} = 1 \neq 0.$$

— Si $a = 0$ et $c \neq 0$, on a :

$$q(v) = 2bxy + cy^2 = c \left(y + \frac{b}{c}x \right)^2 + \frac{\delta}{c}x^2$$

où $\delta = -b^2$ est encore le déterminant de A et il y a deux possibilités :

— soit $b = 0$ et :

$$q(v) = cy^2 = c\ell_1^2(v)$$

où $\ell_1 : v \mapsto y$ est une forme linéaire non nulle

— soit $b \neq 0$ et :

$$q(v) = c \left(y + \frac{b}{c}x \right)^2 + \frac{\delta}{c}x^2 = a\ell_1^2(v) + \frac{\delta}{a}\ell_2^2(v)$$

où $\ell_1 : v \mapsto y + \frac{b}{c}x$ et $\ell_2 : v \mapsto x$ sont deux formes linéaires indépendantes.

— Si $a = 0$ et $c = 0$, on a alors $b \neq 0$ et :

$$q(x, y) = 2bxy = \frac{b}{2}((x+y)^2 - (x-y)^2) = \frac{b}{2}\ell_1^2(v) - \frac{b}{2}\ell_2^2(v)$$

où $\ell_1 : v \mapsto x + y$ et $\ell_2 : v \mapsto x - y$ sont deux formes linéaires indépendantes puisque

$$\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} = -2 \neq 0.$$

On a donc montré le résultat suivant.

Théorème 11.10 *Toute forme quadratique non nulle q sur \mathbb{K} -espace vectoriel E de dimension 2 peut s'écrire sous la forme $q = \lambda_1 \ell_1^2$ où λ_1 est un scalaire non nul et ℓ_1 une forme linéaire non nulle ou $q = \lambda_1 \ell_1^2 + \lambda_2 \ell_2^2$ où λ_1, λ_2 sont deux scalaires non nuls et ℓ_1, ℓ_2 deux formes linéaires indépendantes.*

Ce résultat se généralise dans le cas des espaces de dimension n comme on le verra au paragraphe suivant. Quand on a trouvé une telle décomposition, on dit qu'on a réduit la forme quadratique, sous-entendu sous forme de combinaison linéaire de carrés de formes linéaires indépendantes.

Si q est une forme quadratique sur $E = \mathbb{R}^2$, on notera $q(x, y)$ pour $q(v)$, où $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$.

Exercice 11.15 *Réduire les formes quadratiques définies sur \mathbb{R}^2 par :*

$$\begin{aligned} q_1(x, y) &= x^2 - 6xy + 5y^2 \\ q_2(x, y) &= xy \end{aligned}$$

Solution 11.15 *On a :*

$$\begin{aligned} q_1(x, y) &= (x - 3y)^2 - 4y^2 \\ q_2(x, y) &= \frac{1}{4}(x + y)^2 - \frac{1}{4}(x - y)^2 \end{aligned}$$

On peut remarquer qu'une telle décomposition n'est pas unique. Par exemple, pour q_2 , on peut aussi écrire :

$$q_2(x, y) = \left(\frac{1}{2}x + \frac{1}{2}y \right)^2 - \left(\frac{1}{2}x - \frac{1}{2}y \right)^2$$

11.5.2 Cas des espaces de dimension $n \geq 1$

Commençons par un exemple.

Exercice 11.16 *En s'inspirant de la méthode exposée au paragraphe précédent, réduire la forme quadratique q définie sur \mathbb{R}^3 par :*

$$q(x) = x_1^2 + x_2^2 + x_3^2 + 2x_1x_3 + 2x_2x_3.$$

Solution 11.16 *On regroupe les termes contenant x_1 pour l'écrire comme le début d'un carré, soit :*

$$x_1^2 + 2x_1x_3 = (x_1 + x_3)^2 - x_3^2$$

ce qui donne :

$$q(x) = (x_1 + x_3)^2 + x_2^2 + 2x_2x_3.$$

On utilise ensuite la méthode développée pour le cas $n = 2$ à la forme q' définie sur \mathbb{R}^2 par $q'(x_2, x_3) = x_2^2 + 2x_2x_3$, soit :

$$q'(x_2, x_3) = (x_2 + x_3)^2 - x_3^2$$

ce qui donne :

$$q(x) = (x_1 + x_3)^2 + (x_2 + x_3)^2 - x_3^2 = \ell_1^2(x) + \ell_2^2(x) - \ell_3^2(x)$$

les formes ℓ_1, ℓ_2 et ℓ_3 étant indépendantes puisque :

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 1 \neq 0.$$

La démonstration du théorème qui suit s'inspire de cette méthode.

Si E est un \mathbb{K} -espace vectoriel de dimension $n \geq 1$, on notera $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E et pour tout vecteur x de E , x_1, \dots, x_n désignent les coordonnées de x dans cette base, soit $x = \sum_{i=1}^n x_i e_i$. On associe toujours à ce vecteur x de E le vecteur colonne $X = (x_i)_{1 \leq i \leq n}$ dans \mathbb{K}^n .

Théorème 11.11 *Pour toute forme quadratique non nulle q sur E , il existe un entier p compris entre 1 et n , des scalaires non nuls $\lambda_1, \dots, \lambda_p$ et des formes linéaires ℓ_1, \dots, ℓ_p indépendantes dans E^* tels que :*

$$\forall x \in E, \quad q(x) = \sum_{j=1}^p \lambda_j \ell_j^2(x)$$

Démonstration. On procède par récurrence sur $n \geq 1$. Pour $n = 1$, il n'y a rien à montrer et pour $n = 2$ c'est fait.

On suppose le résultat acquis au rang $n - 1$ et on se donne une forme quadratique non nulle q définie dans une base \mathcal{B} d'un espace vectoriel E de dimension $n \geq 3$ par :

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

Supposons tout d'abord que cette expression contient au moins un terme carré, c'est-à-dire qu'il existe un indice i compris entre 1 et n tel que $a_{ii} \neq 0$. Quitte à effectuer une permutation

sur les vecteurs de base, on peut supposer que $a_{11} \neq 0$. En regroupant les termes contenant x_1 , on écrit que :

$$\begin{aligned} a_{11}x_1^2 + 2 \sum_{j=2}^n a_{1j}x_1x_j &= a_{11} \left(x_1^2 + 2x_1 \sum_{j=2}^n \frac{a_{1j}}{a_{11}}x_j \right) \\ &= a_{11} \left(\left(x_1 + \sum_{j=2}^n \frac{a_{1j}}{a_{11}}x_j \right)^2 - \left(\sum_{j=2}^n \frac{a_{1j}}{a_{11}}x_j \right)^2 \right) \end{aligned}$$

et :

$$\begin{aligned} q(x) &= a_{11} \left(x_1 + \sum_{j=2}^n \frac{a_{1j}}{a_{11}}x_j \right)^2 + q'(x') \\ &= a_{11}\ell_1^2(x) + q'(x') \end{aligned}$$

où $\ell_1(x) = x_1 + \sum_{j=2}^n \frac{a_{1j}}{a_{11}}x_j$, q' est une forme quadratique définie sur le sous espace vectoriel H

de E engendré par e_2, \dots, e_n et $x' = \sum_{i=2}^n x_i e_i$ si $x = \sum_{i=1}^n x_i e_i$.

Si $q' = 0$, on a alors $q = a_{11}\ell_1^2$ avec a_{11} et ℓ_1 non nuls.

Si $q' \neq 0$, l'hypothèse de récurrence nous dit qu'il existe un entier p compris entre 2 et n , des scalaires non nuls $\lambda_2, \dots, \lambda_p$ et des formes linéaires indépendantes ℓ_2, \dots, ℓ_p définies sur H tels que :

$$\forall x' \in H, q'(x') = \sum_{j=2}^p \lambda_j \ell_j^2(x')$$

et en prolongeant les formes linéaires ℓ_2, \dots, ℓ_p à E (en posant $\ell_j(x) = \ell_j(x')$), on a :

$$q(x) = a_{11}\ell_1^2(x) + \sum_{j=2}^p \lambda_j \ell_j^2(x)$$

ce qui donne une décomposition de q comme combinaison linéaire de carrés de formes linéaires.

Il reste à vérifier que les formes $\ell_1, \ell_2, \dots, \ell_p$ sont linéairement indépendantes dans E^* .

L'égalité $\sum_{j=1}^p \lambda_j \ell_j$ équivaut à dire que $\sum_{j=1}^p \lambda_j \ell_j(x) = 0$ pour tout $x \in E$. Prenant $x = e_1$, on

a $\ell_1(x) = 1$ et $\ell_j(x) = 0$ pour j compris entre 2 et p , ce qui donne $\lambda_1 = 0$ et $\sum_{j=2}^p \lambda_j \ell_j(x') = 0$

pour tout $x' \in H$, ce qui équivaut à $\sum_{j=2}^p \lambda_j \ell_j = 0$ et la nullité de tous les λ_j puisque le système (ℓ_2, \dots, ℓ_p) est libre dans H^* . On a donc le résultat annoncé.

Il reste enfin à traiter le cas où q est sans facteurs carrés, c'est-à-dire le cas où tous les coefficients a_{ii} sont nuls. Comme q est non nulle, il existe deux indices $i < j$ tels que $a_{ij} \neq 0$. Quitte à effectuer une permutation sur les vecteurs de base, on peut supposer que $a_{12} \neq 0$. On regroupe alors dans l'expression de q tous les termes contenant x_1 et x_2 que l'on fait apparaître comme fragment d'un produit de deux formes linéaires, soit :

$$\begin{aligned} Q &= a_{12}x_1x_2 + x_1 \sum_{j=3}^n a_{1j}x_j + x_2 \sum_{j=3}^n a_{2j}x_j \\ &= \left(a_{12}x_1 + \sum_{j=3}^n a_{2j}x_j \right) \left(x_2 + \sum_{j=3}^n \frac{a_{1j}}{a_{12}}x_j \right) - \left(\sum_{j=3}^n a_{2j}x_j \right) \left(\sum_{j=3}^n \frac{a_{1j}}{a_{12}}x_j \right) \end{aligned}$$

ce qui donne :

$$\begin{aligned} q(x) &= 2 \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j \\ &= 2Q + 2 \sum_{3 \leq i < j \leq n} a_{ij} x_i x_j \\ &= 2L_1(x) L_2(x) + q'(x') \end{aligned}$$

où $L_1(x) = a_{12}x_1 + \sum_{j=3}^n a_{2j}x_j$, $L_2(x) = x_2 + \sum_{j=3}^n \frac{a_{1j}}{a_{12}}x_j$ et q' est une forme quadratique définie sur le sous espace vectoriel H de E engendré par e_3, \dots, e_n et $x' = \sum_{i=3}^n x_i e_i$ si $x = \sum_{i=1}^n x_i e_i$.

En écrivant que :

$$\begin{aligned} 2L_1(x) L_2(x) &= \frac{1}{2} (L_1(x) + L_2(x))^2 - \frac{1}{2} (L_1(x) - L_2(x))^2 \\ &= \frac{1}{2} \ell_1^2(x) - \frac{1}{2} \ell_2^2(x), \end{aligned}$$

on a :

$$q(x) = \frac{1}{2} \ell_1^2(x) - \frac{1}{2} \ell_2^2(x) + q'(x')$$

Si $q' = 0$, on a alors $q = \frac{1}{2} \ell_1^2 - \frac{1}{2} \ell_2^2$, les formes linéaires ℓ_1 et ℓ_2 étant indépendantes puisque la matrice :

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = \begin{pmatrix} a_{12} & 1 & \alpha_{13} & \dots & \alpha_{1n} \\ a_{12} & -1 & \alpha_{23} & \dots & \alpha_{2n} \end{pmatrix}$$

est de rang 2 car le déterminant extrait $\begin{vmatrix} a_{12} & 1 \\ a_{12} & -1 \end{vmatrix} = -2a_{12}$ est non nul.

Si $q' \neq 0$, l'hypothèse de récurrence nous dit qu'il existe un entier p compris entre 3 et n , des scalaires non nuls $\lambda_3, \dots, \lambda_p$ et des formes linéaires indépendantes ℓ_3, \dots, ℓ_p définies sur H tels que :

$$\forall x' \in H, q'(x') = \sum_{j=3}^p \lambda_j \ell_j^2(x')$$

et en prolongeant les formes linéaires ℓ_3, \dots, ℓ_n à E , on a :

$$q(x) = \frac{1}{2} \ell_1^2(x) - \frac{1}{2} \ell_2^2(x) + \sum_{j=3}^p \lambda_j \ell_j^2(x)$$

ce qui donne une décomposition de q comme combinaison linéaire de carrés de formes linéaires.

Il reste à vérifier que les formes $\ell_1, \ell_2, \dots, \ell_p$ sont linéairement indépendantes dans E^* .

L'égalité $\sum_{j=1}^p \lambda_j \ell_j$ équivaut à dire que $\sum_{j=1}^p \lambda_j \ell_j(x) = 0$ pour tout $x \in E$. Prenant $x = e_1$ et $x = e_2$, on obtient $\lambda_1 a_{12} + \lambda_2 a_{21} = 0$ et $\lambda_1 - \lambda_2 = 0$, ce qui équivaut à $\lambda_1 = \lambda_2 = 0$ puisque $a_{21} \neq 0$ et $\sum_{j=3}^p \lambda_j \ell_j(x') = 0$ pour tout $x' \in H$, ce qui équivaut à $\sum_{j=3}^p \lambda_j \ell_j = 0$ et la nullité de tous les λ_j puisque le système (ℓ_3, \dots, ℓ_p) est libre dans H^* . On a donc le résultat annoncé. ■

On peut remarquer que cette démonstration est constructive, c'est-à-dire qu'elle fournit un algorithme permettant d'obtenir une réduction en combinaison linéaire de carrés.

Une telle décomposition est appelée réduction de Gauss, ou plus simplement réduction, de la forme quadratique q .

Exercice 11.17 Réduire la forme quadratique définie sur \mathbb{R}^3 par :

$$q(x) = x_1^2 + 3x_2^2 + 5x_3^2 + 4x_1x_2 + 6x_1x_3 + 2x_2x_3.$$

Solution 11.17 On a :

$$\begin{aligned} q(x) &= (x_1 + 2x_2 + 3x_3)^2 - x_2^2 - 4x_3^2 - 10x_2x_3 \\ &= (x_1 + 2x_2 + 3x_3)^2 - (x_2 + 5x_3)^2 + 21x_3^2 \end{aligned}$$

Exercice 11.18 Réduire la forme quadratique définie sur \mathbb{R}^3 par :

$$q(x) = x_1x_2 + 2x_1x_3 + 2x_1x_4 + x_2x_3 + 4x_2x_4 + 2x_3x_4$$

Solution 11.18 On a :

$$\begin{aligned} q(x) &= x_1x_2 + 2x_1x_3 + 2x_1x_4 + x_2x_3 + 4x_2x_4 + 2x_3x_4 \\ &= (x_1 + x_3 + 4x_4)(x_2 + 2x_3 + 2x_4) - 2x_3^2 - 8x_4^2 - 8x_3x_4 \\ &= (x_1 + x_3 + 4x_4)(x_2 + 2x_3 + 2x_4) - 2(x_3 + 2x_4)^2 \\ &= \frac{1}{4}(x_1 + x_2 + 3x_3 + 6x_4)^2 - \frac{1}{4}(x_1 - x_2 - x_3 + 2x_4)^2 - 2(x_3 + 2x_4)^2 \end{aligned}$$

Exercice 11.19 Soit q la forme quadratique définie sur \mathbb{R}^n par :

$$q(x) = \sum_{i=1}^n x_i^2 + \sum_{1 \leq i < j \leq n} x_i x_j.$$

1. Donner la matrice de q dans la base canonique de \mathbb{R}^n .
2. Réduire q dans les cas $n = 2$, $n = 3$ et $n = 4$.

Solution 11.19

1. On a :

$$A = \frac{1}{2} \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \ddots & 1 \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{pmatrix}$$

- 2.

(a) Pour $n = 2$, on a :

$$q(x) = x_1^2 + x_2^2 + x_1x_2 = \left(x_1 + \frac{1}{2}x_2\right)^2 + \frac{3}{4}x_2^2.$$

(b) Pour $n = 3$, on a :

$$\begin{aligned} q(x) &= x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3 \\ &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}(x_2^2 + x_3^2) + \frac{1}{2}x_2x_3 \\ &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}\left(x_2^2 + x_3^2 + \frac{2}{3}x_2x_3\right) \\ &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}\left(x_2 + \frac{1}{3}x_3\right)^2 + \frac{2}{3}x_3^2 \end{aligned}$$

(c) Pour $n = 4$, on a :

$$\begin{aligned}
 q(x) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
 &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}(x_2^2 + x_3^2) + \frac{1}{2}x_2x_3 \\
 &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}\left(x_2^2 + x_3^2 + \frac{2}{3}x_2x_3\right) \\
 &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 + \frac{1}{2}x_4\right)^2 + \frac{3}{4}\left(x_2 + \frac{1}{3}x_3 + \frac{1}{3}x_4\right)^2 \\
 &\quad + \frac{2}{3}\left(x_3 + \frac{1}{4}x_4\right)^2 + \frac{5}{8}x_4^2
 \end{aligned}$$

Exercice 11.20 On considère à nouveau la forme quadratique q définie sur \mathbb{R}^n par :

$$q(x) = \sum_{i=1}^n x_i^2 + \sum_{1 \leq i < j \leq n} x_i x_j$$

avec $n \geq 3$.

1. Écrire q sous la forme :

$$q(x) = \ell_1^2(x) + q_1(x')$$

où ℓ_1 est une forme linéaire sur \mathbb{R}^n et q_1 une forme quadratique sur \mathbb{R}^{n-1} en notant $x' = (x_2, x_3, \dots, x_n)$.

2. Écrire q_1 sous la forme :

$$q_1(x) = \frac{3}{4}\ell_2^2(x) + q_2(x'')$$

où ℓ_2 est une forme linéaire sur \mathbb{R}^{n-1} et q_2 une forme quadratique sur \mathbb{R}^{n-2} en notant $x'' = (x_3, \dots, x_n)$.

3. Montrer que pour tout p compris entre 1 et $n-1$, on peut écrire q sous la forme :

$$q(x) = \ell_1^2(x) + \frac{3}{4}\ell_2^2(x) + \dots + \frac{p+1}{2p}\ell_p^2(x) + \frac{p+2}{2p+2}q_{p+1}(x)$$

avec :

$$\left\{ \begin{array}{l} \ell_1(x) = x_1 + \frac{1}{2} \sum_{j=2}^n x_j \\ \ell_2(x) = x_2 + \frac{1}{3} \sum_{j=3}^n x_j \\ \vdots \\ \ell_p(x) = x_p + \frac{1}{p+1} \sum_{j=p+1}^n x_j \end{array} \right.$$

et :

$$q_{p+1}(x) = \sum_{i=p+1}^n x_i^2 + \frac{2}{p+2} \sum_{p+1 \leq i < j \leq n} x_i x_j$$

4. Réduire q .

Solution 11.20

1. On a :

$$\begin{aligned}
 q(x) &= x_1^2 + x_1 \sum_{j=2}^n x_j + \sum_{i=2}^n x_i^2 + \sum_{2 \leq i < j \leq n} x_i x_j \\
 &= \left(x_1 + \frac{1}{2} \sum_{j=2}^n x_j \right)^2 - \frac{1}{4} \left(\sum_{j=2}^n x_j \right)^2 + \sum_{i=2}^n x_i^2 + \sum_{2 \leq i < j \leq n} x_i x_j \\
 &= \left(x_1 + \frac{1}{2} \sum_{j=2}^n x_j \right)^2 + \frac{3}{4} \sum_{i=2}^n x_i^2 + \frac{1}{2} \sum_{2 \leq i < j \leq n} x_i x_j \\
 &= \ell_1^2(x) + q_1(x')
 \end{aligned}$$

avec :

$$\ell_1(x) = x_1 + \frac{1}{2} \sum_{j=2}^n x_j$$

et :

$$q_1(x') = \frac{3}{4} \sum_{i=2}^n x_i^2 + \frac{1}{2} \sum_{2 \leq i < j \leq n} x_i x_j$$

2. On a :

$$\begin{aligned}
 q_1(x') &= \frac{3}{4} x_2^2 + \frac{1}{2} x_2 \sum_{j=3}^n x_j + \frac{3}{4} \sum_{i=3}^n x_i^2 + \frac{1}{2} \sum_{3 \leq i < j \leq n} x_i x_j \\
 &= \frac{3}{4} \left(x_2 + \frac{1}{3} \sum_{j=3}^n x_j \right)^2 - \frac{1}{12} \left(\sum_{j=3}^n x_j \right)^2 + \frac{3}{4} \sum_{i=3}^n x_i^2 + \frac{1}{2} \sum_{3 \leq i < j \leq n} x_i x_j \\
 &= \frac{3}{4} \left(x_2 + \frac{1}{3} \sum_{j=3}^n x_j \right)^2 + \frac{2}{3} \sum_{i=3}^n x_i^2 + \frac{1}{3} \sum_{3 \leq i < j \leq n} x_i x_j \\
 &= \frac{3}{4} \ell_2^2(x) + q_2(x'')
 \end{aligned}$$

avec :

$$\ell_2(x) = x_2 + \frac{1}{3} \sum_{j=3}^n x_j$$

et :

$$q_2(x'') = \frac{2}{3} \sum_{i=3}^n x_i^2 + \frac{1}{3} \sum_{3 \leq i < j \leq n} x_i x_j$$

3. Le résultat est vrai pour $p = 1$. Supposons le acquis pour p compris entre 1 et $n - 2$. On a alors :

$$\begin{aligned}
 q_{p+1}(x) &= \sum_{i=p+1}^n x_i^2 + \frac{2}{p+2} \sum_{p+1 \leq i < j \leq n} x_i x_j \\
 &= x_{p+1}^2 + \frac{2}{p+2} x_{p+1} \sum_{j=p+2}^n x_j + \sum_{i=p+2}^n x_i^2 + \frac{2}{p+2} \sum_{p+2 \leq i < j \leq n} x_i x_j \\
 &= \left(x_{p+1} + \frac{1}{p+2} \sum_{j=p+2}^n x_j \right)^2 - \frac{1}{(p+2)^2} \left(\sum_{j=p+2}^n x_j \right)^2 \\
 &\quad + \sum_{i=p+2}^n x_i^2 + \frac{2}{p+2} \sum_{p+2 \leq i < j \leq n} x_i x_j \\
 &= \ell_{p+1}^2(x) + Q_{p+2}(x)
 \end{aligned}$$

avec :

$$\ell_{p+1}(x) = x_{p+1} + \frac{1}{p+2} \sum_{j=p+2}^n x_j$$

et :

$$\begin{aligned}
 Q_{p+2}(x) &= \left(1 - \frac{1}{(p+2)^2} \right) \sum_{i=p+2}^n x_i^2 + \frac{2}{p+2} \left(1 - \frac{1}{p+2} \right) \sum_{p+2 \leq i < j \leq n} x_i x_j \\
 &= \frac{(p+1)(p+3)}{(p+2)^2} \sum_{i=p+2}^n x_i^2 + \frac{2(p+1)}{(p+2)^2} \sum_{p+2 \leq i < j \leq n} x_i x_j \\
 &= \frac{(p+1)(p+3)}{(p+2)^2} \left(\sum_{i=p+2}^n x_i^2 + \frac{2}{p+3} \sum_{p+2 \leq i < j \leq n} x_i x_j \right) \\
 &= \frac{(p+1)(p+3)}{(p+2)^2} q_{p+2}(x)
 \end{aligned}$$

Ce qui donne :

$$\begin{aligned}
 q(x) &= \ell_1^2(x) + \frac{3}{4} \ell_2^2(x) + \cdots + \frac{p+1}{2p} \ell_p^2(x) + \frac{p+2}{2p+2} \ell_{p+1}^2(x) \\
 &\quad + \frac{p+2}{2p+2} Q_{p+2}(x) \\
 &= \ell_1^2(x) + \frac{3}{4} \ell_2^2(x) + \cdots + \frac{p+1}{2p} \ell_p^2(x) + \frac{p+2}{2p+2} \ell_{p+1}^2(x) \\
 &\quad + \frac{p+2}{2p+2} \frac{(p+1)(p+3)}{(p+2)^2} q_{p+2}(x) \\
 &= \ell_1^2(x) + \frac{3}{4} \ell_2^2(x) + \cdots + \frac{p+1}{2p} \ell_p^2(x) + \frac{p+2}{2p+2} \ell_{p+1}^2(x) \\
 &\quad + \frac{p+3}{2p+4} q_{p+2}(x)
 \end{aligned}$$

soit le résultat au rang $p + 1$.

4. Faisant $p = n - 1$, on a :

$$q(x) = \ell_1^2(x) + \frac{3}{4}\ell_2^2(x) + \cdots + \frac{n}{2(n-1)}\ell_{n-1}^2(x) + \frac{n+1}{2n}q_n(x)$$

avec $q_n(x) = x_n^2 = \ell_n^2(x)$, soit :

$$q(x) = \sum_{p=1}^n \frac{p+1}{2p} \ell_p^2(x)$$

avec :

$$\ell_p(x) = x_p + \frac{1}{p+1} \sum_{j=p+1}^n x_j$$

pour p compris entre 1 et n (pour $p = n$, la somme $\sum_{j=p+1}^n$ est nulle).

Le théorème 11.11 nous fournit aussi une expression intéressante de la forme polaire de la forme quadratique q comme nous allons le voir avec le théorème qui suit.

Pour la suite de ce paragraphe, q désigne une forme quadratique non nulle sur E et $q = \sum_{j=1}^p \lambda_j \ell_j^2$ une réduction de Gauss de cette forme quadratique où p est un entier compris entre 1 et n , $\lambda_1, \dots, \lambda_p$ sont des scalaires non nuls et ℓ_1, \dots, ℓ_p des formes linéaires indépendantes.

On notera φ la forme polaire de q .

Théorème 11.12 Avec les notations qui précèdent, la forme polaire φ de q est alors définie par :

$$\forall (x, y) \in E \times E, \varphi(x, y) = \sum_{j=1}^p \lambda_j \ell_j(x) \ell_j(y)$$

Démonstration. Il est clair que φ est une forme bilinéaire symétrique sur E et pour tout $x \in E$, on a $\varphi(x, x) = \sum_{j=1}^p \lambda_j \ell_j^2(x) = q(x)$, ce qui signifie que φ est la forme polaire de q . ■

Les formes linéaires ℓ_1, \dots, ℓ_p étant linéairement indépendantes dans l'espace vectoriel $E^* = \mathcal{L}(E, \mathbb{K})$ des formes linéaires sur E , elles peuvent se compléter en une base de cet espace (qui on le sait est de dimension n), c'est-à-dire qu'il existe des formes linéaires $\ell_{p+1}, \dots, \ell_n$ (dans le cas où $p \leq n - 1$) telles que (ℓ_1, \dots, ℓ_n) soit une base de E^* .

La réduction de Gauss du théorème 11.11 peut alors s'écrire :

$$\forall x \in E, q(x) = \sum_{j=1}^n \lambda_j \ell_j^2(x)$$

où on a posé $\lambda_{p+1} = \dots = \lambda_n = 0$ dans le cas où $p \leq n - 1$.

Théorème 11.13 Étant donnée une base $(\ell_i)_{1 \leq i \leq n}$ de l'espace vectoriel E^* des formes linéaires sur E , il existe une base $(f_i)_{1 \leq i \leq n}$ de E telle que :

$$\ell_i(f_j) = \delta_{ij} \quad (1 \leq i, j \leq n)$$

où les δ_{ij} sont définis par :

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

(symboles de Kronecker).

Démonstration. En notant, pour tout entier i compris entre 1 et n et tout vecteur $x \in E$:

$$\ell_i(x) = \alpha_{i1}x_1 + \cdots + \alpha_{in}x_n$$

l'expression de ℓ_i dans la base $\mathcal{B} = (e_i)_{1 \leq i \leq n}$, la matrice $Q = ((\alpha_{ij}))_{1 \leq i, j \leq n}$ est inversible puisque les ℓ_i forment une base de E^* (la ligne i de Q est la matrice de ℓ_i dans la base \mathcal{B}). En notant F_1, \dots, F_n les colonnes de la matrice Q^{-1} , l'égalité $QQ^{-1} = I_n$ s'écrit :

$$Q(F_1, \dots, F_n) = (QF_1, \dots, QF_n) = (E_1, \dots, E_n)$$

où $(E_i)_{1 \leq i \leq n}$ est la base canonique de \mathbb{K}^n . On a donc, pour tout entier j compris entre 1 et n :

$$QF_j = E_j$$

En remarquant que pour tout $x \in E$, on a :

$$QX = \begin{pmatrix} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n \\ \vdots \\ \alpha_{n1}x_1 + \cdots + \alpha_{nn}x_n \end{pmatrix} = \begin{pmatrix} \ell_1(x) \\ \vdots \\ \ell_n(x) \end{pmatrix}$$

et en désignant par f_j le vecteur de E de composantes F_j dans la base \mathcal{B} , les égalités $QF_j = E_j$ se traduisent par :

$$\begin{pmatrix} \ell_1(f_j) \\ \vdots \\ \ell_n(f_j) \end{pmatrix} = E_j = \begin{pmatrix} \delta_{1j} \\ \vdots \\ \delta_{nj} \end{pmatrix}$$

et on a bien $\ell_i(f_j) = \delta_{ij}$ pour tous i, j compris entre 1 et n . ■

Dans la situation du théorème précédent, on dit que $(\ell_i)_{1 \leq i \leq n}$ est la base duale de $(f_i)_{1 \leq i \leq n}$ ou que $(f_i)_{1 \leq i \leq n}$ est la base anté-duale de $(\ell_i)_{1 \leq i \leq n}$.

Le théorème de réduction de Gauss peut alors se traduire matriciellement comme suit.

Théorème 11.14 Avec les notations qui précèdent, il existe une base $(f_i)_{1 \leq i \leq n}$ de E dans laquelle la matrice de q est diagonale de la forme :

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

(les p premiers λ_i sont non nuls et les suivants sont nuls).

Démonstration. Partant de la réduction de Gauss $q = \sum_{j=1}^p \lambda_j \ell_j^2$ avec $1 \leq p \leq n$ et les λ_i tous non nuls, on complète (ℓ_1, \dots, ℓ_p) en une base $(\ell_i)_{1 \leq i \leq n}$ de E^* et on construit une base $(f_i)_{1 \leq i \leq n}$ de E telle que $\ell_i(f_j) = \delta_{ij}$ pour tous i, j compris entre 1 et n .

En posant $\lambda_{p+1} = \cdots = \lambda_n = 0$ dans le cas où $p \leq n-1$, la forme polaire φ de q est définie par $\varphi(x, y) = \sum_{k=1}^n \lambda_k \ell_k(x) \ell_k(y)$ et pour i, j compris entre 1 et n , on a :

$$\varphi(f_i, f_j) = \sum_{k=1}^n \lambda_k \ell_k(f_i) \ell_k(f_j) = \lambda_i \ell_i(f_j) = \begin{cases} \lambda_i & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

ce qui donne le résultat annoncé. ■

Une telle base $(f_i)_{1 \leq i \leq n}$ est dite orthogonale pour la forme quadratique q (cette définition sera précisée un peu plus loin).

Comme une matrice symétrique définit une unique forme quadratique dans la base canonique de $E = \mathbb{K}^n$, on déduit de tout ce qui précède, en utilisant la formule de changement de base pour les formes quadratiques, le corollaire qui suit.

Corollaire 11.1 *Si A est une matrice symétrique d'ordre n à coefficients dans \mathbb{K} , il existe alors une matrice inversible P telle que la matrice tPAP soit diagonale.*

Démonstration. En gardant toujours les mêmes notations, la matrice $P = Q^{-1}$ de colonnes f_1, \dots, f_n est la matrice de passage de la base canonique de \mathbb{K}^n à la base $(f_i)_{1 \leq i \leq n}$ et la matrice D de q dans cette base est diagonale et s'écrit $D = {}^tPAP$. ■

Avec l'exercice qui suit nous résumons sur un exemple une première méthode permettant d'obtenir une base orthogonale pour q . Nous verrons un peu plus loin comment faire l'économie du calcul des formes linéaires complétant (ℓ_1, \dots, ℓ_p) en une base de E^* .

Exercice 11.21 Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$.

1. Déterminer la forme quadratique q sur \mathbb{R}^3 (ou \mathbb{C}^3) ayant pour matrice A dans la base canonique.
2. Déterminer deux formes linéaires indépendantes ℓ_1 et ℓ_2 telles que $q = \ell_1^2 - \ell_2^2$.
3. Déterminer une forme linéaire ℓ_3 (aussi simple que possible) telle que (ℓ_1, ℓ_2, ℓ_3) soit une base $\mathcal{L}(\mathbb{R}^3, \mathbb{R})$.
4. Déterminer une base (f_1, f_2, f_3) de \mathbb{R}^3 telle que $\ell_i(f_j) = \delta_{ij}$ pour tous i, j compris entre 1 et 3.
5. Déterminer une base de \mathbb{R}^3 orthogonale pour q et une matrice inversible P telle que $D = {}^tPAP$ soit diagonale.

Solution 11.21 On note x, y, z les coordonnées d'un vecteur v de \mathbb{R}^3 et $q(x, y, z)$ pour $q(v)$.

1. La forme q est définie par :

$$q(x, y, z) = x^2 + 3y^2 + 5z^2 + 2(2xy + 3xz + 4yz).$$

2. On a la réduction de Gauss $q = \ell_1^2 - \ell_2^2$ avec :

$$\begin{cases} \ell_1(x, y, z) = x + 2y + 3z \\ \ell_2(x, y, z) = y + 2z \end{cases}$$

3. On peut prendre ℓ_3 définie par :

$$\ell_3(x, y, z) = z$$

(ℓ_1, ℓ_2, ℓ_3) est bien une base $\mathcal{L}(\mathbb{R}^3, \mathbb{R})$ puisque :

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{vmatrix} = 1 \neq 0$$

4. Il s'agit d'inverser la matrice :

$$Q = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Pour ce faire on résout le système :

$$\begin{cases} x + 2y + 3z = x' \\ y + 2z = y' \\ z = z' \end{cases}$$

ce qui donne :

$$\begin{cases} x = x' - 2y' + z' \\ y = y' - 2z' \\ z' = z \end{cases}$$

et f_1, f_2, f_3 sont les colonnes de :

$$P = Q^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

5. La base (f_1, f_2, f_3) est alors orthogonale pour q , ce qui signifie que la matrice de q dans cette base est diagonale. Précisément, on a :

$$D = {}^tPAP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

ce qui peut aussi se vérifier par le calcul :

$${}^tPAP = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Exercice 11.22 Soit q la forme quadratique définie sur \mathbb{R}^n par :

$$q(x) = x_1^2 + 2 \sum_{i=2}^{n-1} x_i^2 + 2 \sum_{1 \leq i < j \leq n} x_i x_j$$

avec $n \geq 3$.

1. Donner la matrice de q dans la base canonique de \mathbb{R}^n .
2. Réduire q dans le cas $n = 3$.
3. Déterminer une base orthogonale pour q dans le cas $n = 3$.
4. Traiter le cas général.

Solution 11.22

1. On a :

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \cdots & 1 & 2 & 1 \\ 1 & \cdots & 1 & 1 & 0 \end{pmatrix}$$

2. Pour $n = 3$, on a :

$$\begin{aligned} q(x) &= x_1^2 + 2x_2^2 + 2(x_1x_2 + x_1x_3 + x_2x_3) \\ &= (x_1 + x_2 + x_3)^2 + x_2^2 - x_3^2 \\ &= \ell_1^2(x) + \ell_2^2(x) - \ell_3^2(x) \end{aligned}$$

avec :

$$\begin{cases} \ell_1(x) = x_1 + x_2 + x_3 \\ \ell_2(x) = x_2 \\ \ell_3(x) = x_3 \end{cases}$$

formes linéaires indépendantes.

3. On résout le système :

$$\begin{cases} x_1 + x_2 + x_3 = y_1 \\ x_2 = y_2 \\ x_3 = y_3 \end{cases}$$

ce qui donne :

$$\begin{cases} x_1 = y_1 - y_2 - y_3 \\ x_2 = y_2 \\ x_3 = y_3 \end{cases}$$

et :

$$f_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, f_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, f_3 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

pour base q -orthogonale. La matrice de q dans cette base est :

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

4. Pour $n \geq 3$, on a :

$$\begin{aligned} q(x) &= x_1^2 + 2 \sum_{i=2}^{n-1} x_i^2 + 2 \sum_{1 \leq i < j \leq n} x_i x_j \\ &= \left(\sum_{i=1}^n x_i \right)^2 - \left(\sum_{i=2}^n x_i \right)^2 + 2 \sum_{i=2}^{n-1} x_i^2 + 2 \sum_{2 \leq i < j \leq n} x_i x_j \\ &= \ell_1^2(x) + \sum_{i=2}^{n-1} x_i^2 - x_n^2 = \sum_{i=1}^{n-1} \ell_i^2(x) - \ell_n^2(x) \end{aligned}$$

avec :

$$\begin{cases} \ell_1(x) = \sum_{i=1}^n x_i \\ \ell_i(x) = x_i \quad (2 \leq i \leq n) \end{cases}$$

formes linéaires indépendantes.

Pour trouver une base q -orthogonale, on résout le système :

$$\begin{cases} \sum_{i=1}^n x_i = y_1 \\ x_i = y_i \quad (2 \leq i \leq n) \end{cases}$$

ce qui donne :

$$\begin{cases} x_1 = y_1 - \sum_{i=2}^n y_i \\ x_i = y_i \quad (2 \leq i \leq n) \end{cases}$$

et :

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

est la matrice de passage de la base canonique $(e_i)_{1 \leq i \leq n}$ à une base q -orthogonale $(f_i)_{1 \leq i \leq n}$.
On a donc :

$$\begin{cases} f_1 = e_1 \\ f_i = e_i - e_1 \quad (2 \leq i \leq n) \end{cases}$$

et la matrice de q dans la base $(f_i)_{1 \leq i \leq n}$ est :

$$D = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & -1 \end{pmatrix}.$$

Exercice 11.23 Soit q la forme quadratique définie sur \mathbb{R}^3 par :

$$q(x) = x^2 + (1+a)y^2 + (1+a+a^2)z^2 + 2xy - 2ayz$$

1. Donner la matrice A de q dans la base canonique de \mathbb{R}^3 .
2. Calculer le déterminant de A .
3. Pour quelles valeurs de A la forme q est-elle non dégénérée ?
4. Réduire q et donner son rang et sa signature en fonction de a .
5. Déterminer une base orthogonale pour q .
6. En déduire une matrice inversible P telle que $D = {}^tPAP$ soit diagonale.

Solution 11.23

1. La matrice de q dans la base canonique de \mathbb{R}^3 est :

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1+a & -a \\ 0 & -a & 1+a+a^2 \end{pmatrix}.$$

2. On a :

$$\det(A) = a(1+a^2)$$

3. La forme q est dégénérée si, et seulement si, $a = 0$.

4. On a :

$$q(x) = (x+y)^2 + a(y-z)^2 + (1+a^2)z^2$$

Pour $a = 0$, q est de rang 2 et de signature $(2, 0)$.

Pour $a \neq 0$, q est de rang 3 et de signature $(3, 0)$ pour $a > 0$ et $(2, 1)$ pour $a < 0$.

5. Dans tous les cas, il s'agit de résoudre le système :

$$\begin{cases} x + y = \alpha \\ y - z = \beta \\ z = \gamma \end{cases}$$

Ce système a pour solution :

$$\begin{cases} x = \alpha - \beta - \gamma \\ y = \beta + \gamma \\ z = \gamma \end{cases}$$

ce qui donne pour base q -orthogonale :

$$f_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, f_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, f_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$$

6. La matrice de q dans la base (f_1, f_2, f_3) est :

$$D = {}^tPAP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 + a^2 \end{pmatrix}$$

où :

$$P = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

11.6 Orthogonalité, noyau et rang

Pour ce paragraphe, φ est une forme bilinéaire symétrique sur un espace vectoriel E et q la forme quadratique associée.

Définition 11.11 On dit que deux vecteurs x, y de E sont orthogonaux relativement à φ si $\varphi(x, y) = 0$.

Exemple 11.6 Sur \mathbb{R}^2 ou \mathbb{R}^3 le produit scalaire usuel :

$$(x, y) \mapsto x \cdot y = x_1y_1 + x_2y_2 \text{ ou } (x, y) \mapsto x \cdot y = x_1y_1 + x_2y_2 + x_3y_3$$

définit une forme bilinéaire symétrique et la définition de l'orthogonalité correspond bien à celle étudiée au Lycée.

Définition 11.12 Si X est une partie non vide E , l'orthogonal de X relativement à φ est le sous-ensemble de E formé des vecteurs orthogonaux à tous les vecteurs de X .

L'orthogonal d'une partie non vide X de E est notée X^\perp et on a :

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

Exemple 11.7 Pour $X = \{0\}$, on a $X^\perp = E$.

Les propriétés suivantes se déduisent immédiatement de la définition.

Théorème 11.15 Soient X, Y deux parties non vides de E .

1. X^\perp est un sous-espace vectoriel de E .
2. $X \subset (X^\perp)^\perp$.
3. Si $X \subset Y$, alors $Y^\perp \subset X^\perp$.

Comme, pour toute partie non vide X de E , X^\perp est un sous-espace vectoriel de E , l'inclusion $X \subset (X^\perp)^\perp$ sera stricte pour X non sous-espace vectoriel.

Pour le produit scalaire usuel sur $E = \mathbb{R}^2$, on a $E^\perp = \{0\}$. En effet si $y \in E^\perp$, il est en particulier orthogonal à lui-même, donc $y \cdot y = y_1^2 + y_2^2 = 0$ et $y_1 = y_2 = 0$, soit $y = 0$.

Mais de manière générale un vecteur peut être orthogonal à lui-même sans être nécessairement nul.

Considérons par exemple la forme bilinéaire symétrique φ définie sur \mathbb{R}^2 par :

$$\varphi(x, y) = x_1 y_1 - x_2 y_2$$

Un vecteur x est orthogonal à lui-même si, et seulement si, $x_1^2 - x_2^2 = 0$, ce qui équivaut à $x_2 = \pm x_1$.

Définition 11.13 On dit qu'un vecteur x de E est *isotrope* relativement à φ s'il est orthogonal à lui-même.

Définition 11.14 L'ensemble des vecteurs isotropes de E , relativement à φ , est le *cône isotrope* de φ .

Le cône isotrope de φ est donc le sous-ensemble de E :

$$C_\varphi = \{x \in E \mid \varphi(x, x) = 0\}.$$

On dit aussi que C_φ est le cône isotrope de la forme quadratique q et on le note alors C_q ou $q^{-1}\{0\}$.

Définition 11.15 Le *noyau* de φ est l'orthogonal de E .

En notant $\ker(\varphi)$ le noyau de φ , on a :

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

et ce noyau est un sous-espace vectoriel de E .

On dit aussi que $\ker(\varphi)$ est le noyau de la forme quadratique q et on le note alors $\ker(q)$.

Lemme 11.1 Le noyau de φ est contenu dans son cône isotrope, soit :

$$\ker(\varphi) \subset C_\varphi.$$

Démonstration. Si $x \in \ker(\varphi)$, il est orthogonal à tout vecteur de E et en particulier à lui-même, ce qui signifie qu'il est dans le cône isotrope de φ . ■

Exercice 11.24 Déterminer le noyau et le cône isotrope de la forme bilinéaire symétrique φ définie sur \mathbb{R}^3 par :

$$\varphi(x, y) = x_1 y_1 + x_2 y_2 - x_3 y_3$$

Solution 11.24 Dire que y est dans le noyau de φ signifie que $\varphi(x, y) = 0$ pour tout vecteur x de \mathbb{R}^3 , ce qui équivaut à $\varphi(e_i, y) = 0$ pour chacun des vecteurs de base canonique e_1, e_2, e_3 . Le noyau de φ est donc l'ensemble des solutions du système linéaire :

$$\begin{cases} \varphi(e_1, y) = y_1 = 0 \\ \varphi(e_2, y) = y_2 = 0 \\ \varphi(e_3, y) = -y_3 = 0 \end{cases}$$

soit :

$$\ker(\varphi) = \{0\}.$$

Le cône isotrope de φ est formé des vecteurs x tels que $x_1^2 + x_2^2 - x_3^2 = 0$, et on reconnaît là l'équation d'un cône de \mathbb{R}^3 (figure 11.1).

FIGURE 11.1 – Cône : $x_1^2 + x_2^2 - x_3^2 = 0$

Exercice 11.25 Déterminer le noyau et le cône isotrope de la forme bilinéaire symétrique φ définie sur \mathbb{R}^3 par :

$$\varphi(x, y) = x_1y_1 - x_3y_3$$

Solution 11.25 Dire que y est dans le noyau de φ signifie que $\varphi(x, y) = 0$ pour tout vecteur x de \mathbb{R}^3 , ce qui équivaut à $\varphi(e_i, y) = 0$ pour chacun des vecteurs de base canonique e_1, e_2, e_3 . Le noyau de φ est donc l'ensemble des solutions du système linéaire :

$$\begin{cases} \varphi(e_1, y) = y_1 = 0 \\ \varphi(e_2, y) = 0 = 0 \\ \varphi(e_3, y) = -y_3 = 0 \end{cases}$$

soit :

$$\ker(\varphi) = \left\{ y = \begin{pmatrix} 0 \\ y_2 \\ 0 \end{pmatrix} \mid y_2 \in \mathbb{R} \right\}$$

c'est donc la droite vectorielle dirigée par e_2 .

Le cône isotrope de φ est formé des vecteurs x tels que $x_1^2 - x_3^2 = 0$, soit :

$$C_\varphi = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \end{pmatrix} \mid (x_1, x_2) \in \mathbb{R}^2 \right\} \cup \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ -x_1 \end{pmatrix} \mid (x_1, x_2) \in \mathbb{R}^2 \right\}$$

et il contient bien le noyau. Ce cône isotrope est la réunion de deux plans.

Exercice 11.26 Soient F, G deux sous-espaces vectoriels de E . Montrer que :

$$(F + G)^\perp = F^\perp \cap G^\perp \text{ et } (F \cap G)^\perp \supset F^\perp + G^\perp$$

Solution 11.26 Si $x \in (F + G)^\perp$, on a alors $\varphi(x, y + z) = 0$ pour tous vecteurs $y \in F$ et $z \in G$ et en particulier :

$$\begin{cases} \forall y \in F, \varphi(x, y) = \varphi(x, y + 0) = 0 \\ \forall z \in G, \varphi(x, z) = \varphi(x, 0 + z) = 0 \end{cases}$$

ce qui nous dit que $x \in F^\perp \cap G^\perp$.

Réciproquement si $x \in F^\perp \cap G^\perp$, on a alors $\varphi(x, y) = \varphi(x, z) = 0$ pour tous vecteurs $y \in F$ et $z \in G$ et conséquence $\varphi(x, y + z) = 0$ pour ces vecteurs y, z , ce qui nous dit que $x \in (F + G)^\perp$. Si $x = u + v \in F^\perp + G^\perp$ avec $u \in F^\perp$ et $v \in G^\perp$, on a alors pour tout $y \in F \cap G$:

$$\varphi(x, y) = \varphi(u, y) + \varphi(v, y) = 0$$

et $x \in (F \cap G)^\perp$.

L'égalité $(F \cap G)^\perp = F^\perp + G^\perp$ n'est pas assurée en général. Par exemple pour F, G supplémentaires dans E , on a $F \cap G = \{0\}$ et $(F \cap G)^\perp = \{0\}^\perp = E$ n'est en général pas égal à $F^\perp + G^\perp$.

Dans le cas où E est de dimension finie, en désignant par A la matrice de φ dans une base \mathcal{B} et u l'endomorphisme de E ayant A pour matrice dans cette base, le noyau de φ est égal au noyau de u .

Théorème 11.16 Soient E un espace vectoriel de dimension n , $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base de E , A la matrice de la forme bilinéaire φ dans la base \mathcal{B} et u l'endomorphisme de E de matrice A dans la base \mathcal{B} . On a alors :

$$\ker(\varphi) = \ker(u).$$

Démonstration. Un vecteur x est dans le noyau de φ si, et seulement si, il est orthogonal à tout vecteur de E , ce qui équivaut à dire du fait de la linéarité à droite de φ que x est orthogonal à chacun des vecteurs de la base \mathcal{B} , soit :

$$x \in \ker(\varphi) \Leftrightarrow (\forall i \in \{1, 2, \dots, n\}, \varphi(x, e_i) = 0)$$

ce qui revient à dire les coordonnées x_1, x_2, \dots, x_n de x dans la base \mathcal{B} sont solutions du système linéaire de n équations à n inconnues :

$$\varphi \left(\sum_{j=1}^n x_j e_j, e_i \right) = \sum_{j=1}^n x_j \varphi(e_j, e_i) = \sum_{j=1}^n \varphi(e_i, e_j) x_j = 0 \quad (1 \leq i \leq n)$$

Ce système s'écrit $AX = 0$ où $A = ((\varphi(e_i, e_j)))_{1 \leq i, j \leq n}$ où A est la matrice de φ dans \mathcal{B} et X le vecteur colonne formé des composantes de x dans cette base. Ce système est encore équivalent à $u(x) = 0$, où u l'endomorphisme de E de matrice A dans \mathcal{B} , ce qui revient à dire que $x \in \ker(u)$.

■

On retiendra qu'en dimension finie, le noyau de φ se calcule en résolvant le système $AX = 0$, en utilisant les notations du théorème précédent.

Ce résultat peut aussi se montrer comme suit. Dire que $x \in \ker(\varphi)$ équivaut à dire que $\varphi(y, x) = 0$ pour tout $y \in E$, soit à ${}^tYAX = 0$ pour tout $Y \in \mathbb{R}^n$ et prenant $Y = AX$, on a ${}^t(AX)AX = 0$. Mais pour $Z \in \mathbb{R}^n$, on a ${}^tZZ = \sum_{i=1}^n z_i^2$ et ${}^tZZ = 0$ équivaut à $Z = 0$. Donc $AX = 0$ pour $x \in \ker(\varphi)$. La réciproque est évidente.

Définition 11.16 On dit que la forme bilinéaire symétrique φ (ou de manière équivalente la forme quadratique q) est non dégénérée si son noyau est réduit à $\{0\}$.

Du théorème précédent, on déduit qu'en dimension finie, une forme bilinéaire symétrique est non dégénérée si, et seulement si, sa matrice dans une quelconque base de E est inversible, ce qui équivaut à dire que son déterminant est non nul.

Comme pour les applications linéaires, on peut définir le rang d'une forme quadratique à partir de la dimension de son noyau.

Définition 11.17 Si E est de dimension finie égale à n , le rang de φ (ou de q) est l'entier :

$$\text{rg}(q) = n - \dim(\ker(q)).$$

Du théorème précédent, on déduit qu'en dimension finie le rang d'une forme quadratique est égal à celui de sa matrice dans une quelconque base.

Exercice 11.27 On note $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{R}^n et on désigne par q la forme quadratique définie dans cette base par :

$$q(x) = \sum_{i=1}^n x_i^2 + \sum_{1 \leq i < j \leq n} x_i x_j.$$

1. Déterminer la matrice de q dans la base \mathcal{B} .
2. Déterminer le noyau et le rang de q .
3. On suppose que $n = 2$.
 - (a) Effectuer la décomposition en carrés de Gauss de q .
 - (b) En déduire une base q -orthogonale de \mathbb{R}^2 .
 - (c) Écrire la matrice de q dans cette base.
4. On suppose que $n = 3$.
 - (a) Effectuer la décomposition en carrés de Gauss de q .

(b) En déduire une base q -orthogonale de \mathbb{R}^2 .

(c) Écrire la matrice de q dans cette base.

5. On suppose que $n \geq 4$ et on note $f_1 = e_1$.

(a) Déterminer l'orthogonal relativement à q de e_1 . On notera H cet orthogonal.

(b) Pour tout j compris entre 2 et n , on note $f_j = e_1 + \cdots + e_{j-1} - je_j$.

Montrer que $(f_j)_{2 \leq j \leq n}$ est une base de H .

(c) Calculer Af_j pour tout j compris entre 2 et n .

(d) Montrer que $\mathcal{B}' = (f_j)_{1 \leq j \leq n}$ est une base q -orthogonale de \mathbb{R}^n .

(e) Écrire la matrice de q dans la base \mathcal{B}' .

(f) En déduire une décomposition de q comme combinaison linéaire de carrés de formes linéaires indépendantes.

Solution 11.27

$$1. A = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{2} \\ \frac{1}{2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{1}{2} \\ \frac{1}{2} & \cdots & \frac{1}{2} & 1 \end{pmatrix}.$$

2. $x \in \ker(q) \Leftrightarrow Ax = 0 \Leftrightarrow x_1 + \cdots + x_{j-1} + 2x_j + x_{j+1} + \cdots + x_n = 0$ pour $1 \leq j \leq n$. En ajoutant toutes ces équations on obtient $\sum_{j=1}^n x_j = 0$ qui retranchée à l'équation j donne $x_j = 0$. On a donc $\ker(q) = \{0\}$ et $\text{rang}(q) = n$.

3. Pour $n = 2$, on a :

$$(a) q(x) = x_1^2 + x_2^2 + x_1x_2 = \left(x_1 + \frac{1}{2}x_2\right)^2 + \frac{3}{4}x_2^2.$$

(b) En résolvant le système $\begin{cases} x_1 + \frac{1}{2}x_2 = a \\ x_2 = b \end{cases}$ pour $(a, b) = (1, 0)$ et $(a, b) = (0, 1)$, on

obtient la base q -orthogonale : $f_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $f_2 = \begin{pmatrix} -\frac{1}{2} \\ 1 \end{pmatrix}$.

(c) La matrice de q dans cette base est $D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{3}{4} \end{pmatrix}$.

4. Pour $n = 3$, on a :

(a)

$$\begin{aligned} q(x) &= x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3 \\ &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}\left(x_2^2 + x_3^2 + \frac{2}{3}x_2x_3\right) \\ &= \left(x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3\right)^2 + \frac{3}{4}\left(x_2 + \frac{1}{3}x_3\right)^2 + \frac{2}{3}x_3^2. \end{aligned}$$

(b) En résolvant le système :

$$\begin{cases} x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 = a \\ x_2 + \frac{1}{3}x_3 = b \\ x_3 = c \end{cases}$$

pour $(a, b, c) = (1, 0, 0)$, $(0, 1, 0)$ et $(0, 0, 1)$ on obtient la base q -orthogonale :

$$f_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, f_2 = \begin{pmatrix} -\frac{1}{2} \\ 1 \\ 0 \end{pmatrix}, f_3 = \begin{pmatrix} -\frac{1}{3} \\ -\frac{1}{3} \\ 1 \end{pmatrix}$$

(c) La matrice de q dans cette base est $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{4} & 0 \\ 0 & 0 & \frac{2}{3} \end{pmatrix}$.

5.

(a) $x \in \{e_1\}^\perp \Leftrightarrow \varphi(x, e_1) = 0 \Leftrightarrow {}^t x A e_1 = 0 \Leftrightarrow (x_1, \dots, x_n) \begin{pmatrix} 1 \\ \frac{1}{2} \\ \vdots \\ \frac{1}{2} \end{pmatrix} = 0$. Une équation

de H est donc : $2x_1 + x_2 + \dots + x_n = 0$.

(b) Les coordonnées de f_j dans \mathcal{B} sont données par :

$$x_1 = \dots = x_{j-1} = 1, x_j = -j, x_{j+1} = \dots = x_n = 0$$

et :

$$2x_1 + x_2 + \dots + x_n = 2 + (j-2) - j = 0.$$

Les vecteurs f_j sont bien dans H et ils sont libres, donc forment une base.

$$(c) A f_j = \frac{1}{2} \begin{pmatrix} 2 & 1 & \dots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ \vdots \\ 1 \\ -j \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -j-1 \\ -1 \\ \vdots \\ -1 \end{pmatrix} \leftarrow j$$

(d) Pour $2 \leq i < j$, on a :

$$\varphi(f_i, f_j) = \frac{1}{2} (1, \dots, 1, -i, 0, \dots, 0) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -j-1 \\ -1 \\ \vdots \\ -1 \end{pmatrix} = 0$$

et on sait déjà que f_1 est q -orthogonal aux f_j pour $j \geq 2$.

(e) On a $q(f_j) = \frac{j(j+1)}{2}$ et la matrice de q dans \mathcal{B}' est :

$$D = \frac{1}{2} \begin{pmatrix} 2 & 0 & \cdots & \cdots & 0 \\ 0 & 6 & \ddots & & \vdots \\ \vdots & \ddots & 12 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & n(n+1) \end{pmatrix}$$

(f) L'expression de q dans \mathcal{B}' est :

$$q(x) = \frac{1}{2} \sum_{j=1}^n j(j+1) x_j'^2 = \frac{1}{2} \sum_{j=1}^n j(j+1) \ell_j^2(x)$$

avec $X' = P^{-1}X$ où :

$$P = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & -2 & 1 & & \vdots \\ \vdots & 0 & -3 & \ddots & \vdots \\ \vdots & & \vdots & \ddots & 1 \\ 0 & 0 & 0 & 0 & -n \end{pmatrix}$$

est la matrice de passage de \mathcal{B} à \mathcal{B}' . Pour $n = 5$, on a :

$$P^{-1} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & -\frac{1}{2} & -\frac{1}{6} & -\frac{1}{6} & -\frac{1}{6} \\ 0 & 0 & -\frac{1}{3} & -\frac{1}{12} & -\frac{1}{12} \\ 0 & 0 & 0 & -\frac{1}{4} & -\frac{1}{20} \\ 0 & 0 & 0 & 0 & -\frac{1}{5} \end{pmatrix}$$

et pour $n \geq 4$, la ligne 1 de P^{-1} est :

$$\left(1 \quad \frac{1}{2} \quad \frac{1}{2} \quad \cdots \quad \frac{1}{2} \right)$$

et la ligne $j \geq 2$ est :

$$\left(0, \cdots, 0, -\frac{1}{j}, -\frac{1}{j(j+1)}, \cdots, -\frac{1}{j(j+1)} \right).$$

On a donc :

$$\begin{cases} \ell_1(x) = x_1 + \frac{1}{2}x_2 + \cdots + \frac{1}{2}x_n \\ \ell_j(x) = \frac{1}{j}x_j + \frac{1}{j(j+1)}x_{j+1} + \cdots + \frac{1}{j(j+1)}x_n \\ \ell_n(x) = \frac{1}{n}x_n \end{cases}$$

ou encore :

$$q(x) = \frac{1}{2} \sum_{j=1}^{n-1} \frac{1}{j(j+1)} ((j+1)x_j + x_{j+1} + \cdots + x_n)^2 + \frac{n+1}{2n} x_n^2.$$

En dimension finie la réduction de Gauss d'une forme quadratique nous permet d'obtenir son rang et son noyau.

Pour la suite de ce paragraphe, q désigne une forme quadratique non nulle sur un espace vectoriel E de dimension n et $q = \sum_{j=1}^p \lambda_j \ell_j^2$ la réduction de Gauss de cette forme quadratique où p est un entier compris entre 1 et n , $\lambda_1, \dots, \lambda_p$ sont des scalaires non nuls et ℓ_1, \dots, ℓ_p des formes linéaires indépendantes.

On a vu que la forme polaire de q est définie par :

$$\varphi(x, y) = \sum_{j=1}^p \lambda_j \ell_j(x) \ell_j(y).$$

Théorème 11.17 *Avec les notations qui précèdent, on a :*

$$\text{rg}(q) = p$$

et :

$$\ker(q) = \{x \in E \mid \ell_1(x) = \ell_2(x) = \dots = \ell_p(x) = 0\}$$

Démonstration. À la réduction de Gauss $q = \sum_{j=1}^p \lambda_j \ell_j^2$ est associée une base $(f_i)_{1 \leq i \leq n}$ de E dans laquelle la matrice de q est diagonale de la forme :

$$D = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}$$

où les p premiers λ_i sont non nuls et les suivants nuls (théorème 11.14). Il en résulte que $\text{rg}(q) = \text{rg}(D) = p$ et $\ker(q)$ est de dimension $n - p$.

Comme les formes linéaires $\ell_1, \ell_2, \dots, \ell_p$ sont linéairement indépendantes, l'espace vectoriel :

$$F = \{x \in E \mid \ell_1(x) = \dots = \ell_p(x) = 0\}$$

est de dimension $n - p$. De plus pour tout $x \in F$ et $y \in E$, on a :

$$\varphi(x, y) = \sum_{j=1}^p \lambda_j \ell_j(x) \ell_j(y) = 0$$

ce qui signifie que F est contenu dans le noyau de q .

Ces espaces étant de même dimension, on a l'égalité $F = \ker(q)$. ■

Le résultat précédent nous permet de simplifier la recherche d'une base q -orthogonale $(f_i)_{1 \leq i \leq n}$ de E en se passant de compléter le système libre $(\ell_i)_{1 \leq i \leq n}$ en une base du dual de E .

Dans le cas où $p = n$, la forme q est non dégénérée et une telle base q -orthogonale se calcule en résolvant les n systèmes linéaires :

$$\ell_i(f_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \quad (1 \leq i, j \leq n)$$

ce qui revient à inverser la matrice $Q = ((\alpha_{ij}))_{1 \leq i, j \leq n}$, où les α_{ij} sont définis par :

$$\ell_i(x) = \alpha_{i1}x_1 + \dots + \alpha_{in}x_n$$

(les ℓ_i étant exprimés dans une base canonique donnée de E).

Dans le cas où $1 \leq p \leq n-1$, on détermine tout d'abord une base (f_{p+1}, \dots, f_n) du noyau de q en résolvant le système linéaire de p équations à n inconnues :

$$\ell_i(x) = 0 \quad (1 \leq i \leq p)$$

Ces vecteurs sont deux à deux orthogonaux puisque orthogonaux à tout vecteur de E .

Il suffit ensuite de résoudre les p systèmes linéaires :

$$\ell_i(f_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \quad (1 \leq i, j \leq p)$$

ce qui fournit une famille q -orthogonale (f_1, \dots, f_p) formée de vecteurs non nuls. Pour j fixé entre 1 et p , le système linéaire $\ell_i(f_j) = \delta_{ij}$ où i varie de 1 à p a des solutions puisque la matrice de ce système est de rang p et deux solutions de ce système diffèrent d'un élément du noyau de q .

La famille $(f_i)_{1 \leq i \leq n}$ est alors une base q -orthogonale de E (exercice : vérifier qu'on a bien une base).

Dans la pratique, on résout d'abord le système :

$$\begin{cases} \ell_1(x) = b_1 \\ \vdots \\ \ell_p(x) = b_p \end{cases}$$

où $b = (b_1, \dots, b_p)$ est un élément quelconque de \mathbb{K}^p . La valeur $b = 0$ nous donne une base du noyau de q , puis les valeurs successives $b = (1, 0, \dots, 0)$, $b = (0, 1, 0, \dots, 0)$, \dots , $b = (0, \dots, 0, 1)$ nous permettent de déterminer des vecteurs f_1, \dots, f_p .

Exercice 11.28 Soit q la forme quadratique définie sur \mathbb{R}^3 par :

$$q(x) = x^2 + (1+a)y^2 + (1+a+a^2)z^2 + 2xy - 2ayz$$

1. Donner la matrice A de q dans la base canonique de \mathbb{R}^3 .
2. Calculer le déterminant de A .
3. Pour quelles valeurs de A la forme q est-elle non dégénérée ?
4. Réduire q et donner son rang en fonction de a .
5. Déterminer une base orthogonale pour q .
6. En déduire une matrice inversible P telle que $D = {}^tPAP$ soit diagonale.

Solution

1. La matrice de q dans la base canonique de \mathbb{R}^3 est :

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1+a & -a \\ 0 & -a & 1+a+a^2 \end{pmatrix}.$$

2. On a :

$$\det(A) = a(1+a^2)$$

3. La forme q est dégénérée si, et seulement si, $a = 0$.

4. On a :

$$q(x) = (x + y)^2 + a(y - z)^2 + (1 + a^2)z^2$$

Pour $a = 0$, q est de rang 2.

Pour $a \neq 0$, q est de rang 3.

5. Dans tous les cas, il s'agit de résoudre le système :

$$\begin{cases} x + y = \alpha \\ y - z = \beta \\ z = \gamma \end{cases}$$

Ce système a pour solution :

$$\begin{cases} x = \alpha - \beta - \gamma \\ y = \beta + \gamma \\ z = \gamma \end{cases}$$

ce qui donne pour base q -orthogonale :

$$f_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, f_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, f_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$$

6. La matrice de q dans la base (f_1, f_2, f_3) est :

$$D = {}^t P A P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 + a^2 \end{pmatrix}$$

où :

$$P = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

11.7 Signature d'une forme quadratique réelle en dimension finie

Pour ce paragraphe, q est une forme quadratique non nulle a priori sur un espace vectoriel réel E de dimension finie égale à $n \geq 1$ et on note φ sa forme polaire.

Théorème 11.18 *Il existe un unique couple (s, t) d'entiers naturels tel que pour toute base $(e_i)_{1 \leq i \leq n}$ de E qui est orthogonale relativement à q , le nombre de vecteurs e_i tels que $q(e_i) > 0$ est égal à s et le nombre de vecteurs e_i tels que $q(e_i) < 0$ est égal à t . De plus, on a $s + t = \text{rg}(q)$.*

Démonstration. Soient $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ deux bases q -orthogonales de E telles que :

$$\begin{cases} q(e_i) > 0 & (1 \leq i \leq s) \\ q(e'_i) > 0 & (1 \leq i \leq s') \\ q(e_i) < 0 & (s + 1 \leq i \leq s + t) \\ q(e'_i) < 0 & (s' + 1 \leq i \leq s' + t') \\ q(e_i) = 0 & (s + t + 1 \leq i \leq n) \\ q(e'_i) = 0 & (s' + t' + 1 \leq i \leq n) \end{cases}$$

où s, t, s', t' sont des entiers compris entre 0 et n avec la convention que la condition correspondante sur le signe de $q(e_i)$ ou $q(e'_i)$ n'a pas lieu quand l'encadrement de l'indice i n'a pas de sens.

Considérant les matrices de q dans chacune de ces bases, on voit que nécessairement on a $s + t = s' + t' = \text{rg}(q)$.

On désigne par F le sous-espace vectoriel de E engendré par $\{e_1, \dots, e_s\}$ ($F = \{0\}$ pour $s = 0$) et par G' celui engendré par $\{e'_{s'+1}, \dots, e'_n\}$ ($G' = \{0\}$ pour $s' = n$). En supposant que $s \geq 1$, on a alors :

$$\forall x \in F \setminus \{0\}, \quad q(x) = \sum_{i=1}^s \lambda_i x_i^2 > 0$$

et :

$$\forall x \in G', \quad q(x) = \sum_{i=s'+1}^n \lambda'_i x_i^2 \leq 0$$

et en conséquence $F \cap G' = \{0\}$. Ce dernier résultat étant encore valable pour $s = 0$. On en déduit alors que :

$$\begin{aligned} \dim(F \oplus G') &= \dim(F) + \dim(G') \\ &= s + n - s' \leq n \end{aligned}$$

et $s \leq s'$.

En permutant les rôles joués par s et s' , on montre de même que $s' \leq s$. On a donc $s = s'$ et $t = t'$ puisque $s + t = s' + t' = \text{rg}(q)$. ■

Définition 11.18 *Le couple (s, t) d'entiers naturels défini par le théorème précédent est appelé signature de q et on le note $\text{sgn}(q)$.*

Une forme quadratique q est donc de signature (s, t) si, et seulement si, elle admet une réduction de Gauss de la forme :

$$q = \sum_{j=1}^s \lambda_j \ell_j^2 - \sum_{j=s+1}^{s+t} \lambda_j \ell_j^2$$

où les λ_j sont tous strictement positifs (pour $s = 0$ la première somme n'existe pas et $s = n$ c'est la deuxième qui n'existe pas). En définissant les formes linéaires L_j par $L_j(x) = \ell_j(\sqrt{\lambda_j}x)$, on a la décomposition :

$$q = \sum_{j=1}^s L_j^2 - \sum_{j=s+1}^{s+t} L_j^2$$

et à cette décomposition est associée une base q -orthogonale de E dans laquelle la matrice de q est :

$$D = \begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

où I_r est la matrice identité d'ordre r . Les blocs diagonaux I_s , $-I_t$ ou 0 n'existent pas si $s = 0$, $s = n$ ou $s + t = n$.

Définition 11.19 *On dit que la forme bilinéaire symétrique φ (ou de manière équivalente la forme quadratique q) est positive [resp. définie positive] si $q(x) \geq 0$ [resp. $q(x) > 0$] pour tout x dans E [resp. dans $E \setminus \{0\}$].*

Une forme quadratique non nulle est donc positive [resp. définie positive] si, et seulement si, sa signature est $(s, 0)$ [resp. $(n, 0)$] où s est compris entre 1 et n .

On définit de manière analogue les formes quadratiques négative [resp. définie négative] et une forme quadratique non nulle est négative [resp. définie négative] si, et seulement si, sa signature est $(0, t)$ [resp. $(0, n)$] où t est compris entre 1 et n .

Exercice 11.29 On dit qu'une forme quadratique q sur E est définie si $q(x) \neq 0$ pour tout $x \in E \setminus \{0\}$. Montrer que si q est une forme quadratique définie (au sens de la définition qui vient d'être donnée) sur un espace vectoriel réel E de dimension finie, alors elle est positive ou négative.

Solution 11.28 Dans une base q -orthogonale $\mathcal{B} = (e_i)_{1 \leq i \leq n}$, la matrice de q est, a priori, de

la forme $D = \begin{pmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Si $p = s + t < n$, on a alors $q(e_{p+1}) \neq 0$ avec $e_{p+1} \neq 0$, ce qui

contredit le caractère définie de q . La forme q est donc de rang $p = n$.

Supposons que $1 \leq s \leq n - 1$. On a alors $q(e_s) = 1$, $q(e_{s+1}) = -1$ et :

$$q(e_s + e_{s+1}) = q(e_s) + q(e_{s+1}) = 1 - 1 = 0$$

avec $e_s + e_{s+1} \neq 0$, ce qui contredit encore le caractère définie de q . On a donc $s = 0$ et q est définie négative ou $s = 0$ et q est définie positive.

On peut aussi dire que, pour $n \geq 2$, la fonction continue q de \mathbb{R}^n dans \mathbb{R} transforme le connexe $\mathbb{R}^n \setminus \{0\}$ en un connexe de \mathbb{R}^* et en conséquence $q(\mathbb{R}^n \setminus \{0\})$ est contenu dans $\mathbb{R}^{-,*}$ ou $\mathbb{R}^{+,*}$.

À partir d'une réduction de Gauss, $q = \sum_{j=1}^p \lambda_j \ell_j^2$, on déduit que q est positive [resp. définie positive] si, et seulement si, tous les λ_j sont strictement positifs [resp. $p = n$ et tous les λ_j sont strictement positifs]. En effet, la condition suffisante est évidente et pour la condition nécessaire, en supposant $\lambda_1 < 0$ (on peut toujours s'y ramener) et en désignant par $(e_i)_{1 \leq i \leq n}$ une base q -orthogonale de E déduite de cette réduction de Gauss, on a $q(e_1) = \lambda_1 < 0$ et q n'est pas positive.

Exercice 11.30 Soit q la forme quadratique positive définie sur \mathbb{R}^3 par :

$$q(x, y, z) = 2x^2 + y^2 + z^2 + 2xy - 2xz.$$

1. Calculer la matrice de q dans la base canonique de \mathbb{R}^3 .
2. Donner une expression réduite de cette forme et en déduire le rang et la signature de q .

Solution 11.29

1. On a :

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

2. On a :

$$\begin{aligned} q(x, y, z) &= 2(x^2 + xy - xz) + y^2 + z^2 \\ &= 2 \left(\left(x + \frac{1}{2}y - \frac{1}{2}z \right)^2 - \frac{1}{4}y^2 - \frac{1}{4}z^2 + \frac{1}{2}yz \right) + y^2 + z^2 \\ &= 2 \left(x + \frac{1}{2}y - \frac{1}{2}z \right)^2 + \frac{1}{2}(y + z)^2. \end{aligned}$$

q est de rang 2 et de signature $(2, 0)$.

Une définition équivalente de la signature qu'une forme quadratique est donnée par le théorème qui suit.

La démonstration de ce théorème nécessite les lemmes suivants.

Lemme 11.2 *Soit F un sous-espace vectoriel de E . La restriction de q à F est non dégénérée si, et seulement si, $F \cap F^\perp = \{0\}$.*

Démonstration. Dire que la restriction de q à F est non dégénérée équivaut à dire que :

$$\{x \in F \mid \forall y \in F, \varphi(x, y) = 0\} = \{0\}$$

et ce ensemble est justement $F \cap F^\perp$ (c'est aussi le noyau la restriction de q à F). ■

Lemme 11.3 *Soit F un sous-espace vectoriel de E . Si la restriction de q à F est non dégénérée on a alors $E = F \oplus F^\perp$.*

Démonstration. Laissée au lecteur. ■

Théorème 11.19 *En désignant par \mathcal{P} [resp. \mathcal{N}] l'ensemble de tous les sous-espaces vectoriels F de E tels que la restriction de q à F soit définie positive [resp. définie négative] (\mathcal{P} ou \mathcal{N} peut être vide), la signature (s, t) de q est donnée par :*

$$s = \begin{cases} 0 & \text{si } \mathcal{P} = \emptyset \\ \max_{F \in \mathcal{P}} \dim(F) & \text{si } \mathcal{P} \neq \emptyset \end{cases}$$

et :

$$t = \begin{cases} 0 & \text{si } \mathcal{N} = \emptyset \\ \max_{F \in \mathcal{N}} \dim(F) & \text{si } \mathcal{N} \neq \emptyset \end{cases}$$

Démonstration. Notons :

$$s' = \begin{cases} 0 & \text{si } \mathcal{P} = \emptyset \\ \max_{F \in \mathcal{P}} \dim(F) & \text{si } \mathcal{P} \neq \emptyset \end{cases}$$

et :

$$t' = \begin{cases} 0 & \text{si } \mathcal{N} = \emptyset \\ \max_{F \in \mathcal{N}} \dim(F) & \text{si } \mathcal{N} \neq \emptyset \end{cases}$$

Par définition de la signature de q , on a $s \leq s'$ et $t \leq t'$.

Si $\mathcal{P} = \emptyset$, on a alors $s = s' = 0$.

Si $\mathcal{P} \neq \emptyset$, on peut trouver $F \in \mathcal{P}$ tel que $\dim(F) = s'$ et on a nécessairement $\dim(F) \leq s$. En effet si $\dim(F) > s$, on désigne par $(e_1, \dots, e_{s'})$ une base q -orthogonale de F et on peut compléter cette base en une base (e_1, \dots, e_n) de E qui est aussi q -orthogonale puisque la restriction de q à F est non dégénérée (elle est définie positive) et $E = F \oplus F^\perp$. Comme $F \in \mathcal{P}$ est de dimension maximale, la restriction de q à F^\perp est négative et la signature de q est (s', t') avec $s' > s$, ce qui n'est pas possible. On a donc $s' \leq s$ et $s = s'$.

On montre de manière analogue que $t = t'$. ■

Si q est définie positive, on a donc une réduction de Gauss $q = \sum_{j=1}^n \lambda_j \ell_j^2$ où tous les λ_j sont strictement positifs et la matrice de q dans une base q -orthogonale adaptée à cette réduction est diagonale de termes diagonaux $\lambda_1, \lambda_2, \dots, \lambda_n$. En notant D cette matrice, on a $\det(D) =$

$\prod_{k=1}^n \lambda_k > 0$. La matrice de q dans une autre base de \mathbb{R}^n s'écrivant $A = {}^tPDP$ avec P inversible, on a $\det(A) = (\det(P))^2 \det(D) > 0$.

L'utilisation des mineurs principaux de la matrice de q dans une quelconque base de \mathbb{R}^n nous permet de savoir si une forme quadratique est définie positive ou non.

On rappelle que si $A = ((a_{ij}))_{1 \leq i, j \leq n}$ est une matrice carrée d'ordre n , les mineurs principaux de A sont les déterminants des matrices extraites $A_k = ((a_{ij}))_{1 \leq i, j \leq k}$ où k est un entier compris entre 1 et n .

Théorème 11.20 *Soit q une forme quadratique non nulle sur un espace vectoriel réel E de dimension n de matrice $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans une base $(e_i)_{1 \leq i \leq n}$. La forme q est définie positive si, et seulement si, tous les mineurs principaux de A sont strictement positifs.*

Démonstration. Supposons q définie positive sur E . Pour k compris entre 1 et n , la matrice $A_k = ((a_{ij}))_{1 \leq i, j \leq k}$ est la matrice de la forme quadratique q_k égale à la restriction de q au sous-espace vectoriel E_k de E engendré par les vecteurs e_1, \dots, e_k . Cette forme q_k étant définie positive comme q , il en résulte que $\det(A_k) > 0$.

Pour la réciproque, on raisonne par récurrence sur la dimension $n \geq 1$ de E .

Pour $n = 1$, le résultat est évident puisque $E = \mathbb{R}e_1$ est une droite vectoriel et q s'écrit $q(x) = q(x_1e_1) = \lambda x_1^2$ avec $\lambda = q(e_1) = \det(A)$.

Supposons le résultat acquis pour tous les espaces de dimension au plus égal à n et soit q une forme quadratique sur un espace E de dimension $n + 1$. On se donne une base $(e_i)_{1 \leq i \leq n+1}$ de E et on suppose que tous les mineurs principaux de la matrice $A = ((a_{ij}))_{1 \leq i, j \leq n+1}$ de q dans cette base sont strictement positifs. En désignant par H le sous-espace vectoriel de E engendré par les vecteurs e_1, \dots, e_n , la matrice extraite $A_n = ((a_{ij}))_{1 \leq i, j \leq n}$ est la matrice de la forme quadratique q_n égale à la restriction de q à H . Tous les mineurs principaux de A_n étant strictement positifs, cette forme q_n est définie positive sur H .

La restriction de q à H étant définie positive et q non dégénérée ($\det(A) \neq 0$), la signature de q ne peut être que $(n, 1)$ ou $(n + 1, 0)$ (par définition de la signature). Si cette signature est $(n, 1)$, cela signifie qu'on a une décomposition de Gauss de la forme $q = \sum_{j=1}^n \lambda_j \ell_j^2 - \lambda_{n+1} \ell_n^2$ où tous les λ_j sont strictement positifs et la matrice de q dans une base q -orthogonale adaptée à cette réduction est diagonale de termes diagonaux $\lambda_1, \lambda_2, \dots, \lambda_n, -\lambda_{n+1}$. En notant D cette matrice, on a $\det(D) = -\lambda_{n+1} \prod_{k=1}^n \lambda_k < 0$, ce qui contredit $\det(D) = (\det(P))^2 \det(A) > 0$. La signature de q est donc $(n + 1, 0)$ et q est définie positive. ■

11.8 Quadriques dans \mathbb{R}^n ou \mathbb{C}^n

Pour ce paragraphe, \mathbb{K} désigne encore le corps de réels ou des complexes. (ou un corps commutatif de caractéristique différente de 2).

Pour $n \geq 2$, on munit l'espace vectoriel \mathbb{K}^n de sa base canonique et les coordonnées d'un vecteur X de \mathbb{K}^n sont notées x_1, \dots, x_n .

Pour $n = 2$ [resp. $n = 3$] et $\mathbb{K} = \mathbb{R}$ les coordonnées seront notées x, y [resp. x, y, z].

Définition 11.20 *On appelle quadrique dans \mathbb{K}^n toute partie \mathcal{C} de \mathbb{K}^n définie par :*

$$\mathcal{C} = \left\{ X \in \mathbb{K}^n \mid \sum_{i=1}^n a_{ii}x_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij}x_i x_j + \sum_{i=1}^n b_i x_i + c = 0 \right\}$$

où c , les a_{ij} et les b_i sont des scalaires avec $(a_{11}, \dots, a_{nn}) \neq 0$.

On dit aussi que \mathcal{C} est la courbe d'équation :

$$P(X) = \sum_{i=1}^n a_{ii}x_i^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij}x_i x_j + \sum_{i=1}^n b_i x_i + c = 0$$

dans la base canonique.

On notera aussi $\mathcal{C} = P^{-1}\{0\}$ où P est une fonction polynomiale de degré 2 sur \mathbb{K}^n .

Remarque 11.7 Une telle courbe peut être vide comme le montre l'exemple de :

$$P(X) = x^2 + y^2 + 1$$

dans \mathbb{R}^2 .

Exemple 11.8 Pour $P(X) = x^2 + y^2$ dans \mathbb{R}^2 , \mathcal{C} est réduit à $\{0\}$.

Pour $P(X) = x^2 + y^2 - 1$ dans \mathbb{R}^2 , \mathcal{C} est le cercle de centre 0 et de rayon 1.

Pour $P(X) = x^2$ dans \mathbb{K}^2 , \mathcal{C} est la droite d'équation $x = 0$.

Pour $P(X) = xy$ dans \mathbb{K}^2 , \mathcal{C} est la réunion des droites d'équations respectives $x = 0$ et $y = 0$.

On peut remarquer que le polynôme P s'écrit $P = q + \ell + c$, où q est une forme quadratique, ℓ une forme linéaire et c une constante.

En désignant par A et L les matrices de q et ℓ dans la base canonique de \mathbb{K}^n , on a :

$$P(X) = {}^t X A X + L X + c$$

Pour tout X_0 dans \mathbb{K}^n , on a pour tout X dans \mathbb{K}^n , en désignant par φ la forme polaire de q :

$$\begin{aligned} P(X + X_0) &= q(X + X_0) + \ell(X + X_0) + c \\ &= q(X) + 2\varphi(X, X_0) + \ell(X) + \ell(X_0) + q(X_0) + c \end{aligned}$$

l'application $X \mapsto \varphi(X, X_0)$ étant une forme linéaire sur \mathbb{K}^n .

Définition 11.21 On dit que la quadrique $\mathcal{C} = P^{-1}\{0\}$ est à centre s'il existe un unique élément X_0 dans \mathbb{K}^n tel que $P(X + X_0) = q(X) + d$ pour tout X dans \mathbb{K}^n , où d est une constante.

Théorème 11.21 La quadrique $\mathcal{C} = P^{-1}\{0\}$ est à centre si, et seulement si, la forme quadratique q est non dégénérée.

Démonstration. Dire que \mathcal{C} est à centre revient à dire qu'il existe un unique X_0 dans \mathbb{K}^n tel que pour tout X dans \mathbb{K}^n , on ait $2\varphi(X, X_0) + \ell(X) = 0$, soit :

$$\forall X \in \mathbb{K}^n, 2 {}^t X_0 A X + L X = 0$$

c'est-à-dire :

$$\forall X \in \mathbb{K}^n, (2 {}^t X_0 A + L) X = 0$$

ce qui équivaut à $2 {}^t X_0 A + L = 0$ ou à $2 {}^t A X_0 = 2 A X_0 = - {}^t L$ (la matrice A de q est symétrique) X_0 étant unique.

En définitive, \mathcal{C} est à centre si, et seulement si, l'équation $2 A X_0 = - {}^t L$ a une unique solution, ce qui équivaut à dire que A est inversible. En effet, pour A inversible, la solution est $X_0 = -\frac{1}{2} A^{-1} {}^t L$ et pour A non inversible, l'ensemble des solutions de ce système est soit vide soit infini puisque pour toute solution X_0 , l'ensemble $X_0 + \ker(A)$, avec $\dim(\ker(A)) \geq 1$, nous donne une infinité de solutions. Et A inversible signifie que q non dégénérée. ■

Remarque 11.8 Si la quadrique \mathcal{C} est à centre de centre X_0 , en effectuant le changement de variable $X' = X - X_0$ (on ramène l'origine en X_0), on a :

$$\begin{aligned} P(X) &= P((X - X_0) + X_0) = q(X - X_0) + d = q(X') + d \\ &= \sum_{i=1}^n a_{ii} (x'_i)^2 + 2 \sum_{1 \leq i < j \leq n} a_{ij} x'_i x'_j + d \end{aligned}$$

Tenant compte du fait que pour tout $X' \in \mathbb{K}^n$ on a $q(X') = q(-X')$, on déduit que :

$$\begin{aligned} (X = X_0 + X' \in \mathcal{C}) &\Leftrightarrow P(X) = P(X' + X_0) = q(X') + d = 0 \\ &\Leftrightarrow q(-X') + d = P(-X' + X_0) = 0 \\ &\Leftrightarrow (X_0 - X' \in \mathcal{C}) \end{aligned}$$

ce qui se traduit en disant que le centre X_0 est un centre de symétrie pour \mathcal{C} .

Remarque 11.9 Le système linéaire permettant de déterminer le centre, quand il est unique, est donné par :

$$2 \sum_{j=1}^n a_{ij} x_j + b_i = 0 \quad (1 \leq i \leq n)$$

Dans \mathbb{R}^n , on a :

$$\begin{aligned} \frac{\partial}{\partial x_k} P(X) &= \frac{\partial}{\partial x_k} \left(\sum_{1 \leq i, j \leq n} a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c \right) \\ &= \frac{\partial}{\partial x_k} \left(\sum_{i=1}^n x_i \sum_{j=1}^n a_{ij} x_j + \sum_{i=1}^n b_i x_i + c \right) \\ &= \sum_{j=1}^n a_{kj} x_j + \sum_{i=1}^n x_i a_{ik} + b_k \\ &= \sum_{j=1}^n a_{kj} x_j + \sum_{i=1}^n a_{ki} x_i + b_k \\ &= 2 \sum_{j=1}^n a_{kj} x_j + b_k \quad (1 \leq k \leq n) \end{aligned}$$

et notre système linéaire s'écrit simplement :

$$\frac{\partial}{\partial x_k} P(X) = 0 \quad (1 \leq k \leq n)$$

Exemple 11.9 Dans \mathbb{R}^2 la quadrique d'équation $y - x^2 = 0$ n'est pas à centre puisque la forme quadratique $q : (x, y) \mapsto -x^2$ est dégénérée. Cette quadrique du plan \mathbb{R}^2 est une parabole.

Exemple 11.10 Considérons dans \mathbb{R}^2 la quadrique d'équation :

$$x^2 + y^2 - 2xy - 8(x + y) + 16 = 0$$

La forme quadratique q de matrice $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ est dégénérée ($\det(A) = 0$) et donc n'est pas à centre. En effectuant le changement de variable $x' = x - y$, $y' = x + y$, cette équation s'écrit $(x')^2 - 8y' + 16 = 0$, soit $y' = \frac{1}{8}(x')^2 - 16$ et \mathcal{C} est une parabole.

En définitive, si \mathcal{C} est une quadrique à centre, en plaçant l'origine au centre, cette conique à une équation de la forme :

$$q(X) = \alpha$$

où q est une forme quadratique non dégénérée et α une constante.

Le théorème de réduction de Gauss nous permet d'écrire q comme combinaison linéaire de n carrés de formes linéaires, ce qui revient à dire qu'il existe une base de \mathbb{K}^n dans laquelle l'expression de q est $q(X) = \sum_{i=1}^n \lambda_i y_i^2$, les scalaires λ_i étant non nuls et dans cette base (orthogonale pour q), une équation de \mathcal{C} est :

$$\sum_{i=1}^n \lambda_i y_i^2 = \alpha.$$

11.9 Quadriques dans \mathbb{R}^n

Dans le cas des quadratiques à centre réelles, en désignant par (s, t) la signature de q avec $s + t = n$, il existe une base de \mathbb{R}^n dans laquelle une équation de \mathcal{C} est :

$$\sum_{i=1}^s y_i^2 - \sum_{i=s+1}^n y_i^2 = \alpha.$$

avec la convention que $\sum_{i=1}^s = 0$ pour $s = 0$ et $\sum_{i=s+1}^n = 0$ pour $t = 0$.

En particulier dans le plan \mathbb{R}^2 , on a les possibilités suivantes en désignant par x, y les coordonnées de X dans une base q -orthogonale, l'origine étant ramenée au centre de la quadrique :

- $x^2 + y^2 = \pm\alpha = \beta$ pour q de signature $(2, 0)$ ou $(0, 2)$ et \mathcal{C} est vide pour $\beta < 0$, réduite à $\{(0, 0)\}$ pour $\beta = 0$ ou une ellipse pour $\beta > 0$;
- $x^2 - y^2 = \alpha$ pour q de signature $(1, 1)$ et \mathcal{C} est une hyperbole.

Exemple 11.11 Considérons dans \mathbb{R}^2 la quadrique d'équation :

$$x^2 + y^2 + 4xy + 4(x + y) - 8 = 0.$$

La forme quadratique q est non dégénérée puisque sa matrice dans la base canonique est :

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

a pour déterminant $\det(A) = -3 \neq 0$.

Son centre est solution du système linéaire :

$$\begin{cases} \frac{\partial P}{\partial x} P(X) = 2x + 4y + 4 = 0 \\ \frac{\partial P}{\partial y} P(X) = 2y + 4x + 4 = 0 \end{cases}$$

soit :

$$\begin{cases} x + 2y = -2 \\ 2x + y = -2 \end{cases}$$

ce qui donne $X_0 = -\frac{2}{3}(1, 1)$.

Le changement de variables $X' = X - X_0$, soit $x' = x + \frac{2}{3}$, $y' = y + \frac{2}{3}$ donne :

$$\left(x' - \frac{2}{3}\right)^2 + \left(y' - \frac{2}{3}\right)^2 + 4\left(x' - \frac{2}{3}\right)\left(y' - \frac{2}{3}\right) + 4\left(x' - \frac{2}{3} + y' - \frac{2}{3}\right) - 8 = 0$$

soit :

$$(x')^2 + (y')^2 + 4x'y' = \frac{32}{3}$$

comme prévu.

La réduction de Gauss donne :

$$(x' + 2y')^2 - 3(y')^2 = \frac{32}{3}$$

et \mathcal{C} est une hyperbole.

En restant dans \mathbb{R}^2 , une quadrique \mathcal{C} a une équation de la forme :

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0$$

Si la forme quadratique q est dégénérée et non nulle, elle est de rang 1, ce qui équivaut à dire que la matrice $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ est de rang 1 et il existe un réel non nul λ tel que $\begin{pmatrix} b \\ c \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix}$ et l'équation de \mathcal{C} devient :

$$a(x^2 + 2\lambda xy + \lambda^2 y^2) + dx + ey + f = 0$$

soit :

$$a(x + \lambda y)^2 + dx + ey + f = 0$$

Si $a = 0$, on a l'équation :

$$dx + ey + f = 0$$

qui définit une droite si $(e, d) \neq (0, 0)$, l'ensemble vide si $(e, d) = (0, 0)$ et $f \neq 0$ ou \mathbb{R}^2 tout entier si $(e, d) = (0, 0)$ et $f = 0$.

Pour $a \neq 0$, on distingue alors deux cas de figure.

Soit $e = \lambda d$ et notre équation devient :

$$(x + \lambda y)^2 + \frac{d}{a}(x + \lambda y) + \frac{f}{a} = 0$$

soit :

$$\left(x + \lambda y + \frac{d}{2a}\right)^2 = \frac{d^2 - 4af}{4a^2}$$

ce qui définit la réunion de deux droites si $d^2 - 4af > 0$ (les droites d'équations $x + \lambda y = \frac{\sqrt{d^2 - 4af} - d}{2a}$ et $x + \lambda y = -\frac{\sqrt{d^2 - 4af} + d}{2a}$), une droite si $d^2 - 4af = 0$ (la droite d'équation $x + \lambda y = -\frac{d}{2a}$) ou l'ensemble vide si $d^2 - 4af < 0$.

Soit $e \neq \lambda d$ et le changement de variable $x' = x + \lambda y$, $y' = dx + ey$ nous donne l'équation $a(x')^2 + y' + f = 0$, ce qui définit une parabole (le changement de variable est validé par $\begin{vmatrix} 1 & \lambda \\ d & e \end{vmatrix} = e - \lambda d \neq 0$).

En définitive, dans une base adaptée, une quadrique de \mathbb{R}^2 a une équation de l'une des formes suivantes :

- $x^2 + y^2 = \beta$;
- $x^2 - y^2 = \alpha$;
- $dx + ey + f = 0$;
- $x^2 = \alpha$;
- $ax^2 + y + f = 0$.

Espaces préhilbertiens

On désigne par E un espace vectoriel réel non réduit à $\{0\}$.

12.1 Produit scalaire

Définition 12.1 On dit qu'une forme bilinéaire symétrique φ sur E est :

- positive si $\varphi(x, x) \geq 0$ pour tout x dans E ;
- définie si pour x dans E l'égalité $\varphi(x, x) = 0$ équivaut à $x = 0$.

Définition 12.2 On appelle produit scalaire sur E toute forme bilinéaire symétrique définie positive.

Définition 12.3 Un espace préhilbertien est un espace vectoriel réel muni d'un produit scalaire. Un espace préhilbertien de dimension finie est dit euclidien.

Dans le cas où E est un espace euclidien, on peut aussi dire qu'un produit scalaire sur E est la forme polaire d'une forme quadratique de signature $(n, 0)$.

On notera, quand il n'y a pas d'ambiguïté :

$$(x, y) \longmapsto \langle x | y \rangle$$

un tel produit scalaire et pour $y = x$, on note :

$$\|x\| = \sqrt{\langle x | x \rangle}.$$

L'application $x \mapsto \|x\|^2 = \langle x | x \rangle$ est tout simplement la forme quadratique associée à $\langle \cdot | \cdot \rangle$.

Les trois égalités qui suivent, expressions de la forme polaire d'une forme quadratique, sont utiles en pratique.

Théorème 12.1 Pour tous x, y dans E on a :

$$\begin{aligned} \langle x | y \rangle &= \frac{1}{2} (\|x + y\|^2 - \|x\|^2 - \|y\|^2) \\ &= \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2), \end{aligned}$$

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

La deuxième identité est l'égalité du parallélogramme. Elle est caractéristique des produits scalaires dans le sens où une norme est déduite d'un produit scalaire si, et seulement si, elle vérifie l'identité du parallélogramme (voir le chapitre sur les espaces normés).

Exercice 12.1 Montrer que l'application $\varphi : (P, Q) \mapsto P(1)Q'(0) + P'(0)Q(1)$ définit une forme bilinéaire sur $E = \mathbb{R}[x]$. Est-ce un produit scalaire ?

Solution 12.1 Avec la structure de corps commutatif de \mathbb{R} et la linéarité des applications d'évaluation en un point d'un polynôme et de dérivation, on déduit que φ est une forme bilinéaire symétrique sur E . Pour $P \in E$ la quantité $\varphi(P, P) = 2P(1)P'(0)$ n'est pas nécessairement positive (prendre $P(x) = 2 - x$ par exemple), donc φ n'est pas un produit scalaire.

Exemple 12.1 L'espace vectoriel \mathbb{R}^n étant muni de sa base canonique $(e_i)_{1 \leq i \leq n}$, l'application :

$$(x, y) \mapsto \langle x | y \rangle = \sum_{k=1}^n x_k y_k$$

définit un produit scalaire sur \mathbb{R}^n . On dit que c'est le produit scalaire euclidien canonique de \mathbb{R}^n .

Exercice 12.2 L'espace vectoriel \mathbb{R}^n est toujours muni de sa base canonique $(e_i)_{1 \leq i \leq n}$. Soit $\omega \in \mathbb{R}^n$. À quelle condition sur ω l'application :

$$\varphi : (x, y) \mapsto \sum_{k=1}^n \omega_k x_k y_k$$

définit-elle un produit scalaire sur l'espace vectoriel \mathbb{R}^n ?

Solution 12.2 L'application φ définit une forme bilinéaire symétrique sur \mathbb{R}^n pour tout $\omega \in \mathbb{R}^n$.

Si φ est un produit scalaire, on a alors $\omega_j = \varphi(e_j, e_j) > 0$ pour tout j compris entre 1 et n .

Réciproquement si tous les ω_j sont strictement positifs, on a $\varphi(x, x) = \sum_{i=1}^n \omega_i x_i^2 \geq 0$ pour tout $x \in \mathbb{R}^n$ et $\varphi(x, x) = 0$ équivaut à $\omega_i x_i^2 = 0$ pour tout i , ce qui équivaut à $x_i = 0$ pour tout i , soit à $x = 0$.

En conclusion, φ définit un produit scalaire sur \mathbb{R}^n si, et seulement si, tous les ω_i sont strictement positifs.

Exercice 12.3 Donner une condition nécessaire et suffisante sur les réels a, b, c, d pour que l'application :

$$(x, y) \mapsto \langle x | y \rangle = ax_1y_1 + bx_1y_2 + cx_2y_1 + dx_2y_2$$

définisse un produit scalaire sur $E = \mathbb{R}^2$.

Solution 12.3 Cette application est bilinéaire pour tous réels a, b, c, d . Elle est symétrique si, et seulement si, sa matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans la base canonique de \mathbb{R}^2 est symétrique, ce qui équivaut à $b = c$.

Pour $b = c$, φ est bilinéaire symétrique et pour tout $x \in \mathbb{R}^2$, on a :

$$\langle x | x \rangle = ax_1^2 + 2bx_1x_2 + dx_2^2.$$

Si on a un produit scalaire, alors $a = \langle e_1 | e_1 \rangle > 0$, $d = \langle e_2 | e_2 \rangle > 0$ et pour tout vecteur $x = e_1 + te_2$, où t est un réel quelconque, on a $\langle x | x \rangle = a + 2bt + dt^2 > 0$, ce qui équivaut à $\delta = b^2 - ad < 0$.

Réciproquement si $b = c$, $a > 0$, $d > 0$ et $b^2 - ad < 0$ alors $\langle \cdot | \cdot \rangle$ est bilinéaire symétrique et pour tout $x \in E$, on a :

$$\begin{aligned}\langle x | x \rangle &= ax_1^2 + 2bx_1x_2 + dx_2^2 \\ &= a \left(x_1^2 + 2\frac{b}{a}x_1x_2 + \frac{d}{a}x_2^2 \right) \\ &= a \left(\left(x_1 + \frac{b}{a}x_2 \right)^2 + \frac{ad - b^2}{a^2}x_2^2 \right) \geq 0\end{aligned}$$

avec $\langle x | x \rangle = 0$ si, et seulement si, $x_1 + \frac{b}{a}x_2 = 0$ et $x_2 = 0$, ce qui équivaut à $x = 0$.

Donc $\langle \cdot | \cdot \rangle$ est un produit scalaire si, et seulement si, $b = c$, $a > 0$, $d > 0$ et $b^2 - ad < 0$.

Exercice 12.4 Soient n un entier naturel non nul, x_0, \dots, x_n des réels deux à deux distincts et $\omega \in \mathbb{R}^{n+1}$. À quelle condition sur ω l'application :

$$\varphi : (P, Q) \mapsto \sum_{i=0}^n \omega_i P(x_i) Q(x_i)$$

définit-elle un produit scalaire sur l'espace vectoriel $\mathbb{R}_n[x]$?

Solution 12.4 L'application φ définit une forme bilinéaire symétrique sur $\mathbb{R}_n[x]$ pour tout $\omega \in \mathbb{R}^n$.

Si φ est un produit scalaire, en désignant par $(L_i)_{0 \leq i \leq n}$ la base de Lagrange de $\mathbb{R}_n[x]$ définie par :

$$L_i(x) = \prod_{\substack{k=0 \\ k \neq i}}^n \frac{x - x_k}{x_i - x_k} \quad (0 \leq i \leq n)$$

(L_i est le polynôme de degré n qui vaut 1 en x_i et 0 en x_k pour $k \neq i$), on a alors $\omega_j = \varphi(L_j, L_j) > 0$ pour tout j compris entre 1 et n .

Réciproquement si tous les ω_j sont strictement positifs, on a $\varphi(P, P) = \sum_{i=1}^n \omega_i P^2(x_i) \geq 0$ pour

tout $x \in \mathbb{R}^n$ et $\varphi(P, P) = 0$ équivaut à $\omega_i P^2(x_i) = 0$ pour tout i , ce qui équivaut à $P(x_i) = 0$ pour tout i compris entre 0 et n soit à $P = 0$ (P est un polynôme dans $\mathbb{R}_n[x]$ qui a $n+1$ racines distinctes, c'est donc le polynôme nul).

En conclusion, φ définit un produit scalaire sur $\mathbb{R}_n[x]$ si, et seulement si, tous les ω_i sont strictement positifs.

Exercice 12.5 n étant un entier naturel non nul, on note \mathcal{P}_n l'ensemble des polynômes trigonométriques de degré inférieur ou égal à n , c'est-à-dire l'ensemble des fonctions de \mathbb{R} dans \mathbb{R} la forme :

$$P : x \mapsto P(x) = a_0 + \sum_{k=1}^n (a_k \cos(kx) + b_k \sin(kx)).$$

1. Montrer que \mathcal{P}_n est un espace vectoriel et préciser sa dimension.
2. Montrer que si $P \in \mathcal{P}_n$ s'annule en $2n+1$ points deux à deux distincts dans $[-\pi, \pi[$, alors $P = 0$ (utiliser les expressions complexes des fonctions cos et sin).

3. Montrer que si x_0, \dots, x_{2n} sont des réels deux à deux distincts dans $[-\pi, \pi[$, alors l'application :

$$\varphi : (P, Q) \mapsto \sum_{i=0}^{2n} P(x_i) Q(x_i)$$

définit un produit scalaire sur l'espace vectoriel \mathcal{P}_n .

Solution 12.5

1. Il est clair que \mathcal{P}_n est un sous-espace vectoriel de l'espace vectoriel des applications de \mathbb{R} dans \mathbb{R} . En notant respectivement c_k et s_k les fonctions $x \mapsto \cos(kx)$ pour $k \geq 0$ et $x \mapsto \sin(kx)$ pour $k \geq 1$, \mathcal{P}_n est engendré par la famille $\mathcal{B}_n = \{c_k \mid 0 \leq k \leq n\} \cup \{s_k \mid 1 \leq k \leq n\}$, c'est donc un espace vectoriel de dimension au plus égale à $2n + 1$. Montrons que cette famille de fonctions est libre. Pour ce faire, on procède par récurrence sur $n \geq 1$ (comme avec l'exercice 9.4).

Pour $n = 1$, si $a_0 + a_1 \cos(x) + b_1 \sin(x) = 0$, en évaluant cette fonction en $0, \frac{\pi}{2}$ et π successivement, on aboutit au système linéaire :

$$\begin{cases} a_0 + a_1 = 0 \\ a_0 + b_1 = 0 \\ a_0 - a_1 = 0 \end{cases}$$

qui équivaut à $a_0 = b_0 = b_1 = 0$. La famille $\{c_0, c_1, s_1\}$ est donc libre.

Supposons le résultat acquis au rang $n - 1 \geq 1$. Si $P = a_0 + \sum_{k=1}^n (a_k c_k + b_k s_k) = 0$, en dérivant deux fois, on a :

$$P'' = - \sum_{k=1}^n k^2 (a_k c_k + b_k s_k) = 0$$

Il en résulte que :

$$n^2 P + P'' = n^2 a_0 + \sum_{k=1}^{n-1} (n^2 - k^2) (a_k c_k + b_k s_k) = 0$$

et l'hypothèse de récurrence nous dit que $n^2 a_0 = 0$, $(n^2 - k^2) a_k = 0$ et $(n^2 - k^2) b_k$ pour tout k compris entre 1 et $n - 1$, ce qui équivaut à dire que $a_0 = 0$ et $a_k = b_k = 0$ pour tout k compris entre 1 et $n - 1$ puisque $n^2 - k^2 \neq 0$. Il reste alors $a_n c_n + b_n s_n = 0$, ce qui implique $a_n = 0$, en évaluant en $x = 0$ et $b_n = 0$. La famille \mathcal{B}_n est donc libre.

On verra un peu plus loin que cette famille est orthogonale, formée de fonctions non nulles, et en conséquence libre (exercice 12.15).

2. Posant $z = e^{ix}$ pour tout réel x , on a :

$$\begin{aligned} P(x) &= a_0 + \sum_{k=1}^n \left(a_k \frac{z^k + \bar{z}^k}{2} + b_k \frac{z^k - \bar{z}^k}{2i} \right) \\ &= a_0 + \frac{1}{2} \sum_{k=1}^n \left(a_k \left(z^k + \frac{1}{z^k} \right) - ib_k \left(z^k - \frac{1}{z^k} \right) \right) \\ &= a_0 + \frac{1}{2} \sum_{k=1}^n \left((a_k - ib_k) z^k + (a_k + ib_k) \frac{1}{z^k} \right) \end{aligned}$$

ou encore :

$$z^n P(x) = a_0 z^{2n} + \frac{1}{2} \sum_{k=1}^n ((a_k - ib_k) z^{n+k} + (a_k + ib_k) z^{n-k}) = Q(z)$$

Il en résulte que si P s'annule en $2n+1$ points deux à deux distincts, x_0, \dots, x_{2n} , dans $[-\pi, \pi[$, alors le polynôme complexe $Q \in \mathbb{C}_{2n}[z]$ s'annule en $2n+1$ points distincts du cercle unité, $e^{ix_0}, \dots, e^{ix_{2n}}$, ce qui revient à dire que c'est le polynôme nul et $P = 0$.

3. On vérifie facilement que φ est une forme bilinéaire symétrique et positive. L'égalité $\varphi(P, P) = 0$ entraîne que $P \in \mathcal{P}_n$ s'annule en $2n+1$ points deux à deux distincts dans $[-\pi, \pi[$ et en conséquence $P = 0$.

Exercice 12.6 Montrer que, pour toute fonction $\alpha \in \mathcal{C}^0([a, b], \mathbb{R}_+^*)$, l'application :

$$\varphi : (f, g) \mapsto \int_a^b f(t) g(t) \alpha(t) dt$$

définit un produit scalaire sur l'espace vectoriel $E = \mathcal{C}^0([a, b], \mathbb{R})$.

Solution 12.6 Avec la structure de corps commutatif de \mathbb{R} et la linéarité et positivité de l'intégrale, on déduit que φ est une forme bilinéaire symétrique positive sur E . Sachant que l'intégrale sur $[a, b]$ d'une fonction continue et à valeurs positives est nulle si, et seulement si, cette fonction est nulle, on déduit que φ est une forme définie. Donc φ est un produit scalaire sur E .

Exercice 12.7 Montrer que l'application :

$$(f, g) \mapsto \int_{-\pi}^{\pi} f(t) g(t) dt$$

définit un produit scalaire sur l'espace vectoriel \mathcal{F} des fonctions définies sur \mathbb{R} à valeurs réelles, continues et périodiques de période 2π .

Solution 12.7 Ce sont les mêmes arguments qu'à l'exercice précédent compte tenu qu'une fonction de \mathcal{F} est nulle si, et seulement si, elle est nulle sur $[-\pi, \pi]$.

12.2 Inégalités de Cauchy-Schwarz et de Minkowski

Dans tout ce qui suit E désigne un espace préhilbertien.

Théorème 12.2 (Inégalité de Cauchy-Schwarz) Pour tous x, y dans E on a :

$$|\langle x | y \rangle| \leq \|x\| \|y\|,$$

l'égalité étant réalisée si, et seulement si, x et y sont liés.

Démonstration. Si $x = 0$, on a alors l'égalité pour tout $y \in E$.

Si $x \neq 0$ et $y = \lambda x$ avec $\lambda \in \mathbb{R}$, on a encore l'égalité.

On suppose donc que x est non nul et y non lié à x . La fonction polynomiale P défini par :

$$P(t) = \|y + tx\|^2 = \|x\|^2 t^2 + 2 \langle x | y \rangle t + \|y\|^2$$

est alors à valeurs strictement positives, le coefficient de t^2 étant non nul, il en résulte que son discriminant est strictement négatif, soit :

$$\langle x | y \rangle^2 - \|x\|^2 \|y\|^2 < 0,$$

ce qui équivaut à $|\langle x | y \rangle| < \|x\| \|y\|$. ■

Sur \mathbb{R}^n muni du produit scalaire canonique, l'inégalité de Cauchy-Schwarz prend la forme suivante :

$$\left| \sum_{k=1}^n x_k y_k \right|^2 \leq \left(\sum_{k=1}^n x_k^2 \right) \left(\sum_{k=1}^n y_k^2 \right)$$

On peut déduire de cette inégalité quelques inégalités intéressantes sur les réels.

Exercice 12.8

1. On se donne un entier $n \geq 1$ et des réels x_1, \dots, x_n . Montrer que :

$$\left(\sum_{k=1}^n x_k \right)^2 \leq n \sum_{k=1}^n x_k^2$$

Dans quel cas a-t-on égalité ?

2. En déduire une condition nécessaire et suffisante, sur les réels a et b , pour que l'application $\varphi : (x, y) \mapsto a \sum_{i=1}^n x_i y_i + b \sum_{1 \leq i < j \leq n} x_i y_j$ définissent un produit scalaire sur \mathbb{R}^n , où $n \geq 2$.

Solution 12.8

1. L'inégalité de Cauchy-Schwarz nous donne :

$$\left(\sum_{k=1}^n x_k \cdot 1 \right)^2 \leq \left(\sum_{k=1}^n 1^2 \right) \left(\sum_{k=1}^n x_k^2 \right) = n \sum_{k=1}^n x_k^2$$

l'égalité étant réalisée si, et seulement si, tous les x_k sont égaux.

2. L'application φ est bilinéaire et symétrique. Pour $x \in \mathbb{R}^n$, on a :

$$\begin{aligned} q(x) = \varphi(x, x) &= a \sum_{i=1}^n x_i^2 + 2b \sum_{1 \leq i < j \leq n} x_i x_j \\ &= a \sum_{i=1}^n x_i^2 + b \left(\left(\sum_{i=1}^n x_i \right)^2 - \sum_{i=1}^n x_i^2 \right) \\ &= (a - b) \sum_{i=1}^n x_i^2 + b \left(\sum_{i=1}^n x_i \right)^2 \end{aligned}$$

Si φ est un produit scalaire, on a alors $a = q(e_1) > 0$, $a - b = q(e_1 - e_2) > 0$ et $q\left(\sum_{i=1}^n e_i\right) = n(a + (n-1)b) > 0$.

Réciproquement si $a > 0$, $a - b > 0$ et $a + (n - 1)b > 0$, on a alors pour $x \in \mathbb{R}^n \setminus \{0\}$ ayant au moins deux composantes distinctes :

$$\begin{aligned} q(x) &= (a - b) \sum_{i=1}^n x_i^2 + b \left(\sum_{i=1}^n x_i \right)^2 \\ &> (a - b) \frac{1}{n} \left(\sum_{i=1}^n x_i \right)^2 + b \left(\sum_{i=1}^n x_i \right)^2 \\ &= \frac{1}{n} (a + (n - 1)b) \left(\sum_{i=1}^n x_i \right)^2 \geq 0 \end{aligned}$$

et $q(x) > 0$. Si $x \in \mathbb{R}^n \setminus \{0\}$ a toutes ses composantes égales à $\lambda \neq 0$, on a alors :

$$q(x) = q\left(\lambda \sum_{i=1}^n e_i\right) = n\lambda^2 (a + (n - 1)b) > 0.$$

Donc φ est un produit scalaire.

Exercice 12.9 Montrer que pour tout entier $n \geq 1$, on a :

$$\sum_{k=1}^n k\sqrt{k} \leq \frac{n(n+1)}{2\sqrt{3}} \sqrt{2n+1}$$

Solution 12.9 L'inégalité de Cauchy-Schwarz nous donne :

$$\sum_{k=1}^n k\sqrt{k} \leq \sqrt{\sum_{k=1}^n k^2} \sqrt{\sum_{k=1}^n k}$$

avec $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ et $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$, ce qui donne :

$$\sum_{k=1}^n k\sqrt{k} \leq \sqrt{\frac{n^2(n+1)^2(2n+1)}{12}} = \frac{n(n+1)}{2\sqrt{3}} \sqrt{2n+1}.$$

Exercice 12.10 On se donne un entier $n \geq 1$ et des réels x_1, \dots, x_n strictement positifs.

1. Montrer que :

$$\left(\sum_{k=1}^n x_k \right) \left(\sum_{k=1}^n \frac{1}{x_k} \right) \geq n^2.$$

Dans quel cas a-t-on égalité ?

2. Montrer que :

$$\sum_{k=1}^n \frac{1}{k^2} \geq \frac{6n}{(n+1)(2n+1)}.$$

Solution 12.10

1. L'inégalité de Cauchy-Schwarz nous donne :

$$n = \sum_{k=1}^n \sqrt{x_k} \frac{1}{\sqrt{x_k}} \leq \sqrt{\sum_{k=1}^n x_k} \sqrt{\sum_{k=1}^n \frac{1}{x_k}}$$

encore équivalent à l'inégalité proposée.

L'égalité est réalisée si, et seulement si, il existe un réel λ tel que $\sqrt{x_k} = \lambda \frac{1}{\sqrt{x_k}}$ pour tout k compris entre 1 et n , ce qui équivaut à $x_k = \lambda$ pour tout k compris entre 1 et n , où λ est un réel strictement positif.

2. Prenant $x_k = k^2$ pour tout k compris entre 1 et n , on en déduit que :

$$\left(\sum_{k=1}^n k^2 \right) \left(\sum_{k=1}^n \frac{1}{k^2} \right) \geq n^2$$

et avec $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$, on en déduit que :

$$\sum_{k=1}^n \frac{1}{k^2} \geq \frac{6n}{(n+1)(2n+1)}.$$

Exercice 12.11

1. Montrer que pour tous réels a, b et λ , on a :

$$(2\lambda - 1)a^2 - 2\lambda ab = \lambda(a - b)^2 - \lambda b^2 + (\lambda - 1)a^2$$

2. Soit q la forme quadratique définie sur $E = \mathbb{R}^n$ par :

$$q(x) = \sum_{k=1}^n (2k-1)x_k^2 - 2 \sum_{k=1}^{n-1} kx_k x_{k+1}$$

(a) Effectuer une réduction de q en combinaison linéaire de carrés de formes linéaires indépendantes.

(b) Préciser le rang le noyau et la signature de q .

3. On note $(x, y) = (x_1, \dots, x_n, y_1, \dots, y_n)$ un vecteur de $H = \mathbb{R}^{2n}$ et Q la forme quadratique définie sur H par :

$$Q(x, y) = \sum_{k=1}^n (y_k^2 - 2x_k y_k).$$

(a) Effectuer une réduction de Q en combinaison linéaire de carrés de formes linéaires indépendantes.

(b) Préciser le rang le noyau et la signature de Q .

4. Pour $n \geq 1$ et $x = (x_1, \dots, x_n)$ dans \mathbb{R}^n , on définit $y = (y_1, \dots, y_n)$ par :

$$y_k = \frac{1}{k} \sum_{j=1}^k x_j.$$

(a) Montrer que :

$$\begin{cases} x_1 = y_1 \\ \forall k \in \{2, \dots, n\}, x_k = ky_k - (k-1)y_{k-1} \end{cases}$$

(b) Montrer que :

$$Q(x, y) = -q(y).$$

(c) En déduire :

$$\sum_{k=1}^n y_k^2 \leq \sum_{k=1}^n 2x_k y_k.$$

puis montrer que :

$$\sum_{k=1}^n y_k^2 \leq 4 \sum_{k=1}^n x_k^2.$$

(d) En déduire que si $(x_n)_{n \geq 1}$ est une suite de réels telle que la série $\sum x_n^2$ soit convergente et si $(y_n)_{n \geq 1}$ est la suite des moyennes de Césaro définie par $y_n = \frac{1}{n} \sum_{j=1}^n x_j$ pour tout

$n \geq 1$, alors la série $\sum y_n^2$ est convergente et $\sum_{n=1}^{+\infty} y_n^2 \leq 4 \sum_{n=1}^{+\infty} x_n^2$.

Solution 12.11

1. On a :

$$\begin{aligned} (2\lambda - 1)a^2 - 2\lambda ab &= \lambda(a^2 - 2ab) + (\lambda - 1)a^2 \\ &= \lambda((a - b)^2 - b^2) + (\lambda - 1)a^2 \\ &= \lambda(a - b)^2 - \lambda b^2 + (\lambda - 1)a^2 \end{aligned}$$

2.

(a) En utilisant le résultat précédent, on a :

$$\begin{aligned} q(x) &= (2n - 1)x_n^2 + \sum_{k=1}^{n-1} ((2k - 1)x_k^2 - 2kx_k x_{k+1}) \\ &= (2n - 1)x_n^2 + \sum_{k=1}^{n-1} k(x_k - x_{k+1})^2 - \sum_{k=1}^{n-1} kx_{k+1}^2 + \sum_{k=1}^{n-1} (k - 1)x_k^2 \\ &= (2n - 1)x_n^2 + \sum_{k=1}^{n-1} k(x_k - x_{k+1})^2 + \sum_{k=1}^{n-2} kx_{k+1}^2 - \sum_{k=1}^{n-1} kx_{k+1}^2 \\ &= (2n - 1)x_n^2 + \sum_{k=1}^{n-1} k(x_k - x_{k+1})^2 - (n - 1)x_n^2 \\ &= \sum_{k=1}^{n-1} k(x_k - x_{k+1})^2 + nx_n^2. \end{aligned}$$

soit :

$$q(x) = \sum_{k=1}^n k\ell_k^2(x)$$

où les formes linéaires ℓ_k sont définies par :

$$\begin{cases} \ell_k(x) = x_k - x_{k+1} & (1 \leq k \leq n-1) \\ \ell_n(x) = x_n \end{cases}$$

Il est facile de vérifier que ces formes linéaires sont indépendantes.

(b) On en déduit que $\text{rg}(q) = n$, $\ker(q) = \{0\}$ et $\text{sgn}(q) = (n, 0)$.

3.

(a) On a :

$$Q(x, y) = \sum_{k=1}^n (y_k - x_k)^2 - \sum_{k=1}^n x_k^2$$

soit

$$Q(x, y) = \sum_{k=1}^n L_k^2(x, y) - \sum_{k=n+1}^{2n} L_k^2(x, y)$$

où les formes linéaires L_k sont définies par :

$$\begin{cases} L_k(x, y) = y_k - x_k & (1 \leq k \leq n) \\ L_k(x, y) = x_k & (k+1 \leq k \leq 2n) \end{cases}$$

Il est facile de vérifier que ces formes linéaires sont indépendantes.

(b) On en déduit que $\text{rg}(Q) = 2n$, $\ker(Q) = \{0\}$ et $\text{sgn}(Q) = (n, n)$.

4.

(a) On a $x_1 = y_1$ et pour $k \geq 2$, de $ky_k = \sum_{j=1}^k x_j$, on déduit que :

$$x_k = ky_k - (k-1)y_{k-1}.$$

(b) En posant $y_{-1} = 0$, on a :

$$\begin{aligned} Q(x, y) &= \sum_{k=1}^n (y_k - 2x_k) y_k \\ &= \sum_{k=1}^n (y_k - 2(ky_k - (k-1)y_{k-1})) y_k \\ &= \sum_{k=1}^n ((1-2k)y_k + 2(k-1)y_{k-1}) y_k \\ &= \sum_{k=1}^n (1-2k)y_k^2 + 2 \sum_{k=1}^n (k-1)y_{k-1}y_k \end{aligned}$$

soit :

$$Q(x, y) = \sum_{k=1}^n (1-2k)y_k^2 + 2 \sum_{k=1}^{n-1} ky_k y_{k+1} = -q(y).$$

(c) Comme q est positive, on a :

$$Q(x, y) = \sum_{k=1}^n (y_k^2 - 2x_k y_k) = -q(y) \leq 0$$

soit :

$$\sum_{k=1}^n y_k^2 \leq \sum_{k=1}^n 2x_k y_k.$$

En utilisant l'inégalité de Cauchy-Schwarz dans \mathbb{R}^n , on a :

$$\sum_{k=1}^n y_k^2 \leq 2 \sum_{k=1}^n x_k y_k \leq 2 \sqrt{\sum_{k=1}^n x_k^2} \sqrt{\sum_{k=1}^n y_k^2}$$

et :

$$\sum_{k=1}^n y_k^2 \leq 4 \sum_{k=1}^n x_k^2.$$

(d) Résulte de ce qui précède.

On peut montrer que l'égalité est réalisée si, et seulement si, $(x_n)_{n \geq 1}$ est la suite nulle (voir RMS, Mai-Juin 1996, page 973).

Dans l'espace $\mathcal{C}^0([a, b], \mathbb{R})$ des fonctions continues de $[a, b]$ dans \mathbb{R} muni du produit scalaire $(f, g) \mapsto \int_a^b f(t) g(t) dt$, l'inégalité de Cauchy-Schwarz s'écrit :

$$\left(\int_a^b f(t) g(t) dt \right)^2 \leq \int_a^b f^2(t) dt \int_a^b g^2(t) dt.$$

De cette inégalité, on peut déduire des inégalités intéressantes.

Exercice 12.12 Soit $f \in \mathcal{C}^0([a, b], \mathbb{R})$. Montrer que :

$$\left(\int_a^b f(t) dt \right)^2 \leq (b-a) \int_a^b f^2(t) dt$$

Dans quel cas a-t-on égalité ?

Solution 12.12 L'inégalité de Cauchy-Schwarz nous donne :

$$\left(\int_a^b f(t) \cdot 1 dt \right)^2 \leq \int_a^b f^2(t) dt \int_a^b 1 dt = (b-a) \int_a^b f^2(t) dt$$

l'égalité étant réalisée si, et seulement si, la fonction f est constante.

Exercice 12.13 Soit $f \in \mathcal{C}^0([a, b], \mathbb{R}_+^*)$. Montrer que $\left(\int_a^b \frac{1}{f(t)} dt \right) \left(\int_a^b f(t) dt \right) \geq (b-a)^2$.

Dans quel cas a-t-on égalité ?

Solution 12.13 L'inégalité de Cauchy-Schwarz nous donne :

$$(b-a)^2 = \left(\int_a^b \sqrt{f}(t) \cdot \frac{1}{\sqrt{f}(t)} dt \right)^2 \leq \int_a^b f(t) dt \int_a^b \frac{1}{f(t)} dt$$

l'égalité étant réalisée si, et seulement si, il existe un réel λ tel que $\sqrt{f} = \lambda \frac{1}{\sqrt{f}}$, ce qui équivaut à dire que f est constante.

Exercice 12.14 Soit $f \in \mathcal{C}^1([a, b], \mathbb{R})$ telle que $f(a) = 0$. Montrer que :

$$\int_a^b |f(t)|^2 dt \leq \frac{(b-a)^2}{2} \int_a^b |f'(t)|^2 dt.$$

Solution 12.14 Pour tout $t \in]a, b]$, on a :

$$|f(t)|^2 = \left(\int_a^t f'(x) dx \right)^2 \leq \int_a^t 1 dx \int_a^t |f'(x)|^2 dx \leq (t-a) \int_a^t |f'(x)|^2 dx$$

et en intégrant :

$$\int_a^b |f(t)|^2 dt \leq \int_a^b |f'(t)|^2 dt \int_a^b (t-a) dt = \frac{(b-a)^2}{2} \int_a^b |f'(t)|^2 dt.$$

Pour $f \in \mathcal{C}^1([a, b], \mathbb{R})$ sans hypothèse sur $f(a)$, la fonction g définie par $g(x) = f(x) - f(a)$ vérifie les hypothèses de l'exercice et avec $g(a) = 0$, $g' = f'$, on obtient l'inégalité :

$$\int_a^b |f(t) - f(a)|^2 dt \leq \frac{(b-a)^2}{2} \int_a^b |f'(t)|^2 dt$$

Une conséquence importante de l'inégalité de Cauchy-Schwarz est l'inégalité triangulaire de Minkowski.

Théorème 12.3 (Inégalité de Minkowski) Pour tous x, y dans E on a :

$$\|x + y\| \leq \|x\| + \|y\|,$$

l'égalité étant réalisée si, et seulement si, $x = 0$ ou $x \neq 0$ et $y = \lambda x$ avec $\lambda \geq 0$ (on dit que x et y sont positivement liés).

Démonstration. Si $x = 0$, on a alors l'égalité pour tout $y \in E$.

Si $x \neq 0$ et $y = \lambda x$ avec $\lambda \in \mathbb{R}$, on a :

$$\|x + y\| = |1 + \lambda| \|x\| \leq (1 + |\lambda|) \|x\| = \|x\| + \|\lambda x\| = \|x\| + \|y\|,$$

l'égalité étant réalisée pour $\lambda \geq 0$. Pour $\lambda < 0$, l'inégalité est stricte puisque dans ce cas $|1 + \lambda| < 1 + |\lambda| = 1 - \lambda$.

On suppose que x est non nul et y non lié à x . On a :

$$\|x + y\|^2 = \|x\|^2 + 2 \langle x | y \rangle + \|y\|^2$$

et avec l'inégalité de Cauchy-Schwarz :

$$\|x + y\|^2 < \|x\|^2 + 2 \|x\| \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$$

ce qui équivaut à $\|x + y\| < \|x\| + \|y\|$. ■

L'inégalité de Minkowski ajoutée aux propriétés de positivité ($\|x\| > 0$ pour tout $x \neq 0$) et d'homogénéité ($\|\lambda x\| = |\lambda| \|x\|$ pour tout réel λ et tout vecteur x) se traduit en disant que l'application $x \mapsto \|x\| = \sqrt{\langle x|x \rangle}$ définit une norme sur E .

De cette inégalité, on déduit l'inégalité suivante :

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

Par récurrence, on montre facilement que pour tous vecteurs x_1, \dots, x_p , on a :

$$\|x_1 + \dots + x_p\| \leq \|x_1\| + \dots + \|x_p\|.$$

Sur \mathbb{R}^n muni du produit scalaire canonique, l'inégalité de Minkowski prend la forme suivante :

$$\sqrt{\sum_{k=1}^n (x_k + y_k)^2} \leq \sqrt{\sum_{k=1}^n x_k^2} + \sqrt{\sum_{k=1}^n y_k^2}$$

Dans l'espace $\mathcal{C}^0([a, b], \mathbb{R})$ des fonctions continues de $[a, b]$ dans \mathbb{R} muni du produit scalaire $(f, g) \mapsto \int_a^b f(t)g(t)dt$, l'inégalité de Minkowski s'écrit :

$$\sqrt{\int_a^b (f(t) + g(t))^2 dt} \leq \sqrt{\int_a^b f^2(t) dt} + \sqrt{\int_a^b g^2(t) dt}.$$

12.3 Orthogonalité

Définition 12.4 On dit que deux vecteurs x et y appartenant à E sont orthogonaux si $\langle x | y \rangle = 0$.

Cette définition sera justifiée d'un point de vue géométrique en utilisant l'inégalité de Cauchy-Schwarz au paragraphe 13.1.

Théorème 12.4 (Pythagore) Les vecteurs x et y sont orthogonaux dans E si, et seulement si

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

On montre facilement par récurrence sur $p \geq 2$, que si x_1, \dots, x_p sont deux à deux orthogonaux, on a alors :

$$\left\| \sum_{k=1}^p x_k \right\|^2 = \sum_{k=1}^p \|x_k\|^2$$

Définition 12.5 On appelle famille orthogonale dans E toute famille $(e_i)_{i \in I}$ de vecteurs de E telle que $\langle e_i | e_j \rangle = 0$ pour tous $i \neq j$ dans I . Si de plus $\|e_i\| = 1$ pour tout $i \in I$, on dit alors que cette famille est orthonormée ou orthonormale.

Définition 12.6 L'orthogonal d'une partie non vide X de E est l'ensemble :

$$X^\perp = \{y \in E \mid \forall x \in X, \langle x | y \rangle = 0\}.$$

Il est facile de vérifier que X^\perp est un sous espace vectoriel de E .

Théorème 12.5 Une famille orthogonale de vecteurs non nuls de E est libre.

Démonstration. Si $(e_i)_{i \in I}$ est une telle famille et si $\sum_{j \in J} \lambda_j e_j = 0$ où J est une partie finie de I on a alors pour tout $k \in J$:

$$0 = \left\langle \sum_{j \in J} \lambda_j e_j \mid e_k \right\rangle = \lambda_k \|e_k\|^2,$$

avec $\|e_k\| \neq 0$ et nécessairement $\lambda_k = 0$. ■

Exercice 12.15 Montrer que la famille $\{\cos(nt), \sin(mt) \mid (n, m) \in \mathbb{N} \times \mathbb{N}^*\}$ est orthogonale dans l'espace vectoriel \mathcal{F} des fonctions continues et 2π -périodiques sur \mathbb{R} muni du produit scalaire $(f, g) \mapsto \langle f \mid g \rangle = \int_{-\pi}^{\pi} f(t) g(t) dt$ défini sur

Solution 12.15 Pour $n \neq m$ dans \mathbb{N} , on a :

$$\int_{-\pi}^{\pi} \cos(nt) \cos(mt) dt = \frac{1}{2} \int_{-\pi}^{\pi} (\cos((n+m)t) + \cos((n-m)t)) dt = 0,$$

pour $n \neq m$ dans \mathbb{N}^* , on a :

$$\int_{-\pi}^{\pi} \sin(nt) \sin(mt) dt = \frac{1}{2} \int_{-\pi}^{\pi} (\cos((n-m)t) - \cos((n+m)t)) dt = 0$$

et pour $(n, m) \in \mathbb{N} \times \mathbb{N}^*$, on a :

$$\int_{-\pi}^{\pi} \cos(nt) \sin(mt) dt = \frac{1}{2} \int_{-\pi}^{\pi} (\sin((n+m)t) - \sin((n-m)t)) dt = 0.$$

Pour $n = 0$, on a :

$$\int_{-\pi}^{\pi} dt = 2\pi$$

et pour $n \geq 1$:

$$\begin{cases} \int_{-\pi}^{\pi} \cos^2(nt) dt = \frac{1}{2} \int_{-\pi}^{\pi} (\cos(2nt) + 1) dt = \pi, \\ \int_{-\pi}^{\pi} \sin^2(nt) dt = \frac{1}{2} \int_{-\pi}^{\pi} (1 - \cos(2nt)) dt = \pi. \end{cases}$$

De l'exercice précédent, on déduit que la famille de fonctions :

$$\left\{ \frac{1}{\sqrt{2\pi}} \right\} \cup \left\{ \frac{1}{\sqrt{\pi}} \cos(nt), \frac{1}{\sqrt{\pi}} \sin(mt) \mid (n, m) \in \mathbb{N}^* \times \mathbb{N}^* \right\}$$

est orthonormée dans \mathcal{F} .

Pour tout $n \in \mathbb{N}^*$, la famille :

$$\mathcal{T}_n = \left\{ \frac{1}{\sqrt{2\pi}} \right\} \cup \left\{ \frac{\cos(jt)}{\sqrt{\pi}}, \frac{\sin(kt)}{\sqrt{\pi}} \mid 1 \leq j, k \leq n \right\}$$

est une base orthonormée de l'espace \mathcal{P}_n des polynômes trigonométriques de degré inférieur ou égal à n .

Exercice 12.16 Étant donnée une famille $(x_i)_{0 \leq i \leq n}$ de $n+1$ réels deux à deux distincts, on munit $\mathbb{R}_n[x]$ du produit scalaire :

$$(P, Q) \mapsto \langle P | Q \rangle = \sum_{i=0}^n P(x_i) Q(x_i).$$

Montrer que la famille $(L_i)_{0 \leq i \leq n}$ des polynômes de Lagrange définie par :

$$L_i(x) = \prod_{\substack{k=0 \\ k \neq i}}^n \frac{x - x_k}{x_i - x_k} \quad (0 \leq i \leq n)$$

est une base orthonormée de $\mathbb{R}_n[x]$.

Solution 12.16 Pour i, j compris entre 1 et n , on a :

$$\langle L_i | L_j \rangle = \sum_{k=0}^n L_i(x_k) L_j(x_k) = L_i(x_j) = \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

La famille $(L_i)_{0 \leq i \leq n}$ est orthonormée, donc libre et comme elle est formée de $n+1$ polynômes, c'est une base de $\mathbb{R}_n[x]$.

12.4 Le procédé d'orthogonalisation de Gram-Schmidt

Théorème 12.6 (orthonormalisation de Gram-Schmidt) Pour toute famille libre $(x_i)_{1 \leq i \leq p}$ dans E , il existe une unique famille orthonormée $(e_i)_{1 \leq i \leq p}$ dans E telle que :

$$\forall k \in \{1, 2, \dots, p\}, \begin{cases} \text{Vect}\{e_1, \dots, e_k\} = \text{Vect}\{x_1, \dots, x_k\}, \\ \langle x_k | e_k \rangle > 0. \end{cases}$$

Démonstration. On procède par récurrence sur $p \geq 1$.

Pour $p = 1$, on a nécessairement $e_1 = \lambda_1 x_1$ avec $\lambda_1 \in \mathbb{R}^*$ et $1 = \|e_1\|^2 = \lambda_1^2 \|x_1\|^2$, donc $\lambda_1^2 = \frac{1}{\|x_1\|^2}$ ce qui donne deux solutions pour λ_1 . La condition supplémentaire $\langle x_1 | e_1 \rangle > 0$

entraîne $\lambda_1 > 0$ et on obtient ainsi l'unique solution $e_1 = \frac{1}{\|x_1\|} x_1$.

Supposons $p \geq 2$ et construite la famille orthonormée $(e_i)_{1 \leq i \leq p-1}$ vérifiant les conditions :

$$\forall k \in \{1, 2, \dots, p-1\}, \begin{cases} \text{Vect}\{e_1, \dots, e_k\} = \text{Vect}\{x_1, \dots, x_k\}, \\ \langle x_k | e_k \rangle > 0. \end{cases}$$

Si $(e'_1, e'_2, \dots, e'_{p-1}, e_p)$ est une solution à notre problème on a alors nécessairement $e'_k = e_k$ pour tout k compris entre 1 et $p-1$ (unicité pour le cas $p-1$). La condition $\text{Vect}\{e_1, \dots, e_p\} = \text{Vect}\{x_1, \dots, x_p\}$ entraîne :

$$e_p = \sum_{j=1}^{p-1} \lambda_j e_j + \lambda_p x_p.$$

Avec les conditions d'orthogonalité :

$$\forall j \in \{1, \dots, p-1\}, \langle e_p | e_j \rangle = 0,$$

on déduit que :

$$\lambda_j + \lambda_p \langle x_p | e_j \rangle = 0 \quad (1 \leq j \leq p-1)$$

et :

$$e_p = \lambda_p \left(x_p - \sum_{j=1}^{p-1} \langle x_p | e_j \rangle e_j \right) = \lambda_p y_p.$$

Du fait que $x_p \notin \text{Vect} \{x_1, \dots, x_{p-1}\} = \text{Vect} \{e_1, \dots, e_{p-1}\}$ on déduit que $y_p \neq 0$ et la condition $\|e_p\| = 1$ donne :

$$|\lambda_p| = \frac{1}{\|y_p\|}.$$

La condition supplémentaire :

$$0 < \langle x_p | e_p \rangle = \left\langle \frac{1}{\lambda_p} \left(e_p - \sum_{j=1}^{p-1} \lambda_j e_j \right) | e_p \right\rangle = \frac{1}{\lambda_p}$$

entraîne $\lambda_p > 0$. Ce qui donne en définitive une unique solution pour e_p . ■

La construction d'une famille orthonormée $(e_i)_{1 \leq i \leq p}$ peut se faire en utilisant l'algorithme suivant :

$$\begin{cases} y_1 = x_1, & e_1 = \frac{1}{\|y_1\|} y_1 \\ y_k = x_k - \sum_{j=1}^{k-1} \langle x_k | e_j \rangle e_j, & e_k = \frac{1}{\|y_k\|} y_k, \quad (k = 2, \dots, p) \end{cases}$$

Le calcul de $\|y_k\|$ peut être simplifié en écrivant que :

$$\begin{aligned} \|y_k\|^2 &= \left\langle y_k | x_k - \sum_{j=1}^{k-1} \langle x_k | e_j \rangle e_j \right\rangle \\ &= \langle y_k | x_k \rangle = \left\langle x_k - \sum_{j=1}^{k-1} \langle x_k | e_j \rangle e_j | x_k \right\rangle \\ &= \|x_k\|^2 - \sum_{j=1}^{k-1} \langle x_k | e_j \rangle^2 \end{aligned}$$

(y_k est orthogonal à e_j pour $1 \leq j \leq k-1$). Les $\langle x_k | e_j \rangle$ étant déjà calculés (pour obtenir y_k), il suffit donc de calculer $\|x_k\|^2$. En fait le calcul de $\langle y_k | x_k \rangle$ est souvent plus rapide.

Corollaire 12.1 *Si F est un sous-espace vectoriel de dimension finie ou infinie dénombrable de E , alors il existe une base orthonormée pour F .*

Démonstration. On raisonne par récurrence en utilisant le théorème de Gram-Schmidt. ■

Si E est un espace euclidien de dimension finie et $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E , alors tout vecteur $x \in E$ s'écrit $x = \sum_{k=1}^n \langle x | e_k \rangle e_k = \sum_{k=1}^n x_k e_k$ et on a pour tous vecteurs x, y dans E , en notant X la matrice de x dans la base \mathcal{B} :

$$\langle x | y \rangle = \sum_{k=1}^n \langle x | e_k \rangle \langle y | e_k \rangle = \sum_{k=1}^n x_k y_k = {}^t X Y$$

et :

$$\|x\|^2 = \sum_{k=1}^n \langle x | e_k \rangle^2 = \sum_{k=1}^n x_k^2.$$

Ces égalités sont des cas particuliers des égalités de Parseval valables de manière plus générale dans les espaces de Hilbert.

Théorème 12.7 Si E est un espace euclidien de dimension $n \geq 1$, $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ sont deux bases orthonormées de E , alors la matrice de passage P de \mathcal{B} à \mathcal{B}' est telle que $P^{-1} = {}^tP$. En particulier, on a $\det(P) = \pm 1$.

Démonstration. Les colonnes de la matrice P sont formées des vecteurs colonnes E'_1, \dots, E'_n , où E'_j est la matrice de e'_j dans la base \mathcal{B} et on a :

$$\begin{aligned} {}^tPP &= \begin{pmatrix} {}^tE'_1 \\ \vdots \\ {}^tE'_n \end{pmatrix} (E'_1, \dots, E'_n) = (({}^tE'_i E'_j))_{1 \leq i, j \leq n} \\ &= ((\langle e'_i | e'_j \rangle))_{1 \leq i, j \leq n} = ((\delta_{ij}))_{1 \leq i, j \leq n} = I_n \end{aligned}$$

ce équivaut à dire que $P^{-1} = {}^tP$.

On a alors :

$$1 = \det(I_n) = \det({}^tPP) = \det({}^tP) \det(P) = \det^2(P)$$

et $\det(P) = \pm 1$. ■

Définition 12.7 On appelle matrice orthogonale toute matrice réelle d'ordre n inversible telle que $P^{-1} = {}^tP$.

La matrice de passage d'une base orthonormée \mathcal{B} de E à une autre base orthonormée \mathcal{B}' est donc une matrice orthogonale et réciproquement une telle matrice est la matrice de passage d'une base orthonormée de E à une autre.

Nous retrouverons cette notion de matrice orthogonale au paragraphe 13.10.

Exercice 12.17 Soient $(E, \langle \cdot | \cdot \rangle)$ un espace euclidien et u un automorphisme de E .

1. Montrer que l'application :

$$\varphi : (x, y) \mapsto \langle u(x) | u(y) \rangle$$

définit un produit scalaire sur E .

2. Dans le cas où E est de dimension finie, donner la matrice de φ dans une base orthonormée de E en fonction de celle de u .

Solution 12.17

1. De la linéarité de u , on déduit que φ est bilinéaire symétrique.

Pour $x \in E$, on a $\varphi(x, x) = \|u(x)\|^2 \geq 0$ et $\varphi(x, x) = 0$ équivaut à $x \in \ker(u)$, soit à $x = 0$ puisque u est bijectif. Donc φ est un produit scalaire sur E .

2. Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E et A la matrice de u dans cette base. Pour x, y dans E , on a :

$$\varphi(x, y) = \langle u(x) | u(y) \rangle = {}^t(AX)(AY) = {}^tX({}^tAA)Y$$

et la matrice de φ dans \mathcal{B} est tAA .

Exercice 12.18 Montrer que l'application $(P, Q) \mapsto \langle P | Q \rangle = \int_0^2 (2-t) P(t) Q(t) dt$ définit un produit scalaire sur $\mathbb{R}_2[x]$. Donner une base orthonormée.

Solution 12.18 La fonction $t \mapsto 2-t$ étant à valeurs strictement positives sur $]0, 2[$, il est facile de vérifier que $\langle \cdot | \cdot \rangle$ est un produit scalaire.

En utilisant l'algorithme de Gram-Schmidt, on définit la base orthonormée $(P_i)_{0 \leq i \leq 2}$ par :

$$\left\{ \begin{array}{l} Q_0 = 1, \quad \|Q_0\|^2 = \int_0^2 (2-t) dt = 2, \quad P_0 = \frac{1}{\sqrt{2}} \\ Q_1 = x - \langle x | P_0 \rangle P_0 = x - \frac{2}{3}, \\ \|Q_1\|^2 = \langle Q_1 | x \rangle = \frac{4}{9}, \quad P_1 = \frac{3}{2}x - 1, \\ Q_2 = x^2 - \langle x^2 | P_0 \rangle P_0 - \langle x^2 | P_1 \rangle P_1 = x^2 - \frac{8}{5}x + \frac{2}{5}, \\ \|Q_2\|^2 = \langle Q_2 | x^2 \rangle = \frac{8}{75}, \quad P_2 = \frac{\sqrt{6}}{4} (5x^2 - 8x + 2) \end{array} \right.$$

Une base orthonormée de $\mathbb{R}_2[x]$ est donc :

$$\left(\frac{1}{\sqrt{2}}, \frac{3}{2}x - 1, \frac{\sqrt{6}}{4} (5x^2 - 8x + 2) \right)$$

Exercice 12.19 Montrer que l'application $(P, Q) \mapsto \int_{-1}^1 P(t) Q(t) dt$ définit un produit scalaire sur $\mathbb{R}_2[x]$. Donner la matrice dans la base canonique et déterminer une base orthonormée.

Solution 12.19 On sait déjà que $\langle \cdot | \cdot \rangle$ est un produit scalaire.

En utilisant l'algorithme de Gram-Schmidt, on définit la base orthonormée $(P_i)_{0 \leq i \leq 2}$ par :

$$\left\{ \begin{array}{l} Q_0 = 1, \quad \|Q_0\|^2 = \int_{-1}^1 dt = 2, \quad P_0 = \frac{1}{\sqrt{2}} \\ Q_1 = x - \langle x | P_0 \rangle P_0 = x, \\ \|Q_1\|^2 = \langle Q_1 | x \rangle = \frac{2}{3}, \quad P_1 = \frac{\sqrt{3}}{\sqrt{2}}x, \\ Q_2 = x^2 - \langle x^2 | P_0 \rangle P_0 - \langle x^2 | P_1 \rangle P_1 = x^2 - \frac{1}{3}, \\ \|Q_2\|^2 = \langle Q_2 | x^2 \rangle = \frac{8}{45}, \quad P_2 = \frac{3}{4}\sqrt{10} \left(x^2 - \frac{1}{3} \right) \end{array} \right.$$

Une base orthonormée de $\mathbb{R}_2[x]$ est donc :

$$\left(\frac{1}{\sqrt{2}}, \frac{\sqrt{3}}{\sqrt{2}}x, \frac{3}{4}\sqrt{10} \left(x^2 - \frac{1}{3} \right) \right)$$

Exercice 12.20 On note $\langle \cdot | \cdot \rangle$ le produit scalaire défini sur $\mathbb{R}[X]$ par :

$$(P, Q) \mapsto \langle P | Q \rangle = \int_{-1}^{+1} \frac{P(t) Q(t)}{\sqrt{1-t^2}} dt.$$

1. Montrer que :

$$\forall n \in \mathbb{N}, \int_0^1 \frac{t^{2n}}{\sqrt{1-t^2}} dt = \frac{(2n)!}{2^{2n} (n!)^2} \frac{\pi}{2}.$$

2. En utilisant le procédé d'orthogonalisation de Gram-Schmidt, déduire de la base canonique $(1, X, X^2)$ de $\mathbb{R}_2[X]$, une base orthonormée de $\mathbb{R}_2[X]$.

Solution 12.20

1. Pour tout entier naturel n , on note :

$$T_n = \int_0^1 \frac{t^{2n}}{\sqrt{1-t^2}} dt.$$

La fonction à intégrer est positive et équivalente au voisinage de 1 à la fonction $\frac{1}{\sqrt{2}\sqrt{1-t}}$, elle est donc intégrable sur $[0, 1]$.

On a :

$$T_0 = \int_0^1 \frac{1}{\sqrt{1-t^2}} dt = \arcsin(1) = \frac{\pi}{2}$$

et pour $n \geq 1$, une intégration par parties donne :

$$\begin{aligned} T_n &= \int_0^1 t^{2n-1} \frac{t}{\sqrt{1-t^2}} dt = (2n-1) \int_0^1 x^{2n-2} \sqrt{1-t^2} dt \\ &= (2n-1) \int_0^1 \frac{t^{2(n-1)}}{\sqrt{1-t^2}} (1-t^2) dx = (2n-1) (T_{n-1} - T_n). \end{aligned}$$

On a donc la relation de récurrence :

$$\forall n \geq 1, T_n = \frac{2n-1}{2n} T_{n-1}$$

et avec la valeurs initiale T_0 , on déduit que :

$$\begin{aligned} T_n &= \frac{2n-1}{2n} \frac{2n-3}{2(n-1)} \cdots \frac{3}{4} \frac{1}{2} \frac{\pi}{2} \\ &= \frac{2n}{2n} \frac{2n-1}{2n} \frac{2n-2}{2(n-1)} \frac{2n-3}{2(n-1)} \cdots \frac{3}{4} \frac{2}{2} \frac{1}{2} \frac{\pi}{2} \\ &= \frac{(2n)!}{2^{2n} (n!)^2} \frac{\pi}{2}. \end{aligned}$$

2. On pose $Q_0 = 1$ et on a

$$\|Q_0\|^2 = \int_{-1}^1 \frac{1}{\sqrt{1-t^2}} dt = 2 \int_0^1 \frac{1}{\sqrt{1-t^2}} dt = \pi.$$

Donc :

$$P_0 = \frac{1}{\|Q_0\|} Q_0 = \frac{1}{\sqrt{\pi}}.$$

Puis $Q_1(X) = X - \lambda P_0$ où λ est tel que $\langle P_0 | Q_0 \rangle = 0$, ce qui donne :

$$\lambda = \langle P_0 | X \rangle = \int_{-1}^1 \frac{t}{\sqrt{1-t^2}} dt = 0$$

par parité. On a $Q_1(X) = X$ et :

$$\|Q_1\|^2 = \int_{-1}^1 \frac{t^2}{\sqrt{1-t^2}} dt = 2 \int_0^1 \frac{t^2}{\sqrt{1-t^2}} dt = \frac{2}{2^2} \pi = \frac{\pi}{2}.$$

Donc :

$$P_1 = \frac{1}{\|Q_1\|} Q_1 = \sqrt{\frac{2}{\pi}} X.$$

Puis $Q_2(X) = X^2 - \lambda P_0 - \mu P_1$ où λ, μ sont tels que $\langle P_0 | Q_2 \rangle = \langle P_1 | Q_2 \rangle = 0$, ce qui donne :

$$\lambda = \langle P_0 | X^2 \rangle = \frac{1}{\sqrt{\pi}} \int_{-1}^1 \frac{t^2}{\sqrt{1-t^2}} dt = \frac{1}{\sqrt{\pi}} \frac{\pi}{2} = \frac{\sqrt{\pi}}{2}$$

et :

$$\mu = \langle P_1 | X^2 \rangle = \sqrt{\frac{2}{\pi}} \int_{-1}^1 \frac{t^3}{\sqrt{1-t^2}} dt = 0$$

par parité. On a $Q_2(X) = X^2 - \lambda P_0 = X^2 - \frac{\sqrt{\pi}}{2} \frac{1}{\sqrt{\pi}} = X^2 - \frac{1}{2}$ et :

$$\begin{aligned} \|Q_2\|^2 &= \langle Q_2 | X^2 - \lambda P_0 \rangle = \langle Q_2 | X^2 \rangle \\ &= \int_{-1}^1 \frac{t^4}{\sqrt{1-t^2}} dt - \frac{1}{2} \int_{-1}^1 \frac{t^2}{\sqrt{1-t^2}} dt \\ &= \frac{4!}{2^4 2^2} \pi - \frac{1}{2} \frac{\pi}{2} = \frac{\pi}{8}. \end{aligned}$$

Donc :

$$P_2 = \frac{1}{\|Q_2\|} Q_2 = \sqrt{\frac{2}{\pi}} (2X^2 - 1).$$

Conclusion, une base orthonormée de $\mathbb{R}_2[X]$ est donnée par :

$$(P_0, P_1, P_2) = \left(\frac{1}{\sqrt{\pi}}, \sqrt{\frac{2}{\pi}} X, \sqrt{\frac{2}{\pi}} (2X^2 - 1) \right)$$

Exercice 12.21 Pour tout entier n positif ou nul, on note $\pi_{2n}(x) = (x^2 - 1)^n$ et $R_n = \pi_{2n}^{(n)}$. On munit $E = \mathbb{R}[x]$ du produit scalaire défini par :

$$\forall (P, Q) \in E^2, \langle P | Q \rangle = \int_{-1}^1 P(x) Q(x) dx.$$

1. Montrer que R_n est un polynôme de degré n de la parité de n .
2. Calculer, pour $n \geq 1$, les coefficients de x^n et x^{n-1} dans R_n .
3. Montrer que, pour $n \geq 1$, pour tout entier k compris entre 1 et n et tout $P \in \mathbb{R}[x]$, on a :

$$\int_{-1}^1 \pi_{2n}^{(k)}(t) P(t) dt = - \int_{-1}^1 \pi_{2n}^{(k-1)}(t) P'(t) dt.$$

4. Montrer que, pour $n \geq 1$ et tout polynôme $P \in \mathbb{R}_{n-1}[x]$, on a $\langle R_n | P \rangle = 0$.
5. En déduire que la famille $(R_n)_{n \in \mathbb{N}}$ est orthogonale dans E .

6. Calculer $\|R_n\|$, pour tout entier n positif ou nul. Les polynômes $P_n = \frac{1}{\|R_n\|} R_n$ sont les polynômes de Legendre normalisés.

Solution 12.21

1. Pour $n = 0$ on a $R_0 = \pi_0 = 1$. Pour $n \geq 1$ le polynôme :

$$\pi_{2n}(x) = \sum_{k=0}^n (-1)^{n-k} C_n^k x^{2k}$$

est de degré $2n$ et sa dérivée d'ordre n :

$$R_n(x) = \sum_{\frac{n}{2} \leq k \leq n} (-1)^{n-k} C_n^k \frac{(2k)!}{(2k-n)!} x^{2k-n}$$

est un polynôme de degré n .

Le polynôme π_{2n} est pair donc sa dérivée d'ordre n , R_n est de la parité de n .

2. Le coefficient dominant de R_n est $\beta_n^{(n)} = \frac{(2n)!}{n!}$ et le coefficient de x^{n-1} est nul du fait que R_n est de la parité de n .
3. Une intégration par parties donne, pour tout entier k compris entre 1 et n et tout $P \in \mathbb{R}[x]$:

$$\int_{-1}^1 \pi_{2n}^{(k)}(t) P(t) dt = \left[\pi_{2n}^{(k-1)}(t) P(t) \right]_{-1}^1 - \int_{-1}^1 \pi_{2n}^{(k-1)}(t) P'(t) dt$$

Et utilisant le fait que -1 et 1 sont racines d'ordre n du polynôme $\pi_{2n}(x) = (x-1)^n(x+1)^n$, on a $\pi_{2n}^{(k-1)}(\pm 1) = 0$, de sorte que :

$$\int_{-1}^1 \pi_{2n}^{(k)}(t) P(t) dt = - \int_{-1}^1 \pi_{2n}^{(k-1)}(t) P'(t) dt.$$

4. En effectuant n intégrations par parties, on obtient :

$$\int_{-1}^1 \pi_{2n}^{(n)}(t) P(t) dt = (-1)^n \int_{-1}^1 \pi_{2n}(t) P^{(n)}(t) dt$$

Pour $P \in \mathbb{R}_{n-1}[X]$, on a $P^{(n)} = 0$ et :

$$\langle R_n | P \rangle = \left\langle \pi_{2n}^{(n)} | P \right\rangle = \langle \pi_{2n} | P^{(n)} \rangle = 0.$$

5. Chaque polynôme R_k étant de degré k , on déduit de la question précédente que $\langle R_n | R_m \rangle = 0$ pour $0 \leq n < m$ et par symétrie $\langle R_n | R_m \rangle = 0$ pour $n \neq m$ dans \mathbb{N} . La famille $\{R_n | n \in \mathbb{N}\}$ est donc orthogonal dans $\mathbb{R}[x]$.

6. En utilisant 4. on a :

$$\begin{aligned} \|R_n\|^2 &= \int_{-1}^1 \pi_{2n}^{(n)}(t) R_n(t) dt = (-1)^n \int_{-1}^1 \pi_{2n}(t) R_n^{(n)}(t) dt \\ &= (-1)^n \beta_n^{(n)} n! \int_{-1}^1 \pi_{2n}(t) dt = (2n)! (-1)^n I_n \end{aligned}$$

où :

$$I_n = \int_{-1}^1 \pi_{2n}(t) dt = \int_{-1}^1 (t^2 - 1)^n dt.$$

Pour $n \geq 1$, on a :

$$I_n = \int_{-1}^1 (t^2 - 1)^{n-1} (t^2 - 1) dt = \int_{-1}^1 (t^2 - 1)^{n-1} t \cdot t dt - I_{n-1}$$

et une intégration par parties donne :

$$\begin{aligned} \int_{-1}^1 (t^2 - 1)^{n-1} t \cdot t dt &= \left[t \frac{1}{2n} (t^2 - 1)^n \right] - \int_{-1}^1 \frac{1}{2n} (t^2 - 1)^n dt \\ &= -\frac{1}{2n} I_n \end{aligned}$$

soit la relation de récurrence :

$$I_n = -\frac{1}{2n} I_n - I_{n-1}$$

soit $I_n = -\frac{2n}{2n+1} I_{n-1}$. Il en résulte que :

$$I_n = (-1)^n \frac{(2n)(2(n-1)) \cdots 2}{(2n+1)(2n-1) \cdots 1} I_0 = (-1)^n \frac{2^{2n} (n!)^2}{(2n+1)!} 2$$

et :

$$\|R_n\|^2 = (2n)! \frac{2^{2n} (n!)^2}{(2n+1)!} 2 = \frac{2}{2n+1} 2^{2n} (n!)^2$$

soit $\|R_n\| = 2^n n! \sqrt{\frac{2}{2n+1}}$.

12.5 Projection orthogonale sur un sous-espace de dimension finie

$(E, \langle \cdot | \cdot \rangle)$ est toujours un espace préhilbertien de dimension finie ou non.

Théorème 12.8 (projection orthogonale) *Soit F un sous espace vectoriel de dimension finie de E non réduit à $\{0\}$. Pour tout vecteur $x \in E$, il existe un unique vecteur y dans F tel que :*

$$\|x - y\| = d(x, F) = \inf_{z \in F} \|x - z\|.$$

Ce vecteur est également l'unique vecteur appartenant à F tel que $x - y \in F^\perp$. Son expression dans une base orthonormée $(e_i)_{1 \leq i \leq n}$ de F est donnée par :

$$y = \sum_{k=1}^n \langle x | e_k \rangle e_k$$

et on a :

$$\|x - y\|^2 = \|x\|^2 - \|y\|^2 = \|x\|^2 - \sum_{k=1}^n \langle x | e_k \rangle^2. \quad (12.1)$$

Démonstration. Soit $(e_i)_{1 \leq i \leq n}$ une base orthonormée de F (le théorème de Gram–Schmidt nous assure l'existence d'une telle base). Pour x dans E , on définit le vecteur $y \in F$ par :

$$y = \sum_{k=1}^n \langle x | e_k \rangle e_k.$$

On a alors $\langle x - y | e_j \rangle = 0$ pour tout $j \in \{1, \dots, n\}$, c'est-à-dire que $x - y \in F^\perp$. Le théorème de Pythagore donne alors, pour tout $z \in F$:

$$\begin{aligned} \|x - z\|^2 &= \|(x - y) + (y - z)\|^2 \\ &= \|x - y\|^2 + \|y - z\|^2 \geq \|x - y\|^2 \end{aligned}$$

et on a bien $\|x - y\| = d(x, F)$.

S'il existe un autre vecteur $u \in F$ tel que $\|x - u\| = d(x, F) = \delta$, de :

$$\delta^2 = \|x - u\|^2 = \|x - y\|^2 + \|y - u\|^2 = \delta^2 + \|y - u\|^2,$$

on déduit alors que $\|y - u\| = 0$ et $y = u$.

On sait déjà que le vecteur $y \in F$ est tel que $x - y \in F^\perp$. Supposons qu'il existe un autre vecteur $u \in F$ tel que $x - u \in F^\perp$, pour tout $z \in F$, on a alors :

$$\begin{aligned} \|x - z\|^2 &= \|(x - u) + (u - z)\|^2 \\ &= \|x - u\|^2 + \|u - z\|^2 \geq \|x - u\|^2, \end{aligned}$$

donc $\|x - u\| = d(x, F)$ et $u = y$ d'après ce qui précède.

La dernière égalité se déduit de :

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

■

Si x est un vecteur de E , alors le vecteur y de F qui lui est associé dans le théorème précédent est la meilleure approximation de x dans F . En considérant la caractérisation géométrique $x - y \in F^\perp$, on dit aussi que y est la projection orthogonale de x sur F .

On note $y = p_F(x)$. On a donc :

$$(y = p_F(x)) \Leftrightarrow (y \in F \text{ et } x - y \in F^\perp) \Leftrightarrow (y \in F \text{ et } \|x - y\| = d(x, F))$$

et dans une base orthonormée de F , une expression de p_F est :

$$\forall x \in E, p_F(x) = \sum_{k=1}^n \langle x | e_k \rangle e_k.$$

On dit que l'application p_F est la projection orthogonale de E sur F .

Remarque 12.1 Si $F = \{0\}$, on peut définir p_F et c'est l'application nulle. On suppose donc, a priori, F non réduit à $\{0\}$.

Dans le cas où E est de dimension finie et $F = E$, p_F est l'application identité.

Remarque 12.2 $p_F(x) = x$ équivaut à dire que $x \in F$ et $p_F(x) = 0$ équivaut à dire que $x \in F^\perp$.

Exemple 12.2 Si $D = \mathbb{R}a$ est une droite vectorielle, une base orthonormée de D est $\left(\frac{1}{\|a\|}a\right)$ et pour tout $x \in E$, on a $p_D(x) = \frac{\langle x | a \rangle}{\|a\|^2}a$.

De l'inégalité (12.1), on déduit que pour tout vecteur $x \in E$, on a :

$$\|p_F(x)\|^2 = \sum_{k=1}^n \langle x | e_k \rangle^2 \leq \|x\|^2.$$

Cette inégalité est l'inégalité de Bessel.

Exercice 12.22 On munit l'espace vectoriel $\mathbb{R}[x]$ du produit scalaire :

$$(P, Q) \mapsto \langle P | Q \rangle = \int_0^{+\infty} P(t) Q(t) e^{-t} dt.$$

1. Justifier la convergence des intégrales $\langle P | Q \rangle$ pour tous P, Q dans $\mathbb{R}[x]$ et le fait qu'on a bien un produit scalaire.
2. Construire une base orthonormée de $\mathbb{R}_3[x]$.
3. Soit $P = 1 + x + x^3$. Déterminer $Q \in \mathbb{R}_2[x]$ tel que $\|P - Q\|$ soit minimal.

Solution 12.22

1. On vérifie par récurrence que :

$$\forall k \in \mathbb{N}, \int_0^{+\infty} t^k e^{-t} dt = k!$$

et de ce résultat on déduit que l'application $\langle \cdot | \cdot \rangle$ est bien définie sur $\mathbb{R}[x]$. On vérifie ensuite facilement que c'est un produit scalaire.

2. En utilisant le procédé de Gram-Schmidt sur la base $(1, x, x^2, x^3)$ de $\mathbb{R}_3[x]$, on a :

$$\left\{ \begin{array}{l} Q_0 = 1, \|Q_0\|^2 = 1, P_0 = \frac{Q_0}{\|Q_0\|} = 1 \\ P_1 = x - \langle x | P_0 \rangle P_0 = x - 1, \|Q_1\|^2 = 1, P_1 = \frac{Q_1}{\|Q_1\|} = x - 1, \\ Q_2 = x^2 - \langle x^2 | P_0 \rangle P_0 - \langle x^2 | P_1 \rangle P_1 = x^2 - 4x + 2, \\ \|Q_2\|^2 = 4, P_2 = \frac{Q_2}{\|Q_2\|} = \frac{1}{2}(x^2 - 4x + 2), \\ Q_3 = x^3 - \langle x^3 | P_0 \rangle P_0 - \langle x^3 | P_1 \rangle P_1 - \langle x^3 | P_2 \rangle P_2 \\ = x^3 - 9x^2 + 18x - 6, \\ \|Q_3\|^2 = 36, P_3 = \frac{Q_3}{\|Q_3\|} = \frac{1}{6}(x^3 - 9x^2 + 18x - 6). \end{array} \right.$$

3. Le polynôme Q est la projection orthogonale de P sur $F = \mathbb{R}_2[x]$ donnée par :

$$Q = \sum_{k=0}^2 \langle P | P_k \rangle P_k.$$

Le calcul des $\langle P | P_k \rangle$ peut être évité en remarquant que dans la base orthonormée (P_0, P_1, P_2, P_3) de $E = \mathbb{R}_3[x]$, on a :

$$P = \sum_{k=0}^3 \langle P | P_k \rangle P_k = Q + \langle P | P_3 \rangle P_3$$

le coefficient $\langle P | P_3 \rangle$ s'obtenant en identifiant les coefficients de x^3 dans cette égalité (P est de degré 2 au plus), soit :

$$\langle P | P_3 \rangle = 6.$$

On a donc :

$$Q = P - \langle P | P_3 \rangle P_3 = 9x^2 - 17x + 7$$

et :

$$d(P, \mathbb{R}_2[x]) = \|P - Q\| = |\langle P | P_3 \rangle| = 6.$$

Il est parfois commode d'exprimer (12.1) sous la forme :

$$\inf_{(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n} \left\| x - \sum_{k=1}^n \lambda_k e_k \right\|^2 = \|x - y\|^2 = \|x\|^2 - \sum_{k=1}^n \langle x | e_k \rangle^2,$$

où $(e_i)_{1 \leq i \leq n}$ est un système orthonormé dans E et $x \in E$.

Exercice 12.23 Calculer $\inf_{(a,b) \in \mathbb{R}^2} \int_{-1}^1 (x^2 - ax - b)^2 dx$.

Solution 12.23 En munissant l'espace $E = \mathcal{C}^0([-1, 1])$ du produit scalaire :

$$\langle f, g \rangle = \int_{-1}^1 f(x) g(x) dx$$

on a :

$$M = \inf_{(a,b) \in \mathbb{R}^2} \int_{-1}^1 (x^2 - ax - b)^2 dx = \inf_{Q \in \mathbb{R}_1[x]} \|f - Q\|^2$$

où $f(x) = x^2$. Le théorème de projection orthogonale donne :

$$M = \|f - P\|^2 = \|f\|^2 - \|P\|^2$$

où P est la projection orthogonale de f sur $\mathbb{R}_1[x]$, soit $P = \langle f, P_0 \rangle P_0 + \langle f, P_1 \rangle P_1$ où (P_0, P_1) est une base orthonormée de $\mathbb{R}_1[x]$. Le procédé de Gram-Schmidt donne :

$$P_0(x) = \frac{1}{\sqrt{2}}, \quad P_1(x) = \frac{\sqrt{3}}{\sqrt{2}}x$$

et on a :

$$\langle f, P_0 \rangle = \frac{2}{3} \frac{1}{\sqrt{2}}, \quad \langle f, P_1 \rangle = 0$$

donc :

$$P(x) = \frac{1}{3}$$

et :

$$M = \frac{2}{5} - \frac{2}{9} = \frac{8}{45}$$

Remarque 12.3 Si $(e_i)_{1 \leq i \leq n}$ est une base (non nécessairement orthonormée) de F , alors la projection orthogonale d'un vecteur x de E sur F est le vecteur $y = \sum_{j=1}^n y_j e_j$, où les composantes y_j , pour j compris entre 1 et n , sont solutions du système linéaire :

$$\langle x - y \mid e_i \rangle = 0 \quad (1 \leq i \leq n),$$

soit :

$$\sum_{j=1}^n \langle e_i \mid e_j \rangle y_j = \langle x \mid e_i \rangle \quad (1 \leq i \leq n).$$

Ce système est appelé système d'équations normales.

Pour l'exercice précédent, $(1, x)$ est une base de $\mathbb{R}_1[x]$ et le système d'équations normales est :

$$\begin{cases} \langle 1 \mid 1 \rangle y_1 + \langle 1 \mid x \rangle y_2 = \langle x^2 \mid 1 \rangle \\ \langle x \mid 1 \rangle y_1 + \langle x \mid x \rangle y_2 = \langle x^2 \mid x \rangle \end{cases}$$

soit :

$$\begin{cases} 2y_1 = \frac{2}{3} \\ \frac{2}{3}y_2 = 0 \end{cases}$$

ce qui donne $y_1 = \frac{1}{3}$ et $y_2 = 0$, soit $P = \frac{1}{3}$ et $M = \|f\|^2 - \|P\|^2 = \frac{8}{45}$.

Exercice 12.24 Calculer $\inf_{(a,b) \in \mathbb{R}^2} \int_0^1 x^2 (\ln(x) - ax - b)^2 dx$.

Solution 12.24 On munit l'espace vectoriel $E = \mathcal{C}([0, 1])$ du produit scalaire :

$$(f, g) \mapsto \langle f \mid g \rangle = \int_0^1 f(x) g(x) dx$$

et on note f la fonction définie sur $[0, 1]$ par :

$$f(x) = \begin{cases} x \ln(x) & \text{si } x \in]0, 1], \\ 0 & \text{si } x = 0. \end{cases}$$

Avec $\lim_{x \rightarrow 0} x \ln(x) = 0$, on déduit que $f \in E$.

Avec ces notations il s'agit donc de calculer :

$$\delta^2 = d(f, F)^2 = \inf_{(a,b) \in \mathbb{R}^2} \|f - ax^2 - bx\|^2,$$

où $F = \text{Vect}\{x, x^2\}$. On sait que si (P_1, P_2) est une base orthonormée de F , alors :

$$\begin{aligned} \delta^2 &= \|f - \langle f \mid P_1 \rangle P_1 - \langle f \mid P_2 \rangle P_2\|^2 \\ &= \|f\|^2 - \langle f \mid P_1 \rangle^2 - \langle f \mid P_2 \rangle^2. \end{aligned}$$

Une telle base orthonormée s'obtient avec le procédé de Gram-Schmidt :

$$\begin{cases} P_1 = \sqrt{3}x, \\ P_2 = \sqrt{5}(4x^2 - 3x). \end{cases}$$

Puis avec :

$$\begin{cases} \forall n \in \mathbb{N}, \langle f | x^n \rangle = \int_0^1 x^{n+1} \ln(x) dx = -\frac{1}{(n+2)^2}, \\ \|f\|^2 = \int_0^1 x^2 \ln^2(x) dx = \frac{2}{27}, \end{cases}$$

on obtient :

$$\begin{cases} \langle f | P_1 \rangle = -\frac{\sqrt{3}}{9}, \\ \langle f | P_2 \rangle = \frac{\sqrt{5}}{12} \end{cases}$$

et :

$$\delta^2 = \frac{1}{2^4 3^3} = \frac{1}{432}.$$

La projection orthogonale de f sur F étant donnée par :

$$P = \langle f | P \rangle P_1 + \langle f | P_2 \rangle P_2 = \frac{5}{3}x^2 - \frac{19}{12}x.$$

On peut aussi déterminer cette projection orthogonale $P = ax^2 + bx$ en utilisant le système d'équations normales :

$$\begin{cases} \langle f - P | x \rangle = 0, \\ \langle f - P | x^2 \rangle = 0, \end{cases}$$

soit :

$$\begin{cases} 3a + 4b = -\frac{4}{3}, \\ 4a + 5b = -\frac{5}{4}, \end{cases}$$

ce qui donne $a = \frac{5}{3}$ et $b = -\frac{19}{12}$. Le minimum cherché est alors :

$$\delta^2 = \|f\|^2 - \|P\|^2 = \frac{2}{27} - \frac{31}{432} = \frac{1}{432}.$$

Sur l'espace vectoriel \mathcal{F} des fonctions continues et 2π -périodiques muni du produit scalaire :

$$(f, g) \mapsto \langle f | g \rangle = \int_{-\pi}^{\pi} f(x) g(x) dx,$$

la meilleure approximation, pour la norme déduite de ce produit scalaire, d'une fonction $f \in \mathcal{F}$ par un polynôme trigonométrique de degré inférieur ou égal à n est donnée par :

$$\begin{aligned} S_n(f) &= \left\langle f \left| \frac{c_0}{\sqrt{2\pi}} \right\rangle \frac{c_0}{\sqrt{2\pi}} + \sum_{k=1}^n \left\langle f \left| \frac{c_k}{\sqrt{\pi}} \right\rangle \frac{c_k}{\sqrt{\pi}} + \sum_{k=1}^n \left\langle f \left| \frac{s_k}{\sqrt{\pi}} \right\rangle \frac{s_k}{\sqrt{\pi}} \right. \\ &= \frac{1}{2\pi} \langle f | c_0 \rangle c_0 + \frac{1}{\pi} \sum_{k=1}^n \langle f | c_k \rangle c_k + \frac{1}{\pi} \sum_{k=1}^n \langle f | s_k \rangle s_k \end{aligned}$$

où $c_k : x \mapsto \cos(kx)$ pour $k \geq 0$ et $s_k : x \mapsto \sin(kx)$ pour $k \geq 1$. Soit :

$$S_n(f)(x) = \frac{a_0(f)}{2} + \sum_{k=1}^n a_k(f) \cos(kx) + \sum_{k=1}^n b_k(f) \sin(kx)$$

où les $a_k(f)$ et $b_k(f)$ sont les coefficients de Fourier trigonométriques de f définis par :

$$a_k(f) = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \cos(kt) dt \text{ et } b_k(f) = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin(kt) dt$$

L'opérateur S_n de projection orthogonale de \mathcal{F} sur l'espace \mathcal{P}_n des polynômes trigonométriques de degré inférieur ou égal à n est l'opérateur de Fourier.

La série :

$$a_0(f) + \sum (a_n(f) \cos(nx) + b_n(f) \sin(nx))$$

est la série de Fourier de f .

L'inégalité de Bessel s'écrit :

$$\left\langle f \mid \frac{c_0}{\sqrt{2\pi}} \right\rangle^2 + \sum_{k=1}^n \left\langle f \mid \frac{ck}{\sqrt{\pi}} \right\rangle^2 + \sum_{k=1}^n \left\langle f \mid \frac{sk}{\sqrt{\pi}} \right\rangle^2 \leq \|f\|^2$$

ou encore :

$$\frac{a_0^2(f)}{2} + \sum_{k=1}^n (a_k^2(f) + b_k^2(f)) \leq \frac{1}{\pi} \int_{-\pi}^{\pi} f^2(t) dt$$

Il en résulte que la série numérique $a_0^2(f) + \frac{1}{2} \sum (a_n^2(f) + b_n^2(f))$ converge avec :

$$\frac{a_0^2(f)}{2} + \sum_{n=1}^{+\infty} (a_n^2(f) + b_n^2(f)) \leq \frac{1}{\pi} \int_{-\pi}^{\pi} f^2(t) dt$$

(théorème de Bessel).

On peut montrer qu'on a fait l'égalité (théorème de Parseval).

De l'inégalité de Bessel, on déduit que $\lim_{n \rightarrow +\infty} a_n(f) = \lim_{n \rightarrow +\infty} b_n(f) = 0$ (théorème de Riemann-Lebesgue).

Exemple 12.3 Si $f \in \mathcal{F}$ est la fonction 2π -périodique, paire valant $x(\pi - x)$ sur $[0, \pi]$, on a $b_n(f) = 0$ pour tout $n \geq 1$ puisque f est paire et :

$$a_0(f) = \frac{2}{\pi} \int_0^{\pi} t(\pi - t) dt = \frac{\pi^2}{3}$$

$$\begin{aligned} a_n(f) &= \frac{2}{\pi} \int_0^{\pi} t(\pi - t) \cos(nt) dt \\ &= -\frac{2}{n^2} (1 + (-1)^n) = \begin{cases} 0 & \text{si } n = 2p + 1 \\ -\frac{1}{p^2} & \text{si } n = 2p \end{cases} \end{aligned}$$

pour $n \geq 1$.

L'identité de Parseval nous donne :

$$\frac{\pi^4}{18} + \sum_{p=1}^{+\infty} \frac{1}{p^4} = \frac{2}{\pi} \int_0^{\pi} t^2 (\pi - t)^2 dt = \frac{\pi^4}{15}$$

soit :

$$\sum_{p=1}^{+\infty} \frac{1}{p^4} = \frac{\pi^4}{90}.$$

Du théorème de projection orthogonale, on déduit le résultat suivant valable en dimension finie.

Corollaire 12.2 *Pour tout sous espace vectoriel F de dimension finie de E on a $E = F \oplus F^\perp$ et $(F^\perp)^\perp = F$.*

Démonstration. Pour tout $x \in F \cap F^\perp$, on a $\|x\|^2 = \langle x | x \rangle = 0$ et $x = 0$. Donc $F \cap F^\perp = \{0\}$. Soit $x \in E$ et $y \in F$ sa projection orthogonale dans F . On a $x - y \in F^\perp$ et $x = y + (x - y) \in F + F^\perp$. D'où l'égalité $E = F \oplus F^\perp$.

Il en résulte que $\dim(F^\perp) = \dim(E) - \dim(F)$. On a donc $\dim((F^\perp)^\perp) = \dim(F)$ et avec l'inclusion $F \subset (F^\perp)^\perp$, on déduit qu'on a l'égalité. ■

Remarque 12.4 *Pour F de dimension infinie, on a toujours $F \cap F^\perp = \{0\}$ mais pas nécessairement $E = F \oplus F^\perp$, ni même $(F^\perp)^\perp = F$. On considère par exemple l'espace vectoriel $E = C^0([0, 1], \mathbb{R})$ muni du produit scalaire $\langle f | g \rangle = \int_0^1 f(t) g(t) dt$. Pour $F = \mathbb{R}[x]$, du théorème de Weierstrass on déduit que $F^\perp = \{0\}$ et pourtant on a $E \neq F \oplus F^\perp$ et $(F^\perp)^\perp = E \neq F$.*

Avec le théorème qui suit, on donne les principales propriétés des projections orthogonales.

Théorème 12.9 *Soit F un sous espace vectoriel de dimension finie de E .*

1. *Pour $x \in E$, on a $x \in F$ si, et seulement si, $p_F(x) = x$.*
2. *$p_F \circ p_F = p_F$.*
3. *La projection orthogonale p_F de E sur F est une application linéaire surjective de E sur F .*
4. *Le noyau de p_F est F^\perp .*
5. *Pour tous x, y dans E , on a :*

$$\langle p_F(x) | y \rangle = \langle x | p_F(y) \rangle = \langle p_F(x) | p_F(y) \rangle$$

(on dit que p_F est auto-adjoint).

6. *Pour E de dimension finie, on a $p_F + p_{F^\perp} = Id$.*
7. *Pour E de dimension finie, on a $p_F \circ p_{F^\perp} = p_{F^\perp} \circ p_F = 0$.*

Démonstration.

1. Si $x = p_F(x)$, on a alors $x \in F$. Réciproquement si $x \in F$, avec $x - x = 0 \in F^\perp$, on déduit que $p_F(x) = x$.
2. Résulte de $p_F(x) = x$ pour tout $x \in F$.
3. Si $(e_i)_{1 \leq i \leq n}$ est une base orthonormée de F , on a alors :

$$\forall x \in E, p_F(x) = \sum_{k=1}^n \langle x | e_k \rangle e_k$$

et p_F est linéaire puisque chaque application $x \mapsto \langle x | e_k \rangle e_k$ est linéaire.

L'égalité $p_F(x) = x$ pour tout $x \in F$ nous dit en particulier que p_F est surjective de E sur F .

4. Si $x \in \ker(p_F)$, on a $p_F(x) = 0$ et $x = x - p_F(x) \in F^\perp$. Réciproquement si $x = x - 0 \in F^\perp$, on a $p_F(x) = 0$ puisque $0 \in F$.
5. Pour x, y dans E , on a $p_F(x) \in F$ et $y - p_F(y) \in F^\perp$, donc :

$$\langle p_F(x) | y \rangle = \langle p_F(x) | y - p_F(y) + p_F(y) \rangle = \langle p_F(x) | p_F(y) \rangle$$

l'expression $\langle p_F(x) | p_F(y) \rangle$ étant symétrique en x, y . Il en résulte que $\langle p_F(x) | y \rangle = \langle x | p_F(y) \rangle$.

En utilisant une base orthonormée $(e_i)_{1 \leq i \leq n}$ de F on peut aussi écrire que $p_F(x) = \sum_{k=1}^n \langle x | e_k \rangle e_k$, $p_F(y) = \sum_{k=1}^n \langle y | e_k \rangle e_k$ et :

$$\langle p_F(x) | y \rangle = \sum_{k=1}^n \langle x | e_k \rangle \langle y | e_k \rangle = \langle x | p_F(y) \rangle = \langle p_F(x) | p_F(y) \rangle.$$

6. Dans $E = F \oplus F^\perp$, on a les deux écritures :

$$x = (x - p_F(x)) + p_F(x) = (x - p_{F^\perp}(x)) + p_{F^\perp}(x)$$

avec $(p_F(x), x - p_F(x))$ et $(x - p_{F^\perp}(x), p_{F^\perp}(x))$ dans $F \times F^\perp$, ce qui entraîne $x - p_F(x) = p_{F^\perp}(x)$ du fait de l'unicité de l'écriture dans une somme directe. On a donc bien $p_F(x) + p_{F^\perp}(x) = x$ pour tout $x \in E$.

7. On en déduit que :

$$p_F(x - p_{F^\perp}(x)) = p_F(p_F(x)) = p_F(x)$$

et $p_F(p_{F^\perp}(x)) = 0$. L'égalité $p_{F^\perp} \circ p_F = 0$ se montre de manière analogue. ■

Exercice 12.25 On suppose que E est euclidien et on se donne une base orthonormée \mathcal{B} de E .

- Déterminer la matrice dans \mathcal{B} de la projection orthogonale sur la droite $D = \mathbb{R}a$ engendrée par un vecteur non nul a .
- Déterminer la matrice de la projection orthogonale sur un hyperplan H de E dans \mathcal{B} .

Solution 12.25

1. Par définition de p_D , on a, pour tout $x \in E$, $p_D(x) = \frac{\langle x | a \rangle}{\|a\|^2} a$. En écrivant que $a =$

$\sum_{i=1}^n a_i e_i$, on a, pour tout j compris entre 1 et n :

$$p_D(e_j) = \frac{\langle e_j | a \rangle}{\|a\|^2} a = \sum_{i=1}^n \frac{a_i a_j}{\|a\|^2} e_i$$

et la matrice A de p_D dans \mathcal{B} est $A = \left(\left(\frac{a_i a_j}{\|a\|^2} \right) \right)_{1 \leq i, j \leq n}$, ce qui peut aussi s'écrire

$A = \frac{1}{\|a\|^2} C {}^t C$, où C est le vecteur colonne formé des composantes de a dans \mathcal{B} .

2. On a $H = \{a\}^\perp = (\mathbb{R}a)^\perp$ avec $a \neq 0$ et pour tout $x \in E$, $p_H(x) = x - \frac{\langle x | a \rangle}{\|a\|^2} a$. La matrice de p_H dans \mathcal{B} est donc :

$$B = I_n - A = I_n - \frac{1}{\|a\|^2} C {}^t C = \left(\left(\delta_{ij} - \frac{a_i a_j}{\|a\|^2} \right) \right)_{1 \leq i, j \leq n}$$

12.6 Caractérisation des projecteurs orthogonaux dans un espace euclidien

On rappelle que, sur un espace vectoriel E , un projecteur est une application linéaire p de E dans E telle que $p \circ p = p$.

Il est facile de vérifier que si p est un projecteur de E , alors $\ker(p)$ et $\operatorname{Im}(p)$ sont en somme directe et pour tout $x = y + z$ avec $(y, z) \in \ker(p) \times \operatorname{Im}(p)$, on a $p(x) = y$.

En effet, si $x \in \ker(p) \cap \operatorname{Im}(p)$, on a $x = p(y)$ et $0 = p(x) = p \circ p(y) = p(y) = x$, donc $\ker(p) \cap \operatorname{Im}(p) = \{0\}$ et tout $x \in E$ s'écrit $x = x - p(x) + p(x)$ avec $x - p(x) \in \ker(p)$ et $p(x) \in \operatorname{Im}(p)$, donc $E = \ker(p) + \operatorname{Im}(p)$. On a donc bien $E = \ker(p) \oplus \operatorname{Im}(p)$ et pour tout $x = y + z \in E$ avec $(y, z) \in \ker(p) \times \operatorname{Im}(p)$, on a $p(x) = p(y) + p(z) = p(z) = z$.

On dit que p est le projecteur sur $F = \operatorname{Im}(p)$ parallèlement à $\ker(p)$.

Réciproquement si $E = F \oplus G$, l'application qui associe à $x = y + z$, où $(y, z) \in F \times G$, le vecteur y est un projecteur sur F parallèlement à G .

Les projecteurs orthogonaux sont des cas particuliers de projecteurs. Ce sont en fait les projecteurs de E caractérisés par la propriété **5.** du théorème 12.9 ou par $\|p(x)\| \leq \|x\|$ pour tout $x \in E$.

Théorème 12.10 *Soit p un projecteur d'un espace euclidien E . Les propriétés suivantes sont équivalentes :*

1. p est un projecteur orthogonal ;
2. pour tous x, y dans E , on a : $\langle p(x) | y \rangle = \langle x | p(y) \rangle$;
3. pour tout $x \in E$, on a $\|p(x)\| \leq \|x\|$.

Démonstration. Si $p = p_F$ est un projecteur orthogonal, on sait déjà qu'il est auto-adjoint, c'est-à-dire que **1.** implique **2.**

Si p est un projecteur qui vérifie **2.** on a, en utilisant l'inégalité de Cauchy-Schwarz, pour tout $x \in E$:

$$\begin{aligned} \|p(x)\|^2 &= \langle p(x) | p(x) \rangle = \langle x | p(p(x)) \rangle \\ &= \langle x | p(x) \rangle \leq \|x\| \|p(x)\| \end{aligned}$$

et $\|p(x)\| \leq \|x\|$ pour $x \neq 0$, l'égalité étant réalisée pour $x = 0$.

Supposons que p soit un projecteur vérifiant **3.** On a $E = \ker(p) \oplus \operatorname{Im}(p)$ et si p est un projecteur orthogonal sur F , on a nécessairement $\ker(p) = F^\perp$ et $\operatorname{Im}(p) = F = (\ker(p))^\perp$. Réciproquement si $\operatorname{Im}(p) = (\ker(p))^\perp$, on a alors pour tout $x \in E$, $p(x) \in F = \operatorname{Im}(p)$ et $x - p(x) \in \ker(p) = F^\perp$, ce qui signifie que $p(x)$ est le projeté orthogonal de x sur F . Il s'agit donc de montrer que $\operatorname{Im}(p) = (\ker(p))^\perp$. Pour $x \in \ker(p)$ et $y \in \operatorname{Im}(p)$, en notant $z = y - \lambda x$ où λ est un réel, on a $p(z) = p(y) = y$ et :

$$\|y\|^2 = \|p(z)\|^2 \leq \|z\|^2 = \|y\|^2 - 2\lambda \langle x | y \rangle + \lambda^2 \|x\|^2$$

soit :

$$\lambda (\lambda \|x\|^2 - 2 \langle x | y \rangle) \geq 0$$

ce qui entraîne $\lambda \|x\|^2 - 2 \langle x | y \rangle \geq 0$ pour $\lambda > 0$ et $\lambda \|x\|^2 - 2 \langle x | y \rangle \leq 0$ pour $\lambda < 0$. Faisant tendre λ vers 0 par valeurs positives et négatives respectivement, on obtient $\langle x | y \rangle \leq 0$ et $\langle x | y \rangle \geq 0$, soit $\langle x | y \rangle = 0$. Le projecteur p est donc un projecteur orthogonal. ■

12.7 Réduction des matrices symétriques réelles

Pour ce paragraphe, $(E, \langle \cdot | \cdot \rangle)$ désigne un espace euclidien de dimension $n \geq 1$ et $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base orthonormée de E .

Définition 12.8 On dit qu'un endomorphisme u de E est symétrique si :

$$\forall (x, y) \in E \times E, \langle u(x) | y \rangle = \langle x | u(y) \rangle.$$

Théorème 12.11 Un endomorphisme u de E est symétrique si, et seulement si, sa matrice A dans la base orthonormée \mathcal{B} de E est symétrique.

Exemple 12.4 Un projecteur orthogonal est un endomorphisme symétrique et on a vu que réciproquement si un projecteur est symétrique, c'est alors un projecteur orthogonal (théorème 12.10).

Définition 12.9 Si u est un endomorphisme de u , on dit qu'un réel λ est valeur propre de u si l'endomorphisme $u - \lambda Id$ n'est pas inversible.

Dire que $u - \lambda Id$ n'est pas inversible équivaut à dire que son noyau $\ker(u - \lambda Id)$ n'est pas réduit à $\{0\}$, ce qui équivaut à dire qu'il existe un vecteur $x \neq 0$ tel que $u(x) = \lambda x$. Il est encore équivalent de dire que $\det(u - \lambda Id) \neq 0$.

Les valeurs propres de u sont donc les racines du polynôme $P_u(\lambda) = \det(u - \lambda Id)$. Ce polynôme est appelé polynôme caractéristique de u .

Comme P_u est de degré n , l'endomorphisme u a au plus n valeurs propres réelles.

Pour toute valeur propre réelle λ d'un endomorphisme u de E , le sous-espace vectoriel $E_\lambda = \ker(u - \lambda Id)$ est appelé l'espace propre associé à la valeur propre λ .

En désignant par A la matrice de u dans une base de u , on a $\det(u - \lambda Id) = \det(A - \lambda I_n)$. Le polynôme $P_A(\lambda) = \det(A - \lambda I_n)$ est appelé polynôme caractéristique de A et les racines de ce polynôme (réelles ou complexes) sont appelées les valeurs propres de A .

Par exemple, pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on a $P_A(\lambda) = \lambda^2 + 1$ qui n'a pas de racines réelles, mais a deux racines complexes i et $-i$.

Théorème 12.12 Si u est un endomorphisme symétrique de E , alors son polynôme caractéristique a n racines réelles distinctes ou confondues.

Corollaire 12.3 Les valeurs propres d'une matrice symétrique réelle sont toutes réelles.

Théorème 12.13 Soient u un endomorphisme symétrique de E , λ, μ deux valeurs propres (réelles) distinctes de u et E_λ, E_μ les espaces propres associés. Pour tout $x \in E_\lambda$ et $y \in E_\mu$, on a $\langle x | y \rangle = 0$. C'est-à-dire que les espaces propres associés à des valeurs propres distinctes de u sont orthogonaux.

Théorème 12.14 Si u un endomorphisme symétrique de E , il existe alors une base orthonormée de E dans laquelle la matrice de u est diagonale.

Corollaire 12.4 Si A est une matrice symétrique réelle d'ordre n , il existe alors une matrice inversible P telle que $P^{-1} = {}^tP$ (une telle matrice est dite orthogonale) et $P^{-1}AP = {}^tPAP$ est une matrice diagonale.

Ce corollaire s'exprime en disant que toute matrice symétrique réelle est diagonalisable dans une base orthonormée de \mathbb{R}^n .

Corollaire 12.5 Si q une forme quadratique sur E , il existe alors une base orthonormée de E dans laquelle la matrice de q est diagonale.

On retrouve ainsi le théorème de réduction de Gauss relatif aux formes quadratiques réelles.

Géométrie dans les espaces préhilbertiens

Pour ce chapitre $(E, \langle \cdot | \cdot \rangle)$ est un espace préhilbertien et $\|\cdot\|$ est la norme associée.

13.1 Mesures de l'angle non orienté de deux vecteurs non nuls

L'inégalité de Cauchy-Schwarz nous dit que pour tous vecteurs x et y non nuls dans E , on a :

$$-1 \leq \frac{\langle x | y \rangle}{\|x\| \|y\|} \leq 1,$$

ce qui implique qu'il existe un unique réel θ dans $[0, \pi]$ tel que :

$$\langle x | y \rangle = \cos(\theta) \|x\| \|y\|.$$

Le réel θ est la mesure dans $[0, \pi]$ de l'angle géométrique (ou angle non orienté) que font les vecteurs x et y dans $E - \{0\}$. On note $\widehat{(x, y)}$ cette mesure. On a donc :

$$\widehat{(x, y)} = \arccos \left(\frac{\langle x | y \rangle}{\|x\| \|y\|} \right) \in [0, \pi].$$

Pour $\theta \in \{0, \pi\}$, on a $|\langle x | y \rangle| = \|x\| \|y\|$, ce qui équivaut à dire que les vecteurs x et y sont liés (cas d'égalité dans l'inégalité de Cauchy-Schwarz).

Pour $\theta = \frac{\pi}{2}$, on a $\langle x | y \rangle = 0$ et les vecteurs x, y sont orthogonaux.

De manière générale, on a :

$$\|x + y\|^2 = \|x\|^2 + 2 \cos(\theta) \|x\| \|y\| + \|y\|^2$$

où θ est la mesure dans $[0, \pi]$ de l'angle que font les vecteurs non nuls x et y .

On peut remarquer que si λ, μ sont deux réels strictement positifs, alors :

$$\widehat{(\lambda x, \mu y)} = \arccos \left(\frac{\langle \lambda x | \mu y \rangle}{\|\lambda x\| \|\mu y\|} \right) = \widehat{(x, y)}$$

ce qui permet de définir la mesure dans $[0, \pi]$ de l'angle géométrique de deux demi-droites $\Delta_1 = \mathbb{R}^+ x_1$ et $\Delta_2 = \mathbb{R}^+ x_2$ par :

$$\widehat{(\Delta_1, \Delta_2)} = \widehat{(x_1, x_2)}$$

où x_1 est un vecteur directeur de Δ_1 et x_2 un vecteur directeur de Δ_2 .

On dit parfois que $\widehat{(\Delta_1, \Delta_2)}$ est l'angle géométrique ou l'écart angulaire de Δ_1 et Δ_2 .

On a :

- $\widehat{(\Delta_1, \Delta_2)} = 0$ si, et seulement si, $\Delta_1 = \Delta_2$;
- $\widehat{(\Delta_1, \Delta_2)} = \pi$ si, et seulement si, $\Delta_1 = -\Delta_2$ (i. e. Δ_1 et Δ_2 sont opposées) ;
- $\widehat{(\Delta_1, \Delta_2)} = \frac{\pi}{2}$ si, et seulement si, Δ_1 et Δ_2 sont orthogonales.

13.2 Sphères dans un espace préhilbertien

Le fait de disposer d'une norme sur E permet de définir les notions de sphère et de boule ouverte ou fermée dans E .

Définition 13.1 *On dit qu'une partie S de E est une sphère s'il existe un point ω dans E et un réel R positif ou nul tels que :*

$$S = \{x \in E \mid \|x - \omega\| = R\}$$

On dit alors que ω est un centre et R un rayon de cette sphère.

On notera $S(\omega, R)$ une telle sphère.

Il semble intuitif que le centre et le rayon d'une sphère sont uniquement déterminés, c'est ce que nous allons vérifier.

Théorème 13.1 *Le centre et le rayon d'une sphère sont uniquement déterminés.*

Démonstration. Soit $S = S(\omega, R)$ une sphère.

Si $R = 0$, on a alors $S = \{\omega\}$ et il n'y a rien à prouver.

On suppose donc que $R > 0$.

Pour tous x, y dans $S = S(\omega, R)$, on a :

$$\|y - x\| \leq \|y - \omega\| + \|\omega - x\| = 2R$$

l'égalité étant réalisée pour $(x, y) = (\omega + Ru, \omega - Ru) \in S^2$ où $\|u\| = 1$ (pour tout vecteur non nul $v \in E$ le vecteur $u = \frac{1}{\|v\|}v$ est de norme 1). On a donc :

$$2R = \sup_{(x,y) \in S^2} \|y - x\|$$

ce qui prouve l'unicité du rayon R .

Si a, b dans $S(\omega, R)$ sont tels que $\|b - a\| = 2R$, on a l'égalité :

$$\|b - a\| = \|b - \omega\| + \|\omega - a\| = 2R$$

et il existe un réel $\lambda > 0$ tel que $b - \omega = \lambda(\omega - a)$ (cas d'égalité dans l'inégalité de Minkowski).

Avec $\|b - \omega\| = \|\omega - a\| = R > 0$, on déduit que $\lambda = 1$ et $\omega = \frac{1}{2}(a + b)$, ce qui prouve l'unicité du centre ω . ■

Définition 13.2 *Si $S(\omega, R)$ une sphère de centre ω et de rayon R , on appelle diamètre de $S(\omega, R)$ tout segment $[a, b]$ où a, b sont deux points de S tels que $\|b - a\| = 2R$.*

Définition 13.3 Soient ω un point de E et R un réel positif ou nul.
La boule fermée [resp. ouverte] de centre ω et de rayon R est l'ensemble :

$$B(\omega, R) = \{x \in E \mid \|x - \omega\| \leq R\}$$

$$[\text{resp. } \overset{\circ}{B}(\omega, R) = \{x \in E \mid \|x - \omega\| < R\}]$$

Remarque 13.1 Pour $R = 0$, on a $S(\omega, R) = B(\omega, R) = \{\omega\}$ et $\overset{\circ}{B}(\omega, R) = \emptyset$.

Dans le cas où $\omega = 0$ et $R = 1$, on dit que $S(0, 1)$ [resp. $B(0, 1)$] est la sphère [resp. boule] unité.

Si $R > 0$, le centre ω n'est pas dans $S(\omega, R)$ et on a vu dans la démonstration du théorème précédent que $S(\omega, R)$ contient au moins deux points.

Dans le cas où E est une droite dirigée par e_1 de norme 1, on a, pour $R > 0$:

$$(x \in S(\omega, R)) \Leftrightarrow (|x_1 - \omega_1| = R) \Leftrightarrow (x_1 = \omega_1 \pm R)$$

c'est-à-dire que $S(\omega, R)$ est réduit aux deux points $\{\omega_1 - R, \omega_1 + R\}$.

Si E est de dimension 2, une sphère est appelée cercle.

L'utilisation de l'identité polaire pour le produit scalaire nous fournit une autre définition géométrique d'une sphère.

Théorème 13.2 Soient a, b deux points de E . L'ensemble :

$$S = \{x \in E \mid \langle x - a \mid x - b \rangle = 0\}$$

est une sphère de centre $\omega = \frac{a+b}{2}$ et de rayon $R = \left\| \frac{b-a}{2} \right\|$ (sphère de diamètre $[a, b]$).

Démonstration. En utilisant l'identité polaire, on a :

$$\begin{aligned} \langle x - a \mid x - b \rangle &= \frac{1}{4} (\|(x - a) + (x - b)\|^2 - \|(x - a) - (x - b)\|^2) \\ &= \left\| x - \frac{a+b}{2} \right\|^2 - \left\| \frac{b-a}{2} \right\|^2 \end{aligned}$$

et :

$$(x \in S) \Leftrightarrow \left(\left\| x - \frac{a+b}{2} \right\| = \left\| \frac{b-a}{2} \right\| \right)$$

ce qui signifie que S est la sphère de centre $\omega = \frac{a+b}{2}$ et de rayon $\left\| \frac{b-a}{2} \right\|$. ■

Cette sphère passe par a et b . Pour $R > 0$ et E de dimension 2, on retrouve la caractérisation du cercle de diamètre $[a, b]$ dans le plan euclidien comme l'ensemble des points x tels que le triangle axb soit rectangle en x (figure 13.1).

FIGURE 13.1 – Sphère : $\langle x - a, x - b \rangle = 0$

13.3 Sphères dans un espace euclidien

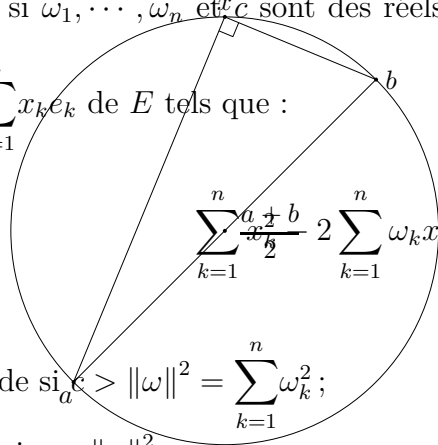
Dans le cas où E est un espace euclidien de dimension $n \geq 2$ (le cas $n = 1$ étant trivial), l'utilisation d'une base orthonormée permet de donner une définition analytique d'une sphère.

On suppose, a priori, que le rayon R d'une sphère $S(\omega, R)$ est non nul.

Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base orthonormée de E euclidien, on a alors en notant x_1, \dots, x_n les coordonnées d'un vecteur $x \in E$ dans cette base :

$$\begin{aligned} (x \in S(\omega, R)) &\Leftrightarrow \left(\sum_{k=1}^n (x_k - \omega_k)^2 = R^2 \right) \\ &\Leftrightarrow \left(\sum_{k=1}^n x_k^2 - 2 \sum_{k=1}^n \omega_k x_k + \sum_{k=1}^n \omega_k^2 - R^2 = 0 \right) \end{aligned}$$

Réciproquement si $\omega_1, \dots, \omega_n$ et c sont des réels, alors en notant $\omega = \sum_{k=1}^n \omega_k e_k$, l'ensemble des vecteurs $x = \sum_{k=1}^n x_k e_k$ de E tels que :



$$\sum_{k=1}^n x_k^2 - 2 \sum_{k=1}^n \omega_k x_k + c = 0$$

est :

- l'ensemble vide si $c > \|\omega\|^2 = \sum_{k=1}^n \omega_k^2$;
- réduit à $\{\omega\}$ si $c = \|\omega\|^2$;
- la sphère de centre ω et de rayon $R = \sqrt{\|\omega\|^2 - c}$ si $c < \|\omega\|^2$.

Il suffit en effet d'écrire que :

$$\sum_{k=1}^n x_k^2 - 2 \sum_{k=1}^n \omega_k x_k + c = \sum_{k=1}^n (x_k - \omega_k)^2 + c - \sum_{k=1}^n \omega_k^2.$$

Dans le cas où E est un plan euclidien, on peut donner une représentation paramétrique d'un cercle.

Pour ce faire, on rappelle que si u, v sont deux réels tels que $u^2 + v^2 = 1$, il existe un unique réel θ dans $]-\pi, \pi]$ tel que $u = \cos(\theta)$ et $v = \sin(\theta)$ (voir la définition de l'argument d'un nombre complexe non nul).

Désignant par $\mathcal{B} = (e_1, e_2)$ une base orthonormée de E , on en déduit que tout point x du cercle $S(\omega, R)$ s'écrit de manière unique $x = x_1 e_1 + x_2 e_2$ avec :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta) \\ x_2 = \omega_2 + R \sin(\theta) \end{cases}$$

avec $\theta \in]-\pi, \pi]$.

En écrivant $(x_1, x_2) = (\rho \cos(t), \rho \sin(t))$ et $(\omega_1, \omega_2) = (r \cos(\alpha), r \sin(\alpha))$ où $\rho = \|x\|$, $r = \|\omega\|$ et α, t réels, on a aussi :

$$\begin{aligned} (x \in S(\omega, R)) &\Leftrightarrow (\rho^2 - 2\rho r (\cos(t) \cos(\alpha) + \sin(t) \sin(\alpha)) + r^2 - R^2 = 0) \\ &\Leftrightarrow (\rho^2 - 2\rho r \cos(t - \alpha) + r^2 - R^2 = 0) \end{aligned}$$

Ce cercle passe par 0 si, et seulement si $r = \|\omega\| = R$ et dans ce cas, on a :

$$(x \in S(\omega, R)) \Leftrightarrow (\rho(\rho - 2r \cos(t - \alpha)) = 0)$$

On en déduit qu'une équation polaire d'un cercle passant par 0 est donnée par $\rho = 2r \cos(t - \alpha)$ où t décrit \mathbb{R} et $\rho = \|x\|$ ($t = \alpha + \frac{\pi}{2}$ donne le point 0 du cercle).

Dans le cas où $n = 3$, on peut aboutir à une représentation paramétrique de $S(\omega, R)$ dans une base orthonormée $\mathcal{B} = (e_1, e_2, e_3)$ de E comme suit.

Pour $x \in S(\omega, R)$, on a :

$$x_3 - \omega_3 = \langle x - \omega \mid e_3 \rangle = \|x - \omega\| \|e_3\| \cos(\theta_3) = R \cos(\theta_3)$$

avec $\theta_3 = \widehat{(x - \omega, e_3)} \in [0, \pi]$ et de :

$$\begin{aligned} (x_1 - \omega_1)^2 + (x_2 - \omega_2)^2 &= R^2 - (x_3 - \omega_3)^2 \\ &= R^2 (1 - \cos^2(\theta_3)) = R^2 \sin^2(\theta_3) \end{aligned}$$

avec $\sin(\theta_3) \geq 0$, on déduit qu'il existe un réel $\theta_2 \in]-\pi, \pi]$ tel que :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta_2) \sin(\theta_3) \\ x_2 = \omega_2 + R \sin(\theta_2) \sin(\theta_3) \\ x_3 = \omega_3 + R \cos(\theta_3) \end{cases} \quad (13.1)$$

Réciproquement, on vérifie facilement que (13.1) définit la sphère de centre ω et de rayon R .

Pour $n = 4$, de :

$$x_4 - \omega_4 = \langle x - \omega \mid e_4 \rangle = \|x - \omega\| \|e_4\| \cos(\theta_4) = R \cos(\theta_4)$$

avec $\theta_4 \in [0, \pi]$ et :

$$(x_1 - \omega_1)^2 + (x_2 - \omega_2)^2 + (x_3 - \omega_3)^2 = R^2 \sin^2(\theta_4)$$

on déduit, en remplaçant R par $R \sin(\theta_4) \geq 0$, que :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta_2) \sin(\theta_3) \sin(\theta_4) \\ x_2 = \omega_2 + R \sin(\theta_2) \sin(\theta_3) \sin(\theta_4) \\ x_3 = \omega_3 + R \cos(\theta_3) \sin(\theta_4) \end{cases}$$

et la paramétrisation :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta_2) \sin(\theta_3) \sin(\theta_4) \\ x_2 = \omega_2 + R \sin(\theta_2) \sin(\theta_3) \sin(\theta_4) \\ x_3 = \omega_3 + R \cos(\theta_3) \sin(\theta_4) \\ x_4 = \omega_4 + R \cos(\theta_4) \end{cases}$$

avec $\theta_2 \in]-\pi, \pi]$ et θ_3, θ_4 dans $[0, \pi]$.

Par récurrence, on déduit que pour $n \geq 3$, une paramétrisation de la sphère $S(\omega, R)$ est donnée par :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \\ x_2 = \omega_2 + R \sin(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \\ x_3 = \omega_3 + R \cos(\theta_3) \sin(\theta_4) \cdots \sin(\theta_n) \\ \vdots \\ x_{n-2} = \omega_{n-2} + R \cos(\theta_{n-2}) \sin(\theta_{n-1}) \sin(\theta_n) \\ x_{n-1} = \omega_{n-1} + R \cos(\theta_{n-1}) \sin(\theta_n) \\ x_n = \omega_n + R \cos(\theta_n) \end{cases} \quad (13.2)$$

avec $\theta_2 \in]-\pi, \pi]$ et $\theta_3, \dots, \theta_n$ dans $[0, \pi]$.

En effet, pour $n = 3$, c'est vrai. Le supposant acquis pour $n \geq 3$, on a pour $x \in S(\omega, R)$ dans E de dimension $n + 1$:

$$x_{n+1} - \omega_{n+1} = \langle x - \omega \mid e_{n+1} \rangle = \|x - \omega\| \|e_{n+1}\| \cos(\theta_{n+1}) = R \cos(\theta_{n+1})$$

avec $\theta_{n+1} \in [0, \pi]$ et le vecteur $x' = x - x_{n+1}e_{n+1} = \sum_{k=1}^n x_k e_k$ est tel que :

$$\sum_{k=1}^n (x_k - \omega_k)^2 = R^2 - (x_{n+1} - \omega_{n+1})^2 = R^2 \sin^2(\theta_{n+1})$$

avec $\sin(\theta_{n+1}) \geq 0$, ce qui signifie qu'il est sur la sphère $S(\omega', R')$ où $\omega' = \omega - \omega_{n+1}e_{n+1} = \sum_{k=1}^n \omega_k e_k$ et $R' = R \sin(\theta_{n+1})$ de l'espace euclidien de dimension n , E' engendré par e_1, \dots, e_n .

Il existe donc un réel $\theta_2 \in]-\pi, \pi]$ et des réels $\theta_3, \dots, \theta_n$ dans $[0, \pi]$ tels que :

$$\begin{cases} x_1 = \omega_1 + R \sin(\theta_{n+1}) \cos(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \\ x_2 = \omega_2 + R \sin(\theta_{n+1}) \sin(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \\ x_3 = \omega_3 + R \sin(\theta_{n+1}) \cos(\theta_3) \sin(\theta_4) \cdots \sin(\theta_n) \\ \vdots \\ x_{n-2} = \omega_{n-2} + R \sin(\theta_{n+1}) \cos(\theta_{n-2}) \sin(\theta_{n-1}) \sin(\theta_n) \\ x_{n-1} = \omega_{n-1} + R \sin(\theta_{n+1}) \cos(\theta_{n-1}) \sin(\theta_n) \\ x_n = \omega_n + R \sin(\theta_{n+1}) \cos(\theta_n) \end{cases}$$

et on a la paramétrisation :

$$\begin{cases} x_1 = \omega_1 + R \cos(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \sin(\theta_{n+1}) \\ x_2 = \omega_2 + R \sin(\theta_2) \sin(\theta_3) \cdots \sin(\theta_n) \sin(\theta_{n+1}) \\ x_3 = \omega_3 + R \cos(\theta_3) \sin(\theta_4) \cdots \sin(\theta_n) \sin(\theta_{n+1}) \\ \vdots \\ x_{n-2} = \omega_{n-2} + R \cos(\theta_{n-2}) \sin(\theta_{n-1}) \sin(\theta_n) \sin(\theta_{n+1}) \\ x_{n-1} = \omega_{n-1} + R \cos(\theta_{n-1}) \sin(\theta_n) \sin(\theta_{n+1}) \\ x_n = \omega_n + R \cos(\theta_n) \sin(\theta_{n+1}) \\ x_{n+1} = \omega_{n+1} + R \cos(\theta_{n+1}). \end{cases} \quad (13.3)$$

Réciproquement, on vérifie que (13.2) définit bien la sphère de centre ω et de rayon R dans E de dimension n .

Pour $n = 3$, si $x \in E$ vérifie (13.1), on a :

$$\begin{aligned} \|x - \omega\|^2 &= R^2 (\cos^2(\theta_2) \sin^2(\theta_3) + \sin^2(\theta_2) \sin^2(\theta_3) + \cos^2(\theta_3)) \\ &= R^2 ((\cos^2(\theta_2) + \sin^2(\theta_2)) \sin^2(\theta_3) + \cos^2(\theta_3)) \\ &= R^2 (\sin^2(\theta_3) + \cos^2(\theta_3)) = R^2 \end{aligned}$$

et $x \in S(\omega, R)$.

Supposant le résultat acquis pour les espaces euclidiens de dimension $n \geq 3$, si x dans E de dimension $n + 1$ vérifie (13.3), alors $x' = x - x_{n+1}e_{n+1} = \sum_{k=1}^n x_k e_k$ vérifie (13.2) dans E' engendré par e_1, \dots, e_n avec $R' = R \sin(\theta_{n+1}) \geq 0$, il est donc sur la sphère $S(\omega', R')$ où $\omega' = \omega - \omega_{n+1}e_{n+1} = \sum_{k=1}^n \omega_k e_k$ et on a :

$$\begin{aligned} \|x - \omega\|^2 &= \|x' - \omega'\|^2 + (x_{n+1} - \omega_{n+1})^2 \\ &= R'^2 \sin^2(\theta_{n+1}) + R'^2 \cos^2(\theta_{n+1}) = R^2 \end{aligned}$$

et $x \in S(\omega, R)$.

13.4 Hyperplans dans un espace euclidien

On rappelle qu'un hyperplan vectoriel d'un espace vectoriel E est le noyau d'une forme linéaire non nulle.

Plus généralement on peut définir un hyperplan affine par :

$$H = \ell^{-1}\{\lambda\} = \{x \in E \mid \ell(x) = \lambda\}$$

où ℓ est une forme linéaire non nulle et λ un réel.

Une forme linéaire non nulle étant surjective, il existe un vecteur $x_0 \in E$ tel que $\lambda = \ell(x_0)$ (donc H est non vide) et un vecteur x est dans l'hyperplan d'équation $\ell(x) = \lambda$ si, et seulement si, $x - x_0$ est dans l'hyperplan vectoriel $\ker(\ell)$. On a donc $H = x_0 + \ker(\ell)$, ce qui revient à placer l'origine en x_0 . On dit que H est l'hyperplan affine passant par x_0 et dirigé par $\ker(\ell)$.

Les notions d'espace et sous-espace affines seront étudiées plus loin.

Pour tout vecteur non nul a d'un espace préhilbertien, l'application $x \mapsto \langle a \mid x \rangle$ est une forme linéaire non nulle et pour tout réel λ l'ensemble des vecteurs $x \in E$ tel que $\langle a \mid x \rangle = \lambda$ est un hyperplan.

Dans le cas où E est un espace euclidien, la réciproque est vraie, c'est-à-dire que toute forme linéaire et tout hyperplan peuvent être ainsi décrits.

Théorème 13.3 Soit E un espace euclidien de dimension n . Pour toute forme linéaire ℓ sur E , il existe un unique vecteur $a \in E$ tel que :

$$\forall x \in E, \ell(x) = \langle a | x \rangle.$$

Si H est un hyperplan vectoriel de E , il existe alors un vecteur non nul a tel que $H = \{a\}^\perp$.
Si H est un hyperplan affine de E ne contenant pas 0 , il existe alors un vecteur non nul b tel que $H = \{x \in E \mid \langle b | x \rangle = 1\}$.

Démonstration. On note $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de l'espace euclidien E .

Dans la base \mathcal{B} l'expression de ℓ est $\ell(x) = \sum_{k=1}^n a_k x_k = \langle a | x \rangle$, où on a noté $a = \sum_{k=1}^n a_k e_k$.

Prenant $x = e_j$ avec j compris entre 1 et n , on a $\ell(e_j) = a_j = \langle a | e_j \rangle$.

Si a' est un autre vecteur tel que $\ell(x) = \langle a' | x \rangle$ pour tout $x \in E$, on a $\langle a | x \rangle = \langle a' | x \rangle$ pour tout $x \in E$, soit $\langle a - a' | x \rangle = 0$ pour tout $x \in E$ et $a - a' \in E^\perp = \{0\}$, soit $a = a'$.

Si H est un hyperplan vectoriel de E , il existe une forme linéaire ℓ non nulle telle que $H = \ker(\ell)$ et désignant a le vecteur qui définit ℓ , on a :

$$(x \in H) \Leftrightarrow (\ell(x) = \langle a | x \rangle = 0) \Leftrightarrow (x \in \{a\}^\perp).$$

Si H est un hyperplan affine de E d'équation $\ell(x) = \langle a | x \rangle = \lambda$ dans \mathcal{B} , avec $\lambda \neq 0$, on a :

$$(x \in H) \Leftrightarrow (\langle a | x \rangle = \lambda) \Leftrightarrow (\langle b | x \rangle = 1)$$

en notant $b = \frac{1}{\lambda}a$. ■

Ce résultat peut s'exprimer en disant que pour E euclidien, l'application qui associe à tout vecteur $a \in E$ la forme linéaire $x \mapsto \langle a | x \rangle$ réalise un isomorphisme de E sur son dual E^* .

Le théorème précédent n'est pas valable pour E préhilbertien de dimension infinie comme le montre l'exercice qui suit.

Exercice 13.1 Soit $E = \mathcal{C}^0([0, 1], \mathbb{R})$ muni du produit scalaire défini par $\langle f | g \rangle = \int_0^1 f(t)g(t)dt$ et ℓ la forme linéaire définie sur E par $\ell(f) = f(0)$ pour tout $f \in E$. Peut-on trouver une fonction $a \in E$ telle que $\ell(f) = \langle a | f \rangle$ pour tout $f \in E$?
Construire un hyperplan H de E qui n'est pas l'orthogonal d'une droite.

Solution 13.1 Supposons qu'une telle fonction existe. Comme $\ell \neq 0$, on a $a \neq 0$. Prenant $f : t \mapsto t \cdot a(t)$, on a :

$$\ell(f) = f(0) = 0 = \int_0^1 t a^2(t) dt$$

ce qui est impossible puisque f est continue positive et non identiquement nulle. Le premier point du théorème précédent est donc faux en dimension infinie.

Prenons pour hyperplan le noyau de ℓ et supposons que $H = \{a\}^\perp$ avec $a \neq 0$. La fonction $f : t \mapsto t \cdot a(t)$ est non identiquement nulle dans H et $\langle f | a \rangle = \int_0^1 t a^2(t) dt > 0$, donc $f \notin \{a\}^\perp$. Une telle fonction a ne peut donc exister.

Pour ce qui suit, on suppose que E est un espace euclidien de dimension $n \geq 2$ et $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base orthonormée de E .

En notant p_F la projection orthogonale sur un sous-espace F de E , l'identité $p_F + p_{F^\perp} = Id$ et le théorème précédent nous permettent d'obtenir une expression simple de la projection orthogonale sur un hyperplan vectoriel et de la distance d'un point à un hyperplan vectoriel ou affine.

Théorème 13.4 Soit H un hyperplan de E d'équation $\sum_{k=1}^n a_k x_k = 0$ dans la base \mathcal{B} et p_H la projection orthogonale sur H . En posant $a = \sum_{k=1}^n a_k e_k$, on a :

$$\forall x \in E, p_H(x) = x - \frac{\langle x | a \rangle}{\|a\|^2} a$$

et pour tout $x = \sum_{k=1}^n x_k e_k$ dans E , la distance de x à H est :

$$d(x, H) = \frac{|\langle a | x \rangle|}{\|a\|} = \frac{\left| \sum_{k=1}^n a_k x_k \right|}{\sqrt{\sum_{k=1}^n a_k^2}}.$$

Démonstration. L'hyperplan H s'écrit $H = \{a\}^\perp = (\mathbb{R}a)^\perp$ avec $a \neq 0$ et pour tout $x \in E$, on a :

$$p_H(x) = x - p_{H^\perp}(x) = x - p_{\mathbb{R}a}(x) = x - \frac{\langle x | a \rangle}{\|a\|^2} a.$$

De plus pour tout $x \in E$, on a :

$$d(x, H) = \|x - p_H(x)\| = \|p_{H^\perp}(x)\|$$

avec $p_{H^\perp}(x) = \frac{\langle x | a \rangle}{\|a\|^2} a$, ce qui donne :

$$d(x, H) = \frac{|\langle x | a \rangle|}{\|a\|} = \frac{\left| \sum_{k=1}^n a_k x_k \right|}{\sqrt{\sum_{k=1}^n a_k^2}}.$$

■

De manière un peu plus générale, si H est un hyperplan affine d'équation $\ell(x) = \lambda$, on peut encore définir la distance de $x \in E$ à H par $d(x, H) = \inf_{z \in H} \|x - z\|$.

En désignant par x_0 un point de H , on a $\lambda = \ell(x_0)$ et $H = x_0 + \ker(\ell)$, de sorte qu'en notant $H_0 = \ker(\ell)$, on a :

$$\begin{aligned} d(x, H) &= \inf_{z \in H} \|x - z\| = \inf_{y \in H_0} \|x - x_0 - y\| \\ &= d(x - x_0, H_0) = \|x - x_0 - p_{H_0}(x - x_0)\| \end{aligned}$$

Le vecteur $x_0 + p_{H_0}(x - x_0) \in H$ est la projection orthogonale de x sur H , on le note $p_H(x)$. On a :

$$(y = p_H(x)) \Leftrightarrow (y \in H \text{ et } x - y \in H_0^\perp) \Leftrightarrow (y \in H \text{ et } \|x - y\| = d(x, H))$$

En effet, si $y = p_H(x) = x_0 + p_{H_0}(x - x_0) \in H$, alors $x - y = x - x_0 - p_{H_0}(x - x_0) \in H_0^\perp$ et $\|x - y\| = \|x - x_0 - p_{H_0}(x - x_0)\| = d(x, H)$ comme on vient de le voir. Si $\|x - y\| = d(x, H)$ avec $y \in H = x_0 + H_0$, on a $y - x_0 \in H_0$ et :

$$\|(x - x_0) - (y - x_0)\| = \|x - y\| = d(x, H) = d(x - x_0, H_0)$$

ce qui signifie que $y - x_0 = p_{H_0}(x - x_0)$ et $y = p_H(x)$.

On peut remarquer que la définition de $p_H(x)$ ne dépend pas du choix d'un point x_0 de H . En effet, si x_1 est un autre élément de H , on a :

$$x_1 + p_{H_0}(x - x_1) - x_0 - p_{H_0}(x - x_0) = (x_1 - x_0) - p_{H_0}(x_1 - x_0) = 0$$

puisque $x_1 - x_0 \in H$.

On peut aussi remarquer que l'application p_H (projection orthogonale sur H) n'est pas une application linéaire si $0 \notin H$. En fait c'est une application affine.

Corollaire 13.1 Soit H un hyperplan de E d'équation $\sum_{k=1}^n a_k x_k = \lambda$ dans la base \mathcal{B} . Pour tout $x = \sum_{k=1}^n x_k e_k$ dans E , la distance de x à H est :

$$d(x, H) = \frac{\left| \sum_{k=1}^n a_k x_k - \lambda \right|}{\sqrt{\sum_{k=1}^n a_k^2}}.$$

Démonstration. On note $a = \sum_{k=1}^n a_k e_k$ et ℓ est la forme linéaire définie sur E par $\ell(x) =$

$$\langle a | x \rangle = \sum_{k=1}^n a_k x_k.$$

En désignant par x_0 un point de H , on a $\lambda = \ell(x_0)$ et $H = x_0 + \ker(\ell)$, de sorte que :

$$\begin{aligned} d(x, H) &= d(x - x_0, \ker(\ell)) = \frac{|\langle x - x_0 | a \rangle|}{\|a\|} \\ &= \frac{|\ell(x) - \ell(x_0)|}{\|a\|} = \frac{\left| \sum_{k=1}^n a_k x_k - \lambda \right|}{\sqrt{\sum_{k=1}^n a_k^2}} \end{aligned}$$

■

Exemple 13.1 La distance d'un point $M = \begin{pmatrix} x \\ y \end{pmatrix}$ du plan \mathbb{R}^2 à la droite D d'équation $ax + by + c = 0$ est :

$$d(M, D) = \frac{|ax + by + c|}{\sqrt{a^2 + b^2}}.$$

La distance d'un point M de l'espace \mathbb{R}^3 au plan P d'équation $ax + by + cz + d = 0$ est :

$$d(M, P) = \frac{|ax + by + cz + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

13.5 Hyperplan médiateur dans un espace préhilbertien

E est un espace préhilbertien.

Théorème 13.5 Soient a, b deux points distincts de E . L'ensemble :

$$H = \{x \in E \mid \|x - a\| = \|x - b\|\}$$

est l'hyperplan affine passant par $c = \frac{1}{2}(a + b)$ (milieu du segment $[a, b]$) et de direction $H_0 = \{b - a\}^\perp$, soit :

$$H = \{x \in E \mid \langle x - c \mid b - a \rangle = 0\}$$

Démonstration. En notant $d = \frac{1}{2}(b - a)$, on a $a = c - d$, $b = c + d$ et :

$$\begin{aligned} \|x - a\|^2 - \|x - b\|^2 &= \|x - c + c - a\|^2 - \|x - c + c - b\|^2 \\ &= \|x - c + d\|^2 - \|x - c - d\|^2 \\ &= 4 \langle x - c \mid d \rangle \end{aligned}$$

de sorte que :

$$(x \in H) \Leftrightarrow (\|x - a\| = \|x - b\|) \Leftrightarrow (\langle x - c \mid d \rangle = 0)$$

■

Définition 13.4 Avec les notations du théorème, on dit que H est l'hyperplan médiateur du segment $[a, b]$.

Dans le cas où E est un plan euclidien, on parle plutôt de médiatrice.

À un tel hyperplan médiateur on associe les demi-hyperplans qui contiennent a et b respectivement, soit :

$$H_a = \{x \in E \mid \|x - a\| < \|x - b\|\}$$

et :

$$H_b = \{x \in E \mid \|x - a\| > \|x - b\|\}$$

La démonstration du théorème précédent nous dit que :

$$H_a = \{x \in E \mid \langle x - c \mid b - a \rangle < 0\}$$

et :

$$H_b = \{x \in E \mid \langle x - c \mid b - a \rangle > 0\}$$

où $c = \frac{1}{2}(a + b)$ est le milieu du segment $[a, b]$.

On a alors la partition de E :

$$E = H_a \cup H \cup H_b.$$

Comme dans le plan euclidien, on a le résultat suivant.

Théorème 13.6 Avec les notations précédentes, pour $x \in H_a$ et $y \in H_b$, l'intersection $[x, y] \cap H$ est réduite à un point.

Démonstration. Tout point de $[x, y]$ s'écrit de manière unique $z(t) = (1-t)x + ty$, où t est un réel dans $[0, 1]$ et il s'agit alors de montrer qu'il existe un unique réel $t \in [0, 1]$ tel que $z(t) \in H$. Pour ce faire, on introduit la fonction :

$$\begin{aligned} \varphi : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto \langle z(t) - c \mid b - a \rangle \end{aligned}$$

On a :

$$\begin{aligned} \varphi(t) &= \langle (1-t)x + ty - c \mid b - a \rangle \\ &= \langle t(y - x) + x - c \mid b - a \rangle \\ &= \langle y - x \mid b - a \rangle t + \langle x - c \mid b - a \rangle \end{aligned}$$

Cette fonction est dérivable de dérivée :

$$\begin{aligned} \varphi'(t) &= \langle y - x \mid b - a \rangle \\ &= \langle y - c \mid b - a \rangle - \langle x - c \mid b - a \rangle > 0 \end{aligned}$$

($x \in H_a$ et $y \in H_b$), elle donc strictement croissante et avec $\varphi(0) = \langle x - c \mid b - a \rangle < 0$, $\varphi(1) = \langle y - c \mid b - a \rangle > 0$, on déduit qu'il existe un unique $t \in]0, 1[$ tel que $\varphi(t) = 0$, ce qui équivaut à dire que $[x, y] \cap H$ est réduit à un point. ■

13.6 Intersection d'un hyperplan et d'une sphère dans un espace euclidien

E est toujours un espace euclidien.

Théorème 13.7 Soient S une sphère de centre ω et de rayon $R > 0$ et $H = x_0 + H_0$ un hyperplan affine de E avec $H_0 = \ker(\ell)$ où ℓ une forme linéaire non nulle. On note $d = d(\omega, H)$ la distance de ω à H .

1. Si $d > R$, alors $H \cap S = \emptyset$.
2. Si $d = R$, alors $H \cap S = \{p_H(\omega)\}$, où $p_H(\omega)$ est la projection orthogonale de ω sur H .
3. Si $d < R$, alors $H \cap S$ est une sphère de H de centre et de rayon $\sqrt{R^2 - d^2}$.

Démonstration. En posant $\omega_0 = \omega - x_0$, on a :

$$d = d(\omega, H) = d(\omega_0, H_0) = \|\omega_0 - p_{H_0}(\omega_0)\|.$$

Pour tout $x = x_0 + y \in H$ avec $y \in H_0$, on a :

$$\begin{aligned} \|x - \omega\|^2 &= \|y - (\omega - x_0)\|^2 = \|y - \omega_0\|^2 \\ &= \|(y - p_{H_0}(\omega_0)) + (p_{H_0}(\omega_0) - \omega_0)\|^2 \\ &= \|y - p_{H_0}(\omega_0)\|^2 + \|p_{H_0}(\omega_0) - \omega_0\|^2 \\ &= \|y - p_{H_0}(\omega_0)\|^2 + d^2 \end{aligned}$$

puisque $y - p_{H_0}(\omega_0) \in H_0$ et $p_{H_0}(\omega_0) - \omega_0 \in F^\perp$.

1. Si $d > R$, on a pour $x \in H$, $\|x - \omega\|^2 \geq d^2 > R^2$ et $x \notin S$. On a donc $H \cap S = \emptyset$.

2. Si $d = R$, on a pour $x \in H$, $\|x - \omega\|^2 = \|y - p_{H_0}(\omega_0)\|^2 + R^2$ et $\|x - \omega\| = R$ équivaut à $y = p_{H_0}(\omega_0)$. On a donc $H \cap S = \{x_0 + p_{H_0}(\omega_0)\} = \{p_H(\omega)\}$.
3. Supposons $d < R$. Si $x \in H \cap S$, on a alors :

$$\|y - p_{H_0}(\omega_0)\|^2 = \|x - \omega\|^2 - d^2 = R^2 - d^2$$

et $y \in S_0 = S(p_{H_0}(\omega_0), \sqrt{R^2 - d^2}) \subset H_0$, ce qui entraîne $x = x_0 + y \in S' = S(x_0 + p_{H_0}(\omega_0), \sqrt{R^2 - d^2}) \subset H$. Réciproquement si $x \in S'$, il est dans H , $y = x - x_0$ est dans S_0 et $\|x - \omega\|^2 = \|y - p_{H_0}(\omega_0)\|^2 + d^2 = R^2 - d^2 + d^2 = R^2$, soit $x \in S$. ■

Dans le cas où $H \cap S$ est réduit à un point, on dit que l'hyperplan H est tangent à la sphère S .

13.7 Intersection de deux sphères dans un espace euclidien

Si S et S' sont deux sphères de E de même centre ω (sphères concentriques) et de rayons respectifs R et R' , on vérifie facilement que $S \cap S' = \emptyset$ si $R \neq R'$ et $S \cap S' = S = S'$ si $R = R'$.

On s'intéresse maintenant à l'intersection de deux sphères non concentriques.

On se donne deux sphères non concentriques $S = S(\omega, R)$, $S' = S(\omega', R')$ (i. e. $\omega \neq \omega'$) et on note $\delta = \|\omega - \omega'\| > 0$ la distance entre les deux centres.

En supposant $S \cap S'$ non vide, on a pour tout $x \in S \cap S'$:

$$\begin{aligned} |R' - R| &= ||x - \omega'| - \|x - \omega|| \\ &\leq \|(x - \omega') - (x - \omega)\| = \|\omega - \omega'\| = \delta \\ &\leq \|x - \omega'\| + \|x - \omega\| = R + R' \end{aligned}$$

soit $|R' - R| \leq \delta \leq R + R'$.

Il en résulte que $S \cap S' = \emptyset$ si $\delta \notin [|R' - R|, R + R']$.

On suppose donc que $\delta \in [|R' - R|, R + R']$.

En notant $\omega_0 = \frac{1}{2}(\omega + \omega')$ le milieu du segment $[\omega, \omega']$ et $x_0 = \frac{1}{2}(\omega' - \omega)$, on a pour tout vecteur $x \in E$:

$$\|x - \omega'\|^2 - \|x - \omega\|^2 = 2\langle x | \omega - \omega' \rangle + \|\omega'\|^2 - \|\omega\|^2$$

avec $\omega - \omega' = -2x_0$ et :

$$\|\omega'\|^2 - \|\omega\|^2 = \|\omega_0 + x_0\|^2 - \|\omega_0 - x_0\|^2 = 4\langle \omega_0 | x_0 \rangle$$

ce qui donne :

$$\begin{aligned} \|x - \omega'\|^2 - \|x - \omega\|^2 &= 4(\langle \omega_0 | x_0 \rangle - \langle x | x_0 \rangle) \\ &= 4\langle \omega_0 - x | x_0 \rangle \end{aligned}$$

Si $x \in S \cap S'$, on a $\|x - \omega'\| = R'$, $\|x - \omega\| = R$ et l'identité précédente nous dit que x est dans l'hyperplan H d'équation $4\langle \omega_0 - x | x_0 \rangle = R'^2 - R^2$. Réciproquement si $x \in S \cap H$, on a $\|x - \omega\| = R$, $4\langle \omega_0 - x | x_0 \rangle = R'^2 - R^2$ et avec l'identité précédente, on déduit que :

$$\|x - \omega'\|^2 = \|x - \omega\|^2 + 4\langle \omega_0 - x | x_0 \rangle = R'^2$$

soit $x \in S \cap S'$.

On a donc $S \cap S' = S \cap H = S' \cap H$ (S et S' jouent des rôles symétriques), où H est l'hyperplan d'équation $4 \langle \omega_0 - x \mid x_0 \rangle = R'^2 - R^2$.

Si $R = R'$, H est alors l'hyperplan d'équation $\langle \omega_0 - x \mid x_0 \rangle = 0$, soit l'hyperplan passant par $\omega_0 = \frac{1}{2}(\omega + \omega')$ et de direction $H_0 = \{x_0\}^\perp = \{\omega' - \omega\}^\perp$, c'est-à-dire l'hyperplan médiateur de $[\omega, \omega']$. Dans ce cas, on a :

$$p_H(\omega) = \omega_0 + p_{H_0}(\omega - \omega_0) = \omega_0$$

puisque $\omega - \omega_0 = -x_0 \in H_0^\perp$. On a alors :

$$\begin{aligned} d &= d(\omega, H) = \|\omega - p_H(\omega)\| = \|\omega - \omega_0\| \\ &= \|x_0\| = \frac{\|\omega' - \omega\|}{2} = \frac{\delta}{2} \end{aligned}$$

avec $0 = |R' - R| \leq \delta \leq R + R' = 2R$.

Le théorème 13.7 nous dit alors que :

- si $\delta = \|\omega - \omega'\| = 2R$, alors $S \cap S' = S \cap H = \{\omega_0\}$;
- si $0 < \delta = \|\omega - \omega'\| < 2R$, alors $S \cap S'$ est la sphère de H de centre ω_0 et de rayon $\sqrt{R^2 - d^2} = \frac{\sqrt{4R^2 - \delta^2}}{2}$.

Dans le cas général x est dans $S \cap S' = S \cap H$ si, et seulement si :

$$\begin{cases} \|x - \omega\| = R \\ 4 \langle x - \omega_0 \mid x_0 \rangle = R^2 - R'^2 \end{cases} \quad (13.4)$$

En écrivant que $E = H_0 \oplus D_0$, où $H_0 = \{x_0\}^\perp$ et $D_0 = \mathbb{R}x_0$ et en plaçant l'origine en ω_0 , on a $x - \omega_0 = y + \lambda x_0$ avec $y \in H_0$ et $\lambda \in \mathbb{R}$. Avec $\omega = \omega_0 - x_0$, on a alors :

$$\begin{cases} \|x - \omega\|^2 = \|x - \omega_0 + x_0\|^2 = \|y + (\lambda + 1)x_0\|^2 = \|y\|^2 + (\lambda + 1)^2 \|x_0\|^2 \\ 4 \langle x - \omega_0 \mid x_0 \rangle = 4\lambda \|x_0\|^2 \end{cases}$$

de sorte que (13.4) est équivalent à :

$$\begin{cases} \|y\|^2 + (\lambda + 1)^2 \|x_0\|^2 = R^2 \\ 4\lambda \|x_0\|^2 = R^2 - R'^2 \end{cases}$$

ou encore en tenant compte de $\|x_0\| = \frac{\|\omega' - \omega\|}{2} = \frac{\delta}{2}$, à :

$$\begin{cases} \lambda = \frac{R^2 - R'^2}{\delta^2} \\ \|y\|^2 = \frac{4R^2 - (\lambda + 1)^2 \delta^2}{4} = \frac{(2R - (\lambda + 1)\delta)(2R + (\lambda + 1)\delta)}{4} \end{cases}$$

On a donc $\lambda + 1 = \frac{R^2 - R'^2 + \delta^2}{\delta^2}$ et :

$$\begin{aligned} 4R^2 - (\lambda + 1)^2 \delta^2 &= (2R - (\lambda + 1)\delta)(2R + (\lambda + 1)\delta) \\ &= \left(2R - \frac{R^2 - R'^2 + \delta^2}{\delta}\right) \left(2R + \frac{R^2 - R'^2 + \delta^2}{\delta}\right) \\ &= \frac{(R'^2 - (R^2 - 2R\delta + \delta^2))((R^2 + 2R\delta + \delta^2) - R'^2)}{\delta^2} \\ &= \frac{(R'^2 - (R - \delta)^2)((R + \delta)^2 - R'^2)}{\delta^2} \end{aligned}$$

ce qui donne :

$$\begin{aligned}
 \|y\|^2 &= \frac{(R'^2 - (R - \delta)^2)((R + \delta)^2 - R'^2)}{4\delta^2} \\
 &= \frac{(R' - (R - \delta))(R' + (R - \delta))((R + \delta) - R')((R + \delta) + R')}{4\delta^2} \\
 &= \frac{(R' - R + \delta)(R + \delta - R')(R' + R - \delta)(R + \delta + R')}{4\delta^2} \\
 &= \frac{(\delta^2 - (R' - R)^2)((R' + R)^2 - \delta^2)}{4\delta^2}
 \end{aligned}$$

Pour $|R' - R| \leq \delta \leq R + R'$, on a $\delta^2 - (R' - R)^2 \geq 0$ et $(R' + R)^2 - \delta^2 \geq 0$ et y est sur la sphère de H_0 de centre 0 et de rayon $R'' = \frac{\sqrt{\delta^2 - (R' - R)^2} \sqrt{(R' + R)^2 - \delta^2}}{2\delta}$, ce qui entraîne que $x = \omega_0 + \lambda x_0 + y$ est sur la sphère S'' de H de centre $\omega_0 + \lambda x_0$ et de rayon R'' (la condition $\lambda = \frac{R^2 - R'^2}{\delta^2} = \frac{R^2 - R'^2}{4\|x_0\|^2}$ donne $4\langle \omega_0 + \lambda x_0 - \omega_0 | x_0 \rangle = 4\lambda \|x_0\|^2 = R^2 - R'^2$ et $\omega_0 + \lambda x_0$ est bien dans H).

Réciproquement si $x = \omega_0 + \lambda x_0 + y$ avec $\lambda = \frac{R^2 - R'^2}{\delta^2}$ et $\|y\| = R''$ dans H_0 , on a $\omega_0 + \lambda x_0 \in H$, donc $x \in H$ et :

$$\begin{aligned}
 \|x - \omega\|^2 &= \|\omega_0 + \lambda x_0 + y - \omega\|^2 = \|y + (\lambda + 1)x_0\|^2 \\
 &= \|y\|^2 + (\lambda + 1)^2 \|x_0\|^2 \\
 &= \frac{(\delta^2 - (R' - R)^2)((R' + R)^2 - \delta^2)}{4\delta^2} + \left(\frac{R^2 - R'^2}{\delta^2} + 1\right)^2 \frac{\delta^2}{4} \\
 &= \frac{(\delta^2 - (R' - R)^2)((R' + R)^2 - \delta^2)}{4\delta^2} + \frac{(R^2 - R'^2 + \delta^2)^2}{4\delta^2} \\
 &= \frac{(\delta^2 - (R' - R)^2)((R' + R)^2 - \delta^2) + (R^2 - R'^2 + \delta^2)^2}{4\delta^2} = R^2
 \end{aligned}$$

(il suffit en fait de remonter les calculs).

En définitive, pour $|R' - R| \leq \delta \leq R + R'$, $S \cap S'$ est la sphère de H de centre $\omega_0 + \lambda x_0$ et de rayon R'' .

Cette sphère est réduite à un point pour $|R' - R| = \delta$ ou $\delta = R + R'$.

On a donc montré le théorème suivant qui généralise celui qu'on connaît pour l'intersection de deux cercles dans le plan euclidien.

Théorème 13.8 Soient $S = S(\omega, R)$, $S' = S(\omega', R')$ deux sphères non concentriques et $\delta = \|\omega - \omega'\|$ la distance entre les deux centres.

1. Si $\delta \notin [|R' - R|, R + R']$, alors $S \cap S' = \emptyset$.
2. Si $\delta \in [|R' - R|, R + R']$, alors $S \cap S'$ est non vide et $S \cap S' = S \cap H = S' \cap H$, où H est l'hyperplan d'équation $4\langle \omega_0 - x | x_0 \rangle = R^2 - R'^2$.

Cette intersection est la sphère de H de centre $\omega_0 + \lambda x_0$ et de rayon R'' , où $\omega_0 =$

$$\frac{1}{2}(\omega + \omega'), \quad x_0 = \frac{1}{2}(\omega' - \omega), \quad \lambda = \frac{R^2 - R'^2}{\delta^2} \quad \text{et} \quad R'' = \frac{\sqrt{\delta^2 - (R' - R)^2} \sqrt{(R' + R)^2 - \delta^2}}{2\delta}.$$

Pour $|R' - R| = \delta$ ou $\delta = R + R'$, cette sphère est réduite au point $\omega_0 + \lambda x_0$.

13.8 Inversion

Dans le plan complexe privé de l'origine, on définit l'inversion par $z \mapsto \frac{1}{\bar{z}} = \frac{z}{|z|^2}$.

De manière plus générale, on définit sur un espace préhilbertien E , l'inversion u par :

$$\forall x \in E \setminus \{0\}, u(x) = \frac{1}{\|x\|^2} x.$$

Lemme 13.1 *L'inversion u est involutive de $E \setminus \{0\}$ sur $E \setminus \{0\}$ et conserve les angles géométriques de vecteurs.*

Démonstration. L'application u est bien à valeurs dans $E \setminus \{0\}$. Pour tout $x \in E \setminus \{0\}$, on a $\|u(x)\| = \frac{1}{\|x\|}$ et :

$$u(u(x)) = \frac{1}{\|u(x)\|^2} u(x) = \|x\|^2 \frac{1}{\|x\|^2} x = x$$

c'est-à-dire que $u \circ u = Id$.

Pour tout $x \in E \setminus \{0\}$, le vecteur $u(x)$ est non nul et colinéaire à x , donc :

$$(u(x), u(y)) = (x, y)$$

pour tous x, y dans $E \setminus \{0\}$. ■

Lemme 13.2 *Pour tous x, y dans $E \setminus \{0\}$, on a :*

$$\|u(x) - u(y)\| = \frac{\|x - y\|}{\|x\| \|y\|}$$

Démonstration. On a :

$$\langle u(x) | u(y) \rangle = \frac{1}{\|x\|^2 \|y\|^2} \langle x | y \rangle$$

et :

$$\begin{aligned} \|u(x) - u(y)\|^2 &= \|u(x)\|^2 - 2 \langle u(x) | u(y) \rangle + \|u(y)\|^2 \\ &= \frac{1}{\|x\|^2} - 2 \frac{1}{\|x\|^2 \|y\|^2} \langle x | y \rangle + \frac{1}{\|y\|^2} \\ &= \frac{1}{\|x\|^2 \|y\|^2} (\|y\|^2 - 2 \langle x | y \rangle + \|x\|^2) \\ &= \frac{\|x - y\|^2}{\|x\|^2 \|y\|^2}. \end{aligned}$$
■

L'inversion peut être utilisée pour montrer une inégalité de Ptolémée comme suit.

Théorème 13.9 *Pour tous vecteurs x, y, z, t dans E , on a :*

$$\|t - x\| \|y - z\| \leq \|t - y\| \|x - z\| + \|t - z\| \|x - y\|$$

(inégalité de Ptolémée).

Démonstration. On suppose tout d'abord que $t = 0$. Il s'agit alors de montrer que pour x, y, z dans E , on a :

$$\|x\| \|y - z\| \leq \|y\| \|x - z\| + \|z\| \|x - y\|$$

Pour $x = 0$, on a $0 \leq \|y\| \|z\| + \|z\| \|y\|$, pour $y = 0$, on a $\|x\| \|z\| \leq \|z\| \|x\|$ et pour $z = 0$, on a $\|x\| \|y\| \leq \|y\| \|x\|$.

En supposant x, y, z non nuls, en divisant par $\|x\| \|y\| \|z\|$, il est équivalent de montrer que :

$$\frac{\|y - z\|}{\|y\| \|z\|} \leq \frac{\|x - z\|}{\|x\| \|z\|} + \frac{\|x - y\|}{\|x\| \|y\|}$$

soit :

$$\|u(y) - u(z)\| \leq \|u(x) - u(z)\| + \|u(x) - u(y)\|$$

ce qui se déduit de l'inégalité triangulaire :

$$\begin{aligned} \|u(y) - u(z)\| &= \|(u(y) - u(x)) + (u(x) - u(z))\| \\ &\leq \|u(y) - u(x)\| + \|u(x) - u(z)\|. \end{aligned}$$

On place ensuite, pour t quelconque, l'origine en t , ce qui revient à poser $x' = x - t$, $y' = y - t$ et $z' = z - t$ dans l'inégalité :

$$\|x'\| \|y' - z'\| \leq \|y'\| \|x' - z'\| + \|z'\| \|x' - y'\|$$

et donne :

$$\|t - x\| \|y - z\| \leq \|t - y\| \|x - z\| + \|t - z\| \|x - y\|.$$

■

Remarque 13.2 On peut montrer que l'inégalité de Ptolémée est caractéristique des normes qui dérivent d'un produit scalaire.

13.9 Symétries orthogonales dans les espaces euclidiens

On suppose ici que E est un espace euclidien de dimension n .

Définition 13.5 Si F est un sous-espace vectoriel de E , la symétrie orthogonale par rapport à F est l'application définie sur E par :

$$\forall x \in E, s_F(x) = p_F(x) - p_{F^\perp}(x).$$

Comme p_F et p_{F^\perp} , l'application s_F est linéaire.

Remarque 13.3 Pour $F = \{0\}$, on a $s_F = -Id$ et pour $F = E$, $s_F = Id$. On supposera a priori que F distinct de $\{0\}$ et de E (sous-espace vectoriel propre de E).

Avec $p_F + p_{F^\perp} = Id$, on déduit que s_F est aussi définie par :

$$\forall x \in E, s_F(x) = 2p_F(x) - x = x - 2p_{F^\perp}(x).$$

Si $D = \mathbb{R}a$ est une droite vectorielle, on a :

$$s_D(x) = 2p_D(x) - x = 2 \frac{\langle x | a \rangle}{\|a\|^2} a - x.$$

Si $H = D^\perp$ est un hyperplan d'un espace euclidien, on a :

$$s_H(x) = 2p_H(x) - x = x - 2 \frac{\langle x | a \rangle}{\|a\|^2} a.$$

Définition 13.6 On appelle *réflexion* une symétrie orthogonale par rapport à un hyperplan et *demi-tour* ou *retournement* une symétrie orthogonale par rapport à une droite.

Des propriétés des projections orthogonales, on déduit le résultat suivant.

Théorème 13.10 Soit F un sous espace vectoriel de E .

1. Pour $x \in E$, on a $x \in F$ si, et seulement si, $s_F(x) = x$ et $x \in F^\perp$ si, et seulement si, $s_F(x) = -x$.
2. $s_F \circ s_F = Id$ (on dit que s_F est une involution). Une symétrie orthogonale est donc un automorphisme de E avec $s_F^{-1} = s_F$.
3. Pour tous x, y dans E , on a :

$$\langle s_F(x) | y \rangle = \langle x | s_F(y) \rangle$$

(s_F est auto-adjoint).

4. Pour tous x, y dans E , on a :

$$\langle s_F(x) | s_F(y) \rangle = \langle x | y \rangle$$

(on dit que s_F est une isométrie).

5. On a $s_F + s_{F^\perp} = 0$ et $s_F \circ s_{F^\perp} = s_{F^\perp} \circ s_F = -Id$.
6. Si F est de dimension $p \in \{1, \dots, n-1\}$, il existe alors une base orthonormée de E dans laquelle la matrice de s_F est $\begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}$ et $\det(s_F) = (-1)^{n-p}$.

Démonstration.

1. On a :

$$x \in F \Leftrightarrow p_F(x) = x \Leftrightarrow s_F(x) = x$$

et :

$$x \in F^\perp \Leftrightarrow p_{F^\perp}(x) = x \Leftrightarrow s_F(x) = -x$$

2. On a :

$$\begin{aligned} s_F \circ s_F &= (p_F - p_{F^\perp}) \circ (p_F - p_{F^\perp}) \\ &= p_F \circ p_F - p_{F^\perp} \circ p_F - p_F \circ p_{F^\perp} + p_{F^\perp} \circ p_{F^\perp} \\ &= p_F + p_{F^\perp} = Id \end{aligned}$$

3. On a :

$$\begin{aligned} \langle s_F(x) | y \rangle &= 2 \langle p_F(x) | y \rangle - \langle x | y \rangle \\ &= 2 \langle x | p_F(y) \rangle - \langle x | y \rangle \\ &= \langle x | 2p_F(y) \rangle - \langle x | y \rangle = \langle x | s_F(y) \rangle \end{aligned}$$

4. On a :

$$\langle s_F(x) | s_F(y) \rangle = \langle x | s_F \circ s_F(y) \rangle = \langle x | y \rangle$$

5. On a :

$$s_F + s_{F^\perp} = (p_F - p_{F^\perp}) + (p_{F^\perp} - p_F) = 0$$

et :

$$\begin{aligned} s_F \circ s_{F^\perp} &= (p_F - p_{F^\perp}) \circ (p_{F^\perp} - p_F) \\ &= p_F \circ p_{F^\perp} - p_{F^\perp} \circ p_{F^\perp} - p_F \circ p_F + p_{F^\perp} \circ p_F \\ &= -p_{F^\perp} - p_F = -Id. \end{aligned}$$

6. Il suffit de se placer dans une base formée de la réunion d'une base orthonormée de F et d'une base orthonormée de F^\perp . ■

Exemple 13.2 Si s_H est une réflexion, on a $\det(s_H) = -1$ et si s_D est un demi-tour, on a $\det(s_D) = (-1)^{n-1}$.

Exercice 13.2 Soient F, G deux sous espaces vectoriels de E tels que $F \subset G^\perp$ (F et G sont orthogonaux). Montrer que $s_F \circ s_G = s_G \circ s_F = s_H$, où $H = (F \oplus G)^\perp$.

Solution 13.2 Pour $x \in H^\perp = F \oplus G$, il existe $(y, z) \in F \times G \subset G^\perp \times G$ tel que $x = y + z$ et on a :

$$s_G(x) = z - y$$

puis comme $G = (G^\perp)^\perp \subset F^\perp$, on a aussi $(y, z) \in F \times F^\perp$ et :

$$s_F(s_G(x)) = -y - z = -x$$

Pour $x \in H = (F \oplus G)^\perp = F^\perp \cap G^\perp$, on a :

$$s_G(s_F(x)) = s_G(-x) = -(-x) = x$$

On a donc $s_F \circ s_G = s_H$ et comme les sous-espaces F et G jouent des rôles symétriques, on a aussi $s_G \circ s_F = s_H$.

13.10 Isométries

E est un espace préhilbertien.

Définition 13.7 Une isométrie (ou application orthogonale) de E est une application $u : E \rightarrow E$ qui conserve le produit scalaire, c'est-à-dire que :

$$\forall (x, y) \in E \times E, \langle u(x) | u(y) \rangle = \langle x | y \rangle$$

On note $\mathcal{O}(E)$ l'ensemble des isométries de E .

Exemple 13.3 Les seules homothéties $x \mapsto \lambda x$ qui sont des isométries sont Id et $-Id$. En effet pour $e \in E$ de norme égale à 1, on a $1 = \|e\|^2 = \|u(e)\|^2 = \lambda^2$ et $\lambda = \pm 1$.

Exemple 13.4 Les symétries orthogonales sont des isométries (point 4. du théorème 13.10).

Exercice 13.3 Soient a un vecteur non nul dans E , α un réel et u l'application linéaire définie par :

$$\forall x \in E, u(x) = x + \alpha \langle x | a \rangle a$$

Déterminer les valeurs de α pour lesquelles u est une isométrie.

Solution 13.3 Pour $\alpha = 0$, u est l'identité et c'est une isométrie.

Pour $\alpha \neq 0$ et $x \in E$, on a :

$$\|u(x)\|^2 = \langle x | a \rangle^2 \|a\|^2 \alpha^2 + 2 \langle x | a \rangle^2 \alpha + \|x\|^2$$

Si $u \in \mathcal{O}(E)$, on a alors $\|u(x)\|^2 = \|x\|^2$ pour tout $x \in E$, ce qui équivaut à :

$$\langle x | a \rangle^2 (\|a\|^2 \alpha + 2) = 0$$

ou encore à $\|a\|^2 \alpha + 2 = 0$ et donne $\alpha = -\frac{2}{\|a\|^2}$.

Réciproquement, si $\alpha = -\frac{2}{\|a\|^2}$, l'application u est définie par :

$$\forall x \in E, u(x) = x - 2 \frac{\langle x | a \rangle}{\|a\|^2} a$$

et on reconnaît ici la réflexion par rapport à l'hyperplan orthogonal au vecteur a (on a $u(x) = x$ pour $\langle x | a \rangle = 0$ et $u(a) = -a$).

Exercice 13.4 Soient a un vecteur non nul dans E , α un réel et u l'application linéaire définie par :

$$\forall x \in E, u(x) = \alpha \langle x | a \rangle a - x$$

Déterminer les valeurs de α pour lesquelles u est une isométrie.

Solution 13.4 Pour $\alpha = 0$, u est l'homothétie de rapport -1 ($u = -Id$) et c'est une isométrie.

Pour $\alpha \neq 0$ et $x \in E$, on a :

$$\|u(x)\|^2 = \langle x | a \rangle^2 \|a\|^2 \alpha^2 - 2 \langle x | a \rangle^2 \alpha + \|x\|^2$$

Si $u \in \mathcal{O}(E)$, on a alors $\|u(x)\|^2 = \|x\|^2$ pour tout $x \in E$, ce qui équivaut à :

$$\langle x | a \rangle^2 (\|a\|^2 \alpha - 2) = 0$$

ou encore à $\|a\|^2 \alpha - 2 = 0$ et donne $\alpha = \frac{2}{\|a\|^2}$.

Réciproquement, si $\alpha = \frac{2}{\|a\|^2}$, l'application u est définie par :

$$\forall x \in E, u(x) = 2 \frac{\langle x | a \rangle}{\|a\|^2} a - x$$

et on reconnaît ici le demi-tour par rapport à la droite dirigée par a (on a $u(x) = -x$ pour $\langle x | a \rangle = 0$ et $u(a) = a$).

Remarque 13.4 Une isométrie conserve l'orthogonalité, c'est-à-dire que pour tous x, y dans E , on a :

$$\langle x | y \rangle = 0 \Rightarrow \langle u(x) | u(y) \rangle = 0$$

mais une application qui conserve l'orthogonalité n'est pas nécessairement une isométrie comme le montre l'exemple d'une homothétie de rapport $\lambda \notin \{-1, 1\}$.

Exercice 13.5 Soit E un espace euclidien de dimension $n \geq 2$, $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base ortho-normée de E et u une application linéaire de E dans E qui conserve l'orthogonalité.

1. Montrer que $\|u(e_i)\| = \|u(e_j)\|$ pour tous i, j compris entre 1 et n . On notera λ cette valeur commune.
2. Montrer que $\|u(x)\| = \lambda \|x\|$ pour tout $x \in E$ (pour $\lambda > 0$, on dit que u est une similitude de rapport λ).

Solution 13.5

1. Pour $1 \leq i, j \leq n$, on vérifie facilement que les vecteurs $e_i - e_j$ et $e_i + e_j$ sont orthogonaux, donc :

$$\langle u(e_i - e_j) | u(e_i + e_j) \rangle = 0$$

et avec :

$$\begin{aligned} \langle u(e_i - e_j) | u(e_i + e_j) \rangle &= \langle u(e_i) - u(e_j) | u(e_i) + u(e_j) \rangle \\ &= \|u(e_i)\|^2 - \|u(e_j)\|^2 \end{aligned}$$

on déduit que $\|u(e_i)\| = \|u(e_j)\|$.

2. Pour tout vecteur $x = \sum_{i=1}^n x_i e_i$, on a $u(x) = \sum_{i=1}^n x_i u(e_i)$ et :

$$\begin{aligned} \|u(x)\|^2 &= \sum_{i=1}^n x_i^2 \|u(e_i)\|^2 + 2 \sum_{1 \leq i < j} x_i x_j \langle u(e_i) | u(e_j) \rangle \\ &= \sum_{i=1}^n x_i^2 \|u(e_i)\|^2 = \lambda^2 \sum_{i=1}^n x_i^2 = \lambda^2 \|x\|^2 \end{aligned}$$

$$(\langle e_i | e_j \rangle = 0 \text{ pour } i \neq j \Rightarrow \langle u(e_i) | u(e_j) \rangle = 0).$$

Théorème 13.11 Une application $u : E \rightarrow E$ est une isométrie si, et seulement si, elle est linéaire et conserve la norme, c'est-à-dire que :

$$\forall x \in E, \|u(x)\| = \|x\|$$

Démonstration. Si u est linéaire et conserve la norme, on déduit alors de l'identité de polarisation qu'elle conserve le produit scalaire. En effet, pour tous x, y dans E , on a :

$$\begin{aligned} \langle u(x) | u(y) \rangle &= \frac{1}{4} (\|u(x) + u(y)\|^2 - \|u(x) - u(y)\|^2) \\ &= \frac{1}{4} (\|u(x + y)\|^2 - \|u(x - y)\|^2) \quad (\text{linéarité}) \\ &= \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2) \quad (\text{conservation de la norme}) \\ &= \langle x | y \rangle \end{aligned}$$

Réciproquement, si u est une application de E dans E qui conserve le produit scalaire, il est clair qu'elle conserve la norme. Il nous reste à montrer qu'elle est linéaire.

Pour x, y dans E et λ dans \mathbb{R} , on a :

$$\begin{aligned}\|u(x + \lambda y) - u(x) - \lambda u(y)\|^2 &= \|u(x + \lambda y)\|^2 + \|u(x)\|^2 + \lambda^2 \|u(y)\|^2 \\ &\quad - 2(\langle u(x + \lambda y) | u(x) \rangle + \lambda \langle u(x + \lambda y) | u(y) \rangle) \\ &\quad + 2\lambda \langle u(x) | u(y) \rangle \\ &= \|x + \lambda y\|^2 + \|x\|^2 + \lambda^2 \|y\|^2 \\ &\quad - 2(\langle x + \lambda y | x \rangle + \lambda \langle x + \lambda y | y \rangle) \\ &\quad + 2\lambda \langle x | y \rangle \\ &= 2\|x\|^2 + 2\lambda^2 \|y\|^2 + 2\lambda \langle x | y \rangle \\ &\quad - 2\|x\|^2 - 4\lambda \langle x | y \rangle - 2\lambda^2 \|y\|^2 \\ &\quad + 2\lambda \langle x | y \rangle = 0\end{aligned}$$

ce qui équivaut à $u(x + \lambda y) = u(x) + \lambda u(y)$ et u est linéaire. ■

Remarque 13.5 Une application $u : E \rightarrow E$ qui conserve la norme n'est pas nécessairement linéaire et n'est donc pas une isométrie en général. Par exemple pour $e \in E$ de norme égale à 1, l'application $u : x \mapsto \|x\|e$ conserve la norme et n'est pas linéaire ($u(-x) = u(x) \neq -u(x)$ pour $x \neq 0$).

Exercice 13.6 Soit u une application de E dans E qui conserve les distances, c'est-à-dire que :

$$\forall (x, y) \in E \times E, \|u(x) - u(y)\| = \|x - y\|$$

Montrer qu'il existe un vecteur $a \in E$ et une isométrie v de E tels que $u(x) = a + v(x)$ pour tout $x \in E$.

Solution 13.6 Soient $a = u(0)$ et $v : E \rightarrow E$ définie par $v(x) = u(x) - a$, pour tout $x \in E$. Pour tous x, y dans E , on a :

$$\begin{aligned}\|v(x)\| &= \|u(x) - u(0)\| = \|x - 0\| = \|x\| \\ \|v(x) - v(y)\|^2 &= \|u(x) - u(y)\|^2 = \|x - y\|^2\end{aligned}$$

soit :

$$\|v(x)\|^2 - 2\langle v(x) | v(y) \rangle + \|v(y)\|^2 = \|x\|^2 - 2\langle x | y \rangle + \|y\|^2$$

et en conséquence $\langle v(x) | v(y) \rangle = \langle x | y \rangle$. L'application v est donc orthogonale.

Théorème 13.12 Si E est un espace euclidien (donc de dimension finie), alors une isométrie est un automorphisme de E et $\mathcal{O}(E)$ est un sous-groupe de $GL(E)$.

Démonstration. Soit $u \in \mathcal{O}(E)$. Pour $x \in \ker(u)$, on a $0 = \|u(x)\| = \|x\|$ et $x = 0$. Donc $\ker(u) = \{0\}$ et u est injective, ce qui équivaut à dire que u est un automorphisme de E dans le cas où E est de dimension finie.

On a $Id \in \mathcal{O}(E)$ et pour u, v dans $\mathcal{O}(E)$, x dans E , on a :

$$\begin{aligned}\|u \circ v(x)\| &= \|u(v(x))\| = \|v(x)\| = \|x\| \\ \|u^{-1}(x)\| &= \|u(u^{-1}(x))\| = \|x\|\end{aligned}$$

donc $u \circ v$ et u^{-1} sont dans $\mathcal{O}(E)$. L'ensemble $\mathcal{O}(E)$ est donc bien un sous-groupe de $GL(E)$. ■

On dit, dans le cas où E est de dimension finie, que $\mathcal{O}(E)$ est le groupe orthogonal de E .

Remarque 13.6 Si E est de dimension finie, une isométrie est toujours injective (son noyau est réduit à $\{0\}$), mais n'est pas nécessairement surjective.

Donc, dans le cas de la dimension infinie, $\mathcal{O}(E)$ n'est pas un groupe.

Considérons par exemple un espace préhilbertien E de dimension infinie dénombrable (par exemple $E = \mathbb{R}[x]$ muni du produit scalaire $(P, Q) \mapsto \int_0^1 P(x)Q(x)dx$). On se donne une base orthonormée $(e_n)_{n \in \mathbb{N}}$ (le procédé de Gram-Schmidt nous permet de construire une telle base) et on définit l'endomorphisme u par $u(e_n) = e_{n+1}$ pour tout entier $n \geq 0$. Pour $x = \sum_{k=0}^{n_x} x_k e_k$

dans E , on a $u(x) = \sum_{k=0}^{n_x} x_k e_{k+1}$ et $\|u(x)\|^2 = \sum_{k=0}^{n_x} x_k^2 = \|x\|^2$ et u est une isométrie. Comme $\text{Im}(u) = \text{Vect}\{e_k \mid k \in \mathbb{N}^*\} \neq E$, cette application n'est pas surjective.

Remarque 13.7 On peut donner, dans un espace préhilbertien, la définition suivante d'une isométrie : une isométrie est un automorphisme qui conserve la norme et dans ce cas $\mathcal{O}(E)$ est un sous-groupe de $GL(E)$.

De l'injectivité et de la conservation de l'orthogonalité par une isométrie, on déduit le résultat suivant.

Théorème 13.13 Soit u une isométrie de l'espace préhilbertien E . Si F est un sous-espace vectoriel de E de dimension finie stable par u , alors son orthogonal F^\perp est aussi stable par u .

Démonstration. Comme u est injective, on a $\dim(u(F)) = \dim(F)$ et avec $u(F) \subset D$, on déduit que $u(F) = F$.

Pour $x \in F^\perp$ et $y \in F$, on a :

$$\langle u(x) \mid u(y) \rangle = \langle x \mid y \rangle = 0$$

donc $u(x) \in (u(F))^\perp = F^\perp$. ■

Théorème 13.14 Soient E un espace euclidien, $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E et u une application linéaire de E dans E . L'application u est une isométrie si, et seulement si, elle transforme \mathcal{B} en une base orthonormée de E .

Démonstration. Supposons que $u \in \mathcal{O}(E)$. Avec $\langle u(e_i) \mid u(e_j) \rangle = \langle e_i \mid e_j \rangle = \delta_{ij}$ pour $1 \leq i, j \leq n$, on déduit que $u(\mathcal{B}) = (u(e_i))_{1 \leq i \leq n}$ est orthonormé. Il en résulte que $u(\mathcal{B})$ est libre et c'est une base puisque formé de $n = \dim(E)$ vecteurs.

Réciproquement supposons que $u \in \mathcal{L}(E)$ transforme \mathcal{B} en une base orthonormée de E . On a alors pour tout $x = \sum_{i=1}^n x_i e_i$ dans E :

$$\|u(x)\|^2 = \left\| \sum_{i=1}^n x_i u(e_i) \right\|^2 = \sum_{i=1}^n x_i^2 = \|x\|^2$$

et $u \in \mathcal{O}(E)$. ■

Ce théorème va nous donner une caractérisation des matrices d'isométries dans une base orthonormée de E .

En munissant \mathbb{R}^n de sa structure euclidienne canonique et en notant pour toute matrice réelle $A = ((a_{ij}))_{1 \leq i, j \leq n}$ par $C_j = (a_{ij})_{1 \leq i \leq n} \in \mathbb{R}^n$ la colonne numéro $j \in \{1, \dots, n\}$ de A , on a :

$${}^tAA = ((\alpha_{ij}))_{1 \leq i, j \leq n}$$

avec :

$$\begin{aligned} \alpha_{ij} &= (\text{ligne } i \text{ de } {}^tA) (\text{colonne } j \text{ de } A) = {}^tC_i C_j \\ &= (a_{1i}, \dots, a_{ni}) \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = \sum_{k=1}^n a_{ki} a_{kj} = \langle C_i \mid C_j \rangle. \end{aligned}$$

De plus si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est une base orthonormée de E , en notant pour tout $x = \sum_{i=1}^n x_i e_i$ dans E , $X = (x_i)_{1 \leq i \leq n} \in \mathbb{R}^n$ le vecteur colonne formé des composantes de X dans \mathcal{B} , on a pour tous x, y dans E :

$$\langle x \mid y \rangle = \sum_{k=1}^n x_k y_k = \langle X \mid Y \rangle$$

le produit scalaire de gauche étant celui de E et celui de droite celui de \mathbb{R}^n .

Théorème 13.15 *Soient E un espace euclidien, $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E et u une application linéaire de E dans E de matrice A dans \mathcal{B} . L'application u est une isométrie si, et seulement si, ${}^tAA = A {}^tA = I_n$.*

Démonstration. Supposons que $u \in \mathcal{O}(E)$. En notant ${}^tAA = ((\alpha_{ij}))_{1 \leq i, j \leq n}$ et en utilisant les notations qui précèdent, on a, pour $1 \leq i, j \leq n$:

$$\alpha_{ij} = \langle C_i \mid C_j \rangle = \langle u(e_i) \mid u(e_j) \rangle = \langle e_i \mid e_j \rangle = \delta_{ij}$$

ce qui signifie que ${}^tAA = I_n$. La matrice A est donc inversible d'inverse tA et en conséquence, on a aussi $A {}^tA = I_n$.

Réciproquement, si ${}^tAA = A {}^tA = I_n$, on a alors pour $1 \leq i, j \leq n$:

$$\langle u(e_i) \mid u(e_j) \rangle = \langle C_i \mid C_j \rangle = \delta_{ij}$$

ce qui signifie que $u(\mathcal{B})$ est une base orthonormée de E et $u \in \mathcal{O}(E)$. ■

Définition 13.8 *On appelle matrice orthogonale, une matrice réelle A telle que ${}^tAA = A {}^tA = I_n$.*

On note $\mathcal{O}_n(\mathbb{R})$ l'ensemble des matrices orthogonales.

Il revient au même de dire qu'une matrice orthogonale est une matrice inversible A d'inverse tA .

Le théorème précédent nous dit qu'une application linéaire u de E dans E est une isométrie si, et seulement si, sa matrice dans une base orthonormée quelconque de E est orthogonale.

Théorème 13.16 *Pour toute matrice A dans $\mathcal{O}_n(\mathbb{R})$, on a $\det(A) = \pm 1$ et $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.*

Démonstration. De $\det(A) = \det({}^t A)$ pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$ et ${}^t AA = A {}^t A = I_n$ pour $A \in \mathcal{O}_n(\mathbb{R})$, on déduit que $(\det(A))^2 = 1$ et $\det(A) = \pm 1$.

Il en résulte que $\mathcal{O}_n(\mathbb{R}) \subset GL_n(\mathbb{R})$.

Comme $I_n \in \mathcal{O}_n(\mathbb{R})$ et pour A, B dans $\mathcal{O}_n(\mathbb{R})$, on a :

$$(A^{-1})^{-1} = ({}^t A)^{-1} = {}^t A^{-1}$$

$$(AB)^{-1} = B^{-1}A^{-1} = {}^t B {}^t A = {}^t (AB)$$

on en déduit que $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$. ■

Corollaire 13.2 Si u est une isométrie d'un espace euclidien E , on a alors $\det(u) = \pm 1$.

Démonstration. On a $\det(u) = \det(A)$ où A est la matrice de u dans une base orthonormée et $u \in \mathcal{O}(E)$ si, et seulement si, $A \in \mathcal{O}_n(\mathbb{R})$, ce qui entraîne $\det(A) = \pm 1$. ■

On note :

$$\mathcal{O}^+(E) = \{u \in \mathcal{O}(E) \mid \det(u) = 1\}$$

$$\mathcal{O}_n^+(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) = 1\}$$

$$\mathcal{O}^-(E) = \{u \in \mathcal{O}(E) \mid \det(u) = -1\}$$

$$\mathcal{O}_n^-(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) = -1\}$$

et on dit que les éléments de $\mathcal{O}^+(E)$ [resp. $\mathcal{O}_n^+(\mathbb{R})$] sont des automorphismes orthogonaux positifs ou des isométries directes ou des rotations vectorielles [resp. des matrices orthogonales positives] et les éléments de $\mathcal{O}^-(E)$ [resp. $\mathcal{O}_n^-(\mathbb{R})$] sont des automorphismes orthogonaux négatifs [resp. les matrices orthogonales négative].

Théorème 13.17 $\mathcal{O}^+(E)$ [resp. $\mathcal{O}_n^+(\mathbb{R})$] est un sous-groupe distingué de $\mathcal{O}(E)$ [resp. de $\mathcal{O}_n(\mathbb{R})$] d'indice 2.

Démonstration. Voir le paragraphe 20.8. ■

Exercice 13.7 Dans l'espace vectoriel $E = \mathbb{R}^4$ muni de sa structure euclidienne canonique, on désigne par u l'endomorphisme dont la matrice dans la base canonique est :

$$A = \frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \end{pmatrix}$$

1. Montrer que $u \in \mathcal{O}^+(E)$.
2. Soit H un hyperplan de E d'équation $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4 = 0$, où les α_i ne sont pas tous nuls. Déterminer l'image de H par u .

Solution 13.7

1. On vérifie que $A \in \mathcal{O}_4^+(\mathbb{R})$, ce qui équivaut à $u \in \mathcal{O}^+(E)$.
2. On a $H = \{a\}^\perp$, où a est le vecteurs de coordonnées $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ dans la base canonique et pour tout $x \in H$, on a $\langle u(x) \mid u(a) \rangle = \langle x \mid a \rangle = 0$, ce qui signifie que $u(x) \in \{u(a)\}^\perp$. On a donc $H \subset \{u(a)\}^\perp$, avec $u(a) \neq 0$ puisque $a \neq 0$ et u est un isomorphisme, donc $\{u(a)\}^\perp$ est un hyperplan et $H = \{u(a)\}^\perp$ puisque ces deux espaces sont de dimension 3.

En définitive, $u(H)$ est l'hyperplan d'équation $\langle u(a) \mid x \rangle = 0$.

On rappelle que si $A = ((a_{ij}))_{1 \leq i, j \leq n}$ est une matrice carrée d'ordre n , la matrice des cofacteurs de A est la matrice $C = ((c_{ij}))_{1 \leq i, j \leq n}$, où $c_{ij} = (-1)^{i+j} \det(A_{ij})$ en notant A_{ij} la matrice carrée d'ordre $n-1$ déduite de A en supprimant la ligne numéro i et la colonne numéro j . On a alors :

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

et dans le cas où A est inversible, $A^{-1} = \frac{1}{\det(A)} {}^t C$.

Théorème 13.18 Si $A \in \mathcal{O}_n^+(\mathbb{R})$ [resp. $A \in \mathcal{O}_n^-(\mathbb{R})$], on a alors $A = C$ [resp. $A = -C$], où C est la matrice des cofacteurs de A .

Démonstration. Résulte de :

$$A^{-1} = \frac{1}{\det(A)} {}^t C = \pm {}^t C = {}^t A$$

pour $A \in \mathcal{O}_n(\mathbb{R})$. ■

13.11 Orientation d'un espace euclidien

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

La notion d'isométrie nous permet de retrouver le théorème 12.7.

Théorème 13.19 Si $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ sont deux bases orthonormées de E , alors la matrice de passage P de \mathcal{B} à \mathcal{B}' est une matrice orthogonale.

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

Avec les notations du théorème, on a $\det(P) = \pm 1$.

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

Théorème 13.20 La relation \sim ainsi définie est une relation d'équivalence et il y a exactement deux classes d'équivalence pour cette relation.

Démonstration. Cette relation est réflexive puisque $I_n \in \mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{B} = I_d(\mathcal{B})$.

Cette relation est symétrique puisque $P \in \mathcal{O}_n^+(\mathbb{R})$ entraîne $P^{-1} \in \mathcal{O}_n^+(\mathbb{R})$ et si P est la matrice de passage de \mathcal{B} à \mathcal{B}' , alors P^{-1} est la matrice de passage de \mathcal{B}' à \mathcal{B} .

Cette relation est transitive puisque le produit de deux matrices de $\mathcal{O}_n^+(\mathbb{R})$ est dans $\mathcal{O}_n^+(\mathbb{R})$ ($\mathcal{O}_n^+(\mathbb{R})$ est un groupe).

Soit $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E fixée.

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

$$\mathcal{B}^- = (e_1, \dots, e_{n-1}, -e_n)$$

la matrice de passage P^- de \mathcal{B}^- à \mathcal{B}' est :

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

et $\det(P^-) = -\det(P) = 1$, donc $P^{-1} \in \mathcal{O}_n^+(\mathbb{R})$ et $\mathcal{B}' \sim \mathcal{B}^-$.

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

Définition 13.9 Orienter l'espace euclidien E revient à choisir une base orthonormée E .

Le théorème précédent nous dit qu'il n'y a que deux orientations possibles pour E .

Définition 13.10 Si l'espace E est orienté par le choix d'une base orthonormée \mathcal{B} , on dit qu'une base orthonormée \mathcal{B}' est directe (ou qu'elle définit la même orientation que \mathcal{B}) si \mathcal{B}' est dans la classe d'équivalence de \mathcal{B} et on dit que cette base \mathcal{B}' est indirecte dans le cas contraire.

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

Exercice 13.8 On suppose que E est orienté par le choix d'une base orthonormée $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et on se donne une permutation σ de $\{1, 2, \dots, n\}$. À quelle condition portant sur σ la base $\mathcal{B}_\sigma = (e_{\sigma(i)})_{1 \leq i \leq n}$ est-elle directe ?

Solution 13.8 En notant $\varepsilon(\sigma)$ la signature de la permutation σ , on a $\det_{\mathcal{B}}(\mathcal{B}_\sigma) = \varepsilon(\sigma) \det(I_n) = \varepsilon(\sigma)$ et \mathcal{B}_σ est directe si, et seulement si, σ est une permutation paire.

13.12 Produit vectoriel dans un espace euclidien

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

On rappelle que si \mathcal{B} est une autre base de E , alors pour tout n -uplet (x_1, x_2, \dots, x_n) de vecteurs de E , on a :

$$\det_{\mathcal{B}_0}(x_1, x_2, \dots, x_n) = \det_{\mathcal{B}_0}(\mathcal{B}) \det_{\mathcal{B}}(x_1, x_2, \dots, x_n)$$

(théorème 10.13).

Il en résulte que la quantité $\det_{\mathcal{B}}(x_1, x_2, \dots, x_n)$ est indépendante du choix d'une base orthonormée directe \mathcal{B} de E . On la note $\det(x_1, x_2, \dots, x_n)$ (ce qui suppose le choix d'une orientation de E) et on dit que c'est le produit mixte des vecteurs ordonnés x_1, x_2, \dots, x_n . On le note parfois $[x_1, x_2, \dots, x_n]$.

En remarquant que, pour tout $(n-1)$ -uplet x_1, x_2, \dots, x_{n-1} de vecteurs de E , l'application $x \mapsto \det(x_1, x_2, \dots, x_{n-1}, x)$ est une forme linéaire, on déduit du théorème 13.3 qu'il existe un unique vecteur $a \in E$ tel que :

$$\forall x \in E, \det(x_1, x_2, \dots, x_{n-1}, x) = \langle a | x \rangle \quad (13.5)$$

ce vecteur a étant fonction des vecteurs x_1, x_2, \dots, x_{n-1} .

On peut donc donner la définition suivante.

Définition 13.11 *Le produit vectoriel (ou produit extérieur) des $n-1$ vecteurs x_1, x_2, \dots, x_{n-1} de E est le vecteur a défini par (13.5). On le note $x_1 \wedge x_2 \wedge \dots \wedge x_{n-1}$.*

Dans la base orthonormée \mathcal{B}_0 , en notant $x_i = \sum_{j=1}^n x_{ij} e_j$ pour tout i compris entre 1 et n , les réels :

$$\det(x_1, x_2, \dots, x_{n-1}, e_i) = \langle x_1 \wedge x_2 \wedge \dots \wedge x_{n-1} \mid e_i \rangle$$

sont les composantes du vecteur $x_1 \wedge x_2 \wedge \dots \wedge x_{n-1}$ dans la base \mathcal{B}_0 . On a donc :

$$x_1 \wedge x_2 \wedge \dots \wedge x_{n-1} = \sum_{i=1}^n (-1)^{i+n} \delta_i e_i \quad (13.6)$$

où δ_i est le déterminant de la matrice d'ordre $n-1$ déduite de la matrice $(X_1, X_2, \dots, X_{n-1})$ en supprimant de cette matrice la ligne numéro i (X_i étant le vecteur de \mathbb{R}^n formé des composantes de x_i dans la base \mathcal{B}).

Remarque 13.8 $(-1)^{i+n} \delta_i$ est aussi le cofacteur $C_{i,n}(x_1, x_2, \dots, x_{n-1})$ d'indice (i, n) de la matrice $(X_1, X_2, \dots, X_{n-1}, 0)$ (i. e. celui en ligne i et colonne n)

Par exemple dans l'espace euclidien $E = \mathbb{R}^3$ muni de sa base canonique, le produit vectoriel de $x = (x_1, x_2, x_3)$ et $y = (y_1, y_2, y_3)$ est le vecteur $z = (z_1, z_2, z_3)$ défini par :

$$\begin{aligned} z_1 &= \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} = x_2 y_3 - x_3 y_2 \\ z_2 &= - \begin{vmatrix} x_1 & y_1 \\ x_3 & y_3 \end{vmatrix} = x_3 y_1 - x_1 y_3 \\ z_3 &= \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1 y_2 - x_2 y_1 \end{aligned}$$

Exercice 13.9 *On suppose que E est de dimension 3. Montrer que si (f_1, f_2, f_3) est une base orthonormée directe, on a alors :*

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

Solution 13.9 *Le vecteur $f_1 \wedge f_2$ est orthogonal au plan engendré par f_1, f_2 , donc colinéaire à f_3 et il existe un réel λ tel que $f_1 \wedge f_2 = \lambda f_3$. Ce réel λ est déterminé par :*

$$\lambda = \langle f_1 \wedge f_2 \mid f_3 \rangle = \det(f_1, f_2, f_3) = 1$$

De même $f_2 \wedge f_3 = \lambda f_1$ avec :

$$\begin{aligned} \lambda &= \langle f_2 \wedge f_3 \mid f_1 \rangle = \det(f_2, f_3, f_1) \\ &= -\det(f_2, f_1, f_3) = \det(f_1, f_2, f_3) = 1 \end{aligned}$$

et $f_3 \wedge f_1 = f_2$ se montre de manière analogue

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

Théorème 13.21

- *Le produit vectoriel est une application $(n-1)$ -linéaire alternée de E^{n-1} dans E ;*
- *le vecteur $x_1 \wedge x_2 \wedge \dots \wedge x_{n-1}$ est orthogonal à tous les vecteurs x_i ($1 \leq i \leq n-1$) ;*

- $x_1 \wedge x_2 \wedge \dots \wedge x_{n-1} = 0$ si et seulement si la famille $(x_1, x_2, \dots, x_{n-1})$ est liée ;
- si la famille $(x_1, x_2, \dots, x_{n-1})$ est libre, alors la famille $(x_1, \dots, x_{n-1}, x_1 \wedge x_2 \wedge \dots \wedge x_{n-1})$ est une base de E .

Démonstration.

- Chacune des applications :

$$(x_1, \dots, x_{n-1}) \mapsto (-1)^{i+n} \delta_i = C_{i,n}(x_1, x_2, \dots, x_{n-1})$$

étant $(n-1)$ -linéaire alternée, il en est de même de l'application $(x_1, \dots, x_{n-1}) \mapsto x_1 \wedge \dots \wedge x_{n-1}$.

- Avec :

$$\langle x_1 \wedge \dots \wedge x_{n-1} \mid x_i \rangle = \det(x_1, \dots, x_{n-1}, x_i) = 0$$

on déduit que $x_1 \wedge \dots \wedge x_{n-1}$ est orthogonal à x_i .

- Si la famille (x_1, \dots, x_{n-1}) est liée, il en est de même de la famille (x_1, \dots, x_{n-1}, x) pour tout $x \in E$ et :

$$\langle x_1 \wedge \dots \wedge x_{n-1} \mid x \rangle = \det(x_1, \dots, x_{n-1}, x) = 0$$

et donc $x_1 \wedge \dots \wedge x_{n-1} \in E^\perp = \{0\}$.

Si la famille (x_1, \dots, x_{n-1}) est libre, elle se prolonge en une base (x_1, \dots, x_{n-1}, x) et :

$$\langle x_1 \wedge \dots \wedge x_{n-1} \mid x \rangle = \det(x_1, \dots, x_{n-1}, x) \neq 0$$

ce qui entraîne $x_1 \wedge \dots \wedge x_{n-1} \neq 0$.

- Si (x_1, \dots, x_{n-1}) est libre, on a $x_1 \wedge \dots \wedge x_{n-1} \neq 0$ et :

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

ce qui revient à dire que $(x_1, \dots, x_{n-1}, x_1 \wedge \dots \wedge x_{n-1})$ est une base de E . ■

Remarque 13.9 Avec $\det(x_1, \dots, x_{n-1}, x_1 \wedge \dots \wedge x_{n-1}) = \|x_1 \wedge \dots \wedge x_{n-1}\|^2 > 0$ dans le cas où (x_1, \dots, x_{n-1}) est libre, on déduit que la base $(x_1, \dots, x_{n-1}, x_1 \wedge \dots \wedge x_{n-1})$ est directe.

Remarque 13.10 Pour $n = 3$, le caractère 2-linéaire alterné du produit vectoriel se traduit par :

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

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

Exercice 13.10 Montrer que si (x_1, \dots, x_{n-1}) est une famille orthonormée dans E , alors $(x_1, \dots, x_{n-1}, x_1 \wedge \dots \wedge x_{n-1})$ est une base orthonormée directe de E .

Solution 13.10 On sait déjà que $(x_1, \dots, x_{n-1}, x_1 \wedge \dots \wedge x_{n-1})$ est une base directe de E . En prolongeant (x_1, \dots, x_{n-1}) en une base orthonormée directe de E , $(x_1, \dots, x_{n-1}, x_n)$, on a $x_1 \wedge \dots \wedge x_{n-1} = \lambda x_n$ avec :

$$\lambda = \langle x_1 \wedge \dots \wedge x_{n-1} \mid x_n \rangle = \det(x_1, \dots, x_{n-1}, x_n) = 1$$

et $x_1 \wedge \dots \wedge x_{n-1} = x_n$ est de norme 1.

Théorème 13.22 Si H est un hyperplan de E et (x_1, \dots, x_{n-1}) une base de H , alors la droite $D = H^\perp$ est dirigée par le vecteur $x_1 \wedge \dots \wedge x_{n-1}$ et pour tout vecteur x de E , la projection orthogonale de x sur H est :

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

et la distance de x à H est donnée par :

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

Démonstration. Le vecteur $x_1 \wedge \dots \wedge x_{n-1}$ étant orthogonal à tous les x_i qui engendrent H , est nécessairement dans H^\perp . Comme H^\perp est une droite et $x_1 \wedge \dots \wedge x_{n-1}$ non nul, la droite $D = H^\perp$ est dirigée par $x_1 \wedge \dots \wedge x_{n-1}$.

On a $d(x, H) = \|x - y\|$ où $y = p_H(x)$ est la projection orthogonale de x sur H . Comme $x - y \in H^\perp$, il existe un réel λ tel que $x - y = \lambda(x_1 \wedge \dots \wedge x_{n-1})$ et avec :

$$\lambda \|x_1 \wedge \dots \wedge x_{n-1}\|^2 = \langle x - y \mid x_1 \wedge \dots \wedge x_{n-1} \rangle = \langle x \mid x_1 \wedge \dots \wedge x_{n-1} \rangle$$

(puisque $y \in H$ et $x_1 \wedge \dots \wedge x_{n-1} \in H^\perp$), on déduit que :

$$\lambda = \frac{\langle x_1 \wedge \dots \wedge x_{n-1} \mid x \rangle}{\|x_1 \wedge \dots \wedge x_{n-1}\|^2}$$

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

et :

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

■

Remarque 13.11 Le théorème précédent nous dit aussi qu'une équation de l'hyperplan H de base (x_1, \dots, x_{n-1}) est donnée par :

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

Remarque 13.12 En prenant pour (x_1, \dots, x_{n-1}) une base orthonormée de H (c'est toujours possible avec le procédé d'orthogonalisation de Gram-Schmidt), on a :

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

et :

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

Exercice 13.11 Donner une équation du plan vectoriel P de \mathbb{R}^3 engendré par les vecteurs $u = (1, 1, 1)$ et $v = (1, 2, 3)$. Calculer la distance de $x = (1, -1, 1)$ à P .

Solution 13.11 Ce plan est orthogonal au vecteur :

$$u \wedge v = (1, -2, 1)$$

et une équation est donc $x_1 - 2x_2 + x_3 = 0$.

La distance de $x = (1, -1, 1)$ à P est donnée par :

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

Exercice 13.12 Montrer que si u et v sont deux applications dérivables d'un intervalle réel I dans \mathbb{R}^n , alors l'application $u \wedge v$ est dérivable avec :

$$\forall t \in I, (u \wedge v)'(t) = u'(t) \wedge v(t) + u(t) \wedge v'(t)$$

Solution 13.12 *Laissée au lecteur.*

13.13 Isométries en dimension 2

Pour ce paragraphe, E est un espace euclidien de dimension 2 et il est orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_1, e_2)$.

13.13.1 Isométries directes ou rotations. Angles orientés de vecteurs

Théorème 13.23 *Un endomorphisme u de E est une isométrie positive [resp. négative] si, et seulement si, il existe un réel θ tel que la matrice de u dans la base orthonormée \mathcal{B}_0 soit de la forme :*

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

$$\text{resp. } S_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

Démonstration. Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}_2(\mathbb{R})$ la matrice de u dans \mathcal{B}_0 et $C = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ sa comatrice.

Si $u \in \mathcal{O}^+(E)$, on a alors $A = C$, soit $a = d$ et $b = -c$, de sorte que $A = \begin{pmatrix} a & -c \\ c & a \end{pmatrix}$ avec $\det(A) = a^2 + c^2 = 1$ et il existe un réel θ tel que $a = \cos(\theta)$ et $c = \sin(\theta)$ (on peut le voir simplement en écrivant que, dans \mathbb{C} on a, $|a + ic| = \sqrt{a^2 + c^2} = 1$, ce qui entraîne $a + ic = e^{i\theta}$).

Si $u \in \mathcal{O}^-(E)$, on a alors $A = -C$, soit $d = -a$ et $b = c$, de sorte que $A = \begin{pmatrix} a & c \\ c & -a \end{pmatrix}$ avec $\det(A) = a^2 + c^2 = 1$ et il existe un réel θ tel que $a = \cos(\theta)$ et $c = \sin(\theta)$. ■

Remarque 13.13 *Le réel θ qui intervient dans le théorème précédent est unique si on le prend dans $[-\pi, \pi[$, c'est la détermination principale de l'argument de $a + ic$.*

Corollaire 13.3 *Les groupes $\mathcal{O}^+(E)$ et $\mathcal{O}_2^+(\mathbb{R})$ sont commutatifs.*

Démonstration. Pour θ, θ' dans \mathbb{R} , on vérifie facilement que $R_\theta R_{\theta'} = R_{\theta+\theta'} = R_{\theta'} R_\theta$. ■

Corollaire 13.4 *Si \mathcal{B}_0 et \mathcal{B} sont deux bases orthonormées de E définissant la même orientation et si $u \in \mathcal{O}^+(E)$, alors les matrices de u dans \mathcal{B}_0 et \mathcal{B} sont égales.*

Démonstration. La matrice de passage P de \mathcal{B}_0 à \mathcal{B} est dans $\mathcal{O}_2^+(\mathbb{R})$ puisque les bases \mathcal{B}_0 et \mathcal{B} sont orthonormées et définissent la même orientation. Comme le groupe $\mathcal{O}_2^+(\mathbb{R})$ est commutatif, en désignant respectivement par A et A' les matrices de u dans \mathcal{B}_0 et \mathcal{B} , on a $A' = P^{-1}AP = P^{-1}PA = A$. ■

Théorème 13.24 *Soit $u \in \mathcal{O}^+(E)$ de matrice $R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ dans \mathcal{B}_0 .*

Si \mathcal{B} est une base orthonormée directe [resp. indirecte], alors la matrice de u dans \mathcal{B} est R_θ [resp. ${}^t R_\theta = R_\theta^{-1} = R_{-\theta}$].

Démonstration. Soit R la matrice de u dans \mathcal{B} .

Si la base \mathcal{B} est directe, on a alors $R = R_\theta$.

Si la base \mathcal{B} est indirecte, elle définit alors la même orientation que $\mathcal{B}_0^- = (e_1, -e_2)$, la matrice de passage de \mathcal{B}_0 à \mathcal{B}_0^- est $Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la matrice de u dans \mathcal{B}_0^- est :

$$\begin{aligned} R &= Q^{-1} R_\theta Q = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = R_{-\theta} \end{aligned}$$

cette matrice étant aussi celle de u dans \mathcal{B} . ■

En résumé, une isométrie $u \in \mathcal{O}^+(E)$ de matrice R_θ dans une base orthonormée directe \mathcal{B} , est une rotation et θ est une mesure de l'angle de cette rotation. Si $\theta \in]-\pi, \pi[$, on dit que c'est la mesure principale de la rotation. Dans une base indirecte, cette mesure principale est $-\theta$.

On dit aussi, de manière plus précise, que $\bar{\theta} = \{\theta + 2k\pi \mid k \in \mathbb{Z}\} \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$ (groupe quotient) est l'angle de la rotation dans l'espace orienté E .

Par abus de langage, on dit parfois que θ est l'angle de la rotation, étant entendu que le réel θ est définie modulo 2π .

Exemple 13.5 *L'identité est la rotation d'angle $\bar{0}$, $-Id$ est la rotation d'angle $\bar{\pi}$.*

Exemple 13.6 *Si ρ est la rotation d'angle $\frac{\pi}{2}$ et (f_1, f_2) une base orthonormée directe, on a alors $\rho(f_1) = f_2$ et $\rho(f_2) = -f_1$.*

De l'étude du groupe commutatif $\mathcal{O}_2^+(\mathbb{R})$, on déduit que l'inverse de la rotation d'angle $\bar{\theta}$ est la rotation d'angle $-\bar{\theta}$ et la composée des rotations ρ d'angle $\bar{\theta}$ et ρ' d'angle $\bar{\theta}'$ est la rotation $\rho \circ \rho' = \rho' \circ \rho$ d'angle $\bar{\theta} + \bar{\theta}'$.

Remarque 13.14 *Les seules rotations involutives sont Id et $-Id$.*

Cette notion d'angle de rotation permet de définir la notion d'angle orienté de deux vecteurs non nuls dans l'espace orienté E .

Théorème 13.25 *Si x, y sont deux vecteurs non nuls dans E , il existe alors une unique rotation $\rho \in \mathcal{O}^+(E)$ telle que $\frac{1}{\|y\|}y = \rho\left(\frac{1}{\|x\|}x\right)$.*

Démonstration. Il suffit de montrer le résultat pour des vecteurs x, y unitaires (i. e. de norme égale à 1).

En choisissant une base orthonormée directe (f_1, f_2) où $f_1 = x$, il existe deux réels a, b tels que $y = af_1 + bf_2$ et avec $\|y\|^2 = a^2 + b^2 = 1$, on déduit qu'il existe un réel θ tel que $a = \cos(\theta)$ et $b = \sin(\theta)$. On a alors, en désignant par ρ la rotation d'angle $\bar{\theta} \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$:

$$\rho(x) = \rho(f_1) = \cos(\theta)f_1 + \sin(\theta)f_2 = y$$

Si ρ' est une autre rotation d'angle $\bar{\theta}' \in \frac{\mathbb{R}}{2\pi\mathbb{Z}}$ telle que $\rho'(x) = y$, on a alors $\rho(f_1) = \rho'(f_1)$, soit :

$$\cos(\theta)f_1 + \sin(\theta)f_2 = \cos(\theta')f_1 + \sin(\theta')f_2$$

donc $\cos(\theta) = \cos(\theta')$ et $\sin(\theta) = \sin(\theta')$, ce qui équivaut à $\overline{\theta'} = \overline{\theta}$ et entraîne $\rho' = \rho$. ■

Si, avec les notations du théorème qui précède, ρ est la rotation d'angle $\overline{\theta}$, on dit alors que $\overline{\theta}$ est l'angle orienté des vecteurs x et y et on note $\widehat{(x, y)} = \overline{\theta}$. Un réel θ dans la classe d'équivalence $\overline{\theta}$ est une mesure de l'angle orienté $\widehat{(x, y)}$, le représentant $\theta \in [-\pi, \pi[$ est la mesure principale de $\widehat{(x, y)}$.

Exercice 13.13 *Quels sont les points fixes d'une rotation du plan.*

Solution 13.13 *Tout revient à déterminer le noyau de $\rho - Id$.*

Si $\rho = Id$ (rotation d'angle 0), alors tous les points de E sont fixes. Sinon, 0 est l'unique point fixe puisque dans une base orthonormée de E la matrice de $\rho - Id$ est :

$$R_\theta - I_2 = \begin{pmatrix} \cos(\theta) - 1 & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) - 1 \end{pmatrix}$$

et :

$$\begin{aligned} \det(\rho - Id) &= (\cos(\theta) - 1)^2 + \sin^2(\theta) \\ &= 2(1 - \cos(\theta)) \neq 0 \end{aligned}$$

pour $\theta \notin 2\pi\mathbb{Z}$, ce qui signifie que $\rho - Id$ est injective et $\ker(\rho - Id) = \{0\}$.

Exercice 13.14 *On se place dans un plan euclidien E et on se donne deux droites distinctes D et D' dans E .*

1. *Déterminer toutes les rotations ρ telles que $\rho(D) = D$.*
2. *Montrer qu'il existe une rotation ρ telle que $\rho(D) = D'$ et $\rho(D') = D$ si, et seulement si, les droites D et D' sont orthogonales. Préciser alors le nombre de ces rotations.*

Solution 13.14

1. *On a déjà $\rho = Id$ qui laisse D stable. Si $\rho \neq Id$ est une rotation qui laisse stable D , pour tout vecteur directeur unitaire f_1 de D , on a alors $\rho(f_1) = -f_1$ et $\rho = -Id$ (il y a une unique rotation qui transforme un vecteur unitaire en un autre).*
2. *Soit f_1 un vecteur unitaire qui dirige la droite D . Si $D' = \rho(D)$, le vecteur unitaire $\rho(f_1)$ dirige D' et si $\rho(D') = D$, on a alors $\rho^2(f_1) = \pm f_1$. Comme $D \neq D'$, les vecteurs f_1 et $\rho(f_1)$ sont linéairement indépendants et la matrice de ρ dans la base $(f_1, \rho(f_1))$ est $D = \begin{pmatrix} 0 & \pm 1 \\ 1 & 0 \end{pmatrix}$ et comme $\det(D) = 1$, on a nécessairement $\rho^2(f_1) = -f_1$ et :*

$$\langle f_1 | \rho(f_1) \rangle = -\langle \rho^2(f_1) | \rho(f_1) \rangle = -\langle \rho(f_1) | f_1 \rangle$$

entraîne $\langle f_1 | \rho(f_1) \rangle = 0$, ce qui signifie que les droites D et D' sont orthogonales.

Réciproquement, si les droites D et D' sont orthogonales, alors les rotations d'angle $\frac{\pi}{2}$ et $-\frac{\pi}{2}$ transforment D en D' et ce sont les seules.

13.13.2 Isométries indirectes ou réflexions

On sait déjà que les réflexions du plan euclidien (i. e. les symétries orthogonales par rapport à une droite) sont des isométries indirectes (théorème 13.10).

Nous allons vérifier que ce sont les seules.

Si s_D est une réflexion par rapport à la droite D , on a alors $s_D(x) = x$ pour tout $x \in D$ et $s_D(x) = -x$ pour tout $x \in D^\perp$. En désignant par f_1 un vecteur non nul de D et f_2 un vecteur non nul de D^\perp , la famille (f_1, f_2) est une base orthogonale de s_D et la matrice de s_D dans cette base est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. De plus la droite D est l'ensemble des points fixes de s_D , soit $D = \ker(s_D - Id)$.

Si σ est une isométrie indirecte, on a vu que sa matrice dans la base \mathcal{B}_0 est de la forme :

$$S_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

où θ est un réel uniquement déterminé modulo 2π .

L'ensemble des points fixes de σ est formé des vecteurs $x = x_1 e_1 + x_2 e_2$ tels que $\sigma(x) = x$, ce qui revient à dire que les réels x_1, x_2 sont solutions du système linéaire :

$$\begin{cases} (\cos(\theta) - 1)x_1 + \sin(\theta)x_2 = 0 \\ \sin(\theta)x_1 - (\cos(\theta) + 1)x_2 = 0 \end{cases}$$

ce qui s'écrit aussi :

$$\begin{cases} \sin\left(\frac{\theta}{2}\right) \left(-\sin\left(\frac{\theta}{2}\right)x_1 + \cos\left(\frac{\theta}{2}\right)x_2\right) = 0 \\ \cos\left(\frac{\theta}{2}\right) \left(-\sin\left(\frac{\theta}{2}\right)x_1 - \cos\left(\frac{\theta}{2}\right)x_2\right) = 0 \end{cases}$$

et est équivalent à :

$$-\sin\left(\frac{\theta}{2}\right)x_1 + \cos\left(\frac{\theta}{2}\right)x_2 = 0 \quad (13.7)$$

puisque $\left(\cos\left(\frac{\theta}{2}\right), \sin\left(\frac{\theta}{2}\right)\right) \neq (0, 0)$.

L'ensemble des points fixes de σ est donc la droite D d'équation (13.7). Cette droite est dirigée par le vecteur unitaire $f_1 = \cos\left(\frac{\theta}{2}\right)e_1 + \sin\left(\frac{\theta}{2}\right)e_2$, la droite D^\perp est dirigée par le vecteur unitaire $f_2 = -\sin\left(\frac{\theta}{2}\right)e_1 + \cos\left(\frac{\theta}{2}\right)e_2$ et on a $u(f_1) = f_1$, $u(f_2) = \lambda f_2$ puisque D^\perp est aussi stable par u (théorème 13.13). La matrice de u dans la base (f_1, f_2) est donc $A = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ et avec $\det(u) = -1$, on déduit que $\lambda = -1$, ce qui signifie que u est la réflexion par rapport à D .

On peut remarquer que la droite D est la droite d'angle polaire $\frac{\theta}{2}$ et que pour $\theta \notin \pi\mathbb{Z}$, c'est la droite d'équation $x_2 = \tan\left(\frac{\theta}{2}\right)x_1$.

On a donc montré le résultat suivant.

Théorème 13.26 *Les isométries indirectes d'un plan euclidien sont les réflexions.*

Exercice 13.15 *On se place dans un plan euclidien E .*

1. Soient ρ une rotation et σ, σ' deux réflexions. Préciser la nature géométrique de $\rho \circ \sigma'$, $\sigma' \circ \rho$, $\sigma \circ \sigma'$ et $\sigma' \circ \sigma$, en précisant les caractéristiques de ces applications.

2. Montrer que pour toute rotation ρ et toute réflexion σ , on a $\sigma \circ \rho \circ \sigma = \rho^{-1}$.

Solution 13.15

1. Toutes ces applications sont des isométries et avec $\det(\rho \circ \sigma') = \det(\sigma' \circ \rho) = -1$, $\det(\sigma \circ \sigma') = \det(\sigma' \circ \sigma) = 1$, on déduit que la composée d'une rotation et d'une réflexion est une réflexion et que la composée de deux réflexions est une rotation. En désignant respectivement par R_θ , S_θ et $S_{\theta'}$ les matrices de ρ , σ et σ' dans une base orthonormée directe \mathcal{B}_0 , on vérifie par un calcul direct que :

$$R_\theta S_{\theta'} = S_{\theta+\theta'}, S_{\theta'} R_\theta = S_{\theta-\theta'}, S_\theta S_{\theta'} = R_{\theta-\theta'}, S_{\theta'} S_\theta = R_{\theta'+\theta} = (R_{\theta-\theta'})^{-1}$$

ce qui signifie que :

- $\rho \circ \sigma'$ est la réflexion par rapport à la droite d'angle polaire $\frac{\theta + \theta'}{2}$;
 - $\sigma' \circ \rho$ est la réflexion par rapport à la droite d'angle polaire $\frac{\theta - \theta'}{2}$;
 - $\sigma \circ \sigma'$ est la rotation d'angle $\theta - \theta'$ (modulo 2π) ;
 - $\sigma' \circ \sigma$ est la rotation inverse d'angle $\theta - \theta'$, ce qui est normal puisque $(\sigma \circ \sigma')^{-1} = (\sigma')^{-1} \circ \sigma^{-1} = \sigma' \circ \sigma$ (une réflexion est involutive).
2. On peut utiliser les expressions matricielles des rotations et réflexions dans une base orthonormée \mathcal{B}_0 et vérifier par un calcul direct que pour tous réels θ et θ' , on a :

$$S_{\theta'} R_\theta S_{\theta'} = S_{\theta-\theta'} S_{\theta'} = R_{-\theta}$$

On peut aussi dire que $\rho \circ \sigma$ qui est une réflexion est involutive, donc $\rho \circ \sigma = (\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$ et composant à gauche par σ , on obtient $\sigma \circ \rho \circ \sigma = \rho^{-1}$.

13.14 Isométries en dimension 3

Pour ce paragraphe, E est un espace euclidien de dimension 3 et il est orienté par le choix d'une base orthonormée $\mathcal{B}_0 = (e_1, e_2, e_3)$.

Nous aurons besoin du résultat suivant sur les isométries de l'espace euclidien E .

Théorème 13.27 Pour toute isométrie $u \in \mathcal{O}(E)$, le polynôme P_u défini par :

$$P_u(\lambda) = \det(u - \lambda Id)$$

a au moins une racine réelle et cette racine est dans $\{-1, 1\}$. Il existe donc un vecteur non nul x tel que $u(x) = \pm x$.

Démonstration. En développant le déterminant, on voit que :

$$P_u(\lambda) = -\lambda^3 + \text{Tr}(u)\lambda^2 + \alpha_2\lambda + \det(u)$$

où $\text{Tr}(u)$ est la trace de u et α_2 un réel. Ce polynôme est donc de degré 3 à coefficients réels et le théorème des valeurs intermédiaires nous dit qu'il a au moins une racine réelle (de manière plus générale, un polynôme réel de degré impair a au moins une racine réelle).

Dire que $\lambda \in \mathbb{R}$ est racine de P_u équivaut à dire que $u - \lambda Id$ est non injective, ce qui revient à dire que $\ker(u - \lambda Id) \neq \{0\}$ et il existe un vecteur non nul x tel que $u(x) = \lambda x$. Puis comme u est une isométrie, on a $\|u(x)\| = \|x\|$ et nécessairement $|\lambda| = 1$, ce qui signifie que ± 1 . ■

Remarque 13.15 Nous verrons plus loin que ce polynôme P_u est appelé le polynôme caractéristique de u et ses racines sont les valeurs propres de u .

Exemple 13.7 Pour $u = Id$, on a $P_u(\lambda) = (1 - \lambda)^3$ et $\lambda = 1$ est l'unique valeur propre.

Exemple 13.8 Pour $u = -Id$, on a $P_u(\lambda) = -(1 + \lambda)^3$ et $\lambda = -1$ est l'unique valeur propre.

Exemple 13.9 Si u est une réflexion, alors sa matrice dans une base convenablement choisie est :

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

donc $P_u(\lambda) = -(1 - \lambda)^2(1 + \lambda)$ et les valeurs propres de u sont -1 et 1 .

Exemple 13.10 Si u est un retournement, alors sa matrice dans une base convenablement choisie est :

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

donc $P_u(\lambda) = (1 - \lambda)(1 + \lambda)^2$ et les valeurs propres de u sont -1 et 1 .

13.14.1 Isométries directes

Théorème 13.28 Soit $u \in \mathcal{O}^+(E) \setminus \{Id\}$.

L'ensemble des points fixes de u est une droite D .

Si (f_1, f_2) est une base orthonormée du plan D^\perp , alors $(f_1, f_2, f_1 \wedge f_2)$ est une base orthonormée directe de E et la matrice de u dans cette base est :

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Démonstration. Soit $D = \ker(u - Id)$ l'ensemble des points fixes de u .

Si D est de dimension 3, il est égal à E et $u = Id$, ce qui n'est pas le cas.

Si D est de dimension 2, alors D^\perp est de dimension 1 et stable par u , donc en désignant par (g_1, g_2) une base orthonormée de D , g_3 un vecteur unitaire de D^\perp , on a $u(g_3) = \pm g_3$ et la matrice de u dans la base (g_1, g_2, g_3) est :

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$$

avec $\det(A) = 1$, ce qui impose $u(g_3) = g_3$ et $u = Id$, ce qui n'est pas le cas.

Si D est réduit à $\{0\}$, il n'existe pas de vecteur non nul tel que $u(x) = x$ et le théorème 13.27 nous dit qu'il existe alors un vecteur non nul x tel que $u(x) = -x$. Ce vecteur dirige une droite Δ qui est stable par u et le plan Δ^\perp est également stable par u . La restriction v de u au plan Δ^\perp est aussi une isométrie et en désignant par g_1 un vecteur unitaire directeur de Δ , (g_2, g_3) une base orthonormée de Δ^\perp , la matrice de u dans la base (g_1, g_2, g_3) est :

$$A = \begin{pmatrix} -1 & 0 \\ 0 & B \end{pmatrix}$$

où B est la matrice de v dans (g_2, g_3) . On a donc

$$1 = \det(u) = \det(A) = -\det(B) = -\det(v)$$

donc $\det(v) = -1$ et v est une réflexion. Mais alors v a des points fixes non nuls et ces points fixes sont des points fixes de u , ce qui contredit $F = \{0\}$.

On a donc en définitive $\dim(D) = 1$, c'est-à-dire que D est une droite.

La restriction de u au plan stable D^\perp est une isométrie qui ne peut être une réflexion (sinon elle a des points fixes non nuls et l'ensemble des points fixes de u est de dimension 2), c'est donc une rotation.

Si (f_1, f_2) est une base orthonormée du plan D^\perp , on oriente le plan D^\perp avec le choix de cette base et il existe un réel θ tel que la matrice dans (f_1, f_2) de la restriction de u à D^\perp est $R'_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. Le vecteur $f_3 = f_1 \wedge f_2$ est unitaire, orthogonal au plan engendré par (f_1, f_2) donc dans D , la famille $(f_1, f_2, f_1 \wedge f_2)$ est une base orthonormée directe de E (exercice 13.10) et la matrice de u dans cette base est :

$$R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

■

Avec les notations du théorème, on dit que u est la rotation d'axe D orienté par $f_1 \wedge f_2$ et d'angle θ (défini modulo 2π).

Si $A \in \mathcal{O}_3^+(\mathbb{R}) \setminus \{I_3\}$ est la matrice de $u \in \mathcal{O}^+(E) \setminus \{Id\}$ dans la base orthonormée \mathcal{B}_0 , alors l'axe de la rotation u est obtenu en déterminant le noyau de $u - Id$, ce qui revient à résoudre un système linéaire $(A - I_3)X = 0$, où la matrice $A - I_3$ est de rang 2.

Pour ce qui est de la mesure principale $\theta \in [-\pi, \pi[\setminus \{0\}$ de l'angle de cette rotation, avec :

$$\text{Tr}(u) = \text{Tr}(A) = \text{Tr}(R_\theta) = 2 \cos(\theta) + 1$$

on en déduit la valeur de $\cos(\theta)$ et celle de θ au signe près.

Si $\text{Tr}(u) = -1$, on a alors $\cos(\theta) = -1$, donc $\sin(\theta) = 0$ et $\theta = -\pi$.

Dans le cas où $\theta \in]-\pi, \pi[\setminus \{0\}$, on peut déterminer le signe de $\sin(\theta)$, et donc de θ , comme suit.

Avec $u(f_1) = \cos(\theta)f_1 + \sin(\theta)f_2$, on déduit que $\sin(\theta) = \langle u(f_1) | f_2 \rangle$. De plus, en notant $f_3 = f_1 \wedge f_2$, on a $f_3 \wedge f_1 = f_2$ (exercice 13.9) et :

$$\begin{aligned} \sin(\theta) &= \langle u(f_1) | f_2 \rangle = \langle u(f_1) | f_3 \wedge f_1 \rangle = \det(f_3, f_1, u(f_1)) \\ &= \det(f_1, u(f_1), f_3) \end{aligned}$$

ce qui permet de déterminer $\sin(\theta)$ et θ .

En fait, comme seul le signe de θ nous importe, on choisit un vecteur non nul x dans D^\perp , on pose $f_1 = \frac{1}{\|x\|}x$, on complète ce vecteur en une base orthonormée (f_1, f_2, f_3) de E et $\sin(\theta) = \frac{\det(x, u(x), f_3)}{\|x\|^2}$ est du signe de $\det(x, u(x), f_3)$, ce qui permet de déterminer θ .

Exercice 13.16 On se place dans l'espace $E = \mathbb{R}^3$ muni de sa structure euclidienne canonique. On désigne par u l'endomorphisme de E de matrice :

$$A = \frac{1}{3} \begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$$

dans la base canonique \mathcal{B}_0 .

1. Montrer que u est une rotation.
2. Donner un vecteur unitaire e_3 appartenant à l'axe de cette rotation.
3. Déterminer la mesure principale $\theta \in [-\pi, \pi[$ de l'angle de cette rotation.

Solution 13.16

1. Avec $A \neq I_3$, $A^t A = I_3$ et $\det(A) = 1$, on déduit que u est une rotation d'angle non nul (modulo 2π).
2. L'axe de cette rotation est obtenu en résolvant le système linéaire $(A - I_3)X = 0$, soit :

$$\begin{cases} -2x + y + z = 0 \\ x - 2y + z = 0 \\ x + y - 2z = 0 \end{cases}$$

ce qui donne $x = y = z$ et l'axe D de u est la droite dirigée par $e_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

3. Avec $\text{Tr}(u) = -1 = 2 \cos(\theta) + 1$, on déduit que $\cos(\theta) = -1$ et $\theta = -\pi$.

Exercice 13.17 On se place dans l'espace $E = \mathbb{R}^3$ muni de sa structure euclidienne canonique, on se donne des réels a, b, c et on désigne par u l'endomorphisme de E de matrice :

$$A = \begin{pmatrix} a^2 & ab - c & ac + b \\ ab + c & b^2 & bc - a \\ ac - b & bc + a & c^2 \end{pmatrix}$$

dans la base canonique \mathcal{B}_0 .

1. Déterminer les réels a, b, c tels que u soit une isométrie.
2. Préciser, dans le cas où u est une isométrie, sa nature géométrique.

Solution 13.17

1. On a :

$$A^t A = (a^2 + b^2 + c^2 - 1) \begin{pmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix} + (a^2 + b^2 + c^2) I_3$$

et l'égalité $A^t A = I_3$ est réalisée si, et seulement si, $a^2 + b^2 + c^2 = 1$.

2. On a :

$$\begin{aligned} \det(A) &= a^4 + b^4 + c^4 + 2a^2b^2 + 2a^2c^2 + 2b^2c^2 \\ &= (a^2 + b^2 + c^2)^2 = 1 \end{aligned}$$

si u est une isométrie. Donc $u \in \mathcal{O}_3^+(\mathbb{R}) \setminus \{I_3\}$ et c'est une rotation d'angle $\theta \in [-\pi, \pi[$ tel que $2 \cos(\theta) + 1 = \text{Tr}(A) = 1$, ce qui donne $\theta = \pm \frac{\pi}{2}$.

L'axe D de cette rotation est obtenu en résolvant le système linéaire $(A - I_3)X = 0$, soit :

$$\begin{cases} (a^2 - 1)x + (ab - c)y + (ac + b)z = 0 & (1) \\ (ab + c)x + (b^2 - 1)y + (bc - a)z = 0 & (2) \\ (ac - b)x + (bc + a)y + (c^2 - 1)z = 0 & (3) \end{cases}$$

En effectuant les opérations $(1) + c \cdot (2) - b \cdot (3)$, $-c \cdot (1) + (2) + a \cdot (3)$ et $b \cdot (1) - a \cdot (2) + (3)$, on obtient :

$$\begin{cases} -cy + bz = 0 \\ cx - az = 0 \\ -bx + ay = 0 \end{cases}$$

Comme $(a, b, c) \neq 0$, l'un de ces coefficients est non nul. En supposant $a \neq 0$, on obtient $z = \frac{c}{a}x$ et $y = \frac{b}{a}x$ et l'axe D de u est la droite dirigée par $f_3 = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ (les deux autres possibilités donnent le même résultat).

En désignant par x un vecteur non nul dans D^\perp , par exemple $x = \begin{pmatrix} -b \\ a \\ 0 \end{pmatrix}$ si $a \neq 0$, $\sin(\theta)$ est du signe de :

$$\det(x, u(x), f_3) = \begin{vmatrix} -b & -ac & a \\ a & -bc & b \\ 0 & 1 - c^2 & c \end{vmatrix} = a^2 + b^2 > 0$$

et en conséquence $\theta = \frac{\pi}{2}$. On dit que u est un quart de tour.

Exercice 13.18 Soient D la droite de \mathbb{R}^3 dirigée par $e = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$ et ρ la rotation d'axe

D et d'angle de mesure $\frac{2\pi}{3}$, le plan P^\perp étant orienté par le choix de e . Donner la matrice de ρ dans la base canonique de \mathbb{R}^3 .

Solution 13.18 Pour $x \in \mathbb{R}^3$, en désignant par y le projeté orthogonal de x sur D^\perp , on a $x = y + \langle x | e \rangle e$ et $\rho(x) = \rho(y) + \langle x | e \rangle e$. Pour $y \in D^\perp$, on a :

$$\rho(y) = \cos\left(\frac{2\pi}{3}\right)y + \sin\left(\frac{2\pi}{3}\right)y \wedge e = -\frac{1}{2}y + \frac{\sqrt{3}}{2}y \wedge e$$

donc :

$$\begin{aligned} \rho(x) &= -\frac{1}{2}x + \frac{\sqrt{3}}{2}x \wedge e + \frac{3}{2}\langle x | e \rangle e \\ &= -\frac{1}{2} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \wedge \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} + \frac{1}{2}(x_1 - x_2 + x_3) \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \\ &= -\frac{1}{2} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} x_2 + x_3 \\ x_3 - x_1 \\ -x_1 - x_2 \end{pmatrix} + \frac{1}{2}(x_1 - x_2 + x_3) \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} x_3 \\ -x_1 \\ -x_2 \end{pmatrix} \end{aligned}$$

et :

$$A = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

Espaces préhilbertiens complexes

On désigne par E un espace vectoriel complexe non réduit à $\{0\}$.

14.1 Produits scalaires

Si on définit sur $E = \mathbb{C}^n$ un « produit scalaire » par $\langle x | y \rangle = \sum_{k=1}^n x_k y_k$, pour $y = x$ la quantité $\langle x | x \rangle = \sum_{k=1}^n x_k^2$ n'est pas en général un réel positif et cette condition est essentielle dans le cadre des espaces euclidiens.

Par contre, l'application $(x, y) \mapsto \langle x | y \rangle = \sum_{k=1}^n x_k \overline{y_k}$, où \bar{z} désigne le conjugué d'un nombre complexe z donne bien $\langle x | x \rangle = \sum_{k=1}^n |x_k|^2 \in \mathbb{R}^+$ avec $\langle x | x \rangle = 0$ si, et seulement si, $x = 0$. Mais cette application n'est ni symétrique ($\langle y | x \rangle = \overline{\langle x | y \rangle}$) ni bilinéaire ($\langle x | \lambda y \rangle = \bar{\lambda} \langle x | y \rangle$) ce qui ne sera pas gênant.

Définition 14.1 On appelle *forme anti-linéaire* sur un espace vectoriel complexe E toute application $\ell : E \rightarrow \mathbb{C}$ telle que :

1. $\ell(x + y) = \ell(x) + \ell(y)$ pour tous x, y dans E ;
2. $\ell(\lambda x) = \bar{\lambda} \ell(x)$ pour tout nombre complexe λ et tout vecteur $x \in E$.

Définition 14.2 On appelle *forme hermitienne* sur un espace vectoriel complexe E toute application $\varphi : E \times E \rightarrow \mathbb{C}$ telle que :

1. $\varphi(y, x) = \overline{\varphi(x, y)}$ pour tous x, y dans E (symétrie hermitienne) ;
2. pour tout $y \in E$, l'application $x \mapsto \varphi(x, y)$ est linéaire.

Remarque 14.1 Pour tout $x \in E$, on a $\varphi(x, x) = \overline{\varphi(x, x)}$, ce qui signifie que $\varphi(x, x)$ est réel.

Remarque 14.2 Pour tout $x \in E$, l'application $y \mapsto \varphi(x, y) = \overline{\varphi(y, x)}$ est anti-linéaire.

Remarque 14.3 Une application $\varphi : E \times E \rightarrow \mathbb{C}$ telle que :

1. pour tout $y \in E$, l'application $x \mapsto \varphi(x, y)$ est linéaire ;
 2. pour tout $x \in E$, l'application $y \mapsto \varphi(x, y)$ est anti-linéaire
- est dite *sesquilinéaire*.

Cette notion de forme hermitienne complexe généralise la notion de forme bilinéaire symétrique réelle.

Définition 14.3 On dit qu'une forme hermitienne φ sur E est :

- positive si $\varphi(x, x) \geq 0$ pour tout x dans E ;
- définie si pour x dans E l'égalité $\varphi(x, x) = 0$ équivaut à $x = 0$.

Définition 14.4 On appelle produit scalaire sur E toute forme hermitienne définie positive.

Définition 14.5 Un espace préhilbertien complexe est un espace vectoriel complexe muni d'un produit scalaire.

Dans le cas où E est de dimension finie, on dit que E est un espace hermitien.

On notera, quand il n'y a pas d'ambiguïté :

$$(x, y) \mapsto \langle x | y \rangle$$

un tel produit scalaire et pour $y = x$, on note :

$$\|x\| = \sqrt{\langle x | x \rangle}.$$

Pour $x \in E$ et $\lambda \in \mathbb{C}$, on a :

$$\|\lambda x\|^2 = \langle \lambda x | \lambda x \rangle = \lambda \bar{\lambda} \|x\|^2 = |\lambda|^2 \|x\|^2.$$

Pour x, y dans E , on a :

$$\begin{cases} \|x + y\|^2 = \langle x + y | x + y \rangle = \|x\|^2 + 2\Re(\langle x | y \rangle) + \|y\|^2 \\ \|x - y\|^2 = \langle x - y | x - y \rangle = \|x\|^2 - 2\Re(\langle x | y \rangle) + \|y\|^2 \\ \|x + iy\|^2 = \langle x + iy | x + iy \rangle = \|x\|^2 + 2\Im(\langle x | y \rangle) + \|y\|^2 \\ \|x - iy\|^2 = \langle x - iy | x - iy \rangle = \|x\|^2 - 2\Im(\langle x | y \rangle) + \|y\|^2 \end{cases}$$

Il en résulte que :

$$\begin{cases} \Re(\langle x | y \rangle) = \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2) \\ \Im(\langle x | y \rangle) = \frac{1}{4} (\|x + iy\|^2 - \|x - iy\|^2) \end{cases}$$

et :

$$\langle x | y \rangle = \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2) + \frac{i}{4} (\|x + iy\|^2 - \|x - iy\|^2)$$

Cette identité est l'analogue de l'identité de polarisation pour les produits scalaires réels.

On a aussi l'égalité du parallélogramme :

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

Exemple 14.1 L'espace vectoriel \mathbb{C}^n étant muni de sa base canonique $(e_i)_{1 \leq i \leq n}$, l'application :

$$(x, y) \mapsto \langle x | y \rangle = \sum_{k=1}^n x_k \bar{y}_k$$

définit un produit scalaire sur \mathbb{C}^n . On dit que c'est le produit scalaire euclidien canonique de \mathbb{C}^n .

Exercice 14.1 L'espace vectoriel \mathbb{C}^n est toujours muni de sa base canonique $(e_i)_{1 \leq i \leq n}$. Soit $\omega \in \mathbb{C}^n$. À quelle condition sur ω l'application :

$$\varphi : (x, y) \mapsto \sum_{k=1}^n \omega_k x_k \overline{y_k}$$

définit-elle un produit scalaire sur l'espace vectoriel \mathbb{C}^n ?

Solution 14.1 Pour tout $y \in E$, l'application $x \mapsto \varphi(x, y)$ est linéaire, quel que soit $\omega \in \mathbb{C}^n$. Si φ est un produit scalaire, on a alors $\omega_j = \varphi(e_j, e_j) \in \mathbb{R}^{+,*}$ pour tout j compris entre 1 et n . Réciproquement si tous les ω_j sont réels strictement positifs, on a $\varphi(y, x) = \overline{\varphi(x, y)}$ pour tous x, y dans E , $\varphi(x, x) = \sum_{i=1}^n \omega_i |x_i|^2 \geq 0$ pour tout $x \in \mathbb{C}^n$ et $\varphi(x, x) = 0$ équivaut à $\omega_i |x_i|^2 = 0$ pour tout i , ce qui équivaut à $x_i = 0$ pour tout i , soit à $x = 0$. En conclusion, φ définit un produit scalaire sur \mathbb{C}^n si, et seulement si, tous les ω_i sont strictement positifs.

Exercice 14.2 Donner une condition nécessaire et suffisante sur les nombres complexes a, b, c, d pour que l'application :

$$(x, y) \mapsto \langle x | y \rangle = ax_1 \overline{y_1} + bx_1 \overline{y_2} + cx_2 \overline{y_1} + dx_2 \overline{y_2}$$

définisse un produit scalaire sur $E = \mathbb{C}^2$.

Solution 14.2 Pour tout $y \in E$, l'application $x \mapsto \langle x | y \rangle$ est linéaire. Si c'est un produit scalaire, on a alors $a = \langle e_1 | e_1 \rangle \in \mathbb{R}^{+,*}$, $d = \langle e_2 | e_2 \rangle \in \mathbb{R}^{+,*}$, $b = \langle e_1 | e_2 \rangle = \overline{\langle e_2 | e_1 \rangle} = \overline{c}$ et :

$$\begin{aligned} \langle x | x \rangle &= a|x_1|^2 + bx_1 \overline{x_2} + \overline{b}x_2 \overline{x_1} + d|x_2|^2 \\ &= a \left(|x_1|^2 + 2\Re \left(\frac{b}{a} x_1 \overline{x_2} \right) + \frac{d}{a} |x_2|^2 \right) \\ &= a \left(\left| x_1 + \frac{\overline{b}}{a} x_2 \right|^2 + \frac{ad - |b|^2}{a^2} |x_2|^2 \right) > 0 \end{aligned}$$

pour $x \neq 0$ entraîne $ad - |b|^2 > 0$ (si $ad - |b|^2 \leq 0$ alors $\langle x | x \rangle \leq 0$ pour $x = \left(-\frac{\overline{b}}{a}, 1 \right) \neq 0$).

Réciproquement si ces conditions sont vérifiées, on a un produit scalaire.

Donc $\langle \cdot | \cdot \rangle$ est un produit scalaire si, et seulement si, $b = \overline{c}$, $a > 0$, $d > 0$ et $ad - |b|^2 > 0$.

Exercice 14.3 Soient n un entier naturel non nul, x_0, \dots, x_n des réels deux à deux distincts et $\omega \in \mathbb{R}^{n+1}$. À quelle condition sur ω l'application :

$$\varphi : (P, Q) \mapsto \sum_{i=0}^n \omega_i P(x_i) Q(x_i)$$

définit-elle un produit scalaire sur l'espace vectoriel $\mathbb{R}_n[x]$?

Solution 14.3 L'application φ définit une forme bilinéaire symétrique sur $\mathbb{R}_n[x]$ pour tout $\omega \in \mathbb{R}^n$.

Si φ est un produit scalaire, en désignant par $(L_i)_{0 \leq i \leq n}$ la base de Lagrange de $\mathbb{R}_n[x]$ définie par :

$$L_i(x) = \prod_{\substack{k=0 \\ k \neq i}}^n \frac{x - x_k}{x_i - x_k} \quad (0 \leq i \leq n)$$

(L_i est le polynôme de degré n qui vaut 1 en x_i et 0 en x_k pour $k \neq i$), on a alors $\omega_j = \varphi(L_j, L_j) > 0$ pour tout j compris entre 1 et n .

Réciproquement si tous les ω_j sont strictement positifs, on a $\varphi(P, P) = \sum_{i=1}^n \omega_i P^2(x_i) \geq 0$ pour tout $x \in \mathbb{R}^n$ et $\varphi(P, P) = 0$ équivaut à $\omega_i P^2(x_i) = 0$ pour tout i , ce qui équivaut à $P(x_i) = 0$ pour tout i compris entre 0 et n soit à $P = 0$ (P est un polynôme dans $\mathbb{R}_n[x]$ qui a $n+1$ racines distinctes, c'est donc le polynôme nul).

En conclusion, φ définit un produit scalaire sur $\mathbb{R}_n[x]$ si, et seulement si, tous les ω_i sont strictement positifs.

Exercice 14.4 n étant un entier naturel non nul, on note \mathcal{P}_n l'ensemble des polynômes trigonométriques de degré inférieur ou égal à n , c'est-à-dire l'ensemble des fonctions de \mathbb{R} dans \mathbb{R} la forme :

$$P : x \mapsto P(x) = a_0 + \sum_{k=1}^n (a_k \cos(kx) + b_k \sin(kx)).$$

1. Montrer que \mathcal{P}_n est un espace vectoriel et préciser sa dimension.
2. Montrer que si $P \in \mathcal{P}_n$ s'annule en $2n+1$ points deux à deux distincts dans $[-\pi, \pi[$, alors $P = 0$ (utiliser les expressions complexes des fonctions cos et sin).
3. Montrer que si x_0, \dots, x_{2n} sont des réels deux à deux distincts dans $[-\pi, \pi[$, alors l'application :

$$\varphi : (P, Q) \mapsto \sum_{i=0}^{2n} P(x_i) Q(x_i)$$

définit un produit scalaire sur l'espace vectoriel \mathcal{P}_n .

Solution 14.4

1. Il est clair que \mathcal{P}_n est un sous-espace vectoriel de l'espace vectoriel des applications de \mathbb{R} dans \mathbb{R} . En notant respectivement c_k et s_k les fonctions $x \mapsto \cos(kx)$ pour $k \geq 0$ et $x \mapsto \sin(kx)$ pour $k \geq 1$, \mathcal{P}_n est engendré par la famille $\mathcal{B}_n = \{c_k \mid 0 \leq k \leq n\} \cup \{s_k \mid 1 \leq k \leq n\}$, c'est donc un espace vectoriel de dimension au plus égale à $2n+1$. Montrons que cette famille de fonctions est libre. Pour ce faire, on procède par récurrence sur $n \geq 1$ (comme avec l'exercice 9.4).

Pour $n = 1$, si $a_0 + a_1 \cos(x) + b_1 \sin(x) = 0$, en évaluant cette fonction en 0, $\frac{\pi}{2}$ et π successivement, on aboutit au système linéaire :

$$\begin{cases} a_0 + a_1 = 0 \\ a_0 + b_1 = 0 \\ a_0 - a_1 = 0 \end{cases}$$

qui équivaut à $a_0 = b_0 = b_1 = 0$. La famille $\{c_0, c_1, s_1\}$ est donc libre.

Supposons le résultat acquis au rang $n-1 \geq 1$. Si $P = a_0 + \sum_{k=1}^n (a_k c_k + b_k s_k) = 0$, en

dérivant deux fois, on a :

$$P'' = - \sum_{k=1}^n k^2 (a_k c_k + b_k s_k) = 0$$

Il en résulte que :

$$n^2 P + P'' = n^2 a_0 + \sum_{k=1}^{n-1} (n^2 - k^2) (a_k c_k + b_k s_k) = 0$$

et l'hypothèse de récurrence nous dit que $n^2 a_0 = 0$, $(n^2 - k^2) a_k = 0$ et $(n^2 - k^2) b_k$ pour tout k compris entre 1 et $n-1$, ce qui équivaut à dire que $a_0 = 0$ et $a_k = b_k = 0$ pour tout k compris entre 1 et $n-1$ puisque $n^2 - k^2 \neq 0$. Il reste alors $a_n c_n + b_n s_n = 0$, ce qui implique $a_n = 0$, en évaluant en $x = 0$ et $b_n = 0$. La famille \mathcal{B}_n est donc libre.

On verra un peu plus loin que cette famille est orthogonale, formée de fonctions non nulles, et en conséquence libre (exercice 12.15).

2. Posant $z = e^{ix}$ pour tout réel x , on a :

$$\begin{aligned} P(x) &= a_0 + \sum_{k=1}^n \left(a_k \frac{z^k + \bar{z}^k}{2} + b_k \frac{z^k - \bar{z}^k}{2i} \right) \\ &= a_0 + \frac{1}{2} \sum_{k=1}^n \left(a_k \left(z^k + \frac{1}{z^k} \right) - ib_k \left(z^k - \frac{1}{z^k} \right) \right) \\ &= a_0 + \frac{1}{2} \sum_{k=1}^n \left((a_k - ib_k) z^k + (a_k + ib_k) \frac{1}{z^k} \right) \end{aligned}$$

ou encore :

$$z^n P(x) = a_0 z^{2n} + \frac{1}{2} \sum_{k=1}^n ((a_k - ib_k) z^{n+k} + (a_k + ib_k) z^{n-k}) = Q(z)$$

Il en résulte que si P s'annule en $2n+1$ points deux à deux distincts, x_0, \dots, x_{2n} , dans $[-\pi, \pi[$, alors le polynôme complexe $Q \in \mathbb{C}_{2n}[z]$ s'annule en $2n+1$ points distincts du cercle unité, $e^{ix_0}, \dots, e^{ix_{2n}}$, ce qui revient à dire que c'est le polynôme nul et $P = 0$.

3. On vérifie facilement que φ est une forme bilinéaire symétrique et positive. L'égalité $\varphi(P, P) = 0$ entraîne que $P \in \mathcal{P}_n$ s'annule en $2n+1$ points deux à deux distincts dans $[-\pi, \pi[$ et en conséquence $P = 0$.

Exercice 14.5 Montrer que, pour toute fonction $\alpha \in \mathcal{C}^0([a, b], \mathbb{R}_+^*)$, l'application :

$$\varphi : (f, g) \mapsto \int_a^b f(t) g(t) \alpha(t) dt$$

définit un produit scalaire sur l'espace vectoriel $E = \mathcal{C}^0([a, b], \mathbb{R})$.

Solution 14.5 Avec la structure de corps commutatif de \mathbb{R} et la linéarité et positivité de l'intégrale, on déduit que φ est une forme bilinéaire symétrique positive sur E . Sachant que l'intégrale sur $[a, b]$ d'une fonction continue et à valeurs positives est nulle si, et seulement si, cette fonction est nulle, on déduit que φ est une forme définie. Donc φ est un produit scalaire sur E .

Exercice 14.6 Montrer que l'application :

$$(f, g) \mapsto \int_{-\pi}^{\pi} f(t) g(t) dt$$

définit un produit scalaire sur l'espace vectoriel \mathcal{F} des fonctions définies sur \mathbb{R} à valeurs réelles, continues et périodiques de période 2π .

Solution 14.6 Ce sont les mêmes arguments qu'à l'exercice précédent compte tenu qu'une fonction de \mathcal{F} est nulle si, et seulement si, elle est nulle sur $[-\pi, \pi]$.

14.2 Inégalités de Cauchy-Schwarz et de Minkowski

Dans tout ce qui suit E désigne un espace préhilbertien.

Théorème 14.1 (Inégalité de Cauchy-Schwarz) Pour tous x, y dans E on a :

$$|\langle x | y \rangle| \leq \|x\| \|y\|,$$

l'égalité étant réalisée si, et seulement si, x et y sont liés.

Démonstration. Si $x = 0$, on a alors l'égalité pour tout $y \in E$.

Si $x \neq 0$ et $y = \lambda x$ avec $\lambda \in \mathbb{R}$, on a encore l'égalité.

On suppose donc que x est non nul et y non lié à x . La fonction polynomiale P défini par :

$$P(t) = \|y + tx\|^2 = \|x\|^2 t^2 + 2 \langle x | y \rangle t + \|y\|^2$$

est alors à valeurs strictement positives, le coefficient de t^2 étant non nul, il en résulte que son discriminant est strictement négatif, soit :

$$\langle x | y \rangle^2 - \|x\|^2 \|y\|^2 < 0,$$

ce qui équivaut à $|\langle x | y \rangle| < \|x\| \|y\|$. ■

Sur \mathbb{R}^n muni du produit scalaire canonique, l'inégalité de Cauchy-Schwarz prend la forme suivante :

$$\left| \sum_{k=1}^n x_k y_k \right|^2 \leq \left(\sum_{k=1}^n x_k^2 \right) \left(\sum_{k=1}^n y_k^2 \right)$$

On peut déduire de cette inégalité quelques inégalités intéressantes sur les réels.

Exercice 14.7

1. On se donne un entier $n \geq 1$ et des réels x_1, \dots, x_n . Montrer que :

$$\left(\sum_{k=1}^n x_k \right)^2 \leq n \sum_{k=1}^n x_k^2$$

Dans quel cas a-t-on égalité ?

2. En déduire une condition nécessaire et suffisante, sur les réels a et b , pour que l'application

$\varphi : (x, y) \mapsto a \sum_{i=1}^n x_i y_i + b \sum_{1 \leq i \neq j \leq n} x_i y_j$ définissent un produit scalaire sur \mathbb{R}^n , où $n \geq 2$.

Solution 14.7

1. L'inégalité de Cauchy-Schwarz nous donne :

$$\left(\sum_{k=1}^n x_k \cdot 1\right)^2 \leq \left(\sum_{k=1}^n 1^2\right) \left(\sum_{k=1}^n x_k^2\right) = n \sum_{k=1}^n x_k^2$$

l'égalité étant réalisée si, et seulement si, tous les x_k sont égaux.

2. L'application φ est bilinéaire et symétrique. Pour $x \in \mathbb{R}^n$, on a :

$$\begin{aligned} q(x) = \varphi(x, x) &= a \sum_{i=1}^n x_i^2 + 2b \sum_{1 \leq i < j \leq n} x_i x_j \\ &= a \sum_{i=1}^n x_i^2 + b \left(\left(\sum_{i=1}^n x_i \right)^2 - \sum_{i=1}^n x_i^2 \right) \\ &= (a - b) \sum_{i=1}^n x_i^2 + b \left(\sum_{i=1}^n x_i \right)^2 \end{aligned}$$

Si φ est un produit scalaire, on a alors $a = q(e_1) > 0$, $a - b = q(e_1 - e_2) > 0$ et $q\left(\sum_{i=1}^n e_i\right) = n(a + (n-1)b) > 0$.

Réciproquement si $a > 0$, $a - b > 0$ et $a + (n-1)b > 0$, on a alors pour $x \in \mathbb{R}^n \setminus \{0\}$ ayant au moins deux composantes distinctes :

$$\begin{aligned} q(x) &= (a - b) \sum_{i=1}^n x_i^2 + b \left(\sum_{i=1}^n x_i \right)^2 \\ &> (a - b) \frac{1}{n} \left(\sum_{i=1}^n x_i \right)^2 + b \left(\sum_{i=1}^n x_i \right)^2 \\ &= \frac{1}{n} (a + (n-1)b) \left(\sum_{i=1}^n x_i \right)^2 \geq 0 \end{aligned}$$

et $q(x) > 0$. Si $x \in \mathbb{R}^n \setminus \{0\}$ a toutes ses composantes égales à $\lambda \neq 0$, on a alors :

$$q(x) = q\left(\lambda \sum_{i=1}^n e_i\right) = n\lambda^2 (a + (n-1)b) > 0.$$

Donc φ est un produit scalaire.

Troisième partie

Géométrie affine

Espaces affines

15.1 Définition d'un espace affine

15.2 Sous-espaces affines

15.3 Barycentres

15.4 Équations cartésiennes d'une droite du plan

On note \mathcal{P} le plan affine, $\vec{\mathcal{P}}$ le plan vectoriel associé et $\mathcal{R} = (O, \vec{i}, \vec{j})$ est un repère affine de \mathcal{P} . On notera $\mathcal{B} = (\vec{i}, \vec{j})$ la base de $\vec{\mathcal{P}}$ correspondante.

Si M est un point de \mathcal{P} de coordonnées (x, y) dans le repère \mathcal{R} , on notera $M(x, y)$, ce qui signifie que $\overrightarrow{OM} = x\vec{i} + y\vec{j}$.

Si A est un point de \mathcal{P} et \vec{v} un vecteur non nul, on note $\mathcal{D}(A, \vec{v})$ la droite passant par A et dirigée par \vec{v} , soit :

$$\mathcal{D}(A, \vec{v}) = \left\{ M \in \mathcal{P} \mid \exists \lambda \in \mathbb{R} ; \overrightarrow{AM} = \lambda \vec{v} \right\}$$

Pour A et \vec{v} fixés, on notera simplement \mathcal{D} une telle droite.

On dit que \vec{v} est un vecteur directeur de la droite \mathcal{D} et la droite vectorielle $\vec{\mathcal{D}} = \mathbb{R}\vec{v}$ est la direction de \mathcal{D} .

Définition 15.1 On dit que deux droites sont parallèles si elles ont même direction.

Théorème 15.1 Pour $A(x_A, y_A) \in \mathcal{P}$ et $\vec{v} = \alpha\vec{i} + \beta\vec{j} \in \vec{\mathcal{P}} \setminus \{\vec{0}\}$, on a :

$$\mathcal{D}(A, \vec{v}) = \{M(x, y) \in \mathcal{P} \mid ax + by + c = 0\}$$

où $(a, b) = (\beta, -\alpha) \neq (0, 0)$ et $c = \alpha y_A - \beta x_A$.

Réciproquement si a, b, c sont des réels tels que $(a, b) \neq (0, 0)$, alors l'ensemble $\mathcal{D} = \{M(x, y) \in \mathcal{P} \mid ax + by + c = 0\}$ est une droite dirigée par $\vec{v} = -b\vec{i} + a\vec{j}$.

Démonstration. Dire que $M(x, y) \in \mathcal{D}(A, \vec{v})$ équivaut à dire que les vecteurs \overrightarrow{AM} et \vec{v} sont liés, ce qui est encore équivalent à :

$$\det_B(\overrightarrow{AM}, \vec{v}) = \begin{vmatrix} x - x_A & \alpha \\ y - y_A & \beta \end{vmatrix} = \beta(x - x_A) - \alpha(y - y_A) = 0$$

et donc :

$$\mathcal{D}(A, \vec{v}) = \{M(x, y) \in \mathcal{P} \mid ax + by + c = 0\}$$

avec :

$$(a, b, c) = (\beta, -\alpha, \alpha y_A - \beta x_A)$$

et $(a, b) = (\beta, -\alpha) \neq (0, 0)$.

Si on veut se passer des déterminants, on écrit que $M(x, y) \in \mathcal{D}(A, \vec{v})$ si, et seulement si, il existe un réel λ tel que $\overrightarrow{AM} = \lambda \vec{v}$ ce qui se traduit par :

$$\begin{cases} x - x_A = \lambda \alpha \\ y - y_A = \lambda \beta \end{cases}$$

et $\beta(x - x_A) - \alpha(y - y_A) = \lambda\alpha\beta - \lambda\alpha\beta = 0$.

Réciproquement soit :

$$\mathcal{D} = \{M(x, y) \in \mathcal{P} \mid ax + by + c = 0\}$$

On a $\mathcal{D} \neq \emptyset$ puisque $(0, -\frac{c}{b}) \in \mathcal{D}$ si $b \neq 0$ ou $(-\frac{c}{a}, 0) \in \mathcal{D}$ si $a \neq 0$ (on peut aussi dire qu'une forme linéaire non nulle est surjective, il existe donc $(x, y) \in \mathbb{R}^2$ tel que $ax + by = -c$ pour tout réel c). En se fixant un point $A(x_A, y_A)$ dans \mathcal{D} , on a pour tout point $M(x, y) \in \mathcal{D}$:

$$ax + by = -c = ax_A + by_A$$

soit $a(x - x_A) + b(y - y_A) = 0$ ou encore $\begin{vmatrix} x - x_A & -b \\ y - y_A & a \end{vmatrix} = 0$, ce qui traduit le fait que les vecteurs \overrightarrow{AM} et $\vec{v} = -b\vec{i} + a\vec{j}$ sont liés avec \vec{v} non nul. On a donc $\mathcal{D} \subset \mathcal{D}(A, \vec{v})$ et le premier point de la démonstration nous donne l'autre inclusion. On a donc bien $\mathcal{D} = \mathcal{D}(A, \vec{v})$.

■

Avec les notations du théorème, on dit que \mathcal{D} est la droite d'équation cartésienne (ou d'équation implicite) $ax + by + c = 0$ dans le repère \mathcal{R} . En réalité on a obtenu ainsi une équation polynomiale de degré 1 de \mathcal{D} et une telle équation n'est pas unique. Précisément on a le résultat suivant.

Théorème 15.2 Soient a, b, c et a', b', c' des réels avec $(a, b) \neq (0, 0)$ et $(a', b') \neq (0, 0)$. Les équations $ax + by + c = 0$ et $a'x + b'y + c' = 0$ (dans le repère \mathcal{R}) définissent la même droite si, et seulement si, les vecteurs de \mathbb{R}^3 (a, b, c) et (a', b', c') sont colinéaires (ce qui équivaut à dire qu'il existe un réel non nul λ tel que $(a', b', c') = \lambda(a, b, c)$).

Lorsque l'on parle de la droite d'équation $ax + by + c = 0$, les coefficients a, b, c sont uniques à la multiplication près d'un réel non nul.

Remarque 15.1 Si \mathcal{D} est une droite d'équation $ax + by + c = 0$, alors sa direction \vec{D} a pour équation $ax + by = 0$.

Théorème 15.3 Les droites \mathcal{D} et \mathcal{D}' d'équations respectives $ax + by + c = 0$ et $a'x + b'y + c' = 0$ sont parallèles si, et seulement si, $\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} = ab' - a'b = 0$.

Si \mathcal{D} est une droite d'équation $ax + by + c = 0$, alors toute droite parallèle a pour équation $ax + by + c' = 0$

Théorème 15.4 Deux droites \mathcal{D} et \mathcal{D}' sont parallèles si, et seulement si, elles sont égales ou sans point commun.

Définition 15.2 Deux droites ayant un unique point commun sont dites sécantes.

Exercice 15.1 Soient a, b deux réels non nuls. À quelles conditions portant sur a et b les droites d'équations respectives $\frac{x}{a} + \frac{y}{b} - 1 = 0$ et $\frac{x}{b} + \frac{y}{a} - 1 = 0$ sont-elles sécantes ? Déterminer le point d'intersection de ces droites dans ce cas.

Définition 15.3 Soit p un entier supérieur ou égal à 2. On dit que des droites $\mathcal{D}_1, \dots, \mathcal{D}_p$ sont concourantes si l'intersection $\bigcap_{k=1}^p \mathcal{D}_k$ est réduite à un point.

Théorème 15.5 Soient \mathcal{D} , \mathcal{D}' et \mathcal{D}'' trois droites d'équations respectives $ax + by + c = 0$, $a'x + b'y + c' = 0$ et $a''x + b''y + c'' = 0$. Ces droites sont parallèles ou concourantes si, et seulement si,
$$\begin{vmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{vmatrix} = 0.$$

15.5 Le triangle dans le plan affine euclidien

On note \mathcal{P} le plan affine, $\vec{\mathcal{P}}$ le plan vectoriel associé et $\mathcal{R} = (O, \vec{i}, \vec{j})$ est un repère affine de \mathcal{P} . On notera $\mathcal{B} = (\vec{i}, \vec{j})$ la base de $\vec{\mathcal{P}}$ correspondante.

Si A, B sont deux points de \mathcal{P} , on note $AB = \|\vec{AB}\|$ la distance de A à B .

Définition 15.4 Un triangle (non dégénéré) est la figure formée par trois points distincts A, B, C du plan \mathcal{P} . On le note ABC .

On dit que les points A, B, C sont les sommets du triangle et les segments $[B, C]$, $[A, C]$ et $[A, B]$ sont les cotés du triangle opposés respectivement aux sommets A, B et C .

On dit que le triangle est aplati si les points A, B, C sont alignés.

Les triangles considérés sont a priori non aplatis. Un triangle non aplati est aussi appelé vrai triangle.

Définition 15.5 On dit qu'un triangle ABC est isocèle en A , si $AB = AC$.

Dire qu'un triangle est isocèle en A revient à dire que le sommet A est sur la médiatrice du côté opposé $[B, C]$.

15.5.1 Médianes d'un triangle, centre de gravité

Définition 15.6 Si ABC est un triangle, la médiane issue du sommet A est la droite \mathcal{M}_A qui joint A au milieu I_A du côté opposé $[B, C]$.

On définit de manière analogue les médianes issues des sommets B et C .

Théorème 15.6 Les trois médianes d'un triangle ABC concourent en un point G qui est l'isobarycentre G de A, B, C .

Démonstration. C'est une conséquence de la propriété d'associativité du barycentre.

Si G est le barycentre de $\{(A, 1), (B, 1), (C, 1)\}$, c'est aussi le barycentre de $\{(A, 1), (I_A, 1)\}$ où I_A est le milieu de $[B, C]$ (c'est-à-dire le barycentre de $\{(B, 1), (C, 1)\}$) et on a $\overrightarrow{GA} + 2\overrightarrow{GI_A} = \vec{0}$, soit $\overrightarrow{AG} = \frac{2}{3}\overrightarrow{AI_A}$ et $G \in \mathcal{M}_A$. Comme A, B, C jouent des rôles analogues, G est aussi sur les médianes \mathcal{M}_B et \mathcal{M}_C .

Le point G est donc à l'intersection des trois médianes. ■

Les relations $\overrightarrow{MG} = \frac{2}{3}\overrightarrow{MI_M}$ pour $M \in \{A, B, C\}$ nous disent que G est situé sur chaque médiane au $\frac{2}{3}$ de la longueur MI_M en partant du sommet M .

On dit que le point G , isobarycentre des sommets du triangle ABC , est le centre de gravité de ce triangle.

Exercice 15.2 *Étant données trois droites distinctes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ concourantes en un point G , construire un (vrai) triangle ABC de médianes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$.*

Solution 15.1 *On procède comme suit :*

- choisir un point I_A sur \mathcal{D}_1 distinct de G ;
- construire avec un compas le point J sur \mathcal{D}_1 tel que $\overrightarrow{GJ} = -\overrightarrow{GI_A}$, puis le point A tel que $\overrightarrow{GJ} = \overrightarrow{JA}$;
- construire à la règle et au compas la droite \mathcal{D} parallèle à \mathcal{D}_3 et passant par J ;
- on note I_B l'intersection de \mathcal{D} et \mathcal{D}_2 et C l'intersection de \mathcal{D}_3 et (AI_B) ;
- le théorème de Thalès nous dit que I_B est le milieu de $[A, C]$;
- on note B l'intersection de (CI_A) et \mathcal{D}_1 ;
- le triangle ABC convient.

15.5.2 Médiatrices d'un triangle

Définition 15.7 *Si A, B sont deux points distincts du plan \mathcal{P} , alors la médiatrice du segment $[A, B]$ est la droite :*

$$\mathcal{M}_{[A, B]} = \{M \in \mathcal{P} \mid MA = MB\}$$

Les médiatrices d'un triangle sont les médiatrices de ses cotés.

Un tracé à la règle et au compas de cette médiatrice peut se faire comme indiqué sur la figure 15.1.

On rappelle que le milieu du segment $[A, B]$ est le point I défini par $\overrightarrow{AB} = 2\overrightarrow{AI}$. C'est l'isobarycentre de A et B . Il est aussi caractérisé par :

$$\forall M \in \mathcal{P}, 2\overrightarrow{MI} = \overrightarrow{MA} + \overrightarrow{MB}$$

On en déduit que :

$$\forall M \in \mathcal{P}, MB^2 - MA^2 = (\overrightarrow{MB} + \overrightarrow{MA}) \cdot (\overrightarrow{MB} - \overrightarrow{MA}) = 2\overrightarrow{MI} \cdot \overrightarrow{AB}$$

Ce dernier résultat nous donne une définition équivalente de la médiatrice d'un segment.

Théorème 15.7 *Si A, B sont deux points distincts du plan \mathcal{P} , alors la médiatrice du segment $[A, B]$ est la droite $\mathcal{M}_{[A, B]}$ orthogonale à (AB) et passant par le milieu I de $[A, B]$.*

FIGURE 15.1 – Tracé de la médiatrice de $[A, B]$

Démonstration. Notons

$$\mathcal{M}'_{[A,B]} = \left\{ M \in \mathcal{P} \mid \overrightarrow{MI} \cdot \overrightarrow{AB} = 0 \right\}$$

la droite orthogonale à (AB) passant par I .

Avec l'égalité $2\overrightarrow{MI} \cdot \overrightarrow{AB} = MB^2 - MA^2$, on déduit que :

$$\overrightarrow{MI} \cdot \overrightarrow{AB} = 0 \Leftrightarrow MA = MB$$

ce qui revient à dire que $\mathcal{M}_{[A,B]} = \mathcal{M}'_{[A,B]}$. ■

Définition 15.8 On dit qu'un cercle \mathcal{C} est circonscrit à un triangle ABC si les trois sommets A, B, C appartiennent au cercle \mathcal{C} .

Théorème 15.8 Les trois médiatrices d'un triangle ABC sont concourantes en un point Ω qui est le centre du cercle circonscrit à ce triangle.

Démonstration. Si Ω est à l'intersection des médiatrices de $\mathcal{M}_{[B,C]}$ et $\mathcal{M}_{[A,B]}$ (ces droites ne sont pas parallèles puisque ABC est un vrai triangle), on a $\Omega B = \Omega C$ et $\Omega A = \Omega B$, donc $\Omega A = \Omega C$ et Ω est sur la médiatrice de $\mathcal{M}_{[A,C]}$, il est donc à l'intersection des trois médiatrices et les sommets du triangle sont sur le cercle de centre Ω et de rayon $R = \Omega A = \Omega B = \Omega C$. ■

Remarque 15.2 Si le triangle ABC est aplati, alors les médiatrices sont parallèles et donc non sécantes.

Exercice 15.3 Étant donné un cercle \mathcal{C} , construire son centre.

Solution 15.2 On prend trois points A, B, C sur ce cercle et l'intersection $\mathcal{M}_{[B,C]} \cap \mathcal{M}_{[A,C]}$ est le centre du cercle.

Exercice 15.4 Étant données trois droites distinctes $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ concourantes en un point Ω , construire un (vrai) triangle ABC de médiatrices $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$.

Solution 15.3 On procède comme suit :

- choisir un point M distinct de Ω ;

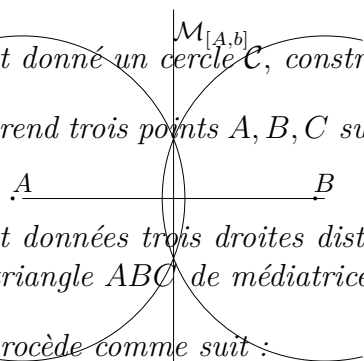


FIGURE 15.2 – Cercle circonscrit à un triangle

- construire M' symétrique orthogonal de M par rapport à \mathcal{D}_1 ;
- construire M'' symétrique orthogonal de M' par rapport à \mathcal{D}_2 ;
- construire la médiatrice \mathcal{D} de $[MM'']$;
- prendre $A \in \mathcal{D}$ distinct de Ω ;
- construire B symétrique orthogonal de A par rapport à \mathcal{D}_1 ;
- construire C symétrique orthogonal de B par rapport à \mathcal{D}_2 ;
- le triangle ABC convient.

15.5.3 Hauteurs d'un triangle

Définition 15.9 Si ABC est un triangle, la hauteur issue du sommet A est la droite

$$\mathcal{H}_A = \{M \in \mathcal{P} \mid \overrightarrow{AM} \cdot \overrightarrow{BC} = 0\}$$

passant A et orthogonale au côté opposé $[B, C]$.

On définit de manière analogue les hauteurs passant par les sommets B et C .

Lemme 15.1 (Stewart) Si ABC est un triangle, on a alors pour tout point M :

$$\overrightarrow{MA} \cdot \overrightarrow{BC} + \overrightarrow{MB} \cdot \overrightarrow{CA} + \overrightarrow{MC} \cdot \overrightarrow{AB} = 0$$

Démonstration. En posant $\varphi(M) = \overrightarrow{MA} \cdot \overrightarrow{BC} + \overrightarrow{MB} \cdot \overrightarrow{CA} + \overrightarrow{MC} \cdot \overrightarrow{AB}$, on a :

$$\begin{aligned} \varphi(M) &= \overrightarrow{MA} \cdot (\overrightarrow{BC} + \overrightarrow{CA} + \overrightarrow{AB}) + \overrightarrow{AB} \cdot \overrightarrow{CA} + \overrightarrow{AC} \cdot \overrightarrow{AB} \\ &= \overrightarrow{MA} \cdot \overrightarrow{BB} \cdot \overrightarrow{AC} (\overrightarrow{AB} - \overrightarrow{AB}) = 0 \end{aligned}$$

■

Théorème 15.9 *Les trois hauteurs d'un triangle ABC sont concourantes.*

Démonstration. Si H est le point d'intersection des hauteurs \mathcal{H}_A et \mathcal{H}_B , on a $\overrightarrow{HA} \cdot \overrightarrow{BC} = 0$, $\overrightarrow{HB} \cdot \overrightarrow{CA} = 0$ et l'identité de Stewart nous donne $\overrightarrow{HC} \cdot \overrightarrow{AB} = 0$, ce qui signifie que $H \in \mathcal{H}_C$. Les trois hauteurs sont donc concourantes. ■

Définition 15.10 *Le point d'intersection H des trois hauteurs d'un triangle ABC est l'orthocentre de ce triangle.*

Exercice 15.5 *Soit ABC un triangle et $A'B'C'$ le triangle construit en menant, pour chacun des cotés du triangle ABC , la parallèle à ce coté qui passe par le sommet opposé. Montrer que les hauteurs de ABC sont les médiatrices de $A'B'C'$ (ce qui permet de retrouver le fait que les hauteurs de ABC sont concourantes puisqu'on sait que les médiatrices de $A'B'C'$ sont concourantes).*

Solution 15.4 *On a $(AC) \parallel (BC')$ et $(BC) \parallel (AC')$, donc $AC'BC$ est un parallélogramme et $AC' = BC$.*

De même, $(AB') \parallel (BC)$ et $(B'C) \parallel (AB)$, donc $B'ABC$ est un parallélogramme et $AB' = BC$. Il en résulte que $AC' = AB'$ et A est le milieu de $[B', C']$.

La hauteur \mathcal{H}_A passe par A et est orthogonale à $(B'C')$ puisque cette hauteur est orthogonale à (BC) qui est parallèle à $(B'C')$. Cette hauteur est donc la médiatrice de $[B', C']$.

Procédant de manière analogue pour les deux autres hauteurs, on a le résultat annoncé.

16

Espaces affines euclidiens

17

Applications affines

Coniques

On se place dans le plan affine euclidien \mathcal{P} .

On note $\vec{u} \cdot \vec{v}$ le produit scalaire des vecteurs \vec{u} et \vec{v} .

Si A, B sont deux points de \mathcal{P} , on notera $d(A, B)$, AB ou $\|\overrightarrow{AB}\|$ la distance de A à B , $[AB]$ le segment d'extrémités A et B et pour $A \neq B$, (AB) la droite passant par A et B .

Si A est un point de \mathcal{P} et \mathcal{D} une droite de \mathcal{P} , on note :

$$d(A, \mathcal{D}) = \inf_{M \in \mathcal{D}} AM$$

la distance de A à \mathcal{D} . En désignant par H la projection orthogonale de A sur \mathcal{D} , on a $d(A, \mathcal{D}) = AH$ (figure 18.1). On a $d(A, \mathcal{D}) = 0$ si, et seulement si, $A \in \mathcal{D}$.

FIGURE 18.1 – Projection orthogonale

On rappelle que le barycentre d'une famille de points pondérés $\{(A_i, \alpha_i); 1 \leq i \leq n\}$, la somme $\sum_{i=1}^n \alpha_i$ étant non nulle, est le point défini par :

$$\sum_{i=1}^n \alpha_i \overrightarrow{GA_i} = \vec{0}$$

Ce point G est aussi défini par :

$$\forall M \in \mathcal{P}, \left(\sum_{i=1}^n \alpha_i \right) \overrightarrow{MG} = \sum_{i=1}^n \alpha_i \overrightarrow{MA_i}$$

18.1 Définition par directrice, foyer et excentricité

On se donne une droite \mathcal{D} , un point $F \notin \mathcal{D}$ et un réel $e > 0$.

À l'origine les sections coniques ont été définies dans l'espace comme intersection d'un plan avec un cône, d'où leur nom.

Nous donnons dans ce paragraphe une première définition métrique des coniques.

Définition 18.1 On appelle conique de directrice \mathcal{D} , de foyer F et d'excentricité e l'ensemble :

$$\Gamma = \{M \in \mathcal{P} \mid d(M, F) = e \cdot d(M, \mathcal{D})\}$$

- pour $e < 1$, on dit que Γ est une ellipse ;
- pour $e = 1$, on dit que Γ est une parabole ;
- pour $e > 1$, on dit que Γ est une hyperbole.

La distance $d(M, \mathcal{D})$ étant nulle si, et seulement si $M \in \mathcal{D}$, on aura $d(M, \mathcal{D}) > 0$ pour tout $M \in \Gamma$ puisque F n'est pas sur \mathcal{D} et on peut écrire que :

$$\Gamma = \left\{ M \in \mathcal{P} \setminus \mathcal{D} \mid \frac{d(M, F)}{d(M, \mathcal{D})} = e \right\}$$

ou encore, en désignant par H la projection orthogonale d'un point M du plan sur \mathcal{D} :

$$\Gamma = \left\{ M \in \mathcal{P} \setminus \mathcal{D} \mid \frac{MF}{MH} = e \right\}$$

On peut aussi dire que Γ est une ligne de niveau de la fonction $M \mapsto \frac{MF}{MH}$ définie sur $\mathcal{P} \setminus \mathcal{D}$.

On dit que la perpendiculaire Δ à \mathcal{D} passant par F est l'axe focal de la conique Γ (le mot focal signifie « qui est relatif au(x) foyers(s) »).

Le point K à l'intersection de \mathcal{D} et Δ est le projeté orthogonal de F sur \mathcal{D} .

La distance $d = KF$ est non nulle et le réel $p = ed$ est appelé paramètre de la conique.

Dans ce qui suit, on se donne une conique Γ de directrice \mathcal{D} , de foyer F et d'excentricité e et Δ est son axe focal.

Lemme 18.1 L'axe focal est un axe de symétrie de la conique.

Démonstration. En effet, on notant σ la symétrie orthogonale par rapport à Δ , on a $\sigma(F) = F$ et en remarquant que pour $M \in \mathcal{P}$, la projection orthogonale de $M' = \sigma(M)$ sur \mathcal{D} est $H' = \sigma(H)$ où H est la projection orthogonale sur \mathcal{D} de M , on a :

$$\frac{d(\sigma(M), F)}{d(\sigma(M), \mathcal{D})} = \frac{\sigma(M) \sigma(F)}{\sigma(M) \sigma(H)} = \frac{MF}{MH}$$

et en conséquence M est sur Γ si, et seulement si, $\sigma(M)$ est sur Γ (figure 18.2). ■

Le résultat qui suit nous confirme qu'une conique n'est pas vide.

FIGURE 18.2 – L'axe focal est une axe de symétrie

Théorème 18.1

1. L'intersection d'une parabole Γ avec son axe focal est réduite à un point qui est le milieu du segment $[FK]$.
2. L'intersection d'une ellipse ou d'une hyperbole Γ avec son axe focal est réduite aux deux points A, A' où A est le barycentre du système de points pondérés $\{(F, 1), (K, e)\}$ et A' le barycentre de $\{(F, 1), (K, -e)\}$.

Démonstration.

1. On suppose que Γ est une parabole, c'est-à-dire que $e = 1$.

Dire $M \in \Delta \cap \Gamma$ équivaut à dire que $M \in \Delta$ et $MF = d(M, \mathcal{D})$, ce qui équivaut à $M \in \Delta$ et $MF = MK$ (les points de Δ se projettent sur K), ce qui revient à dire que M est à l'intersection de la médiatrice de $[KF]$ et de Δ , c'est donc le milieu de $[KF]$.

2. On suppose que $e \neq 1$.

Dire $M \in \Delta \cap \Gamma$ équivaut à dire que $M \in \Delta$ et $MF^2 = e^2 MH^2$, ce qui équivaut à :

les points M, K, F étant alignés (ils sont tous sur Δ), ce qui équivaut à $\overrightarrow{MF} + e\overrightarrow{MK} = \vec{0}$ ou $\overrightarrow{MF} - e\overrightarrow{MK} = \vec{0}$ (de manière générale, on a $\vec{u} \cdot \vec{v} = \|\vec{u}\| \|\vec{v}\| \cos(\vec{u}, \vec{v})$ et ici $(\vec{u}, \vec{v}) \equiv 0 \text{ modulo } \pi$) encore équivaut à dire que M le barycentre de $\{(F, 1), (K, e)\}$ (on a $1 + e \neq 0$) ou celui de $\{(F, 1), (K, -e)\}$ (on a $1 - e \neq 0$). ■

Le résultat suivant nous donne une autre définition de la parabole comme lieu géométrique.

On rappelle que si \mathcal{C} est un cercle de centre O et de rayon $R > 0$ et \mathcal{D} une droite, on a alors, en notant $d = d(O, \mathcal{D})$:

$$\mathcal{C} \cap \mathcal{D} = \begin{cases} \emptyset & \text{si } d > R \\ \{H\} & \text{si } d = R \\ \{M_1, M_2\} & \text{si } d < R \end{cases}$$

où H est la projection orthogonale de O sur \mathcal{D} et $M_1 \neq M_2$ pour $d < R$. Le cas où cette intersection est réduite à un point est équivalent à dire que le cercle et la droite sont tangents, ce qui équivaut encore à dire que $O \notin \mathcal{D}$ et la droite \mathcal{D} est perpendiculaire à la droite (OH) .

Lemme 18.2 *La parabole Γ de directrice \mathcal{D} et foyer F est aussi le lieu des centres des cercles tangents à \mathcal{D} et passant par F (figure 18.3).*

FIGURE 18.3 – Parabole comme lieu des centres des cercles ...

Démonstration. Si $M \in \Gamma$, la condition $MF = MH$ nous dit alors que le cercle \mathcal{C} de centre M et de rayon MF (donc passant par F) est tangent à la droite \mathcal{D} .

Réciproquement si $M \in \mathcal{P}$ est le centre d'un cercle \mathcal{C} tangent à \mathcal{D} et passant par F , on a alors $R = MF = MH$ et $M \in \Gamma$. ■

18.2 Équation réduite d'une conique

Le lemme 18.1 nous incite à prendre l'axe focal Δ pour axe des abscisses (ou des ordonnées) puisque c'est un axe de symétrie.

Théorème 18.2 *Il existe un repère orthonormé (O, \vec{i}, \vec{j}) dans lequel la conique Γ a pour équation :*

$$(1 - e^2)x^2 + y^2 - 2(x_F - e^2x_K)x = e^2x_K^2 - x_F^2 \quad (18.1)$$

Démonstration. On se donne un repère orthonormé (O, \vec{i}, \vec{j}) , où l'origine O est sur l'axe focal Δ et est à préciser et \vec{i} est un vecteur directeur unitaire de $\vec{\Delta}$. On note (x, y) les

coordonnées d'un point $M \in \mathcal{P}$ dans ce repère. Les coordonnées du point F sont $(x_F, 0)$ et l'équation de la droite \mathcal{D} est $x = x_K$. On a alors les équivalences :

$$\begin{aligned}(M \in \Gamma) &\Leftrightarrow (MF^2 = e^2 MH^2) \Leftrightarrow ((x - x_F)^2 + y^2 = e^2 (x - x_K)^2) \\ &\Leftrightarrow ((1 - e^2) x^2 + y^2 - 2(x_F - e^2 x_K) x = e^2 x_K^2 - x_F^2)\end{aligned}$$

■

Les points d'intersection de la conique Γ avec l'axe focal sont les points $M(x, y) \in \Gamma$ tels que $y = 0$, ce qui donne :

$$(1 - e^2) x^2 - 2(x_F - e^2 x_K) x = e^2 x_K^2 - x_F^2$$

Pour $e = 1$, on obtient :

$$2(x_F - x_K) x = x_K^2 - x_F^2$$

avec $x_F \neq x_K$ puisque $F \notin \mathcal{D}$, ce qui donne :

$$x = \frac{x_F + x_K}{2}$$

et on retrouve le milieu du segment $[FK]$ comme unique point d'intersection.

Pour $e \neq 1$, on a une équation polynomiale de degré 2 de discriminant réduit :

$$\begin{aligned}\delta &= (x_F - e^2 x_K)^2 + (1 - e^2) (e^2 x_K^2 - x_F^2) \\ &= e^2 (x_F^2 + x_K^2 - 2x_F x_K) = e^2 (x_K - x_F)^2 = (ed)^2 = p^2\end{aligned}$$

et on a les deux solutions :

$$x_1 = \frac{x_F - e^2 x_K - ed}{1 - e^2} \text{ et } x_2 = \frac{x_F - e^2 x_K + ed}{1 - e^2}$$

ce qui s'écrit aussi, compte tenu de $d = |x_K - x_F|$:

$$x_1 = \frac{x_F - ex_K}{1 - e} \text{ et } x_2 = \frac{x_F + ex_K}{1 + e}$$

ou :

$$x_1 = \frac{x_F + ex_K}{1 + e} \text{ et } x_2 = \frac{x_F - ex_K}{1 - e}$$

et on retrouve les deux points d'intersection, A barycentre de $\{(F, 1), (K, e)\}$ et A' barycentre de $\{(F, 1), (K, -e)\}$.

De ce résultat on déduit une représentation polaire de Γ .

Théorème 18.3 Dans un repère orthonormé (F, \vec{i}, \vec{j}) , où $\vec{i} = \frac{1}{FK} \overrightarrow{FK}$, la conique Γ a pour équation polaire :

$$\rho = \frac{ed}{1 + e \cos(\theta)}$$

avec $\rho \in \mathbb{R}^*$ et $\theta \in \mathbb{R}$. (figure 18.4).

Démonstration. Prenant pour origine $O = F$ et pour premier vecteur de base $\vec{i} = \frac{1}{FK} \overrightarrow{FK}$, on a $x_F = 0$, $x_K = FK = d$ et une équation cartésienne de Γ est :

$$(1 - e^2) x^2 + y^2 + 2e^2 dx - e^2 d^2 = 0.$$

18.2.1 Les paraboles

Équation réduite d'une parabole

Si Γ est une parabole, on a alors $e = 1$ et :

$$(M \in \Gamma) \Leftrightarrow (y^2 - 2(x_F - x_K)x = (x_F - x_K)(x_F + x_K))$$

ce qui nous conduit à choisir l'origine O de sorte que $x_F = -x_K$, c'est-à-dire que O est le milieu de $[FK]$, soit l'unique point d'intersection de Γ avec son axe focal. En prenant $\vec{i} = \frac{1}{OF}\overrightarrow{OF}$, on a alors $x_F = OF = \frac{KF}{2} = \frac{p}{2}$, $x_K = -x_F$ et $x_F - x_K = p$, de sorte que dans ce repère une équation de la parabole est $y^2 = 2px$.

On dit que le point O , milieu de $[KF]$, est le sommet de la parabole.

Réciproquement si Γ est une courbe d'équation $y^2 = 2px$ dans un repère orthonormé (O, \vec{i}, \vec{j}) avec $p > 0$, en remontant les calculs précédents, on vérifie que Γ est une parabole de directrice \mathcal{D} d'équation $x = -\frac{p}{2}$ et de foyer $F\left(\frac{p}{2}, 0\right)$. En effet, en posant $x_F = \frac{p}{2}$ et $x_K = -x_F$, on a :

$$(y^2 = 2px) \Leftrightarrow ((x - x_F)^2 + y^2 = (x - x_K)^2) \Leftrightarrow (MF = MH).$$

Cette équation nous permet un tracé de la parabole Γ dans le repère orthonormé (O, \vec{i}, \vec{j}) .

Avec la parité de $y \mapsto \frac{1}{2p}y^2$, on étudie cette courbe pour $y \geq 0$, puis on complète le graphe obtenu par symétrie par rapport à l'axe $\Delta = Ox$. Cette fonction est strictement croissante de \mathbb{R}^+ sur \mathbb{R}^+ avec $\frac{x}{y} \xrightarrow{y \rightarrow +\infty} +\infty$, on a donc une branche parabolique de direction Ox (c'est la définition). En O on a une tangente verticale. Le tracé du graphe de Γ s'en suit.

Paramétrisation et tangentes à une parabole

De cette équation cartésienne de la parabole dans un repère orthonormé (O, \vec{i}, \vec{j}) , on peut déduire la paramétrisation :

$$\gamma : t \in \mathbb{R} \mapsto \left(\frac{t^2}{2p}, t\right)$$

Le vecteur dérivé $\gamma'(t) = \left(\frac{t}{p}, 1\right)$ ne s'annulant jamais, on déduit que la parabole Γ admet une tangente en chacun de ces points $\gamma(t_0) = \left(\frac{t_0^2}{2p}, t_0\right)$, cette tangente étant dirigée par $\gamma'(t_0) = \left(\frac{t_0}{p}, 1\right)$. Une représentation paramétrique de cette tangente est donc :

$$\begin{cases} x = \frac{t_0^2}{2p} + \lambda \frac{t_0}{p} \\ y = t_0 + \lambda \end{cases} \quad \lambda \in \mathbb{R}$$

Une équation cartésienne est obtenue en écrivant que :

$$\begin{vmatrix} x - \frac{t_0^2}{2p} & \frac{t_0}{p} \\ (y - t_0) & 1 \end{vmatrix} = x - \frac{t_0^2}{2p} - \frac{t_0}{p}(y - t_0) = 0$$

ce qui donne :

$$p(x - x_0) - y_0(y - y_0) = 0.$$

Cette équation cartésienne peut aussi être obtenue à partir de l'équation implicite $f(x, y) = 2px - y^2 = 0$ de Γ . La différentielle de f ne s'annulant jamais, la tangente à Γ en $M_0(x_0, y_0)$ a pour équation :

$$\frac{\partial f}{\partial x}(M_0)(x - x_0) + \frac{\partial f}{\partial y}(M_0)(y - y_0) = 0$$

soit :

$$p(x - x_0) - y_0(y - y_0) = 0.$$

Ce qui peut aussi s'écrire, compte tenu de $y_0^2 = 2px_0$:

$$px - y_0y + px_0 = 0.$$

On peut remarquer que les tangentes à une parabole ne sont jamais parallèles à l'axe focal (l'axe des abscisses) puisque une telle droite serait d'équation $ax + by + c = 0$ avec $a = 0$ et le coefficient p est strictement positif.

Si une telle tangente est parallèle à la directrice \mathcal{D} , elle est alors perpendiculaire à l'axe focal donc d'équation $x = x_0$ et $y_0 = 0$ dans l'équation ci-dessus, ce qui donne $x_0 = 0$ ($y_0^2 = 2px_0$) et M_0 est le sommet O de la parabole.

Construction à la règle et au compas d'une parabole

Des considérations géométriques élémentaires nous fournissent un procédé de construction de la parabole à la règle et au compas.

Pour $H \in \mathcal{D}$ on désigne par D_H la perpendiculaire à \mathcal{D} passant par H et par D'_H la médiatrice du segment $[HF]$ (comme $F \notin \mathcal{D}$, on a $H \neq F$). On a alors :

$$(M \in D_H \cap \Gamma) \Leftrightarrow (M \in D_H \text{ et } MF = MH) \Leftrightarrow (M \in D_H \cap D'_H)$$

L'intersection $D_H \cap D'_H$ étant bien réduite à un point puisque D'_H n'est pas parallèle à D_H (sinon (HF) serait perpendiculaire à Δ et F serait sur \mathcal{D}).

Les points de la parabole sont donc les points d'intersection de la perpendiculaire D_H à \mathcal{D} passant par H avec la médiatrice D'_H du segment $[HF]$.

Remarque 18.1 En notant $D_H \cap D'_H = \{M_H\}$, l'application $H \mapsto M_H$ nous donne une paramétrisation de la parabole dans un repère orthonormé (O, \vec{i}, \vec{j}) , où O est le sommet de la parabole.

En notant $M_0(x_0, y_0) = M_H$ un point de la parabole ainsi construit, on a $H(-\frac{p}{2}, y_0)$, $F(\frac{p}{2}, 0)$, $\overrightarrow{HF} = (p, -y_0)$ et la médiatrice D'_H a pour équation :

$$\overrightarrow{HF} \cdot \overrightarrow{M_0M} = p(x - x_0) - y_0(y - y_0) = 0$$

c'est donc la tangente à Γ en M_0 . Cette tangente coupe $[HF]$ en son milieu $I_H(p, 0)$.

Théorème 18.4 Soient Γ une parabole, M un point de Γ et H le projeté orthogonal de M sur la directrice \mathcal{D} . La tangente à Γ en M est la médiatrice de $[HF]$. Si M n'est pas sur l'axe focal Δ , cette tangente est aussi la hauteur issue de M dans le triangle FMH et la bissectrice intérieure de l'angle en M (figure 18.5).

FIGURE 18.5 – Tangente à une parabole

Démonstration. On vient de voir que la tangente à Γ en M est la médiatrice de $[HF]$. Considérant que le triangle MFH est isocèle en M ($MF = MH$), cette médiatrice est aussi la hauteur issue de M et la bissectrice intérieure de l'angle en M .

On peut aussi montrer ce résultat en utilisant une paramétrisation régulière :

de Γ dans un repère orthonormé (F, \vec{i}, \vec{j}) , où $\vec{i} = \frac{1}{FK} \overrightarrow{FK}$.

En notant $H(t)$ la projection orthogonale de $M(t)$ sur \mathcal{D} et en dérivant l'égalité :

$$\|\overrightarrow{FM(t)}\|^2 - \|\overrightarrow{M(t)H(t)}\|^2 = 0,$$

on a :

$$\overrightarrow{FM(t)} \cdot \overrightarrow{FM'(t)} - \overrightarrow{M(t)H(t)} \cdot (\overrightarrow{FH'(t)} - \overrightarrow{FM'(t)}) = 0.$$

Comme $\overrightarrow{M(t)H(t)}$ est orthogonal à \mathcal{D} et les points $F, H'(t)$ sont sur l'axe des y qui est parallèle à \mathcal{D} (on a $H(t) = (x_k, y(t))$ et $H'(t) = (0, y'(t))$), les vecteurs $\overrightarrow{M(t)H(t)}$ et $\overrightarrow{FH'(t)}$ sont orthogonaux, de sorte que :

$$\overrightarrow{FM(t)} \cdot \overrightarrow{FM'(t)} + \overrightarrow{M(t)H(t)} \cdot \overrightarrow{FM'(t)} = 0$$

soit :

$$(\overrightarrow{FM(t)} + \overrightarrow{M(t)H(t)}) \cdot \overrightarrow{FM'(t)} = 0$$

c'est-à-dire :

$$\overrightarrow{FH(t)} \cdot \overrightarrow{FM'(t)} = 0$$

La tangente à Γ en $M(t)$ qui est la droite passant par $M(t)$ et dirigée par $\overrightarrow{FM'(t)}$ est donc perpendiculaire à $[FH]$, ce qui signifie que c'est la hauteur issue de $M = M(t)$ dans le triangle MFH . Le triangle étant isocèle en M , on a les autres résultats. ■

De ce théorème, on déduit que tout rayon lumineux parallèle à l'axe focal Δ se réfléchit en un rayon qui passe par le foyer. C'est le principe des miroirs paraboliques.

Exercice 18.1 Soit Γ une parabole. Pour tout $M \in \Gamma$ qui n'est pas sur l'axe focal, on désigne par P la projection orthogonale de M sur Δ et par Q le point d'intersection de la normale à Γ en M avec Δ . Montrer que la longueur PQ est constante.

Solution 18.1 On utilise la paramétrisation :

$$\gamma : t \in \mathbb{R} \mapsto \left(\frac{t^2}{2p}, t \right)$$

de Γ dans un repère orthonormé (O, \vec{i}, \vec{j}) où \vec{i} dirige $\vec{\Delta}$ et on note $M = \gamma(t)$ un point de Γ , $P\left(\frac{t^2}{2p}, 0\right) = P(t)$ sa projection orthogonale sur Δ et $Q(x_Q(t), 0) = Q(t)$ le point d'intersection de la normale à Γ en M avec Δ . Avec la condition d'orthogonalité :

$$0 = \overrightarrow{QM} \cdot \gamma'(t) = \left(\frac{t^2}{2p} - x_Q(t) \right) \frac{t}{p} + t$$

et $t \neq 0$ ($M \notin \Delta$), on déduit que $x_Q(t) = p + \frac{t^2}{2p}$ et :

$$PQ = |x_Q(t) - x_P(t)| = p = d(F, \mathcal{D}).$$

(figure ??).

Un exemple de parabole

Considérons par exemple, dans le plan euclidien \mathbb{R}^2 muni de sa base canonique $(\Omega, \vec{e}_1, \vec{e}_2)$ la parabole ayant pour directrice la droite \mathcal{D} d'équation $X + Y = 0$ et pour foyer le point $F(2, 2)$. La droite \mathcal{D} est dirigée par $\vec{v} = (-1, 1)$ et pour $M(X, Y) \in \mathbb{R}^2$ la projection orthogonale $H(X_H, Y_H)$ de M sur \mathcal{D} est définie par :

$$\begin{cases} X_H + Y_H = 0 & (H \in \mathcal{D}) \\ -(X - X_H) + (Y - Y_H) = 0 & (\overrightarrow{HM} \cdot \vec{v} = 0) \end{cases}$$

ou encore :

$$\begin{cases} X_H + Y_H = 0 \\ X_H - Y_H = X - Y \end{cases}$$

ce qui donne $Y_H = -X_H = \frac{Y - X}{2}$.

En particulier, pour $M = F$, cette projection est $K(0, 0) = \Omega$.

La condition $MF = MH$ se traduit alors par :

$$(X - 2)^2 + (Y - 2)^2 = \frac{(X + Y)^2}{2}$$

FIGURE 18.6 – Sous-normale à une parabole

ou encore :

$$X^2 + Y^2 - 2XY - 8(X + Y) + 16 = 0 \quad (18.2)$$

(c'est l'équation de la parabole dans le repère $(\Omega, \vec{e}_1, \vec{e}_2)$).

Sur la figure 18.7, on représente cette parabole avec la construction du point intersection de la perpendiculaire D_H à \mathcal{D} passant par $H(-1, 1)$ et de la médiatrice de $[HF]$.

Le paramètre p de cette parabole est $p = KF = \|\vec{\Omega F}\| = 2\sqrt{2}$, le sommet est le milieu $O(1, 1)$ de $[KF]$ (c'est aussi le point d'intersection de la parabole avec l'axe focal d'équation $Y = X$, ce qui donne $2X^2 - 2X^2 - 16X + 16 = 0$) et dans un repère adapté, une équation est $y^2 = 2px = 4\sqrt{2}x$. Ce repère est (O, \vec{i}, \vec{j}) , où $O(1, 1)$, $\vec{i} = \frac{1}{\sqrt{2}}(\vec{e}_1 + \vec{e}_2)$ et $\vec{j} = \frac{1}{\sqrt{2}}(-\vec{e}_1 + \vec{e}_2)$.

Nous verrons plus loin comment trouver la directrice et le foyer d'une parabole définie par une équation du type 18.2.

Intersection d'une parabole et d'une droite

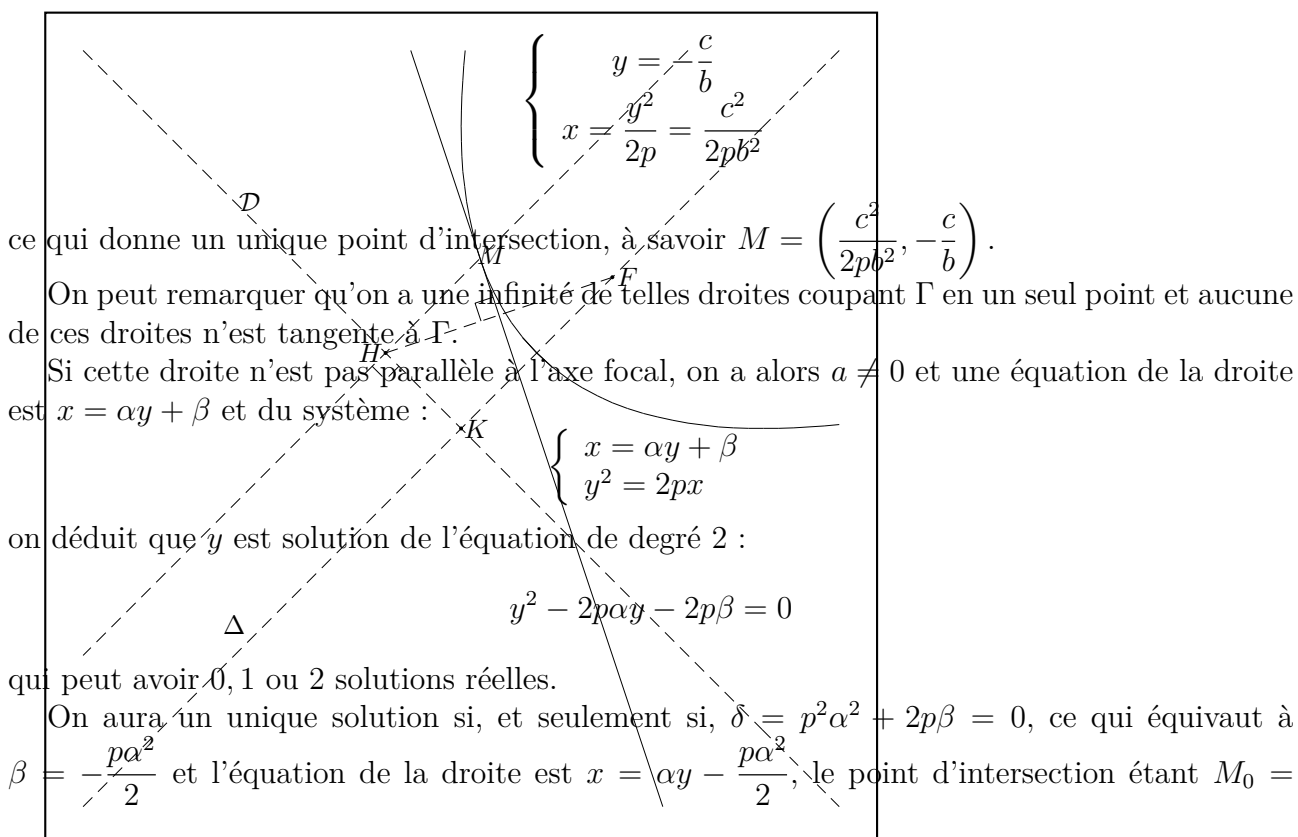
Soit Γ une parabole et $y^2 = 2px$ une équation réduite dans un repère adapté.

Les points d'intersection de cette parabole avec une droite d'équation $ax + by + c = 0$ où $(a, b) \neq (0, 0)$ sont obtenus en résolvant le système de deux équations à deux inconnues suivant :

$$\begin{cases} ax + by + c = 0 \\ y^2 = 2px \end{cases}$$

FIGURE 18.7 – Parabole : $X^2 + Y^2 - 2XY - 8(X + Y) + 16 = 0$

Si la droite est parallèle à l'axe focal Δ (l'axe des abscisses), on a alors $a = 0$, $b \neq 0$ et le système d'équations précédent nous donne :



$(x_0, y_0) = \left(\frac{p\alpha^2}{2}, p\alpha \right)$. La droite a donc pour équation :

$$x = \frac{y_0}{p}y - x_0 = \frac{y_0}{p}(y - y_0) + \frac{y_0^2}{p} - x_0 = \frac{y_0}{p}(y - y_0) + 2x_0 - x_0$$

ou encore $p(x - x_0) - y_0(y - y_0) = 0$ et cette droite est la tangente à Γ en M_0 .

Réciproquement, les tangentes à Γ sont les droites non parallèles à l'axe focal qui coupent Γ en un seul point.

18.2.2 Les coniques à centres, ellipses et hyperboles

On suppose pour ce paragraphe que $e \neq 1$, c'est-à-dire que Γ est une ellipse ou une hyperbole. Dans un repère orthonormé (O, \vec{i}, \vec{j}) on a une équation :

$$(M \in \Gamma) \Leftrightarrow ((1 - e^2)x^2 + y^2 - 2(x_F - e^2x_K)x = e^2x_K^2 - x_F^2) \quad (18.3)$$

Équation réduite des coniques à centre

On choisit l'origine O sur l'axe focal Δ de sorte que $x_F - e^2x_K = 0$, ce qui équivaut à $\overrightarrow{OF} - e^2\overrightarrow{OK} = \vec{0}$ et revient à dire que O est le barycentre de $\{(F, 1), (K, -e^2)\}$ (on a $1 - e^2 \neq 0$).

En désignant par A et A' les points d'intersection de la conique Γ avec son axe focal Δ , on a :

$$x_A = \frac{x_F + ex_K}{1 + e} = ex_K \text{ et } x_{A'} = \frac{x_F - ex_K}{1 - e} = -ex_K$$

c'est-à-dire que O est le milieu de $[AA']$.

En notant $a = x_A$ l'abscisse de A dans ce repère, on a $K\left(\frac{a}{e}, 0\right)$, $F(ea, 0)$ et (18.3) devient :

$$(1 - e^2)x^2 + y^2 = a^2 - a^2e^2$$

ou encore :

$$\frac{x^2}{a^2} + \frac{y^2}{a^2(1 - e^2)} = 1.$$

Avec cette équation, on retrouve le fait que Δ est un axe de symétrie et on constate aussi que le point O , milieu de $[AA']$ est un centre de symétrie et l'axe des y , à savoir la perpendiculaire à Δ passant par O est un axe de symétrie.

Précisément, on déduit de cette équation le résultat suivant.

Théorème 18.5 *Si Γ est une conique d'excentricité $e \neq 1$, alors :*

1. Γ a un unique centre de symétrie qui est le milieu O de $[AA']$, où A est le barycentre de $\{(F, 1), (K, e)\}$ et A' celui de $\{(F, 1), (K, -e)\}$;
2. Γ est aussi la conique de directrice \mathcal{D}' , de foyer F' et d'excentricité e , où \mathcal{D}' [resp. F'] est la symétrique de \mathcal{D} [resp. F] par rapport à O .

On dit que le point O est le centre de la conique et que Γ est une conique à centre.

Exercice 18.2 *Montrer que les paraboles n'ont pas de centre de symétrie.*

Pour $e > 1$, Γ est une hyperbole et en posant $b^2 = a^2(e^2 - 1)$, elle a pour équation réduite dans (O, \vec{i}, \vec{j}) :

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

On dit que a est le demi axe (ou que $2a$ est l'axe) de l'hyperbole.

On peut remarquer que l'axe des x (l'axe focal) coupe l'hyperbole en $A(a, 0)$ et $A'(-a, 0)$ et que l'axe des y ne coupe pas Γ .

On dit que les points A, A' sont les sommets de l'hyperbole.

L'excentricité est $e = \frac{\sqrt{a^2 + b^2}}{a}$, la directrice \mathcal{D} a pour équation $x = x_k = \frac{a}{e} = \frac{a^2}{\sqrt{a^2 + b^2}}$ et le foyer est $F(x_F, 0)$ avec $x_F = ea = \sqrt{a^2 + b^2}$.

Réciproquement une courbe Γ d'équation $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ dans un repère orthonormé est une hyperbole d'excentricité, directrice et foyer définis ci-dessus (il suffit de remonter les calculs).

De $\frac{x^2}{a^2} = 1 + \frac{y^2}{b^2} \geq 1$, on déduit que $x^2 \geq a^2$ et l'hyperbole est strictement contenu dans \mathcal{P} privé de la bande délimité par les droites \mathcal{D} (d'équation $x = x_K = \frac{a}{e}$) et \mathcal{D}' (d'équation $x = -\frac{a}{e}$).

On déduit de cette équation implicite que la tangente à l'hyperbole Γ en $M_0(x_0, y_0)$ a pour équation :

$$\frac{x_0}{a^2}(x - x_0) - \frac{y_0}{b^2}(y - y_0) = 0$$

ce qui peut encore s'écrire compte tenu de $\frac{x_0^2}{a^2} - \frac{y_0^2}{b^2} = 1$:

$$\frac{x_0}{a^2}x - \frac{y_0}{b^2}y = 1.$$

Pour $e < 1$, Γ est une ellipse et en posant $b^2 = a^2(1 - e^2)$, elle a pour équation dans (O, \vec{i}, \vec{j}) :

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

avec $0 < b < a$.

L'excentricité est $e = \frac{\sqrt{a^2 - b^2}}{a}$, la directrice \mathcal{D} a pour équation $x = x_k = \frac{a}{e} = \frac{a^2}{\sqrt{a^2 - b^2}}$ et le foyer est $F(x_F, 0)$ avec $x_F = ea = \sqrt{a^2 - b^2}$.

Réciproquement une courbe Γ d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ avec $0 < b < a$ dans un repère orthonormé est une ellipse d'excentricité, directrice et foyer définis ci-dessus (il suffit de remonter les calculs).

Remarque 18.2 Pour $a = b$, l'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ définit un cercle qui n'est pas une ellipse définie par directrice foyer et excentricité (on verra qu'un cercle peut être vu comme une ellipse d'excentricité nulle et de directrice rejetée à l'infini).

On dit que a est le demi grand axe (ou que $2a$ est le grand axe) et que b est le demi petit axe (ou que $2b$ est le petit axe) de l'ellipse.

On peut remarquer que l'axe des x coupe l'ellipse en $A(a, 0)$ et $A'(-a, 0)$ et que l'axe des y la coupe en $B(0, b)$ et $B'(0, -b)$.

On dit que les points A, A', B, B' sont les sommets de l'ellipse.

Remarque 18.3 En utilisant le théorème de Pythagore, on a :

$$FB^2 = OB^2 + OF^2 = b^2 + e^2 a^2 = a^2.$$

Il en résulte que :

$$FB = FB' = F'B = F'B' = a$$

De $\frac{x^2}{a^2} = 1 - \frac{y^2}{b^2} \leq 1$, on déduit que $x^2 \leq a^2 < \frac{a^2}{e^2}$, soit $-\frac{a}{e} < x < \frac{a}{e}$ et l'ellipse est strictement contenu dans la bande délimitée par les droites \mathcal{D} (d'équation $x = x_K = \frac{a}{e}$) et \mathcal{D}' (d'équation $x = -\frac{a}{e}$).

On déduit de cette équation implicite que la tangente à l'ellipse Γ en $M_0(x_0, y_0)$ a pour équation :

$$\frac{x_0}{a^2}(x - x_0) + \frac{y_0}{b^2}(y - y_0) = 0$$

ce qui peut encore s'écrire compte tenu de $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = 1$:

$$\frac{x_0}{a^2}x + \frac{y_0}{b^2}y = 1.$$

Exercice 18.3 Soit Γ une ellipse d'équation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ dans un repère orthonormé (O, \vec{i}, \vec{j}) , avec $0 < b < a$.

Montrer que le produit des distances des foyers de Γ à une tangente quelconque est constant égal à b^2 (le carré du demi petit axe).

Solution 18.2 On a $F(x_F, 0)$ et $F'(-x_F, 0)$ avec $x_F = ea = \sqrt{a^2 - b^2}$ et la tangente T_0 à Γ en $M_0(x_0, y_0)$ a pour équation :

$$\frac{x_0}{a^2}x + \frac{y_0}{b^2}y = 1.$$

avec $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = 1$.

La distance d'un point M à T_0 est donnée par :

$$d(M, T_0) = \frac{\left| \frac{x_0}{a^2}x + \frac{y_0}{b^2}y - 1 \right|}{\sqrt{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}}}$$

et :

$$\begin{aligned} d(F, T_0) d(F', T_0) &= \frac{\left| \frac{x_0}{a^2}x_F - 1 \right|}{\sqrt{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}}} \frac{\left| \frac{x_0}{a^2}x_F + 1 \right|}{\sqrt{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}}} = \frac{\left| \frac{x_0^2}{a^4}x_F^2 - 1 \right|}{\frac{x_0^2}{a^4} + \frac{y_0^2}{b^4}} \\ &= b^4 \frac{|x_0^2 x_F^2 - a^4|}{b^4 x_0^2 + a^4 y_0^2} = b^4 \frac{|x_0^2 (a^2 - b^2) - a^4|}{b^4 x_0^2 + a^4 y_0^2} \end{aligned}$$

ce qui s'écrit, compte tenu de $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = 1$:

$$\begin{aligned} d(F, T_0) d(F', T_0) &= b^4 \frac{|x_0^2(a^2 - b^2) - a^4|}{b^4 x_0^2 + a^4 b^2 \left(1 - \frac{x_0^2}{a^2}\right)} \\ &= b^2 \frac{|x_0^2(a^2 - b^2) - a^4|}{b^2 x_0^2 + a^4 - a^2 x_0^2} = b^2. \end{aligned}$$

Paramétrisation des coniques à centre

Ces équations implicites de Γ permettent d'obtenir des paramétrisation.

Pour l'hyperbole, en posant $y = b \operatorname{sh}(t)$ avec $t \in \mathbb{R}$ (sh est bijective de \mathbb{R} sur \mathbb{R}), on a $\frac{x^2}{a^2} = 1 + \operatorname{sh}^2(t) = \operatorname{ch}^2(t)$ et $x = \pm a \operatorname{ch}(t)$ où \pm est le signe de x . Réciproquement tout point $(\pm a \operatorname{ch}(t), b \operatorname{sh}(t))$ est sur l'hyperbole. On a donc $\Gamma = \Gamma_1 \cup \Gamma_2$, où Γ_1 et Γ_2 sont les courbes d'équations paramétriques respectives :

$$t \in \mathbb{R} \mapsto \gamma_1(t) = (a \operatorname{ch}(t), b \operatorname{sh}(t))$$

et :

$$t \in \mathbb{R} \mapsto \gamma_2(t) = (-a \operatorname{ch}(t), b \operatorname{sh}(t))$$

Γ_1 et Γ_2 sont les deux branches de l'hyperbole.

De $\gamma_2(-t) = -\gamma_1(t)$, on déduit que Γ_2 est l'image de Γ_1 par la symétrie de centre O .

Ces paramétrisations nous permettent un tracé de Γ . Pour ce faire, il suffit de tracer Γ_1 . L'étude de γ_1 se fait pour $t \geq 0$ puis on complète le graphe obtenu par symétrie par rapport à l'axe Ox . Les fonctions ch et sh sont strictement croissantes, avec $\gamma_1'(0) = b \vec{j}$, on déduit qu'on a une tangente verticale en $A(a, 0)$ et avec $\frac{y_1(t)}{x_1(t)} = \frac{b e^t - e^{-t}}{a e^t + e^{-t}} \xrightarrow{t \rightarrow +\infty} \frac{b}{a}$, on déduit que la droite d'équation $ay - bx = 0$ est asymptote à l'infini.

De même avec $\frac{y_1(t)}{x_1(t)} \xrightarrow{t \rightarrow -\infty} -\frac{b}{a}$, on déduit que la droite d'équation $ay + bx = 0$ est asymptote à l'infini.

Les tracés de Γ_1, Γ_2 et Γ s'en suivent.

Pour $a = b$, les diagonales d'équations $y = x$ et $y = -x$ sont asymptotes et on dit que Γ est une hyperbole équilatère (les asymptotes sont perpendiculaires). Dans ce cas, de $b^2 = a^2(e^2 - 1)$, on déduit que $e = \sqrt{2}$.

Une hyperbole équilatère est donc une conique d'excentricité $\sqrt{2}$.

Une autre paramétrisation peut s'obtenir comme suit.

En posant $y = b \tan(t)$ avec $t \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ (\tan est bijective de $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ sur \mathbb{R}), on a $\frac{x^2}{a^2} = 1 + \tan^2(t) = \frac{1}{\cos^2(t)}$ et $x = \pm \frac{a}{\cos(t)}$. Réciproquement tout point $\left(\pm \frac{a}{\cos(t)}, b \tan(t)\right)$ est sur l'hyperbole. On a donc $\Gamma = \Gamma_1 \cup \Gamma_2$, où Γ_1 et Γ_2 sont les courbes d'équations paramétriques respectives :

$$t \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\mapsto \gamma_1(t) = \left(\frac{a}{\cos(t)}, b \tan(t)\right)$$

et :

$$t \in \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\mapsto \gamma_2(t) = \left(-\frac{a}{\cos(t)}, b \tan(t)\right)$$

En posant $u = \tan\left(\frac{t}{2}\right)$, on a $u \in]-1, 1[$, $\cos(t) = \frac{1-u^2}{1+u^2}$, $\tan(t) = \frac{2u}{1-u^2}$ et les paramétrisations :

$$u \in]-1, 1[\mapsto \left(\pm a \frac{1+u^2}{1-u^2}, b \frac{2u}{1-u^2} \right).$$

Pour l'ellipse, le résultat qui suit nous conduit à une paramétrisation.

Théorème 18.6 *Si x, y sont deux réels tels que $x^2 + y^2 = 1$, il existe alors un unique réel $t \in [-\pi, \pi[$ tel que $x = \cos(t)$ et $y = \sin(t)$.*

Démonstration. Comme $x^2 + y^2 = 1$, x est dans $[-1, 1]$ et il existe un unique réel $\alpha \in [0, \pi]$ tel que $x = \cos(\alpha)$. Avec $y^2 = 1 - x^2 = \sin^2(\alpha)$, on déduit que $y = \pm \sin(\alpha)$, soit $y = \sin(\pm\alpha)$. Avec la parité de la fonction \cos , on peut écrire que $x = \cos(\pm\alpha)$ et on aboutit à $(x, y) = (\cos(t), \sin(t))$ avec $t \in [-\pi, \pi[$ (pour $(x, y) = (\cos(\pi), \sin(\pi)) = (-1, 0)$, on écrit $(x, y) = (\cos(-\pi), \sin(-\pi))$).

Si $t' \in [-\pi, \pi[$ est une autre solution, de $\cos(t) = \cos(t')$, on déduit que $t' = \pm t$. Si $t' = t$, c'est terminé, sinon $t' = -t$ et de $\sin(t) = \sin(t') = -\sin(t)$, on déduit que t vaut 0 ou $-\pi$, 0 étant la seule solution puisque $t' = \pi \notin [-\pi, \pi[$. D'où l'unicité. ■

On en déduit la paramétrisation de l'ellipse :

$$t \in [-\pi, \pi[\mapsto \gamma(t) = (a \cos(t), b \sin(t))$$

Là encore, cette paramétrisation permet un tracé de l'ellipse. L'étude se fait pour $t \in \left[0, \frac{\pi}{2}\right]$ puis on complète par symétrie par rapport aux axes. On a des tangentes verticales en A, A' et des tangentes horizontales en B, B' .

Un exemple d'hyperbole

Considérons dans le plan euclidien \mathbb{R}^2 muni de sa base canonique $(\Omega, \vec{e}_1, \vec{e}_2)$ l'hyperbole ayant pour excentricité $e = 2$, pour directrice la droite \mathcal{D} d'équation $X + Y = 0$ et pour foyer le point $F(2, 2)$. La droite \mathcal{D} est dirigée par $\vec{v} = (-1, 1)$ et pour $M(X, Y) \in \mathbb{R}^2$ on a déjà vu que la projection orthogonale $H(X_H, Y_H)$ de M sur \mathcal{D} est définie par $Y_H = -X_H = \frac{Y - X}{2}$.

En particulier, pour $M = F$, cette projection est $K(0, 0) = \Omega$.

La condition $MF = 2MH$ se traduit alors par :

$$(X - 2)^2 + (Y - 2)^2 = 2(X + Y)^2$$

ou encore :

$$X^2 + Y^2 + 4XY + 4(X + Y) - 8 = 0 \quad (18.4)$$

(c'est l'équation de l'hyperbole dans le repère $(\Omega, \vec{e}_1, \vec{e}_2)$).

Les sommets de cette hyperbole sont les points d'intersection avec l'axe focal d'équation $Y = X$, ce qui donne l'équation $3X^2 + 4X - 4 = 0$ de racines -2 et $\frac{2}{3}$ et les sommets $A\left(\frac{2}{3}, \frac{2}{3}\right)$ et $A'(-2, -2)$.

Le centre est le milieu de $[AA']$, soit $O\left(-\frac{2}{3}, -\frac{2}{3}\right)$.

Le demi axe est $a = OA = \frac{4\sqrt{2}}{3}$ et dans un repère adapté, une équation est $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ où $b = a\sqrt{e^2 - 1} = \frac{4\sqrt{2}}{\sqrt{3}}$. Ce repère est (O, \vec{i}, \vec{j}) , où $O\left(-\frac{2}{3}, -\frac{2}{3}\right)$, $\vec{i} = \frac{3}{4\sqrt{2}}\vec{OA} =$

$\frac{1}{\sqrt{2}}(\vec{e}_1 + \vec{e}_2)$, $\vec{f} = \frac{1}{\sqrt{2}}(-\vec{e}_1 + \vec{e}_2)$ et l'équation est :

$$9x^2 - 3y^2 = 32.$$

(figure 18.8).

FIGURE 18.8 – Hyperbole : $X^2 + Y^2 + 4XY + 4(X + Y) - 8 = 0$

Un exemple d'ellipse

Considérons aussi, dans le plan euclidien \mathbb{R}^2 muni de sa base canonique $(\Omega, \vec{e}_1, \vec{e}_2)$ l'ellipse ayant pour excentricité $e = \frac{1}{2}$, pour directrice la droite \mathcal{D} d'équation $X + Y = 0$ et pour foyer le point $F(2, 2)$. La droite \mathcal{D} est dirigée par $\vec{v} = (-1, 1)$ et pour $M(X, Y) \in \mathbb{R}^2$ la projection orthogonale $H(X_H, Y_H)$ de M sur \mathcal{D} est définie par $Y_H = -X_H = \frac{Y - X}{2}$.

En particulier, pour $M = \Omega$, cette projection est $K(0, 0) = \Omega$.

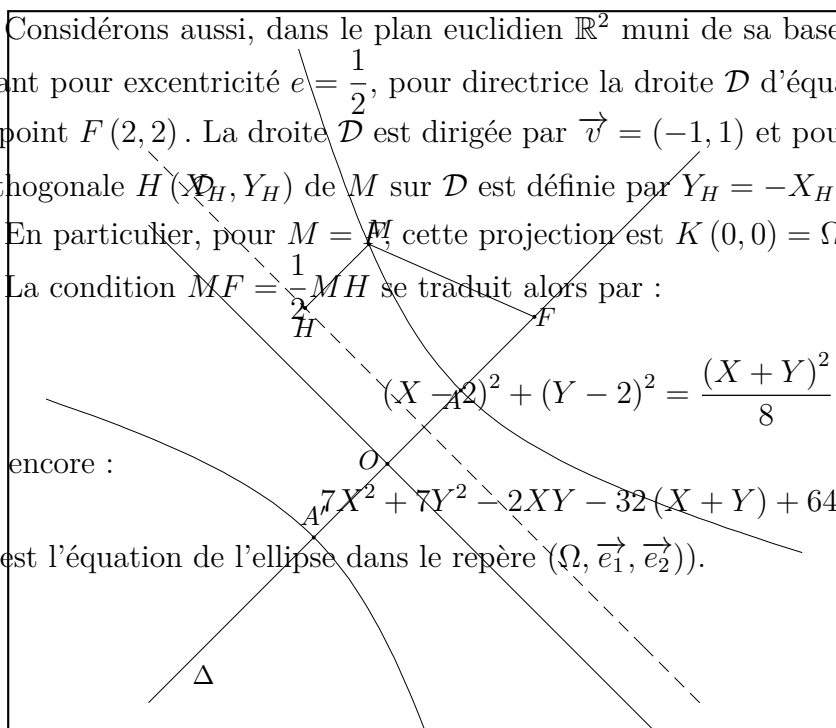
La condition $MF = \frac{1}{2}MH$ se traduit alors par :

$$(X - 2)^2 + (Y - 2)^2 = \frac{(X + Y)^2}{8}$$

ou encore :

$$7X^2 + 7Y^2 - 2XY - 32(X + Y) + 64 = 0 \quad (18.5)$$

(c'est l'équation de l'ellipse dans le repère $(\Omega, \vec{e}_1, \vec{e}_2)$).



Les sommets de cette ellipse sont les points d'intersection de l'ellipse avec l'axe focal d'équation $Y = X$, ce qui donne l'équation $3X^2 - 16X + 16 = 0$ de racines $\frac{4}{3}$ et 4 et les sommets $A(4, 4)$ et $A'\left(\frac{4}{3}, \frac{4}{3}\right)$.

Le centre est le milieu de $[AA']$, soit $O\left(\frac{8}{3}, \frac{8}{3}\right)$.

Le demi axe est $a = OA = \frac{4}{3}\sqrt{2}$ et dans un repère adapté, une équation est $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ où $b = a\sqrt{1 - e^2} = \frac{2\sqrt{2}}{\sqrt{3}}$. Ce repère est (O, \vec{i}, \vec{j}) , où $O\left(\frac{8}{3}, \frac{8}{3}\right)$, $\vec{i} = \frac{1}{OA}\vec{OA} = \frac{1}{\sqrt{2}}(\vec{e}_1 + \vec{e}_2)$, $\vec{j} = \frac{1}{\sqrt{2}}(-\vec{e}_1 + \vec{e}_2)$ et l'équation est :

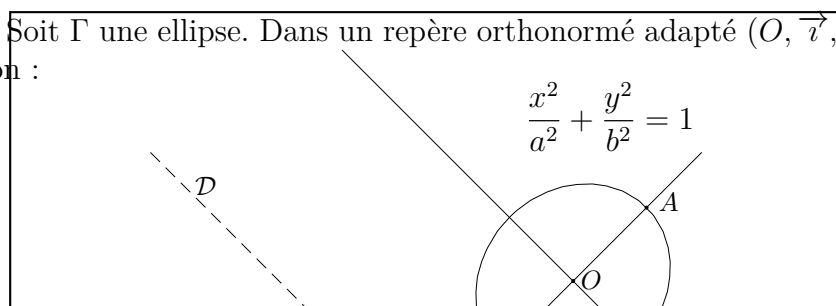
$$9x^2 + 12y^2 = 32.$$

(figure 18.9).

FIGURE 18.9 – $7X^2 + 7Y^2 - 2XY - 32(X + Y) + 64 = 0$

Intersection d'une ellipse et d'une droite

Soit Γ une ellipse. Dans un repère orthonormé adapté (O, \vec{i}, \vec{j}) , cette ellipse a pour équation :



avec $0 < b < a$.

On se donne une droite D d'équation :

$$ux + vy + w = 0$$

avec $(u, v) \neq (0, 0)$.

Un vecteur directeur de D est $\vec{V} = (-v, u)$ et désignant par $M_0(x_0, y_0)$ un point quelconque de D , une paramétrisation de cette droite est :

$$\begin{cases} x = x_0 - \lambda v \\ y = y_0 + \lambda u \end{cases}$$

L'intersection $D \cap \Gamma$ est non vide si, et seulement si, il existe un réel λ tel que :

$$\begin{cases} x = x_0 - \lambda v \\ y = y_0 + \lambda u \\ \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \end{cases}$$

ce qui entraîne que λ est solution de l'équation :

$$b^2(x_0 - \lambda v)^2 + a^2(y_0 + \lambda u)^2 = a^2b^2$$

qui est équivalente à :

$$(a^2u^2 + b^2v^2)\lambda^2 + 2(a^2uy_0 - b^2vx_0)\lambda + (a^2y_0^2 + b^2x_0^2 - a^2b^2) = 0.$$

Cette équation est de degré 2 puisque $a^2u^2 + b^2v^2 \neq 0$ du fait que $a > 0$, $b > 0$ et $(u, v) \neq (0, 0)$. Elle a donc 0, 1 ou 2 solutions réelles.

Le discriminant de cette équation est :

$$\begin{aligned} \delta &= (a^2uy_0 - b^2vx_0)^2 - (a^2u^2 + b^2v^2)(a^2y_0^2 + b^2x_0^2 - a^2b^2) \\ &= a^2b^2(a^2u^2 + b^2v^2 - u^2x_0^2 - 2uvx_0y_0 - v^2y_0^2) \\ &= a^2b^2(a^2u^2 + b^2v^2 - (ux_0 + vy_0)^2) \end{aligned}$$

soit en tenant compte de $ux_0 + vy_0 = -w$ ($M_0 \in D$) :

$$\delta = a^2b^2(a^2u^2 + b^2v^2 - w^2).$$

On en déduit alors que :

- si $a^2u^2 + b^2v^2 < w^2$, alors $\delta < 0$ et D ne coupe pas Γ ;
- si $a^2u^2 + b^2v^2 = w^2$, alors $\delta = 0$ et D coupe Γ en un unique point. Prenant ce point comme origine M_0 de D , on a $M_0 \in D \cap \Gamma$ et :

$$a^2y_0^2 + b^2x_0^2 - a^2b^2 = a^2b^2\left(\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} - 1\right) = 0$$

de sorte que :

$$0 = \delta = (a^2uy_0 - b^2vx_0)^2$$

et :

$$a^2uy_0 - b^2vx_0 = a^2b^2\left(u\frac{y_0}{b^2} - v\frac{x_0}{a^2}\right)$$

ce qui signifie que $\vec{V} = (-v, u)$ est orthogonal au vecteur $\left(\frac{x_0}{a^2}, \frac{y_0}{b^2}\right)$ qui est orthogonal à la tangente à Γ en M_0 . La droite D est donc tangente à Γ .

- si $a^2u^2 + b^2v^2 > w^2$, alors $\delta > 0$ et D coupe Γ en deux points distincts. En prenant pour origine M_0 de D l'un de ces points de contact, on a $\delta = (a^2uy_0 - b^2vx_0)^2 > 0$, donc le produit scalaire de \vec{V} avec le vecteur $\left(\frac{x_0}{a^2}, \frac{y_0}{b^2}\right)$ qui est orthogonal à la tangente à Γ en M_0 n'est pas nul et D n'est pas tangente à Γ en M_0 .

On a donc montré le résultat suivant.

Théorème 18.7 Soit D une droite d'équation $ux + vy + w = 0$ avec $(u, v) \neq (0, 0)$.

- si $a^2u^2 + b^2v^2 < w^2$, alors D ne coupe pas Γ ;
- si $a^2u^2 + b^2v^2 = w^2$, alors D coupe Γ en un unique point M_0 et est tangente à Γ en ce point ;
- si $a^2u^2 + b^2v^2 > w^2$, alors D coupe Γ en deux points distincts et n'est pas tangente à Γ .

Les droites tangentes à une ellipse sont donc celles qui coupent cette ellipse en un unique point (un point double). On peut remarquer que ce résultat est faux pour la parabole.

Les théorèmes d'Appolonius

Soit Γ une ellipse de paramétrisation :

$$t \mapsto \gamma(t) = (a \cos(t), b \sin(t))$$

dans un repère orthonormé adapté (O, \vec{i}, \vec{j}) .

Théorème 18.8 (premier théorème d'Appolonius) Soient $M \in \Gamma$ et $N \in \Gamma$ tel que la tangente à Γ en N soit parallèle à (OM) . L'aire du triangle OMN est alors constante égale à $\frac{ab}{2}$ et $OM^2 + ON^2 = a^2 + b^2$.

Démonstration. En notant $M = \gamma(t)$, dire que la tangente à Γ en $N = \gamma(t')$ est parallèle à OM équivaut à dire que :

$$\begin{aligned} \det(\gamma(t), \gamma'(t')) &= \begin{vmatrix} a \cos(t) & -a \sin(t') \\ b \sin(t) & b \cos(t') \end{vmatrix} \\ &= ab(\cos(t) \cos(t') + \sin(t) \sin(t')) \\ &= ab \cos(t - t') = 0 \end{aligned}$$

ce qui est encore équivalent à $t' = t \pm \frac{\pi}{2}$ modulo 2π et donne deux possibilités pour N .

L'aire du triangle OMN est alors :

$$\begin{aligned} \mathcal{A} &= \frac{1}{2} |\det(\gamma(t), \gamma(t'))| = \frac{1}{2} \left| \det \begin{pmatrix} a \cos(t) & a \cos(t') \\ b \sin(t) & b \sin(t') \end{pmatrix} \right| \\ &= \frac{1}{2} ab |\cos(t) \sin(t') - \sin(t) \cos(t')| \\ &= \frac{1}{2} ab |\sin(t' - t)| = \frac{1}{2} ab. \end{aligned}$$

On a aussi :

$$\begin{aligned} OM^2 + ON^2 &= a^2 (\cos^2(\theta) + \cos^2(\theta')) + b^2 (\sin^2(\theta) + \sin^2(\theta')) \\ &= a^2 (\cos^2(\theta) + \sin^2(\theta)) + b^2 (\sin^2(\theta) + \cos^2(\theta)) \\ &= a^2 + b^2. \end{aligned}$$

■

Théorème 18.9 (deuxième théorème d'Appolonius) *En gardant les notations du théorème précédent, on désigne par I la projection de M sur l'axe focal (l'axe des abscisses) et par J celle de N . On a alors :*

$$OI^2 + OJ^2 = a^2.$$

Démonstration. On a :

$$\begin{aligned} OI^2 + OJ^2 &= a^2 (\cos^2(\theta) + \cos^2(\theta')) \\ &= a^2 (\cos^2(\theta) + \sin^2(\theta)) = a^2. \end{aligned}$$

■

Projection orthogonale d'un cercle de l'espace sur un plan

Les ellipses peuvent aussi être vues comme les projections orthogonales d'un cercle de l'espace euclidien sur un plan.

Théorème 18.10 *Soient \mathcal{P} et \mathcal{P}' deux plans non orthogonaux de l'espace et \mathcal{C} un cercle inclus dans \mathcal{P} . La projection orthogonale de \mathcal{C} sur \mathcal{P}' est une ellipse ou un cercle.*

Si les plans \mathcal{P} et \mathcal{P}' sont orthogonaux, cette projection est alors un segment que l'on peut voir comme une ellipse écrasée.

18.2.3 Construction des tangentes à une conique

Un procédé de construction de la tangente à une conique en point M qui n'est pas sur l'axe focal est donné par le résultat suivant.

Théorème 18.11 *Soient Γ une conique et M un point de Γ qui n'est pas sur l'axe focal Δ . La tangente à Γ en M coupe la directrice \mathcal{D} en un point T tel que le triangle MFT soit rectangle en F (figure 18.10).*

Démonstration. Soit $\gamma : t \mapsto M(t)$ une paramétrisation régulière de Γ dans un repère orthonormé (F, \vec{i}, \vec{j}) , où $\vec{i} = \frac{1}{FK} \overrightarrow{FK}$.

En dérivant l'égalité $\|\overrightarrow{MF}\| = e \|\overrightarrow{MH}\|$, on a :

$$\frac{1}{\|\overrightarrow{MF}\|} \overrightarrow{MF} \cdot \frac{d}{dt} \overrightarrow{MF} = \frac{e}{\|\overrightarrow{MH}\|} \overrightarrow{MH} \cdot \frac{d}{dt} \overrightarrow{MH}.$$

avec $\frac{1}{\|\overrightarrow{MH}\|} \overrightarrow{MH} = \pm \vec{i}$ puisque ces deux vecteurs sont colinéaires et de norme 1 et en notant $\vec{u}(t) = \frac{1}{\|\overrightarrow{MF}\|} \overrightarrow{MF}$, on a :

$$\vec{u}(t) \cdot \frac{d}{dt} \overrightarrow{MF} = \pm e \vec{i} \cdot \frac{d}{dt} \overrightarrow{MH},$$

avec :

$$\vec{i} \cdot \frac{d}{dt} \overrightarrow{MH} = \vec{i} \cdot \frac{d}{dt} \overrightarrow{MF} + \vec{i} \cdot \frac{d}{dt} \overrightarrow{FH}$$

FIGURE 18.10 – Tangente en un point d'une conique

et :

$$\vec{v} \cdot \frac{d}{dt} \overrightarrow{FH} = \frac{d}{dt} (\vec{v} \cdot \overrightarrow{FH}) = \frac{d}{dt} (\vec{v} \cdot (\overrightarrow{FK} + \overrightarrow{KH})) = \frac{d}{dt} (\vec{v} \cdot \overrightarrow{FK}) = 0$$

du fait que \overrightarrow{KH} est orthogonal à \vec{v} et $\vec{v} \cdot \overrightarrow{FK} = \|\overrightarrow{FK}\|$ ne dépend pas de t . On a donc :

$$u(t) \cdot \frac{d}{dt} \overrightarrow{MF} = \pm e \vec{v} \cdot \frac{d}{dt} \overrightarrow{MF}.$$

Si T est le point d'intersection de la tangente à Γ en M avec la directrice \mathcal{D} , on a $\overrightarrow{MT} = \lambda \frac{d}{dt} \overrightarrow{MF}$ et :

$$u(t) \cdot \overrightarrow{MT} = \lambda u(t) \cdot \frac{d}{dt} \overrightarrow{MF} = \lambda e (\pm \vec{v}) \cdot \frac{d}{dt} \overrightarrow{MF} = e (\pm \vec{v}) \cdot \overrightarrow{MT}$$

ce qui entraîne :

$$\begin{aligned} \overrightarrow{FM} \cdot \overrightarrow{FT} &= \overrightarrow{FM} \cdot (\overrightarrow{FM} + \overrightarrow{MT}) = \|\overrightarrow{MF}\|^2 - \|\overrightarrow{MF}\| u(t) \cdot \overrightarrow{MT} \\ &= \|\overrightarrow{MF}\| (\|\overrightarrow{MF}\| - e (\pm \vec{v}) \cdot \overrightarrow{MT}) \end{aligned}$$

avec :

$$\Delta \quad \vec{v} \cdot \overrightarrow{MT} = \vec{v} \cdot \overrightarrow{MH} + \vec{v} \cdot \overrightarrow{HT} = \vec{v} \cdot \overrightarrow{MH} = \pm \|\overrightarrow{MH}\|,$$

ce qui donne en définitive :

$$\overrightarrow{FM} \cdot \overrightarrow{FT} = \|\overrightarrow{MF}\| (\|\overrightarrow{MF}\| - e \|\overrightarrow{MH}\|) = 0,$$

c'est-à-dire que le triangle MFT est rectangle en F . ■

18.3 Définition bifocale des coniques à centre

On a vu qu'une conique à centre a deux foyers et deux directrices (théorème 18.5).

De ce résultat nous allons déduire une autre caractérisation métrique des coniques à centre.

Théorème 18.12 *Soit Γ une ellipse de directrice \mathcal{D} , de foyer F et d'excentricité $e < 1$. En désignant par F' le deuxième foyer de Γ (le symétrique de F par rapport au centre O de Γ) et par $2a$ le grand axe, on a :*

$$\Gamma \subset \{M \in \mathcal{P} \mid MF + MF' = 2a\}$$

avec $2a > FF'$.

Démonstration. On se place dans un repère orthonormé (O, \vec{i}, \vec{j}) , où O est le centre de Γ et $\vec{i} = \frac{1}{OA} \overrightarrow{OA}$. Dans ce repère, en notant $a = OA$, on a $K\left(\frac{a}{e}, 0\right)$, $F(ea, 0)$, $F'(-ea, 0)$ et pour tout point $M(x, y)$ de l'ellipse, on a :

$$MF^2 = (x - ea)^2 + y^2 = e^2 MH^2 = e^2 \left(x - \frac{a}{e}\right)^2$$

soit :

$$MF = e \left|x - \frac{a}{e}\right|$$

et :

$$(MF')^2 = (x + ea)^2 + y^2 = e^2 (MH')^2 = e^2 \left(x + \frac{a}{e}\right)^2$$

soit :

$$MF' = e \left|x + \frac{a}{e}\right|$$

Sachant que $x^2 \leq a^2 < \frac{a^2}{e^2}$ (dédit de $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ et $e < 1$), on déduit que $-\frac{a}{e} < x < \frac{a}{e}$ et :

$$MF + MF' = e \left(\frac{a}{e} - x\right) + e \left(x + \frac{a}{e}\right) = 2a.$$

De plus $FF' = 2ea < 2a$ puisque $e < 1$. ■

On peut aussi remarquer que l'encadrement $-\frac{a}{e} < x < \frac{a}{e}$ pour $M(x, y) \in \Gamma$ nous dit que l'ellipse Γ est strictement contenue dans la bande verticale limitée par les directrices \mathcal{D} et \mathcal{D}' (d'équations respectives $x = \frac{a}{e}$ et $x = -\frac{a}{e}$). Il en résulte que tout point M de l'ellipse est à l'intérieur du segment $[HH']$ et en conséquence :

$$MF + MF' = e(MH + MH') = eHH' = eKK' = 2a.$$

Réciproquement, on a le résultat suivant.

Théorème 18.13 *Si F, F' sont deux points distincts de \mathcal{P} et a un réel tel que $2a > FF'$, alors l'ensemble :*

$$\Gamma = \{M \in \mathcal{P} \mid MF + MF' = 2a\}$$

est une ellipse de foyers F, F' et de grand axe $2a$.

Démonstration. On note O le milieu de $[FF']$ et on se place dans un repère orthonormé (O, \vec{i}, \vec{j}) , où $\vec{i} = \frac{1}{OF} \overrightarrow{OF}$. Les calculs précédents nous conduisent à poser $x_F = OF = ea$, soit $e = \frac{OF}{a} = \frac{FF'}{2a} < 1$ et à définir la droite \mathcal{D} d'équation $x = \frac{a}{e}$.

De $MF + MF' = 2a$, on déduit que :

$$MF^2 - (MF')^2 = (MF + MF')(MF - MF') = 2a(MF - MF')$$

avec :

$$MF^2 = (x - ea)^2 + y^2 \text{ et } (MF')^2 = (x + ea)^2 + y^2$$

ce qui donne :

$$2a(MF - MF') = -2eax$$

et de :

$$\begin{cases} MF + MF' = 2a \\ MF - MF' = -2ex \end{cases}$$

on déduit que :

$$MF = a - ex > 0.$$

Le projeté orthogonal de $M \in \Gamma$ sur \mathcal{D} étant $H\left(\frac{a}{e}, y\right)$, on a :

$$MH = \left| \frac{a}{e} - x \right| = \frac{1}{e}(a - ex)$$

et $MF = eMH$. Donc Γ est contenu dans l'ellipse de foyers F, F' et de grand axe $2a$.

La réciproque a été établie avec le théorème précédent.

On peut aussi travailler analytiquement toujours dans le même repère orthonormé (O, \vec{i}, \vec{j}) .

La condition $MF + MF' = 2a$ équivaut à $MF^2 + MF'^2 + 2MF \cdot MF' = 4a^2$, soit à :

$$(x - ea)^2 + y^2 + (x + ea)^2 + y^2 + 2MF \cdot MF' = 4a^2$$

ou encore à :

$$x^2 + y^2 + e^2a^2 + MF \cdot MF' = 2a^2$$

ce qui peut aussi s'écrire :

$$MF \cdot MF' = 2a^2 - x^2 - y^2 - e^2a^2$$

On a donc :

$$\begin{aligned} (M \in \Gamma) &\Rightarrow (MF^2 \cdot MF'^2 = (2a^2 - x^2 - y^2 - e^2a^2)^2) \\ &\Rightarrow (((x - ea)^2 + y^2)((x + ea)^2 + y^2) = (2a^2 - x^2 - y^2 - e^2a^2)^2) \\ &\Rightarrow ((1 - e^2)x^2 + y^2 = a^2(1 - e^2)) \end{aligned}$$

avec $0 < e < 1$ et Γ est contenu dans l'ellipse de foyers F, F' et de grand axe $2a$.

Réciproquement si M est un point de l'ellipse de foyers F, F' et de grand axe $2a$, ses coordonnées vérifient l'équation $x^2 + \frac{y^2}{1 - e^2} = a^2$, ce qui équivaut à :

$$MF^2 \cdot MF'^2 = (2a^2 - x^2 - y^2 - e^2a^2)^2$$

et avec $x^2 \leq a^2$, $\frac{y^2}{1-e^2} \leq a^2$, on déduit que :

$$2a^2 - x^2 - y^2 - e^2a^2 = (a^2 - x^2) + (1 - e^2) \left(a^2 - \frac{y^2}{1-e^2} \right) \geq 0$$

et $MF \cdot MF' = 2a^2 - x^2 - y^2 - e^2a^2$, ce qui équivaut à $MF + MF' = 2a$. ■

Remarque 18.4 Dans le cas où les foyers F et F' sont confondus, on obtient le cercle d'équation $MF = a$ que l'on peut voir comme une ellipse d'excentricité nulle et de directrice rejetée à l'infini.

Remarque 18.5 Si $M \in \mathcal{P}$ est tel que $MF + MF' = 2a$ où $a > 0$ est donné, en utilisant l'inégalité triangulaire, on déduit que :

$$FF' \leq FM + MF' = 2a$$

l'inégalité étant stricte si $M \notin [FF']$, en conséquence l'ensemble $\{M \in \mathcal{P} \mid MF + MF' = 2a\}$ est vide si $2a < FF'$ et pour $2a = FF'$ c'est le segment $[FF']$.

Pour ce qui est des hyperboles, on a des résultats similaires.

Théorème 18.14 Soit Γ une hyperbole de directrice \mathcal{D} , de foyer F et d'excentricité $e > 1$. En désignant par F' le deuxième foyer de Γ (le symétrique de F par rapport au centre O de Γ) et par $2a$ le grand axe, on a :

$$\Gamma \subset \{M \in \mathcal{P} \mid |MF - MF'| = 2a\}$$

avec $2a < FF'$.

Démonstration. On se place dans un repère orthonormé (O, \vec{i}, \vec{j}) , où O est le centre de Γ et $\vec{i} = \frac{1}{OA} \overrightarrow{OA}$. Dans ce repère, en notant $a = OA$, on a $K\left(\frac{a}{e}, 0\right)$, $F(ea, 0)$ et $F'(-ea, 0)$ et pour tout point $M(x, y)$ de l'hyperbole, on a :

$$MF^2 = (x - ea)^2 + y^2 = e^2 MH^2 = e^2 \left(x - \frac{a}{e}\right)^2$$

soit :

$$MF = e \left| x - \frac{a}{e} \right|$$

et :

$$(MF')^2 = (x + ea)^2 + y^2 = e^2 (MH')^2 = e^2 \left(x + \frac{a}{e}\right)^2$$

soit :

$$MF' = e \left| x + \frac{a}{e} \right|$$

Sachant que $x^2 \geq a^2 > \frac{a^2}{e^2}$ (dédit de $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ et $e > 1$), on déduit que $x < -\frac{a}{e}$ ou $x > \frac{a}{e}$ et :

$$MF - MF' = \begin{cases} e \left(\frac{a}{e} - x\right) + e \left(x + \frac{a}{e}\right) = 2a \\ \text{ou} \\ e \left(x - \frac{a}{e}\right) - e \left(x + \frac{a}{e}\right) = -2a \end{cases}.$$

soit $|MF - MF'| = 2a$

De plus $FF' = 2ea > 2a$ puisque $e > 1$. ■

Théorème 18.15 Si F, F' sont deux points distincts de \mathcal{P} et a un réel tel que $0 < 2a < FF'$, alors l'ensemble :

$$\Gamma = \{M \in \mathcal{P} \mid |MF - MF'| = 2a\}$$

est une hyperbole de foyers F, F' et de grand axe $2a$.

Démonstration. Démonstration analogue à celle concernant l'ellipse. ■

Remarque 18.6 Si $M \in \mathcal{P}$ est tel que $|MF - MF'| = 2a$ où $a > 0$ est donné, en utilisant l'inégalité triangulaire, on déduit que :

$$2a = |MF - MF'| \leq FF'$$

l'inégalité étant stricte si $M \notin [FF']$, en conséquence l'ensemble $\{M \in \mathcal{P} \mid |MF - MF'| = 2a\}$ est vide si $2a > FF'$ et pour $2a = FF'$, on a :

$$|MF - MF'| = 2a = FF' \Leftrightarrow \begin{cases} MF - MF' = FF' \\ \text{ou} \\ MF' - MF = FF' \end{cases}$$

ce qui équivaut à dire que Γ est la droite (FF') privée du segment ouvert $]FF'[,$

En utilisant la définition bi-focale des coniques à centres, on a les résultats suivants sur les tangentes.

Théorème 18.16 Soient Γ une ellipse de foyers F, F' et M un point de Γ . La tangente à Γ en M est la bissectrice extérieure issue de M du triangle MFF' .

Démonstration. Soit $M : t \mapsto M(t)$ une paramétrisation régulière de Γ . En dérivant l'égalité $\|\overrightarrow{MF}\| + \|\overrightarrow{MF'}\| = 2a$, on a :

$$\frac{1}{\|\overrightarrow{MF}\|} \overrightarrow{MF} \cdot \frac{d}{dt} \overrightarrow{MF} + \frac{1}{\|\overrightarrow{MF'}\|} \overrightarrow{MF'} \cdot \frac{d}{dt} \overrightarrow{MF'} = 0.$$

En remarquant que :

$$\frac{d}{dt} \overrightarrow{MF'} = \frac{d}{dt} \overrightarrow{MF} + \frac{d}{dt} \overrightarrow{FF'} = \frac{d}{dt} \overrightarrow{MF}$$

et en posant $\overrightarrow{u}(t) = \frac{1}{\|\overrightarrow{MF}\|} \overrightarrow{MF}$ et $\overrightarrow{v}(t) = \frac{1}{\|\overrightarrow{MF'}\|} \overrightarrow{MF'}$ on a :

$$\left(\overrightarrow{u}(t) + \overrightarrow{v}(t) \right) \cdot \frac{d}{dt} \overrightarrow{MF} = 0$$

ce qui signifie que le vecteur tangent $\frac{d}{dt} \overrightarrow{MF}$ est orthogonal au vecteur $\overrightarrow{u}(t) + \overrightarrow{v}(t)$ qui dirige la bissectrice intérieure issue de M du triangle MFF' , encore équivalent à dire que la tangente à Γ en M est la bissectrice extérieure issue de M du triangle MFF' . ■

Une démonstration analogue donne le résultat suivant pour l'hyperbole.

Théorème 18.17 Soient Γ une hyperbole de foyers F, F' et M un point de Γ . La tangente à Γ en M est la bissectrice intérieure issue de M du triangle MFF' .

18.4 Lieu orthoptique d'une conique

Étant donnée une conique Γ , on s'intéresse au lieu des points M du plan euclidien \mathcal{P} d'où l'on peut mener deux tangentes à Γ qui sont orthogonales.

18.4.1 Lieu orthoptique d'une ellipse

Soit Γ une ellipse dans le plan euclidien \mathcal{P} d'équation :

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \quad (18.6)$$

dans un repère orthonormé (O, \vec{i}, \vec{j}) , où $0 < b < a$.

On rappelle que la tangente à Γ en $M_1(x_1, y_1)$ est la droite d'équation :

$$\frac{x_1}{a^2}x + \frac{y_1}{b^2}y = 1.$$

De l'équation cartésienne (18.6), on déduit la paramétrisation :

$$\gamma : t \in \mathbb{R} \mapsto (a \cos(t), b \sin(t))$$

et la tangente à Γ en $\gamma(t)$ est dirigée par $\gamma'(t) = (-a \sin(t), b \cos(t))$. Une équation de cette tangente est donc donnée par :

$$\begin{aligned} \begin{vmatrix} x - a \cos(t) & -a \sin(t) \\ y - b \sin(t) & b \cos(t) \end{vmatrix} &= b \cos(t) (x - a \cos(t)) + a \sin(t) (y - b \sin(t)) \\ &= b \cos(t) x + a \sin(t) y - ab = 0 \end{aligned}$$

Lemme 18.3 Soit $M_0(x_0, y_0) \in \mathcal{P}$.

1. Si $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} < 1$ (i. e. M_0 est extérieur à Γ), il ne passe alors aucune tangente à Γ par M_0 ;
2. si $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = 1$ (i. e. M_0 sur Γ), il passe alors une seule tangente à Γ par M_0 ;
3. si $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} > 1$ (i. e. M_0 est intérieur à Γ), il passe alors exactement deux tangentes à Γ par M_0 .

Démonstration. Une droite D_0 passant par M_0 a une équation de la forme :

$$u(x - x_0) + v(y - y_0) = 0$$

où $(u, v) \neq (0, 0)$ et elle est tangente à Γ si, et seulement si :

$$a^2 u^2 + b^2 v^2 = (ux_0 + vy_0)^2$$

ce qui est encore équivalent à :

$$(a^2 - x_0^2) u^2 - 2x_0 y_0 uv + (b^2 - y_0^2) v^2 = 0 \quad (18.7)$$

qui signifie que (u, v) est dans le cône isotrope de la forme quadratique q définie par :

$$q(X, Y) = (a^2 - x_0^2) X^2 - 2x_0 y_0 XY + (b^2 - y_0^2) Y^2.$$

Le discriminant de cette forme quadratique est :

$$\begin{aligned}\delta &= \begin{vmatrix} a^2 - x_0^2 & -x_0 y_0 \\ -x_0 y_0 & b^2 - y_0^2 \end{vmatrix} = (a^2 - x_0^2)(b^2 - y_0^2) - x_0^2 y_0^2 \\ &= -a^2 b^2 \left(\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} - 1 \right) = -\delta'\end{aligned}$$

(δ' est le discriminant des équations de degré au plus égal à 2, $(a^2 - x_0^2)t^2 - 2x_0 y_0 t + (b^2 - y_0^2)$ et $(a^2 - x_0^2) - 2x_0 y_0 t + (b^2 - y_0^2)t^2$).

Pour $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} < 1$, on a $\delta > 0$, donc $(a^2 - x_0^2)(b^2 - y_0^2) \neq 0$ et les équations de degré 2 $(a^2 - x_0^2)t^2 - 2x_0 y_0 t + (b^2 - y_0^2)$ et $(a^2 - x_0^2) - 2x_0 y_0 t + (b^2 - y_0^2)t^2$ n'ont pas de racine réelle (puisque $\delta' < 0$), ce qui entraîne que le cône isotrope de q est réduit à $\{(0, 0)\}$ et il ne passe pas de tangente à Γ par M_0 .

Pour $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = 1$, on a $\delta = \delta' = 0$, donc $(a^2 - x_0^2)(b^2 - y_0^2) \neq 0$ et les équations de degré 2 $(a^2 - x_0^2)t^2 - 2x_0 y_0 t + (b^2 - y_0^2)$ et $(a^2 - x_0^2) - 2x_0 y_0 t + (b^2 - y_0^2)t^2$ ont une unique racine réelle, ce qui entraîne que le cône isotrope de q est une droite vectorielle et il passe une seule tangente à Γ par M_0 .

Pour $\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} > 1$, on a $\delta < 0$.

Si $(x_0^2, y_0^2) = (a^2, b^2)$, l'équation (18.7) devient :

$$2x_0 y_0 uv = 0$$

et $u = 0$ ou $v = 0$, de sorte que D_0 est une droite passant par $(\pm a, \pm b)$ parallèle à l'un des axes. Cette droite et sa perpendiculaire en M_0 sont alors tangentes à Γ (par exemple pour $M_0 = (a, b)$, la tangente à Γ en $A(a, 0)$ est la droite d'équation $x = a$ et la tangente en $B(0, b)$ est la droite $y = b$).

Si $(x_0^2, y_0^2) \neq (a^2, b^2)$, alors l'une des équations de degré 2 $(a^2 - x_0^2)t^2 - 2x_0 y_0 t + (b^2 - y_0^2)$ ou $(a^2 - x_0^2) - 2x_0 y_0 t + (b^2 - y_0^2)t^2$ ($\delta' > 0$) a deux racines réelles distinctes et le cône isotrope de q est la réunion de deux droites vectorielles distinctes. Il passe donc exactement deux tangentes à Γ par M_0 . ■

Remarque 18.7 On peut aussi utiliser la signature de q dans la démonstration précédente.

- Si $\text{sgn}(q) = (2, 0)$ ou $(0, 2)$, son discriminant δ est strictement positif et la forme q est définie (positive ou négative), donc son cône isotrope est réduit à $\{(0, 0)\}$.
- Si $\text{sgn}(q) = (1, 0)$ ou $(0, 1)$, son discriminant est nul, donc q se réduit à $q(X) = \ell_1^2(X)$ et son cône isotrope est la droite d'équation $\ell_1(X) = 0$.
- Si $\text{sgn}(q) = (1, 1)$, son discriminant est strictement négatif, donc q se réduit à $q(X) = \ell_1^2(X) - \ell_2^2(X)$ et son cône isotrope est la réunion des deux droites distinctes d'équations respectives $\ell_1(X) - \ell_2(X) = 0$ et $\ell_1(X) + \ell_2(X) = 0$.

Théorème 18.18 Le lieu des points M du plan euclidien \mathcal{P} d'où l'on peut mener deux tangentes à l'ellipse Γ qui sont orthogonales est le cercle d'équation :

$$x^2 + y^2 = a^2 + b^2.$$

(figure 18.11).

FIGURE 18.11 – Cercle orthoptique à une ellipse

Démonstration. Notons Λ ce lieu orthoptique.

Si $M_0(x_0, y_0) \in \Lambda$, il passe alors par M_0 exactement deux tangentes à Γ . Ces tangentes T_1 et T_2 ont pour équation :

$$u_k(x - x_0) + v_k(y - y_0) = 0 \quad (k = 1, 2)$$

où (u_1, v_1) et (u_2, v_2) sont deux solutions linéairement indépendantes de l'équation :

$$(a^2 - x_0^2)u^2 - 2x_0y_0uv + (b^2 - y_0^2)v^2 = 0$$

et dire qu'elles sont orthogonales signifie que :

$$u_1u_2 + v_1v_2 = 0 \quad (18.8)$$

(le vecteur (u_k, v_k) est orthogonal à T_k pour $k = 1, 2$).

Supposons d'abord $a^2 \neq x_0^2$. Si $v_k = 0$, on a alors $(a^2 - x_0^2)u_k^2 = 0$ et $u_k = 0$, ce qui est impossible. Donc $v_k \neq 0$ pour $k = 1, 2$ et $m_k = \frac{u_k}{v_k}$ sont les deux solutions réelles de :

$$(a^2 - x_0^2)t^2 - 2x_0y_0t + (b^2 - y_0^2) = 0$$

et le produit de ces racines d'une équation de degré 2 est :

$$m_1m_2 = \frac{b^2 - y_0^2}{a^2 - x_0^2}$$

mais en divisant (18.8) par $v_1 v_2$, on a :

$$m_1 m_2 = \frac{u_1}{v_1} \frac{u_2}{v_2} = -1$$

et $\frac{b^2 - y_0^2}{a^2 - x_0^2} = -1$, ce qui équivaut à $x_0^2 + y_0^2 = a^2 + b^2$.

Si $a^2 = x_0^2$ et $b^2 \neq y_0^2$, (u_1, v_1) et (u_2, v_2) sont deux solutions linéairement indépendantes de l'équation :

$$(-2x_0 y_0 u + (b^2 - y_0^2) v) v = 0$$

et $u_k \neq 0$ pour $k = 1, 2$. Avec $u_1 u_2 + v_1 v_2 = 0$, on déduit que $v_k \neq 0$ pour $k = 1, 2$ et (u_1, v_1) et (u_2, v_2) sont solutions de :

$$-2x_0 y_0 u + (b^2 - y_0^2) v = 0$$

donc sur une même droite, ce qui n'est pas possible. On a donc $b^2 = y_0^2$ pour $a^2 = x_0^2$ et encore $x_0^2 + y_0^2 = a^2 + b^2$.

On donc montré que Λ est contenu dans le cercle d'équation $x^2 + y^2 = a^2 + b^2$.

Réciproquement soit $M_0(x_0, y_0)$ sur le cercle d'équation $x^2 + y^2 = a^2 + b^2$. On a alors :

$$\frac{x_0^2}{a^2} + \frac{y_0^2}{b^2} = \frac{a^2 + b^2 - y_0^2}{a^2} + \frac{y_0^2}{b^2} = \frac{a^2 + b^2}{a^2} + y_0^2 \left(\frac{1}{b^2} - \frac{1}{a^2} \right) > 1$$

et il passe par M_0 exactement deux tangentes T_1 et T_2 à Γ .

Si $x_0^2 = a^2$, on a alors $y_0 = b^2$, soit $M_0(\pm a, \pm b)$ (ce sont les sommets d'un rectangle) et ces deux tangentes sont l'une parallèle à l'axe Ox et l'autre parallèle à l'axe Oy , donc perpendiculaires. Par exemple pour $M_0(a, b)$, T_1 est la tangente à Γ en $M_1(0, b)$ d'équation $\frac{x_1}{a^2}x + \frac{y_1}{b^2}y = 1$, soit $y = b$ et T_2 est la tangente à Γ en $M_1(a, 0)$ d'équation $\frac{x_1}{a^2}x + \frac{y_1}{b^2}y = 1$, soit $\frac{a^2}{x} = a$.

Si $x_0^2 \neq a^2$, alors l'équation $(a^2 - x_0^2)t^2 - 2x_0 y_0 t + (b^2 - y_0^2) = 0$ a deux racines réelles distinctes m_1 et m_2 qui sont les pentes de ces tangentes et la relation $m_1 m_2 = \frac{b^2 - y_0^2}{a^2 - x_0^2} = -1$ nous dit que ces tangentes sont orthogonales. ■

18.4.2 Lieu orthoptique d'une hyperbole

Soit Γ une hyperbole dans le plan euclidien \mathcal{P} d'équation :

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \quad (18.9)$$

dans un repère orthonormé (O, \vec{i}, \vec{j}) , où $0 < b < a$.

Théorème 18.19 *Le lieu des points M du plan euclidien \mathcal{P} d'où l'on peut mener deux tangentes à l'hyperbole Γ qui sont orthogonales est le cercle d'équation :*

$$x^2 + y^2 = a^2 - b^2.$$

18.4.3 Lieu orthoptique d'une parabole

Soit Γ une parabole et $y^2 = 2px$ une équation réduite dans un repère adapté.

Théorème 18.20 *Le lieu des points M du plan euclidien \mathcal{P} d'où l'on peut mener deux tangentes à la parabole Γ qui sont orthogonales est la directrice \mathcal{D} d'équation $x = -\frac{p}{2}$.*

18.5 Cocyclicité de 4 points sur une conique

18.5.1 Cocyclicité de 4 points sur une parabole

Soit Γ une parabole et $y^2 = 2px$ une équation réduite dans un repère adapté.

Dire que les quatre points $M_k(x_k, y_k)$ de Γ sont cocycliques équivaut à dire qu'il existe un point $M_0(x_0, y_0)$ de \mathcal{P} et un réel $R > 0$ tels que :

$$\begin{cases} y_k^2 = 2px_k \\ (x_k - x_0)^2 + (y_k - y_0)^2 = R^2 \end{cases}$$

et les 4 réels y_k sont nécessairement racines du polynôme de degré 4 :

$$Q(t) = \left(\frac{1}{2p} t^2 - x_0 \right)^2 + (t - y_0)^2 - R^2$$

soit de :

$$P(t) = t^4 + 4p(p - x_0)t^2 - 8p^2 y_0 t + 4p^2(x_0^2 + y_0^2 - R^2).$$

On a donc :

$$\begin{aligned} P(t) &= t^4 + 4p(p - x_0)t^2 - 8p^2 y_0 t + 4p^2(x_0^2 + y_0^2 - R^2) \\ &= \prod_{k=1}^4 (t - y_k) = t^4 - \sigma_1 t^3 + \sigma_2 t^2 - \sigma_3 t + \sigma_4 \end{aligned}$$

avec :

$$\begin{cases} \sigma_1 = \sum_{k=1}^4 y_k = 0 \\ \sigma_2 = \sum_{1 \leq i < j \leq 4} y_i y_j = 4p(x_0 - p) \\ \sigma_3 = \sum_{1 \leq i < j < k \leq 4} y_i y_j y_k = -8p^2 y_0 \\ \sigma_4 = y_1 y_2 y_3 y_4 = 4p^2(x_0^2 + y_0^2 - R^2) \end{cases}$$

(fonctions symétriques élémentaires des racines).

Une condition nécessaire de cocyclicité est donc $\sigma_1 = \sum_{k=1}^4 y_k = 0$, les réels y_k étant deux à deux distincts.

Réciproquement, étant donnés des réels y_1, y_2, y_3, y_4 deux à deux distincts tels que $\sigma_1 = \sum_{k=1}^4 y_k = 0$, on définit les réels x_0 et y_0 par :

$$\begin{cases} 4p(x_0 - p) = \sigma_2 = \sum_{1 \leq i < j \leq 4} y_i y_j \\ -8p^2 y_0 = \sigma_3 = \sum_{1 \leq i < j < k \leq 4} y_i y_j y_k \end{cases}$$

et le réel r par :

$$4p^2(x_0^2 + y_0^2 - r) = \sigma_4 = y_1 y_2 y_3 y_4.$$

Il s'agit alors de vérifier que $r > 0$. Les conditions imposées nous disent que les y_k sont racines de :

$$\begin{aligned} P(t) &= t^4 - \sigma_1 t^3 + \sigma_2 t^2 - \sigma_3 t + \sigma_4 \\ &= t^4 + 4p(p - x_0)t^2 - 8p^2 y_0 t + 4p^2(x_0^2 + y_0^2 - r) \end{aligned}$$

et en remarquant que $P(y_1) = 0$ équivaut à :

$$Q(y_1) = \left(\frac{1}{2p}y_1^2 - x_0\right)^2 + (y_1 - y_0)^2 - r = 0,$$

on déduit que :

$$r = \left(\frac{1}{2p}y_1^2 - x_0\right)^2 + (y_1 - y_0)^2 > 0$$

($r = 0$ donnerait $y_1 = y_0$ et $x_0 = \frac{1}{2p}y_1^2 = \frac{1}{2p}y_0^2$, soit $M_0 \in \Gamma$, ce qui n'est pas) et peut poser $r = R^2$ avec $R > 0$. Les conditions $Q(y_k) = 0$ pour $1 \leq k \leq 4$ nous disent alors que les points M_k sont cocycliques.

On a donc montré le résultat suivant.

Théorème 18.21 *Les points deux à deux distincts $M_k(x_k, y_k)$, pour $1 \leq k \leq 4$, sont cocycliques sur la parabole Γ d'équation $y^2 = 2px$ si, et seulement si, $\sum_{k=1}^4 y_k = 0$.*

18.5.2 Cocyclicité de 4 points sur une ellipse

Soit Γ une ellipse de paramétrisation :

$$\gamma : t \in \mathbb{R} \mapsto (a \cos(t), b \sin(t))$$

dans un repère orthonormé (O, \vec{i}, \vec{j}) , où $0 < b < a$.

Théorème 18.22 (Joachimstal) *Les points deux à deux distincts $M_k(x_k, y_k)$, pour $1 \leq k \leq 4$, sont cocycliques sur l'ellipse Γ de paramétrisation $(x, y) = (a \cos(t), b \sin(t))$ si, et seulement si, $\sum_{k=1}^4 y_k \equiv 0$ modulo 2π .*

18.6 Équations des coniques dans un repère quelconque

On peut définir une conique dans un repère cartésien (non nécessairement orthonormé) par une équation implicite $\varphi(x, y) = 0$ où $\varphi = q + h$ est la somme d'une forme quadratique non nulle et d'une fonction affine, soit :

$$q(x, y) = ax^2 + 2bxy + cy^2 \text{ et } h(x, y) = 2dx + 2ey + f$$

avec $(a, b, c) \in \mathbb{R}^3 \setminus \{0\}$ et $(d, e, f) \in \mathbb{R}^3$.

Le réel $\delta = b^2 - ac$ est le discriminant (réduit) de la forme quadratique q .

On désigne par Γ une telle courbe d'équation $\varphi(x, y) = 0$.

Théorème 18.23

1. Si $\delta < 0$, alors Γ est soit vide, soit une ellipse, soit un cercle éventuellement réduit à un point.
2. Si $\delta = 0$, alors Γ est soit vide, soit une droite, soit la réunion de deux droites parallèles, soit une parabole.
3. Si $\delta > 0$, alors Γ est soit la réunion de deux droites sécantes, soit une hyperbole.

Dans le cas où $\delta \neq 0$ et Γ est une conique, les valeurs propres de la matrice A de q définissent les directions principales (ou les axes) de la conique. Cette conique est à centre et les coordonnées du centre s'obtiennent en résolvant le système :

$$\begin{cases} \frac{\partial \varphi}{\partial x} f(x, y) = 0 \\ \frac{\partial \varphi}{\partial y} f(x, y) = 0 \end{cases}$$

soit :

$$\begin{cases} ax + by + d = 0 \\ bx + cy + e = 0 \end{cases}$$

Nombres complexes et géométrie euclidienne

Le corps \mathbb{C} des nombres complexes est supposé construit (voir le chapitre 7).

On rappelle que \mathbb{C} est un corps commutatif et un \mathbb{R} -espace vectoriel de dimension 2, de base canonique $(1, i)$ où i est une solution complexe de l'équation $x^2 + 1 = 0$.

19.1 Le plan affine euclidien

On suppose connu le plan affine euclidien que l'on note \mathcal{P} et que l'on munit d'un repère orthonormé $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$, en désignant par $\vec{\mathcal{P}}$ le plan vectoriel associé à \mathcal{P} .

Nous rappelons rapidement quelques notions utiles pour la suite.

Un point $M \in \mathcal{P}$ est repéré par ses coordonnées $(x, y) \in \mathbb{R}^2$, ce qui signifie qu'on a l'égalité $\vec{OM} = x\vec{e}_1 + y\vec{e}_2$ dans $\vec{\mathcal{P}}$.

On notera :

- $\vec{v}_1 \cdot \vec{v}_2 = x_1x_2 + y_1y_2$: le produit scalaire des vecteurs \vec{v}_1 et \vec{v}_2 de $\vec{\mathcal{P}}$;
- $\det_{\mathcal{B}}(\vec{v}_1, \vec{v}_2) = x_1y_2 - x_2y_1$: le déterminant de (\vec{v}_1, \vec{v}_2) dans la base $\mathcal{B} = (\vec{e}_1, \vec{e}_2)$;
- $AB = \|\vec{AB}\| = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}$: la distance de A à B dans \mathcal{P} .

On rappelle que si $\mathcal{B}' = (\vec{e}'_1, \vec{e}'_2)$ est une autre base de $\vec{\mathcal{P}}$, on a :

$$\det_{\mathcal{B}}(\vec{v}_1, \vec{v}_2) = \det_{\mathcal{B}}(\mathcal{B}') \det_{\mathcal{B}'}(\vec{v}_1, \vec{v}_2)$$

Dans le cas où \mathcal{B}' est orthonormée comme \mathcal{B} , on a $\det_{\mathcal{B}}(\mathcal{B}') = \pm 1$.

On rappelle aussi que la base \mathcal{B}' définit la même orientation de $\vec{\mathcal{P}}$ que \mathcal{B} si, et seulement si, $\det_{\mathcal{B}}(\mathcal{B}') > 0$.

En se fixant une base \mathcal{B} , on écrira \det pour $\det_{\mathcal{B}}$.

19.2 Le plan d'Argand-Cauchy

Le plan \mathcal{P} est muni d'un repère orthonormé $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$.

Théorème 19.1 *L'application φ [resp. $\vec{\varphi}$] qui associe à tout nombre complexe $z = x + iy$ le point $\varphi(z) \in \mathcal{P}$ [resp. le vecteur $\vec{\varphi}(z) \in \vec{\mathcal{P}}$] de coordonnées (x, y) dans le repère \mathcal{R} [resp. dans la base (\vec{e}_1, \vec{e}_2)] réalise une bijection de \mathbb{C} sur \mathcal{P} [resp. sur $\vec{\mathcal{P}}$].*

Démonstration. Résulte du fait que tout nombre complexe [resp. tout point de \mathcal{P} ou tout vecteur de $\vec{\mathcal{P}}$] est uniquement déterminé par sa partie réelle et sa partie imaginaire [resp. par ses coordonnées dans le repère \mathcal{R} ou dans la base (\vec{e}_1, \vec{e}_2)]. ■

Tout point M du plan affine \mathcal{P} [resp. tout vecteur \vec{v} du plan vectoriel $\vec{\mathcal{P}}$] s'écrit donc de manière unique $M = \varphi(z)$ [resp. $\vec{v} = \vec{\varphi}(z)$] et peut ainsi être identifié au nombre complexe z .

Remarque 19.1 Les bijections φ et $\vec{\varphi}$ dépendent du repère orthonormé \mathcal{R} choisi.

Remarque 19.2 L'application $\vec{\varphi}$ est linéaire et donc réalise un isomorphisme d'espace vectoriel de \mathbb{C} sur $\vec{\mathcal{P}}$, puisqu'elle est bijective.

Le plan \mathcal{P} muni de cette identification est appelé plan complexe ou plan d'Argand-Cauchy.

Si $M \in \mathcal{P}$ [resp. $\vec{v} \in \vec{\mathcal{P}}$] s'écrit $M = \varphi(z)$ [resp. $\vec{v} = \vec{\varphi}(z)$], on dit que z est l'afixe de M [resp. l'afixe de \vec{v}] et M [resp. \vec{v}] le point [resp. vecteur] image de z .

On a $\varphi(0) = O$, le vecteur \vec{OM} est le vecteur image de z et z est l'afixe de \vec{OM} . Précisément si $z = x + iy$, on a :

$$\overrightarrow{\varphi(0)\varphi(z)} = \vec{OM} = x\vec{e}_1 + y\vec{e}_2 = \vec{\varphi}(z)$$

ce qui peut s'écrire dans \mathcal{P} :

$$\varphi(z) = \varphi(0) + \vec{\varphi}(z)$$

et s'interprète en disant que φ est une application affine de \mathbb{C} dans \mathcal{P} d'application linéaire associée $\vec{\varphi}$ (le plan vectoriel \mathbb{C} est naturellement muni d'une structure d'espace affine).

En utilisant cette identification entre \mathcal{P} et \mathbb{C} , on peut donner les interprétations géométriques suivantes où a, b, z, z' désignent des nombres complexes et A, B, M, M' leurs images respectives dans \mathcal{P} .

1. L'axe $O_x = \mathbb{R}\vec{e}_1$ est identifié à l'ensemble des nombres réels.
2. L'axe $O_y = \mathbb{R}\vec{e}_2$ est identifié à l'ensemble des imaginaires purs.
3. $a + b$ est l'afixe du vecteur $\vec{OC} = \vec{OA} + \vec{OB}$ et $b - a$ l'afixe du vecteur $\vec{AB} = \vec{OB} - \vec{OA}$ (résulte de la linéarité de $\vec{\varphi}$).

$$4. \Re(\bar{z}z') = \Re(\bar{z}z') = xx' + yy' = \vec{OM} \cdot \vec{OM'}.$$

$$5. \Im(\bar{z}z') = xy' - x'y = \det(\vec{OM}, \vec{OM'}).$$

$$6. \bar{z}z' = \Re(\bar{z}z') + i\Im(\bar{z}z') = \overrightarrow{OM} \cdot \overrightarrow{OM'} + i \det(\overrightarrow{OM}, \overrightarrow{OM'}).$$

7. Si A, B, C sont deux à deux distincts, alors ces points sont alignés si, et seulement si, il existe un réel λ tel que $\overrightarrow{AB} = \lambda \overrightarrow{AC}$, ce qui équivaut à dire que $\frac{b-a}{c-a}$ est réel.

On peut aussi dire que A, B, C sont alignés si, et seulement si :

$$\det(\overrightarrow{AC}, \overrightarrow{AB}) = \Im((b-a)(\overline{c-a})) = 0$$

ce qui équivaut à dire que $(b-a)(\overline{c-a})$ est réel.

8. Si les points A, B, C, D sont deux à deux distincts, alors les droites (AB) et (CD) sont orthogonales si, et seulement si :

$$\overrightarrow{AB} \cdot \overrightarrow{CD} = \Re((b-a)(\overline{d-c})) = 0$$

ce qui équivaut à dire que $(b-a)(\overline{d-c})$ est imaginaire pur.

Remarque 19.3 Si u, v sont deux nombres complexes avec v non nul, on a les équivalences :

$$\left(\frac{u}{v} = \frac{1}{|v|^2} u\bar{v} \text{ est réel} \right) \Leftrightarrow (u\bar{v} \text{ est réel})$$

et :

$$\left(\frac{u}{v} = \frac{1}{|v|^2} u\bar{v} \text{ est imaginaire pur} \right) \Leftrightarrow (u\bar{v} \text{ est imaginaire pur})$$

En utilisant les propriétés 7. et 8. précédentes, on en déduit que si A, B, C, D sont des points deux à deux distincts, alors :

$$(A, B, C \text{ sont alignés}) \Leftrightarrow ((b-a)(\overline{c-a}) \in \mathbb{R}) \Leftrightarrow \left(\frac{b-a}{c-a} \in \mathbb{R} \right)$$

et :

$$((AB) \text{ et } (CD) \text{ sont orthogonales}) \Leftrightarrow ((b-a)(\overline{d-c}) \in i\mathbb{R}) \Leftrightarrow \left(\frac{b-a}{d-c} \in i\mathbb{R} \right)$$

Dans ce qui suit, on identifie le plan d'Argand-Cauchy \mathcal{P} à \mathbb{C} .

Si $A, B, M, M', \Omega, \dots$ sont des points de \mathcal{P} , nous noterons $a, b, z, z', \omega, \dots$ (noter que les affixes de points variables M, M', \dots sont notées z, z', \dots).

19.3 Équations complexes des droites et cercles du plan

19.3.1 Droites dans le plan complexe

Soit \mathcal{D} une droite passant par deux points distincts A, B . Dire que M appartient à \mathcal{D} équivaut à dire que les points A, M, B sont alignés, ce qui équivaut encore à dire que $(z-a)(\bar{z}-\bar{b})$ est réel, soit :

$$(z-a)(\bar{z}-\bar{b}) = (\bar{z}-\bar{a})(z-b)$$

ce qui s'écrit :

$$(\bar{b}-\bar{a})z - (b-a)\bar{z} - (a\bar{b}-\bar{a}b) = 0$$

le nombre complexe $\overline{ab} - \overline{ab} = 2i\Im(ab)$ étant imaginaire pur. En multipliant par i , une équation complexe de la droite \mathcal{D} est alors :

$$\overline{\beta}z + \beta\overline{z} + \gamma = 0 \quad (19.1)$$

où $\beta = i(a - b) \in \mathbb{C}^*$ et γ est réel.

Le nombre complexe $\beta = i(a - b)$ est l'affixe d'un vecteur \vec{v} qui est orthogonal à \mathcal{D} . En effet, on a :

$$\vec{v} \cdot \overrightarrow{AB} = \Re(\overline{\beta}(b - a)) = \Re(i|b - a|^2) = 0.$$

On peut aussi aboutir à ce résultat en utilisant une équation cartésienne de \mathcal{D} :

$$ux + vy + w = 0$$

avec $(u, v) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ et $w \in \mathbb{R}$. En écrivant que $x = \frac{1}{2}(z + \overline{z})$ et $y = \frac{1}{2i}(z - \overline{z})$ pour M d'affixe z , cette équation devient :

$$u(z + \overline{z}) - vi(z - \overline{z}) + 2w = 0$$

soit :

$$(u - iv)z + (u + iv)\overline{z} + 2w = 0$$

avec $\beta = u + iv$ affixe du vecteur $\vec{v} = u\vec{e}_1 + v\vec{e}_2$ orthogonal à \mathcal{D} .

Réciproquement une équation du type (19.1) définit une droite. En effet, en écrivant $z = x + iy$, $\beta = u + iv$, cette équation devient :

$$(u - iv)(x + iy) + (u + iv)(x - iy) + \gamma = 0$$

soit :

$$ux + vy + \frac{\gamma}{2} = 0$$

et c'est une droite dirigée par le vecteur d'affixe $-v + iu = i\beta$ (ou orthogonale au vecteur d'affixe $\beta = u + iv$).

19.3.2 Cercles dans le plan complexe

Soit \mathcal{C} un cercle de centre Ω et de rayon $R > 0$ dans le plan \mathcal{P} .

Dire que $M \in \mathcal{C}$ équivaut à dire que :

$$(x - x_\Omega)^2 + (y - y_\Omega)^2 = R^2$$

ce qui se traduit dans le plan complexe par :

$$|z - \omega|^2 = R^2$$

et peut aussi s'écrire :

$$(z - \omega)(\overline{z} - \overline{\omega}) = z\overline{z} - \overline{\omega}z - \omega\overline{z} + |\omega|^2 - R^2 = 0$$

Une équation complexe de ce cercle \mathcal{C} est donc :

$$z\overline{z} - \overline{\omega}z - \omega\overline{z} + \gamma = 0 \quad (19.2)$$

où $\gamma = |\omega|^2 - R^2$ est réel avec $|\omega|^2 - \gamma = R^2 > 0$.

Réciproquement une telle équation définit un cercle. En effet, en écrivant $z = x + iy$, $\omega = u + iv$, cette équation devient :

$$x^2 + y^2 - 2ux - 2vy + \gamma = 0$$

soit :

$$(x - u)^2 + (y - v)^2 + \gamma - u^2 - v^2 = 0$$

et en posant $R^2 = u^2 + v^2 - \gamma = |\omega|^2 - \gamma$ (ce réel est positif), on constate qu'on a le cercle de centre ω et de rayon $\sqrt{|\omega|^2 - \gamma}$.

On a donc montré le résultat suivant.

Théorème 19.2 *Toute équation de la forme :*

$$\alpha z \bar{z} + \bar{\beta} z + \beta \bar{z} + \gamma = 0$$

où α, γ sont des réels et β un nombre complexe représente :

- l'ensemble \mathbb{C} tout entier si $\alpha = \beta = \gamma = 0$;
- l'ensemble vide si $\alpha = \beta = 0$ et $\gamma \neq 0$;
- une droite dirigée par le vecteur d'affixe $i\beta$ (ou orthogonale vecteur d'affixe β) si $\alpha = 0$ et $\beta \neq 0$;
- l'ensemble vide si $\alpha \neq 0$ et $\frac{|\beta|^2}{\alpha^2} - \frac{\gamma}{\alpha} < 0$;
- le cercle de centre $\omega = -\frac{\beta}{\alpha}$ et de rayon $\sqrt{\frac{|\beta|^2}{\alpha^2} - \frac{\gamma}{\alpha}}$ si $\alpha \neq 0$ et $\frac{|\beta|^2}{\alpha^2} - \frac{\gamma}{\alpha} \geq 0$.

19.4 Interprétation géométrique du module d'un nombre complexe

A priori, a, b, z, z', ω désignent des nombres complexes et A, B, M, M', Ω leurs images respectives dans \mathcal{P} relativement à un repère orthonormé $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$.

19.4.1 Module et distance euclidienne

Théorème 19.3

1. $|z| = OM = \sqrt{x^2 + y^2}$ est la distance de O à M ;
2. $|b - a| = AB$ est la distance de A à B ;
3. l'ensemble des nombres complexes z tels que $|z - \omega| = \rho$ est identifié au cercle de centre Ω et de rayon $\rho \geq 0$;
4. l'ensemble des nombres complexes z tels que $|z - \omega| < \rho$ [resp. $|z - \omega| \leq \rho$] est identifié au disque ouvert [resp. fermé] de centre Ω et de rayon $\rho \geq 0$;
5. pour $A \neq B$, le point M est sur la médiatrice du segment $[AB]$ si, et seulement si, $|z - a| = |z - b|$.

Démonstration. Il suffit de vérifier. ■

Remarque 19.4 Si $\mathcal{R}' = (O', \vec{e}_1', \vec{e}_2')$ est un autre repère orthonormé de \mathcal{P} , en désignant par $M' = \varphi'(z)$ l'image dans \mathcal{P} du nombre complexe $z = x + iy$ relativement à \mathcal{R}' , on a :

$$\|\vec{O'M'}\|^2 = \|x\vec{e}_1' + y\vec{e}_2'\|^2 = x^2 + y^2 = |z|^2 = \|\vec{OM}\|^2$$

et $|z| = OM$ est bien indépendant du repère orthonormé choisi. On peut donc aussi définir le module de z comme la distance de O à M où $M = \varphi(z)$ et $O = \varphi(0)$, φ étant la bijection de \mathbb{C} sur \mathcal{P} relative à un repère quelconque \mathcal{R} .

Remarque 19.5 L'équation complexe $|z - a| = |z - b|$ de la médiatrice du segment $[AB]$ s'écrit aussi $|z - a|^2 - |z - b|^2 = 0$, soit :

$$(\bar{a} - \bar{b})z + (a - b)\bar{z} + (|b|^2 - |a|^2) = 0$$

et c'est une droite dirigée par le vecteur \vec{u} d'affixe $i\beta = i(a - b)$ (ou orthogonale au vecteur \vec{v} d'affixe $\beta = b - a$). On constate que le point I d'affixe $z = \frac{a + b}{2}$, c'est-à-dire le milieu de $[A, B]$, est bien sur cette médiatrice.

Une équation complexe de cette médiatrice est donc :

$$z = \frac{a + b}{2} + i\lambda(b - a)$$

où λ décrit \mathbb{R} .

19.4.2 L'égalité du parallélogramme

L'égalité suivante valable pour tous nombres complexes z et z' :

$$|z + z'|^2 = |z|^2 + 2\Re(z\bar{z}') + |z'|^2$$

se traduit géométriquement par :

$$\|\vec{u} + \vec{v}\|^2 = \|\vec{u}\|^2 + 2\vec{u} \cdot \vec{v} + \|\vec{v}\|^2 \quad (19.3)$$

pour tous vecteurs \vec{u}, \vec{v} du plan euclidien $\vec{\mathcal{P}}$.

De cette identité, on déduit que :

$$|z + z'|^2 + |z - z'|^2 = 2(|z|^2 + |z'|^2)$$

qui se traduit géométriquement par :

$$\|\vec{u} + \vec{v}\|^2 + \|\vec{u} - \vec{v}\|^2 = 2(\|\vec{u}\|^2 + \|\vec{v}\|^2)$$

et s'interprète en disant que la somme des carrés des diagonales d'un parallélogramme est égale à la somme des carrés des cotés. En effet, en notant M'' le point d'affixe $z + z'$, $OMM''M'$ est un parallélogramme avec :

- $|z| = OM = M'M''$ puisque l'affixe de $\vec{M'M''} = \vec{OM''} - \vec{OM'}$ est $z + z' - z' = z$;
- $|z'| = OM' = MM''$, puisque l'affixe de $\vec{MM''} = \vec{OM''} - \vec{OM}$ est $z + z' - z = z'$;
- $|z + z'| = OM''$ (une diagonale) et $|z' - z| = MM'$ (l'autre diagonale).

Cette identité du parallélogramme est caractéristique des normes qui se déduisent d'un produit scalaire.

Nous reviendrons sur cette identité du parallélogramme au paragraphe sur le triangle.

$$\text{FIGURE 19.1} - OM'^2 + MM'^2 = 2(OM^2 + OM'^2)$$

19.4.3 L'inégalité de Cauchy-Schwarz

L'inégalité de Cauchy-Schwarz dans \mathbb{C} :

$$|\Re(z\overline{z'})| \leq |z||z'|$$

l'égalité étant réalisée si, et seulement si, z et z' sont liés sur \mathbb{R} (théorème 7.5), nous permet de retrouver la même inégalité dans le plan euclidien $\vec{\mathcal{P}}$:

$$|\vec{u} \cdot \vec{v}| \leq \|\vec{u}\| \|\vec{v}\|$$

l'égalité étant réalisée si, et seulement si, les vecteurs \vec{u} et \vec{v} sont liés.

De cette inégalité, on déduit l'inégalité triangulaire dans \mathbb{C} :

$$|z + z'| \leq |z| + |z'|$$

l'égalité étant réalisée si, et seulement si, z et z' sont positivement liés sur \mathbb{R} (théorème 7.6), qui nous permet de retrouver la même inégalité dans le plan euclidien $\vec{\mathcal{P}}$:

$$\|\vec{u} + \vec{v}\| \leq \|\vec{u}\| + \|\vec{v}\|$$

l'égalité étant réalisée si, et seulement si, les vecteurs \vec{u} et \vec{v} sont positivement liés.

Cette inégalité triangulaire s'interprète en disant que dans un vrai triangle ABC la longueur d'un coté est strictement inférieure à la somme des longueurs des deux autres cotés :

$$\begin{aligned} \|\vec{BC}\| &= \|\vec{AC} - \vec{AB}\| = |z - z'| \\ &< |z| + |z'| = \|\vec{AC}\| + \|\vec{AB}\| \end{aligned}$$

en notant z l'afixe de \vec{AC} et z' celle de \vec{AB} .

De manière plus générale, on a vu que pour toute suite finie z_1, \dots, z_n de nombres complexes non nuls avec $n \geq 2$, on a :

$$\left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$$

l'égalité étant réalisée si, et seulement si, il existe des réels $\lambda_2, \dots, \lambda_n$ tels que $z_k = \lambda_k z_1$ pour $k = 2, \dots, n$ (exercice 7.7). Du point de vue géométrique, en désignant par M_k les points d'afixe z_k , on en déduit que l'égalité $\left\| \sum_{k=1}^n \vec{OM_k} \right\| = \sum_{k=1}^n \|\vec{OM_k}\|$ équivaut à dire que les points O, M_1, \dots, M_n sont alignés sur la demi-droite $[OM_1]$.

19.5 Lignes de niveau associées aux module

Si X est une partie non vide de \mathbb{C} et f une application de \mathbb{C} dans \mathbb{R} , on appelle lignes de niveau associées à f les sous-ensembles E_λ de \mathbb{C} définis par :

$$E_\lambda = \{z \in X \mid f(z) = \lambda\}$$

où λ décrit \mathbb{R} .

À chaque ligne de niveau E_λ , on associe la partie \mathcal{E}_λ de \mathcal{P} formée des points d'affixes $z \in E_\lambda$. On identifiera les ensembles E_λ et \mathcal{E}_λ .

Précisément, on a :

$$\mathcal{E}_\lambda = \{M \in \mathcal{P} \mid f \circ \varphi^{-1}(M) = \lambda\}$$

Par exemple pour $\omega \in \mathbb{C}$ donné, les lignes de niveau de :

$$f : z \mapsto |z - \omega|$$

sont définies par :

$$\mathcal{E}_\lambda = \begin{cases} \emptyset & \text{si } \lambda < 0, \\ \{\Omega\} & \text{si } \lambda = 0, \\ \text{le cercle de centre } \Omega \text{ et de rayon } \lambda & \text{si } \lambda > 0. \end{cases}$$

Du cours sur les coniques, on déduit les résultats suivants.

Pour $a \neq b$ donnés \mathbb{C} , les lignes de niveau de :

$$f : z \mapsto |z - a| + |z - b|$$

sont définies par :

$$\mathcal{E}_\lambda = \begin{cases} \emptyset & \text{si } \lambda < |a - b|, \\ \text{le segment } [AB] & \text{si } \lambda = |a - b|, \\ \text{l'ellipse de foyers } A, B \text{ et de grand axe } \lambda & \text{si } \lambda > |a - b|. \end{cases}$$

Pour $a \neq b$ donnés \mathbb{C} , les lignes de niveau de :

$$f : z \mapsto ||z - a| - |z - b||$$

sont définies par :

$$\mathcal{E}_\lambda = \begin{cases} \emptyset & \text{si } \lambda > |a - b|, \\ \text{la droite } (AB) \text{ privée du segment ouvert }]AB[& \text{si } \lambda = |a - b|, \\ \text{l'hyperbole de foyers } A, B \text{ et de grand axe } \lambda & \text{si } \lambda < |a - b|. \end{cases}$$

En utilisant la représentation complexe des droites et cercles (théorème 19.2), on peut étudier les lignes de niveau de la fonction :

$$f : z \in \mathbb{C} \setminus \{a\} \mapsto \frac{|z - b|}{|z - a|}$$

Pour tout réel λ , on a :

$$E_\lambda = \left\{ z \in \mathbb{C} \setminus \{a\} \mid \frac{|z - b|}{|z - a|} = \lambda \right\} = \{z \in \mathbb{C} \mid |z - b| = \lambda |z - a|\}$$

Pour $\lambda < 0$, cet ensemble est vide et pour $\lambda = 0$, il est réduit à $\{b\}$.

Théorème 19.4 (Appolonius) Soient a, b deux nombres complexes distincts et λ un réel strictement positif. La ligne de niveau :

$$E_\lambda = \{z \in \mathbb{C} \mid |z - b| = \lambda |z - a|\}$$

est identifiée dans \mathcal{P} à la médiatrice du segment $[AB]$ si $\lambda = 1$ ou au cercle de centre Ω d'affixe $\frac{b - \lambda^2 a}{1 - \lambda^2}$ et de rayon $R = \frac{\lambda |a - b|}{|1 - \lambda^2|}$ si $\lambda \neq 1$.

Démonstration. L'ensemble E_λ a pour équation :

$$|z - b|^2 = \lambda^2 |z - a|^2$$

soit :

$$(z - b)(\bar{z} - \bar{b}) = \lambda^2 (z - a)(\bar{z} - \bar{a})$$

c'est-à-dire :

$$\alpha z \bar{z} + \bar{\beta} z + \beta \bar{z} + \gamma = 0$$

où on a posé :

$$\begin{cases} \alpha = 1 - \lambda^2 \\ \beta = \lambda^2 a - b \\ \gamma = |b|^2 - \lambda^2 |a|^2 \end{cases}$$

C'est donc une droite ou un cercle quand il n'est pas vide ou \mathbb{C} tout entier.

Pour $\lambda = 1$, on a :

$$E_\lambda = \{z \in \mathbb{C} \mid |z - b| = |z - a|\}$$

c'est donc l'ensemble des points équidistants de A et B , c'est-à-dire la médiatrice du segment $[AB]$. Cette médiatrice ayant pour équation complexe :

$$(\bar{a} - \bar{b})z + (a - b)\bar{z} + (|b|^2 - |a|^2) = 0$$

(ce qui a été déjà vu avec la remarque 19.5).

Pour $\lambda \neq 1$, on a :

$$\frac{|\beta|^2}{\alpha^2} - \frac{\gamma}{\alpha} = \frac{|\beta|^2 - \alpha\gamma}{\alpha^2}$$

avec :

$$\begin{aligned} |\beta|^2 - \alpha\gamma &= (\lambda^2 a - b)(\lambda^2 \bar{a} - \bar{b}) - (1 - \lambda^2)(|b|^2 - \lambda^2 |a|^2) \\ &= \lambda^2 (|a|^2 + |b|^2 - \bar{a}b - a\bar{b}) = \lambda^2 |a - b|^2 > 0 \end{aligned}$$

et \mathcal{E}_λ est le cercle de centre Ω ayant pour affixe $\omega = -\frac{\beta}{\alpha} = \frac{b - \lambda^2 a}{1 - \lambda^2}$ et de rayon $R = \frac{\lambda |a - b|}{|1 - \lambda^2|}$.

■

Remarque 19.6 Pour $\lambda = 1$, la médiatrice du segment $[A, B]$ coupe le plan affine en deux demi-plans respectivement définis par les inéquations complexes $|z - b| < |z - a|$ (c'est le demi-plan qui contient b) et $|z - b| > |z - a|$ (c'est le demi-plan qui contient a).

Remarque 19.7 Pour $\lambda \neq 1$, on a :

$$\omega = a + \frac{1}{1 - \lambda^2} (b - a) = b + \frac{\lambda^2}{1 - \lambda^2} (b - a)$$

et le centre Ω du cercle \mathcal{E}_λ est sur la droite (AB) privée du segment $[AB]$ (pour $|\lambda| > 1$, on a $\frac{1}{1 - \lambda^2} < 0$, donc Ω est sur la demi-droite $]-\infty, A]$, et pour $|\lambda| < 1$, on a $\frac{\lambda^2}{1 - \lambda^2} > 0$, donc Ω est sur la demi-droite $[B, +\infty[$).

Remarque 19.8 Pour $\lambda \neq 1$, l'égalité $(1 - \lambda^2)\omega = b - \lambda^2 a$, se traduit par :

$$(1 - \lambda^2) \overrightarrow{O\Omega} = \overrightarrow{OB} - \lambda^2 \overrightarrow{OA}$$

et signifie que le centre Ω est le barycentre de $(A, -\lambda^2)$ et $(B, 1)$. On retrouve le fait que ce centre est sur la droite (AB) .

Remarque 19.9 Pour $\lambda \neq 1$, les points de $\mathcal{E}_\lambda \cap (AB)$ sont ceux dont l'affixe z est telle que :

$$\begin{cases} |z - \omega| = R \\ z = \omega + t(b - a) \end{cases}$$

où t est un réel. Pour de tels points, on a :

$$|z - \omega| = |t| |b - a| = R = \frac{\lambda |a - b|}{|1 - \lambda^2|}$$

et :

$$t = \pm \frac{\lambda}{|1 - \lambda^2|}$$

Pour $\lambda > 1$, on a les deux solutions :

$$\begin{aligned} c &= \omega + \frac{\lambda}{\lambda^2 - 1} (b - a) = a + \frac{1}{1 - \lambda^2} (b - a) + \frac{\lambda}{\lambda^2 - 1} (b - a) \\ &= a + \frac{\lambda - 1}{\lambda^2 - 1} (b - a) = a + \frac{1}{\lambda + 1} (b - a) = \frac{\lambda}{\lambda + 1} a + \frac{1}{\lambda + 1} b \end{aligned}$$

et :

$$\begin{aligned} d &= \omega - \frac{\lambda}{\lambda^2 - 1} (b - a) = a + \frac{1}{1 - \lambda^2} (b - a) - \frac{\lambda}{\lambda^2 - 1} (b - a) \\ &= a - \frac{\lambda + 1}{\lambda^2 - 1} (b - a) = a - \frac{1}{\lambda - 1} (b - a) = \frac{\lambda}{\lambda - 1} a - \frac{1}{\lambda - 1} b \end{aligned}$$

ou encore :

$$\begin{cases} (\lambda + 1)c = \lambda a + b \\ (\lambda - 1)c = \lambda a - b \end{cases}$$

ce qui signifie que $\mathcal{E}_\lambda \cap (AB) = \{C, D\}$ où C est le barycentre de (A, λ) et $(B, 1)$ et D le barycentre de (A, λ) et $(B, -1)$.

On procède de manière analogue pour $0 < \lambda < 1$.

Par exemple, pour $a = 0$, $b = -3$ et $\lambda = 2$, l'ensemble :

$$E_\lambda = \{z \in \mathbb{C} \mid |z + 3| = 2|z|\}$$

est le cercle de centre 1 et de rayon 2.

Exercice 19.1 Déterminer l'ensemble E des nombres complexes z tels que $|z - i| = |z - iz| = |z - 1|$.

FIGURE 19.2 - $|z + 3| = 2|z|$ FIGURE 19.3 - $|z - i| = |z - iz| = |z - 1|$

Solution 19.1 L'ensemble :

$$E_1 = \left\{ z \in \mathbb{C} \mid |z - i| = |z - iz| = \sqrt{2}|z| \right\}$$

est le cercle de centre $-i$ et de rayon $\sqrt{2}$ et l'ensemble :

$$E_2 = \{ z \in \mathbb{C} \mid |z - i| = |z - 1| \}$$

est la médiatrice du segment $[1, i]$. L'ensemble E est l'intersection de ces ensembles, soit :

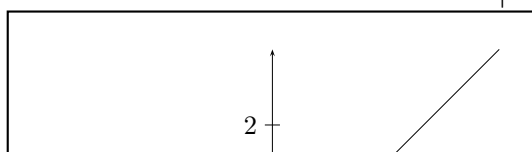
$$E = \left\{ -\frac{1 + \sqrt{3}}{2}(1 + i), \frac{\sqrt{3} - 1}{2}(1 + i) \right\}$$

(figure 19.3).

Exercice 19.2

1. Montrer que pour tous nombres complexes a, b, z , on a :

$$|z - a|^2 + |z - b|^2 = 2 \left| z - \frac{a + b}{2} \right|^2 + \frac{|b - a|^2}{2}$$



2. Déterminer l'ensemble \mathcal{C} des points M de \mathcal{P} tels que :

$$MA^2 + MB^2 = \lambda$$

où λ est un réel donné (lignes de niveau de $f : z \mapsto |z - a|^2 + |z - b|^2$).

Solution 19.2

1. En posant $z = \frac{a+b}{2} + t$ (ce qui revient à placer l'origine en I d'affixe $\frac{a+b}{2}$, c'est-à-dire au milieu du segment $[A, B]$), on a :

$$\begin{aligned} |z - a|^2 + |z - b|^2 &= \left| t + \frac{b-a}{2} \right|^2 + \left| t - \frac{b-a}{2} \right|^2 \\ &= 2 \left(|t|^2 + \left| \frac{b-a}{2} \right|^2 \right) \\ &= 2 \left| z - \frac{a+b}{2} \right|^2 + \frac{|b-a|^2}{2} \end{aligned}$$

2. Désignant par I le milieu de $[A, B]$, l'identité précédente s'écrit :

$$MA^2 + MB^2 = 2MI^2 + \frac{|b-a|^2}{2}$$

et l'égalité $MA^2 + MB^2 = \lambda$ se traduit par :

$$MI^2 = \frac{2\lambda - |b-a|^2}{4}$$

Il en résulte que :

- $\mathcal{C} = \emptyset$ pour $\lambda < \frac{|b-a|^2}{2}$;
- $\mathcal{C} = \{I\}$ pour $\lambda = \frac{|b-a|^2}{2}$;
- \mathcal{C} est le cercle de centre I et de rayon $\frac{\sqrt{2\lambda - |b-a|^2}}{2}$ pour $\lambda > \frac{|b-a|^2}{2}$.

19.6 Interprétation géométrique de l'argument d'un nombre complexe

On rappelle que pour tout nombre complexe non nul z , il existe un réel θ tel que :

$$\frac{z}{|z|} = \cos(\theta) + i \sin(\theta) = e^{i\theta}$$

et un tel réel est unique s'il est pris dans $]-\pi, \pi]$.

On dit que le réel θ est un argument de z et on dit que c'est l'argument principal s'il est pris dans $]-\pi, \pi]$.

Par abus de langage, on écrira $\theta = \arg(z)$ quand il n'y a pas d'ambiguïté.

On suppose toujours \mathcal{P} muni d'un repère orthonormé $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$.

En utilisant la forme polaire des nombres complexes et l'identité :

$$\overline{z_1}z_2 = \Re(\overline{z_1}z_2) + i\Im(\overline{z_1}z_2) = \vec{v_1} \cdot \vec{v_2} + i \det(\vec{v_1}, \vec{v_2})$$

on peut définir les mesures d'un angle orienté de deux vecteurs non nuls $\vec{v_1}$ et $\vec{v_2}$.

Pour ce faire on écrit que $\overline{z_1}z_2 = \rho e^{i\theta}$ où $\rho = |\overline{z_1}z_2| > 0$ ($\vec{v_1}$ et $\vec{v_2}$ sont non nuls) et $\theta \in \mathbb{R}$ est un argument de $\overline{z_1}z_2$.

On dit alors que θ est une mesure de l'angle orienté de vecteurs $(\vec{v_1}, \vec{v_2})$, relativement au repère orthonormé $\mathcal{R} = (O, \vec{e_1}, \vec{e_2})$.

Si les affixes sont considérées relativement à un autre repère orthonormé $\mathcal{R}' = (O', \vec{e'_1}, \vec{e'_2})$, en notant z' l'affixe du vecteur \vec{v} relativement à \mathcal{R}' , on a :

$$\overline{z'_1}z'_2 = \vec{v_1} \cdot \vec{v_2} + i \det_{\mathcal{B}'}(\vec{v_1}, \vec{v_2})$$

avec :

$$\det_{\mathcal{B}'}(\vec{v_1}, \vec{v_2}) = \det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}(\vec{v_1}, \vec{v_2}) = \pm \det_{\mathcal{B}}(\vec{v_1}, \vec{v_2})$$

(le calcul du produit scalaire $\vec{v_1} \cdot \vec{v_2}$ ne dépend pas du choix d'une base orthonormée). Dans le cas où \mathcal{R}' définit la même orientation que \mathcal{R} , on aura $\det_{\mathcal{B}'}(\mathcal{B}) = 1$ et $\overline{z'_1}z'_2 = \overline{z_1}z_2$.

Cette définition d'une mesure d'angle orienté de vecteur est donc indépendante du choix d'un repère orthonormé orienté.

On suppose donc ici que \mathcal{P} est orienté par le choix d'un repère orthonormé $\mathcal{R} = (O, \vec{e_1}, \vec{e_2})$. Tout repère orthonormé définissant la même orientation que \mathcal{R} est dit direct.

Remarque 19.10 *Le choix d'une orientation de $\vec{\mathcal{P}}$ nous permet de définir sans ambiguïté la mesure principale dans $]-\pi, \pi]$ d'un angle de vecteurs. Ce choix d'une orientation correspond au choix d'une racine carrée i de -1 dans \mathbb{C} .*

Par abus de langage, on notera $(\vec{v_1}, \vec{v_2})$ une mesure de l'angle orienté de vecteurs. $(\vec{v_1}, \vec{v_2})$.

On peut remarquer que :

$$\theta = (\vec{v_1}, \vec{v_2}) = \arg(\overline{z_1}z_2) = \arg\left(\frac{z_2}{z_1}\right).$$

Une telle mesure d'angle orienté est donc définie par :

$$\begin{cases} \vec{v_1} \cdot \vec{v_2} = \rho \cos(\theta) = \|\vec{v_1}\| \|\vec{v_2}\| \cos(\theta) \\ \det(\vec{v_1}, \vec{v_2}) = \rho \sin(\theta) = \|\vec{v_1}\| \|\vec{v_2}\| \sin(\theta) \end{cases}$$

On vérifie facilement que pour tout réel non nul λ , on a $(\lambda\vec{v_1}, \lambda\vec{v_2}) = (\vec{v_1}, \vec{v_2})$. En particulier, $(-\vec{v_1}, -\vec{v_2}) = (\vec{v_1}, \vec{v_2})$.

Les vecteurs $\vec{v_1}$ et $\vec{v_2}$ sont orthogonaux si, et seulement si, $\vec{v_1} \cdot \vec{v_2} = 0$, ce qui équivaut à $\cos(\theta)$ ou encore à $\theta = \frac{\pi}{2}$ modulo π .

De l'identité (19.3), on déduit que :

$$\|\vec{u} + \vec{v}\|^2 = \|\vec{u}\|^2 + 2\|\vec{u}\| \|\vec{v}\| \cos(\theta) + \|\vec{v}\|^2$$

Pour $\theta = \frac{\pi}{2}$ modulo π , on retrouve le théorème de Pythagore.

Les vecteurs $\vec{v_1}$ et $\vec{v_2}$ sont colinéaires si, et seulement si, $\det(\vec{v_1}, \vec{v_2}) = 0$, ce qui équivaut à $\sin(\theta)$ ou encore à $\theta = 0$ modulo π , soit $\theta \in \{0, \pi\}$ pour la détermination principale.

On en déduit que les points deux à deux distincts A, B, C sont alignés si, et seulement si, $(\overrightarrow{AB}, \overrightarrow{AC}) \equiv 0$ modulo π . Précisément, en utilisant la détermination principale de la mesure d'angle (ou de l'argument), on aura $(\overrightarrow{AB}, \overrightarrow{AC}) = 0$ si, et seulement si, $\overrightarrow{AC} = \lambda \overrightarrow{AB}$ avec $\lambda > 0$ ($\overrightarrow{AB} \cdot \overrightarrow{AC} = \|\overrightarrow{AB}\| \|\overrightarrow{AC}\| > 0$) et $(\overrightarrow{AB}, \overrightarrow{AC}) = \pi$ si, et seulement si, $\overrightarrow{AC} = \lambda \overrightarrow{AB}$ avec $\lambda < 0$ ($\overrightarrow{AB} \cdot \overrightarrow{AC} = -\|\overrightarrow{AB}\| \|\overrightarrow{AC}\| < 0$) (figure 19.4).

FIGURE 19.4 – Points alignés

Si les points A, B, C sont deux à deux distincts alors un argument de $\frac{c-a}{b-a}$ (ou de $(\bar{b}-\bar{a})(c-a)$) est une mesure de l'angle orienté $\theta_A = (\overrightarrow{AB}, \overrightarrow{AC})$ et on a :

$$\begin{cases} \cos(\theta_A) = \frac{\overrightarrow{AB} \cdot \overrightarrow{AC}}{AB \cdot AC} \\ \sin(\theta_A) = \frac{\det(\overrightarrow{AB}, \overrightarrow{AC})}{AB \cdot AC} \end{cases} \quad (19.4)$$

En utilisant les propriétés de l'argument, on obtient les résultats suivants.

— Si A, B, C dans \mathcal{P} sont deux à deux distincts, alors ces points sont alignés si, et seulement si, $\arg(b-a) \equiv \arg(c-a)$ modulo π .

En effet dire que A, B, C sont alignés équivaut à dire que $\arg\left(\frac{b-a}{c-a}\right) \equiv 0 \pmod{\pi}$ et avec

$\arg\left(\frac{b-a}{c-a}\right) \equiv \arg(b-a) - \arg(c-a) \pmod{2\pi}$, on a le résultat annoncé.

$$(\vec{v}_2, \vec{v}_1) \equiv \arg\left(\frac{z_1}{z_2}\right) \equiv -\arg\left(\frac{z_2}{z_1}\right) \equiv -(\vec{v}_1, \vec{v}_2) \pmod{2\pi}$$

— La relation de Chasles sur les mesures d'angle :

$$\begin{array}{c} \text{A} \quad \quad \quad \text{B} \quad \quad \quad \text{C} \\ \hline (\vec{v}_1, \vec{v}_2) + (\vec{v}_2, \vec{v}_3) \equiv (\vec{v}_1, \vec{v}_3) \pmod{2\pi} \\ (\overrightarrow{AB}, \overrightarrow{AC}) \equiv 0 \pmod{2\pi} \end{array}$$

$$\begin{array}{c} \text{C} \quad \quad \quad \text{A} \quad \quad \quad \text{B} \\ \hline \end{array}$$

En effet, on a :

$$\begin{aligned} (\vec{v}_1, \vec{v}_2) + (\vec{v}_2, \vec{v}_3) &\equiv \arg\left(\frac{z_2}{z_1}\right) + \arg\left(\frac{z_3}{z_2}\right) \\ &\equiv \arg\left(\frac{z_3}{z_1}\right) \equiv (\vec{v}_1, \vec{v}_3) \pmod{2\pi} \end{aligned}$$

19.7 Lignes de niveau associées à l'argument

Le plan \mathcal{P} est muni d'un repère orthonormé direct $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$

On s'intéresse tout d'abord à l'étude des lignes de niveau de la fonction :

$$f : z \in \mathbb{C} \setminus \{\omega\} \mapsto \arg(z - \omega)$$

où ω est un nombre complexe donné, cette fonction étant a priori à valeurs dans le groupe quotient $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ (voir le chapitre 20).

Pour tout nombre réel θ , on note :

$$E_\theta = \{z \in \mathbb{C} \setminus \{\omega\} \mid \arg(z - \omega) \equiv \theta \pmod{2\pi}\}$$

et \mathcal{E}_θ est la partie de \mathcal{P} correspondante, c'est l'ensemble :

$$\mathcal{E}_\theta = \left\{ M \in \mathcal{P} \setminus \{\Omega\} \mid \left(\vec{e}_1, \overrightarrow{\Omega M} \right) \equiv \theta \pmod{2\pi} \right\}$$

Théorème 19.5 *Si θ est un nombre réel, alors l'ensemble E_θ est identifié à la demi-droite passant par le point Ω d'affixe ω et d'angle polaire θ privée du point Ω , soit :*

$$\mathcal{E}_\theta = \left\{ M \in \mathcal{P} \mid \overrightarrow{\Omega M} = \rho (\cos(\theta) \vec{e}_1 + \sin(\theta) \vec{e}_2) \text{ avec } \rho > 0 \right\}$$

(figure 19.5).

Démonstration. Un nombre complexe z est dans E_θ si, et seulement si, il s'écrit $z = \omega + \rho e^{i\theta}$ avec $\rho > 0$, ce qui se traduit dans le plan \mathcal{P} par $\overrightarrow{\Omega M} = \rho \vec{v}$ avec $\rho > 0$, où $\vec{v} = \cos(\theta) \vec{e}_1 + \sin(\theta) \vec{e}_2$ est le vecteur d'affixe $e^{i\theta}$. L'ensemble \mathcal{E}_θ est donc la demi droite d'origine Ω et dirigée par \vec{v} . ■

Remarque 19.11 *De manière analogue, on vérifie que l'ensemble :*

$$E_\theta = \{z \in \mathbb{C} \setminus \{\omega\} \mid \arg(z - \omega) \equiv \theta \pmod{\pi}\}$$

est identifié à la droite passant par le point Ω d'affixe ω et d'angle polaire θ privée du point Ω .

L'étude des lignes de niveau de la fonction :

$$f : z \in \mathbb{C} \setminus \{a, b\} \mapsto \arg\left(\frac{z-a}{z-b}\right)$$

où a, b sont deux nombres complexes distincts, nous fournira un critère de cocyclicité de 4 points du plan.

On s'intéresse tout d'abord aux lignes de niveau :

$$E_\theta = \left\{ z \in \mathbb{C} \setminus \{a, b\} \mid \arg\left(\frac{z-a}{z-b}\right) \equiv \theta \pmod{\pi} \right\}$$

où θ est un réel donné. La fonction f est dans ce cas à valeurs dans le groupe quotient $\frac{\mathbb{R}}{\pi\mathbb{Z}}$.

On note \mathcal{E}_θ la partie de \mathcal{P} correspondante, c'est l'ensemble :

$$\mathcal{E}_\theta = \left\{ M \in \mathcal{P} \setminus \{A, B\} \mid \left(\overrightarrow{MA}, \overrightarrow{MB}\right) \equiv \theta \pmod{\pi} \right\}$$

Lemme 19.1 *Soient $z \in \mathbb{C}^*$ et $\theta \in \mathbb{R}$. On a :*

$$(\arg(z) \equiv \theta \pmod{\pi}) \Leftrightarrow (z = \bar{z}e^{2i\theta})$$

Démonstration. On désigne par α un argument de z . On a donc $z = |z|e^{i\alpha}$ et :

$$(\arg(z) \equiv \theta \pmod{\pi}) \Rightarrow (z = \pm |z|e^{i\theta}) \Rightarrow (z^2 = |z|^2 e^{2i\theta} = z\bar{z}e^{2i\theta}) \Rightarrow (z = \bar{z}e^{2i\theta})$$

Réciproquement, supposons que $z = \bar{z}e^{2i\theta}$. On a alors :

$$z = |z|e^{i\alpha} = \bar{z}e^{2i\theta} = |z|e^{i(2\theta-\alpha)}$$

et $\alpha \equiv 2\theta - \alpha \pmod{2\pi}$, soit $\alpha \equiv \theta \pmod{\pi}$. ■

Dans le cas où $\theta \equiv 0 \pmod{\pi}$, on retrouve :

$$(z \in \mathbb{R}) \Leftrightarrow (z = \bar{z} = \bar{z}e^{2i\theta}) \Leftrightarrow (\arg(z) \equiv 0 \pmod{\pi})$$

Théorème 19.6 *Si a, b sont deux nombres complexes distincts et θ un réel, alors l'ensemble :*

$$E_\theta = \left\{ z \in \mathbb{C} \setminus \{a, b\} \mid \arg\left(\frac{z-a}{z-b}\right) \equiv \theta \pmod{\pi} \right\}$$

est identifié à :

— la droite (AB) privée des points A et B si θ est congru à 0 modulo π ;

FIGURE 19.6 –

— au cercle de centre Ω ayant pour affixe $\omega = \frac{a+b}{2} - i \cotan(\theta) \frac{b-a}{2}$ et de rayon $R = \frac{1}{|\sin(\theta)|} \left| \frac{b-a}{2} \right|$ privé des points A et B si θ n'est pas congru à 0 modulo π . (figure 19.6).

Démonstration. On a déjà vu que les points M, A, B sont alignés si, et seulement si, $\arg\left(\frac{z-a}{z-b}\right) \equiv 0 \pmod{\pi}$, donc pour $\theta \equiv 0 \pmod{\pi}$, E_θ est la droite (AB) privée des points A et B .

En désignant par α un argument de $\frac{z-a}{z-b}$, pour $z \in \mathbb{C} \setminus \{a, b\}$, en utilisant le lemme précédent, on a :

$$\begin{aligned} \left(\arg\left(\frac{z-a}{z-b}\right) \equiv \theta \pmod{\pi} \right) &\Leftrightarrow \left(\frac{z-a}{z-b} = \frac{\bar{z}-\bar{a}}{\bar{z}-\bar{b}} e^{2i\theta} \right) \\ &\Leftrightarrow (1 - e^{2i\theta}) z\bar{z} + (\bar{a}e^{2i\theta} - \bar{b})z + (be^{2i\theta} - a)\bar{z} + a\bar{b} - \bar{a}be^{2i\theta} = 0 \end{aligned}$$

Pour $\theta \equiv 0 \pmod{\pi}$, on a $e^{2i\theta} = 1$ et la condition :

$$(\bar{b} - \bar{a})z - (b - a)\bar{z} - (a\bar{b} - \bar{a}b) = 0$$

avec $z \in \mathbb{C} \setminus \{a, b\}$, qui est bien l'équation de la droite (AB) privée de A et B .

Pour θ non congru à 0 modulo π , on peut diviser par $1 - e^{2i\theta}$ et on obtient l'équation :

$$z\bar{z} + \frac{\bar{a}e^{2i\theta} - \bar{b}}{1 - e^{2i\theta}}z + \frac{be^{2i\theta} - a}{1 - e^{2i\theta}}\bar{z} + \frac{a\bar{b} - \bar{a}be^{2i\theta}}{1 - e^{2i\theta}} = 0$$

En écrivant que $1 - e^{2i\theta} = -2i \sin(\theta) e^{i\theta}$, cette équation s'écrit :

$$z\bar{z} - \frac{\bar{a}e^{2i\theta} - \bar{b}}{2i \sin(\theta) e^{i\theta}} z - \frac{be^{2i\theta} - a}{2i \sin(\theta) e^{i\theta}} \bar{z} - \frac{a\bar{b} - \bar{a}be^{2i\theta}}{2i \sin(\theta) e^{i\theta}} = 0$$

soit :

$$z\bar{z} - \frac{\bar{a}e^{i\theta} - \bar{b}e^{-i\theta}}{2i \sin(\theta)} z - \frac{be^{i\theta} - ae^{-i\theta}}{2i \sin(\theta)} \bar{z} - \frac{a\bar{b}e^{-i\theta} - \bar{a}be^{i\theta}}{2i \sin(\theta)} = 0$$

ou encore :

$$z\bar{z} - \bar{\omega}z - \omega\bar{z} + \gamma = 0 \quad (19.5)$$

en posant :

$$\omega = \frac{be^{i\theta} - ae^{-i\theta}}{2i \sin(\theta)}$$

et :

$$\gamma = \frac{\bar{a}be^{i\theta} - \bar{a}be^{-i\theta}}{2i \sin(\theta)} = \frac{2i\Im(\bar{a}be^{i\theta})}{2i \sin(\theta)} = \frac{\Im(\bar{a}be^{i\theta})}{\sin(\theta)} \in \mathbb{R}.$$

Le nombre complexe ω peut s'écrire sous la forme :

$$\begin{aligned} \omega &= \frac{(b-a) \cos(\theta) + i(b+a) \sin(\theta)}{2i \sin(\theta)} \\ &= \frac{a+b}{2} - i \cotan(\theta) \frac{b-a}{2}. \end{aligned}$$

En écrivant que $\gamma = \frac{a\bar{b} - \bar{a}be^{2i\theta}}{1 - e^{2i\theta}}$ et $\omega = \frac{a - be^{2i\theta}}{1 - e^{2i\theta}}$, on a :

$$\begin{aligned} |\omega|^2 - \gamma &= \frac{|a - be^{2i\theta}|^2 - (a\bar{b} - \bar{a}be^{2i\theta})(1 - e^{-2i\theta})}{|1 - e^{2i\theta}|^2} \\ &= \frac{|a|^2 + |b|^2 - 2\Re(\bar{a}be^{2i\theta}) - a\bar{b} + \bar{a}be^{2i\theta} + \bar{a}be^{-2i\theta} - a\bar{b}}{|1 - e^{2i\theta}|^2} \\ &= \frac{|a|^2 + |b|^2 - 2\Re(\bar{a}be^{2i\theta}) - 2\Re(a\bar{b}) + 2\Re(\bar{a}be^{2i\theta})}{|1 - e^{2i\theta}|^2} \\ &= \frac{|a|^2 + |b|^2 - 2\Re(a\bar{b})}{|1 - e^{2i\theta}|^2} = \frac{|b-a|^2}{|1 - e^{2i\theta}|^2} = \frac{|b-a|^2}{4 \sin^2(\theta)} \end{aligned}$$

L'équation (19.5) est donc celle du cercle de centre $\omega = \frac{a+b}{2} - i \cotan(\theta) \frac{b-a}{2}$ et de rayon $R = \frac{|b-a|}{2 |\sin(\theta)|}$.

L'ensemble \mathcal{E}_θ est donc le cercle de centre ω et de rayon R privé des points A et B . ■

Remarque 19.12 Les points A et B sont bien sur le cercle de centre ω et de rayon R puisque :

$$|a - \omega| = |b - \omega| = \left| \frac{b-a}{2} \right| |1 + i \cotan(\theta)| = R$$

Remarque 19.13 Le centre du cercle \mathcal{E}_θ , pour θ non congru à 0 modulo π , ayant une affixe de la forme $\omega = \frac{a+b}{2} + i\lambda'(b-a)$ est sur la droite passant par le milieu de $[AB]$ et perpendiculaire à la droite (AB) , c'est-à-dire sur la médiatrice du segment $[AB]$.

En particulier, pour $\theta = \frac{\pi}{2}$, on a $R = \frac{|b-a|}{2}$ et $\omega = \frac{a+b}{2}$ est l'affixe du milieu de $[A, B]$. L'ensemble :

$$\mathcal{E}_{\frac{\pi}{2}} = \left\{ M \in \mathcal{P} \setminus \{A, B\} \mid \left(\overrightarrow{MA}, \overrightarrow{MB} \right) \equiv \frac{\pi}{2} \ (\pi) \right\}$$

est donc le cercle de diamètre $[A, B]$ privé des points A et B .

Remarque 19.14 Au vu du résultat obtenu, il eut été judicieux d'utiliser le repère orthonormé direct $\mathcal{R}' = (O, \vec{e}_1, \vec{e}_2)$, où O est le milieu de $[AB]$ et \vec{e}_1 dirige la droite (AB) (ce repère est-il, a priori, si naturel que ça ?). Avec ce choix les affixes de A et B sont respectivement a' et $-a'$ avec a' réel non nul et le lieu géométrique :

$$\mathcal{E}_\theta = \left\{ M \in \mathcal{P} \setminus \{A, B\} \mid \left(\overrightarrow{MA}, \overrightarrow{MB} \right) \equiv \theta \ (\pi) \right\}$$

correspond à la ligne di niveau :

$$E_\theta = \left\{ z \in \mathbb{C} \setminus \{-a', a'\} \mid \arg \left(\frac{z - a'}{z + a'} \right) \equiv \theta \ (\pi) \right\}$$

On a alors :

$$\begin{aligned} \left(\arg \left(\frac{z - a'}{z + a'} \right) \equiv \theta \ (\pi) \right) &\Leftrightarrow \left(\frac{z - a'}{z + a'} = \frac{\bar{z} - a'}{\bar{z} + a'} e^{2i\theta} \right) \\ \Leftrightarrow (1 - e^{2i\theta}) z \bar{z} + a' (e^{2i\theta} + 1) z - a' (e^{2i\theta} + 1) \bar{z} - a'^2 (1 - e^{2i\theta}) &= 0 \\ \Leftrightarrow z \bar{z} + a' \frac{1 + e^{2i\theta}}{1 - e^{2i\theta}} z - a' \frac{1 + e^{2i\theta}}{1 - e^{2i\theta}} \bar{z} - a'^2 &= 0 \\ \Leftrightarrow z \bar{z} + ia' \cotan(\theta) z - ia' \cotan(\theta) \bar{z} - a'^2 &= 0 \\ \Leftrightarrow z \bar{z} - \bar{\omega} z - \omega \bar{z} + \gamma &= 0 \end{aligned}$$

avec $\omega = ia' \cotan(\theta)$ et $\gamma = -a'^2$. Et comme :

$$|\omega|^2 - \gamma = a'^2 (\cotan^2(\theta) + 1) = \frac{a'^2}{\sin^2(\theta)}$$

on reconnaît là le cercle centré en Ω d'affixe ω et de rayon $R = \frac{|a'|}{|\sin(\theta)|}$ avec $|a'| = OA =$

$$\frac{AB}{2} = \left| \frac{b-a}{2} \right|.$$

Remarque 19.15 Quand le point M sur le cercle \mathcal{E}_θ tend vers B , la droite (BM) devient tangente au cercle et cette tangente T_B fait un angle géométrique θ avec la droite (AB) .

On peut déduire du théorème 19.6 le critère de cocyclicité suivant.

Corollaire 19.1 Soient A, B, C, D des points deux à deux distincts. Ces points sont alignés ou cocycliques si, et seulement si, $\frac{c-b}{c-a} \frac{d-a}{d-b}$ est réel.

Démonstration. On a :

$$\begin{aligned} \left(\frac{c-b}{c-a} \frac{d-a}{d-b} \in \mathbb{R} \right) &\Leftrightarrow \left(\arg \left(\frac{c-b}{c-a} \frac{d-a}{d-b} \right) \equiv 0 \pmod{\pi} \right) \\ &\Leftrightarrow \left(\arg \left(\frac{d-b}{d-a} \right) \equiv \arg \left(\frac{c-b}{c-a} \right) \pmod{\pi} \right) \end{aligned}$$

On distingue alors deux cas.

Soit A, B, C sont alignés et dans ce cas $\arg \left(\frac{c-b}{c-a} \right) \equiv 0 \pmod{\pi}$, de sorte que :

$$\left(\frac{c-b}{c-a} \frac{d-a}{d-b} \in \mathbb{R} \right) \Leftrightarrow \left(\arg \left(\frac{d-b}{d-a} \right) \equiv 0 \pmod{\pi} \right) \Leftrightarrow (A, B, C, D \text{ alignés}).$$

Soit A, B, C ne sont pas alignés et dans ce cas $\arg \left(\frac{c-b}{c-a} \right) \equiv \theta \pmod{\pi}$ avec θ non congru à 0 modulo π , de sorte que :

$$\left(\frac{c-b}{c-a} \frac{d-a}{d-b} \in \mathbb{R} \right) \Leftrightarrow \left(\arg \left(\frac{d-b}{d-a} \right) \equiv \theta \pmod{\pi} \right) \Leftrightarrow (A, B, C, D \text{ cocycliques}).$$

■

Théorème 19.7 Soient a, b deux nombres complexes distincts et θ un nombre réel. L'ensemble :

$$\left\{ z \in \mathbb{C} \setminus \{a, b\} \mid \arg \left(\frac{z-a}{z-b} \right) \equiv \theta \pmod{2\pi} \right\}$$

est la droite (AB) privée du segment $[AB]$ si $\theta \equiv 0 \pmod{2\pi}$, le segment $[AB]$ privé de A et B si $\theta \equiv \pi \pmod{2\pi}$, ou un arc de cercle d'extrémités A, B privé de ces points (arc capable), si θ n'est pas congru à 0 modulo π .

En utilisant l'inégalité triangulaire avec son cas d'égalité dans \mathbb{C} , on a le résultat suivant.

Théorème 19.8 (Ptolémée) Soient A, B, C, D des points deux à deux distincts. Le quadrilatère convexe $ABCD$ est inscriptible dans un cercle si, et seulement si, $AC \cdot BD = AB \cdot CD + AD \cdot BC$ (le produit des diagonales est égal à la somme des produits des cotés opposés).

Démonstration. Dans tous les cas, on a :

$$\begin{aligned} AC \cdot BD &= |(c-a)(d-b)| \\ &= |(b-a)(d-c) + (d-a)(c-b)| \\ &\leq |(b-a)(d-c)| + |(d-a)(c-b)| = AB \cdot CD + AD \cdot BC \end{aligned}$$

(inégalité de Ptolémée) l'égalité étant réalisée si, et seulement si, il existe un réel $\lambda > 0$ tel que :

$$(b-a)(d-c) = \lambda (d-a)(c-b)$$

ce qui équivaut à $\frac{b-a}{d-a} \frac{d-c}{b-c} = -\lambda \in \mathbb{R}^{*, -}$ qui est encore équivalent à :

$$\arg \left(\frac{b-a}{d-a} \frac{d-c}{b-c} \right) \equiv \pi \pmod{2\pi}$$

ou à :

$$\arg\left(\frac{b-a}{d-a}\right) - \arg\left(\frac{b-c}{d-c}\right) \equiv \pi \pmod{2\pi}$$

et entraîne :

$$\arg\left(\frac{b-a}{d-a}\right) \equiv \arg\left(\frac{b-c}{d-c}\right) \pmod{\pi}$$

soit :

$$(\overrightarrow{AB}, \overrightarrow{AD}) \equiv (\overrightarrow{CB}, \overrightarrow{CD}) \pmod{\pi}$$

et A, B, C, D sont cocycliques.

Réciproquement si ces points sont cocycliques, on a :

$$\arg\left(\frac{b-a}{d-a}\right) \equiv \arg\left(\frac{b-c}{d-c}\right) \pmod{\pi}$$

donc $\mu = \frac{b-a}{d-a} \frac{d-c}{b-c} \in \mathbb{R}$. Si $\mu > 0$, alors $(\overrightarrow{AB}, \overrightarrow{AD}) \equiv (\overrightarrow{CB}, \overrightarrow{CD}) \pmod{2\pi}$ et les points A, C sont dans le même demi-plan délimité par la droite (BD) , ce qui contredit le fait que $ABCD$ est convexe. On a donc $\mu < 0$ et $(b-a)(d-c) = \lambda(d-a)(c-b)$ avec $\lambda > 0$, ce qui entraîne l'égalité dans l'inégalité de Ptolémée. ■

19.8 Le triangle dans le plan complexe

Définition 19.1 On appelle *vrai triangle* dans le plan \mathcal{P} , la donnée de trois points non alignés A, B, C .

Si $T = ABC$ est un vrai triangle, on notera :

$$\theta_A = (\overrightarrow{AB}, \overrightarrow{AC}), \quad \theta_B = (\overrightarrow{BC}, \overrightarrow{BA}), \quad \theta_C = (\overrightarrow{CA}, \overrightarrow{CB})$$

les mesures principales des angles orientés de vecteurs en A, B et C respectivement (figure 20).

FIGURE 19.7 –

Usuellement, on note respectivement a, b, c les cotés opposés à A, B, C (à ne pas confondre avec les abscisses).

19.8.1 Relations trigonométriques pour un triangle

Lemme 19.2 Si $T = ABC$ est un vrai triangle, on a alors :

$$\det(\overrightarrow{AB}, \overrightarrow{AC}) = \det(\overrightarrow{CA}, \overrightarrow{CB}) = \det(\overrightarrow{BC}, \overrightarrow{BA}) \quad (19.6)$$

Démonstration. En utilisant les propriétés du déterminant, on a :

$$\det(\overrightarrow{AB}, \overrightarrow{AC}) = \det(\overrightarrow{AC} + \overrightarrow{CB}, \overrightarrow{AC}) = \det(\overrightarrow{CB}, \overrightarrow{AC}) = \det(\overrightarrow{CA}, \overrightarrow{CB})$$

et :

$$\det(\overrightarrow{AB}, \overrightarrow{AC}) = \det(\overrightarrow{AB}, \overrightarrow{AB} + \overrightarrow{BC}) = \det(\overrightarrow{AB}, \overrightarrow{BC}) = \det(\overrightarrow{BC}, \overrightarrow{BA}).$$

■

Définition 19.2 On dit que le triangle T est orienté positivement [resp. négativement] ou qu'il est direct [resp. indirect] relativement au repère \mathcal{R} , si $\det(\overrightarrow{AB}, \overrightarrow{AC}) > 0$ [resp. $\det(\overrightarrow{AB}, \overrightarrow{AC}) < 0$].

Du lemme précédent et des relations :

$$\sin(\theta_A) = \frac{\det(\overrightarrow{AB}, \overrightarrow{AC})}{AB \cdot AC}, \quad \sin(\theta_B) = \frac{\det(\overrightarrow{BC}, \overrightarrow{BA})}{BC \cdot BA}, \quad \sin(\theta_C) = \frac{\det(\overrightarrow{CA}, \overrightarrow{CB})}{CA \cdot CB} \quad (19.7)$$

on déduit que les quantités $\sin(\theta_A)$, $\sin(\theta_B)$ et $\sin(\theta_C)$ sont toutes de même signes. Les déterminations principales de ces mesures d'angle seront donc tous dans $]0, \pi[$ pour T direct ou toutes dans $]-\pi, 0[$ pour T indirect.

Lemme 19.3 Si $T = ABC$ est un vrai triangle, on a alors :

$$\theta_A + \theta_B + \theta_C \equiv \pi \pmod{2\pi}$$

Démonstration. En utilisant la relation de Chasles pour les angles orientés, on a :

$$\begin{aligned} \theta_A + \theta_B + \theta_C &= (\overrightarrow{AB}, \overrightarrow{AC}) + (\overrightarrow{AC}, \overrightarrow{BC}) + (\overrightarrow{BC}, \overrightarrow{BA}) \\ &= (\overrightarrow{AB}, \overrightarrow{BC}) + (\overrightarrow{BC}, \overrightarrow{BA}) \\ &= (\overrightarrow{AB}, \overrightarrow{BA}) \equiv \pi \pmod{2\pi} \end{aligned}$$

■

Pour un vrai triangle direct [resp. indirect] les déterminations principales de ces angles sont toutes dans $]0, \pi[$ [resp. dans $]-\pi, 0[$], donc la somme est dans $]0, 3\pi[$ [resp. dans $]-3\pi, 0[$] congrue à π modulo 2π et en conséquence est égale à π [resp. $-\pi$].

On a donc $\theta_A + \theta_B + \theta_C = \pi$ pour un triangle direct et $\theta_A + \theta_B + \theta_C = -\pi$ pour un triangle indirect.

Des relations (19.7) et (19.6) on déduit que :

$$AB \cdot AC \sin(\theta_A) = BC \cdot BA \sin(\theta_B) = CA \cdot CB \sin(\theta_C)$$

ce qui donne :

$$\frac{BC}{\sin(\theta_A)} = \frac{AC}{\sin(\theta_B)} = \frac{AB}{\sin(\theta_C)} \quad (19.8)$$

ou encore avec les notations usuelles :

$$\frac{a}{\sin(\theta_A)} = \frac{b}{\sin(\theta_B)} = \frac{c}{\sin(\theta_C)}.$$

Pour T direct rectangle en A , on a :

$$\cos(\theta_A) = \frac{\overrightarrow{AB} \cdot \overrightarrow{AC}}{AB \cdot AC} = 0$$

avec $\theta_A \in]0, \pi[$, donc $\theta_A = \frac{\pi}{2}$.

De plus, avec :

$$\overrightarrow{BC} \cdot \overrightarrow{BA} = (\overrightarrow{BA} + \overrightarrow{AC}) \cdot \overrightarrow{BA} = BA^2$$

$$\begin{aligned} \det(\overrightarrow{BC}, \overrightarrow{BA}) &= \det(\overrightarrow{AB}, \overrightarrow{AC}) = AB \cdot AC \sin(\theta_A) \\ &= AB \cdot AC \sin\left(\frac{\pi}{2}\right) = AB \cdot AC \end{aligned}$$

on déduit que :

$$\cos(\theta_B) = \frac{\overrightarrow{BC} \cdot \overrightarrow{BA}}{BC \cdot BA} = \frac{BA^2}{BC \cdot BA} = \frac{BA}{BC}$$

(coté adjacent à l'angle droit sur l'hypoténuse) et :

$$\sin(\theta_B) = \frac{\det(\overrightarrow{BC}, \overrightarrow{BA})}{BC \cdot BA} = \frac{AB \cdot AC}{BC \cdot BA} = \frac{AC}{BC}$$

(coté opposé à l'angle droit sur l'hypoténuse), ce qui donne aussi :

$$\tan(\theta_B) = \frac{\sin(\theta_B)}{\cos(\theta_B)} = \frac{AC}{AB}$$

(coté opposé à l'angle droit sur coté adjacent).

Dans le cas où le triangle direct T est isocèle en A , on a $AB = AC$, donc A est sur la médiatrice du segment $[BC]$ et en désignant par I le milieu de ce segment, on peut écrire pour les triangles rectangles en I , AIC et AIB :

$$\cos(\theta_B) = \frac{IB}{AB} = \frac{IC}{AC} = \cos(\theta_C)$$

avec θ_B et θ_C dans $]0, \pi[$, ce qui équivaut à $\theta_B = \theta_C$ et entraîne $\theta_A = \pi - 2\theta_B$.

Réciproquement si $\theta_B = \theta_C$, de $\frac{AC}{\sin(\theta_B)} = \frac{AB}{\sin(\theta_C)}$ (formule (19.8)), on déduit que $AB = AC$ et T est isocèle en A .

Pour un triangle direct quelconque T , en écrivant que :

$$\|\overrightarrow{CB}\|^2 = \|\overrightarrow{AB} - \overrightarrow{AC}\|^2 = \|\overrightarrow{AB}\|^2 - 2\overrightarrow{AB} \cdot \overrightarrow{AC} + \|\overrightarrow{AC}\|^2$$

on déduit que :

$$CB^2 = AB^2 - 2AB \cdot AC \cos(\theta_A) + AC^2.$$

ou encore en utilisant les notations usuelles :

$$a^2 = b^2 + c^2 - 2bc \cos(\theta_A).$$

Pour T rectangle en A , on a $\theta_A = \frac{\pi}{2}$ et on retrouve le théorème de Pythagore.

Par permutations circulaires des sommets, on a les deux autres formules :

$$b^2 = c^2 + a^2 - 2ca \cos(\theta_B)$$

et :

$$c^2 = a^2 + b^2 - 2ab \cos(\theta_C).$$

19.8.2 Aire d'un triangle

Définition 19.3 *L'aire d'un triangle $T = ABC$ est le réel :*

$$m(T) = \frac{1}{2} \left| \det \left(\overrightarrow{AB}, \overrightarrow{AC} \right) \right|.$$

En prenant pour origine du repère \mathcal{R} le projeté H du point A sur la droite (BC) , le vecteur $\overrightarrow{e_1}$ dirigeant cette droite (BC) , on a :

$$\begin{cases} \overrightarrow{AB} = \overrightarrow{HB} - \overrightarrow{HA} = x_B \overrightarrow{e_1} - y_A \overrightarrow{e_2} \\ \overrightarrow{AC} = \overrightarrow{HC} - \overrightarrow{HA} = x_C \overrightarrow{e_1} - y_A \overrightarrow{e_2} \end{cases}$$

de sorte que :

$$\det \left(\overrightarrow{AB}, \overrightarrow{AC} \right) = \begin{vmatrix} x_B & x_C \\ -y_A & -y_A \end{vmatrix} = y_A (x_C - x_B)$$

et :

$$m(T) = \frac{1}{2} |y_A| |x_C - x_B| = \frac{AH \cdot BC}{2}$$

soit la formule : « base que multiplie hauteur divisé par 2 ».

Pour un triangle direct, on a :

$$m(T) = \frac{1}{2} \det \left(\overrightarrow{AB}, \overrightarrow{AC} \right) = \frac{1}{2} AB \cdot AC \sin(\theta_A)$$

et pour un triangle indirect, on a :

$$m(T) = -\frac{1}{2} \det \left(\overrightarrow{AB}, \overrightarrow{AC} \right) = -\frac{1}{2} AB \cdot AC \sin(\theta_A)$$

en notant θ_A la détermination principale de l'angle en A .

On retrouve l'aire d'un triangle T rectangle en A , $m(T) = \frac{1}{2} AB \cdot AC$.

Réciproquement si $m(T) = \frac{1}{2} AB \cdot AC$, on a alors $\sin(\theta_A) = \pm 1$, soit $\theta_A = \pm \frac{\pi}{2}$ (suivant que T est direct ou non) et T est rectangle en A .

Pour un triangle direct, en utilisant la formule (19.8), on obtient :

$$2 \frac{m(T)}{AB \cdot AC \cdot BC} = \frac{\sin(\theta_A)}{BC} = \frac{\sin(\theta_B)}{AC} = \frac{\sin(\theta_C)}{AB}$$

qui s'écrit aussi avec des notations usuelles :

$$2 \frac{m(T)}{abc} = \frac{\sin(\theta_A)}{a} = \frac{\sin(\theta_B)}{b} = \frac{\sin(\theta_C)}{c}$$

($a = BC, \dots$).

Dans un repère orthonormé \mathcal{R} quelconque, en utilisant les propriétés du déterminant, on peut écrire que :

$$\begin{aligned} \det(\overrightarrow{AB}, \overrightarrow{AC}) &= \begin{vmatrix} x_B - x_A & x_C - x_A \\ y_B - y_A & y_C - y_A \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ x_A & x_B - x_A & x_C - x_A \\ y_A & y_B - y_A & y_C - y_A \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & 1 \\ x_A & x_B & x_C \\ y_A & y_B & y_C \end{vmatrix} = \begin{vmatrix} x_A & y_A & 1 \\ x_B & y_B & 1 \\ x_C & y_C & 1 \end{vmatrix} \end{aligned}$$

et en désignant par a, b, c les affixes relatives au repère \mathcal{R} des points A, B, C , cela s'écrit aussi :

$$\begin{aligned} \det(\overrightarrow{AB}, \overrightarrow{AC}) &= \begin{vmatrix} x_A & y_A & 1 \\ x_B & y_B & 1 \\ x_C & y_C & 1 \end{vmatrix} = \begin{vmatrix} \frac{a+\bar{a}}{2} & \frac{a-\bar{a}}{2i} & 1 \\ \frac{b+\bar{b}}{2} & \frac{b-\bar{b}}{2i} & 1 \\ \frac{c+\bar{c}}{2} & \frac{c-\bar{c}}{2i} & 1 \end{vmatrix} \\ &= \frac{1}{4i} \begin{vmatrix} a+\bar{a} & a-\bar{a} & 1 \\ b+\bar{b} & b-\bar{b} & 1 \\ c+\bar{c} & c-\bar{c} & 1 \end{vmatrix} = \frac{1}{4i} \begin{vmatrix} 2a & a-\bar{a} & 1 \\ 2b & b-\bar{b} & 1 \\ 2c & c-\bar{c} & 1 \end{vmatrix} \\ &= \frac{1}{2i} \begin{vmatrix} a & a-\bar{a} & 1 \\ b & b-\bar{b} & 1 \\ c & c-\bar{c} & 1 \end{vmatrix} = -\frac{1}{2i} \begin{vmatrix} a & \bar{a} & 1 \\ b & \bar{b} & 1 \\ c & \bar{c} & 1 \end{vmatrix} \end{aligned}$$

et :

$$m(T) = \pm \frac{1}{4i} \det \begin{pmatrix} a & \bar{a} & 1 \\ b & \bar{b} & 1 \\ c & \bar{c} & 1 \end{pmatrix}$$

le signant \pm étant celui qui assure la positivité de $m(T)$.

En calculant ce déterminant, on a :

$$\begin{aligned} \det \begin{pmatrix} a & \bar{a} & 1 \\ b & \bar{b} & 1 \\ c & \bar{c} & 1 \end{pmatrix} &= \det \begin{pmatrix} a & \bar{a} & 1 \\ b-a & \bar{b}-\bar{a} & 0 \\ c-a & \bar{c}-\bar{a} & 0 \end{pmatrix} \\ &= \det \begin{pmatrix} b-a & \bar{b}-\bar{a} \\ c-a & \bar{c}-\bar{a} \end{pmatrix} = (b-a)(\bar{c}-\bar{a}) - (\bar{b}-\bar{a})(c-a) \\ &= 2i\Im((b-a)(\bar{c}-\bar{a})) \end{aligned}$$

et on obtient la formule :

$$m(T) = \pm \frac{1}{2} \Im((b-a)(\bar{c}-\bar{a})) \quad (19.9)$$

En traduisant le fait que M est sur la droite (AB) si, et seulement si, l'aire du triangle ABM est nulle, on en déduit l'équation complexe suivante de la droite (AB) :

$$(M \in (AB)) \Leftrightarrow \left(\det \begin{pmatrix} a & \bar{a} & 1 \\ b & \bar{b} & 1 \\ z & \bar{z} & 1 \end{pmatrix} = 0 \right)$$

En utilisant l'expression (19.9) de $m(T)$, on retrouve la condition :

$$(M \in (AB)) \Leftrightarrow (\Im((\bar{b} - \bar{a})(z - a)) = 0)$$

ce qui est encore équivalent à dire que $(b - a)(\overline{c - a})$ est réel.

Cette formule (19.9) nous donne aussi le résultat suivant.

Théorème 19.9 *Si $T = ABC$ est un vrai triangle, on a alors :*

$$m(T) \leq \frac{1}{2} AB \cdot AC$$

l'égalité étant réalisée si, et seulement si, le triangle T est rectangle en A .

Démonstration. On a :

$$\begin{aligned} m(T) &= \frac{1}{2} |\Im((b - a)(\bar{c} - \bar{a}))| \\ &\leq \frac{1}{2} |b - a| |c - a| = \frac{1}{2} AB \cdot AC \end{aligned}$$

l'égalité étant réalisée si, et seulement si, $(b - a)(\bar{c} - \bar{a})$ est imaginaire pur, ce qui équivaut à dire que les droites (AB) et (AC) sont perpendiculaires. ■

19.8.3 Centre de gravité d'un triangle

Si $T = ABC$ est un vrai triangle, la médiane issue de A est la droite \mathcal{M}_A qui joint les points A et le milieu I_A du segment $[BC]$.

Théorème 19.10 *Les trois médianes d'un vrai triangle $T = ABC$ concourent en G d'affixe $\frac{a + b + c}{3}$.*

Démonstration. L'affixe du milieu I_A de $[BC]$ étant $\frac{b + c}{2}$, une équation de la médiane \mathcal{M}_A est :

$$\det \begin{pmatrix} a & \bar{a} & 1 \\ \frac{b+c}{2} & \frac{\bar{b}+\bar{c}}{2} & 1 \\ z & \bar{z} & 1 \end{pmatrix} = 0$$

soit :

$$\det \begin{pmatrix} a & \bar{a} & 1 \\ \frac{b+c-2a}{2} & \frac{\bar{b}+\bar{c}-2\bar{a}}{2} & 0 \\ z - a & \bar{z} - \bar{a} & 0 \end{pmatrix} = 0$$

ou encore :

$$\det \begin{pmatrix} b + c - 2a & \bar{b} + \bar{c} - 2\bar{a} \\ z - a & \bar{z} - \bar{a} \end{pmatrix}.$$

On constate que $z = \frac{a + b + c}{3}$ est solution de cette équation ($z - a = \frac{1}{3}(b + c - 2a)$).

Définissant de manière analogue les médianes en B et C , on constate encore que le point G d'affixe $\frac{a + b + c}{3}$ est sur ces médianes. ■

Définition 19.4 *Avec les notations du théorème qui précède, on dit que le point G d'affixe $\frac{a + b + c}{3}$ est le centre de gravité du triangle.*

Le centre de gravité est aussi l'iso-barycentre des points A, B, C .

19.8.4 Cercle circonscrit à un triangle

Si A, B, C sont trois points non alignés, alors $\theta = \arg \left(\frac{a-c}{b-c} \right)$ n'est pas congru à 0 modulo π et ces points sont sur le cercle $\mathcal{E}_\theta \cup \{A, B\}$, où :

$$\mathcal{E}_\theta = \left\{ M \in \mathcal{P} \setminus \{A, B\} \mid \left(\overrightarrow{MA}, \overrightarrow{MB} \right) \equiv \theta \pmod{\pi} \right\}$$

Ce cercle, qui est uniquement déterminé, est le cercle circonscrit au triangle $T = ABC$ et son centre Ω est à l'intersection des trois médiatrices de T .

Un point M est sur ce cercle circonscrit à T si, et seulement si :

$$\arg \left(\frac{a-z}{b-z} \right) \equiv \arg \left(\frac{a-c}{b-c} \right) \pmod{\pi}$$

ce qui est encore équivalent à :

$$\left(\overrightarrow{MA}, \overrightarrow{MB} \right) \equiv \left(\overrightarrow{CA}, \overrightarrow{CB} \right) \pmod{\pi} \quad (19.10)$$

c'est ce qu'on appelle l'équation angulaire du cercle passant par A, B, C .

L'utilisation de la relation de Chasles pour les angles orientés de vecteurs nous permet de montrer le théorème de l'angle inscrit qui suit.

Théorème 19.11 *Soient $T = ABC$ un vrai triangle et Ω le centre du cercle circonscrit à ce triangle. On a alors :*

$$2 \left(\overrightarrow{AB}, \overrightarrow{AC} \right) \equiv \left(\overrightarrow{\Omega B}, \overrightarrow{\Omega C} \right) \pmod{2\pi}$$

Démonstration. En utilisant la relation de Chasles, on a :

$$\left(\overrightarrow{\Omega B}, \overrightarrow{\Omega C} \right) + \left(\overrightarrow{\Omega C}, \overrightarrow{\Omega A} \right) + \left(\overrightarrow{\Omega A}, \overrightarrow{\Omega B} \right) \equiv \left(\overrightarrow{\Omega B}, \overrightarrow{\Omega B} \right) \equiv 0 \pmod{2\pi}$$

Comme les triangles ΩAB et ΩAC sont isocèles en Ω , on a :

$$2 \left(\overrightarrow{AB}, \overrightarrow{A\Omega} \right) + \left(\overrightarrow{\Omega A}, \overrightarrow{\Omega B} \right) \equiv \pi \pmod{2\pi}$$

et :

$$2 \left(\overrightarrow{A\Omega}, \overrightarrow{AC} \right) + \left(\overrightarrow{\Omega C}, \overrightarrow{\Omega A} \right) \equiv \pi \pmod{2\pi}$$

ce qui donne par addition :

$$2 \left(\left(\overrightarrow{AB}, \overrightarrow{A\Omega} \right) + \left(\overrightarrow{A\Omega}, \overrightarrow{AC} \right) \right) + \left(\overrightarrow{\Omega A}, \overrightarrow{\Omega B} \right) + \left(\overrightarrow{\Omega C}, \overrightarrow{\Omega A} \right) \equiv 0 \pmod{2\pi}$$

soit :

$$2 \left(\overrightarrow{AB}, \overrightarrow{AC} \right) + \left(\overrightarrow{\Omega A}, \overrightarrow{\Omega B} \right) + \left(\overrightarrow{\Omega C}, \overrightarrow{\Omega A} \right) \equiv 0 \pmod{2\pi}$$

ou encore :

$$2 \left(\overrightarrow{AB}, \overrightarrow{AC} \right) - \left(\overrightarrow{\Omega B}, \overrightarrow{\Omega C} \right) \equiv 0 \pmod{2\pi}$$

■

FIGURE 19.8 – Théorème de l'angle inscrit

19.8.5 Orthocentre d'un triangle

La caractérisation complexe de l'orthogonalité de deux droites nous permet de retrouver la définition de l'orthocentre d'un triangle.

Lemme 19.4 Soit $T = ABC$ un vrai triangle. Un point M est sur la hauteur issue de A de T si, et seulement si, son affixe z est telle que $(z - a)(\bar{c} - \bar{b})$ (ou de manière équivalente $\frac{z - a}{c - b}$) soit imaginaire pur.

Démonstration. Si $M = A$, on a $z = a$ et $(z - a)(\bar{c} - \bar{b}) = 0$ est bien imaginaire pur.

Sinon M est sur la hauteur issue de A si, et seulement si les droites (AM) et (BC) sont orthogonales, ce qui équivaut à $(z - a)(\bar{c} - \bar{b})$ imaginaire pur, qui est encore équivalent à dire que $\frac{z - a}{c - b}$ est imaginaire pur. ■

Lemme 19.5 Soient a, b, c des nombres complexes deux à deux distincts. Pour tout $z \in \mathbb{C}$, le nombre complexe

$$Z = (z - a)(\bar{c} - \bar{b}) + (z - b)(\bar{a} - \bar{c}) + (z - c)(\bar{b} - \bar{a})$$

est imaginaire pur.

Démonstration. Résulte de :

$$\begin{aligned}(z-c)(\bar{b}-\bar{a}) &= (z-a)(\bar{b}-\bar{a}) + (a-c)(\bar{b}-\bar{a}) \\ &= (z-a)(\bar{b}-\bar{c}) + (z-a)(\bar{c}-\bar{a}) + (a-c)(\bar{b}-\bar{a}) \\ &= (z-a)(\bar{b}-\bar{c}) + (z-b)(\bar{c}-\bar{a}) + (b-a)(\bar{c}-\bar{a}) + (a-c)(\bar{b}-\bar{a}) \\ &= -(z-a)(\bar{c}-\bar{b}) - (z-b)(\bar{a}-\bar{c}) + 2i\Im((b-a)(\bar{c}-\bar{a}))\end{aligned}$$

qui s'écrit :

$$Z = 2i\Im((b-a)(\bar{c}-\bar{a}))$$

■

Le fait que Z soit imaginaire pur se traduit par $\Re(Z) = 0$, soit par :

$$\Re((z-a)(\bar{c}-\bar{b})) + \Re((z-b)(\bar{a}-\bar{c})) + \Re((z-c)(\bar{b}-\bar{a})) = 0$$

ou encore par :

$$\overrightarrow{AM} \cdot \overrightarrow{BC} + \overrightarrow{BM} \cdot \overrightarrow{CA} + \overrightarrow{CM} \cdot \overrightarrow{AB} = 0$$

pour tout point $M \in \mathcal{P}$.

Cette égalité est l'égalité de Wallace.

Lemme 19.6 Soient a, b, c des nombres complexes deux à deux distincts et z un nombre complexe. Si deux quantités parmi $(z-a)(\bar{c}-\bar{b})$, $(z-b)(\bar{a}-\bar{c})$, $(z-c)(\bar{b}-\bar{a})$ sont imaginaires pures, il en est alors de même de la troisième.

Démonstration. Résulte du lemme précédent. ■

Théorème 19.12 Soit $T = ABC$ un vrai triangle. Les trois hauteurs de T sont concourantes.

Démonstration. Notons respectivement T_A , T_B et T_C les hauteurs issues de A , B et C .

Un point M est sur $T_A \cap T_B$ si, et seulement si, les quantités $(z-a)(\bar{c}-\bar{b})$ et $(z-b)(\bar{a}-\bar{c})$ sont imaginaires pures, ce qui entraîne que $(z-c)(\bar{b}-\bar{a})$ est aussi imaginaire pur et M est sur T_C .

Les trois hauteurs sont donc concourantes. ■

Le point d'intersection des trois hauteurs du triangle T est l'orthocentre de T .

Exercice 19.3 Soit $T = ABC$ un vrai triangle. Montrer que l'orthocentre H de T a pour affixe relativement au repère $\mathcal{R} = (O, \vec{e}_1, \vec{e}_2)$:

$$\begin{aligned}h &= a + i \frac{\Re((a-b)(\overline{c-a}))}{\Im((c-b)(\overline{c-a}))} (c-b) \\ &= a + i \frac{\Re\left(\frac{a-b}{c-a}\right)}{\Im\left(\frac{c-b}{c-a}\right)} (c-b)\end{aligned}$$

Solution 19.3 Comme $H \in T_A \cap T_B$, il existe deux réels λ_1 et λ_2 tels que :

$$h = a + i\lambda_1(c-b) = b + i\lambda_2(c-a)$$

ce qui entraîne :

$$i\lambda_2 = \frac{a-b}{c-a} + i\lambda_1 \frac{c-b}{c-a}$$

FIGURE 19.9 – Orthocentre

et en prenant les parties réelles :

$$0 = \Re\left(\frac{a-b}{c-a}\right) + \lambda_1 \Re\left(i \frac{c-b}{c-a}\right) = \Re\left(\frac{a-b}{c-a}\right) - \lambda_1 \Im\left(\frac{c-b}{c-a}\right)$$

Comme les points C, A, B ne sont pas alignés, $\frac{c-a}{c-b} = \frac{a-c}{b-c}$ n'est pas réel et λ_1 est uniquement déterminé. On a donc :

$$\lambda_1 = \frac{\Re\left(\frac{a-b}{c-a}\right)}{\Im\left(\frac{c-b}{c-a}\right)} = \frac{\Re((a-b)(\overline{c-a}))}{\Im((c-b)(\overline{c-a}))}.$$

et :

$$\begin{aligned} h &= a + i \frac{\Re((a-b)(\overline{c-a}))}{\Im((c-b)(\overline{c-a}))} (c-b) \\ &= a + i \frac{\Re\left(\frac{a-b}{c-a}\right)}{\Im\left(\frac{c-b}{c-a}\right)} (c-b) \end{aligned}$$

Par exemple, pour a, b réels et $c = i\gamma$ imaginaire pur, on a :

$$\frac{\Re((a-b)(\overline{c-a}))}{\Im((c-b)(\overline{c-a}))} = \frac{a}{\gamma}$$

et :

$$h = -i \frac{ab}{\gamma} = \frac{ab}{c}.$$

En fait, pour déterminer une affixe de l'orthocentre, il est plus commode de travailler dans un repère d'origine $O = \Omega$ où Ω est le centre du cercle circonscrit au triangle.

Exercice 19.4 Montrer que si ABC est un triangle inscrit dans le cercle de centre Ω et de rayon $R > 0$, alors l'affixe de son orthocentre est $h = a + b + c$. (Ω étant pris comme origine).

Solution 19.4 On désigne par M le point d'affixe $h = a + b + c$. Comme $h - a = b + c$ avec $|b| = |c| = R$, on a $\overrightarrow{AM} = \overrightarrow{\Omega B} + \overrightarrow{\Omega C}$ et ce vecteur est orthogonal à $\overrightarrow{CB} = \overrightarrow{\Omega B} - \overrightarrow{\Omega C}$, $(\overrightarrow{\Omega B} + \overrightarrow{\Omega C}) \cdot (\overrightarrow{\Omega B} - \overrightarrow{\Omega C}) = \Omega B^2 - \Omega C^2 = R^2 - R^2 = 0$, ce qui équivaut à dire que $(h - a)(\overline{b - c})$ est imaginaire pur, qui est encore équivalent à dire que M est sur la hauteur de T issue de A .

On montre de manière analogue que M est sur les deux autres hauteurs et en conséquence c'est l'orthocentre de T .

En utilisant les affixes relativement au repère $(\Omega, \vec{e}_1, \vec{e}_2)$, le théorème 19.10 nous dit que le centre de gravité G a pour affixe $g = \frac{a + b + c}{3}$ et l'exercice 19.4 que l'orthocentre a pour affixe $h = a + b + c$, ce qui se traduit par :

$$\overrightarrow{\Omega H} = 3\overrightarrow{\Omega G}$$

et entraîne que ces trois points sont alignés.

Théorème 19.13 Dans un vrai triangle T , le centre du cercle circonscrit, l'orthocentre et le centre de gravité sont alignés.

La droite passant par ces trois points est la droite d'Euler.

19.8.6 Triangle équilatéral

Théorème 19.14 Soient A, B, C trois points deux à deux distincts de \mathcal{P} et a, b, c leurs affixes respectives. Les propositions suivantes sont équivalentes :

1. le triangle ABC est équilatéral ;
2. $|b - a| = |c - b| = |a - c|$;
3. $\frac{1}{a - b} + \frac{1}{b - c} + \frac{1}{c - a} = 0$;
4. $a^2 + b^2 + c^2 = ab + bc + ca$;
5. j ou \bar{j} est racine de $az^2 + bz + c = 0$ (j et \bar{j} sont les racines cubiques de l'unité).
6. j ou \bar{j} est racine de $\det \begin{pmatrix} a & z^2 & 1 \\ b & z & 1 \\ c & 1 & 1 \end{pmatrix} = 0$.

Démonstration. L'équivalence entre 1. et 2. résulte de la définition d'un triangle équilatéral. Supposons que $|a - b| = |b - c| = |c - a|$.

On a :

$$\begin{aligned} \frac{1}{a-b} &= \frac{\bar{a}-\bar{b}}{|a-b|^2} = \frac{\bar{a}-\bar{b}}{|b-c|^2} = \frac{1}{b-c} \frac{\bar{a}-\bar{b}}{\bar{b}-\bar{c}} \\ &= \frac{1}{b-c} \frac{\bar{a}-\bar{c}+\bar{c}-\bar{b}}{\bar{b}-\bar{c}} = \frac{1}{b-c} \left(\frac{\bar{a}-\bar{c}}{\bar{b}-\bar{c}} - 1 \right) \end{aligned}$$

avec $\frac{\bar{a}-\bar{c}}{\bar{b}-\bar{c}} = \frac{b-c}{a-c}$ puisque $\left| \frac{\bar{a}-\bar{c}}{\bar{b}-\bar{c}} \right| = \left| \frac{a-c}{b-c} \right| = 1$, donc :

$$\begin{aligned} \frac{1}{a-b} &= \frac{1}{b-c} \left(\frac{b-c}{a-c} - 1 \right) = \frac{1}{b-c} \frac{b-c}{a-c} - \frac{1}{b-c} \\ &= \frac{1}{a-c} - \frac{1}{b-c} \end{aligned}$$

et $\frac{1}{a-b} + \frac{1}{b-c} + \frac{1}{c-a} = 0$.

Supposons cette dernière identité réalisée. On a alors en multipliant par $(a-b)(b-c)(c-a)$:

$$(b-c)(c-a) + (a-b)(c-a) + (a-b)(b-c) = 0$$

et en développant, cela est équivalent à :

$$ab + bc + ca - a^2 - b^2 - c^2 = 0.$$

En supposant cette identité vérifiée, on a :

$$(aj^2 + bj + c)(a\bar{j}^2 + b\bar{j} + c) = a^2 + b^2 + c^2 + (j + \bar{j})ab + (j^2 + \bar{j}^2)ac + (j + \bar{j})bc$$

avec $j^2 + \bar{j}^2 = \bar{j} + j = -1$, ce qui donne :

$$(aj^2 + bj + c)(a\bar{j}^2 + b\bar{j} + c) = 0$$

et j ou \bar{j} est racine de $az^2 + bz + c = 0$.

Supposons que j soit racine de $az^2 + bz + c = 0$. Tenant compte de $1 + j + j^2 = 0$, on a alors :

$$0 = aj^2 + bj + c = aj^2 + bj - c(j + j^2) = (b-c)j + (a-c)j^2$$

et $(b-c)j = -(a-c)j^2$ qui entraîne $|b-c| = |c-a|$. On peut aussi écrire :

$$0 = aj^2 + bj + c = aj^2 - b(1 + j^2) + c = (c-b) + (a-b)j^2$$

et on a $(c-b) = -(a-b)j^2$ qui entraîne $|a-b| = |c-b|$.

L'équivalence entre **5.** et **6.** se déduit du calcul suivant. Pour $z \in \{j, \bar{j}\} = \{j, j^2\}$:

$$\begin{aligned} \det \begin{pmatrix} a & z^2 & 1 \\ b & z & 1 \\ c & 1 & 1 \end{pmatrix} &= \det \begin{pmatrix} a-b & z^2-z & 0 \\ b-c & z-1 & 0 \\ c & 1 & 1 \end{pmatrix} = \det \begin{pmatrix} a-b & z^2-z \\ b-c & z-1 \end{pmatrix} \\ &= az + b + cz^2 - (a + bz^2 + cz) \\ &= \bar{z}(az^2 + bz + c) - z(az^2 + bz + c) \\ &= (z - \bar{z})(az^2 + bz + c) = 2i\Im(z)(az^2 + bz + c). \end{aligned}$$

■

Nous verrons un peu plus loin que la caractérisation **6.** des triangles équilatéraux traduit le fait qu'un triangle équilatéral est semblable à un triangle ayant pour sommets les points d'affixes $1, z, z^2$ avec $z = j$ ou $z = \bar{j}$.

19.9 Interprétation géométrique des applications $z \mapsto az + b$, $z \mapsto a\bar{z} + b$

Les nombres complexes peuvent être utilisés pour décrire quelques transformations géométriques de \mathcal{P} . Ainsi :

- $z \mapsto z + a$ est la translation de vecteur \overrightarrow{OA} ;
- $z \mapsto -z$ est la symétrie par rapport à O ;
- $z \mapsto \bar{z}$ est la symétrie orthogonale par rapport à l'axe O_x ;
- $z \mapsto -\bar{z}$ est la symétrie orthogonale par rapport à l'axe O_y ;
- pour tout réel $\rho > 0$, $z \mapsto \rho z$ est l'homothétie de rapport ρ et de centre O ;
- pour tout réel θ , $z \mapsto e^{i\theta}z$ est la rotation de centre O et d'angle θ ;
- pour tous nombres complexes a, b avec $a \notin \{0, 1\}$ d'argument θ , l'application $z \mapsto az + b$ est la composée commutative de la rotation d'angle θ et de centre $\Omega \left(\frac{b}{1-a} \right)$ et de l'homothétie de centre O et de rapport $|a|$, on dit que cette application est la similitude directe de centre Ω , de rapport $|a|$ et d'angle $\arg(a)$.

Exercice 19.5 Soit $\alpha = \rho e^{i\theta}$ un nombre complexe non nul et n un entier naturel non nul. Montrer que les racines n -ièmes de α se déduisent des racines n -ième de l'unité par une similitude directe de centre O , de rapport $\sqrt[n]{\rho}$ et d'angle $\frac{\theta}{n}$.

Solution 19.5 Les racines n -ièmes de α sont les :

$$z_k = \sqrt[n]{\rho} e^{i\frac{\theta+2k\pi}{n}} = \sqrt[n]{\rho} e^{i\frac{\theta}{n}} e^{i\frac{2k\pi}{n}} \quad (0 \leq k \leq n-1)$$

où les $e^{i\frac{2k\pi}{n}}$, pour k compris entre 0 et $n-1$, sont les racines n -ième de l'unité.

Quatrième partie

Structures algébriques et arithmétique

Structure de groupe

On suppose construits les ensembles usuels \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} avec les quatre opérations classiques. Nous reviendrons plus loin sur les constructions de \mathbb{Z} à partir de \mathbb{N} , de \mathbb{Q} à partir de \mathbb{Z} , de \mathbb{R} à partir de \mathbb{Q} et de \mathbb{C} à partir de \mathbb{R} .

L'étude préliminaire de l'algèbre linéaire a nécessité l'utilisation des notions de groupe, anneau et corps sans une étude très approfondie.

On se propose dans ce chapitre et les deux suivants d'étudier plus en détail ces structures algébriques de base.

Les résultats de base en algèbre linéaire sont supposés acquis.

Les espaces de matrices (réelles ou complexes) ainsi que les espaces de fonctions polynomiales (à coefficients réels ou complexes) nous seront utiles pour illustrer certaines notions.

Nous supposerons également acquises les notions basiques d'arithmétique (division euclidienne, pgcd, ppcm, ...). Pour a, b entiers relatifs, on note respectivement $a \wedge b$ et $a \vee b$ le pgcd et le ppcm de a et b .

20.1 Loi de composition interne

Définition 20.1 On appelle loi de composition interne sur un ensemble non vide G toute application φ définie sur $G \times G$ et à valeurs dans G .

Si φ est loi de composition interne sur G , on notera souvent :

$$\forall (a, b) \in G^2, a \star b = \varphi(a, b).$$

Il sera parfois commode de noter une telle loi sous la forme additive $(a, b) \mapsto a + b$ ou sous la forme multiplicative $(a, b) \mapsto a \cdot b$ ou plus simplement $(a, b) \mapsto ab$.

On notera (G, \star) l'ensemble non vide G muni de la loi de composition interne \star .

Exemple 20.1 L'addition et la multiplication usuelles sont des lois de composition interne sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .

Exemple 20.2 Si E est un ensemble non vide et $\mathcal{P}(E)$ l'ensemble de toutes les parties de E , les applications :

$$(A, B) \mapsto A \cap B, (A, B) \mapsto A \cup B, (A, B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$$

sont des lois de composition interne sur $\mathcal{P}(E)$ (\triangle est l'opérateur de différence symétrique).

Exemple 20.3 Si E est un ensemble non vide et $\mathcal{F}(E)$ l'ensemble de toutes les applications de E dans E , alors l'application de composition $(f, g) \mapsto f \circ g$ est une loi de composition interne sur $\mathcal{F}(E)$.

Exemple 20.4 Dans l'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels les opérations usuelles d'addition $(A, B) \mapsto A + B$ et de multiplication $(A, B) \mapsto AB$ sont des lois de composition interne.

Exemple 20.5 Dans l'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels inversibles l'addition n'est pas une loi interne (si A est inversible, il en est de même de $B = -A$ et la somme $A + B = 0$ ne l'est pas) et la multiplication est une loi interne.

Définition 20.2 Soit G un ensemble non vide muni d'une loi de composition interne $(a, b) \mapsto a \star b$. On dit que :

1. cette loi est associative si :

$$\forall (a, b, c) \in G^3, (a \star b) \star c = a \star (b \star c)$$

2. cette loi est commutative si :

$$\forall (a, b) \in G^2, a \star b = b \star a$$

3. e est un élément neutre pour cette loi si :

$$\forall a \in G, a \star e = e \star a = a$$

4. un élément a de G est dit régulier (ou simplifiable) si :

$$\forall (b, c) \in G^2, \begin{cases} a \star b = a \star c \Rightarrow b = c, \\ b \star a = c \star a \Rightarrow b = c. \end{cases}$$

Remarque 20.1 Dire qu'un élément $a \in G$ est régulier à gauche [resp. à droite] signifie que l'application $g \mapsto a \star g$ [resp. $g \mapsto g \star a$] est injective.

Si \star est une loi de composition interne associative sur G , on écrira $a \star b \star c$ pour $(a \star b) \star c$ ou $a \star (b \star c)$.

De manière plus générale, toujours dans le cas d'une loi associative, on peut effectuer les opérations $a_1 \star a_2 \star \cdots \star a_n$ où les a_j sont des éléments de G , ce que l'on notera $\prod_{j=1}^n a_j$ dans le cas

d'une loi multiplicative ou $\sum_{j=1}^n a_j$ dans le cas d'une loi additive. Ce produit (ou cette somme)

est donc défini par $a_1 \in G$ et supposant $\prod_{j=1}^{n-1} a_j$ construit pour $n \geq 2$, on a :

$$\prod_{j=1}^n a_j = \prod_{j=1}^{n-1} a_j \star a_n$$

le parenthésage étant sans importance du fait de l'associativité.

Pour $n = 0$, il sera commode de noter $\prod_{j=1}^n a_j = 1$ (ou $\sum_{j=1}^n a_j = 0$ dans le cas d'une loi additive).

Dans le cas où tous les a_j sont égaux à un même élément a , ce produit est noté a^n et on dit que c'est la puissance n -ième de a . On retiendra que ces éléments de G sont donc définis par la relation de récurrence :

$$\begin{cases} a^0 = 1 \\ \forall n \in \mathbb{N}, a^{n+1} = a^n \star a \end{cases}$$

Dans le cas où la loi est notée additivement, on note plutôt na au lieu de a^n .

On vérifie facilement que $a^n \star a^m = a^m \star a^n = a^{n+m}$ [resp. $(na) + (ma) = (ma) + (na) = (n+m)a$ pour une loi additive] pour tous n, m dans \mathbb{N}^* (voir le théorème 20.9).

Exemple 20.6 Les opérations usuelles d'addition et de multiplication sont commutatives et associatives sur $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} . 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication pour chacun de ces ensembles. Tous les éléments de G sont simplifiables pour l'addition et tous les éléments de $G^* = G \setminus \{0\}$ sont simplifiables pour la multiplication.

Exemple 20.7 Si E est un ensemble non vide, les opérations \cap et \cup sont commutatives et associatives sur $\mathcal{P}(E)$. L'ensemble vide \emptyset est un élément neutre pour \cup et E est un élément neutre pour l'intersection \cap .

Exemple 20.8 Si E est un ensemble non vide la composition des applications est associative et non commutative dans $\mathcal{F}(E)$. L'identité est un élément neutre pour cette loi.

Exemple 20.9 Dans $\mathcal{M}_n(\mathbb{R})$ l'addition est associative et commutative et la multiplication est associative et non commutative.

Exercice 20.1 Montrer que le produit vectoriel est une loi de composition interne non associative sur \mathbb{R}^3 .

Solution 20.1 On rappelle que ce produit vectoriel est la loi interne définie par :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \wedge \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} yz' - y'z \\ x'z - xz' \\ xy' - x'y \end{pmatrix}.$$

En désignant par $(\vec{i}, \vec{j}, \vec{k})$ la base canonique de \mathbb{R}^3 , on a :

$$\vec{j} \wedge (\vec{j} \wedge \vec{k}) = \vec{j} \wedge \vec{i} = -\vec{k}, \quad (\vec{j} \wedge \vec{j}) \wedge \vec{k} = \vec{0} \wedge \vec{k} = \vec{0}.$$

Cette loi n'est donc pas associative.

Comme $\vec{u} \wedge \vec{v} = -\vec{v} \wedge \vec{u}$, cette loi n'est pas commutative (il existe des vecteurs tels que $\vec{v} \wedge \vec{u} \neq \vec{0}$).

Théorème 20.1 Soit (G, \star) un ensemble non vide muni d'une loi de composition interne. Si G admet un élément neutre, alors ce dernier est unique.

Démonstration. Soient e, e' deux éléments neutres. On a alors $e = e \star e'$ puisque e' est neutre et $e' = e \star e'$ puisque e est neutre, ce qui implique $e = e'$. ■

Définition 20.3 Soit (G, \star) un ensemble non vide muni d'une loi de composition interne et admettant un élément neutre e . On dit qu'un élément a de G est inversible s'il existe un élément a' dans G tel que $a \star a' = a' \star a = e$. On dit alors que a' est un inverse (ou un symétrique) de a dans G .

Théorème 20.2 Soit (G, \star) un ensemble non vide muni d'une loi de composition interne associative et admettant un élément neutre e . Si $a \in G$ admet un inverse dans G , alors ce dernier est unique.

Démonstration. Supposons que $a \in G$ admette deux inverses a' et a'' . On a alors :

$$a' \star a \star a'' = (a' \star a) \star a'' = e \star a'' = a''$$

puisque la loi est associative et a' est inverse de a et :

$$a' \star a \star a'' = a' \star (a \star a'') = a' \star e = a'$$

puisque a'' est inverse de a , ce qui implique $a' = a''$. ■

Remarque 20.2 Pour une loi non associative, l'unicité du symétrique n'est pas assurée. Par exemple dans l'ensemble $G = \{0, -1, 1\}$ muni de la loi définie par la table :

| \star | 0 | -1 | 1 |
|---------|----|----|---|
| 0 | 0 | -1 | 1 |
| -1 | -1 | 0 | 0 |
| 1 | 1 | 0 | 0 |

0 est neutre et $1 \star 1 = 1 \star (-1) = 0$.

En cas d'existence, on notera a^{-1} un inverse de a dans (G, \star) , la loi \star étant associative.

Dans le cas d'une loi de composition interne notée de façon additive, on notera plutôt $-a$ un inverse de a et on l'appellera opposé.

Exemple 20.10 Dans $(\mathbb{N}, +)$ seul 0 a un opposé et dans (\mathbb{N}, \cdot) seul 1 a un inverse.

Exemple 20.11 Dans $(\mathbb{Z}, +)$ tout élément admet un opposé et dans (\mathbb{Z}, \cdot) les seuls éléments inversibles sont 1 et -1.

Exemple 20.12 Dans $(\mathbb{R}[x], +)$ tout élément admet un opposé et dans $(\mathbb{R}[x], \cdot)$ les seuls éléments inversibles sont les polynômes constants non nuls.

Exemple 20.13 Le cours d'algèbre linéaire nous dit que l'ensemble des éléments inversibles de $(\mathcal{M}_n(\mathbb{R}), \cdot)$ est $GL_n(\mathbb{R})$.

20.2 Groupes

Définition 20.4 Un groupe est un ensemble non vide G muni d'une loi de composition interne \star possédant les propriétés suivantes :

- la loi \star est associative ;
- il existe un élément neutre e pour la loi \star ;
- tout élément de G admet un symétrique.

Si de plus la loi \star est commutative, on dit que le groupe G est commutatif ou abélien.

En général, s'il n'y pas de confusion possible, on dira tout simplement que G est un groupe pour (G, \star) est un groupe et on notera ab ou $a + b$ le résultat de l'opération $a \star b$. Avec la première notation, on dit que G est un groupe multiplicatif et on notera 1 l'élément neutre, a^{-1} le symétrique d'un élément a de G et avec la seconde notation, on dit que G est un groupe additif et on notera 0 l'élément neutre, $-a$ le symétrique qu'on appelle opposé.

Exemple 20.14 Les ensembles \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} munis de l'addition usuelle sont des groupes abéliens.

Exemple 20.15 L'ensemble \mathbb{N} muni de l'addition usuelle n'est pas un groupe du fait qu'un élément non nul de \mathbb{N} n'a pas d'opposé dans \mathbb{N} (l'équation $a + x = 0$ avec $a \neq 0$ dans \mathbb{N} n'a pas de solution dans \mathbb{N}).

Exemple 20.16 Les ensembles \mathbb{Q}^* , \mathbb{R}^* et \mathbb{C}^* munis de la multiplication usuelle sont des groupes abéliens.

Exemple 20.17 L'ensemble \mathbb{Z}^* muni de la multiplication usuelle n'est pas un groupe du fait qu'un élément de $\mathbb{Z} \setminus \{-1, 0, 1\}$ n'a pas d'inverse dans \mathbb{Z} (l'équation $ax = 1$ avec $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ n'a pas de solution dans \mathbb{Z}).

Exemple 20.18 Si E est un ensemble non vide, l'ensemble $\mathcal{P}(E)$ est alors un groupe pour l'opération de différence symétrique : $(A, B) \mapsto A \triangle B = (A \cup B) \setminus (A \cap B)$.

Exemple 20.19 Si E est un ensemble non vide, l'ensemble des bijections de E dans lui-même muni de la composition des applications est un groupe (en général non abélien). Ce groupe est le groupe des permutations de E , il est noté $S(E)$ ou $\mathfrak{S}(E)$.

Exemple 20.20 L'ensemble $\mathcal{M}_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels est un groupe additif, mais non multiplicatif.

Exemple 20.21 L'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels et inversibles est un groupe multiplicatif, mais non additif.

Théorème 20.3 Dans un groupe (G, \star) tout élément est simplifiable.

Démonstration. Soient a, b, c dans G . Si $a \star b = a \star c$, on a alors $a^{-1} \star a \star b = a^{-1} \star a \star c$, soit $b = c$. De même si $b \star a = c \star a$, alors $b \star a \star a^{-1} = c \star a \star a^{-1}$, soit $b = c$. ■

Exercice 20.2 Montrer que si (G, \star) est un groupe, alors pour tout $a \in G$, la translation à gauche $g_a : x \mapsto a \star x$ [resp. à droite $d_a : x \mapsto x \star a$] est une bijection de G d'inverse $g_{a^{-1}}$ [resp. $d_{a^{-1}}$].

Solution 20.2 L'égalité $g_a(x) = g_a(y)$ équivaut à $a \star x = a \star y$ et multipliant à gauche par a^{-1} , on en déduit que $x = y$. L'application g_a est donc injective.

Pour $y \in G$, l'équation $g_a(x) = y$ équivaut à $a \star x = y$, ce qui entraîne $x = a^{-1} \star y$. L'application g_a est donc surjective.

En fait comme, pour tout $y \in G$, l'équation $g_a(x) = y$ a pour unique solution $x = a^{-1} \star y$, on déduit immédiatement que g_a est bijective d'inverse $g_{a^{-1}}$.

Exercice 20.3 Montrer que si (G, \star) est un groupe et E un ensemble non vide, alors l'ensemble G^E des applications de E dans G muni de la loi \cdot définie par :

$$\forall (f, g) \in G^E \times G^E, \forall x \in E, (f \cdot g)(x) = f(x) \star g(x)$$

est un groupe et que ce groupe est commutatif si G l'est.

Solution 20.3 Pour f, g dans G^E , $f \cdot g$ est bien une application de E dans G , donc un élément de G^E .

L'application $1 : x \mapsto e$ est le neutre pour cette loi.

Si $f \in G^E$, l'application $f' : x \mapsto (f(x))^{-1}$ est l'inverse de f .

Pour f, g, h dans G^E et $x \in E$, on a :

$$\begin{aligned}(f \cdot (g \cdot h))(x) &= f(x) * (g \cdot h)(x) = f(x) * (g(x) \star h(x)) \\ &= (f(x) * g(x)) \star h(x) = (f \cdot g)(x) * h(x) \\ &= ((f \cdot g) \cdot h)(x)\end{aligned}$$

et donc $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.

L'ensemble G^E muni de la loi \cdot est donc un groupe.

Si G est commutatif, on a alors pour f, g dans G^E et tout $x \in E$, $(f \cdot g)(x) = f(x) \star g(x) = g(x) \star f(x) = (g \cdot f)(x)$, ce qui revient à dire que $f \cdot g = g \cdot f$. Le groupe (G^E, \cdot) est donc commutatif si G l'est.

Exercice 20.4 Soient G, H deux groupes multiplicatifs. Montrer que le produit direct $G \times H$ muni de la loi :

$$((a_1, a_2), (b_1, b_2)) \mapsto (a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$$

est un groupe.

Solution 20.4 Laissée au lecteur.

De manière plus générale, si H_1, \dots, H_n sont des groupes multiplicatifs, alors le produit direct $H_1 \times \dots \times H_n$ muni de la loi :

$$((a_1, \dots, a_n), (b_1, \dots, b_n)) \mapsto (a_1b_1, \dots, a_nb_n)$$

est un groupe et ce groupe est commutatif si, et seulement si, tous les H_i le sont.

Si (G, \star) est un groupe tel que G ait un nombre fini $n \geq 1$ d'éléments, on dira alors que G est un groupe fini d'ordre (ou de cardinal) n . Pour un tel groupe fini d'ordre petit, on peut dresser sa table de composition. Cette table est appelée table de Pythagore.

Exercice 20.5 Montrer que l'ensemble $G = \{e, a, b, c\}$ muni de la loi \star définie par la table suivante :

| \star | e | a | b | c |
|---------|-----|-----|-----|-----|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

est un groupe commutatif ($a \star b$ est situé à l'intersection de la ligne de a et de la colonne de b). Ce groupe est le groupe de Klein. Une représentation géométrique est donnée par l'ensemble $\{Id, \sigma_x, \sigma_y, \sigma_z\}$, où Id est l'identité de l'espace \mathbb{R}^3 et $\sigma_x, \sigma_y, \sigma_z$ sont les symétries orthogonales par rapport aux trois axes O_x, O_y et O_z , en munissant cet ensemble de la composition des applications.

Solution 20.5 Laissée au lecteur.

Exercice 20.6 La table suivante :

| | | | | | |
|---------|-----|-----|-----|-----|-----|
| \star | e | a | b | c | d |
| e | e | a | b | c | d |
| a | a | e | d | b | c |
| b | b | c | e | d | a |
| c | c | d | a | e | b |
| d | d | b | c | a | e |

définit-elle un groupe ?

Solution 20.6 La loi n'est pas associative puisque :

$$\begin{cases} a \star (b \star c) = a \star d = c \\ (a \star b) \star c = d \star c = a \neq c \end{cases}$$

Exercice 20.7 Soit (G, \star) un ensemble non vide muni d'une loi de composition interne associative, admettant un élément neutre e à gauche, c'est-à-dire que :

$$\forall a \in G, e \star a = a$$

et telle que tout élément de G admette un symétrique à gauche, c'est-à-dire que :

$$\forall a \in G, \exists a' \in G \mid a' \star a = e.$$

Montrer alors que (G, \star) est un groupe (e est alors le neutre de (G, \star) et a' le symétrique de a).

Solution 20.7 Soient $a \in G$ et $a' \in G$ tel que $a' \star a = e$. En désignant par a'' un inverse à gauche de a' , on a :

$$a \star a' = a'' \star a' \star a \star a' = a'' \star (a' \star a) \star a' = a'' \star a' = e,$$

ce qui signifie que a' est aussi un inverse à droite de a . Et avec :

$$a \star e = a \star (a' \star a) = (a \star a') \star a = e \star a = a,$$

on déduit que e est aussi un neutre à droite. En définitive, e est un élément neutre dans (G, \star) et a' est le symétrique de a . Avec l'associativité de \star , il en résulte que (G, \star) est un groupe.

L'exercice précédent nous dit que pour une loi associative la vérification de l'existence d'un neutre à gauche et d'un inverse à gauche est suffisante pour affirmer qu'on a une structure de groupe.

Exercice 20.8 Montrer que l'ensemble $G =]-1, 1[$ muni de la loi \star définie par :

$$x \star y = \frac{x + y}{1 + xy}$$

est un groupe commutatif.

Solution 20.8 Pour x, y dans $] -1, 1[$, on a $|xy| < 1$, donc $1 + xy > 0$ et $x \star y$ est bien défini. De plus avec :

$$\begin{aligned}(x + y)^2 - (1 + xy)^2 &= x^2 + y^2 - 1 - x^2 y^2 \\ &= (x^2 - 1)(1 - y^2) < 0\end{aligned}$$

on déduit que $|x \star y| < 1$ et \star définit bien une loi interne sur G .

De la commutativité de la somme et du produit sur \mathbb{R} on déduit que \star est commutative.

Pour tout $x \in G$, on a $x \star 0 = x$ et $x \star (-x) = 0$, donc 0 est neutre et tout élément de G est inversible.

Enfin pour x, y, z dans G , on a :

$$\begin{aligned}x \star (y \star z) &= \frac{x + y \star z}{1 + x \cdot y \star z} = \frac{x + \frac{y+z}{1+yz}}{1 + x \frac{y+z}{1+yz}} \\ &= \frac{x + y + z + xyz}{xy + xz + yz + 1}\end{aligned}$$

et :

$$\begin{aligned}(x \star y) \star z &= \frac{x \star y + z}{1 + x \star y \cdot z} = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} \\ &= \frac{x + y + z + xyz}{xy + xz + yz + 1}\end{aligned}$$

donc \star est associative.

Exercice 20.9 Montrer que l'ensemble $G = \left] -\frac{\pi}{2}, \frac{\pi}{2} \right[$ muni de la loi \star définie par :

$$x \star y = \arctan(\tan(x) + \tan(y))$$

est un groupe commutatif.

Solution 20.9 La fonction \arctan étant bijective de \mathbb{R} sur $\left] -\frac{\pi}{2}, \frac{\pi}{2} \right[$ l'application \star définit bien une loi interne sur G .

De la commutativité de la somme sur \mathbb{R} on déduit que \star est commutative.

Pour tout $x \in G$, on a $x \star 0 = x$ et $x \star (-x) = 0$ (la fonction \tan est impaire), donc 0 est neutre et tout élément de G est inversible.

Enfin pour x, y, z dans G , on a :

$$\begin{aligned}x \star (y \star z) &= \arctan(\tan(x) + \tan(y \star z)) \\ &= \arctan(\tan(x) + (\tan(y) + \tan(z)))\end{aligned}$$

et :

$$\begin{aligned}(x \star y) \star z &= \arctan(\tan(x \star y) + \tan(z)) \\ &= \arctan(\tan(x) + (\tan(y) + \tan(z)))\end{aligned}$$

ce qui montre que \star est associative.

Les deux exercices précédents ne sont que des cas particuliers de l'exercice 20.34.

Théorème 20.4 Soit (G, \star) un groupe. Pour tous a, b dans G , on a $(a^{-1})^{-1} = a$ et $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Démonstration. La première égalité se déduit immédiatement de la définition de a^{-1} et la deuxième résulte de :

$$b^{-1} \star a^{-1} \star a \star b = b^{-1} \star e \star b = b^{-1} \star b = e$$

■

Plus généralement, on vérifie facilement par récurrence sur $p \geq 2$ que si a_1, \dots, a_p sont des éléments d'un groupe G , on a alors :

$$(a_1 \star \dots \star a_p)^{-1} = a_p^{-1} \star \dots \star a_1^{-1}.$$

Exercice 20.10 Soit G un groupe multiplicatif d'élément neutre 1. Montrer que si on a $a^2 = 1$ pour tout a dans G , alors G est commutatif.

Solution 20.10 Pour a, b dans G , de $abab = (ab)^2 = 1$, on déduit que $a(abab)b = ab$, soit $a^2bab^2 = ab$ ou encore $ba = ab$.

Exercice 20.11 Soit G un groupe multiplicatif d'élément neutre 1.

1. Montrer que G est commutatif si, et seulement si, on a $(ab)^2 = a^2b^2$ pour tous a, b dans G (ce qui revient à dire que l'application $a \mapsto a^2$ est un morphisme de groupes, cette notion étant définie au paragraphe 20.7).
2. Montrer que G est commutatif si, et seulement si, on a $(ab)^{-1} = a^{-1}b^{-1}$ pour tous a, b dans G (ce qui revient à dire que l'application $a \mapsto a^{-1}$ est un morphisme de groupes).

Solution 20.11

1. Dans le cas où G est commutatif, on a pour tous a, b dans G :

$$(ab)^2 = abab = aabb = a^2b^2.$$

Réciproquement, si $(ab)^2 = a^2b^2$ pour tous a, b dans G , de $abab = (ab)^2 = a^2b^2 = aabb$, on déduit par simplification à gauche par a et à droite par b que $ba = ab$.

On peut retrouver le résultat de l'exercice précédent avec ce résultat. Si $a^2 = 1$ pour tout a dans G , on a alors pour tous a, b dans G , $(ab)^2 = 1 = a^2b^2$ et G est commutatif.

2. Dans le cas où G est commutatif, on a pour tous a, b dans G :

$$a^{-1}b^{-1}ab = a^{-1}b^{-1}ba = 1$$

donc $a^{-1}b^{-1} = (ab)^{-1}$.

Réciproquement, si $(ab)^{-1} = a^{-1}b^{-1}$ pour tous a, b dans G , on a alors $ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = ba$ et G est commutatif.

Dans $(GL_n(\mathbb{R}), \cdot)$ qui est non commutatif, on a en général $(AB)^n \neq A^nB^n$ pour $n \geq 2$ dans \mathbb{N} . Par exemple, pour $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on a $(AB)^2 = \begin{pmatrix} 10 & 24 \\ 24 & 58 \end{pmatrix}$ et $A^2B^2 = \begin{pmatrix} 7 & 24 \\ 15 & 52 \end{pmatrix}$.

On peut aussi remarquer que les éléments de $\mathcal{M}_n(\mathbb{R})$ ne sont pas tous simplifiables pour le produit. Par exemple, pour $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a $AB = 0 = A \cdot 0$ avec $B \neq 0$.

20.3 Sous-groupes

Définition 20.5 Soit (G, \star) un groupe. Un sous-groupe de G est un sous-ensemble H de G tel que :

- H est non vide ;
- pour tous a, b dans H , $a \star b^{-1}$ est dans H .

Le résultat qui suit nous donne une définition équivalente de la notion de sous-groupe.

Théorème 20.5 Soit (G, \star) un groupe. Un sous-ensemble H de G est sous-groupe si, et seulement si :

- H contient l'élément neutre e de G ;
- H est stable pour la loi \star , c'est-à-dire que :

$$\forall (a, b) \in H^2, a \star b \in H$$

- H est stable par passage à l'inverse, c'est-à-dire que :

$$\forall a \in H, a^{-1} \in H.$$

Démonstration. Soit H un sous-groupe de G .

Pour $a \in H$, on a $e = a \star a^{-1} \in H$, $a^{-1} = e \star a^{-1} \in H$ et pour $b \in H$, $a \star b = a \star (b^{-1})^{-1} \in H$.

Réciproquement si H contient e , il est non vide et s'il est stable par multiplication et passage à l'inverse, on a pour a, b dans H , $b^{-1} \in H$ et $a \star b^{-1} \in H$. ■

On vérifie facilement qu'un sous-groupe H d'un groupe G est lui même un groupe et H est commutatif si G l'est.

Exemple 20.22 Si (G, \star) est un groupe d'élément neutre e , alors $H = \{e\}$ et G sont des sous-groupes de G . On dit que ce sont les sous-groupes triviaux de G .

Exemple 20.23 L'ensemble Γ des nombres complexes de module égal à 1 (le cercle unité) est un sous-groupe du groupe multiplicatif \mathbb{C}^* .

Exemple 20.24 Pour tout entier $n \geq 1$, l'ensemble $\Gamma_n = \{z \in \mathbb{C} \mid z^n = 1\}$ des racines n -èmes de l'unité est un sous-groupe de Γ .

Exemple 20.25 Pour tout entier naturel n , l'ensemble $n\mathbb{Z} = \{q \cdot n \mid q \in \mathbb{Z}\}$ des multiples de n est un sous groupe de $(\mathbb{Z}, +)$. En réalité ce sont les seuls, comme le montre le théorème suivant qui est une conséquence du théorème de division euclidienne dans \mathbb{Z} (théorème 23.1).

Théorème 20.6 Si G est un sous-groupe de $(\mathbb{Z}, +)$, il existe alors un unique entier naturel n tel que

$$G = n\mathbb{Z} = \{qn \mid q \in \mathbb{Z}\}$$

Cet entier n est le plus petit élément de $G \cap \mathbb{N}^*$.

Démonstration. Si $G = \{0\}$, on a $G = 0\mathbb{Z}$.

Si $G \neq \{0\}$, il existe dans G un entier a non nul et comme G est un sous-groupe de $(\mathbb{Z}, +)$ $-a$ est aussi dans G et l'un des entiers a ou $-a$ est dans $G^+ = G \cap \mathbb{N}^*$. L'ensemble G^+ est donc une partie non vide de \mathbb{N}^* et en conséquence admet un plus petit élément $n \geq 1$. Comme $n \in G$ et G est un groupe additif, on a $n\mathbb{Z} \subset G$. D'autre part, pour tout $m \in G$, la division

euclidienne par n donne $m = qn + r$ avec $r = m - nq \in G^+$ et $r \leq n - 1$, ce qui impose $r = 0$ par définition de n . On a donc $G \subset n\mathbb{Z}$ et $G = n\mathbb{Z}$.

L'unicité provient du fait que $n\mathbb{Z} = m\mathbb{Z}$ si, et seulement si, $n = \pm m$ et pour n, m positifs, on a nécessairement $n = m$. ■

Nous verrons avec le chapitre sur les anneaux, que le résultat précédent peut se traduire en disant que l'anneau \mathbb{Z} est principal et il a de nombreuses applications.

La notion de sous-groupe est commode pour montrer qu'un ensemble est un groupe : on peut essayer de le voir comme sous-groupe d'un groupe connu, ce qui évite de prouver l'associativité. Les exercices qui suivent illustrent cette idée.

Exercice 20.12 Soit i dans \mathbb{C} tel que $i^2 = -1$. Montrer que $G = \{1, -1, i, -i\}$ est un groupe multiplicatif.

Solution 20.12 On montre que c'est un sous-groupe de \mathbb{C} , ce qui se déduit de la table de multiplication :

| | | | | |
|---------|------|------|------|------|
| \cdot | 1 | -1 | i | $-i$ |
| 1 | 1 | -1 | i | $-i$ |
| -1 | -1 | 1 | $-i$ | i |
| i | i | $-i$ | -1 | 1 |
| $-i$ | $-i$ | i | 1 | -1 |

Exercice 20.13 Montrer que l'ensemble $T_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels triangulaires supérieures à termes diagonaux non nuls est un groupe multiplicatif.

Solution 20.13 On a $T_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ puisque le déterminant d'une matrice triangulaire est égal au produit de ces termes diagonaux. La matrice identité I_n est dans $T_n(\mathbb{R})$ et pour A, B dans $T_n(\mathbb{R})$ de diagonales respectives $(\lambda_1, \dots, \lambda_n)$ et (μ_1, \dots, μ_n) , l'inverse de B est une matrice triangulaire de diagonale $\left(\frac{1}{\mu_1}, \dots, \frac{1}{\mu_n}\right)$ et le produit AB^{-1} est une matrice triangulaire de diagonale $\left(\frac{\lambda_1}{\mu_1}, \dots, \frac{\lambda_n}{\mu_n}\right)$, c'est donc un élément de $T_n(\mathbb{R})$. En définitive, $T_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.

Exercice 20.14 Montrer que l'ensemble $TU_n(\mathbb{R})$ des matrices carrées d'ordre n à coefficients réels triangulaires supérieures à termes diagonaux tous égaux à 1 est un groupe multiplicatif (le groupe des matrices triangulaires unipotentes).

Solution 20.14 On procède comme pour l'exercice précédent.

Exercice 20.15 Montrer que l'ensemble $SL_n(\mathbb{R})$ des matrices carrées réelles d'ordre n de déterminant égal à 1 est un sous-groupe de $GL_n(\mathbb{R})$.

Solution 20.15 Comme les matrices de $SL_n(\mathbb{R})$ ont un déterminant non nul, elles sont inversibles. On a donc $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$.

La matrice identité I_n est dans $SL_n(\mathbb{R})$ et pour A, B dans $SL_n(\mathbb{R})$, on a $\det(AB^{-1}) = \frac{\det(A)}{\det(B)} = 1$, donc $AB^{-1} \in SL_n(\mathbb{R})$.

Exercice 20.16 Montrer que l'ensemble $\mathcal{O}_2^+(\mathbb{R})$ des matrices de rotation défini par :

$$\mathcal{O}_2^+(\mathbb{R}) = \left\{ R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

est un groupe multiplicatif commutatif.

Solution 20.16 On vérifie que c'est un sous-groupe du groupe multiplicatif $SL_2(\mathbb{R})$.

Pour tout réel θ , on a $\det(R_\theta) = 1$, donc $R_\theta \in SL_2(\mathbb{R})$. On vérifie facilement que $R_\theta R_{-\theta} = I_n$, ce qui signifie que $R_\theta^{-1} = R_{-\theta}$.

On a $I_n = R_0 \in \mathcal{O}_2^+(\mathbb{R})$ et pour $R_{\theta_1}, R_{\theta_2}$ dans $\mathcal{O}_2^+(\mathbb{R})$, $R_{\theta_1} R_{\theta_2}^{-1} = R_{\theta_1 - \theta_2} \in \mathcal{O}_2^+(\mathbb{R})$.

Donc $\mathcal{O}_2^+(\mathbb{R})$ est un sous-groupe de $SL_2(\mathbb{R})$.

Avec $R_{\theta_1} R_{\theta_2} = R_{\theta_1 + \theta_2}$, on déduit que $\mathcal{O}_2^+(\mathbb{R})$ est commutatif.

Exercice 20.17 L'ensemble $\mathcal{O}_2^-(\mathbb{R})$ des matrices de réflexion défini par :

$$\mathcal{O}_2^-(\mathbb{R}) = \left\{ S_\theta = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

est-il un groupe multiplicatif? Que dire du produit de deux réflexions?

Solution 20.17 Pour tout réel θ , on a $\det(R_\theta) = -1 \neq 0$, donc $\mathcal{O}_2^-(\mathbb{R}) \subset GL_2(\mathbb{R})$.

Comme $I_n \notin \mathcal{O}_2^-(\mathbb{R})$, cet ensemble n'est pas un sous-groupe de $GL_2(\mathbb{R})$.

Pour θ_1, θ_2 dans \mathbb{R} , on a :

$$\begin{aligned} S_{\theta_1} S_{\theta_2} &= \begin{pmatrix} \cos(\theta_1) & \sin(\theta_1) \\ \sin(\theta_1) & -\cos(\theta_1) \end{pmatrix} \begin{pmatrix} \cos(\theta_2) & \sin(\theta_2) \\ \sin(\theta_2) & -\cos(\theta_2) \end{pmatrix} \\ &= \begin{pmatrix} \cos \theta_1 \cos \theta_2 + \sin \theta_1 \sin \theta_2 & \cos \theta_1 \sin \theta_2 - \cos \theta_2 \sin \theta_1 \\ -\cos \theta_1 \sin \theta_2 + \cos \theta_2 \sin \theta_1 & \cos \theta_1 \cos \theta_2 + \sin \theta_1 \sin \theta_2 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1 - \theta_2) & -\sin(\theta_1 - \theta_2) \\ \sin(\theta_1 - \theta_2) & \cos(\theta_1 - \theta_2) \end{pmatrix} = R_{\theta_1 - \theta_2} \in \mathcal{O}_2^+(\mathbb{R}) \end{aligned}$$

c'est-à-dire que le produit de deux réflexions est une rotation.

Exercice 20.18 Montrer que l'ensemble G des matrices réelles de la forme $M_{(a,b)} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$

avec $a^2 \neq b^2$ est un groupe multiplicatif. Est-il commutatif?

Solution 20.18 On vérifie que c'est un sous-groupe du groupe multiplicatif $GL_2(\mathbb{R})$.

On a $I_n = M_{(1,0)} \in G$ et pour tous réels a, b , on a $\det(M_{(a,b)}) = a^2 - b^2 \neq 0$, donc $M_{(a,b)} \in GL_2(\mathbb{R})$, l'inverse de $M_{(a,b)}$ étant :

$$M_{(a,b)}^{-1} = \frac{1}{a^2 - b^2} \begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = M_{\left(\frac{a}{a^2 - b^2}, \frac{-b}{a^2 - b^2}\right)} \in G.$$

Pour $M_{(a_1, b_1)}, M_{(a_2, b_2)}$ dans G , on a :

$$M_{(a_1, b_1)} M_{(a_2, b_2)} = M_{(a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1)} \in G$$

Donc G est un sous-groupe de $GL_2(\mathbb{R})$.

Avec

$$\begin{aligned} M_{(a_1, b_1)} M_{(a_2, b_2)} &= M_{(a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1)} \\ &= M_{(a_2 a_1 + b_2 b_1, a_2 b_1 + a_1 b_2)} = M_{(a_2, b_2)} M_{(a_1, b_1)} \end{aligned}$$

on déduit que ce groupe est commutatif.

Exercice 20.19 L'ensemble des matrices carrées d'ordre n à coefficients réels symétriques et inversibles est-il un groupe multiplicatif?

Solution 20.19 Le produit de deux matrices symétriques n'étant pas nécessairement symétrique, la réponse est négative. Par exemple, pour $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ et $A' = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$, on a $AA' = \begin{pmatrix} aa' + bb' & ab' + bc' \\ ba' + cb' & bb' + cc' \end{pmatrix}$ et en général, $ba' + cb' \neq ab' + bc'$. En effet l'égalité revient à $b(a' - c') = b'(a - c)$ qui n'est pas réalisée pour $a = c$, $b \neq 0$ et $a' \neq c'$.

Exercice 20.20 Montrer que pour tout groupe (G, \star) et tout élément a de G , le centralisateur de a formé des éléments Z_a de G qui commutent avec a , soit :

$$Z_a = \{b \in G \mid a \star b = b \star a\}$$

est un sous-groupe de G .

Solution 20.20 On a $Z_a \neq \emptyset$ puisque $e \in Z_a$. Pour b, c dans Z_a , on a :

$$\begin{aligned} (b \star c) \star a &= b \star (c \star a) = b \star (a \star c) \\ &= (b \star a) \star c = (a \star b) \star c = a \star (b \star c) \end{aligned}$$

c'est-à-dire que $b \star c \in Z_a$.

Pour b dans Z_a , de $a \star b = b \star a$, on déduit que

$$b^{-1} \star a = b^{-1} \star a \star b \star b^{-1} = b^{-1} \star b \star a \star b^{-1} = a \star b^{-1}$$

c'est-à-dire que $b^{-1} \in Z_a$.

En définitive, Z_a est un sous-groupe de G .

Dans le cas où G est commutatif, on a $Z_a = G$ pour tout $a \in G$.

Exercice 20.21 Montrer que pour tout groupe (G, \star) , le centre (ou commutateur) $Z(G)$ de G formé des éléments de G qui commutent à tous les autres éléments de G , soit :

$$Z(G) = \{a \in G \mid \forall b \in G, a \star b = b \star a\}$$

est un sous-groupe de G .

Solution 20.21 On a $Z(G) \neq \emptyset$ puisque $e \in Z(G)$. Pour a, b dans $Z(G)$, on a pour tout $c \in G$:

$$\begin{aligned} (a \star b^{-1}) \star c &= a \star (c^{-1} \star b)^{-1} = a \star (b \star c^{-1})^{-1} \\ &= (a \star c) \star b^{-1} = c \star (a \star b^{-1}) \end{aligned}$$

c'est-à-dire que $a \star b^{-1} \in Z(G)$.

En définitive, $Z(G)$ est un sous-groupe de G .

On peut remarquer que $Z(G) = G$ si, et seulement si, G est commutatif.

Exercice 20.22 Déterminer les centres des groupes multiplicatifs $GL_n(\mathbb{R})$ et $SL_n(\mathbb{R})$.

Solution 20.22 Le centre de $GL_n(\mathbb{R})$ est formé des homothéties de rapport non nul.

Soit $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans le centre de $GL_n(\mathbb{R})$, c'est-à-dire commutant avec toutes les matrices inversibles. En désignant par $(E_{ij})_{1 \leq i, j \leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{R})$, on a $A(I_n + E_{ij}) =$

$(I_n + E_{ij})A$ pour tous $i \neq j$ compris entre 1 et n , ce qui équivaut à $AE_{ij} = E_{ij}A$ pour tous $i \neq j$. En désignant par $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{R}^n , on a :

$$\begin{cases} AE_{ij}e_j = Ae_i = \sum_{k=1}^n a_{ki}e_k \\ E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^n a_{kj}e_k\right) = a_{jj}e_i \end{cases}.$$

pour tous $i \neq j$ et l'égalité $AE_{ij} = E_{ij}A$ impose $a_{ki} = 0$ pour $k \in \{1, \dots, n\} - \{i\}$ et $a_{ii} = a_{jj}$. C'est-à-dire que $A = \lambda I_n$ avec $\lambda \in \mathbb{R}^*$. Réciproquement ces matrices d'homothéties sont bien dans le centre de $GL_n(\mathbb{R})$.

Comme les matrices $I_n + E_{ij}$ (pour $i \neq j$ compris entre 1 et n) sont aussi dans $SL_n(\mathbb{R})$, le raisonnement précédent nous montre que le centre de $SL_n(\mathbb{R})$ est $\{I_n\}$ pour n impair et $\{-I_n, I_n\}$ pour n pair.

Exercice 20.23 Soit H une partie finie non vide d'un groupe (G, \star) . Montrer que H est un sous-groupe de G si, et seulement si, il est stable pour la multiplication.

Solution 20.23 Il est clair que la condition est nécessaire.

Supposons que H soit fini et stable pour la multiplication. Il s'agit alors de montrer que pour tout $a \in H$, l'inverse a^{-1} est aussi dans H .

La translation à gauche $g_a : x \mapsto a \star x$ est une bijection de G et comme H est stable pour la multiplication, cette translation est injective de H dans H et donc bijective puisque H est fini. Il existe donc $x \in H$ tel que $a \star x = a$, ce qui entraîne $x = e$ (en multipliant à gauche par a^{-1}). On a donc $e \in H$ et il existe $x \in H$ tel que $a \star x = e$, ce qui entraîne $x = a^{-1}$ et $a^{-1} \in H$.

Exercice 20.24 Soient H, K deux sous-groupes d'un groupe multiplicatif G . On définit les sous-ensembles HK et KH de G par :

$$HK = \{hk \mid (h, k) \in H \times K\}, \quad KH = \{kh \mid (k, h) \in K \times H\}.$$

Montrer que :

$$(HK \text{ est un sous-groupe de } G) \Leftrightarrow (HK = KH)$$

Solution 20.24 Supposons que HK soit un sous-groupe de G .

Si $g \in HK$, alors g^{-1} est aussi dans HK puisque HK est un groupe, il existe donc (h, k) dans $H \times K$ tel que $g^{-1} = hk$ et $g = (g^{-1})^{-1} = k^{-1}h^{-1} \in KH$ (H et K sont des groupes). On a donc $HK \subset KH$.

Si $g \in KH$, il existe alors (h, k) dans $H \times K$ tel que $g = kh$ et $g^{-1} = h^{-1}k^{-1} \in HK$ et comme HK est un groupe, il en résulte que $g = (g^{-1})^{-1} \in HK$. On a donc $KH \subset HK$ et l'égalité $HK = KH$.

Réciproquement supposons que $HK = KH$.

On a $1 = 1 \cdot 1 \in HK$.

Si $g_1 = h_1k_1$ et $g_2 = h_2k_2$ sont dans HK avec h_1, h_2 dans H et k_1, k_2 dans K , alors $g_1g_2^{-1} = h_1k_1k_2^{-1}h_2^{-1}$ avec $h_1 \in H$, $k_1k_2^{-1} \in K$ (K est un groupe), donc $h_1(k_1k_2^{-1}) \in HK = KH$ et il existe $(k_3, h_3) \in K \times H$ tel que $h_1(k_1k_2^{-1}) = k_3h_3$, ce qui donne $g_1g_2^{-1} = k_3(h_3h_2^{-1}) \in KH = HK$. On a donc prouvé que HK est un sous-groupe de G .

Dans le cas où G est commutatif, on a toujours $HK = KH$ et HK est un sous-groupe de G si H et K le sont.

Exercice 20.25 Soient G un groupe fini, H, K deux sous-groupes de G et φ l'application :

$$\begin{aligned}\varphi : H \times K &\rightarrow HK \\ (h, k) &\mapsto hk\end{aligned}$$

1. Montrer que pour tout $g \in HK$, on a :

$$\text{card}(\varphi^{-1}(g)) = \text{card}(H \cap K)$$

2. En déduire que :

$$\text{card}(H) \text{card}(K) = \text{card}(HK) \text{card}(H \cap K)$$

puis que :

$$(HK \text{ est un sous-groupe de } G) \Leftrightarrow (HK \subset KH) \Leftrightarrow (HK = KH)$$

Solution 20.25

1. Soit $g = h_1 k_1 \in HK$. L'égalité $g = hk$ avec $(h, k) \in H \times K$ équivaut à $h_1 k_1 = hk$, ce qui entraîne $h = h_1 k_1 k^{-1} = h_1 g$ avec $g = k_1 k^{-1} = h_1^{-1} h \in H \cap K$ et $k = h^{-1} h_1 k_1 = g^{-1} k_1$. On a donc $\varphi^{-1}(g) \subset \{(h_1 g, g^{-1} k_1) \mid g \in H \cap K\}$. Réciproquement si $(h, k) = (h_1 g, g^{-1} k_1)$ avec $g \in H \cap K$, on a alors $(h, k) \in H \times K$ et $hk = h_1 g g^{-1} k_1 = g$. Donc :

$$\varphi^{-1}(g) = \{(h_1 g, g^{-1} k_1) \mid g \in H \cap K\}$$

et $\text{card}(\varphi^{-1}(g)) = \text{card}(H \cap K)$.

2. En écrivant qu'on a la partition :

$$H \times K = \bigcup_{g \in HK} \varphi^{-1}(g)$$

on déduit que :

$$\begin{aligned}\text{card}(H) \text{card}(K) &= \text{card}(H \times K) = \sum_{g \in HK} \text{card}(\varphi^{-1}(g)) = \sum_{g \in HK} \text{card}(H \cap K) \\ &= \text{card}(HK) \text{card}(H \cap K)\end{aligned}$$

Il en résulte que $\text{card}(HK) = \text{card}(KH) = \frac{\text{card}(H) \text{card}(K)}{\text{card}(H \cap K)}$.

3. On en déduit que $(HK \subset KH) \Leftrightarrow (HK = KH)$ et l'exercice précédent permet de conclure.

Exercice 20.26 Soient a, b deux éléments d'un groupe multiplicatif G tels que $(ab)^{-1} = a^{-1}b$ et $(ba)^{-1} = b^{-1}a$. Montrer que $(a^2)^{-1} = b^2 = a^2$ et $a^4 = b^4 = 1$.

Donner un exemple non trivial (i. e. avec a et b distincts de 1) d'une telle situation.

Solution 20.26 De $b^{-1}a^{-1} = (ab)^{-1} = a^{-1}b$, on déduit après multiplication à gauche et à droite par a que $ab^{-1} = ba$ et :

$$b^2 a^2 = b(ba)a = b(ab^{-1})a = (ba)(b^{-1}a) = (ba)(ba)^{-1} = 1,$$

ce qui signifie que $(a^2)^{-1} = b^2$.

On en déduit que :

$$\begin{aligned}b^4 &= b^2 b^2 = (a^2)^{-1} b^2 = (a^{-1})^2 b^2 = a^{-1} (a^{-1} b) b \\ &= a^{-1} (ab)^{-1} b = (a^{-1} b^{-1}) (a^{-1} b) = (ba)^{-1} (a^{-1} b) \\ &= (b^{-1} a) (a^{-1} b) = 1\end{aligned}$$

et de $(a^2)^{-1} = b^2$, on déduit que $a^2b^2 = 1$, donc $a^2b^4 = b^2$, soit $a^2 = b^2$ et $a^4 = 1$.

Les conditions $(ab)^{-1} = a^{-1}b$ et $(ba)^{-1} = b^{-1}a$ reviennent à dire que $b^{-1}a^{-1} = a^{-1}b$, soit $b = ab^{-1}a^{-1}$ et $a^{-1}b^{-1} = b^{-1}a$, soit $a = ba^{-1}b^{-1}$. Dans le cas où a et b commutent, cela donne $b = b^{-1}$ et $a = a^{-1}$, soit $a^2 = b^2 = 1$. Il suffit donc de prendre deux éléments d'ordre 2 qui commutent.

On peut considérer, par exemple, le groupe de Klein $G = \{Id, \sigma_x, \sigma_y, \sigma_z\}$ (isomorphe à $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$), où $\sigma_x, \sigma_y, \sigma_z$ désignent les symétries orthogonales par rapport aux axes dans l'espace euclidien \mathbb{R}^3 .

20.4 Sous-groupe engendré par une partie d'un groupe

Théorème 20.7 Soit (G, \star) un groupe. L'intersection d'une famille quelconque $(H_i)_{i \in I}$ de sous-groupes de G est un sous-groupe de G .

Démonstration. Soit $H = \bigcap_{i \in I} H_i$. Comme l'élément neutre e est dans tous les H_i , il est aussi dans H et $H \neq \emptyset$. Si a, b sont dans H , ils sont alors dans tous les H_i , donc $a \star b^{-1} \in H_i$ pour tout $i \in I$, ce qui signifie que $a \star b^{-1} \in H$. On a donc montré que H un sous-groupe de G . ■

Remarque 20.3 La réunion d'une famille de sous-groupes de G n'est pas nécessairement un sous-groupe. Par exemple $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$, mais la réunion H ne l'est pas puisque 2 et 3 sont dans H alors que $2 + 3 = 5 \notin H$.

Exercice 20.27 Soient H, K deux sous-groupes d'un groupe G . Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.

Solution 20.27 Si $H \subset K$ ou $K \subset H$, on a alors $H \cup K = K$ ou $H \cup K = H$ et c'est un sous-groupe de G .

Réciproquement, supposons que $H \cup K$ soit un sous-groupe de G . Si $H \subset K$ c'est terminé, sinon il existe $g \in H \setminus K$. Pour tout $k \in K \subset H \cup K$, gk est dans $H \cup K$ (c'est un groupe) et gk ne peut être dans K (sinon $g = (gk)k^{-1} \in K$, ce qui n'est pas), donc $gk \in H$ et $k = g^{-1}(gk) \in H$. On a donc $K \subset H$.

Corollaire 20.1 Si X est une partie d'un groupe (G, \star) , l'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G .

Démonstration. L'ensemble des sous-groupes de G qui contiennent X est non vide puisque G en fait partie et le théorème précédent nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de G . ■

Définition 20.6 Si X est une partie d'un groupe (G, \star) , le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X .

On note $\langle X \rangle$ le sous-groupe de G engendré par X et ce sous-groupe $\langle X \rangle$ est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de G qui contiennent X .

Dans le cas où X est l'ensemble vide, on a $\langle X \rangle = \{e\}$.

Définition 20.7 Si X est une partie d'un groupe (G, \star) , on dit que X engendre G si $G = \langle X \rangle$.

Théorème 20.8 Soient (G, \star) un groupe et X, Y deux parties de G .

1. On a $X \subset \langle X \rangle$ et l'égalité est réalisée si, et seulement si X est un sous-groupe de G .
2. Si $X \subset Y$, on a alors $\langle X \rangle \subset \langle Y \rangle$.
3. En notant, pour X non vide, X^{-1} l'ensemble formé des symétriques des éléments de X , soit $X^{-1} = \{x^{-1} \mid x \in X\}$, les éléments de $\langle X \rangle$ sont de la forme $x_1 \star \cdots \star x_n$ où $n \in \mathbb{N}^*$ et les x_k sont dans $X \cup X^{-1}$ pour tout k compris entre 1 et n .

Démonstration. Les points 1. et 2. se déduisent immédiatement des définitions.

Pour le point 3. on montre tout d'abord que l'ensemble :

$$H = \{x_1 \star \cdots \star x_n \mid n \in \mathbb{N} \text{ et } x_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq n\}$$

est un sous-groupe de G .

Pour $x_1 \in X$, on a $e = x_1 \star x_1^{-1} \in H$ et pour $x = x_1 \star \cdots \star x_n$, $y = y_1 \star \cdots \star y_m$ dans H , on a :

$$x \star y^{-1} = x_1 \star \cdots \star x_n \star y_m^{-1} \star \cdots \star y_1^{-1} \in H$$

Donc H est bien un sous-groupe de G .

Comme $X \subset H$, il nous suffit de montrer que H est contenu dans tout sous-groupe de G qui contient X . Si K est un tel sous-groupe, tout produit $x_1 \star \cdots \star x_n$ de H est un produit d'éléments de $X \cup X^{-1} \subset K$, donc dans K , ce qui prouve que $H \subset K$. On a donc bien $\langle X \rangle = H$. ■

Remarque 20.4 Le point 3. du théorème précédent nous dit aussi que $\langle X \rangle = \langle X^{-1} \rangle = \langle X \cup X^{-1} \rangle$.

20.5 Groupes monogènes

Pour ce paragraphe, on se donne un groupe multiplicatif (G, \cdot) .

Si X est une partie de G formée d'un nombre fini d'éléments, x_1, \dots, x_n , on note alors $\langle X \rangle = \langle x_1, \dots, x_n \rangle$.

Pour $n = 1$, on dit que $\langle x_1 \rangle$ est un sous-groupe monogène de G .

Définition 20.8 On dit que G est un groupe monogène s'il existe $x_1 \in G$ tel que $G = \langle x_1 \rangle$. Si de plus, G est fini, on dit alors qu'il est cyclique (ce terme sera justifié après avoir défini la notion d'ordre d'un élément d'un groupe).

Pour tout $a \in G$ nous avons déjà défini les puissances entières positives de a (paragraphe 20.1). Dans un groupe, on définit les puissances entières, positives ou négatives, de $a \in G$ par :

$$\begin{cases} a^0 = 1 \\ \forall n \in \mathbb{N}, a^{n+1} = a^n a \\ \forall n \in \mathbb{N}^*, a^{-n} = (a^n)^{-1} \end{cases}$$

On peut remarquer que pour $n \in \mathbb{N}^*$, on a aussi $a^{-n} = (a^{-1})^n$, ce qui résulte de :

$$(a^{-1})^n a^n = a^{-1} \cdots a^{-1} a \cdots a = 1$$

En notation additive, a^n est noté na pour $n \in \mathbb{Z}$.

Théorème 20.9 Pour a dans G et n, m dans \mathbb{Z} , on a :

$$a^n a^m = a^{n+m}$$

et pour $b \in G$ qui commute avec a , on a :

$$(ab)^n = a^n b^n = b^n a^n$$

Démonstration. On montre tout d'abord le résultat pour n, m dans \mathbb{N} par récurrence sur $m \geq 0$ à n fixé. Le résultat est évident pour $m = 0$ et le supposant acquis pour $m \geq 0$, on a :

$$a^n a^{m+1} = a^n a^m a = a^{n+m} a = a^{n+m+1}.$$

On en déduit que pour n', m' dans \mathbb{N} , on a :

$$a^{-n'} a^{-m'} = \left(a^{n'}\right)^{-1} \left(a^{m'}\right)^{-1} = \left(a^{m'} a^{n'}\right)^{-1} = \left(a^{m'+n'}\right)^{-1} = \left(a^{n'+m'}\right)^{-1} = a^{-n'-m'}$$

c'est-à-dire que le résultat est valable pour $n \leq 0$ et $m \leq 0$.

Pour n, m' dans \mathbb{N} tels que $n \geq m'$ on a :

$$a^{n-m'} a^{m'} = a^n \Rightarrow a^n \left(a^{m'}\right)^{-1} = a^n a^{-m'} = a^{n-m'}$$

et pour $n \leq m'$, on a :

$$a^{n-m'} = \left(a^{m'-n}\right)^{-1} = \left(a^{m'} a^{-n}\right)^{-1} = a^n a^{-m'}$$

donc le résultat est valable pour $n \geq 0$ et $m \leq 0$.

On procède de manière analogue pour $n \leq 0$ et $m \geq 0$.

En définitive, c'est valable pour tous n, m dans \mathbb{Z} .

En supposant que a et b commutent, on montre par récurrence sur $n \geq 0$ que $(ab)^n = a^n b^n$ et $ab^{n+1} = b^{n+1}a$. C'est clair pour $n = 0$ et supposant le résultat acquis pour $n \geq 0$, on a :

$$\begin{aligned} (ab)^{n+1} &= (ab)^n ab = a^n b^n ab = a^n b^n ba \\ &= a^n b^{n+1} a = a^n ab^{n+1} = a^{n+1} b^{n+1}. \end{aligned}$$

Et avec $ab = ba$, on déduit que $(ab)^n = (ba)^n = b^n a^n$.

Ensuite, pour $n' \geq 0$, on a :

$$(ab)^{-n'} = \left((ab)^{n'}\right)^{-1} = \left(a^{n'} b^{n'}\right)^{-1} = \left(b^{n'} a^{n'}\right)^{-1} = a^{-n'} b^{-n'} = b^{-n'} a^{-n'}$$

et le résultat est valable pour $n \leq 0$. ■

On vu que la relation $(ab)^n = a^n b^n$ est fausse si a et b ne commutent pas, des exemples simples étant donnés dans $GL_2(\mathbb{R})$.

Théorème 20.10 Pour tout $a \in G$, le sous-groupe de G engendré par a est :

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Démonstration. En notant $H = \{a^n \mid n \in \mathbb{Z}\}$, on a $\{a\} \subset H$, $1 = a^0 \in H$ et pour n, m dans \mathbb{Z} , $a^n (a^m)^{-1} = a^{n-m} \in H$, donc H est un sous-groupe de G qui contient $\{a\}$ et c'est le plus petit du fait que pour tout sous-groupe K de G qui contient $\{a\}$, on a $a^n \in K$ pour tout $n \in \mathbb{Z}$, ce qui implique $H \subset K$. On a donc bien $H = \langle a \rangle$. ■

Exercice 20.28 Soit G un groupe. Montrer que pour tout n -uplet (x_1, \dots, x_n) d'éléments de G qui commutent deux à deux (avec $n \geq 1$), on a :

$$\langle x_1, \dots, x_n \rangle = \left\{ \prod_{k=1}^n x_k^{\alpha_k} \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \right\}$$

Solution 20.28 En notant $X = \{x_1, \dots, x_n\}$, on a $X^{-1} = \{x_1^{-1}, \dots, x_n^{-1}\}$ et comme les x_k commutent, on déduit que :

$$\begin{aligned} \langle x_1, \dots, x_n \rangle &= \left\{ \prod_{k=1}^m y_k \mid m \in \mathbb{N} \text{ et } y_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq m \right\} \\ &= \left\{ \prod_{k=1}^n x_k^{\alpha_k} \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \right\} \end{aligned}$$

($x_k x_j = x_j x_k$ entraîne $x_j^{-1} x_k x_j x_j^{-1} = x_j^{-1} x_j x_k x_j^{-1}$, soit $x_j^{-1} x_k = x_k x_j^{-1}$ et les éléments de $X \cup X^{-1}$ commutent).

Pour une loi de groupe notée additivement, on a, dans le cas où G est commutatif :

$$\langle x_1, \dots, x_n \rangle = \left\{ \sum_{k=1}^n \alpha_k x_k \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \right\}$$

Par exemple pour le groupe additif $G = \mathbb{Z}$, on a :

$$\langle x_1, \dots, x_n \rangle = \sum_{k=1}^n x_k \mathbb{Z} = \delta \mathbb{Z}$$

où $\delta \in \mathbb{N}$ est pgcd de x_1, \dots, x_n . Cette notion est étudiée au paragraphe 23.6.

Exercice 20.29 Montrer qu'un groupe G engendré par deux éléments a et b qui commutent est commutatif.

Solution 20.29 Comme $ab = ba$, on a $G = \langle a, b \rangle = \{a^\alpha b^\beta \mid (\alpha, \beta) \in \mathbb{Z}^2\}$ et ce groupe est commutatif.

Exercice 20.30 Soit $X = \{r_1, \dots, r_n\}$ une partie finie de \mathbb{Q} et $G = \langle X \rangle$ le sous groupe de $(\mathbb{Q}, +)$ engendré par X . Montrer que G est monogène.

Solution 20.30 En désignant par μ le ppcm des dénominateurs de r_1, \dots, r_n , il existe des entiers relatifs a_1, \dots, a_n tels que $r_k = \frac{a_k}{\mu}$ pour tout k compris entre 1 et n et en désignant par δ le pgcd de a_1, \dots, a_n , on a :

$$\begin{aligned} G &= \left\{ \sum_{k=1}^n \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \right\} \\ &= \left\{ \frac{\delta}{\mu} \sum_{k=1}^n \alpha_k b_k \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n \right\} \end{aligned}$$

où b_1, \dots, b_n sont des entiers relatifs premiers entre eux dans leur ensemble. On a donc $G = \frac{\delta}{\mu} \mathbb{Z}$, ce qui signifie que G est monogène engendré par $\frac{\delta}{\mu}$.

20.6 Groupes finis. Théorème de Lagrange

Pour ce paragraphe, on se donne un groupe multiplicatif (G, \cdot) .

Théorème 20.11 *Pour tout sous-groupe H de G , la relation \sim définie sur G par :*

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

est une relation d'équivalence.

Démonstration. Pour tout $x \in G$, on a $x^{-1}x = 1 \in H$, donc \sim est réflexive.

Si x, y dans G sont tels que $x^{-1}y \in H$, on a alors $(x^{-1}y)^{-1} = y^{-1}x \in H$, ce qui signifie que $y \sim x$. Cette relation est donc symétrique.

Si x, y, z dans G sont tels que $x^{-1}y \in H$ et $y^{-1}z \in H$, on a alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, ce qui signifie que $x \sim z$. Cette relation est donc transitive. ■

Avec les notations du théorème précédent, on note, pour tout $g \in G$, \bar{g} la classe d'équivalence de g et on dit que \bar{g} est la classe à gauche modulo H de g .

On a, pour $g \in G$:

$$h \in \bar{g} \Leftrightarrow g \sim h \Leftrightarrow k = g^{-1}h \in H \Leftrightarrow \exists k \in H \mid h = gk \Leftrightarrow h \in gH$$

soit $\bar{g} = gH$.

L'ensemble de toutes ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H .

On a donc :

$$G/H = \{\bar{g} \mid g \in G\} = \{gH \mid g \in G\}.$$

L'application :

$$\begin{aligned} \pi : G &\rightarrow G/H \\ g &\mapsto \bar{g} = gH \end{aligned}$$

est surjective. On dit que c'est la surjection canonique de G sur G/H .

Dans le cas où G est le groupe additif \mathbb{Z} tout sous-groupe de G est de la forme $n\mathbb{Z}$ où n est un entier naturel et cette construction aboutit au groupe $\frac{\mathbb{Z}}{n\mathbb{Z}}$ des classes résiduelles modulo n (ces groupes seront étudiés plus en détails au chapitre 25).

Définition 20.9 *Si G est un groupe ayant un nombre fini d'éléments son cardinal est appelé l'ordre de G .*

Théorème 20.12 (Lagrange) *Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G .*

1. *Les classes à gauche modulo H forment une partition de G .*
2. *Pour tout $g \in G$ on a $\text{card}(\bar{g}) = \text{card}(H)$.*
3. *L'ordre du sous-groupe H divise l'ordre du groupe G .*

Démonstration.

1. Comme G est fini, il en est de même de G/H . Notons :

$$G/H = \{\overline{g_1}, \dots, \overline{g_p}\}$$

où $1 \leq p \leq n$ et $\overline{g_j} \neq \overline{g_k}$, pour $1 \leq j \neq k \leq p$. Pour tout $g \in G$, il existe un unique indice j tel que $\overline{g} = \overline{g_j}$ et $g \in \overline{g_j}$. On a donc $G = \bigcup_{j=1}^p \overline{g_j}$. Dire que g est dans $\overline{g_j} \cap \overline{g_k}$ signifie que g est équivalent modulo H à g_j et g_k et donc par transitivité g_j et g_k sont équivalents, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$. Les classes à gauche modulo H forment donc bien une partition de G .

2. Pour $g \in G$, l'application $h \mapsto gh$ est injective (dans un groupe tout élément est simplifiable) et en restriction à H elle réalise une bijection de H sur $gH = \overline{g}$. Il en résulte que \overline{g} est de même cardinal que H .
3. Avec la partition $G = \bigcup_{j=1}^p \overline{g_j}$ et $\text{card}(\overline{g_j}) = \text{card}(H)$ pour tout j , on déduit que $\text{card}(G) = p \text{card}(H)$ et $\text{card}(H)$ divise $\text{card}(G)$.

■

Le cardinal p de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G . Le théorème de Lagrange peut aussi se traduire par :

$$[G : H] = \text{card}(G/H) = \frac{\text{card}(G)}{\text{card}(H)}.$$

Exercice 20.31 Montrer qu'un groupe fini d'ordre p un nombre premier est cyclique (et donc commutatif).

Solution 20.31 Si G est d'ordre $p \geq 2$ premier, il a au moins deux éléments et il existe $a \neq 1$ dans G . Le sous-groupe cyclique $\langle a \rangle$ de G est alors d'ordre un diviseur de p supérieur ou égal à 2, il est donc égal à p et $G = \langle a \rangle$ est cyclique.

Exercice 20.32 Soient G un groupe et H, K deux sous-groupes distincts de G d'ordre un même nombre premier $p \geq 2$. Montrer que $H \cap K = \{1\}$.

Solution 20.32 $H \cap K$ est un sous groupe de H , il est donc d'ordre 1 ou p . S'il est d'ordre p , il est égal à H et $H = H \cap K \subset K$ entraîne $H = K$, puisque ces deux ensembles ont le même nombre d'éléments. On a donc, pour $H \neq K$, $p = 1$ et $H \cap K = \{1\}$.

Exercice 20.33 Soient G un groupe, H un sous-groupe de G et K un sous-groupe de H . Montrer que si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a :

$$[G : K] = [G : H] [H : K]$$

Solution 20.33 On note respectivement $(g_i H)_{i \in I}$ et $(h_j K)_{j \in J}$ les classes à gauches modulo H dans G et modulo K dans H deux à deux distinctes.

Nous allons alors montrer que la famille des classes à gauches modulo K dans G deux à deux distinctes est $(g_i h_j K)_{(i,j) \in I \times J}$. Dans le cas où $[G : K]$ est fini, il n'y a qu'un nombre fini de telles classes, ce qui impose que I et J sont finis et on a :

$$[G : K] = \text{card}(I \times J) = \text{card}(I) \text{card}(J) = [G : H] [H : K]$$

Montrons le résultat annoncé.

Si g est un élément de G , il existe un unique indice $i \in I$ tel que $gH = g_iH$ et il existe $h \in H$ tel que $g = g_ih$. De même il existe un unique indice $j \in J$ tel que $hK = h_jK$ et h s'écrit $h = h_jk$ avec $k \in K$, ce qui donne $g = g_ih_jk \in g_ih_jK$ et $gK = g_ih_jK$. Les classes à gauche dans G modulo K sont donc les g_ih_jK pour $(i, j) \in I \times J$. Il reste à montrer que ces classes sont deux à deux distinctes.

Si (i, j) et (i', j') dans $I \times J$ sont tels que $g_ih_jK = g_{i'}h_{j'}K$, il existe $k \in K$ tel que $g_ih_j = g_{i'}h_{j'}k$ et $g_i = g_{i'}(h_{j'}kh_j^{-1})$ avec $h_{j'}kh_j^{-1} \in H$, ce qui impose $g_iH = g_{i'}H$ et $i = i'$. Il en résulte que $h_j = h_{j'}k$ et $h_jK = h_{j'}K$, qui équivaut à $j = j'$.

20.7 Morphismes de groupes

On désigne par (G, \star) et (H, \cdot) deux groupes et on note respectivement e et 1 les éléments neutres de (G, \star) et (H, \cdot) .

Définition 20.10 On dit que φ est un morphisme de groupes de G dans H si φ est une application de G dans H telle que ::

$$\forall (a, b) \in G^2, \varphi(a \star b) = \varphi(a) \cdot \varphi(b).$$

Dans le cas où φ est de plus bijective, on dit que φ est un isomorphisme du groupe G sur le groupe H .

Dans le cas où $H = G$, on dit que φ est un endomorphisme du groupe (G, \star) et que c'est un automorphisme du groupe (G, \star) si φ est de plus bijective.

Si G et H sont deux groupes isomorphes, on notera $G \simeq H$.

Théorème 20.13 Soient G, H, K trois groupes, φ un morphisme de groupes de G dans H et ψ un morphisme de groupes de H dans K . L'application $\psi \circ \varphi$ est un morphisme de groupes de G dans K .

Si φ est un automorphisme de G , alors φ^{-1} est également un automorphisme de G .

Démonstration. En notant les lois de chacun des groupes sous forme multiplicative, on a pour tout $(a, b) \in G^2$:

$$\begin{aligned} (\psi \circ \varphi)(a \cdot b) &= \psi(\varphi(a \cdot b)) = \psi(\varphi(a) \cdot \varphi(b)) \\ &= \psi(\varphi(a)) \psi(\varphi(b)) = \psi \circ \varphi(a) \psi \circ \varphi(b). \end{aligned}$$

Si φ est un automorphisme de G , on a alors pour tous a', b' dans G , en notant $a = \varphi^{-1}(a')$, $b = \varphi^{-1}(b')$:

$$\begin{aligned} \varphi^{-1}(a' \star b') &= \varphi^{-1}(\varphi(a) \star \varphi(b)) = \varphi^{-1}(\varphi(a \star b)) \\ &= a \star b = \varphi^{-1}(a') \star \varphi^{-1}(b') \end{aligned}$$

ce qui signifie que φ^{-1} est un morphisme de groupe. Et on sait déjà qu'il est bijectif, c'est donc un automorphisme de G ■

On déduit du théorème précédent que l'ensemble $(\text{Aut}(G), \circ)$ des automorphismes de G dans lui-même est un sous-groupe du groupe symétrique $(S(G), \circ)$ formé des bijections (ou permutations) de G .

Exemple 20.26 La fonction exponentielle est un isomorphisme de groupes de $(\mathbb{R}, +)$ sur $(\mathbb{R}^{+,*}, \cdot)$.

Exemple 20.27 La fonction logarithme népérien est un isomorphisme de groupes de $(\mathbb{R}^{+,*}, \cdot)$ sur $(\mathbb{R}, +)$.

Exemple 20.28 L'application $\text{tr} : A = ((a_{ij}))_{1 \leq i, j \leq n} \mapsto \sum_{i=1}^n a_{ii}$ qui associe à une matrice sa trace est un morphisme du groupe additif $(\mathcal{M}_n(\mathbb{R}), +)$ dans $(\mathbb{R}, +)$.

Exemple 20.29 L'application $\det : A \mapsto \det(A)$ qui associe à une matrice son déterminant est un morphisme du groupe multiplicatif $(GL_n(\mathbb{R}), \cdot)$ dans (\mathbb{R}^*, \cdot) .

Théorème 20.14 Si φ est un morphisme de groupes de G dans H , on alors :

1. $\varphi(e) = 1$;
2. pour tout $a \in G$, $\varphi(a)^{-1} = \varphi(a^{-1})$.

Démonstration.

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

$$\varphi(a) = \varphi(a \star e) = \varphi(a) \cdot \varphi(e)$$

et multipliant par $\varphi(a)^{-1}$, on obtient $1 = \varphi(e)$.

2. Pour tout $a \in G$, on a :

$$1 = \varphi(e) = \varphi(a \star a^{-1}) = \varphi(a) \cdot \varphi(a^{-1})$$

et multipliant par $\varphi(a)^{-1}$, on obtient $\varphi(a)^{-1} = \varphi(a^{-1})$.

■

Définition 20.11 Soit φ un morphisme de groupes de G dans H .

1. Le noyau de φ est l'ensemble :

$$\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}.$$

2. L'image de φ est l'ensemble :

$$\text{Im}(\varphi) = \{\varphi(x) \mid x \in G\}.$$

Théorème 20.15 Si φ est un morphisme de groupes de G dans H , alors :

1. $\ker(\varphi)$ est un sous-groupe de G .
2. φ est injectif si, et seulement si, $\ker(\varphi) = \{e\}$.
3. $\text{Im}(\varphi)$ est un sous-groupe de H .
4. φ est surjectif si, et seulement si, $\text{Im}(\varphi) = H$.
5. Pour tout sous-groupe G' de G , $\varphi(G')$ est un sous-groupe de H .
6. Pour tout sous-groupe H' de H , $\varphi^{-1}(H')$ est un sous-groupe de G .

Démonstration.

1. On a $\ker(\varphi) \neq \emptyset$ puisque $e \in \ker(\varphi)$ ($\varphi(e) = 1$) et pour x, y dans $\ker(\varphi)$:

$$\varphi(x \star y^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x) \cdot \varphi(y)^{-1} = 1$$

c'est-à-dire que $x \star y^{-1} \in \ker(\varphi)$ et $\ker(\varphi)$ est un sous-groupe de G .

2. Si φ est injectif, on a alors :

$$\forall x \in \ker(\varphi), \varphi(x) = 1 = \varphi(e) \Rightarrow x = e$$

et donc $\ker(\varphi) = \{e\}$.

Réciproquement si $\ker(\varphi) = \{e\}$, pour x, y dans G tels que $\varphi(x) = \varphi(y)$, on a :

$$1 = \varphi(x)^{-1} \cdot \varphi(x) = \varphi(x^{-1}) \cdot \varphi(y) = \varphi(x^{-1} \star y)$$

donc $x^{-1} \star y \in \ker(\varphi)$ et $x^{-1} \star y = e$, ce qui équivaut à $x = y$.

3. On a $\text{Im}(\varphi) \neq \emptyset$ puisque $\varphi(e) \in \text{Im}(\varphi)$ et pour $\varphi(x), \varphi(y)$ dans $\text{Im}(\varphi)$ avec x, y dans G :

$$\varphi(x) \cdot \varphi(y)^{-1} = \varphi(x) \cdot \varphi(y^{-1}) = \varphi(x \star y^{-1}) \in \text{Im}(\varphi)$$

et $\text{Im}(\varphi)$ est un sous-groupe de H .

4. C'est la définition de la surjectivité.

5. On a $e \in G'$, donc $1 = \varphi(e) \in \varphi(G')$ et pour $a' = \varphi(a), b' = \varphi(b)$ dans $\varphi(G')$ avec a, b dans G' , on a :

$$\begin{aligned} a' \star (b')^{-1} &= \varphi(a) \star (\varphi(b))^{-1} = \varphi(a) \star \varphi(b^{-1}) \\ &= \varphi(a \star b^{-1}) \in \varphi(G') \end{aligned}$$

Prenant $G' = G$, on retrouve le fait que $\text{Im}(\varphi)$ est un sous-groupe de H .

6. On a $1 = \varphi(e) \in H'$, donc $e \in \varphi^{-1}(H')$ et pour a, b dans $\varphi^{-1}(H')$, on a :

$$\varphi(a \star b^{-1}) = \varphi(a) \star \varphi(b^{-1}) = \varphi(a) \star (\varphi(b))^{-1} \in H'$$

donc $a \star b^{-1} \in \varphi^{-1}(H')$.

Prenant $H' = \{1\}$, on retrouve le fait que $\ker(\varphi)$ est un sous-groupe de G .

■

Exemple 20.30 L'application $\varphi : \theta \mapsto R_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(SL_2(\mathbb{R}), \cdot)$ et son image $\text{Im}(\varphi) = \mathcal{O}_2^+(\mathbb{R})$ est un sous-groupe commutatif de $(SL_2(\mathbb{R}), \cdot)$ (exercice 20.16).

Exercice 20.34

1. Soient (G, \cdot) un groupe, E un ensemble non vide et $f : G \rightarrow E$ une application bijective. Montrer que l'ensemble E muni de la loi \star définie par :

$$x \star y = f(f^{-1}(x) \cdot f^{-1}(y))$$

est un groupe isomorphe à (G, \cdot) (on dit qu'on a transporté la structure de groupe de G sur E).

2. Retrouver les résultats des exercices 20.8 et 20.9.

3. Montrer que pour tout entier impair $n \geq 1$ impair l'application $(x, y) \mapsto x \star y = \sqrt[n]{x^n + y^n}$ définit une structure de groupe commutatif sur \mathbb{R} .

Solution 20.34

1. La fonction f étant bijective de G sur E l'application \star définit bien une loi interne sur E .
 Pour tout $x \in E$, on a $x \star f(1) = f(1) \star x = x$ et $x \star f((f^{-1}(x))^{-1}) = f((f^{-1}(x))^{-1}) \star x = f(1)$ donc $f(1)$ est neutre et tout élément de E est inversible.
 Enfin pour x, y, z dans E , on a :

$$\begin{aligned} x \star (y \star z) &= f(f^{-1}(x) \cdot f^{-1}(y \star z)) \\ &= f(f^{-1}(x) \cdot f^{-1}(y) \cdot f^{-1}(z)) \end{aligned}$$

et :

$$\begin{aligned} (x \star y) \star z &= f(f^{-1}(x \star y) \cdot f^{-1}(z)) \\ &= f(f^{-1}(x) \cdot f^{-1}(y) \star f^{-1}(z)) \end{aligned}$$

ce qui montre que \star est associative.

Avec $f^{-1}(x \star y) = f^{-1}(x) \cdot f^{-1}(y)$, on déduit que f^{-1} est un morphisme de groupes de (E, \star) sur (G, \cdot) et f est un morphisme de groupes de (G, \cdot) sur (E, \star) .

on dit qu'on a transporté la structure de groupe de (G, \cdot) sur E par la bijection f .

2. Les exercices 20.8 et 20.9 sont des exemples de telle situation avec le groupe $(\mathbb{R}, +)$,
 $f(x) = \operatorname{th}(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ pour $x \in \mathbb{R}$ qui réalise une bijection de \mathbb{R} sur $] -1, 1[$ avec pour
 bijection réciproque argth et $f(x) = \arctan(x)$ pour $x \in \mathbb{R}$ qui réalise une bijection de \mathbb{R}
 sur $] -\frac{\pi}{2}, \frac{\pi}{2}[$ avec pour bijection réciproque \tan . Dans le premier cas, on a :

$$\begin{aligned} x \star y &= f(f^{-1}(x) + f^{-1}(y)) \\ &= \operatorname{th}(\operatorname{argth}(x) + \operatorname{argth}(y)) \\ &= \frac{\operatorname{th}(\operatorname{argth}(x)) + \operatorname{th}(\operatorname{argth}(y))}{1 + \operatorname{th}(\operatorname{argth}(x)) \operatorname{th}(\operatorname{argth}(y))} = \frac{x + y}{1 + xy} \end{aligned}$$

et dans le second, on a :

$$\begin{aligned} x \star y &= f(f^{-1}(x) + f^{-1}(y)) \\ &= \arctan(\tan(x) + \tan(y)) \end{aligned}$$

3. L'application $f : x \mapsto \sqrt[n]{x}$ est bijective de \mathbb{R} sur \mathbb{R} pour n impair, son inverse étant l'application $x \mapsto x^n$ et on a :

$$x \star y = \sqrt[n]{x^n + y^n} = f(f^{-1}(x) + f^{-1}(y))$$

Exercice 20.35 Soit G un groupe multiplicatif.

1. Montrer que pour tout $a \in G$, l'application $f_a : x \mapsto axa^{-1}$ est un automorphisme de G .
 On dit que f_a est un automorphisme intérieur de G .
2. Montrer que l'application $f : a \mapsto f_a$ est un morphisme de groupes de G dans $\operatorname{Aut}(G)$
 et que l'ensemble $\operatorname{Int}(G)$ des automorphismes intérieurs de G est un sous-groupe de $\operatorname{Aut}(G)$.

3. Déterminer le noyau de f .
4. Déterminer ce noyau dans le cas où $G = GL_n(\mathbb{R})$.
5. Vérifier que si on prend pour définition d'automorphisme intérieur les applications $g_a : x \mapsto a^{-1}xa$, l'application $a \mapsto g_a$ n'est pas nécessairement un morphisme de groupes.

Solution 20.35

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

$$f_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y)$$

ce qui signifie que f_a est un endomorphisme de G . Pour $y \in G$, l'égalité $y = f_a(x)$ équivaut à $x = a^{-1}ya = f_{a^{-1}}(y)$, ce qui revient à dire que f_a est bijective d'inverse $f_a^{-1} = f_{a^{-1}}$.

2. On vient de voir que l'application f est une application du groupe G dans le groupe $(\text{Aut}(G), \circ)$.

Pour a, b dans G et x dans G , on a :

$$f_{ab}(x) = abx(ab)^{-1} = a(bxb^{-1})a^{-1} = (f_a \circ f_b)(x)$$

donc $f(ab) = f_{ab} = f_a \circ f_b$ et f est un morphisme de groupes. Donc $\text{Int}(G)$ qui est l'image de f est un sous-groupe de $\text{Aut}(G)$.

3. Le noyau de f est formé des $a \in G$ tels que $f_a = \text{Id}_G$, c'est-à-dire des $a \in G$ tels que $axa^{-1} = x$ pour tout $x \in G$, ce qui équivaut à $ax = xa$ pour tout $x \in G$. Le noyau est donc le commutateur (ou le centre) $Z(G)$ de G .
4. Pour $G = GL_n(\mathbb{R})$, ce noyau est formé des homothéties de rapport non nul. Soit $A = ((a_{ij}))_{1 \leq i, j \leq n}$ dans le centre de $GL_n(\mathbb{R})$, c'est-à-dire commutant avec toutes les matrices inversibles. En désignant par $(E_{ij})_{1 \leq i, j \leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{R})$, on a $A(I_n + E_{ij}) = (I_n + E_{ij})A$ pour tous i, j compris entre 1 et n , ce qui équivaut à $AE_{ij} = E_{ij}A$ pour tous i, j . En désignant par $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{R}^n , on a :

$$AE_{ij}e_j = Ae_i = \sum_{k=1}^n a_{ki}e_k = E_{ij}Ae_j = E_{ij}\left(\sum_{k=1}^n a_{kj}e_k\right) = a_{jj}e_i.$$

Donc $a_{ki} = 0$ pour $k \in \{1, \dots, n\} - \{i\}$ et $a_{ii} = a_{jj}$. C'est-à-dire que $A = \lambda I_n$ avec $\lambda \in \mathbb{R}^*$. Réciproquement ces matrices d'homothéties sont bien dans le centre de $GL_n(\mathbb{R})$.

5. Si on prend pour définition d'automorphismes intérieurs les applications $g_a : x \mapsto a^{-1}xa$, on a $g_{ab} = g_b \circ g_a \neq g_a \circ g_b$ en général et $a \mapsto g_a$ n'est pas un morphisme de groupes.

Par exemple pour le groupe multiplicatif $G = GL_2(\mathbb{R})$, soient $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. On a $A^{-1} = A$, $B^{-1} = \begin{pmatrix} 0 & \frac{1}{2} \\ 1 & 0 \end{pmatrix}$ et pour toute matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$, on a :

$$A^{-1}M = \begin{pmatrix} c & d \\ a & b \end{pmatrix}, \quad B^{-1}M = \begin{pmatrix} \frac{c}{2} & \frac{d}{2} \\ a & b \end{pmatrix}$$

de sorte que :

$$g_A(M) = A^{-1}MA = AMA = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

et :

$$g_B(M) = B^{-1}MB = \begin{pmatrix} d & \frac{c}{2} \\ 2b & a \end{pmatrix}$$

ce qui donne :

$$g_A \circ g_B(M) = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \neq g_B \circ g_A(M) = \begin{pmatrix} a & \frac{b}{2} \\ 2c & d \end{pmatrix}$$

en général.

Exercice 20.36 Déterminer tous les endomorphismes du groupe additif \mathbb{Z} puis tous les automorphismes de ce groupe.

Solution 20.36 Soit φ un endomorphisme du groupe additif \mathbb{Z} . En notant $n = \varphi(1)$, on vérifie facilement par récurrence que pour tout entier $k \in \mathbb{N}$ on a $\varphi(k) = nk$ et avec $\varphi(-k) = -\varphi(k)$, on déduit que cette égalité est valable sur tout \mathbb{Z} . L'endomorphisme φ est donc de la forme $\varphi : k \mapsto nk$. Réciproquement de telles applications définissent bien des endomorphismes de \mathbb{Z} . On a donc :

$$\text{End}(\mathbb{Z}) = \{\varphi : k \mapsto nk \mid n \in \mathbb{Z}\} \approx \mathbb{Z}$$

Si $\varphi : k \mapsto nk$ est un automorphisme de \mathbb{Z} , son inverse est aussi de la forme $\varphi^{-1} : k \mapsto mk$ et l'égalité $\varphi^{-1} \circ \varphi(k) = k$ pour tout $k \in \mathbb{Z}$ s'écrit $mnk = k$ pour tout $k \in \mathbb{Z}$, ce qui est réalisée si, et seulement si, $n = m = \pm 1$. On a donc :

$$\text{Aut}(\mathbb{Z}) = \{Id, -Id\} \approx \frac{\mathbb{Z}}{2\mathbb{Z}}$$

(les groupe $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont définis au chapitre 25).

Exercice 20.37

1. Montrer que si f est un endomorphisme du groupe additif \mathbb{R} , alors :

$$\forall a \in \mathbb{R}, \forall r \in \mathbb{Q}, f(ra) = rf(a).$$

2. Montrer que les seuls endomorphismes du groupe additif \mathbb{R} qui sont monotones sont les homothéties (i. e. les applications $x \mapsto \lambda x$, où λ est une constante réelle).

Solution 20.37 Un endomorphisme du groupe additif \mathbb{R} est une application $f : \mathbb{R} \rightarrow \mathbb{R}$ qui vérifie l'équation fonctionnelle de Cauchy :

$$\forall (x, y) \in \mathbb{R}^2, f(x + y) = f(x) + f(y). \quad (20.1)$$

1. En prenant $(x, y) = (0, 0)$ dans (20.1), on obtient $f(0) = 2f(0)$, ce qui équivaut à $f(0) = 0$ (un morphisme de groupes transforme le neutre en neutre).
En prenant $(x, y) = (x, -x)$ dans (20.1), on obtient $f(x) + f(-x) = 0$. On a donc $f(-x) = -f(x)$ pour tout $x \in \mathbb{R}$, c'est-à-dire que la fonction f est impaire (un morphisme de groupes transforme l'opposé en opposé).
De (20.1) on déduit par récurrence que pour tout $a \in \mathbb{R}$ on a :

$$\forall n \in \mathbb{N}, f(na) = nf(a).$$

En effet, le résultat est vrai pour $n = 0$ et le supposant vrai pour $n \geq 0$, on a :

$$f((n+1)a) = f(na) + f(a) = nf(a) + f(a) = (n+1)f(a),$$

il est donc vrai pour tout $n \in \mathbb{N}$.

En écrivant, pour tout $n \in \mathbb{N} \setminus \{0\}$, que $f(a) = f\left(n \frac{a}{n}\right) = nf\left(\frac{a}{n}\right)$, on déduit que $f\left(\frac{a}{n}\right) = \frac{1}{n}f(a)$ pour tout $a \in \mathbb{R}$ et tout $n \in \mathbb{N} \setminus \{0\}$. Il en résulte que pour tout rationnel positif $r = \frac{p}{q}$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N} \setminus \{0\}$, on a :

$$f(ra) = f\left(p \frac{a}{q}\right) = pf\left(\frac{a}{q}\right) = \frac{p}{q}f(a) = rf(a).$$

Enfin avec l'imparité de f , on déduit que ce dernier résultat est encore vrai pour les rationnels négatifs. On a donc $f(ra) = rf(a)$ pour tout $a \in \mathbb{R}$ et tout $r \in \mathbb{Q}$.

2. Soit f un endomorphisme croissant du groupe additif \mathbb{R} . En particulier, on a $\lambda = f(1) \geq f(0) = 0$.

En désignant, pour $x \in \mathbb{R}$, par $(r_n)_{n \in \mathbb{N}}$ et $(s_n)_{n \in \mathbb{N}}$ des suites d'approximations décimales par défaut et par excès de ce réel, on a pour tout $n \in \mathbb{N}$:

$$\lambda r_n = f(r_n) \leq f(x) \leq f(s_n) = \lambda s_n$$

et faisant tendre n vers l'infini, on en déduit que $f(x) = \lambda x$.

On procède de manière analogue pour f décroissante.

Exercice 20.38 Soient G, H deux sous-groupes du groupe additif \mathbb{R} et φ un morphisme de groupes croissant de G vers H . On suppose que G n'est pas réduit à $\{0\}$.

1. Montrer que l'ensemble $G \cap \mathbb{R}^{+,*}$ est non vide.
2. Montrer que s'il existe a dans $G \cap \mathbb{R}^{+,*}$ tel que $\varphi(a) = 0$, alors φ est le morphisme nul.
3. On suppose que pour tout x dans $G \cap \mathbb{R}^{+,*}$, on a $\varphi(x) \neq 0$.

(a) Montrer que $\varphi(x) > 0$ pour tout x dans $G \cap \mathbb{R}^{+,*}$.

(b) Montrer que la fonction $x \mapsto \frac{\varphi(x)}{x}$ est constante sur $G \cap \mathbb{R}^{+,*}$.

(c) En déduire qu'il existe un réel positif λ tel que $\varphi(x) = \lambda x$ pour tout x dans G .

Solution 20.38 Si $G = \{0\}$ alors $\varphi(0) = 0$.

1. Si G n'est pas réduit à $\{0\}$, alors l'ensemble $G \cap \mathbb{R}^{+,*}$ est non vide du fait que pour tout x non nul dans G , $-x$ est aussi dans G .
2. Supposons qu'il existe a dans $G \cap \mathbb{R}^{+,*}$ tel que $\varphi(a) = 0$. Pour tout x dans $G \cap \mathbb{R}^{+,*}$ on peut trouver un entier naturel n tel que $x < na$ (\mathbb{R} est archimédien) et avec la croissance de φ , on déduit que :

$$0 \leq \varphi(x) \leq \varphi(na) = n\varphi(a) = 0,$$

c'est-à-dire que φ est nul sur $G \cap \mathbb{R}^{+,*}$. Avec $\varphi(-x) = -\varphi(x)$ pour tout x dans G , on déduit que φ est le morphisme nul.

3.

- (a) Si pour tout x dans $G \cap \mathbb{R}^{+,*}$, on a $\varphi(x) \neq 0$, avec la croissance de φ on déduit que $\varphi(x) > 0$ pour tout x dans $G \cap \mathbb{R}^{+,*}$.
- (b) Supposons qu'il existe $a \neq b$ dans $G \cap \mathbb{R}^{+,*}$ tels $\frac{a}{b} \neq \frac{\varphi(a)}{\varphi(b)}$. On peut supposer que $\frac{a}{b} < \frac{\varphi(a)}{\varphi(b)}$ et avec la densité de \mathbb{Q} dans \mathbb{R} on déduit qu'il existe un nombre rationnel $\frac{p}{q}$ tel que $\frac{a}{b} < \frac{p}{q} < \frac{\varphi(a)}{\varphi(b)}$. On a alors $qa < pb$ et avec la croissance de φ on déduit que $q\varphi(a) \leq p\varphi(b)$, ce qui est en contradiction avec $\frac{p}{q} < \frac{\varphi(a)}{\varphi(b)}$. La fonction $x \mapsto \frac{\varphi(x)}{x}$ est donc constante sur $G \cap \mathbb{R}^{+,*}$.
- (c) En notant λ cette constante on a $\lambda \geq 0$ et $\varphi(x) = \lambda x$ pour tout x dans $G \cap \mathbb{R}^{+,*}$, ce qui entraîne $\varphi(x) = \lambda x$ pour tout x dans G puisque φ est un morphisme de groupes. On peut remarquer que λ est nulle si, et seulement si, φ est le morphisme nul. Pour $G = H = \mathbb{R}$ on retrouve le résultat de l'exercice précédent.

Exercice 20.39 Soient G, H deux sous-groupes du groupe multiplicatif $\mathbb{R}^{+,*}$ et σ un morphisme de groupes croissant de G vers H . Montrer qu'il existe un réel positif λ tel que $\sigma(x) = x^\lambda$ pour tout x dans G .

Solution 20.39 Si $G = \{1\}$, alors $\sigma(1) = 1$ et $\lambda = 1$ convient.

Sinon $\ln(G) = \{\ln(x) \mid x \in G\}$ est un sous-groupe du groupe additif \mathbb{R} non réduit à $\{0\}$ et $\varphi : t \mapsto \ln(\sigma(e^t))$ est un morphisme de groupes croissant de $\ln(G)$ vers $\ln(H)$ (la fonction logarithme est un morphisme de groupes strictement croissant de $(\mathbb{R}^{+,*}, \times)$ sur $(\mathbb{R}, +)$). Il existe donc un réel $\lambda \geq 0$ tel que $\varphi(t) = \lambda t$ pour tout t dans $\ln(G)$. On a donc $\sigma(e^t) = e^{\lambda t}$ pour tout t dans $\ln(G)$ et pour tout x dans G , on a $\sigma(x) = \sigma(e^{\ln(x)}) = e^{\lambda \ln(x)} = x^\lambda$.

On peut remarquer que λ est nulle si, et seulement si, σ est l'application constante égale à 1.

20.8 Sous-groupes distingués, groupes quotients

Pour ce paragraphe, on se donne un groupe multiplicatif (G, \cdot) .

Si H est une partie non vide de G , on note, pour tout $g \in G$, $gH = \{g \cdot h \mid h \in H\}$ et $Hg = \{h \cdot g \mid h \in H\}$. Dans le cas où G est commutatif, on a $gH = Hg$.

Définition 20.12 On dit qu'un sous-groupe H de G est distingué (ou normal) si on a $gH = Hg$ pour tout $g \in G$.

On note parfois $H \triangleleft G$ pour signifier que H est un sous-groupe distingué de G .

Si le groupe G est commutatif, alors tous ses sous-groupes sont distingués.

Théorème 20.16 Un sous-groupe H de G est distingué si, et seulement si, on a $ghg^{-1} \in H$ pour tout $(h, g) \in H \times G$, ce qui équivaut encore à dire que H est stable par tout automorphisme intérieur.

Démonstration. Si H est distingué dans G , on a alors $gH = Hg$ pour tout $g \in G$, ce qui équivaut à dire que pour tout $h \in H$ il existe $k \in H$ tel que $gh = kg$ et $ghg^{-1} = k \in H$. Le sous groupe H est donc stable par tout automorphisme intérieur $a \mapsto gag^{-1}$.

Réciproquement si H est stable par tout automorphisme intérieur, on a alors $ghg^{-1} \in H$ pour tout $(h, g) \in H \times G$, ce qui entraîne que $gh = (ghg^{-1})g \in Hg$ et $hg = g(g^{-1}hg) \in gH$ pour tout $(h, g) \in H \times G$, encore équivalent à dire que $gH = Hg$. ■

Exercice 20.40 Montrer que :

$$(H \triangleleft G) \Leftrightarrow (\forall g \in G, gH \subset Hg) \Leftrightarrow (\forall g \in G, gHg^{-1} \subset H)$$

Solution 20.40 On a :

$$\begin{aligned} (H \triangleleft G) &\Leftrightarrow (\forall g \in G, gH = Hg) \Rightarrow (\forall g \in G, gH \subset Hg) \\ &\Rightarrow (\forall g \in G, gHg^{-1} \subset H) \Leftrightarrow (H \triangleleft G) \end{aligned}$$

(si $gH \subset Hg$, alors pour $k \in H$, $gk \in Hg$, donc il existe $k' \in H$ tel que $gk = k'g$ et $gkg^{-1} = k' \in H$, donc $gHg^{-1} \subset H$).

Exercice 20.41 Soient G, G' deux groupes et φ un morphisme de groupes de G dans G' . Montrer que $\ker(\varphi)$ est un sous-groupe distingué de G .

Solution 20.41 Pour $(g, h) \in G \times \ker(\varphi)$, on a :

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g)^{-1} \cdot 1 \cdot \varphi(g) = 1$$

c'est-à-dire que $g^{-1}hg \in \ker(\varphi)$. Le sous-groupe $\ker(\varphi)$ de G est donc distingué.

Exercice 20.42 Montrer que le centre d'un groupe G est distingué.

Solution 20.42 On a vu que le centre $Z(G)$ est le noyau du morphisme de groupes $a \mapsto f_a : g \mapsto aga^{-1}$ de G dans $\text{Aut}(G)$ (exercice 20.35), c'est donc un sous-groupe distingué de G .

Exercice 20.43 Soient G, H deux groupes et φ un morphisme de groupes de G dans H .

1. Montrer que si G_1 est un sous-groupe distingué de G et φ est surjectif, alors $\varphi(G_1)$ est un sous-groupe distingué de H (pour φ non surjectif, $\varphi(G_1)$ est un sous-groupe distingué de $\varphi(G)$).
2. Montrer que si H_1 est un sous-groupe distingué de H , alors $\varphi^{-1}(H_1)$ est un sous-groupe distingué de G .

Solution 20.43 On sait déjà que $\varphi(G_1)$ est un sous-groupe de H (que φ soit surjectif ou non) et que $\varphi^{-1}(H_1)$ est un sous-groupe de G .

1. Si φ est surjectif, tout $h \in H$ s'écrit $h = \varphi(g)$ avec $g \in G$ et pour tout $h_1 = \varphi(g_1) \in \varphi(G_1)$ (avec $g_1 \in G_1$), on a $hh_1 = \varphi(g)\varphi(g_1) = \varphi(gg_1)$ avec $gg_1 \in gG_1 = G_1g$ et il existe alors $g_2 \in G_1$ tel que $gg_1 = g_2g$, ce qui donne $hh_1 = \varphi(g_2g) = \varphi(g_2)\varphi(g) = \varphi(g_2)h \in \varphi(G_1)h$. On a donc $h\varphi(G_1) \subset \varphi(G_1)h$, pour tout $h \in H$, ce qui signifie que $\varphi(G_1)$ est distingué dans H .
2. Pour $g \in G$ et $g_1 \in \varphi^{-1}(H_1)$, on a :

$$\varphi(gg_1g^{-1}) = \varphi(g)\varphi(g_1)(\varphi(g))^{-1} \in \varphi(g)H_1(\varphi(g))^{-1} = H_1$$

et $gg_1g^{-1} \in \varphi^{-1}(H_1)$. Donc $g\varphi^{-1}(H_1)g^{-1} \subset \varphi^{-1}(H_1)$ et $\varphi^{-1}(H_1)$ est distingué dans G .

Théorème 20.17 Un sous-groupe H de G est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi : G \rightarrow G/H$ soit un morphisme de groupes.

Démonstration. Si G/H est muni d'une structure de groupe telle que π soit un morphisme de groupe, on a alors nécessairement pour tous g, g' dans G :

$$\overline{gg'} = \pi(g) \pi(g') = \pi(gg') = \overline{gg'}$$

Pour (g, h) dans $G \times H$, on a alors $\overline{g^{-1}hg} = \overline{g^{-1}h\bar{g}} = \overline{g^{-1}\bar{g}} = \overline{g^{-1}g} = \bar{1} = H$, ce qui signifie que $g^{-1}hg \in H$ (on rappelle que $\bar{g} = gH = \bar{1} = H$ si, et seulement si, $g \in H$).

Supposons H distingué. L'analyse que l'on vient de faire nous montre que la seule loi possible sur G/H est définie par $\overline{gg'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de \bar{g} et $\bar{g'}$. Si $\bar{g} = \bar{g_1}$ et $\bar{g'} = \bar{g'_1}$, on a alors $g^{-1}g_1 \in H$ et $(g')^{-1}g'_1 \in H$, ce qui entraîne :

$$(gg')^{-1}(g_1g'_1) = (g')^{-1}g^{-1}g_1g'_1 = ((g')^{-1}(g^{-1}g_1)g')((g')^{-1}g'_1) \in H$$

$((g')^{-1}(g^{-1}g_1)g')$ est dans H puisque H est stable par automorphismes intérieurs), soit $\overline{gg'} = g_1g'_1$.

Il reste à vérifier que G/H muni de cette loi de composition interne est bien un groupe.

Avec :

$$\begin{aligned} \overline{g_1(\bar{g_2} \bar{g_3})} &= \overline{g_1g_2g_3} = \overline{g_1(g_2g_3)} = \overline{(g_1g_2)g_3} \\ &= \overline{g_1g_2} \bar{g_3} = (\bar{g_1} \bar{g_2}) \bar{g_3} \end{aligned}$$

on déduit que cette loi est associative.

Avec $\bar{g}\bar{1} = \overline{g \cdot 1} = \bar{g}$, on déduit que $\bar{1}$ est le neutre.

Avec $\overline{\bar{g}g^{-1}} = \overline{g \cdot g^{-1}} = \bar{1}$, on déduit que tout élément de G/H est inversible avec $(\bar{g})^{-1} = \overline{g^{-1}}$.

Par définition de cette loi de composition interne, l'application π est surjective. ■

Remarque 20.5 Pour H distingué dans G , le noyau de la surjection canonique est :

$$\ker(\pi) = \{g \in G \mid \bar{g} = \bar{1}\} = \bar{1} = H$$

Comme on a vu que le noyau d'un morphisme de groupes est distingué, on déduit qu'un sous-groupe distingué de G est le noyau d'un morphisme de groupes.

Remarque 20.6 Dans le cas où G est commutatif, pour tout sous-groupe H de G , G/H est un groupe puisque tous les sous-groupes de G sont distingués.

Exemple 20.31 Si G est le groupe additif \mathbb{Z} , on sait alors que ces sous-groupes sont les $n\mathbb{Z}$ où n est un entier naturel et comme $(\mathbb{Z}, +)$ est commutatif, l'ensemble quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est naturellement muni d'une structure de groupe.

D'autre part, le théorème de division euclidienne nous permet d'écrire tout entier relatif k sous la forme $k = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne $k - r \in n\mathbb{Z}$ et $\bar{k} = \bar{r}$. Et comme $\bar{r} \neq \bar{s}$ pour $0 \leq r \neq s \leq n-1$ (on a $0 < |r-s| < n$ et $r-s$ ne peut être multiple de n), on en déduit que :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

a n éléments. Ce groupe est cyclique d'ordre n engendré par $\bar{1}$.

Exercice 20.44 Montrer qu'un sous-groupe H de G d'indice 2 est distingué.

Solution 20.44 On a $\text{card}(G/H) = 2$. Pour $(g, h) \in G \times H$, on a soit $g \in H$ et $ghg^{-1} \in H$, soit $g \notin H$, donc $\bar{g} = gH \neq \bar{1} = H$ et $G = gH \cup H$ avec $gH \cap H = \emptyset$ (les classes d'équivalence forment une partition de G). Si, pour $g \notin H$, ghg^{-1} n'est pas dans H , il est forcément dans gH et il existe $k \in H$ tel que $ghg^{-1} = gk$, ce qui entraîne $hg^{-1} = k$ et $g = hk^{-1} \in H$, en contradiction avec $g \notin H$.

Théorème 20.18 Si G, H sont deux groupes et $\varphi : G \rightarrow H$ un morphisme de groupes, il existe alors un unique isomorphisme de groupes $\bar{\varphi} : G/\ker(\varphi) \rightarrow \text{Im}(\varphi)$ tel que $\varphi = i \circ \bar{\varphi} \circ \pi$, où $i : \text{Im}(\varphi) \rightarrow H$ est l'injection canonique (définie par $i(h) = h$ pour tout $h \in \text{Im}(\varphi)$) et $\pi : G \rightarrow G/\ker(\varphi)$ la surjection canonique (définie par $\pi(g) = \bar{g} = g\ker(\varphi)$ pour tout $g \in G$).

Démonstration. Comme $\ker(\varphi)$ est distingué dans G , $G/\ker(\varphi)$ est un groupe.

Si un tel isomorphisme $\bar{\varphi}$ existe, on a alors, pour tout $g \in G$:

$$\varphi(g) = i \circ \bar{\varphi} \circ \pi(g) = i \circ \bar{\varphi}(\bar{g}) = \bar{\varphi}(\bar{g})$$

ce qui prouve l'unicité de $\bar{\varphi}$.

Vu l'analyse du problème, on montre d'abord que l'on peut définir $\bar{\varphi}$ par $\bar{\varphi}(\bar{g}) = \varphi(g)$ pour tout $\bar{g} \in G/\ker(\varphi)$. Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de \bar{g} . Si $\bar{g} = \bar{g}'$, on a alors $g'g^{-1} \in \ker(\varphi)$, donc $\varphi(g')(\varphi(g))^{-1} = \varphi(g'g^{-1}) = 1$ et $\varphi(g) = \varphi(g')$. L'application $\bar{\varphi}$ est donc bien définie et par construction, on a $\varphi = i \circ \bar{\varphi} \circ \pi$.

$\bar{\varphi}$ est à valeurs dans $\text{Im}(\varphi) = \text{Im}(\bar{\varphi})$, donc surjectif.

Avec :

$$\bar{\varphi}(\overline{gg'}) = \bar{\varphi}(\overline{gg'}) = \varphi(gg') = \varphi(g)\varphi(g') = \bar{\varphi}(\bar{g})\bar{\varphi}(\bar{g}')$$

on voit que c'est un morphisme de groupes.

L'égalité $\bar{\varphi}(\bar{g}) = 1$ équivaut à $\varphi(g) = 1$, soit à $g \in \ker(\varphi)$ ou encore à $\bar{g} = \bar{1}$. Ce morphisme est donc injectif. ■

Corollaire 20.2 Soient G, H deux groupes et $\varphi : G \rightarrow H$ un morphisme de groupes. Si G est fini, on a alors :

$$\text{card}(G) = \text{card}(\ker(\varphi)) \text{card}(\text{Im}(\varphi))$$

Démonstration. Comme $G/\ker(\varphi)$ et $\text{Im}(\varphi)$ sont isomorphes, dans le cas où G est fini, on a :

$$\text{card}(\text{Im}(\varphi)) = \text{card}(G/\ker(\varphi)) = \frac{\text{card}(G)}{\text{card}(\ker(\varphi))}.$$

Le théorème précédent s'exprime aussi en disant qu'on a le diagramme commutatif :

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi \downarrow & & \uparrow i \\ G/\ker(\varphi) & \xrightarrow{\bar{\varphi}} & \text{Im}(\varphi) \end{array}$$

Théorème 20.19 Si $n = \dim(E) \geq 2$, alors $\mathcal{O}^+(E)$ [resp. $\mathcal{O}_n^+(\mathbb{R})$] est un sous-groupe distingué de $\mathcal{O}(E)$ [resp. de $\mathcal{O}_n(\mathbb{R})$] d'indice 2.

Démonstration. $\mathcal{O}^+(E)$ est un sous-groupe distingué de $\mathcal{O}(E)$ comme noyau du morphisme de groupes $\det : \mathcal{O}(E) \rightarrow \{-1, 1\}$. Comme cette application est surjective ($\text{Id} \in \mathcal{O}^+(E)$) et en désignant par $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ une base orthonormée de E , l'application u définie par $u(e_1) = -e_1$ et $u(e_i) = e_i$ pour i compris entre 2 et n est dans $\mathcal{O}^-(E)$, $\mathcal{O}(E)/\mathcal{O}^+(E)$ est isomorphe à $\{-1, 1\}$ et $[\mathcal{O}(E) : \mathcal{O}^+(E)] = 2$. ■

Exercice 20.45 Soient G, H deux groupes, $\varphi : G \rightarrow H$ un morphisme de groupes, G' un sous-groupe distingué de G et H' un sous-groupe distingué de H tel que $\varphi(G') \subset H'$. Montrer qu'il existe un unique morphisme de groupes $\overline{\varphi} = G/G' \rightarrow H/H'$ tel que $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$, où $\pi_G : G \rightarrow G/G'$ et $\pi_H : H \rightarrow H/H'$ sont les surjections canoniques.

Solution 20.45 En supposant que $\overline{\varphi}$, on a nécessairement $\pi_H \circ \varphi(g) = \overline{\varphi} \circ \pi_G(g)$ pour tout $g \in G$, ce qui assure l'unicité de $\overline{\varphi}$.

On définit donc $\overline{\varphi}$ par :

$$\forall \bar{g} \in G/G', \quad \overline{\varphi}(\bar{g}) = \widetilde{\varphi(g)}$$

en notant $\bar{g} = gG'$ la classe de $g \in G$ modulo G' et \tilde{h} la classe de $h \in H$ modulo H' . Pour justifier cette définition, on doit vérifier qu'elle ne dépend pas des choix du choix d'un représentant de \bar{g} . Si $\bar{g}_1 = \bar{g}_2$, on a alors $g_2g_1^{-1} \in G'$, donc $\varphi(g_2)(\varphi(g_1))^{-1} = \varphi(g_2g_1^{-1}) \in \varphi(G') \subset H'$ et $\widetilde{\varphi(g_1)} = \widetilde{\varphi(g_2)}$. L'application $\overline{\varphi}$ est donc bien définie et par construction, on a $\pi_H \circ \varphi = \overline{\varphi} \circ \pi_G$. Avec :

$$\begin{aligned} \overline{\varphi}(\overline{g_1g_2}) &= \overline{\varphi}(\overline{g_1g_2}) = \widetilde{\varphi(g_1g_2)} = \widetilde{\varphi(g_1)\varphi(g_2)} \\ &= \widetilde{\varphi(g_1)}\widetilde{\varphi(g_2)} = \overline{\varphi}(\bar{g}_1)\overline{\varphi}(\bar{g}_2) \end{aligned}$$

on voit que c'est un morphisme de groupes.

Si \mathcal{R} est une relation d'équivalence sur G , on dit que cette relation est compatible avec la loi de G si, pour tous g, g', h, h' dans G , on a :

$$(g\mathcal{R}h \text{ et } g'\mathcal{R}h') \Rightarrow gg'\mathcal{R}hh'$$

Cette compatibilité de \mathcal{R} avec la loi de G est une condition nécessaire et suffisante pour définir naturellement une structure de groupe sur l'ensemble quotient G/\mathcal{R} par :

$$\overline{gg'} = \overline{gg'}$$

Précisément, on a le résultat suivant, où G/\mathcal{R} est l'ensemble des classes d'équivalence modulo \mathcal{R} et $\pi : g \mapsto \bar{g} = \{h \in G \mid g\mathcal{R}h\}$ est la surjection canonique de G sur G/\mathcal{R} .

Théorème 20.20 Soit \mathcal{R} une relation d'équivalence sur G . Cette relation est compatible avec la loi de G si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/\mathcal{R} telle que la surjection canonique $\pi : G \rightarrow G/\mathcal{R}$ soit un morphisme de groupes.

Démonstration. Si G/\mathcal{R} est muni d'une structure de groupe telle que π soit un morphisme de groupe, on a alors nécessairement pour tous g, g' dans G :

$$\overline{gg'} = \pi(g)\pi(g') = \pi(gg') = \overline{gg'}$$

On en déduit que pour g, g', h, h' dans G tels que $g\mathcal{R}h$ et $g'\mathcal{R}h'$, on a :

$$\overline{gg'} = \bar{g}\bar{g'} = \bar{h}\bar{h'} = \overline{hh'}$$

ce qui signifie que $gg'\mathcal{R}hh'$. La relation \mathcal{R} est donc compatible avec la loi de G .

Réciproquement, supposons que \mathcal{R} soit compatible avec la loi de G . L'analyse que l'on vient de faire nous montre que la seule loi possible sur G/\mathcal{R} est définie par $\overline{gg'} = \overline{gg'}$. Pour montrer qu'une telle définition est permise, il s'agit de montrer qu'elle ne dépend pas des choix des représentants de \bar{g} et $\bar{g'}$. Si $\bar{g} = \bar{h}$ et $\bar{g'} = \bar{h'}$, on a alors $g\mathcal{R}h$ et $g'\mathcal{R}h'$, ce qui entraîne $gg'\mathcal{R}hh'$, soit $\overline{gg'} = \overline{hh'}$. ■

Exercice 20.46 Soit \mathcal{R} une relation d'équivalence sur G compatible avec la loi de G . Montrer que :

1. pour tous g, h dans G , on a $g\bar{h} = \overline{gh}$ et $\bar{h}g = \overline{hg}$;
2. $H = \bar{1}$ est un sous-groupe distingué de G ;
3. pour tout $g \in G$, $\bar{g} = gH = Hg$ et $G/\mathcal{R} = G/H$.

Solution 20.46

1. On a :

$$(k \in g\bar{h}) \Leftrightarrow (\exists h' \in G \mid h'\mathcal{R}h \text{ et } k = gh') \Rightarrow (k = gh'\mathcal{R}gh) \Rightarrow (k \in \overline{gh})$$

donc $g\bar{h} \subset \overline{gh}$. Et réciproquement :

$$(k \in \overline{gh}) \Leftrightarrow (k\mathcal{R}gh) \Rightarrow (g^{-1}k\mathcal{R}h) \Rightarrow (g^{-1}k \in \bar{h}) \Rightarrow (k \in g\bar{h})$$

soit $\overline{gh} \subset g\bar{h}$ et $g\bar{h} = \overline{gh}$.

On procède de manière analogue pour l'égalité $\bar{h}g = \overline{hg}$

2. On a $1 \in H = \bar{1}$, si g, h sont dans H , on a $g\mathcal{R}1$ et $h\mathcal{R}1$, donc $gh\mathcal{R}1$ et pour $g \in H$, $1\mathcal{R}g$ et $g^{-1}\mathcal{R}g^{-1}$ entraîne $g^{-1}\mathcal{R}1$, soit $g^{-1} \in H$. Donc H est bien un sous-groupe de G .
pour $g \in G$, on a $gH = g\bar{1} = \bar{g}$ et $Hg = \bar{1}g = \bar{g} = gH$, ce qui signifie que H est distingué dans G .
3. On a aussi montré en 2. que $G/\mathcal{R} = G/H$.

L'exercice précédent nous dit en fait que les relations d'équivalence sur un groupe compatibles avec sa loi sont celles suivant un groupe distingué (à gauche ou à droite).

20.9 Ordre d'un élément dans un groupe

Pour ce paragraphe, on se donne un groupe multiplicatif (G, \cdot) et pour tout $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ est le sous-groupe de G engendré par a .

Définition 20.13 L'ordre d'un élément a de G est l'élément $\theta(a) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :

$$\theta(a) = \text{card}(\langle a \rangle).$$

Si $\theta(a)$ est dans \mathbb{N}^* , on dit alors que a est d'ordre fini, sinon on dit qu'il est d'ordre infini.

Remarque 20.7 Seul l'unité $1 \in G$ est d'ordre 1 dans G . En effet, si $a = 1$, alors $\langle a \rangle = \{1\}$ et si $a \neq 1$, alors $a^0 \neq a^1$ et $\langle a \rangle$ a au moins deux éléments.

Remarque 20.8 Pour tout $a \in G$, on a $\theta(a) = \theta(a^{-1})$ puisque :

$$\begin{aligned} \langle a^{-1} \rangle &= \{(a^{-1})^n \mid n \in \mathbb{Z}\} = \{a^{-n} \mid n \in \mathbb{Z}\} \\ &= \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle \end{aligned}$$

Remarque 20.9 Dans le cas où le groupe G est fini, le théorème de Lagrange (théorème 20.12) nous dit que, pour tout $a \in G$, l'ordre de a divise l'ordre de G .

Un groupe fini G d'ordre n est cyclique si, et seulement si, il existe dans G un élément d'ordre n .

Exercice 20.47 Déterminer l'ordre d'un élément du groupe multiplicatif \mathbb{C}^* .

Solution 20.47 Tout nombre complexe non nul s'écrit $z = \rho e^{i\alpha}$ où $\rho \in \mathbb{R}^{+,*}$ et $\alpha \in [0, 2\pi[$ (avec un tel choix de α , cette écriture est unique).

Si $\rho \neq 1$, on a $|z^k| = \rho^k \neq 1$ pour tout entier relatif k , donc $z^k \neq z^j$ pour $k \neq j$ dans \mathbb{Z} et $\langle z \rangle$ est infini.

Si $\rho = 1$, on a alors, pour k entier relatif non nul, $z^k = e^{ik\alpha} = 1$ si, et seulement si, il existe un entier relatif q tel que $k\alpha = 2q\pi$, ce qui signifie que $\frac{\alpha}{2\pi}$ est rationnel. On en déduit donc que :

- pour $\frac{\alpha}{2\pi}$ irrationnel, $z^k \neq 1$ pour tout entier relatif k et $\langle z \rangle$ est infini ;
- pour $\frac{\alpha}{2\pi} = \frac{p}{q}$ rationnel avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$, en effectuant la division euclidienne d'un entier relatif k par q , on a $k = mq + r$ avec $0 \leq r \leq q - 1$ et :

$$z^k = e^{ik\alpha} = (e^{iq\alpha})^m e^{ir\alpha} = (e^{2ip\pi})^m e^{ir\alpha} = e^{ir\alpha}$$

et $\langle z \rangle = \{e^{ir\alpha} \mid 0 \leq r \leq q - 1\}$ a au plus q éléments.

Pour $0 \leq r \neq s \leq q - 1$ l'égalité $e^{ir\alpha} = e^{is\alpha}$ équivaut à $e^{i(s-r)\alpha} = 1$, ce qui revient à dire $(s - r)\alpha = 2m\pi$ avec $m \in \mathbb{Z}$, qui tenant compte de $\alpha = 2\pi \frac{p}{q}$, donne $(s - r) \frac{p}{q} = m$, soit q divise $p(s - r)$ sachant que q est premier avec p , donc q divise $r - s$ (théorème de Gauss) et nécessairement $r = s$ puisque $|r - s| \leq q - 1$. On a donc exactement q éléments dans $\langle z \rangle$ et z est d'ordre q .

En fait $\langle z \rangle$ est le groupe Γ_q des racines q -èmes de l'unité.

En définitive :

$$\theta(\rho e^{i\alpha}) = \begin{cases} +\infty & \text{si } \rho \neq 1 \text{ ou } \rho = 1 \text{ et } \frac{\alpha}{2\pi} \text{ irrationnel} \\ q & \text{si } \frac{\alpha}{2\pi} = \frac{p}{q} \in \mathbb{Q} \text{ avec } p \wedge q = 1 \end{cases}$$

Exercice 20.48 Déterminer l'ordre d'une matrice de rotation [resp. de réflexion] dans $GL_2(\mathbb{R})$ (exercices 20.16 et 20.17). En déduire qu'on peut trouver deux éléments d'ordre fini dans $GL_2(\mathbb{R})$ dont le produit est d'ordre infini.

Solution 20.48 Pour tout réel α et tout entier $n \geq 1$, on a $R_\alpha^n = R_{n\alpha}$ et $R_\alpha^n = I_n$ équivaut à $e^{-in\alpha} = 1$, ce qui revient à dire qu'il existe un entier relatif q tel que $n\alpha = 2q\pi$. Il en résulte qu'une matrice de rotation R_α est d'ordre fini si, et seulement si, $\frac{\alpha}{2\pi} \in \mathbb{Q}$.

Si S_α est une matrice de réflexion, on a $S_\alpha^2 = R_{\alpha-\alpha} = I_n$ et $S_\alpha \neq I_n$, donc S_α est d'ordre 2.

La composée de deux matrices de réflexions $S_\alpha \circ S_{\alpha'} = R_{\alpha-\alpha'}$ est d'ordre infini si $\frac{\alpha - \alpha'}{2\pi} \notin \mathbb{Q}$.

Pour $a \in G$, le sous-groupe de G engendré par a peut être vu comme l'image du morphisme de groupes :

$$\begin{aligned} \varphi_a : \mathbb{Z} &\rightarrow G \\ k &\mapsto a^k \end{aligned}$$

(pour j, k dans \mathbb{Z} , on a $\varphi_a(j + k) = a^{j+k} = a^j a^k = \varphi_a(j) \varphi_a(k)$ et φ_a est bien un morphisme de groupes).

En utilisant la connaissance des sous-groupes additifs de \mathbb{Z} , on a le résultat suivant.

Théorème 20.21 Pour $a \in G$, on a $\theta(a) = +\infty$ si, et seulement si, φ_a est injective et pour a d'ordre fini, on a $\ker(\varphi_a) = \theta(a)\mathbb{Z}$.

Démonstration. Le noyau de φ_a étant un sous-groupe de \mathbb{Z} , il existe un unique entier $n \geq 0$ tel que $\ker(\varphi_a) = n\mathbb{Z}$.

On aura $n = 0$ si, et seulement si, φ_a est injective, ce qui revient à dire que $\varphi_a(k) = a^k \neq 1$ pour tout $k \in \mathbb{Z}^*$ ou encore que $\varphi_a(k) = a^k \neq \varphi_a(j) = a^j$ pour tous $j \neq k$ dans \mathbb{Z} et le sous-groupe $\langle a \rangle = \text{Im}(\varphi_a)$ est infini.

Si $n \geq 1$, en effectuant, pour $k \in \mathbb{Z}$, la division euclidienne de k par n , on a $k = qn + r$ avec $0 \leq r \leq n - 1$ et $a^k = (a^n)^q a^r = a^r$, ce qui nous donne :

$$\langle a \rangle = \text{Im}(\varphi_a) = \{a^r \mid 0 \leq r \leq n - 1\}$$

De plus pour $1 \leq r \leq n - 1$, on a $a^r \neq 1$ puisque $n = \inf(\ker(\varphi_a) \cap \mathbb{N}^*)$, ce qui entraîne $a^r \neq a^s$ pour $0 \leq r \neq s \leq n - 1$ (pour $s \geq r$, l'égalité $a^r = a^s$ équivaut à $a^{s-r} = 1$ avec $s - r$ compris entre 0 et $n - 1$, ce qui équivaut à $r = s$). Le groupe $\langle a \rangle$ a donc exactement n éléments. ■

Une autre définition de l'ordre d'un élément d'un groupe est donnée par le résultat suivant.

Corollaire 20.3 Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que $a^n = 1$ et $a^k \neq 1$ pour tout k est compris entre 1 et $n - 1$ ($\theta(a)$ est le plus petit entier naturel non nul tel que $a^n = 1$).

Démonstration. Si a est d'ordre $n \geq 1$, on a vu avec la démonstration du théorème précédent que $a^n = 1$ et $a^k \neq 1$ pour tout k est compris entre 1 et $n - 1$.

Réciproquement s'il existe un entier $n \geq 1$ tel que $a^n = 1$ et $a^k \neq 1$ pour k est compris entre 1 et $n - 1$, le morphisme de groupes φ_a est non injectif, donc a est d'ordre fini et $\ker(\varphi_a) = \theta(a)\mathbb{Z}$ avec $\theta(a) = \inf(\ker(\varphi_a) \cap \mathbb{N}^*) = n$. ■

Corollaire 20.4 Dire que $a \in G$ est d'ordre fini $n \geq 1$ équivaut à dire que, pour $k \in \mathbb{Z}$, on a $a^k = 1$ si, et seulement si, k est multiple de n .

Démonstration. Si a est d'ordre n , on a alors $a^n = 1$ et pour $k = qn + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r \leq n - 1$ (division euclidienne), on a $a^k = a^r = 1$ si, et seulement si $r = 0$.

Réciproquement supposons que $a^k = 1$ si, et seulement si, k est multiple de n . On a alors $a^n = 1$ et $a^k \neq 1$ si k est compris entre 1 et $n - 1$, ce qui signifie que a est d'ordre n . ■

En résumé, on retiendra que :

- $(\theta(a) = +\infty) \Leftrightarrow (\varphi_a \text{ injective}) \Leftrightarrow (\ker(\varphi_a) = \{0\}) \Leftrightarrow (\forall k \in \mathbb{Z}^*, a^k \neq 1) \Leftrightarrow (\langle a \rangle \text{ est infini isomorphe à } \mathbb{Z})$;
- $(\theta(a) = n \in \mathbb{N}^*) \Leftrightarrow (\ker(\varphi_a) = n\mathbb{Z}) \Leftrightarrow (\langle a \rangle = \{a^r \mid 0 \leq r \leq n - 1\}) \Leftrightarrow (k \in \mathbb{Z} \text{ et } a^k = 1 \text{ équivaut à } k \equiv 0 \pmod{n}) \Leftrightarrow (n \text{ est le plus petit entier naturel non nul tel que } a^n = 1)$.

Pour a d'ordre fini, le groupe $\langle a \rangle$ est dit cyclique, ce qui est justifié par $a^{qn+r} = a^r$ pour $q \in \mathbb{Z}$ et $0 \leq r \leq n - 1$.

Théorème 20.22 Si G est un groupe cyclique d'ordre n , il est alors isomorphe au groupe $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration. Si $G = \langle a \rangle$ est cyclique d'ordre n , alors l'application $\varphi_a : k \mapsto a^k$ est un morphisme de groupes surjectif de $(\mathbb{Z}, +)$ sur G de noyau $\ker(\varphi_a) = n\mathbb{Z}$ et le théorème d'isomorphisme (théorème 20.18) nous dit $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à G . ■

Exemple 20.32 Le groupe multiplication Γ_n des racines n -èmes de l'unité, qui est cyclique d'ordre n , est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$ par l'application $\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$.

Dans le cas où le groupe G est additif, l'ordre de $a \in G$ est défini comme le plus petit entier $n \geq 1$ tel que $na = 0$, quand cet ordre est fini. L'égalité $ma = 0$ équivaut alors à dire que m est multiple de n . Le groupe engendré par a est alors :

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\} = \{ra \mid 0 \leq r \leq n-1\}.$$

Corollaire 20.5 *Si G est fini d'ordre m , on a alors $a^m = 1$ pour tout $a \in G$.*

Démonstration. $\theta(a)$ est fini et divise m . ■

Exercice 20.49 Déterminer les sous-groupes finis du groupe multiplicatif \mathbb{C}^* .

Solution 20.49 Si $G \subset \mathbb{C}^*$ est un groupe d'ordre $n \geq 1$, on a alors $z^n = 1$ pour $z \in G$ et G est contenu dans l'ensemble $\Gamma_n = \left\{ e^{2i\frac{k\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$ des racines n -èmes de l'unité qui est lui même un groupe d'ordre n . On a donc $G = \Gamma_n$.

Exercice 20.50 Soit G un groupe fini d'ordre m . Montrer que pour tout entier relatif n premier avec m , l'application $g \mapsto g^n$ est une bijection de G sur lui même (c'est donc une permutation de G).

Solution 20.50 Comme $m \wedge n = 1$, le théorème de Bézout nous dit qu'il existe deux entiers relatifs u et v tels que $un + vm = 1$ et pour tout $g \in G$, on a $g = g^{un+vm} = (g^u)^n (g^m)^v = (g^u)^n$, ce qui signifie que l'application $g \mapsto g^n$ est surjective. Comme G est fini, cette application est bijective.

Exercice 20.51

1. Soit G un groupe fini dont tous les éléments sont d'ordre au plus égal à 2. Montrer que G est commutatif et que son ordre est une puissance de 2.
2. Montrer que si G est un groupe fini d'ordre $2p$ avec p premier, il existe alors un élément d'ordre p dans G .

Solution 20.51

1. Si tous les éléments de G sont d'ordre au plus égal à 2, on a alors $a^2 = 1$ pour tout $a \in G$, et G est commutatif (exercice 20.10).

Si G est réduit à $\{1\}$, on a alors $\text{card}(G) = 1 = 2^0$.

Si G d'ordre $n \geq 2$ n'est pas réduit à $\{1\}$, il existe $a \in G \setminus \{1\}$ tel que $\langle a \rangle = \{1, a\}$ et le groupe quotient $\frac{G}{\langle a \rangle}$ est de cardinal strictement inférieur à $n = \text{card}(G)$ avec tous ses éléments d'ordre au plus égal à 2. On conclut alors par récurrence sur l'ordre de G .

En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à n , on a $\text{card}\left(\frac{G}{\langle a \rangle}\right) = 2^p$ et $\text{card}(G) = 2^{p+1}$.

On peut procéder de façon plus rapide (et plus astucieuse) comme suit. En notant la loi de G sous forme additive, on a $2 \cdot a = 0$ pour tout $a \in G$ et on peut munir G d'une structure de $\frac{\mathbb{Z}}{2\mathbb{Z}}$ -espace vectoriel en définissant la loi externe par $\bar{0}a = 0$ et $\bar{1}a = a$ pour tout $a \in G$, la loi interne étant l'addition de G . Si G est fini, il est nécessairement de dimension fini sur $\frac{\mathbb{Z}}{2\mathbb{Z}}$ et notant p sa dimension, on a $\text{card}(G) = \text{card}\left(\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^p\right) = 2^p$.

2. Si G est d'ordre $2p \geq 4$ avec p premier, le théorème de Lagrange nous dit que les éléments de $G \setminus \{1\}$ sont d'ordre 2, p ou $2p$. S'il n'y a aucun élément d'ordre p , il n'y en a pas d'ordre $2p$ (si $g \in G \setminus \{1\}$ est d'ordre $2p$, on a alors $g^2 \neq 1$, $g^p \neq 1$ et $(g^2)^p = g^{2p} = 1$, donc g^2 est d'ordre p), donc tous les éléments de $G \setminus \{1\}$ sont d'ordre 2 et G est d'ordre $2^n = 2p$, d'où $p = 2^{n-1}$, $n = 2$ et $p = 2$ puisque p est premier, soit une contradiction avec l'hypothèse qu'il n'y a pas d'élément d'ordre p ($= 2$). Il existe donc dans G des éléments d'ordre p .

Ce résultat est un cas particulier d'un théorème de Cauchy qui nous dit que si G est un groupe fini de cardinal n , alors pour tout diviseur premier p de n , il existe dans G un élément d'ordre p (théorème 20.1).

Exercice 20.52 Montrer qu'un groupe G est fini si et seulement si l'ensemble de ses sous-groupes est fini.

Solution 20.52 Si G est un groupe fini alors l'ensemble $\mathcal{P}(G)$ des parties de G est fini (de cardinal $2^{\text{card}(G)}$) et il en est de même de l'ensemble des sous-groupes de G .

Réciproquement soit (G, \cdot) un groupe tel que l'ensemble de ses sous-groupes soit fini. On peut

écrire $G = \bigcup_{g \in G} \langle g \rangle$ et cette réunion est finie, soit $G = \bigcup_{k=1}^r \langle g_k \rangle$. Si l'un de ces sous-groupes $\langle g_k \rangle$

est infini, alors les $\langle g_k^n \rangle$ où n décrit \mathbb{N} forment une famille infinie de sous-groupes de G : en effet l'égalité $\langle g_k^n \rangle = \langle g_k^m \rangle$ entraîne $g_k^n = g_k^{jm}$, soit $g_k^{n-jm} = 1$ et $n - jm = 0$ (g_k est d'ordre infini), c'est-à-dire que m divise n . Comme n et m jouent des rôles symétriques, on a aussi n qui divise m et en définitive $n = m$ (on peut aussi dire que $\langle g_k \rangle$ est isomorphe à \mathbb{Z} et de ce fait à une infinité de sous-groupes). On a donc une contradiction si l'un des $\langle g_k \rangle$ est infini. Donc tous les $\langle g_k \rangle$ sont finis et aussi G .

Exercice 20.53 Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.

Solution 20.53 En désignant, pour tout entier $n \geq 1$, par Γ_n le groupe des racines n -èmes de l'unité dans \mathbb{C}^* , la réunion $\Gamma = \bigcup_{n=1}^{+\infty} \Gamma_n$ est un sous-groupe de \mathbb{C}^* ($1 \in \Gamma$, pour $z \in \Gamma$, il existe $n \geq 1$ tel que $z \in \Gamma_n$, donc $z^{-1} \in \Gamma_n \subset \Gamma$ et pour z, z' dans Γ , il existe n, m tels que $z \in \Gamma_n$ et $z' \in \Gamma_m$, donc $zz' \in \Gamma_{n \cdot m} \subset \Gamma$). Ce groupe Γ est infini avec tous ses éléments d'ordre fini.

Le groupe additif $G = \frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ avec p premier est infini et tous ses éléments sont d'ordre 1 ou p .

Si on définit sur le corps \mathbb{Q} des rationnels la relation d'équivalence $r \sim s$ si et seulement si $r - s \in \mathbb{Z}$, alors le groupe quotient $\frac{\mathbb{Q}}{\mathbb{Z}}$ pour cette relation d'équivalence est infini et tous ses éléments sont d'ordre fini ($q \frac{\overline{p}}{q} = \overline{0}$).

Si E est un ensemble infini, alors $(\mathcal{P}(E), \Delta)$ où Δ est l'opérateur de différence symétrique est infini et tous les éléments sont d'ordre 1 ou 2 puisque $A \Delta A = \emptyset$.

Théorème 20.23 Soient $a, b \in G$ d'ordre fini et $k \in \mathbb{Z}^*$.

1. On a $\theta(a^k) = \frac{\theta(a)}{\theta(a) \wedge k}$ (en particulier $\theta(a^{-1}) = \theta(a)$).

2. Si k divise $\theta(a)$, on a alors $\theta(a^k) = \frac{\theta(a)}{|k|}$.

3. Si k est premier avec $\theta(a)$, on a alors $\theta(a^k) = \theta(a)$.
4. Si $ab = ba$, alors ab est d'ordre fini divisant $\theta(a) \vee \theta(b)$.
 Dans le cas où $\langle a \rangle \cap \langle b \rangle = \{1\}$, on a $\theta(ab) = \theta(a) \vee \theta(b)$. Si $\theta(a)$ et $\theta(b)$ sont premiers entre eux, on a alors $\langle a \rangle \cap \langle b \rangle = \{1\}$ et $\theta(ab) = \theta(a) \vee \theta(b) = \theta(a)\theta(b)$.

Démonstration.

1. Soit $\delta = \theta(a) \wedge k$ et n', k' premiers entre eux tels que $\theta(a) = \delta n'$, $k = \delta k'$.
 Pour tout entier relatif j , on a :

$$\begin{aligned}(a^k)^j = a^{kj} = 1 &\Leftrightarrow \exists q \in \mathbb{Z} \mid kj = q\theta(a) \Leftrightarrow \exists q \in \mathbb{Z} \mid k'j = qn' \\ &\Leftrightarrow n' \text{ divise } j \text{ (Gauss)}\end{aligned}$$

et en conséquence $\theta(a^k) = n' = \frac{\theta(a)}{\theta(a) \wedge k}$.

2. Si k divise $\theta(a)$, on a alors $\theta(a) \wedge k = |k|$ et $\theta(a^k) = \frac{\theta(a)}{|k|}$.
3. Si k est premier avec $\theta(a)$, on a alors $\theta(a) \wedge k = 1$ et $\theta(a^k) = \theta(a)$.
4. Soit $\mu = \theta(a) \vee \theta(b)$. Dans le cas où a et b commutent, on a $(ab)^\mu = a^\mu b^\mu = 1$ avec $\mu \geq 1$ et ab est d'ordre fini et cet ordre divise μ . En désignant par $n = \theta(ab)$ l'ordre de ab , on a $a^n b^n = (ab)^n = 1$ et $a^n = b^{-n} \in \langle a \rangle \cap \langle b \rangle$.
 Si $\langle a \rangle \cap \langle b \rangle = \{1\}$, on a alors $a^n = b^n = 1$ et n est multiple de $\theta(a)$ et $\theta(b)$, donc de $\theta(a) \vee \theta(b)$ et $n = \theta(a) \vee \theta(b)$.
 Si $\theta(a) \wedge \vee \theta(b) = 1$, on a alors $\theta(a) \vee \theta(b) = \theta(a)\theta(b)$. De plus avec $\langle a \rangle \cap \langle b \rangle \subset \langle a \rangle$ et $\langle a \rangle \cap \langle b \rangle \subset \langle b \rangle$, on déduit que $\text{card}(\langle a \rangle \cap \langle b \rangle)$ divise $\theta(a) = \text{card}(\langle a \rangle)$ et $\theta(b) = \text{card}(\langle b \rangle)$, donc $\text{card}(\langle a \rangle \cap \langle b \rangle) = 1$ et $\langle a \rangle \cap \langle b \rangle = \{1\}$, ce qui implique que $\theta(ab) = \theta(a) \vee \theta(b) = \theta(a)\theta(b)$.

■

Remarque 20.10 Si $\theta(a)$ et $\theta(b)$ ne sont pas premiers entre eux, avec a, b commutant et d'ordre fini, l'ordre de ab n'est pas nécessairement le ppcm de $\theta(a)$ et $\theta(b)$. En prenant par exemple a d'ordre $n \geq 2$ dans G et $b = a^{-1}$ qui est également d'ordre n , on $ab = ba = 1$ d'ordre $1 \neq \text{ppcm}(n, n) = n$.

Remarque 20.11 Pour a et b ne commutant pas, le produit ab peut être d'ordre infini, même si a et b sont d'ordre fini.

20.10 Sous-groupes des groupes cycliques

Pour ce paragraphe, $G = \langle a \rangle$ un groupe cyclique d'ordre $n \geq 2$.

Si H est un sous-groupe de G , le théorème de Lagrange nous dit que l'ordre de H est un diviseur de n . Le théorème qui suit nous dit que les sous-groupes d'un groupe cyclique sont cycliques et que pour tout diviseur d de n , il existe un sous-groupe de G d'ordre d . Ce résultat n'est pas vrai pour un groupe fini quelconque comme nous le verrons avec l'étude du groupe symétrique.

Théorème 20.24 Pour tout diviseur d de n , il existe un unique sous groupe d'ordre d du groupe cyclique $G = \langle a \rangle$, c'est le groupe cyclique $H = \langle a^{\frac{n}{d}} \rangle$.

Démonstration. Pour tout diviseur d de n , $H = \langle a^{\frac{n}{d}} \rangle$ est un sous-groupe cyclique de G et le théorème 20.23 nous dit qu'il est d'ordre $\theta(a^{\frac{n}{d}}) = \frac{n}{n \wedge \frac{n}{d}} = d$.

Réciproquement soit H un sous-groupe de G d'ordre d , un diviseur de n .

Si $d = 1$, on a alors $H = \{1\} = \langle a^n \rangle$.

Si $d \geq 2$, H n'est pas réduit à $\{1\}$, donc il existe un entier k compris entre 1 et $n-1$ tel que $a^k \in H$ et on peut poser :

$$p = \min \{k \in \{1, \dots, n-1\} \mid a^k \in H\}.$$

En écrivant, pour tout $h = a^k \in H$, $k = pq + r$ avec $0 \leq r \leq p-1$ (division euclidienne par p), on a $a^r = a^k (a^{pq})^{-1} \in H$ et nécessairement $r = 0$. On a donc $H \subset \langle a^p \rangle \subset H$, soit $H = \langle a^p \rangle$. Avec $a^n = 1 \in H$, on déduit que n est multiple de p et l'ordre de H est $d = \frac{n}{n \wedge p} = \frac{n}{p}$, c'est-à-dire que $H = \langle a^{\frac{n}{d}} \rangle$. Un tel sous-groupe d'ordre d est donc unique. ■

Exemple 20.33 Les sous groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont les $\langle \frac{n}{d} \bar{1} \rangle = \langle \frac{\bar{n}}{d} \rangle$ où d est un diviseur de n . Un tel sous-groupe est isomorphe à $\frac{\mathbb{Z}}{d\mathbb{Z}}$ et il y en a autant que de diviseurs de n .

Exemple 20.34 Les sous groupes de $\Gamma_n = \{z \in C \mid z^n = 1\} = \langle e^{\frac{2i\pi}{n}} \rangle$ sont les $\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \rangle = \langle e^{\frac{2i\pi}{d}} \rangle = \Gamma_d$ où d est un diviseur de n et il y en a autant que de diviseurs de n .

Lemme 20.1 (Cauchy) Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p

Démonstration. On procède par récurrence sur l'ordre $n \geq 2$ de G .

Pour $n = 2$, le résultat est trivial (G est le seul sous-groupe d'ordre 2).

Supposons le acquis pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$ et soient G un groupe commutatif d'ordre n , p un diviseur premier de n et $g \in G \setminus \{1\}$.

Si $G = \langle g \rangle$, alors G est cyclique et g est d'ordre n . Pour tout diviseur premier p de n , l'élément $h = g^{\frac{n}{p}}$ est alors d'ordre p dans G .

Si $G \neq \langle g \rangle$ et p divise $m = \text{card}(\langle g \rangle) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément h dans $\langle g \rangle$ qui est d'ordre p .

Supposons enfin que $G \neq \langle g \rangle$ et p ne divise pas $m = \text{card}(\langle g \rangle)$. Comme p est premier ne divisant pas m , il est premier avec m et le groupe quotient $\frac{G}{\langle g \rangle}$ est commutatif d'ordre $r = \frac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m , le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $[h]$ d'ordre p dans $\frac{G}{\langle g \rangle}$. Si s est l'ordre de h dans G , alors $[h]^s = [h^s] = [1]$ et s est multiple de p . L'élément $k = h^{s/p}$ est alors d'ordre p dans G . ■

Structure d'anneau

21.1 Anneaux

Définition 21.1 Soit A un ensemble non vide muni de deux lois de composition interne notées $+$ (une addition) et \cdot (une multiplication). On dit que $(A, +, \cdot)$ est un anneau si :

- $(A, +)$ est un groupe commutatif ;
- la loi \cdot est associative ;
- la loi \cdot est distributive par rapport à la loi $+$, ce qui signifie que :

$$\forall (a, b, c) \in A^3, \begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (b + c) \cdot a = b \cdot a + c \cdot a \end{cases}$$

Si la loi \cdot est commutative, on dit alors que l'anneau A est commutatif.

S'il existe un élément neutre pour la loi \cdot , on dira alors que A est un anneau unitaire.

Si $(A, +, \cdot)$ est un anneau, on notera 0 le neutre pour l'addition et s'il existe on notera 1 le neutre pour la multiplication. L'opposé d'un élément a (i. e. le symétrique pour $+$) sera noté $-a$ et on notera $a - b$ pour $a + (-b)$.

On écrira souvent ab pour $a \cdot b$ dans un anneau.

Dans un anneau unitaire, on supposera que $0 \neq 1$ (sans quoi l'anneau est réduit à $\{0\}$). Un anneau unitaire a donc au moins deux éléments.

Exemple 21.1 Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ muni des opérations usuelles sont des anneaux commutatifs et unitaires.

Exemple 21.2 Soient E un ensemble non vide et A un anneau. On vérifie facilement que l'ensemble A^E des applications de E dans A muni des opérations d'addition et de multiplication définies par :

$$\forall (f, g) \in A^E \times A^E, \forall x \in E, \begin{cases} (f + g)(x) = f(x) + g(x) \\ (f \cdot g)(x) = f(x) \cdot g(x) \end{cases}$$

est un anneau. Cet anneau est commutatif si A l'est et il est unitaire si A l'est avec comme élément neutre pour le produit l'application constante égale à 1 .

En particulier l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites réelles est un anneau commutatif unitaire et pour toute partie non vide I de \mathbb{R} , l'ensemble R^I des fonctions définies sur I et à valeurs réelles est un anneau commutatif unitaire.

Exemple 21.3 L'ensemble $\mathcal{M}_n(\mathbb{R})$ [resp. $\mathcal{M}_n(\mathbb{C})$] des matrices carrées réelles [resp. complexes] d'ordre $n \geq 1$ muni des opérations usuelles d'addition et de multiplication est un anneau unitaire non commutatif.

Exemple 21.4 Plus généralement si A est un anneau commutatif unitaire, l'ensemble $\mathcal{M}_n(A)$ des matrices carrées d'ordre n à coefficients dans A est un anneau unitaire non commutatif pour les opérations d'addition et multiplication définies par :

$$\begin{cases} M + M' = ((m_{ij} + m'_{ij}))_{1 \leq i, j \leq n} \\ MM' = \left(\left(\sum_{k=1}^n m_{ik} m'_{kj} \right) \right)_{1 \leq i, j \leq n} \end{cases}$$

où on note $M = ((m_{ij}))_{1 \leq i, j \leq n}$ la matrice ayant pour coefficient m_{ij} en ligne i et colonne j pour i, j compris entre 1 et n .

On peut aussi définir, pour $\lambda \in A$ et $M = ((m_{ij}))_{1 \leq i, j \leq n} \in \mathcal{M}_n(A)$, la matrice λM par $\lambda M = ((\lambda m_{ij}))_{1 \leq i, j \leq n}$.

Exercice 21.1 Soit A un anneau commutatif unitaire. Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathcal{M}_2(A)$, on définit le déterminant et la trace de M respectivement par :

$$\det(M) = ad - bc ; \operatorname{Tr}(M) = a + d$$

1. Vérifier que, pour toutes matrices M, M' dans $\mathcal{M}_2(A)$, on a $\det(MM') = \det(M) \det(M')$.

2. Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(A)$, on définit la comatrice (en fait la transposée de la comatrice) de M par $\widetilde{M} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

(a) Calculer $M\widetilde{M}$.

(b) Montrer que $M^2 - \operatorname{Tr}(M)M + \det(M)I_2 = 0$, où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Solution 21.1

1. On a :

$$MM' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

et :

$$\begin{aligned} \det(MM') &= (aa' + bc')(cb' + dd') - (ca' + dc')(ab' + bd') \\ &= bcb'c' - adb'c' + ada'd' - bca'd' \\ &= ad(a'd' - b'c') + bc(b'c' - a'd') \\ &= (ad - bc)(a'd' - b'c') \\ &= \det(M) \det(M') \end{aligned}$$

(l'anneau A est commutatif)

2.

(a) On a :

$$\begin{aligned} M\widetilde{M} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \det(M) I_2 \end{aligned}$$

(b) On a :

$$\begin{aligned} M^2 - \operatorname{Tr}(M) M + \det(M) I_2 &= M^2 - \operatorname{Tr}(M) M \cdot I_2 + M \cdot \widetilde{M} \\ &= M \left(M - \operatorname{Tr}(M) I_2 + \widetilde{M} \right) \end{aligned}$$

avec :

$$\begin{aligned} M - \operatorname{Tr}(M) I_2 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} \\ &= \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} = -\widetilde{M} \end{aligned}$$

ce qui donne :

$$M^2 - \operatorname{Tr}(M) M + \det(M) I_2 = 0.$$

Exercice 21.2 Soit E un ensemble non vide. Montrer que l'ensemble $\mathcal{P}(E)$ des parties de E muni des opérations Δ de différence symétrique et \cap d'intersection est un anneau commutatif et unitaire (c'est l'anneau de Boole).

Solution 21.2 On rappelle que pour A, B dans $\mathcal{P}(E)$, on a :

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A),$$

la réunion étant disjointe.

De la commutativité des opérateurs \cup et \cap , on déduit que Δ est commutative.

Pour A, B, C dans $\mathcal{P}(E)$, on a :

$$\begin{aligned} (x \in (A \Delta B) \Delta C) &\Leftrightarrow (x \in A \Delta B \text{ et } x \notin C) \text{ ou } (x \in C \text{ et } x \notin A \Delta B) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in B \text{ et } x \notin A \text{ et } x \notin C) \\ &\text{ou } (x \in C \text{ et } x \notin A \text{ et } x \notin B) \text{ ou } (x \in C \text{ et } x \in A \cap B) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in B \text{ et } x \notin A \text{ et } x \notin C) \\ &\text{ou } (x \in C \text{ et } x \notin A \text{ et } x \notin B) \text{ ou } (x \in A \cap B \cap C) \end{aligned}$$

et :

$$\begin{aligned} (x \in A \Delta (B \Delta C)) &\Leftrightarrow (x \in A \text{ et } x \notin B \Delta C) \text{ ou } (x \in B \Delta C \text{ et } x \notin A) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in A \text{ et } x \in B \cap C) \\ &\text{ou } (x \in B \text{ et } x \notin C \text{ et } x \notin A) \text{ ou } (x \in C \text{ et } x \notin B \text{ et } x \notin A) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in A \cap B \cap C) \\ &\text{ou } (x \in B \text{ et } x \notin C \text{ et } x \notin A) \text{ ou } (x \in C \text{ et } x \notin B \text{ et } x \notin A) \end{aligned}$$

D'où l'égalité $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

L'ensemble vide est le neutre pour Δ et pour tout $A \in \mathcal{P}(E)$, on a :

$$A \Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset,$$

c'est-à-dire que A est l'opposé de A pour la loi Δ (tous les éléments de $\mathcal{P}(E) \setminus \{\emptyset\}$ sont d'ordre 2, ce qui permet de retrouver la commutativité de $(\mathcal{P}(E), \Delta)$ et le fait que $\mathcal{P}(E)$ est de cardinal une puissance de 2 si E est fini).

En définitive, $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.

On vérifie facilement que \cap est commutative et associative. L'ensemble E est le neutre pour \cap . Pour A, B, C dans $\mathcal{P}(E)$, on a :

$$\begin{aligned} (x \in A \cap (B \Delta C)) &\Leftrightarrow (x \in A \text{ et } x \in B \Delta C) \\ &\Leftrightarrow (x \in A \text{ et } x \in B \text{ et } x \notin C) \text{ ou } (x \in A \text{ et } x \in C \text{ et } x \notin B) \\ &\Leftrightarrow (x \in A \cap B \text{ et } x \notin C) \text{ ou } (x \in A \cap C \text{ et } x \notin B) \\ &\Leftrightarrow (x \in A \cap B \text{ et } x \notin A \cap C) \text{ ou } (x \in A \cap C \text{ et } x \notin A \cap B) \\ &\Leftrightarrow (x \in (A \cap B) \setminus (A \cap C)) \text{ ou } (x \in (A \cap C) \setminus (A \cap B)) \\ &\Leftrightarrow x \in (A \cap B) \Delta (A \cap C) \end{aligned}$$

c'est-à-dire que \cap est distributive par rapport à Δ .

En définitive, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif et unitaire.

Exercice 21.3 Soient A_1, A_2 deux anneaux. Montrer que le produit direct $A_1 \times A_2$ muni des lois :

$$\begin{cases} ((a_1, a_2), (b_1, b_2)) \mapsto (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \\ ((a_1, a_2), (b_1, b_2)) \mapsto (a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2) \end{cases}$$

est un anneau.

Solution 21.3 *Laissée au lecteur.*

De manière plus générale, si A_1, \dots, A_p sont des anneaux, on peut alors munir le produit direct $\prod_{k=1}^p A_k = A_1 \times \dots \times A_p$ d'une structure d'anneau comme dans le cas où $p = 2$. Si $A_k = A$ pour tout k compris entre 1 et p , on note alors A^p cet anneau produit.

Avec le théorème qui suit, on donne un résumé des règles de calculs utilisables dans un anneau.

Théorème 21.1 Dans un anneau $(A, +, \cdot)$, on a les règles de calcul suivantes :

- $a \cdot 0 = 0 \cdot a = 0$;
- $(-a) \cdot b = a \cdot (-b) = -a \cdot b$;
- $(-a) \cdot (-b) = a \cdot b$;
- $(a - b) \cdot c = a \cdot c - b \cdot c$;
- $a \cdot (b - c) = a \cdot b - a \cdot c$;
- $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$;
- $a \cdot \left(\sum_{k=1}^p b_k \right) = \sum_{k=1}^p a \cdot b_k$;
- $\left(\sum_{k=1}^p b_k \right) \cdot a = \sum_{k=1}^p b_k \cdot a$;

où a, b, c, a_1, \dots, a_p sont des éléments de A , p un entier naturel non nul et n un entier relatif.

Démonstration.

- On a $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ et simplifiant par $a \cdot 0$ dans le groupe $(A, +)$, on en déduit que $a \cdot 0 = 0$.

- De $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$, on déduit que $(-a) \cdot b = -a \cdot b$.
- On en déduit que $(-a) \cdot (-b) = -a \cdot (-b) = -(-a \cdot b) = a \cdot b$ (dans un groupe, l'opposé de l'opposé et l'élément).
- On en déduit aussi que $(a - b) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c - b \cdot c$.
- On montre d'abord par récurrence sur $n \geq 0$ que $n(a \cdot b) = (na) \cdot b$. C'est vrai pour $n = 0$ et supposant que c'est vrai pour $n \geq 0$, on a :

$$\begin{aligned}(n+1)(a \cdot b) &= n(a \cdot b) + a \cdot b = (na) \cdot b + a \cdot b \\ &= (na + a) \cdot b = ((n+1)a) \cdot b\end{aligned}$$

Ensuite avec $(-n)(a \cdot b) = -n(a \cdot b) = -(na) \cdot b = (-na) \cdot b$, on déduit que le résultat est valable pour les entiers relatifs.

- Les deux derniers résultats se montrent facilement par récurrence sur $p \geq 1$. ■

Sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} , une formule intéressante est celle du binôme de Newton. Elle est en fait valable sur anneau unitaire quand les éléments commutent.

Théorème 21.2 *Soit $(A, +, \cdot)$ un anneau unitaire.*

Si a et b commutent dans A , on a alors pour tout entier naturel n :

$$(a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

(formule du binôme de Newton).

Démonstration. On procède par récurrence sur $n \geq 0$. Pour $n = 0$ et $n = 1$, c'est évident. En supposant le résultat acquis au rang $n \geq 1$, on a :

$$\begin{aligned}(a + b)^{n+1} &= (a + b)^n (a + b) = \left(\sum_{k=0}^n C_n^k a^k b^{n-k} \right) (a + b) \\ &= \sum_{k=0}^n C_n^k a^{k+1} b^{n-k} + \sum_{k=0}^n C_n^k a^k b^{n-(k-1)} \\ &= \sum_{k=1}^{n+1} C_n^{k-1} a^k b^{n-(k-1)} + \sum_{k=0}^n C_n^k a^k b^{n-(k-1)} \\ &= b^{n+1} + \sum_{k=1}^n (C_n^{k-1} + C_n^k) a^k b^{n+1-k} + a^{n+1}\end{aligned}$$

et tenant compte de $C_n^{k-1} + C_n^k = C_{n+1}^k$ (triangle de Pascal), cela s'écrit :

$$(a + b)^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k a^k b^{n+1-k}.$$

Le résultat est donc vrai pour tout $n \geq 0$. ■

Remarque 21.1 *Si a et b ne commutent pas, la formule du binôme n'est plus nécessairement vrai. Par exemple dans $\mathcal{M}_n(\mathbb{R})$ en considérant deux matrices A et B telles que $AB \neq BA$, on a :*

$$(A + B)^2 = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2.$$

Par exemple, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donnent :

$$AB = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad BA = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

et pour $c \neq 0$, on a $AB \neq BA$.

Remarque 21.2 La formule du binôme peut aussi se montrer en utilisant un argument de dénombrement. Comme a et b commutent, $(a+b)^n = (a+b) \cdots (a+b)$, le produit étant effectué n fois, est une somme de monômes $a^k b^{n-k}$ et, pour k fixé entre 0 et n , il y a autant de monômes $a^k b^{n-k}$ que de produits $aabaa \cdots$ où a intervient k fois et b intervient $n-k$ fois. Dans une telle liste, il y a C_n^k façons de choisir la position des k éléments a (les a étant placés, les b le sont automatiquement), ce qui donne la formule.

L'identité remarquable qui suit, pour a et b qui commutent, est aussi intéressante.

Théorème 21.3 Soit $(A, +, \cdot)$ un anneau unitaire.

Si a et b commutent dans A , on a alors pour tout entier naturel n :

$$b^{n+1} - a^{n+1} = (b-a) \sum_{k=0}^n a^k b^{n-k}.$$

Démonstration. On procède par récurrence sur $n \geq 0$. Pour $n = 0$, c'est évident. En supposant le résultat acquis au rang $n \geq 0$, on a :

$$\begin{aligned} b^{n+2} - a^{n+2} &= (b^{n+1} - a^{n+1})b + ba^{n+1} - a^{n+2} \\ &= (b-a) \sum_{k=0}^n a^k b^{n+1-k} + (b-a)a^{n+1} \\ &= (b-a)(b^{n+1} + ab^n + \cdots + a^{n-1}b^2 + a^n b) + (b-a)a^{n+1} \\ &= (b-a) \sum_{k=0}^{n+1} a^k b^{n+1-k}. \end{aligned}$$

Le résultat est donc vrai pour tout $n \geq 0$. ■

Remarque 21.3 Si a et b ne commutent pas, ce résultat n'est plus nécessairement vrai. Par exemple dans $\mathcal{M}_n(\mathbb{R})$ en considérant deux matrices A et B telles que $AB \neq BA$, on a :

$$(B-A)(B+A) = B^2 - AB + BA - A^2 \neq B^2 - A^2.$$

Par exemple, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donnent :

$$AB = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad BA = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

et pour $c \neq 0$, on a $AB \neq BA$.

21.2 Éléments inversibles dans un anneau unitaire

Pour ce paragraphe $(A, +, \cdot)$ est un anneau unitaire.

On note A^\times l'ensemble des éléments de A inversibles pour la multiplication, c'est-à-dire l'ensemble des éléments $a \in A$ pour lesquels il existe un élément $a' \in A$ tel que $a \cdot a' = a' \cdot a = 1$. Quand il existe un tel inverse est unique et on le note a^{-1} .

Comme $1 \neq 0$ dans A , on a $A^\times \subset A \setminus \{0\}$ et cette inclusion peut être stricte.

Remarque 21.4 *L'exercice 20.7 nous dit que pour vérifier qu'un élément a de l'anneau unitaire A est inversible, il suffit de vérifier qu'il a un inverse à gauche (ou à droite) puisque la loi multiplicative est associative.*

Exemple 21.5 On a $\mathbb{Z}^\times = \{-1, 1\}$ et $\mathbb{R}[X]^\times = \mathbb{R}^*$ (ensemble des polynômes constants non nuls).

Exemple 21.6 On a $(\mathcal{M}_n(\mathbb{R}))^\times = GL_n(\mathbb{R})$ [resp. $(\mathcal{M}_n(\mathbb{C}))^\times = GL_n(\mathbb{C})$].

Théorème 21.4 *Soit $(A, +, \cdot)$ un anneau unitaire. L'ensemble A^\times des éléments inversibles de A est un groupe pour le produit.*

Démonstration. A^\times est non vide puisqu'il contient 1.

Si a, b sont dans A^\times , on a alors :

$$b^{-1}a^{-1}ab = b^{-1}b = 1, \quad abb^{-1}a^{-1} = aa^{-1} = 1,$$

c'est-à-dire que ab est inversible d'inverse $b^{-1}a^{-1}$. La multiplication définit donc une loi interne sur A^\times . On sait déjà que cette loi est associative, que 1 en est le neutre et tout $a \in A^\times$ est inversible par construction d'inverse $a^{-1} \in A^\times$ (on $(a^{-1})^{-1} = a$). (A^\times, \cdot) est donc un groupe. ■

Définition 21.2 *On dit que A^\times est le groupe des unités de A .*

Exercice 21.4 *Soit $(A, +, \cdot)$ un anneau unitaire. Montrer que si $a \in A$ est tel que $a^n = 0$ pour un entier $n \geq 1$ (on dit alors que a est nilpotent), alors $1 - a$ est inversible d'inverse $\sum_{k=0}^{n-1} a^k$.*

Solution 21.4 On a :

$$1 - a^n = (1 - a) \sum_{k=0}^{n-1} a^k$$

pour $n \geq 1$ et $a^n = 0$ donne $(1 - a) \sum_{k=0}^{n-1} a^k = 1$, ce qui signifie que $1 - a$ est inversible d'inverse

$$\sum_{k=0}^{n-1} a^k.$$

Exercice 21.5 *Soit $(A, +, \cdot)$ un anneau unitaire.*

1. *Montrer que si a, b sont deux éléments de A tels que $1 - ab$ soit inversible d'inverse u , alors $1 - ba$ est aussi inversible d'inverse $1 + b \cdot u \cdot a$.*
2. *En déduire que si A, B sont deux matrices réelles ou complexes, alors AB et BA ont les mêmes valeurs propres.*

Solution 21.5

1. On a :

$$\begin{aligned}
 (1 - ba)(1 + bua) &= 1 - ba + bua - babua \\
 &= 1 + b(-1 + u - abu)a \\
 &= 1 - b(-1 + (1 - ab)u)a \\
 &= 1 - b(-1 + 1)a = 1
 \end{aligned}$$

puisque $(1 - ab)u = 1$ (l'idée de cet in verse peut être inspirée par le calcul dans \mathbb{R} : $\frac{1}{1 - ba} = 1 + \frac{ba}{1 - ab} = 1 + bua$).

2. Dire que 0 est valeur propre de AB équivaut à dire que $\det(AB) = 0$ et comme $\det(AB) = \det(BA)$, cela équivaut à dire 0 est valeur propre de BA .

Dire que $\lambda \neq 0$ est valeur propre de AB équivaut à dire que $\lambda I_n - AB$ est non inversible, ce qui revient à dire que $I_n - \frac{1}{\lambda}AB$ est non inversible et cela équivaut à dire que $I_n - \frac{1}{\lambda}BA$ est non inversible, donc que λ est aussi valeur propre de BA .

Remarque 21.5 On peut en fait montrer que si A, B sont deux matrices réelles ou complexes, alors AB et BA ont le même polynôme caractéristique.

Définition 21.3 On dit que $a \in A$ est un diviseur de 0 si $a \neq 0$ et s'il existe $b \neq 0$ dans A tel que $a \cdot b = 0$.

Remarque 21.6 Un diviseur de 0 dans un anneau unitaire n'est jamais inversible (pour la multiplication) et, par contraposée, un élément inversible ne peut être un diviseur de 0.

Remarque 21.7 Si a est un diviseur de 0, une égalité de la forme $a \cdot b = a \cdot c$ ne peut être simplifiée a priori. Un élément simplifiable pour le produit ne peut donc être un diviseur de 0.

Définition 21.4 Un anneau est dit intègre s'il est commutatif et n'admet pas de diviseur de 0.

Dans un anneau intègre, on a :

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Exemple 21.7 Dans un anneau de Boole $(\mathcal{P}(E), \Delta, \cap)$, on a pour toute partie A de E :

$$A \cap (E \setminus A) = \emptyset$$

et donc tout $A \neq \emptyset$ est un diviseur de \emptyset (le 0 pour la loi Δ). Donc cet anneau n'est pas intègre.

Exemple 21.8 Les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont intègres.

Exemple 21.9 L'anneau $\mathbb{R}[X]$ est intègre.

Exemple 21.10 L'anneau $\mathcal{M}_n(\mathbb{R})$ [resp. $\mathcal{M}_n(\mathbb{C})$] est non intègre puisque non commutatif. Sans se préoccuper de la commutativité, on peut trouver des diviseurs de 0 dans $\mathcal{M}_n(\mathbb{R})$. Par exemple, pour $n = 2$, on a $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$ et aucune de ces deux matrices n'est nulle.

Exemple 21.11 Soient A_1, A_2 deux anneaux. Dans l'anneau produit $A_1 \times A_2$, on a $(a_1, 0) \cdot (0, a_2) = (0, 0)$, c'est-à-dire que pour $a_1 \neq 0$ et $a_2 \neq 0$, $(a_1, 0)$ et $(0, a_2)$ sont des diviseurs de 0. Donc, pour A_1 et A_2 non réduits à $\{0\}$, $A_1 \times A_2$ n'est jamais intègre.

21.3 Sous-anneaux

Définition 21.5 Soit $(A, +, \cdot)$ un anneau. Un sous-anneau de A est une partie non vide B de A telle que $(B, +)$ est un sous-groupe de A et B est stable pour la multiplication, c'est-à-dire que pour tous a, b dans B , $a \cdot b$ est aussi dans B .

Si l'anneau A est unitaire, B doit contenir 1.

Il est facile de vérifier qu'un sous-anneau d'un anneau et lui-même un anneau.

Théorème 21.5 Soit $(A, +, \cdot)$ un anneau et B une partie non vide de A . B est un sous-anneau de A si, et seulement si :

$$\forall (a, b) \in B^2, \begin{cases} a - b \in B \\ a \cdot b \in B \end{cases}$$

(pour A unitaire, il faut ajouter $1 \in B$).

Démonstration. Laissée au lecteur. ■

Exemple 21.12 Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ muni des opérations usuelles sont des sous-anneaux de \mathbb{C} .

Exemple 21.13 Pour $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou \mathbb{C} , l'ensemble $\mathbb{K}[x]$ des fonctions polynomiales à coefficients dans \mathbb{K} , est un sous-anneau de $\mathbb{K}^{\mathbb{K}}$.

Exercice 21.6 On appelle nombre décimal tout nombre rationnel de la forme $\frac{a}{10^m}$ où a est un entier relatif et m un entier naturel.

1. Montrer que l'ensemble D des nombres décimaux est un anneau unitaire, commutatif et intègre.
2. Montrer que l'ensemble des nombres décimaux inversibles est :

$$D^\times = \{r = \pm 2^\alpha 5^\beta \mid (\alpha, \beta) \in \mathbb{Z}^2\}.$$

Solution 21.6

1. Facile.
2. Un rationnel $r = \frac{a}{10^m}$ est inversible dans \mathbb{D} si, et seulement si, il existe un entier relatif b et un entier naturel n tels que $\frac{a}{10^m} \frac{b}{10^n} = 1$, ce qui revient à dire que $ab = 10^{n+m}$ ou encore que 2 et 5 sont les seuls diviseurs premiers possibles de a et b .

Exercice 21.7 Soit $p \geq 2$ un entier sans facteurs carrés dans sa décomposition en produit de nombres premiers (c'est-à-dire que $p = \prod_{k=1}^r p_k$ où les p_k sont premiers deux à deux distincts).

1. Montrer que l'ensemble :

$$\mathbb{Z}[\sqrt{p}] = \{n + m\sqrt{p} \mid (n, m) \in \mathbb{Z}^2\}$$

est un sous anneau de \mathbb{R} .

2. Montrer que $n + m\sqrt{p} = 0$ dans $\mathbb{Z}[\sqrt{p}]$ si, et seulement si, $n = m = 0$ (ce qui signifie que l'écriture $a = n + m\sqrt{p}$ d'un élément de $\mathbb{Z}[\sqrt{p}]$ est unique).
3. Quels sont les éléments de \mathbb{Z} (qui est contenu dans $\mathbb{Z}[\sqrt{p}]$) qui sont inversibles.

4. Montrer que si $n + m\sqrt{p}$ est inversible dans $\mathbb{Z}[\sqrt{p}]$, il en est alors de même de $n - m\sqrt{p}$.
 5. Montrer que le groupe des éléments inversibles de $\mathbb{Z}[\sqrt{p}]$ est :

$$(\mathbb{Z}[\sqrt{p}])^\times = \{n + m\sqrt{p} \in \mathbb{Z}[\sqrt{p}] \mid n^2 - pm^2 = \pm 1\}$$

Solution 21.7

1. On a $1 = 1 + 0\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Pour $a = n + m\sqrt{p}$ et $a' = n' + m'\sqrt{p}$ dans $\mathbb{Z}[\sqrt{p}]$, on a :

$$\begin{cases} a - a' = (n - n') + (m - m')\sqrt{p} \in \mathbb{Z}[\sqrt{p}] \\ aa' = (nn' + pmm') + (nm' + mn')\sqrt{p} \in \mathbb{Z}[\sqrt{p}] \end{cases}$$

Donc $\mathbb{Z}[\sqrt{p}]$ est un sous anneau de \mathbb{R} .

2. Si $a = n + m\sqrt{p} = 0$ avec $m \neq 0$, on a alors $\sqrt{p} = -\frac{n}{m} \in \mathbb{Q}$, ce qui n'est pas possible si p est sans facteurs carrés. En effet $\sqrt{p} = \frac{a}{b}$ avec a, b premiers entre eux dans \mathbb{N}^* , donne

$$a^2 = pb^2, \text{ donc } p_1 \text{ divise } a, \text{ soit } a = p_1 a_1 \text{ et } p_1^2 a_1^2 = pb^2, \text{ soit } p_1 a_1^2 = \prod_{k=2}^r p_k b^2 \text{ et } p_1 \text{ va}$$

diviser b (il est premier avec $\prod_{k=2}^r p_k$ dans le cas où $r \geq 2$), ce qui contredit $a \wedge b = 1$.

L'égalité $n + m\sqrt{p} = 0$ entraîne donc $m = 0$ et $n = 0$.

3. Si $n \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{p}]$ est inversible, il existe alors $n' + m'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ tel que $n(n' + m'\sqrt{p}) = nn' + nm'\sqrt{p} = 1$, ce qui entraîne $nn' = 1$ et $nm' = 0$, soit $m' = 0$ et $nn' = 1$ dans \mathbb{Z} , ce qui donne $n = n' = \pm 1$. Donc :

$$\mathbb{Z} \cap (\mathbb{Z}[\sqrt{p}])^\times = \mathbb{Z}^\times = \{-1, 1\}$$

4. Si $a = n + m\sqrt{p}$ est inversible dans $\mathbb{Z}[\sqrt{p}]$, il existe alors $a' = n' + m'\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ tel que $aa' = 1$, soit $(nn' + pmm') + (nm' + mn')\sqrt{p} = 1$, ce qui entraîne $nn' + pmm' = 1$ et $nm' + mn' = 0$ (unicité de l'écriture $n + m\sqrt{p}$ dans $\mathbb{Z}[\sqrt{p}]$). Il en résulte que :

$$(n - m\sqrt{p})(n' - m'\sqrt{p}) = (nn' + pmm') - (nm' + mn')\sqrt{p} = 1$$

et $n - m\sqrt{p}$ est inversible dans $\mathbb{Z}[\sqrt{p}]$.

5. Si $a = n + m\sqrt{p}$ est inversible dans $\mathbb{Z}[\sqrt{p}]$, il en est alors de même de $n - m\sqrt{p}$ et du produit $(n + m\sqrt{p})(n - m\sqrt{p}) = n^2 - pm^2$ ($\mathbb{Z}[\sqrt{p}]$ est un groupe multiplicatif), ce qui entraîne $n^2 - pm^2 = \pm 1$. Réciproquement, si n et m sont tels que $n^2 - pm^2 = \pm 1$, on a alors $(n + m\sqrt{p})(n - m\sqrt{p}) = \pm 1$ et $n + m\sqrt{p}$ est inversible d'inverse $\pm(n - m\sqrt{p})$. On peut montrer que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont les éléments de la forme $\pm(1 + \sqrt{2})^n$ où n est un entier relatif, l'inverse de $\pm(1 + \sqrt{2})^n$ étant $\pm(-1 + \sqrt{2})^n$.

Exercice 21.8 On désigne par p un entier naturel non nul et par $\mathbb{Z}[i\sqrt{p}]$ l'ensemble des nombres complexes défini par :

$$\mathbb{Z}[i\sqrt{p}] = \{a + ib\sqrt{p} \mid (a, b) \in \mathbb{Z}^2\}.$$

1. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est un anneau unitaire commutatif et intègre (pour $p = 1$, $\mathbb{Z}[i]$ est l'anneau des entiers de Gauss).
 2. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est contenu dans tout sous anneau unitaire de \mathbb{C} qui contient $i\sqrt{p}$. L'anneau $\mathbb{Z}[i\sqrt{p}]$ est donc le plus petit sous anneau de \mathbb{C} (pour l'ordre de l'inclusion) qui contient $i\sqrt{p}$, on dit que c'est le sous anneau de \mathbb{C} engendré par $i\sqrt{p}$.

3. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est égal à l'intersection de tous les sous anneaux de \mathbb{C} qui contiennent i .
4. Déterminer le groupe $\mathbb{Z}[i\sqrt{p}]^\times$ des éléments inversibles de $\mathbb{Z}[i\sqrt{p}]$.

Solution 21.8

1. Il suffit de montrer que $\mathbb{Z}[i\sqrt{p}]$ est un sous anneau de \mathbb{C} .
On a $1 = 1 + i \cdot 0 \cdot \sqrt{p} \in \mathbb{Z}[i\sqrt{p}]$. Pour $z = a + ib\sqrt{p}$ et $z' = a' + ib'\sqrt{p}$, où a, a', b, b' sont des entiers relatifs, on a :

$$\begin{cases} z - z' = (a - a') + (b - b')i\sqrt{p} \in \mathbb{Z}[i\sqrt{p}] \\ zz' = (aa' - pbb') + (ab' + ba')i\sqrt{p} \in \mathbb{Z}[i\sqrt{p}] \end{cases}$$

Donc $\mathbb{Z}[i\sqrt{p}]$ est un sous anneau de \mathbb{C} et comme \mathbb{C} , il est unitaire commutatif et intègre.

2. Si un anneau A contient $i\sqrt{p}$, il contient également 1 (il s'agit d'anneaux unitaires) et en conséquence il contient tout élément de la forme $a + ib\sqrt{p}$ avec $(a, b) \in \mathbb{Z}^2$. On a donc $\mathbb{Z}[i\sqrt{p}] \subset A$.
3. En désignant par $(A_i)_{i \in I}$ la famille de tous les sous anneaux de \mathbb{C} qui contiennent $i\sqrt{p}$, on a $A = \bigcap_{i \in I} A_i \subset \mathbb{Z}[i\sqrt{p}]$ puisque $\mathbb{Z}[i\sqrt{p}]$ est l'un de ces sous-anneaux et $\mathbb{Z}[i\sqrt{p}] \subset A$ puisque A est un anneau. On a donc bien $\mathbb{Z}[i\sqrt{p}] = A$.
4. Si $z = a + ib\sqrt{p}$ est inversible dans $\mathbb{Z}[i\sqrt{p}]$, il existe alors $z' \in \mathbb{Z}[i\sqrt{p}]$ tel que $zz' = 1$ et $|z|^2 |z'|^2 = 1$ avec $|z|^2 = a^2 + b^2 p^2 \in \mathbb{N}$ et $|z'|^2 \in \mathbb{N}$, ce qui impose $|z|^2 = |z'|^2 = 1$. On a donc $a^2 + b^2 p^2 = 1$ avec $(a^2, b^2 p^2) \in \mathbb{N}^2$, ce qui équivaut à $(a^2, b^2 p^2) = (1, 0)$ ou $(a^2, b^2 p^2) = (0, 1)$ ou encore à $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b^2 p^2 = 1$. Pour $p = 1$, la condition $b^2 p^2 = 1$ équivaut à $b = \pm 1$ et pour $p \geq 2$, elle n'est jamais réalisée puisque, pour tout $b \in \mathbb{Z}$, on a $b^2 p^2 = 0$ ou $b^2 p^2 \geq p^2 \geq 4$. On a donc $\mathbb{Z}[i]^\times \subset \{-1, 1, -i, i\}$ et $\mathbb{Z}[i\sqrt{p}]^\times \subset \{-1, 1\}$ pour $p \geq 2$. Les inclusions réciproques se vérifiant facilement. En définitive, on a :

$$\mathbb{Z}[i\sqrt{p}]^\times = \begin{cases} \{-1, 1, -i, i\} & \text{si } p = 1, \\ \{-1, 1\} & \text{si } p \geq 2. \end{cases}$$

Exercice 21.9 Soit A un anneau commutatif unitaire et $\mathcal{M}_n(A)$ l'anneau des matrices carrées d'ordre n à coefficients dans A .

1. Montrer que l'ensemble $GL_n(A)$ des matrices carrées d'ordre n à coefficients dans A telles que :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{i, \sigma(i)} \in A^\times$$

où \mathfrak{S}_n désigne l'ensemble de toutes les permutations de $\{1, \dots, n\}$ et, pour $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma)$ la signature de σ , est un groupe multiplicatif.

2. Montrer que $GL_n(A)$ est le groupe des unités de $\mathcal{M}_n(A)$ (pour $A = \mathbb{R}$ ou $A = \mathbb{C}$, on retrouve un résultat classique).

Solution 21.9 Laissée au lecteur.

Exercice 21.10 On dit qu'un nombre réel α est algébrique s'il existe un polynôme non nul P dans $\mathbb{Q}[X]$ tel que $P(\alpha) = 0$.

Un nombre réel qui n'est pas algébrique est dit transcendant.

On note \mathbb{A} l'ensemble des nombres réels algébriques.

1. Montrer que les réels $\alpha = \sqrt{2}$ et $\beta = \sqrt{\frac{1+\sqrt{5}}{2}}$ sont algébriques.
2. Montrer que le réel $\beta = \sqrt[3]{2} + \sqrt[3]{4}$ est algébrique.
3. Soient α, β deux nombres algébriques et $P(X) = \sum_{k=0}^n a_k X^k$, $Q(X) = \sum_{k=0}^m b_k X^k$ deux polynômes non nuls dans $\mathbb{Q}[X]$ tels que $P(\alpha) = 0$ et $Q(\beta) = 0$, avec $a_n = b_m = 1$. On note :

$$\{\alpha^i \beta^j \mid 0 \leq i \leq n-1, 0 \leq j \leq m-1\} = \{\gamma_k \mid 1 \leq k \leq p\}$$
 où $p = nm$ et $\gamma_1 = \alpha^0 \beta^0 = 1$. On désigne par V le vecteur de \mathbb{R}^p de composantes $\gamma_1, \dots, \gamma_p$.
 - (a) Montrer qu'il existe deux matrices carrées d'ordre p à coefficients rationnels A et B telles que $\alpha V = AV$ et $\beta V = BV$.
 - (b) Montrer que \mathbb{A} est un anneau commutatif unitaire.

Solution 21.10

1. $\alpha = \sqrt{2}$ est annulé par $X^2 - 2 \in \mathbb{Q}[X] \setminus \{0\}$.
On a $2\beta^2 = 1 + \sqrt{5}$ et $(2\beta^2 - 1)^2 = 5$. Le réel β est donc annulé par le polynôme $P(X) = X^4 - X^2 - 1 \in \mathbb{Q}[X]$ et en conséquence il est algébrique.
2. On a $\beta = \alpha + \alpha^2$, où $\alpha = \sqrt[3]{2}$ est algébrique annulé par $X^3 - 2$. De $\alpha^3 = 2$, on déduit que :

$$\beta^2 = \alpha^2 + 2\alpha + 4, \quad \beta^3 = 6(\alpha^2 + \alpha + 1) = 6\beta + 6$$

β est donc algébrique annulé par $P(X) = X^3 - 6X - 6$.

3.

- (a) Pour tout entier k compris entre 1 et p il existe deux indices i, j tels que $\gamma_k = \alpha^i \beta^j$ et $\alpha \gamma_k = \alpha^{i+1} \beta^j$. Pour i compris entre 0 et $n-2$, $\alpha \gamma_k$ est l'un des γ_r et pour $i = n-1$, on a :

$$\alpha \gamma_k = \alpha^n \beta^j = - \sum_{r=0}^{n-1} a_r \alpha^r \beta^j$$

qui est une combinaison linéaire à coefficients rationnels des $\gamma_1, \dots, \gamma_p$. Il existe donc une matrice A dans $\mathcal{M}_p(\mathbb{Q})$ telle que $\alpha V = AV$.

De manière analogue, on voit qu'il existe une matrice B dans $\mathcal{M}_p(\mathbb{Q})$ telle que $\beta V = BV$.

- (b) On a $1 \in \mathbb{A}$, de manière évidente.

Pour α, β dans \mathbb{A} , on a avec les notations précédentes, $(A - B)V = (\alpha - \beta)V$ avec V non nul dans \mathbb{R}^p , ce qui signifie que $\alpha - \beta$ est une valeur propre de la matrice $A - B$, c'est donc une racine du polynôme caractéristique χ_{A-B} qui est dans $\mathbb{Q}[X]$ puisque $A - B$ est une matrice à coefficients rationnels. Il en résulte que $\alpha - \beta$ est algébrique. De même avec $(AB)V = (\alpha\beta)V$ on déduit que $\alpha\beta$ est algébrique.

En conclusion \mathbb{A} est un sous-anneau de \mathbb{R} .

21.4 Morphismes d'anneaux

Les anneaux considérés sont supposés unitaires.

On désigne par $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux unitaires. On note respectivement 0 et 1 les éléments neutres de ces anneaux pour l'addition et la multiplication (en cas d'ambiguïté, on les notera $0_A, 0_B, 1_A$ et 1_B).

Définition 21.6 On dit que φ est un morphisme d'anneaux de A dans B si φ est une application de A dans B telle que :

- $\varphi(1) = 1$;
- $\forall (a, b) \in A^2, \varphi(a + b) = \varphi(a) + \varphi(b)$;
- $\forall (a, b) \in A^2, \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Dans le cas où φ est de plus bijective, on dit que φ est un isomorphisme d'anneaux A sur B . Dans le cas où $A = B$, on dit que φ est un endomorphisme de l'anneau A et que c'est un automorphisme de l'anneau A si φ est de plus bijective.

On peut remarquer qu'un morphisme d'anneaux de A dans B est en particulier un morphisme de groupes de $(A, +)$ dans $(B, +)$. On a donc $\varphi(0) = 0$ et $\varphi(-a) = -\varphi(a)$ pour tout $a \in A$.

Définition 21.7 Soit φ un morphisme d'anneaux de A dans B

1. Le noyau de φ est l'ensemble :

$$\ker(\varphi) = \{x \in A \mid \varphi(x) = 0\}.$$

2. L'image de φ est l'ensemble :

$$\operatorname{Im}(\varphi) = \{\varphi(x) \mid x \in A\}.$$

Il est facile de vérifier que $\ker(\varphi)$ est un sous-anneau de A et $\operatorname{Im}(\varphi)$ un sous-anneau de B .

En fait pour tout $x \in \ker(\varphi)$ et tout $y \in A$, on a $\varphi(xy) = \varphi(x)\varphi(y) = 0 \cdot \varphi(y) = 0$, c'est-à-dire que $xy \in \ker(\varphi)$. Cette propriété se traduit en disant que $\ker(\varphi)$ est un idéal de l'anneau A .

Un tel morphisme est injectif [resp. surjectif] si, et seulement si, $\ker(\varphi) = \{0\}$ [resp. $\operatorname{Im}(\varphi) = B$].

Structure de corps

22.1 Corps

Définition 22.1 Soit \mathbb{K} un ensemble non vide muni de deux lois de composition interne notées $+$ (une addition) et \cdot (une multiplication). On dit que $(\mathbb{K}, +, \cdot)$ est un corps si :

- $(\mathbb{K}, +, \cdot)$ est un anneau unitaire (avec $1 \neq 0$);
- tous les éléments de $\mathbb{K} \setminus \{0\}$ sont inversibles pour la multiplication (ce qui revient à dire que $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$).

Si de plus l'anneau $(\mathbb{K}, +, \cdot)$ est commutatif, on dit que le corps $(\mathbb{K}, +, \cdot)$ est commutatif.

Pour un corps on note aussi \mathbb{K}^* l'ensemble $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

Dire que $(\mathbb{K}, +, \cdot)$ est un corps équivaut aussi à dire que :

- $(\mathbb{K}, +, \cdot)$ est un anneau unitaire;
- (\mathbb{K}^*, \cdot) est un groupe.

Dans un corps, on notera $-a$ l'opposé d'un élément a (i. e. le symétrique pour la loi $+$) et a^{-1} ou $\frac{1}{a}$ l'inverse d'un élément non nul a (i. e. le symétrique pour la loi \cdot).

Dans un corps tout élément non nul est simplifiable et il n'y a pas de diviseurs de 0. Un corps est donc en particulier un anneau intègre.

Les règles de calcul valables dans un anneau (exercice 21.1) le sont aussi dans un corps avec de plus l'équivalence :

$$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Dans un corps commutatif, pour $(a, b) \in \mathbb{K}^* \times \mathbb{K}$, on écrira $a^{-1} \cdot b = \frac{b}{a}$ (si le corps n'est pas commutatif on a, a priori, $a^{-1} \cdot b \neq b \cdot a^{-1}$ et l'écriture $\frac{b}{a}$ est ambiguë).

Exercice 22.1 Montrer que si \mathbb{K} est un corps, alors l'anneau produit $\mathbb{K}^2 = \mathbb{K} \times \mathbb{K}$ n'est pas un corps.

Solution 22.1 Pour $x \in \mathbb{K}^*$, on a $(x, 0) \cdot (0, x) = (0, 0)$, il existe donc des diviseurs de 0 dans l'anneau produit \mathbb{K}^2 et en conséquence ce n'est pas un corps.

Exemple 22.1 Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ muni des opérations usuelles sont des corps commutatifs. Mais \mathbb{Z} n'est pas un corps.

Exercice 22.2 Montrer que l'ensemble :

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid (a, b) \in \mathbb{C}^2 \right\}$$

(où \bar{a} est le nombre complexe conjugué de a) est un corps non commutatif (corps des quaternions de Hamilton).

Solution 22.2 On montre d'abord que \mathbb{H} est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$. On a $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$ et pour $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $B = \begin{pmatrix} a' & b' \\ -\bar{b}' & \bar{a}' \end{pmatrix}$ dans \mathbb{H} , on a :

$$A - B = \begin{pmatrix} a - a' & b - b' \\ -(\bar{b} - \bar{b}') & \bar{a} - \bar{a}' \end{pmatrix} \in \mathbb{H}$$

et :

$$AB = \begin{pmatrix} aa' - b\bar{b}' & ab' + \bar{a}'b \\ -(\bar{a}b' + a'\bar{b}) & \bar{a}a' - \bar{b}b' \end{pmatrix} \in \mathbb{H}.$$

Donc \mathbb{H} est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$.

Pour $A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in \mathbb{H}$ on a $\det(A) = |a|^2 + |b|^2$, de sorte que $\det(A) \neq 0$ pour $A \neq 0$ et A est inversible dans $\mathcal{M}_2(\mathbb{C})$ d'inverse :

$$A^{-1} = \frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \in \mathbb{H}$$

Il en résulte que \mathbb{H} est un corps.

Au vu de la formule donnant le produit AB de deux matrices dans \mathbb{H} , on voit que ce corps n'est pas commutatif. Par exemple, pour $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, on a :

$$AB = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} \neq BA = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Dans un corps on a en général plus de facilités à résoudre certaines équations que dans un anneau.

Par exemple dans un anneau une équation de la forme $ax + b = 0$ n'a pas nécessairement de solution. On peut considérer le cas d'un anneau de matrices. Si A, B sont des matrices réelles d'ordre n , l'équation $AX + B = 0$ équivaut à $AX = -B$ qui donne $\det(A)\det(X) = (-1)^n \det(B)$ et pour A non inversible, B inversible, on aboutit à une impossibilité puisque $\det(A) = 0$ et $\det(B) \neq 0$.

Exercice 22.3 Soit $(\mathbb{K}, +, \cdot)$ un corps commutatif.

1. Montrer que pour tout $(a, b) \in \mathbb{K}^* \times \mathbb{K}$ l'équation $ax + b = 0$ a une unique solution.
2. Soit $\lambda \in \mathbb{K}$. Montrer que s'il existe $\alpha \in \mathbb{K}$ tel que $\alpha^2 = \lambda$, alors l'équation $x^2 = \lambda$ a deux solutions exactement dans \mathbb{K} , à savoir α et $-\alpha$.
3. Soit $(a, b, c) \in \mathbb{K}^* \times \mathbb{K}^2$. Montrer que si l'équation $ax^2 + bx + c = 0$ a une solution x_1 dans \mathbb{K} , elle en a alors une seconde x_2 . Dans ce cas, on a $x_1 + x_2 = -\frac{b}{a}$, $x_1x_2 = \frac{c}{a}$ et pour tout $x \in \mathbb{K}$, $ax^2 + bx + c = a(x - x_1)(x - x_2)$ (forme factorisée de $ax^2 + bx + c$). Dans un corps commutatif, une équation de degré 2 a donc 0 ou 2 solutions.

Solution 22.3

1. Dans le groupe $(\mathbb{K}, +)$, l'équation $ax + b = 0$ équivaut à $ax = -b$ (unicité de l'opposé) et comme $a \in \mathbb{K}^*$ est inversible, l'équation $ax = -b$ équivaut à $a^{-1}ax = a^{-1}(-b)$, encore équivalent à $x = -a^{-1}b$. D'où l'existence et l'unicité dans \mathbb{K} de la solution de l'équation $ax + b = 0$.
2. L'équation $x^2 = \lambda = \alpha^2$ équivaut à $x^2 - \alpha^2 = (x - \alpha)(x + \alpha) = 0$ encore équivalente à $x = \alpha$ ou $x = -\alpha$.
3. De $ax_1^2 + bx_1 + c = 0$, on déduit que pour tout $x \in \mathbb{K}$, on a :

$$\begin{aligned} ax^2 + bx + c &= ax^2 + bx + c - (ax_1^2 + bx_1 + c) \\ &= a(x^2 - x_1^2) + b(x - x_1) \\ &= (x - x_1)(a(x + x_1) + b) \end{aligned}$$

de sorte que l'équation $ax^2 + bx + c = 0$ est équivalente à $(x - x_1)(a(x + x_1) + b) = 0$ encore équivalent à $x - x_1 = 0$ ou $a(x + x_1) + b = 0$, la dernière équation ayant pour unique solution $x_2 = -a^{-1}b - x_1$. Notre équation a donc exactement deux solutions, à savoir x_1 et $x_2 = -\frac{b}{a} - x_1$. On a donc $x_1 + x_2 = -\frac{b}{a}$ et :

$$x_1x_2 = -\frac{1}{a}(bx_1 + ax_1^2) = -\frac{1}{a}(-c) = \frac{c}{a}.$$

Pour tout $x \in \mathbb{K}$, on a :

$$\begin{aligned} ax^2 + bx + c &= (x - x_1)(a(x + x_1) + b) \\ &= a(x - x_1)\left(x + x_1 + \frac{b}{a}\right) \\ &= a(x - x_1)(x - x_2). \end{aligned}$$

On a donc montré que $ax^2 + bx + c$ est factorisable dans K , si, et seulement si, l'équation $ax^2 + bx + c = 0$ a des solutions dans \mathbb{K} .

Par exemple sur \mathbb{R} , l'équation $x^2 + 1$ n'est pas factorisable.

Remarque 22.1 Dans un corps non commutatif une équation de degré 2 peut avoir plus de deux racines, elle peut même en avoir une infinité. Par exemple dans le corps \mathbb{H} des quaternions (exercice 22.2) une matrice $A \in \mathbb{H}$ est annulée par son polynôme caractéristique $P(X) = X^2 - \text{tr}(A)X + \det(A)$ (théorème de Cayley-Hamilton) et on peut trouver une infinité de matrices dans \mathbb{H} de trace et déterminant donné. Par exemple, pour tout réel θ , on a $A = \begin{pmatrix} 1 & e^{it} \\ -e^{-it} & 1 \end{pmatrix} \in \mathbb{H}$ avec $\text{tr}(A) = \det(A) = 2$. Toutes ces matrices sont solutions de $X^2 - 2X + 2 = 0$.

Exercice 22.4 Montrer qu'un anneau unitaire intègre et fini est un corps.

Solution 22.4 Soit A un anneau unitaire intègre. Pour tout $a \neq 0$ dans A , l'application $x \mapsto ax$ est injective. En effet si $ax = ay$, alors $a(x - y) = 0$ et $x - y = 0$ puisque A est intègre et $a \neq 0$. Si de plus A est fini, alors cette application est bijective et en particulier il existe $b \in A$ tel que $ab = 1$, ce qui prouve que a est inversible à droite. On montre de même que a est inversible à gauche. On a donc montré que tout élément non nul de a est inversible, ce qui revient à dire que A est un corps.

Définition 22.2 Soit $(\mathbb{K}, +, \cdot)$ un corps. On dit qu'une partie \mathbb{L} de \mathbb{K} est un sous-corps de \mathbb{K} si :

- \mathbb{L} est un sous-anneau de \mathbb{K} ;
- $\mathbb{L}^* = \mathbb{L} \setminus \{0\}$ est stable par passage à l'inverse, c'est-à-dire que pour tout $x \in \mathbb{L}^*$, x^{-1} est dans \mathbb{L}^* .

On vérifie facilement qu'un sous-corps d'un corps est lui-même un corps.

Théorème 22.1 Soit $(\mathbb{K}, +, \cdot)$ un corps et \mathbb{L} une partie non vide de \mathbb{K} . \mathbb{L} est un sous-corps de \mathbb{K} si, et seulement si :

- $1 \in \mathbb{L}$;
- $\forall (x, y) \in \mathbb{L}^2, x - y \in \mathbb{L}$;
- $\forall (x, y) \in \mathbb{L} \times \mathbb{L}^*, xy^{-1} \in \mathbb{L}$.

Démonstration. Laissée au lecteur. ■

Si \mathbb{L} est un sous-corps d'un corps \mathbb{K} , on dit alors que \mathbb{K} est une extension de \mathbb{L} .

Exemple 22.2 Les ensembles \mathbb{Q}, \mathbb{R} muni des opérations usuelles sont des sous-corps de \mathbb{C} .

Exercice 22.5 Montrer que le seul sous-corps de \mathbb{Q} est lui-même.

Solution 22.5 Laissée au lecteur.

Exercice 22.6 Soit p un entier sans facteurs carrés dans sa décomposition en produit de nombres premiers. Montrer que l'ensemble :

$$\mathbb{Q}[\sqrt{p}] = \{r + s\sqrt{p} \mid (r, s) \in \mathbb{Q}^2\}$$

est un sous-corps de \mathbb{R} .

Solution 22.6 On vérifie facilement que $\mathbb{Q}[\sqrt{p}]$ est un sous-anneau de \mathbb{R} (même démonstration que pour $\mathbb{Z}[\sqrt{p}]$ déjà rencontré). Comme \sqrt{p} est irrationnel, on a $a = r + s\sqrt{p} = 0$ si, et seulement si, $r = s = 0$. Pour $a \neq 0$ dans $\mathbb{Q}[\sqrt{p}]$, on a ;

$$a^{-1} = \frac{1}{r + s\sqrt{p}} = \frac{r - r\sqrt{p}}{r^2 - ps^2} \in \mathbb{Q}[\sqrt{p}].$$

En conclusion, $\mathbb{Q}[\sqrt{p}]$ est un sous-corps de \mathbb{R} .

Exercice 22.7 Montrer que l'ensemble :

$$\mathbb{Q}[i] = \{r + si \mid (r, s) \in \mathbb{Q}^2\}$$

est un sous-corps de \mathbb{C} .

Solution 22.7 On vérifie facilement que $\mathbb{Q}[i]$ est un sous-anneau de \mathbb{C} (même démonstration que pour $\mathbb{Z}[i]$ déjà rencontré). Pour $z \neq 0$ dans $\mathbb{Q}[i]$, on a ;

$$a^{-1} = \frac{1}{r + si} = \frac{r - si}{r^2 + s^2} \in \mathbb{Q}[i].$$

En conclusion, $\mathbb{Q}[i]$ est un sous-corps de \mathbb{C} .

Exercice 22.8 Montrer que l'ensemble \mathbb{A} des réels algébriques est un corps.

Solution 22.8 On sait déjà que \mathbb{A} est un sous-anneau de \mathbb{R} .

Si $\alpha \in \mathbb{A}^*$ est annulé par $P \in \mathbb{Q}[X] \setminus \{0\}$ de degré $n \geq 1$, alors $\frac{1}{\alpha}$ est annulé par $X^n P\left(\frac{1}{X}\right) \in \mathbb{Q}[X] \setminus \{0\}$ et en conséquence est algébrique. On en déduit que \mathbb{A} est un sous-corps de \mathbb{R} . On a ainsi un exemple de corps strictement compris entre \mathbb{Q} et \mathbb{R} .

22.2 Morphismes de corps

On désigne par $(\mathbb{K}, +, \cdot)$ et $(\mathbb{L}, +, \cdot)$ deux corps. On note respectivement 0 et 1 les éléments neutres de ces corps pour l'addition et la multiplication (en cas d'ambiguïté, on les notera $0_{\mathbb{K}}$, $0_{\mathbb{L}}$, $1_{\mathbb{K}}$ et $1_{\mathbb{L}}$).

Définition 22.3 On dit que φ est un morphisme de corps de \mathbb{K} dans \mathbb{L} si φ est une application de \mathbb{K} dans \mathbb{L} telle que :

- $\varphi(1_{\mathbb{K}}) = 1_{\mathbb{L}}$;
- $\forall (a, b) \in \mathbb{K}^2, \varphi(a + b) = \varphi(a) + \varphi(b)$;
- $\forall (a, b) \in \mathbb{K}^2, \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Dans le cas où φ est de plus bijective, on dit que φ est un isomorphisme de corps de \mathbb{K} sur \mathbb{L} .

Dans le cas où $\mathbb{K} = \mathbb{L}$, on dit que φ est un endomorphisme du corps \mathbb{K} et que c'est un automorphisme du corps \mathbb{K} si φ est de plus bijective.

On peut remarquer qu'un morphisme de corps est en fait un morphisme d'anneaux unitaires.

On a, pour un tel morphisme, $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(-a) = -\varphi(a)$ pour tout $a \in \mathbb{K}$ et $\varphi(a^{-1}) = \varphi(a)^{-1}$ pour tout $a \in \mathbb{K}^*$.

Exercice 22.9 Montrer que l'identité est le seul endomorphisme de corps non identiquement nul de \mathbb{R} .

Solution 22.9 Si f est endomorphisme du corps \mathbb{R} , on a alors $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous x, y dans \mathbb{R} .

Avec $f(1) = (f(1))^2$, on déduit que $f(1) = 0$ ou $f(1) = 1$. Si $f(1) = 0$, alors pour tout $x \in \mathbb{R}$ on a $f(x) = f(x)f(1) = 0$ et f est identiquement nulle. C'est une homothétie de rapport 0.

On suppose donc que f n'est pas identiquement nulle et on a alors $f(1) = 1$.

Avec $f(x^2) = (f(x))^2 \geq 0$, on déduit que $f(x) \geq 0$ pour tout $x \geq 0$ et pour $x \geq y$ dans \mathbb{R} , on a $f(x) - f(y) = f(x - y) \geq 0$, ce qui signifie que f est croissante. On déduit alors de l'exercice 20.37 que $f(x) = x$ pour tout $x \in \mathbb{R}$ ($\lambda = f(1) = 1$). L'identité est donc le seul morphisme de corps non identiquement nul de \mathbb{R} dans lui-même.

Division euclidienne dans \mathbb{Z}

23.1 L'anneau \mathbb{Z} des entiers relatifs

On désigne par \mathbb{Z} l'ensemble des entiers relatifs, soit :

$$\mathbb{Z} = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}.$$

On note \mathbb{Z}^* l'ensemble \mathbb{Z} privé de 0.

On rappelle que l'ensemble $(\mathbb{Z}, +, \cdot)$ des entiers relatifs est un anneau unitaire, commutatif et intègre.

En pratique on notera plutôt nm pour $n \cdot m$.

L'ensemble \mathbb{Z} est muni comme l'ensemble \mathbb{N} des entiers naturels d'une relation d'ordre total. C'est la relation \leq . Cette relation est :

— réflexive :

$$\forall n \in \mathbb{Z}, n \leq n,$$

— antisymétrique :

$$\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z}, (n \leq m, m \leq n) \Leftrightarrow n = m,$$

— transitive :

$$\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z}, \forall p \in \mathbb{Z}, \left\{ \begin{array}{l} n \leq m \\ m \leq p \end{array} \right\} \Rightarrow n \leq p.$$

— Deux éléments quelconques de \mathbb{Z} sont comparables (l'ordre est total). C'est-à-dire que pour n, m dans \mathbb{Z} on a soit $n \leq m$ soit $m \leq n$.

On dit qu'une partie A non vide de \mathbb{Z} est minorée s'il existe un entier m tel que :

$$\forall n \in A, n \geq m.$$

Si de plus m est dans A on dit alors que c'est un plus petit élément. Dans ce cas il est uniquement déterminé.

On dit qu'une partie A non vide de \mathbb{Z} est majorée s'il existe un entier M tel que :

$$\forall n \in A, n \leq M.$$

Si de plus M est dans A on dit alors que c'est un plus grand élément. Dans ce cas il est uniquement déterminé.

L'ensemble \mathbb{Z} est bien ordonné, c'est-à-dire que :

- toute partie non vide et minorée de \mathbb{Z} admet un plus petit élément ;
- toute partie non vide et majorée de \mathbb{Z} admet un plus grand élément.

23.2 Divisibilité et congruences

Définition 23.1 On dit que l'entier relatif a est divisible par l'entier relatif d , ou que a est un multiple de d , s'il existe un entier relatif q tel que $a = qd$. On note d/a .

Remarque 23.1 Si $d = 0$ alors $a = 0$ et pour $d \neq 0$ l'entier q est uniquement déterminé (une égalité $a = dq = dq'$ entraîne $d(q - q') = 0$ et $q - q' = 0$ puisque \mathbb{Z} est intègre). On se limitera donc au cas où $d \in \mathbb{Z}^*$.

Remarque 23.2 La relation de divisibilité est une relation d'ordre non totale sur \mathbb{N} . C'est à dire qu'elle est :

- réflexive : pour tout $a \in \mathbb{N}$, a/a ;
- antisymétrique : si a/b et b/a dans \mathbb{N} alors $a = b$;
- transitive : si a/b et b/c dans \mathbb{N} alors a/c .

Deux éléments quelconques de \mathbb{N} ne sont pas toujours comparables. Par exemple on n'a aucune relation de divisibilité entre 3 et 5 dans \mathbb{N} .

Sur \mathbb{Z} on a les propriétés suivantes :

- les seuls diviseurs de 1 sont 1 et -1 ;
- si d/a et $a \neq 0$, alors $|d| \leq |a|$ (si $a = 0$, on a $0 = 0 \cdot d$ pour tout $d \in \mathbb{Z}$)
- si a/b et b/a dans \mathbb{Z} alors $|a| = |b|$, (si $a = 0$, alors $b = 0$), soit $a = \pm b$ (la relation de divisibilité n'est donc pas antisymétrique sur \mathbb{Z} , elle est seulement réflexive et transitive et ce n'est pas une relation d'ordre) ;
- si d/a et d/b dans \mathbb{Z} alors $d/(\lambda a + \mu b)$ pour tous λ, μ dans \mathbb{Z} .

Pour tout entier relatif n , on note :

$$n\mathbb{Z} = \{n \cdot q \mid q \in \mathbb{Z}\}$$

l'ensemble de tous les multiples de n et :

$$\mathcal{D}_n = \{q \in \mathbb{Z} \mid q \text{ divise } n\}$$

l'ensemble de tous les diviseurs de n .

Exercice 23.1 Montrer que, pour tout entier relatif n , $n\mathbb{Z}$ est un sous-groupe additif de \mathbb{Z} .

Solution 23.1 On a $0 = n \cdot 0 \in n\mathbb{Z}$ et pour $a = pn$, $b = qn$ dans $n\mathbb{Z}$, on a, $b - a = (q - p)n \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} .

En particulier, on a $0\mathbb{Z} = \{0\}$, $\mathcal{D}_0 = \mathbb{Z}$, $1\mathbb{Z} = \mathbb{Z}$, $\mathcal{D}_1 = \{-1, 1\}$.

Nous verrons plus loin que les $n\mathbb{Z}$ sont les seuls sous-groupes de $(\mathbb{Z}, +)$.

On peut remarquer que pour tout $a = qn \in n\mathbb{Z}$ et tout $b \in \mathbb{Z}$, on a $ab = bqn \in n\mathbb{Z}$, ce qui se traduit en disant que $n\mathbb{Z}$ est un idéal de \mathbb{Z} .

Exercice 23.2 Montrer que pour tous a, b dans \mathbb{Z} , on a :

$$a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b/a \Leftrightarrow \mathcal{D}_b \subset \mathcal{D}_a$$

et :

$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b \Leftrightarrow \mathcal{D}_a = \mathcal{D}_b.$$

Solution 23.2 Si $a\mathbb{Z} \subset b\mathbb{Z}$, on a alors $a \in b\mathbb{Z}$, c'est-à-dire qu'il existe un entier q tel que $a = bq$ et b/a .

Si b/a , on a alors $a = qb$ avec $q \in \mathbb{Z}$ et tout diviseur δ de b va diviser a , ce qui signifie que $\mathcal{D}_b \subset \mathcal{D}_a$.

Si $\mathcal{D}_b \subset \mathcal{D}_a$, on a alors $b \in \mathcal{D}_a$, c'est-à-dire qu'il existe un entier q tel que $a = bq$ et pour tout pa dans $a\mathbb{Z}$, on a $pa = pqb \in b\mathbb{Z}$, c'est-à-dire que $a\mathbb{Z} \subset b\mathbb{Z}$.

On a donc ainsi montré la première série d'équivalence.

Si $a\mathbb{Z} = b\mathbb{Z}$, on a alors $a\mathbb{Z} \subset b\mathbb{Z}$ et $b\mathbb{Z} \subset a\mathbb{Z}$, donc b/a et a/b et $a = \pm b$.

Si $a = \pm b$, les entiers a et b ont les mêmes diviseurs, ce qui signifie que $\mathcal{D}_a = \mathcal{D}_b$.

Si $\mathcal{D}_a = \mathcal{D}_b$, on a alors $\mathcal{D}_a \subset \mathcal{D}_b$ et $\mathcal{D}_b \subset \mathcal{D}_a$, donc b/a et a/b et $a = \pm b$ qui équivaut à $a\mathbb{Z} = b\mathbb{Z}$.

Exercice 23.3 Déterminer tous les entiers naturels non nuls n tels que $n+1$ divise n^2+1 .

Solution 23.3 Pour tout $n \geq 1$, on a :

$$n^2 + 1 = n(n+1) - (n-1)$$

et si $n+1$ divise n^2+1 , il va aussi diviser $n-1$, c'est-à-dire qu'il existe $q \in \mathbb{N}$ tel que $n-1 = q(n+1)$. La seule valeur possible pour q est alors $q = 0$, car $q \geq 1$ entraîne $n-1 \geq n+1$ qui est impossible. On a donc nécessairement $n = 1$ et réciproquement cette valeur convient bien.

Exercice 23.4 Déterminer tous les entiers relatifs n différents de 3 tels que $n-3$ divise n^3-3 .

Solution 23.4 Pour tout $n \in \mathbb{Z}$, on a :

$$\begin{aligned} n^3 - 3 &= (n-3+3)^3 - 3 = q(n-3) + 3^3 - 3 \\ &= q(n-3) + 24 \end{aligned}$$

et si $n-3$ divise n^3-3 , il divise alors 24, c'est-à-dire que :

$$n-3 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

et :

$$n \in \{-21, -9, -5, -3, -1, 0, 1, 2, 4, 5, 6, 7, 9, 11, 15, 27\}.$$

Réciproquement ces valeurs conviennent bien.

Définition 23.2 Soient n un entier naturel et a, b deux entiers relatifs. On dit que a est congru à b modulo n si n divise $a-b$. On note

$$a \equiv b \pmod{n}$$

Dire que a est congru à b modulo n équivaut aussi à dire que $a-b \in n\mathbb{Z}$.

Pour $n = 0$, on a $0\mathbb{Z} = \{0\}$ et $a \equiv b \pmod{0}$ revient à dire que $a = b$.

Pour $n = 1$, on a $1\mathbb{Z} = \mathbb{Z}$ et la relation $a \equiv b \pmod{1}$ est toujours vérifiée.

On suppose donc, dans ce qui suit que $n \geq 2$.

On peut facilement vérifier que la relation de congruence est une relation d'équivalence.

C'est-à-dire que :

- $a \equiv a \pmod{n}$ ($a-a=0 \in n\mathbb{Z}$) ;
- $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ ($a-b \in n\mathbb{Z}$ entraîne $b-a \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe) ;
- $(a \equiv b \pmod{n}, b \equiv c \pmod{n}) \Rightarrow a \equiv c \pmod{n}$ ($a-b \in n\mathbb{Z}$ et $b-c \in n\mathbb{Z}$ entraîne $a-c = (a-b) - (b-c) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe).

Cette relation est compatible avec l'addition et la multiplication sur \mathbb{Z} . C'est-à-dire que :

$$(a \equiv b \ (n), c \equiv d \ (n)) \Rightarrow (a + c \equiv b + d \ (n), ac \equiv bd \ (n)).$$

En effet $a - b \in n\mathbb{Z}$ et $c - d \in n\mathbb{Z}$ entraîne $a + c - (b + d) = (a - b) + (c - d) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe et $ac - bd = a(c - d) + d(a - b) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un idéal de \mathbb{Z} .

Cette compatibilité permet de munir l'ensemble \mathbb{Z}_n des classes d'équivalence modulo n d'une structure d'anneau (voir le chapitre 25).

Exercice 23.5 Soient x et y dans \mathbb{Z} . Montrer que si $3x + 7y$ est multiple de 11 alors $4x - 9y$ est aussi multiple de 11.

Solution 23.5 On a $3x \equiv -7y \ (11)$ donc $15x \equiv -35y \ (11)$ avec $15x \equiv 4x \ (11)$ et $-35y \equiv 9y \ (11)$.

Exercice 23.6 Soient a et b dans \mathbb{Z} . Montrer que si $p = a^2 + b^2$ est impair supérieur ou égal à 3 alors $p - 1$ est multiple de 4.

Solution 23.6 Tout entier k est congru à 0, 1, 2 ou 3 modulo 4, donc k^2 est congru à 0 ou 1 modulo 4 et $a^2 + b^2$ est congru à 0, 1 ou 2 modulo 4. Si p est impair et $p = a^2 + b^2$ alors p est congru à 1 modulo 4 et $p - 1$ est multiple de 4.

Exercice 23.7 Soient p, q deux entiers naturels impairs et $a = 3p + 2$, $b = 3q + 2$. Déterminer tous les entiers naturels n tels que $a^n - b^{2n}$ soit divisible par 6.

Solution 23.7 L'entier $m = a^n - b^{2n}$ est pair comme différence de nombres impairs. Il est donc divisible par 6 si, et seulement si, il est divisible par 3. Avec $a \equiv 2 \ (3)$ et $b \equiv 2 \ (3)$ on déduit que $m \equiv 2^n - 2^{2n} \ (3)$ et m est divisible par 3 si, et seulement si $2^n - 2^{2n} \equiv 0 \ (3)$ ce qui équivaut à $2^n \equiv 1 \ (3)$ encore équivalent à dire que n est pair.

23.3 Le théorème de division euclidienne dans \mathbb{Z}

Théorème 23.1 Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r, \\ 0 \leq r < |b|. \end{cases} \quad (23.1)$$

Démonstration. On suppose que $b > 0$ et on pose :

$$A = \{k \in \mathbb{Z} \mid bk \leq a\}.$$

Cet ensemble est non vide (pour $a \geq 0$, 0 est dans A et pour $a < 0$, a est dans A) et majoré (pour $a \geq 0$, a majore A et pour $a < 0$, 0 majore A). Il admet donc un plus grand élément q qui vérifie :

$$qb \leq a < (q + 1)b.$$

Il suffit alors de poser $r = a - bq$.

Pour $b < 0$ on travaille avec $-b$ et on a l'existence de (q', r') vérifiant :

$$\begin{cases} a = -bq' + r', \\ 0 \leq r' < -b. \end{cases}$$

Et il suffit de poser $q = -q'$, $r = r'$.

Supposons qu'il existe deux couples d'entiers (q, r) et (q', r') vérifiant (23.1) avec $q \neq q'$. On a alors :

$$|r - r'| = |b(q - q')| \geq |b|$$

avec r et r' dans $] -|b|, |b| [$ ce qui est impossible. On a donc $q = q'$ et $r = r'$. Le couple (q, r) vérifiant (23.1) est donc unique. ■

Définition 23.3 Avec les notations du théorème 23.1 on dit que a est le dividende, b le diviseur, q le quotient et r le reste dans la division euclidienne de a par b .

L'anneau \mathbb{Z} est un cas particulier d'anneau euclidien et l'application $n \in \mathbb{Z}^* \mapsto |n|$ est un stathme euclidien.

Dire que le reste dans la division euclidienne de a par b est nul revient aussi à dire que b divise a .

En utilisant la division euclidienne par un entier naturel non nul n , $a = qn + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, 1, \dots, n-1\}$, on voit que a est congru modulo n au reste r . Réciproquement, si a est congru à un entier $r \in \{0, 1, \dots, n-1\}$, alors r est le reste dans la division euclidienne de a par n . C'est-à-dire que le reste dans la division euclidienne de a par n est l'unique entier r vérifiant :

$$\begin{aligned} a &\equiv r \pmod{n}, \\ 0 &\leq r < n. \end{aligned}$$

Remarque 23.3 On peut montrer un résultat analogue au théorème 23.1 avec la condition $|r| < b$ (en supposant $b > 0$), mais dans ce cas le couple (q, r) n'est pas unique. Par exemple on a :

$$12 = 3 \times 5 - 3 = 2 \times 5 + 2.$$

On peut également formuler le théorème de division euclidienne comme suit.

Théorème 23.2 Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique entier $q \in \mathbb{Z}$ tel que :

$$0 \leq a - bq < |b|. \quad (23.2)$$

Pour $b \in \mathbb{Z}^*$, l'encadrement (23.2) peut aussi s'écrire :

$$\frac{b}{|b|}q \leq \frac{a}{|b|} < \frac{b}{|b|}q + 1$$

ce qui donne

$$q \leq \frac{a}{b} < q + 1$$

pour $b > 0$ et signifie que $q = \left[\frac{a}{b} \right]$ (partie entière de $\frac{a}{b}$).

Pour $b < 0$, on a $-q \leq -\frac{a}{b} < -q + 1$, soit $q - 1 < \frac{a}{b} \leq q$ et $q - 1 = \left[\frac{a}{b} \right]$ si le reste $r = a - bq$ est non nul et $q = \frac{a}{b} = \left[\frac{a}{b} \right]$ si le reste est nul.

Remarque 23.4 La démonstration précédente du théorème de division euclidienne n'est pas constructive. Un algorithme de détermination du quotient et du reste est donné par la méthode de descente infinie de Fermat qui revient à faire une démonstration par récurrence du théorème 23.1.

Le principe est le suivant en supposant a et b strictement positifs.

Si $a < b$, on prend alors $(q, r) = (0, a)$.

Si $b \leq a$, il existe alors un entier $q_1 \geq 1$ tel que $q_1 b \leq a$ et on pose $r_1 = a - bq_1$.

Si $r_1 < b$ on prend alors $(q, r) = (q_1, r_1)$.

Si $b \leq r_1$, il existe alors un entier $q_2 \geq 1$ tel que $q_2 b \leq r_1$ et on pose $r_2 = r_1 - bq_2$.

En continuant ainsi de suite on construit deux suites d'entiers (q_n) et (r_n) par la relation de récurrence :

si $r_n < b$ alors $(q_{n+1}, r_{n+1}) = (q_n, r_n)$;

si $b \leq r_n$ alors q_{n+1} est choisi tel que $q_{n+1}b \leq r_n$ et on pose $r_{n+1} = r_n - bq_{n+1}$.

La suite (r_n) est une suite strictement décroissante d'entiers naturels. Le procédé s'arrêtera donc au bout d'un nombre fini d'étapes, c'est-à-dire qu'il existe un entier p tel que $r_p < b$ et dans ce cas le couple :

$$(q, r) = (q_1 + \cdots + q_p, r_p)$$

est la solution cherchée. En effet on a :

$$0 \leq r_p = r_{p-1} - q_p b = a - (q_1 + \cdots + q_p) b < b.$$

Exercice 23.8 Calculer, pour tout entier naturel n , le reste dans la division euclidienne par 13 de l'entier $x_n = 4^{2n+1} + 3^{n+2}$.

Solution 23.8 On a :

$$\begin{aligned} x_n &= 4 \cdot 4^{2n} + 9 \cdot 3^n = 4 \cdot 16^n + 9 \cdot 3^n \\ &= 4(16^n - 3^n) + (4 + 9)3^n \\ &= 4(16 - 3) \sum_{k=1}^n 16^{n-k} 3^{k-1} + 13 \cdot 3^n = 13y_n. \end{aligned}$$

Le reste dans la division euclidienne par 13 de x_n est donc nul, le quotient étant donné par :

$$q_n = 4 \sum_{k=1}^n 16^{n-k} 3^{k-1} + 3^n$$

Ce exercice peut en fait se généraliser comme suit.

Exercice 23.9 Soient a et b deux entiers naturels non nuls tels que $a > b$. Donner une condition suffisante sur les entiers a et b pour que tous les entiers $x_n = a^{2n+1} + b^{n+2}$, où n est un entier naturel, soient divisibles par $a + b^2$.

Solution 23.9 On a :

$$\begin{aligned} x_n &= a \cdot a^{2n} + b^2 \cdot b^n = a \cdot (a^2)^n + b^2 \cdot b^n \\ &= a((a^2)^n - b^n) + (a + b^2)b^n \\ &= a(a^2 - b) \sum_{k=1}^n (a^2)^{n-k} b^{k-1} + (a + b^2)b^n. \end{aligned}$$

Si $a = b + 1$ (i. e. b et a sont deux entiers consécutifs), alors $a^2 - b = b^2 + b + 1 = a + b^2$ et x_n est divisible par $a + b^2$ pour tout n (la condition $a^2 = b$ n'est pas possible puisqu'on suppose que $b < a$).

Pour $(a, b) = (4, 3)$ on retrouve l'exercice précédent).

Exercice 23.10 Soient a, b deux entiers relatifs. Montrer que si $a^2 + b^2$ est divisible par 7, alors a et b sont divisibles par 7.

Solution 23.10 On a $a = q_1 7 + r_1$ et $b = q_2 7 + r_2$ avec $0 \leq r_1, r_2 \leq 6$ et :

$$a^2 + b^2 = (q_1 7 + r_1)^2 + (q_2 7 + r_2)^2 = q_3 7 + r_1^2 + r_2^2.$$

Pour $0 \leq r_1, r_2 \leq 6$ et $(r_1, r_2) \neq (0, 0)$, $r_1^2 + r_2^2$ n'est jamais divisible par 7 et donc $a^2 + b^2$ n'est pas divisible par 7. En conclusion, si $a^2 + b^2$ est divisible par 7, alors a et b sont divisibles par 7.

Exercice 23.11 Calculer le reste dans la division euclidienne de 19^{55} par 7.

Solution 23.11 En utilisant la compatibilité de la congruence avec la multiplication on a :

$$19 = 2 \times 7 + 5 \equiv 5 \pmod{7}$$

$$19^{55} \equiv 5^{55} \pmod{7}$$

$$5 \equiv -2 \pmod{7}, \quad 5^2 \equiv 4 \pmod{7}, \quad 5^4 \equiv 4^2 \equiv 2 \pmod{7}, \quad 5^5 \equiv 10 \equiv 3 \pmod{7}$$

$$5^{55} = (5^5)^{11} \equiv 3^{11} \pmod{7}$$

$$3^3 = 27 \equiv -1 \pmod{7}$$

$$3^{11} = 3^{3 \times 3 + 2} \equiv 5 \pmod{7}$$

$$19^{55} \equiv 5 \pmod{7}.$$

Exercice 23.12 Calculer le reste dans la division euclidienne de 17^{51} par 7.

Solution 23.12 Laissée au lecteur.

Les paragraphes qui suivent sont consacrés à quelques applications du théorème de division euclidienne.

23.4 Les systèmes de numération

Une première application importante du théorème de division euclidienne est le théorème de numération dans une base.

Théorème 23.3 Soit b un entier supérieure ou égal à 2. Pour tout entier $n > 0$ il existe un unique entier p et un unique $(p+1)$ -uplet $(n_0, n_1, \dots, n_p) \in \mathbb{N}^{p+1}$ tels que $n_p \neq 0$, $0 \leq n_k \leq b-1$ pour tout $k \in \{0, 1, \dots, p\}$ et :

$$n = \sum_{k=0}^p n_k b^k. \quad (23.3)$$

Démonstration. En remarquant que :

$$\mathbb{N}^* = \bigcup_{j=0}^{+\infty} [b^j, b^{j+1}[$$

il suffit de montrer le résultat pour tout entier n dans $[b^j, b^{j+1}[$ où j décrit \mathbb{N} . Pour ce faire on procède par récurrence sur $j \geq 0$.

Pour $j = 0$ tout $n \in [1, b[$ s'écrit sous la forme (23.3) avec $p = 0$ et $n_0 = n$.

Supposons le résultat acquis pour $j \geq 0$ et soit $n \in [b^{j+1}, b^{j+2}[$. En utilisant le théorème de division euclidienne on peut écrire $n = bq + n_0$ avec $0 \leq n_0 \leq b - 1$. On a alors :

$$bq = n - n_0 > b^{j+1} - b = b(b^j - 1)$$

et donc $q > b^j - 1$, soit $q \geq b^j$. On a également

$$q = \frac{n - n_0}{b} < b^{j+1} - \frac{n_0}{b} \leq b^{j+1}.$$

En définitive $q \in [b^j, b^{j+1}[$ et avec l'hypothèse de récurrence il s'écrit $q = \sum_{k=0}^p q_k b^k$ avec $q_p \neq 0$. D'où :

$$n = bq + n_0 = \sum_{k=0}^{p+1} n_k b^k$$

avec $n_k = q_{k-1}$ pour tout $k \in \{1, 2, \dots, p+1\}$. En particulier $n_{p+1} = q_p \neq 0$.

Supposons que l'on ait deux écritures :

$$n = \sum_{k=0}^p n_k b^k = \sum_{k=0}^{p'} n'_k b^k$$

avec $p' \geq p$, $0 \leq n_k \leq b - 1$, $0 \leq n'_k \leq b - 1$, $n_p \neq 0$ et $n'_{p'} \neq 0$. On a alors :

$$b^p \leq n \leq \sum_{k=0}^p (b - 1) b^k = b^{p+1} - 1 < b^{p+1}.$$

De même $b^{p'} \leq n < b^{p'+1}$. Donc $b^{p'} < b^{p+1}$ soit $b^{p'-p} < b$ et nécessairement $p = p'$. En remarquant que n_0 est le reste dans la division euclidienne de n par b , on déduit que $n_0 = n'_0$ puis par récurrence que $n_k = n'_k$ pour tout $k \in \{1, \dots, p\}$. D'où l'unicité de la décomposition. ■

Remarque 23.5 Dans la décomposition (23.3) on a $b^p \leq n < b^{p+1}$, c'est-à-dire que p est le plus grand entier vérifiant $b^p \leq n$.

Définition 23.4 Avec les notations du théorème 23.3 on dit que (23.3) est la représentation en base b de l'entier n . On note :

$$n = \overline{n_p \cdots n_1 n_0}_b$$

et on dit que les n_k sont les chiffres dans l'écriture en base b de n .

Pour les valeurs successives $b = 2, 8, 10$ et 16 , les écritures en base b correspondantes sont les systèmes de numération binaire (chiffres $0, 1$), octal (chiffres $0, 1, \dots, 7$), décimal (chiffres $0, 1, \dots, 9$) et hexadécimal (chiffres $0, 1, \dots, 9, A, B, \dots, F$).

Pour $b = 10$, on écrit plus simplement $n = n_p \cdots n_1 n_0$ la représentation décimale de l'entier n .

Si $n = \overline{n_p \cdots n_1 n_0}_b$, alors n_0 est le reste dans la division euclidienne de n par b et $\overline{n_p \cdots n_1}_b$ est le quotient. Cette remarque nous permet de donner un algorithme de calcul des chiffres dans l'écriture en base b de n : on divise n par b , puis le quotient par b et ainsi de suite, un quotient

nul indique la fin du processus et les restes successifs donnent, de droite à gauche, l'écriture en base b de n . Par exemple, l'écriture en base $b = 2$ de $n = 120$ s'obtient comme suit :

| | | | | | | | |
|-----|-----|----|----|----|---|---|---|
| n | 120 | 60 | 30 | 15 | 7 | 3 | 1 |
| q | 60 | 30 | 15 | 7 | 3 | 1 | 0 |
| r | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

ce qui donne $120 = \overline{1111000}^2$.

On peut remarquer que l'écriture en base b de l'entier b est $\overline{10}^b$ et plus généralement, pour tout entier $p \geq 1$, l'écriture de l'entier b^p en base b est $\overline{10 \cdots 0}^b$ (1 suivi de p zéros).

On peut également remarquer que si $n = \overline{n_p \cdots n_1 n_0}^b$, alors pour tout entier k compris entre 1 et p , $\overline{n_{k-1} \cdots n_1 n_0}^b$ est le reste dans la division euclidienne de n par b^k et $\overline{n_p \cdots n_k}^b$ est le quotient.

L'écriture en base b peut être utilisée pour comparer deux entiers naturels non nuls, en faire la somme ou le produit (voir [?], chapitre 1, paragraphe 2).

L'écriture en base $b = 10$ permet d'obtenir les critères classiques de divisibilité résumés avec l'exercice qui suit.

Exercice 23.13 Soit n un entier naturel et $n = \overline{n_p \cdots n_1 n_0}$ son écriture décimale. Montrer que :

- n est divisible par 2 si, et seulement si, son chiffre des unités n_0 est pair ;
- n est divisible par 5 si, et seulement si, son chiffre des unités n_0 est égal à 0 ou 5 ;
- n est divisible par 3 si, et seulement si, la somme $\sum_{k=0}^p n_k$ de ses chiffres est divisible par 3 ;
- n est divisible par 9 si, et seulement si, la somme $\sum_{k=0}^p n_k$ de ses chiffres est divisible par 9 ;
- n est divisible par 11 si, et seulement si, la somme alternée $\sum_{k=0}^p (-1)^k n_k$ de ses chiffres est divisible par 11.

Solution 23.13 Ces critères de divisibilité se déduisent de la connaissance du reste dans la division euclidienne de 10 par 2, 3, 5, 9 et 11 respectivement.

Comme 10 est congru à 0 modulo 2 et modulo 5, on déduit que n est congru à n_0 modulo 2 et modulo 5 et donc n est divisible par 2 (resp. par 5) si, et seulement si, son chiffre des unités n_0 est pair, c'est-à-dire égal à 0, 2, 4, 6 ou 8 (resp. multiple de 5, c'est-à-dire égal à 0 ou 5).

Du fait que 10 est congru à 1 modulo 3 et modulo 9, on déduit que 10^k est congru à 1 modulo 3 et modulo 9 pour tout entier k et n est congru à $\sum_{k=0}^p n_k$ modulo 3 et modulo 9. Donc n est divisible par 3 (resp. par 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. par 9).

Enfin du fait que 10 est congru à -1 modulo 11 on déduit que 10^k est congru à $(-1)^k$ modulo 11 pour tout entier k et n est congru à $\sum_{k=0}^p (-1)^k n_k$ modulo 11. Donc n est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

De manière un peu plus générale, on a les résultats suivants.

Exercice 23.14 Soit n un entier naturel et $n = \overline{n_p \cdots n_1 n_0}^b$ son écriture dans une base $b \geq 2$. Montrer que :

- si d est un diviseur premier de $b \geq 2$ (les nombres premiers sont définis au chapitre 24), alors n est divisible par d si, et seulement si, n_0 est divisible par d ;
- si $b \geq 3$ et d est un diviseur premier de $b - 1$, alors n est divisible par d si, et seulement si, $\sum_{k=0}^p n_k$ est divisible par d ;
- si d est un diviseur premier de $b + 1$, alors n est divisible par d si, et seulement si, $\sum_{k=0}^p (-1)^k n_k$ est divisible par d .

Solution 23.14 *Laissée au lecteur.*

Exercice 23.15 Déterminer le reste dans la division euclidienne de k^{100} par 10 pour tout k compris entre 1 et 10. En déduire le dernier chiffre dans l'écriture en base 10 de $\sum_{k=1}^{10} k^{100}$.

Solution 23.15 On a :

$$2^{100} = (2^5)^{20} = (30 + 2)^{20} \equiv 2^{20} = (2^5)^4 \equiv 2^4 = 16 \equiv 6 \pmod{10}$$

$$3^{100} = (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{10}$$

$$4^{100} = (2^{100})^2 \equiv 36 \equiv 6 \pmod{10}$$

$$5^{100} \equiv 5 \pmod{10}$$

$$6^{100} \equiv (-4)^{100} \equiv 6 \pmod{10}$$

$$7^{100} \equiv (-3)^{100} \equiv 1 \pmod{10}$$

$$8^{100} \equiv (-2)^{100} \equiv 6 \pmod{10}$$

$$9^{100} \equiv (-1)^{100} \equiv 1 \pmod{10}$$

et donc $S \equiv 3 \pmod{10}$.

Exercice 23.16 Pour tout entier naturel n , on désigne par a_n et b_n les entiers définis par $a_0 = 16$, $b_0 = 4$ et pour $n \geq 1$, $a_n = 11 \cdots 1155 \cdots 56$, où le chiffre 1 est répété $n + 1$ fois et le chiffre 5 répété n fois et $b_n = 33 \cdots 34$ où le chiffre 3 est répété n fois.

Montrer que $a_n = b_n^2$ pour tout n . Généraliser.

Solution 23.16 Pour les premières valeurs de n , on peut constater que $a_0 = 16 = 4^2 = b_0^2$, $a_1 = 1156 = 34^2 = b_1^2$, $a_2 = 111556 = 334^2 = b_2^2$.

De manière plus générale, pour $n \geq 1$, on a :

$$\begin{aligned} b_n &= 4 + 3 \cdot 10 + \cdots + 3 \cdot 10^n \\ &= 4 + 3 \cdot 10 \frac{10^n - 1}{10 - 1} = 4 + \frac{10}{3} (10^n - 1) \\ &= \frac{2}{3} + \frac{1}{3} 10^{n+1} \end{aligned}$$

et :

$$\begin{aligned} a_n &= 6 + 5 \cdot 10 + \cdots + 5 \cdot 10^n + 10^{n+1} + \cdots + 10^{2n+1} \\ &= 6 + 5 \cdot 10 \frac{10^n - 1}{10 - 1} + 10^{n+1} \frac{10^{n+1} - 1}{10 - 1} \\ &= 6 + \frac{5 \cdot 10}{9} (10^n - 1) + \frac{10^{n+1}}{9} (10^{n+1} - 1) \\ &= \frac{4}{9} + \frac{4}{9} 10^{n+1} + \frac{1}{9} 10^{2n+2} = \left(\frac{2}{3} + \frac{1}{3} 10^{n+1} \right)^2 = b_n^2. \end{aligned}$$

On peut remarquer que :

$$(2b_n)^2 = 66 \cdots 68^2 = 4a_n = 44 \cdots 4622 \cdots 24.$$

On peut aussi montrer ce résultat par récurrence sur $n \geq 0$.

On peut essayer de généraliser. Soit $b_n = bb \cdots bc$ où le chiffre b compris entre 1 et 9 est répété n fois et c est compris entre 0 et 9. On a :

$$\begin{aligned} b_n &= c + b \cdot 10 + \cdots + b \cdot 10^n \\ &= c + b \cdot 10 \frac{10^n - 1}{10 - 1} = c + \frac{10b}{9} (10^n - 1) \\ &= c - \frac{10b}{9} + \frac{b}{9} 10^{n+1} \end{aligned}$$

et :

$$\begin{aligned} b_n^2 &= \left(c - \frac{10b}{9}\right)^2 + \frac{2b}{9} \left(c - \frac{10b}{9}\right) 10^{n+1} + \frac{b^2}{9^2} 10^{2n+2} \\ &= \left(c - \frac{10b}{9}\right)^2 + \frac{2b}{9} \left(c - \frac{10b}{9}\right) 10^{n+1} + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} + \frac{b^2}{9^2} 10^{n+1} \\ &= \left(c - \frac{10b}{9}\right)^2 + b \left(2c - \frac{19}{9}b\right) \frac{10^{n+1}}{9} + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} \\ &= \left(c - \frac{10b}{9}\right)^2 + b \left(2c - \frac{19}{9}b\right) 10 \frac{10^n - 1}{9} + \frac{10b}{9} \left(2c - \frac{19}{9}b\right) \\ &\quad + \frac{b^2}{9} 10^{n+1} \frac{10^{n+1} - 1}{9} \\ &= c^2 - \frac{10}{9}b^2 + b \left(2c - \frac{19}{9}b\right) (10 + \cdots + 10^n) + \frac{b^2}{9} (10^{n+1} + \cdots + 10^{2n+1}) \end{aligned}$$

Il s'agit alors de choisir b et c tels que $\alpha = c^2 - \frac{10}{9}b^2$ et $\beta = b \left(2c - \frac{19}{9}b\right)$ soient entiers compris entre 0 et 9 et $\gamma = \frac{b^2}{9}$ est entier compris entre 1 et 9. Si $b \in \{1, 2, 4, 5, 7, 8\}$, alors $\frac{b^2}{9}$ n'est pas entier.

Pour $b = 3$, on a $\gamma = 1$, $\alpha = c^2 - 10$ et $\beta = 6c - 19$, ce qui impose $c = 4$ ($c \leq 3$ donne $\alpha < 0$ et $c \geq 5$ donne $\alpha > 9$), c'est l'énoncé initiale avec $\alpha = 6$, $\beta = 5$ et $\gamma = 1$.

Pour $b = 6$, on a $\gamma = 4$, $\alpha = c^2 - 40$ et $\beta = 12c - 76$, ce qui impose $c = 7$. On a alors $\alpha = 9$, $\beta = 8$ et $\gamma = 4$, soit $b_n^2 = a_n$ avec $a_n = 44 \cdots 4488 \cdots 89$ et $b_n = 66 \cdots 67$.

Pour $b = 9$ on a $\gamma = 9$, $\alpha = c^2 - 90$ qui est toujours négatif, ce cas est donc exclu.

23.5 Caractéristique d'un anneau ou d'un corps commutatif

Comme deuxième application, nous allons voir que cette la caractérisation des sous-groupes de $(\mathbb{Z}, +)$ peut être utilisée pour définir la caractéristique d'un anneau ou d'un corps commutatif.

Si $(A, +, \cdot)$ est un anneau commutatif unitaire, alors l'application $\varphi : n \mapsto n \cdot 1$ est un morphisme d'anneaux de \mathbb{Z} dans A et son noyau $\ker(\varphi)$ est un sous-groupe de \mathbb{Z} (c'est même un sous-anneau), il existe donc un unique entier naturel p tel que :

$$\ker(\varphi) = \{n \in \mathbb{Z} \mid n \cdot 1 = 0\} = p\mathbb{Z}$$

et on peut alors donner la définition suivante.

Définition 23.5 Si $(A, +, \cdot)$ est un anneau commutatif unitaire, la caractéristique de A est l'entier naturel p qui vérifie $\ker(\varphi) = p\mathbb{Z}$, où φ est le morphisme d'anneaux de \mathbb{Z} dans A défini par $\varphi(n) = n \cdot 1$ pour tout $n \in \mathbb{Z}$.

Dire que la caractéristique d'un anneau commutatif unitaire A est nulle équivaut à dire que l'application φ est injective et dans ce cas $\varphi(\mathbb{Z})$ est un sous-anneau de A isomorphe à \mathbb{Z} , il est donc en particulier infini. On identifie ce sous-anneau $\varphi(\mathbb{Z})$ à \mathbb{Z} .

Un anneau de caractéristique nul est donc infini et contient \mathbb{Z} comme sous-anneau.

Dans le cas où $A = \mathbb{K}$ est un corps commutatif, si sa caractéristique est nulle, il contient non seulement \mathbb{Z} , mais aussi le corps \mathbb{Q} des rationnels, puisque pour tout entier non nul n , on a $(n \cdot 1)^{-1} = \frac{1}{n} \in \mathbb{K}$ et en conséquence tout $r = p\frac{1}{q}$ (où $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$) est aussi dans \mathbb{K} .

Nous verrons plus loin que la caractéristique d'un anneau commutatif unitaire et intègre est soit nulle soit un nombre premier. C'est le cas en particulier pour un corps commutatif.

Le théorème 20.6 combiné avec le fait que la somme et l'intersection de deux sous-groupes de $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Z}, +)$ (voir l'exercice 20.24 pour la somme de deux sous-groupes) nous permet de donner une définition du pgcd et du ppcm de deux entiers relatifs.

23.6 Plus grand commun diviseur

La caractérisation des sous-groupes de $(\mathbb{Z}, +)$ peut être utilisée pour définir le pgcd de deux ou plusieurs entiers relatifs, non tous nuls.

Théorème 23.4 Soient a, b deux entiers relatifs non tous deux nuls. Il existe un unique entier naturel δ tel que :

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = au + bv$ avec $(u, v) \in \mathbb{Z}^2$ et c'est le plus grand entier naturel qui divise a et b .

Démonstration. $a\mathbb{Z} + b\mathbb{Z}$ étant un sous groupe de $(\mathbb{Z}, +)$, le théorème 20.6 nous dit qu'il existe un unique entier naturel δ tel que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$.

Comme $\delta \in \delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $\delta = au + bv$.

De $a\mathbb{Z} \subset \delta\mathbb{Z}$ et $b\mathbb{Z} \subset \delta\mathbb{Z}$, on déduit que δ un diviseur commun à a et b . Si $d \in \mathbb{N}$ est un diviseur commun à a et b , il divise aussi $\delta = au + bv$ et $d \leq \delta$ (a et b n'étant pas tous les deux nuls, on a $\delta \neq 0$). Donc δ est bien le plus grand entier naturel qui divise a et b . ■

On peut donc donner la définition suivante.

Définition 23.6 Soient a, b deux entiers relatifs non tous deux nuls. On appelle plus grand commun diviseur de a et b le plus grand entier naturel qui divise a et b . On le note $\text{pgcd}(a, b)$ ou $a \wedge b$.

La relation $a \wedge b = au + bv$ avec $(u, v) \in \mathbb{Z}^2$ est l'identité de Bézout.

Exercice 23.17 Soient a, b deux entiers relatifs non tous deux nuls et $\mathcal{D}_{a,b}$ l'ensemble des diviseurs communs à a et b dans \mathbb{N}^* , c'est-à-dire :

$$\mathcal{D}_{a,b} = \{d \in \mathbb{N}^* \mid d/a \text{ et } d/b\}.$$

Montrer que $a \wedge b$ est le plus grand élément pour l'ordre de la division dans \mathbb{N} de $\mathcal{D}_{a,b}$ et que $\mathcal{D}_{a,b} = \mathcal{D}_{a \wedge b}$ (ensemble des diviseurs strictement positifs de $a \wedge b$).

Solution 23.17 On sait déjà que $\delta = a \wedge b$ divise a et b , donc $\delta \in \mathcal{D}_{a,b}$ et tout entier $d \in \mathcal{D}_{a,b}$ divisant a et b va diviser $\delta = au + bv$.

Comme tout $d \in \mathcal{D}_{a,b}$ divise δ , on a $\mathcal{D}_{a,b} \subset \mathcal{D}_\delta$ et comme tout $d \in \mathcal{D}_\delta$ divise δ qui divise lui-même a et b , d va diviser a et b , soit $d \in \mathcal{D}_{a,b}$. On a donc $\mathcal{D}_{a,b} = \mathcal{D}_{a \wedge b}$.

On peut aussi donner une définition de $\text{pgcd}(a, b)$ sans référence directe aux sous-groupes de \mathbb{Z} comme indiqué dans l'exercice suivant.

Exercice 23.18 Montrer, sans référence directe aux sous-groupes de \mathbb{Z} , que l'ensemble $\mathcal{D}_{a,b}$ défini à l'exercice précédent admet donc un plus grand élément δ (δ est alors le plus grand diviseur communs à a et b).

Solution 23.18 L'ensemble $\mathcal{D}_{a,b}$ est non vide car il contient 1. Comme a et b ne sont pas tous deux nuls, cet ensemble est fini puisqu'un entier relatif non nul n'a qu'un nombre fini de diviseurs dans \mathbb{N}^* . L'ensemble $\mathcal{D}_{a,b}$ est donc non vide et majoré dans \mathbb{N}^* , il admet donc un plus grand élément $\delta \in \mathbb{N}^*$ qui est bien le plus grand diviseur communs à a et b .

Exercice 23.19 Vérifier les propriétés suivantes du pgcd :

- $\forall (a, b) \in \mathbb{Z}^2 - \{(0, 0)\}, a \wedge b \in \mathbb{N}^*$;
- $\forall a \in \mathbb{Z}^*, a \wedge 0 = a \wedge a = |a|$;
- $\forall a \in \mathbb{Z}, a \wedge 1 = 1$;
- $\forall (a, b) \in \mathbb{Z}^2 - \{(0, 0)\}, a \wedge b = |a| \wedge |b| = |a| \wedge b = a \wedge |b|$;
- $\forall (a, b) \in \mathbb{Z}^2 - \{(0, 0)\}, a \wedge b = b \wedge a$ (commutativité du pgcd) ;
- pour $b \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$, on a $a \wedge b = |b|$ si, et seulement si, b divise a ;
- $\forall (a, b) \in \mathbb{Z}^2 - \{(0, 0)\}, \forall c \in \mathbb{Z}^*, (ac) \wedge (bc) = |c| (b \wedge a)$;
- si $d \in \mathbb{Z}^*$ est un diviseur commun de a et b non tous deux nuls, alors $\frac{a}{d} \wedge \frac{b}{d} = \frac{a \wedge b}{|d|}$;
- pour a, b, c non tous nuls dans \mathbb{Z} , on a $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (associativité du pgcd).

Solution 23.19 Laissée au lecteur.

Exercice 23.20 Soient a, b deux entiers naturels non nuls. Montrer que :

$$a \wedge b = \begin{cases} (a - b) \wedge b & \text{si } a \geq b \\ a \wedge (b - a) & \text{si } b > a \end{cases}$$

En déduire un algorithme simple de calcul de $a \wedge b$.

Solution 23.20 Si $a = b$, alors $a \wedge b = a \wedge a = a = 0 \wedge a$. Si $a > b$, on note $\delta = a \wedge b$ et $\delta' = (a - b) \wedge b$. Comme δ divise a et b , il divise $a - b$ et b , donc il divise leur pgcd δ' . De même δ' qui divise $a - b$ et b va diviser $a = (a - b) + b$ et b , il divise donc δ et $\delta = \delta'$. Pour $a < b$, on a $a \wedge b = b \wedge a = a \wedge (b - a)$.

Un algorithme simple de calcul de $a \wedge b$, pour a, b entiers relatifs est donc le suivant :

Début

Lecture de a et b ;

$a = |a|$; $b = |b|$;

Tant que $a \neq b$ Faire

Début

Si $a > b$ Alors

remplacer a par $a - b$;

Sinon

remplacer b par $b - a$;

Fin si ;

Fin ;

pgcd = a ;

Fin.

Par exemple, pour $(a, b) = (128, 28)$, on a :

$$\begin{aligned} a \wedge b &= 100 \wedge 28 = 72 \wedge 28 = 44 \wedge 28 \\ &= 16 \wedge 28 = 16 \wedge 12 = 4 \wedge 12 = 4 \wedge 8 \\ &= 4 \wedge 4 = 4. \end{aligned}$$

Cet algorithme n'est évidemment pas très performant, il sera amélioré par l'algorithme d'Euclide.

Exercice 23.21 Soient a et b deux entiers relatifs non tous deux nuls. Montrer que :

$$a \wedge b = a \wedge (a + b) = b \wedge (a + b).$$

Solution 23.21 On remarque que si $(a, b) \neq (0, 0)$, alors $(a, a + b) \neq (0, 0)$ et $(b, a + b) \neq (0, 0)$.

En notant $\delta = a \wedge b$ et $\delta' = a \wedge (a + b)$, on a :

$$\begin{aligned} \delta &= au + bv = a(u - v) + (a + b)v \\ &\in a\mathbb{Z} + (a + b)\mathbb{Z} = \delta'\mathbb{Z} \end{aligned}$$

donc $\delta\mathbb{Z} \subset \delta'\mathbb{Z}$ et :

$$\begin{aligned} \delta' &= au' + (a + b)v' = a(u' + v') + bv' \\ &\in a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} \end{aligned}$$

donc $\delta'\mathbb{Z} \subset \delta\mathbb{Z}$ et donc $\delta\mathbb{Z} = \delta'\mathbb{Z}$, ce qui équivaut à $\delta = \delta'$.

On peut aussi dire que comme δ divise a et b , il divise a et $a + b$, donc il divise leur pgcd δ' . De même δ' qui divise a et $a + b$ va diviser a et $b = (a + b) - a$, il divise donc δ et $\delta = \delta'$.

On a donc, en permutant les rôles de a et b :

$$a \wedge b = a \wedge (a + b) = b \wedge (a + b).$$

Exercice 23.22 Soient a, b deux entiers naturels non nuls. Calculer $(5a + 3b) \wedge (7a + 4b)$ en fonction de $a \wedge b$.

Solution 23.22 En utilisant la relation $a \wedge b = (a - b) \wedge b$ pour $a \geq b$, on a :

$$\begin{aligned} (5a + 3b) \wedge (7a + 4b) &= (5a + 3b) \wedge (2a + b) \\ &= (3a + 2b) \wedge (2a + b) \\ &= (a + b) \wedge (2a + b) \\ &= (a + b) \wedge a \\ &= a \wedge b. \end{aligned}$$

On définit de manière analogue le pgcd d'une famille a_1, \dots, a_p formée de p entiers non tous nuls comme le plus grand des diviseurs communs à a_1, \dots, a_p . On le note $\text{pgcd}(a_1, \dots, a_p)$ ou $a_1 \wedge a_2 \wedge \dots \wedge a_p$ et c'est un entier supérieur ou égal à 1. Cette définition est justifiée par le théorème suivant.

Théorème 23.5 Soient a_1, \dots, a_p des entiers relatifs non tous nuls. Il existe un unique entier naturel δ tel que :

$$a_1\mathbb{Z} + \dots + a_p\mathbb{Z} = \delta\mathbb{Z}.$$

Cet entier s'écrit $\delta = \sum_{k=1}^p u_k a_k$ avec $(u_1, \dots, u_p) \in \mathbb{Z}^p$ et c'est le plus grand entier naturel qui divise a_1, \dots, a_p .

Démonstration. Analogue au cas où $p = 2$. ■

Comme dans le cas où $p = 2$, on vérifie que $a_1 \wedge \dots \wedge a_p$ est aussi le plus grand élément pour l'ordre de la division dans \mathbb{N} de l'ensemble des diviseurs positifs communs à a_1, \dots, a_p .

L'égalité $\delta = \sum_{k=1}^p u_k a_k$ est l'identité de Bézout.

La notation $a_1 \wedge a_2 \wedge \dots \wedge a_p$ ne pose pas de problème du fait de la commutativité et l'associativité du pgcd (elle est indépendante de l'ordre des a_k).

23.6.1 Plus petit commun multiple

La caractérisation des sous-groupes de $(\mathbb{Z}, +)$ peut être utilisée pour définir le ppcm de deux ou plusieurs entiers relatifs, non tous nuls.

Théorème 23.6 Soient a, b deux entiers relatifs. Il existe un unique entier naturel μ tel que :

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}.$$

Si $a = 0$ ou $b = 0$, alors $\mu = 0$. Si $a \neq 0$ et $b \neq 0$, alors μ est le plus petit entier naturel non nul multiple de a et de b .

Démonstration. $a\mathbb{Z} \cap b\mathbb{Z}$ étant un sous groupe de $(\mathbb{Z}, +)$, l'existence et l'unicité de μ se déduit du théorème 20.6.

Si $a = 0$ ou $b = 0$, on a $\mu\mathbb{Z} \subset 0\mathbb{Z} = \{0\}$ et $\mu = 0$.

Si $a \neq 0$ et $b \neq 0$, de $\mu\mathbb{Z} \subset a\mathbb{Z}$ et $\mu\mathbb{Z} \subset b\mathbb{Z}$, on déduit que μ est multiple de a et b . Si $m \in \mathbb{N}$ est un multiple commun à a et b , il est dans $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ et c'est donc un multiple de μ , ce qui implique $m \geq \mu$. Donc, μ est bien le plus petit entier naturel non nul multiple de a et de b . ■

On peut donc donner la définition qui suit.

Définition 23.7 Soient a, b deux entiers relatifs. On appelle plus petit commun multiple de a et b le plus petit entier naturel multiple de a et b . On le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Remarque 23.6 La définition de $\text{ppcm}(a, b)$ peut aussi se justifier directement sans référence directe aux sous-groupes de \mathbb{Z} . Pour ce faire, on désigne par $\mathcal{M}_{a,b}$ l'ensemble des multiples communs à a et b . Si $a \neq 0$ et $b \neq 0$, alors l'ensemble $\mathcal{M}_{a,b} \cap \mathbb{N}^*$ des multiples communs à a et b qui sont strictement positifs est non vide car il contient $|ab|$, il admet donc un plus petit élément μ qui est bien plus petit commun multiple de a et b . Pour $a = 0$ ou $b = 0$, on a $\mathcal{M}_{a,b} = \{0\}$ et $\mu = 0$.

Remarque 23.7 Le ppcm de a et b est aussi le plus petit élément pour l'ordre de la division dans \mathbb{Z} de l'ensemble $\mathcal{M}_{a,b}$ des multiples communs à a et b . En effet, $a \vee b$ est un multiple de a et b et tout multiple commun m à a et b qui est dans $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ est un multiple de $a \vee b$.

On vérifie facilement les propriétés suivantes.

Exercice 23.23 Vérifier les propriétés suivantes du ppcm :

- $\forall (a, b) \in (\mathbb{Z}^*)^2, a \vee b \in \mathbb{N}^*$;
- $\forall a \in \mathbb{Z}^*, a \vee 1 = a \vee a = |a|$;
- $\forall (a, b) \in \mathbb{Z}^2, a \vee b = |a| \vee |b| = |a| \vee b = a \vee |b|$;
- $\forall (a, b) \in \mathbb{Z}^2, a \vee b = b \vee a$ (commutativité du ppcm) ;
- pour $b \in \mathbb{Z}$ et $a \in \mathbb{Z}$, on a $a \vee b = |b|$ si, et seulement si, b est multiple de a ;
- $\forall (a, b, c) \in \mathbb{Z}^3, (ac) \vee (bc) = |c| (b \vee a)$;
- si $d \in \mathbb{Z}^*$ est un diviseur commun de a et b , alors $\frac{a}{d} \vee \frac{b}{d} = \frac{a \vee b}{|d|}$;
- pour a, b, c non tous nuls dans \mathbb{Z} , on a $a \vee (b \vee c) = (a \vee b) \vee c$ (associativité du ppcm).

Solution 23.23 Laissée au lecteur.

Lemme 23.1 Soient a, b deux entiers relatifs premiers entre eux. On a alors :

$$a \vee b = |ab|.$$

Démonstration. Du fait que $|ab|$ est un multiple de a et b on déduit que $\mu = a \vee b$ divise ab .

D'autre part il existe deux entiers k, k' tels que $\mu = ka = k'b$ et comme a est premier avec b et divise $k'b$, il divise k' (théorème de Gauss). Ce qui donne $\mu = k''ab$ et ab divise μ . D'où l'égalité $\mu = ab$. ■

Nous verrons que la réciproque du résultat précédent est vraie.

Théorème 23.7 Soient a, b deux entiers relatifs. On a alors :

$$(a \wedge b) (a \vee b) = |ab|.$$

Démonstration. On note $\delta = a \wedge b$ et on a $|a| = \delta a', |b| = \delta b'$ avec a' et b' premiers entre eux. Ce qui donne :

$$\mu = a \vee b = (\delta a') \vee (\delta b') = \delta (a' \vee b') = \delta a' b'$$

et $\delta \mu = \delta a' \delta b' = |ab|$. ■

Du lemme et du théorème précédent, on déduit que :

$$a \wedge b = 1 \Leftrightarrow a \vee b = |ab|.$$

On a donc pour a, b dans \mathbb{Z}^* $a \vee b = \frac{|ab|}{a \wedge b}$.

On peut donc définir de manière naturelle le ppcm de deux entiers relatifs non tous deux nuls par :

$$a \vee b = \frac{|ab|}{a \wedge b}.$$

On peut aussi utiliser cette relation pour calculer le ppcm de deux entiers. On calcule d'abord le pgcd en utilisant l'algorithme d'Euclide (paragraphe 23.7), puis on divise $|ab|$ par ce pgcd.

On définit de manière analogue le ppcm d'une famille a_1, \dots, a_p formée de p entiers non tous nuls comme le plus petit des multiples communs à a_1, \dots, a_p . On le note $\text{ppcm}(a_1, \dots, a_p)$ ou $a_1 \vee a_2 \vee \dots \vee a_p$ et c'est un entier supérieur ou égal à 1. Cette définition est justifiée par le théorème suivant.

Théorème 23.8 Soient a_1, \dots, a_p des entiers relatifs non tous nuls. Il existe un unique entier naturel μ tel que :

$$a_1\mathbb{Z} \cap \dots \cap a_p\mathbb{Z} = \mu\mathbb{Z}.$$

μ est le plus petit entier naturel divisible par a_1, a_2, \dots et a_p .

Démonstration. Analogue au cas où $p = 2$. ■

La notation $a_1 \vee a_2 \vee \dots \vee a_p$ ne pose pas de problème du fait de la commutativité et l'associativité du ppcm (elle est indépendante de l'ordre des a_k).

Comme dans le cas où $p = 2$, on vérifie que $a_1 \vee \dots \vee a_p$ est aussi le plus petit élément pour l'ordre de la division dans \mathbb{N} de l'ensemble des multiples positifs communs à a_1, \dots, a_p .

Exercice 23.24 Montrer que si a_1, \dots, a_p sont des entiers relatifs non nuls deux à deux premiers entre eux alors $a_1 \vee \dots \vee a_p = |a_1 \cdots a_p|$. Ce résultat est-il encore valable si on suppose que a_1, \dots, a_p sont premiers entre eux dans leur ensemble.

Solution 23.24 On sait déjà que si a_1 et a_2 sont premiers entre eux alors $a_1 \vee a_2 = |a_1 a_2|$. Supposons le résultat acquis pour $p - 1 \geq 2$ et soient a_1, \dots, a_p deux à deux premiers entre eux. Les entiers $a_1 \cdots a_{p-1}$ et a_p sont alors premiers entre eux (corollaire 23.2) et en utilisant l'associativité du ppcm, on a :

$$\begin{aligned} a_1 \vee \dots \vee a_p &= (a_1 \vee \dots \vee a_{p-1}) \vee a_p \\ &= |a_1 \cdots a_{p-1}| \vee a_p = |a_1 \cdots a_p|. \end{aligned}$$

Ce résultat n'est plus valable si on suppose seulement que les a_k sont premiers entre eux dans leur ensemble comme le montre l'exemple suivant :

$$2 \vee 3 \vee 4 = 12 \neq 2 \cdot 3 \cdot 4 = 24$$

Exercice 23.25 A-t-on $(a_1 \wedge \dots \wedge a_p)(a_1 \vee \dots \vee a_p) = |a_1 \cdots a_p|$ dans \mathbb{Z}^* ?

Solution 23.25 La réponse est non pour $n \geq 3$ comme le montre l'exercice précédent.

Exercice 23.26 Peut-on trouver des entiers a, b tels que $a \wedge b = 7$ et $a \vee b = 36$.

Solution 23.26 Comme $a \wedge b = 7$ divise a et b , il divise $a \vee b$ et $a \vee b = 36$ est alors impossible.

Exercice 23.27 Déterminer tous les couples (a, b) d'entiers naturels non nuls tels que $a \wedge b = 3$ et $a \vee b = 12$.

Solution 23.27 De $a \vee b = 12$ on déduit que a, b sont des diviseurs de 12 donc dans $\{1, 2, 3, 4, 6, 12\}$. De $a \wedge b = 3$, on déduit que a et b sont multiples de 3, donc dans $\{3, 6, 12\}$. De $ab = (a \wedge b)(a \vee b) = 36$, on déduit que :

- $a = 3$ [resp. $b = 3$] donne $b = 12$ [resp. $a = 12$] et $(3, 12), (12, 3)$ sont deux solutions possibles ;
- $a = 6$ [resp. $b = 6$] donne $b = 6$ [resp. $a = 6$] et $a \wedge b = 6 \neq 3$.

En définitive, $(a, b) \in \{(3, 12), (12, 3)\}$.

Exercice 23.28 On se propose de montrer que pour tout entier naturel $n \geq 2$, on a :

$$\mu_n = \text{ppcm}(1, 2, \dots, n) \geq 2^{n-2}.$$

1. Montrer le résultat pour $n = 2$ et $n = 3$.
2. Pour tout entier naturel n , on, note :

$$I_n = \int_0^1 x^n (1-x)^n dx.$$

(a) Montrer que :

$$\forall n \in \mathbb{N}, 0 < I_n \leq \frac{1}{4^n}.$$

(b) Montrer que, pour tout $n \in \mathbb{N}^*$, il existe un entier naturel non nul a_n tel que $I_n = \frac{a_n}{\mu_{2n+1}}$.

(c) En déduire que :

$$\forall n \in \mathbb{N}^*, \mu_{2n+1} \geq 2^{2n}.$$

(d) En déduire le résultat annoncé.

Solution 23.28

1. On a :

$$\mu_2 = \text{ppcm}(1, 2) = 2 \geq 1 \text{ et } \mu_3 = \text{ppcm}(1, 2, 3) = 6 \geq 2.$$

2.

(a) Pour $0 < x < 1$, on a $0 < x(x-1) \leq \sup_{[0,1]} x(1-x) = \frac{1}{4}$, ce qui donne le résultat.

(b) On a :

$$\begin{aligned} I_n &= \int_0^1 x^n \left(\sum_{k=0}^n C_n^k (-1)^k x^k \right) dx \\ &= \sum_{k=0}^n C_n^k (-1)^k \int_0^1 x^{n+k} dx \\ &= \sum_{k=0}^n C_n^k \frac{(-1)^k}{n+k+1} \end{aligned}$$

et en réduisant au même dénominateur $I_n = \frac{a_n}{\mu_{2n+1}}$, où $a_n \in \mathbb{N}^*$.

(c) On a alors $\mu_{2n+1} I_n = a_n \geq 1$ et :

$$\mu_{2n+1} \geq \frac{1}{I_n} \geq 4^n = 2^{2n}.$$

(d) Pour $n \in \mathbb{N}^*$, on a :

$$\mu_{2n+2} = \mu_{2n+1} \vee (2n+2) \geq 2^{2n}.$$

On a donc montré que $\mu_n \geq 2^{n-2}$ pour tout $n \geq 4$.

On peut en fait montrer que $\mu_n \geq 2^n$ pour tout $n \geq 7$.

23.7 L'algorithme d'Euclide.

Le lemme qui suit permet de déduire du théorème de division euclidienne un algorithme de calcul du pgcd de deux entiers positifs. C'est l'algorithme d'Euclide.

Cet algorithme permet également de déterminer des entiers u et v tels que $au + bv = a \wedge b$.

Théorème 23.9 *Soient a, b deux entiers naturels non nuls et r le reste dans la division euclidienne de a par b . On a alors $a \wedge b = b \wedge r$.*

Démonstration. Par division euclidienne, on a $a = bq + r$ avec $0 \leq r < b$. L'entier naturel $\delta = a \wedge b$ qui est un diviseur commun à a et b va diviser $r = a - bq$, c'est donc un diviseur commun à b et r et $\delta \leq \delta' = b \wedge r$.

L'entier naturel $\delta' = b \wedge r$ qui est un diviseur commun à b et r va diviser $a = bq + r$, c'est donc un diviseur commun à a et b et $\delta' \leq \delta$. On a donc bien $\delta = \delta'$. ■

Le principe de l'algorithme d'Euclide est le suivant pour $a > b$ dans \mathbb{N}^* (par symétrie, on peut supposer que $a \geq b$ et pour $a = b$, on a $a \wedge a = a$).

On note $r_0 = b$ et on désigne par r_1 le reste dans la division euclidienne de a par b .

On a alors $0 \leq r_1 < r_0$ et d'après le lemme précédent :

$$a \wedge b = r_0 \wedge r_1.$$

Si $r_1 = 0$ alors $r_0 \wedge r_1 = r_0 = b$ et c'est terminé.

Si $r_1 \neq 0$ on désigne alors par r_2 le reste dans la division euclidienne de r_0 par r_1 et on a $0 \leq r_2 < r_1$ et :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2.$$

Si $r_2 = 0$ alors $r_1 \wedge r_2 = r_1$ et c'est terminé. Sinon on continue.

On définit donc ainsi une suite d'entiers $(r_n)_{n \geq 0}$ par :

- $r_0 = b$;
- r_1 est le reste dans la division euclidienne de a par b ; on a donc $0 \leq r_1 < b$;
- pour $n \geq 2$, si $r_{n-1} = 0$ alors $r_n = 0$ et sinon r_n est le reste dans la division euclidienne de r_{n-2} par r_{n-1} et on a $0 \leq r_n < r_{n-1}$. Dans tous les cas on $r_n \leq r_{n-1}$ l'égalité étant réalisée si et seulement si les deux termes sont nuls.

La suite $(r_n)_{n \geq -1}$ ainsi construite est donc une suite décroissante d'entiers positifs, elle est donc stationnaire à partir d'un certain rang. Précisément il existe un entier $p \geq 1$ tel que $r_p = 0 < r_{p-1} < \dots < r_1 < r_0$ et :

$$a \wedge b = r_0 \wedge r_1 = \dots = r_{p-1} \wedge r_p = r_{p-1}.$$

C'est à dire que $a \wedge b$ est le dernier reste non nul dans cette suite de divisions euclidiennes.

Par exemple pour calculer le pgcd de $a = 128$ et $b = 28$, on procède comme suit :

$$\begin{cases} a = 128 = 4 \cdot 28 + 16 = q_1 r_0 + r_1 \\ r_0 = 28 = 1 \cdot 16 + 12 = q_2 r_1 + r_2 \\ r_1 = 16 = 1 \cdot 12 + 4 = q_3 r_2 + r_3 \\ r_2 = 12 = 3 \cdot 4 + 0 = q_4 r_3 + r_4 \\ r_4 = 0, r_3 = 4 = 128 \wedge 28 \end{cases} \quad (23.4)$$

On peut utiliser un tableau pour effectuer la suite des calculs. Sur la deuxième ligne, on place d'abord a et b , puis sur la première ligne on place au dessus de b le quotient q_1 et sur la troisième ligne, on place au dessous de a le reste r_1 , ce même reste r_1 étant aussi placé en deuxième ligne après b . On recommence alors avec le couple (b, r_1) . Sur la première ligne

apparaissent les quotients successifs sur la troisième les restes successifs. Le dernier reste non nul, qui apparaît en fin de deuxième ligne, donne alors le pgcd.

$$\begin{array}{cccccccccc}
 & q_1 & q_2 & q_3 & q_4 & & 4 & 1 & 1 & 3 \\
 a & b & r_1 & r_2 & r_3 & 128 & 28 & 16 & 12 & 4 \\
 r_1 & r_2 & r_3 & r_4 = 0 & & 16 & 12 & 4 & r_4 = 0 &
 \end{array}$$

On a donc construit, avec l'algorithme d'Euclide, deux suites d'entiers $(r_n)_{0 \leq n \leq p}$ et $(q_n)_{1 \leq n \leq p}$ de la manière suivante :

$$\left\{ \begin{array}{l}
 a = q_1 r_0 + r_1 \quad (0 < r_1 < r_0 = b) \\
 r_0 = q_2 r_1 + r_2 \quad (0 < r_2 < r_1) \\
 r_1 = q_3 r_2 + r_3 \quad (0 < r_3 < r_2) \\
 \vdots \\
 r_{p-3} = q_{p-1} r_{p-2} + r_{p-1} \quad (0 < r_{p-1} < r_{p-2}) \\
 r_{p-2} = q_p r_{p-1} + r_p \quad (r_p = 0)
 \end{array} \right.$$

On vérifie alors, par récurrence finie sur $n \in \{0, 1, \dots, p-1\}$, qu'il existe des entiers u_n et v_n tels que $r_n = au_n + bv_n$.

Pour $n = 0$ et $n = 1$ on a :

$$\begin{aligned}
 r_0 &= b = a \cdot 0 + b \cdot 1, \\
 r_1 &= a \cdot 1 + b(-q_1).
 \end{aligned}$$

En supposant le résultat acquis jusqu'à l'ordre $n-1$ pour $0 \leq n-1 \leq p-2$ on a :

$$\begin{aligned}
 r_n &= -q_n r_{n-1} + r_{n-2} \\
 &= -q_n (au_{n-1} + bv_{n-1}) + au_{n-2} + bv_{n-2} \\
 &= a(u_{n-2} - q_n u_{n-1}) + b(v_{n-2} - q_n v_{n-1}) = au_n + bv_n.
 \end{aligned}$$

En particulier pour $n = p-1$ on a $a \wedge b = r_{p-1} = au_{p-1} + bv_{p-1} = au + bv$.

Un tel couple d'entiers (u, v) n'est pas unique puisque si (u, v) est une solution, pour tout entier λ , le couple $(u', v') = (u + \lambda v, v - \lambda a)$ est aussi solution. On a en effet :

$$a(u + \lambda b) + b(v - \lambda a) = au + bv = a \wedge b.$$

Une équation dans \mathbb{Z} de la forme $au + bv = \delta$, où a, b, δ sont donnés et u, v sont les inconnues est une équation diophantienne. Ce type d'équation est étudié plus en détails au paragraphe suivant.

Les suites $(r_n)_{0 \leq n \leq p-1}$ $(u_n)_{0 \leq n \leq p-1}$ et $(v_n)_{0 \leq n \leq p-1}$ vérifient la même relation de récurrence :

$$x_n = x_{n-2} - q_n x_{n-1} \quad (2 \leq n \leq p-1)$$

avec les conditions initiales :

$$(r_0, r_1) = (b, 1), \quad (u_0, u_1) = (0, 1), \quad (v_0, v_1) = (1, -q_1)$$

où q_1, r_1 sont, respectivement, le quotient et le reste dans la division euclidienne de a par b .

On peut donner une interprétation matricielle de ces calculs comme suit. On a :

$$\begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix} \quad (2 \leq n \leq p-1)$$

et :

$$\begin{pmatrix} x_{p-1} \\ x_{p-2} \end{pmatrix} = \begin{pmatrix} -q_{p-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_{p-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} \\ = A_{p-1} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix}.$$

Pour l'exemple précédent, la suite de calculs (23.4) donne :

$$p-1 = 3, (q_1, q_2, q_3) = (4, 1, 1)$$

et :

$$\begin{aligned} A_3 &= \begin{pmatrix} -q_3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \end{aligned}$$

d'où :

$$\begin{pmatrix} u_3 \\ u_2 \end{pmatrix} = A_3 \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \\ \begin{pmatrix} v_3 \\ v_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -q_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} -4 \\ 1 \end{pmatrix} = \begin{pmatrix} -9 \\ 5 \end{pmatrix}$$

soit $(u, v) = (u_3, v_3) = (2, -9)$.

Si on veut se passer du calcul matriciel, on peut procéder comme suit. Les divisions successives :

$$\begin{cases} a = q_1 r_0 + r_1 \\ r_0 = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ r_2 = q_4 r_3 \end{cases}$$

donne :

$$\begin{aligned} a \wedge b &= r_3 = r_1 - q_3 r_2 = r_1 - q_3 (r_0 - q_2 r_1) \\ &= r_1 (1 + q_3 q_2) - q_3 r_0 = (a - q_1 r_0) (1 + q_3 q_2) - q_3 r_0 \\ &= (a - q_1 b) (1 + q_3 q_2) - q_3 b = au + bv \end{aligned}$$

(on commence par la fin), soit pour les valeurs particulières 128 et 28 :

$$\begin{cases} 128 = 4 \cdot 28 + 16 \\ 28 = 1 \cdot 16 + 12 \\ 16 = 1 \cdot 12 + 4 \\ 12 = 3 \cdot 4 \end{cases}$$

qui donne :

$$\begin{aligned} 128 \wedge 28 &= 4 = 16 - 12 = 16 - (28 - 16) = 2 \cdot 16 - 28 \\ &= 2(128 - 4 \cdot 28) - 28 \\ &= 2 \cdot 128 - 9 \cdot 28 = ua + vb \end{aligned}$$

23.8 Equations diophantiennes $ax + by = c$

Soient a, b, c trois entiers relatifs, avec a et b non nuls. On s'intéresse ici à l'équation diophantienne dans \mathbb{Z}^2 :

$$ax + by = c. \quad (23.5)$$

En notant δ le pgcd de a et b , on a $a = \delta a'$, $b = \delta b'$ avec a' et b' premiers entre eux.

Lemme 23.2 *L'équation diophantienne (23.5) a des solutions entières si, et seulement si, δ divise c .*

Démonstration. Si c n'est pas un multiple de δ , comme δ divise $ax + by$ pour tous entiers x, y , l'équation (23.5) n'a pas de solutions.

Si $c = \delta c'$ est un multiple de δ , en écrivant que $\delta = au_0 + bv_0$ avec u_0, v_0 dans \mathbb{Z} (théorème de Bézout) on déduit que $(x_0, y_0) = (u_0 c', v_0 c')$ est une solution de (23.5). ■

Théorème 23.10 *Si c est multiple de δ , alors l'ensemble des solutions de (23.5) est :*

$$S = \{(x_0 - kb', y_0 + ka') \mid k \in \mathbb{Z}\}$$

où (x_0, y_0) est une solution particulière.

Démonstration. Si (x, y) est une solution de (23.5), on a alors :

$$\begin{cases} ax_0 + by_0 = c, \\ ax + by = c, \end{cases}$$

ce qui donne par soustraction :

$$a(x_0 - x) = b(y - y_0)$$

et divisant par δ , on obtient :

$$a'(x_0 - x) = b'(y - y_0).$$

Avec le théorème de Gauss on en déduit alors que a' divise $y - y_0$. On a donc $y - y_0 = ka'$ avec $k \in \mathbb{Z}$, ce qui entraîne $a'(x_0 - x) = b'ka'$ et $x_0 - x = kb'$. En définitive on a :

$$(x, y) = (x_0 - kb', y_0 + ka')$$

avec $k \in \mathbb{Z}$. Réciproquement on vérifie que pour tout $k \in \mathbb{Z}$, $(x_0 - kb', y_0 + ka')$ est bien solution de (23.5). En effet on a :

$$ax + by = ax_0 + by_0 + k(a'b - ab') = c + k\delta(a'b' - a'b') = c.$$

■

L'algorithme d'Euclide vu au paragraphe précédent nous permet d'obtenir une solution particulière $(x_0, y_0) = \left(u_0 \frac{c}{\delta}, v_0 \frac{c}{\delta}\right)$.

Exemple 23.1 *Soit à résoudre l'équation :*

$$370x + 45y = 15.$$

Le pgcd de 370 et 45 est égal à 5 qui divise 15.

On cherche tout d'abord une solution particulière de $74x + 9y = 1$. En utilisant l'algorithme d'Euclide, on a :

$$\begin{aligned} 74 &= 8 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

et donc :

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 = 9 - 4 \cdot (74 - 8 \cdot 9) \\ &= 74 \cdot (-4) + 9 \cdot 33 \end{aligned}$$

Le couple $(-12, 99)$ est solution de $74x + 9y = 3$ et de $370x + 45y = 15$.

D'un point de vue géométrique l'ensemble des solutions de (23.5) est formé de la suite de points de \mathbb{Z}^2 définie par :

$$\begin{cases} M_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}, \\ M_k = M_0 + k \begin{pmatrix} -b' \\ a' \end{pmatrix}, \quad k \in \mathbb{Z}. \end{cases}$$

Les points M_k sont sur la droite passant par M_0 et dirigée par le vecteur $\vec{v} = \begin{pmatrix} -b' \\ a' \end{pmatrix}$ ou encore par le vecteur colinéaire $\vec{v} = \begin{pmatrix} -b \\ a \end{pmatrix}$. Ces vecteurs sont orthogonaux au vecteur $\vec{u} = \begin{pmatrix} a \\ b \end{pmatrix}$.

Exercice 23.29 Résoudre dans \mathbb{Z}^2 l'équation diophantienne :

$$128x + 28y = 8.$$

Solution 23.29 En notant $(a, b) = (128, 28)$, $c = 8$ et $\delta = a \wedge b$, on a vu au paragraphe précédent que :

$$\delta = 4 = 2 \cdot 128 - 9 \cdot 28 = au_0 + bv_0$$

et $(x_0, y_0) = \left(u_0 \frac{c}{\delta}, v_0 \frac{c}{\delta}\right) = (4, -18)$ est une solution particulière de notre équations. Toutes les solutions étant données par :

$$(x, y) = (x_0 - kb', y_0 + ka') = (4 - 7k, -18 + 32k)$$

où k décrit \mathbb{Z} .

23.9 Equations $ax \equiv b \pmod{n}$

Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1 et b un entier relatif. On veut résoudre dans \mathbb{Z} l'équation diophantienne :

$$ax \equiv b \pmod{n} \tag{23.6}$$

On s'intéresse tout d'abord au cas où $b = 1$.

Lemme 23.3 Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1. L'équation

$$ax \equiv 1 \pmod{n} \quad (23.7)$$

a des solutions dans \mathbb{Z} si et seulement si a est premier avec n .

Démonstration. Le théorème de Bézout nous dit que a est premier avec n si, et seulement si, il existe des entiers relatifs x et k tels que $ax - kn = 1$, ce qui équivaut à dire que $x \in \mathbb{Z}$ est solution de (23.7). ■

Si a et n sont premiers entre eux alors l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$ de (23.7). Et pour tout autre solution $x \in \mathbb{Z}$ l'entier $a(x - x_0)$ est divisible par n . Comme n est premier avec a , le théorème de Gauss nous dit que nécessairement n divise $x - x_0$. Il est clair que réciproquement pour tout $k \in \mathbb{Z}$, $x_0 + kn$ est solution de (23.7). En définitive, l'ensemble des solutions de (23.7) est :

$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.7).

Remarque 23.8 Si a et n sont premiers entre eux alors il existe une unique solution de (23.7) dans $\{1, \dots, n-1\}$. En effet, si S est l'ensemble des solutions de (23.7) alors $S \cap \mathbb{N}^*$ est non vide et donc admet un plus petit élément $x > 0$. Si $x \geq n$ on a alors $x = qn + r$ avec $q \geq 1$ et $0 \leq r < n$. Comme $ar \equiv ax \equiv 1 \pmod{n}$, on a $r \in S \cap \mathbb{N}$ et nécessairement $r = 0$. Mais $x = qn$ entraîne $ax \equiv 0 \pmod{n}$ en contradiction avec $x \in S$. On a donc $x < n$.

On s'intéresse maintenant au cas où les entiers a et n sont premiers entre eux et b est un entier relatif. Dans ce cas on peut trouver une solution x_0 de l'équation (23.7) et pour tout entier relatif k , $x = bx_0 + kn$ est solution de (23.6). Réciproquement si x est solution de (23.6) alors $a(x - bx_0)$ est divisible par n avec n premier avec a . Le théorème de Gauss nous dit alors que $x - bx_0$ est divisible par n . En définitive, pour a et n premiers entre eux, l'ensemble des solutions de (23.6) est :

$$S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.7).

Considérons maintenant le cas où $\delta = a \wedge n$ n'est pas nécessairement égal à 1 et b est un entier relatif.

On a alors $a = \delta a'$, $n = \delta n'$ et si l'équation (23.6) admet une solution $x \in \mathbb{Z}$ alors $\delta n'$ divise $\delta a' - b$, donc δ divise $\delta a' - b$ et δ divise b . En conclusion si b n'est pas un multiple de δ alors l'équation (23.6) n'a pas de solution dans \mathbb{Z} .

On suppose donc que b est un multiple de δ , soit $b = \delta b'$. Si $x \in \mathbb{Z}$ est solution de (23.6) alors x est solution de :

$$a'x \equiv b' \pmod{n'}$$

avec a' et n' premiers entre eux. On sait alors que x est de la forme $x = b'x'_0 + kn'$ où x'_0 est une solution de $a'x \equiv 1 \pmod{n'}$ et k est un entier relatif. Réciproquement on peut vérifier que pour tout entier $k \in \mathbb{Z}$, $x = b'x'_0 + kn'$ est solution de (23.6). En effet on a :

$$\begin{aligned} ax &= a'x'_0\delta b' + a'k\delta n' = (1 + k'n')\delta b' + a'kn \\ &= b + n(k'b' + ka') \equiv b \pmod{n}. \end{aligned}$$

En définitive, si $b = \delta b'$ où $\delta = a \wedge n$, alors l'ensemble des solutions de (23.6) est :

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 est une solution particulière de $a'x \equiv 1 \pmod{n'}$, où $a = \delta a'$, $n = \delta n'$.

23.10 Le théorème Chinois

On s'intéresse ici aux système d'équations diophantiennes :

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad (23.8)$$

où n, m sont deux entiers naturels supérieur ou égal à 2.

Théorème 23.11 (chinois) *Soient n, m deux entier supérieur ou égal à 2 premiers entre eux. Quels que soient les entiers relatifs a et b le système (23.8) a une infinité de solutions dans \mathbb{Z} .*

Démonstration. Comme n et m sont premiers entre eux on peut trouver une infinité de couples d'entiers relatifs (u, v) tels que :

$$nu + mv = 1.$$

En posant $x = bnu + amv$ on obtient une infinité de solutions de (23.8). ■

Dans le cas où n et m sont premiers entre eux on vient de voir que si (u_0, v_0) est solution de $nu + mv = 1$ (un tel couple peut être obtenu par l'algorithme d'Euclide) alors $x_0 = bnu_0 + amv_0$ est une solution particulière de (23.8).

Si $x \in \mathbb{Z}$ est solution de (23.8) alors x est congru à x_0 modulo n et modulo m , soit :

$$x - x_0 = pn = qm.$$

Mais m est premier avec n , le théorème de Gauss nous dit alors que m divise p . On a donc $x = x_0 + knm$ avec $k \in \mathbb{Z}$. Et réciproquement on vérifie que pour tout entier relatif k , $x_0 + knm$ est solution de (23.8). En définitive, si n et m sont premiers entre eux, alors l'ensemble des solutions de (23.8) est :

$$S = \{x_0 + knm \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.8).

Dans le cas général où m et n ne sont pas nécessairement premiers entre eux on note $\delta = m \wedge n$, $n = \delta n'$, $m = \delta m'$ avec n', m' premiers entre eux et $\mu = m \vee n$.

Si $x \in \mathbb{Z}$ est une solution de (23.8) alors δ qui divise n et m va diviser $x - a$ et $x - b$, il divise donc $a - b$. Donc si $a - b$ n'est pas un multiple de $\delta = m \wedge n$ le système d'équations (23.8) n'a pas de solutions.

On suppose donc que $a - b$ est multiple de δ , c'est-à-dire que $b - a = \delta c'$. Les entiers n' et m' étant premiers entre eux, le théorème de Bézout nous dit qu'il existe des entiers u_0 et v_0 tels que $n'u_0 + m'v_0 = 1$. En posant :

$$x_0 = bn'u_0 + am'v_0$$

on a :

$$\begin{aligned} x_0 &= b(1 - m'v_0) + am'v_0 = b - m'v_0(b - a) \\ &= b - m'v_0\delta c' = b - mv_0c' \equiv b \pmod{m}. \end{aligned}$$

Et de manière analogue on voit que x_0 est congru à a modulo n . L'entier x_0 est donc solution de (23.8).

Si $x \in \mathbb{Z}$ est solution de (23.8) alors x est congru à x_0 modulo n et modulo m , soit :

$$x - x_0 = pn = qm = p\delta n' = q\delta m'.$$

On déduit donc que $\frac{x - x_0}{\delta}$ est un entier et :

$$\frac{x - x_0}{\delta} = pn' = qm'.$$

Mais m' est premier avec n' , le théorème de Gauss nous dit alors que m' divise p . On a donc :

$$\frac{x - x_0}{\delta} = kn'm'$$

avec $k \in \mathbb{Z}$. Ce qui peut aussi s'écrire :

$$x - x_0 = knm' = k \frac{nm}{\delta} = k\mu$$

avec $k \in \mathbb{Z}$.

Et réciproquement on vérifie facilement que pour tout entier relatif k , $x_0 + k\mu$ est solution de (23.8). En définitive, l'ensemble des solutions de (23.8) est :

$$S = \{x_0 + k(m \vee n) \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (23.8).

23.11 Nombres premiers entre eux. Les théorèmes de Bézout et de Gauss

On a vu que, par définition du pgcd, on a $a \wedge b = au + bv$ avec u, v entiers relatifs, mais en général la réciproque est fautive, c'est-à-dire que si δ est entier naturel tel que $\delta = au + bv$ avec u, v entiers relatifs, il n'y a aucune raison pour que δ soit le pgcd de a et b . Par exemple $2 = 3 \cdot 2 + 2 \cdot (-2)$ et $3 \wedge 2 = 1$. Mais pour $\delta = 1$, cette réciproque est vraie et ce résultat est très souvent utilisé.

Définition 23.8 Soient $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. On dit que a et b sont premiers entre eux (ou étrangers) si leur pgcd est égal à 1.

De manière équivalente, on peut dire que a et b sont premiers entre eux si, et seulement si, -1 et 1 sont leurs seuls diviseurs communs, ce qui est encore équivalent à dire que $\mathcal{D}_a \cap \mathcal{D}_b = \{-1, 1\}$ ou encore que le dernier reste non nul dans l'algorithme d'Euclide vaut 1.

Exercice 23.30 Soient $(a_k)_{1 \leq k \leq p}$ et $(b_k)_{1 \leq k \leq q}$ deux suites finies d'entiers relatifs non nuls. Montrer que si $n = \prod_{k=1}^p a_k$ et $m = \prod_{k=1}^q b_k$ sont premiers entre eux, alors chaque a_k , pour k compris entre 1 et p , est premier avec chacun des b_j , pour j compris entre 1 et q .

Solution 23.30 Soit $\delta = a_k \wedge b_j$ où $1 \leq k \leq p$ et $1 \leq j \leq q$. Comme δ est un entier naturel non nul qui divise a_k et b_j , il divise n et m et vaut nécessairement 1.

De manière plus générale, on peut donner la définition suivante.

Définition 23.9 Soient a_1, \dots, a_p des entiers relatifs non tous nuls. On dit que a_1, \dots, a_p sont premiers entre eux dans leur ensemble si leur pgcd est égal à 1.

Exercice 23.31 Est-il équivalent de dire a_1, \dots, a_p sont premiers entre eux dans leur ensemble et a_1, \dots, a_p sont deux à deux premiers entre eux ?

Solution 23.31 On vérifie immédiatement que la réponse est négative en considérant le triplet $(2, 3, 8)$.

Théorème 23.12 Soient $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$ et $\delta = a \wedge b$. Il existe deux entiers p et q premiers entre eux tels que $a = \delta p$ et $b = \delta q$.

Démonstration. Comme δ divise a et b il existe deux entiers p et q tels que $a = \delta p$ et $b = \delta q$. Le pgcd $\delta' = p \wedge q$ est un diviseur de p et q , donc l'entier naturel $\delta\delta'$ divise $a = \delta p$ et $b = \delta q$ et nécessairement $\delta\delta' \leq \delta$, soit $\delta(1 - \delta') \geq 0$ avec $\delta > 0$. On a donc $\delta' \leq 1$. Mais δ' est supérieur ou égal à 1 comme tout pgcd qui se respecte. En définitive, on a $\delta' = 1$, c'est-à-dire que p et q sont premiers entre eux. ■

De manière plus générale, on a le résultat suivant.

Théorème 23.13 Soient a_1, \dots, a_p des entiers relatifs non tous nuls. et $\delta = a_1 \wedge a_2 \wedge \dots \wedge a_p$. Il existe des entiers a'_1, \dots, a'_p premiers entre eux dans leur ensemble tels que $a_k = \delta a'_k$ pour tout k compris entre 1 et p .

Démonstration. Analogie au cas où $p = 2$. ■

Exercice 23.32 Déterminer tous les couples (a, b) d'entiers naturels non nuls tels que $a \wedge b = 3$ et $a + b = 12$.

Solution 23.32 On a $a = 3p$, et $b = 3q$ où p, q sont des entiers naturels non nuls premiers entre eux et $a + b = 12$ équivaut à $p + q = 4$.

Réciproquement si $a = 3p$, $b = 3q$ où p, q sont des entiers naturels non nuls premiers entre eux tels que $p + q = 4$, alors $a \wedge b = 3$ et $a + b = 12$.

Les seuls couples (p, q) possibles sont $(1, 3)$ et $(3, 1)$. Donc $(a, b) = (3, 9)$ ou $(a, b) = (9, 3)$.

Exercice 23.33 Soient a, n deux entiers naturels non nuls. Montrer que :

$$\frac{(a+1)^n - 1}{a} \wedge a = a \wedge n.$$

Solution 23.33 On remarque d'abord que :

$$(a+1)^n - 1 = a \sum_{k=0}^{n-1} (a+1)^k$$

est divisible par a , donc $\frac{(a+1)^n - 1}{a}$ est un entier.

Soit $\delta = \frac{(a+1)^n - 1}{a} \wedge a$. Pour tout $k \geq 0$, on a :

$$(a+1)^k \equiv 1 \pmod{a}$$

(pour $k = 0$, c'est clair et pour $k \geq 1$, on utilise la formule du binôme) et donc :

$$b = \frac{(a+1)^n - 1}{a} = \sum_{k=0}^{n-1} (a+1)^k \equiv n \pmod{a}$$

de sorte que δ qui divise a et b divise aussi $n = b - pa$ ($p \in \mathbb{Z}$). Il en résulte que δ divise $\delta' = a \wedge n$. Comme δ' divise a et n , il divise aussi $b = n + pa$ et en conséquence δ' divise δ . On a donc bien $\delta = \delta'$.

Exercice 23.34 On se donne un entier naturel $a \geq 2$ et on définit la suite $(u_n)_{n \in \mathbb{N}}$ par :

$$\forall n \in \mathbb{N}, u_n = a^{2^n} + 1.$$

1. Montrer que :

$$\forall n \in \mathbb{N}, u_{n+1} = (u_n - 1)^2 + 1.$$

2. Montrer que :

$$\forall n \in \mathbb{N}, u_{n+1} = (a - 1) \prod_{k=0}^n u_k + 2.$$

3. Montrer que, pour $n \neq m$ dans \mathbb{N} , on a :

$$u_n \wedge u_m = \begin{cases} 1 & \text{si } a \text{ est pair} \\ 2 & \text{si } a \text{ est impair} \end{cases}$$

4. Calculer $u_n^p \wedge u_m^p$ pour $n \neq m$ dans \mathbb{N} et p dans \mathbb{N}^* .

Solution 23.34

1. On a :

$$u_{n+1} = a^{2^{n+1}} + 1 = (a^{2^n})^2 + 1 = (u_n - 1)^2 + 1.$$

2. On procède par récurrence sur $n \geq 0$.

Pour $n = 0$, on a :

$$\begin{aligned} u_1 &= a^2 + 1 = (a^2 - 1) + 2 \\ &= (a - 1)u_0 + 2. \end{aligned}$$

En supposant le résultat acquis pour $n - 1 \geq 0$, on a :

$$u_{n+1} = u_n(u_n - 2) + 2 = u_n(a - 1) \prod_{k=0}^{n-1} u_k + 2 = (a - 1) \prod_{k=0}^n u_k + 2.$$

3. Supposons que $m > n$.

On a :

$$\begin{aligned} u_m &= (a - 1) \prod_{k=0}^{m-1} u_k + 2 = (a - 1) u_n \prod_{\substack{k=0 \\ k \neq n}}^{m-1} u_k + 2 \\ &= qu_n + 2 \end{aligned}$$

Le pgcd de u_n et u_m divise alors 2 et il vaut 2 ou 1.

Si a est pair, alors u_n est impair et $\delta = 1$ puisqu'il divise u_n , ce qui signifie que u_n et u_m sont premiers entre eux (pour $a = 2$, c'est le cas des nombres de Fermat).

Si a est impair, alors tous les u_n sont pairs et δ vaut 2.

4. En utilisant le résultat de l'exercice ??, on a :

$$u_n^p \wedge u_m^p = (u_n \wedge u_m)^p = \begin{cases} 1 & \text{si } a \text{ est pair} \\ 2^p & \text{si } a \text{ est impair} \end{cases}$$

Théorème 23.14 (Bézout) Deux entiers relatifs a et b non tous deux nuls sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Démonstration. On sait déjà, par définition, que la condition est nécessaire.

Réciproquement s'il existe deux entiers relatifs u et v tels que $au + bv = 1$ alors $\delta = a \wedge b$ est un entier naturel qui divise a et b , il divise donc $1 = au + bv$ et $\delta = 1$, c'est-à-dire que a et b sont premiers entre eux. ■

Remarque 23.9 La relation de Bézout $au + bv = 1$ implique que u et v sont aussi premiers entre eux. On a aussi $|a| \wedge |b| = |a| \wedge b = a \wedge |b| = a \wedge b = 1$.

Ce théorème peut se généraliser comme suit.

Théorème 23.15 (Bézout) Des entiers relatifs a_1, a_2, \dots, a_p non tous nuls sont premiers entre eux dans leur ensemble si et seulement si il existe deux entiers relatifs u_1, u_2, \dots, u_p tels que $\sum_{k=1}^p u_k a_k = 1$.

Démonstration. On sait déjà, par définition, que la condition est nécessaire.

Réciproquement s'il existe deux entiers relatifs u_1, u_2, \dots, u_p tels que $\sum_{k=1}^p u_k a_k = 1$ alors

$\delta = a_1 \wedge a_2 \wedge \dots \wedge a_p$ est un entier naturel qui divise tous les a_k , il divise donc $1 = \sum_{k=1}^p u_k a_k$ et $\delta = 1$, c'est-à-dire que a_1, a_2, \dots, a_p sont premiers entre eux dans leur ensemble. ■

Corollaire 23.1 Soient a, b, c des entiers relatifs non nuls. Si c est premier avec a alors $a \wedge b = a \wedge (bc)$ (le pgcd de deux entiers est inchangé si on multiplie l'un d'eux par un nombre premier avec l'autre).

Démonstration. Soient $\delta = a \wedge b$ et $\delta' = a \wedge (bc)$. Comme δ divise a et b , il divise a et bc ainsi que leur pgcd δ' . De $au + cv = 1$, on déduit que $abu + bcv = b$ et δ' qui divise a et bc va diviser a et b ainsi que leur pgcd δ . On a donc $\delta = \delta'$. ■

Corollaire 23.2 Soient a_1, a_2, \dots, a_p et c des entiers relatifs non nuls. Si c est premier avec chacun des a_k , pour k compris entre 1 et p , il est alors premier avec leur produit $\prod_{k=1}^p a_k$.

Démonstration. En utilisant le corollaire précédent, on a :

$$c \wedge \prod_{k=1}^p a_k = c \wedge \left(a_1 \prod_{k=2}^p a_k \right) = c \wedge \prod_{k=2}^p a_k$$

puisque a_1 est premier avec c et par récurrence finie, on déduit que :

$$c \wedge \prod_{k=1}^p a_k = c \wedge \prod_{k=2}^p a_k = c \wedge \prod_{k=3}^p a_k = \dots = c \wedge a_p = 1$$

puisque chaque a_k , pour k compris entre 1 et p , est premier avec c . ■

Une conséquence importante du théorème de Bézout est le résultat suivant.

Théorème 23.16 (Gauss) Soient a, b, c des entiers relatifs non nuls. Si a divise bc et a est premier avec b alors a divise c .

Démonstration. Comme a et b sont premiers entre eux, il existe deux entiers u, v tels que $au + bv = 1$ et pour tout entier c , on a $acu + bcv = c$, de sorte que si a divise bc , il va diviser $c = acu + bcv$. ■

Ce résultat peut être utilisé pour donner une unique représentation des nombres rationnels non nuls.

Corollaire 23.3 *Tout nombre rationnel non nul r s'écrit de manière unique $r = \frac{p}{q}$ avec $p \in \mathbb{Z}^*$ et $q \in \mathbb{N}^*$ premiers entre eux.*

Démonstration. Un nombre rationnel non nul r s'écrit $r = \frac{a}{b}$ avec (a, b) dans $\mathbb{Z}^* \times \mathbb{N}^*$. En notant $\delta = a \wedge b$ on a $a = \delta p$, $b = \delta q$ et $r = \frac{p}{q}$ avec p et q premiers entre eux. Si $r = \frac{p}{q} = \frac{p'}{q'}$ avec $(p, q), (p', q')$ dans $\mathbb{Z}^* \times \mathbb{N}^*$ tels que $p \wedge q = p' \wedge q' = 1$, on a alors $pq' = p'q$ avec q premier avec p et q qui divise pq' , donc q divise q' d'après le théorème de Gauss. De manière analogue, on voit que q' divise q . On a donc $q = q'$ (q, q' sont des entiers naturels non nuls) et $p = p'$. L'écriture est donc unique. ■

Corollaire 23.4 *Si un entier relatif non nul n est divisible par des entiers a_1, a_2, \dots, a_p deux à deux premiers entre eux, il est alors divisible par leur produit.*

Démonstration. On procède par récurrence sur $p \geq 2$.

Supposons que n soit divisible par a_1 et a_2 premiers entre eux. On a alors $n = a_1 q_1$ et a_2 divise n en étant premier avec a_1 , il va donc diviser q_1 (théorème de Gauss), c'est-à-dire que $q_1 = a_2 q_2$ et $n = a_1 a_2 q_2$ est divisible par $a_1 a_2$.

En supposons le résultat acquis au rang $p-1 \geq 2$, soient a_1, a_2, \dots, a_p deux à deux premiers entre eux qui divisent n . L'hypothèse de récurrence nous dit que n est divisible par $a = \prod_{k=1}^{p-1} a_k$. Comme a_p est premier avec chacun des a_k , pour k compris entre 1 et $p-1$, il est premier avec leur produit a (corollaire 23.2) et n qui est divisible par a et a_p est aussi divisible par leur produit $\prod_{k=1}^p a_k$. ■

Exercice 23.35

1. Montrer que pour tout entier naturel n , il existe deux entiers p_n et q_n premiers entre eux tels que :

$$(\sqrt{2} + 1)^n = p_n + q_n \sqrt{2}.$$

2. En utilisant l'application φ définie sur l'anneau $\mathbb{Z}[\sqrt{2}]$ par $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ pour tout $(a, b) \in \mathbb{Z}^2$, montrer que, pour tout $n \in \mathbb{N}$, on a :

$$(\sqrt{2} - 1)^n = (-1)^n (p_n - q_n \sqrt{2}).$$

3. En déduire que, pour tout $n \in \mathbb{N}$, il existe un entier naturel r_n tel que :

$$\begin{cases} (\sqrt{2} + 1)^n = \sqrt{r_n} + \sqrt{r_n - 1} \\ (\sqrt{2} - 1)^n = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}.$$

Solution 23.35

1. Le réel $\theta = \sqrt{2} + 1$ est dans l'anneau $\mathbb{Z}[\sqrt{2}]$, il en est donc de même de θ^n pour tout $n \in \mathbb{N}$, ce qui prouve l'existence des suites d'entiers $(p_n)_{n \in \mathbb{N}}$ et $(q_n)_{n \in \mathbb{N}}$.

On peut aussi retrouver ce résultat par récurrence en écrivant que pour tout $n \in \mathbb{N}$, on a :

$$\theta^{n+1} = (\sqrt{2} + 1) (p_n + q_n \sqrt{2}) = (p_n + 2q_n) + (p_n + q_n) \sqrt{2}$$

ce qui donne :

$$\begin{cases} p_{n+1} = p_n + 2q_n \\ q_{n+1} = p_n + q_n \end{cases}$$

et montre en outre que les p_n et q_n sont des entiers naturels non nuls sauf $q_0 = 0$.

On a alors :

$$p_{n+1} \wedge q_{n+1} = (p_n + 2q_n) \wedge (p_n + q_n).$$

En utilisant la relation $a \wedge b = a \wedge (a + b) = b \wedge (a + b)$ (exercice 23.21), on a :

$$\begin{aligned} p_n \wedge q_n &= q_n \wedge (p_n + q_n) = (q_n + p_n) \wedge q_n \\ &= (q_n + p_n) \wedge (p_n + q_n + q_n) = p_{n+1} \wedge q_{n+1}. \end{aligned}$$

On a donc, pour tout $n \in \mathbb{N}$:

$$p_n \wedge q_n = p_0 \wedge q_0 = 1 \wedge 0 = 1.$$

2. L'application φ réalise un automorphisme de l'anneau $A = \mathbb{Z}[\sqrt{2}]$. En effet, pour tous $x = a + b\sqrt{2}$ et $x' = a' + b'\sqrt{2}$ dans A , on a :

$$\begin{cases} \varphi(x + x') = (a + a') - (b + b')\sqrt{2} = \varphi(x) + \varphi(x') \\ \varphi(xx') = (aa' + 2bb') - (ab' + a'b)\sqrt{2} = \varphi(x)\varphi(x') \end{cases}$$

et $x = a + b\sqrt{2}$ a pour unique antécédent $a - b\sqrt{2}$ par φ .

On a donc, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} (\sqrt{2} - 1)^n &= (-1)^n (1 - \sqrt{2})^n = (-1)^n (\varphi(\sqrt{2} + 1))^n \\ &= (-1)^n \varphi((\sqrt{2} + 1)^n) = (-1)^n \varphi(p_n + q_n \sqrt{2}) \\ &= (-1)^n (p_n - q_n \sqrt{2}) \end{aligned}$$

3. Pour tout $n \in \mathbb{N}$, on a $(\sqrt{2} + 1)^n (\sqrt{2} - 1)^n = 1$, soit :

$$(-1)^n (p_n + q_n \sqrt{2}) (p_n - q_n \sqrt{2}) = 1$$

ou encore :

$$p_n^2 - 2q_n^2 = (-1)^n$$

(c'est une relation de Bézout pour p_n et q_n qui sont premiers entre eux) et :

$$\begin{cases} (\sqrt{2} + 1)^n = p_n + q_n \sqrt{2} = p_n + \sqrt{p_n^2 - (-1)^n} \\ (\sqrt{2} - 1)^n = (-1)^n (p_n - q_n \sqrt{2}) = (-1)^n (p_n - \sqrt{p_n^2 - (-1)^n}) \end{cases}$$

En posant $s_n = p_n^2$, on a :

$$\begin{cases} (\sqrt{2} + 1)^n = \sqrt{s_n} + \sqrt{s_n - (-1)^n} \\ (\sqrt{2} - 1)^n = (-1)^n (\sqrt{s_n} - \sqrt{s_n - (-1)^n}) \end{cases}$$

Pour n pair, cela s'écrit :

$$\begin{cases} (\sqrt{2} + 1)^n = \sqrt{s_n} + \sqrt{s_n - 1} = \sqrt{r_n} + \sqrt{r_n - 1} \\ (\sqrt{2} - 1)^n = \sqrt{s_n} - \sqrt{s_n - 1} = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}$$

avec $r_n = s_n$ et pour n impair :

$$\begin{cases} (\sqrt{2} + 1)^n = \sqrt{s_n + 1} + \sqrt{s_n} = \sqrt{r_n} + \sqrt{r_n - 1} \\ (\sqrt{2} - 1)^n = \sqrt{s_n + 1} - \sqrt{s_n} = \sqrt{r_n} - \sqrt{r_n - 1} \end{cases}$$

avec $r_n = s_n - 1$.

Nombres premiers

L'ensemble \mathcal{D}_n des diviseurs dans \mathbb{N}^* d'un entier $n \geq 2$ contient toujours 1 et n , il est donc de cardinal supérieur ou égal à 2. On s'intéresse ici aux entiers $p \geq 2$ tels que \mathcal{D}_p soit de cardinal minimal, à savoir 2.

24.1 L'ensemble \mathcal{P} des nombres premiers

Définition 24.1 On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si les seuls diviseurs positifs de p sont 1 et p .

Remarque 24.1 0 et 1 ne sont pas premiers et 2 est le seul nombre pair qui est premier.

On note \mathcal{P} l'ensemble de tous les nombres premiers.

Exemple 24.1 $n = 111111$ est non premier (la somme des chiffres de n est égale à 6, donc n est divisible par $3 < n$).

Exemple 24.2 Les nombres de Fermat sont les entiers de la forme $F_n = 2^{2^n} + 1$ où n est un entier naturel.

Ces entiers sont premiers pour $n = 0, 1, 2, 3, 4$, mais pas pour $n = 5$ ou $n = 6$.

L'instruction Maple :

`for n from 1 to 6 do factorset(2^(2^n)+1) od;`

nous donne :

$\{5\}, \{17\}, \{257\}, \{65537\}, \{6700417, 641\}, \{67280421310721, 274177\}$

soit pour $n = 5$ et $n = 6$:

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417 = (2^7 \cdot 5 + 1) (2^7 \cdot 3 \cdot 17449 + 1),$$

$$\begin{aligned} F_6 &= 2^{2^6} + 1 = 18446744073709551617 = 274177 \times 67280421310721 \\ &= (2^8 \cdot 3^2 \cdot 7 \cdot 17 + 1) (2^8 \cdot 5 \cdot 47 \cdot 373 \cdot 2998279 + 1). \end{aligned}$$

Euler (sans l'aide de Maple) avait montré que F_5 n'est pas premier.

Le résultat qui suit se déduit du fait que toute partie non vide de \mathbb{N} admet un plus petit élément.

Théorème 24.1 (Euclide) Tout entier n supérieur ou égal à 2 a au moins un diviseur premier.

Démonstration. Pour tout entier $n \geq 2$ l'ensemble \mathcal{D}_n des diviseurs strictement positifs de n a au moins deux éléments, 1 et n , donc $\mathcal{D}_n \setminus \{1\}$ est non vide dans $\mathbb{N} \setminus \{0, 1\}$ et il admet un plus petit élément p qui est nécessairement premier. En effet si p n'est pas premier il admet un diviseur q tel que $2 \leq q < p$ avec q qui divise n , ce qui contredit le caractère minimal de p . ■

Corollaire 24.1 *Tout entier relatif $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ a au moins un diviseur premier.*

Démonstration. Tout diviseur premier de $|n| \geq 2$ convient. ■

Un entier naturel non premier s'écrit donc $n = pq$ avec $p \geq 2$ premier et $q \geq 2$. On dit alors qu'il est composé.

Exercice 24.1 *Soit $b \geq 3$ une base de numération. Montrer que $n = \overline{12 \cdots 21}^b$, où le chiffre 2 est répété $p \geq 2$ fois, est non premier.*

Solution 24.1 On a :

$$\begin{aligned} n &= 1 + 2b + \cdots + 2b^p + b^{p+1} \\ &= 1 + 2b \frac{b^p - 1}{b - 1} + b^{p+1} \\ &= \frac{b^{p+2} + b^{p+1} - b - 1}{b - 1} = \frac{(b^{p+1} - 1)(b + 1)}{b - 1} \\ &= (b + 1)(1 + b + \cdots + b^{p-1} + b^p) \end{aligned}$$

les deux termes de ce produit étant ≥ 2 , donc n n'est pas premier.

Exercice 24.2 *Soient $a \geq 2$ et $m \geq 2$ deux entiers et $p = a^m - 1$. Montrer que si p est premier alors $a = 2$ et m est premier. La réciproque est-elle vraie ? On appelle nombre de Mersenne tout entier de la forme $2^m - 1$. Le plus grand nombre premier connu à ce jour (16 septembre 2006) est le nombre premier de Mersenne : $2^{32582657} - 1$.*

Solution 24.2 *Supposons que p soit premier. On a :*

$$p = a^m - 1 = (a - 1) \sum_{k=0}^{m-1} a^k = (a - 1)q$$

Si $a > 2$, on a $a - 1 \geq 2$ et $q \geq 2$ puisque $m \geq 2$ et p ne peut être premier. On a donc nécessairement $a = 2$ et $p = 2^m - 1$. Si m n'est pas premier, il s'écrit $m = ab$ avec $a \geq 2$, $b \geq 2$ et :

$$p = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \sum_{k=0}^{b-1} (2^a)^k = (2^a - 1)q$$

avec $2^a - 1 \geq 2$ (puisque $2^a \geq 4$) et $q \geq 2$ (puisque $b \geq 2$) et p ne peut être premier. L'entier m est donc nécessairement premier.

Pour $m = 2, 3, 5, 7$, on a $p = 3, 7, 31, 127$ qui sont premiers et pour $m = 11$, on a $p = 2^{11} - 1 = 2047 = 23 \times 89$. La réciproque est donc fausse.

Un diviseur premier de $n \geq 2$ est nécessairement inférieur ou égal à n . En fait, pour n non premier, on peut toujours en trouver un qui est inférieur ou égal à \sqrt{n} , c'est $p = \min(\mathcal{D}_n \setminus \{1\})$.

Théorème 24.2 *Tout entier n supérieur ou égal à 2 qui est composé a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.*

Démonstration. En supposant n composé et en gardant les notations de la démonstration du théorème précédent, on a vu que $p = \min(\mathcal{D}_n \setminus \{1\})$ est un diviseur premier de n . On a donc $n = pq$ avec $2 \leq q \leq n$ (on a $q \neq 1$ puisque n n'est pas premier) et $q \in \mathcal{D}_n \setminus \{1\}$, ce qui implique que $p \leq q$ et $p^2 \leq pq = n$, soit $p \leq \sqrt{n}$.

On peut aussi montrer ce résultat par récurrence sur $n \geq 4$.

$p = 2$ divise $n = 4$.

Supposons le résultat acquis pour tous les entiers composés compris entre 2 et $n - 1 \geq 4$. Si n est premier, il n'y a rien à montrer, sinon il existe deux entiers a et b compris entre 2 et $n - 1$ tels que $n = ab$ et comme ces deux entiers jouent des rôles symétriques, on peut supposer que $a \leq b$. Si a est premier, c'est alors un diviseur premier de n tel que $a^2 \leq ab \leq n$, sinon il admet un diviseur premier $p \leq \sqrt{a}$ et p divise aussi n avec $p \leq \sqrt{n}$. ■

Le théorème précédent nous donne un premier algorithme, relativement simple, permettant de savoir si un entier $n \geq 2$ est premier ou non : on effectue successivement la division euclidienne de n par tous les entiers $p \leq \sqrt{n}$: si l'une de ces divisions donne un reste nul, alors n n'est pas premier, sinon, n est premier.

Une petite amélioration peut être apportée à cet algorithme en remarquant que si 2 ne divise pas n , il est inutile de tester les divisibilités par les entiers $p \leq \sqrt{n}$ pairs.

Pour tester la divisibilité de n par les nombres premiers $p \leq \sqrt{n}$, on doit disposer de la liste de tous ces nombres premiers. Le crible d'Eratosthène nous permet d'obtenir une telle liste. Le principe est le suivant :

- on se donne la liste de tous les entiers compris entre 2 et m (m est la partie entière de \sqrt{n} pour l'algorithme précédent) ;
- on garde 2 et on supprime tous les autres multiples de 2 de cette liste ;
- le premier entier strictement supérieur à 2 est 3 et comme il ne possède pas de diviseur strict, il est premier, on le garde et on supprime tous les autres multiples de 3 de la liste ;
- on continue ainsi de suite et on s'arrête dès que l'on tombe sur un nombre premier strictement plus grand que \sqrt{m} . La liste finale contient alors tous les nombres premiers inférieurs à m .

Par exemple pour $m = 25$, on a la séquence suivante :

- $L_0 = (2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25)$;
- 2 est premier et on supprime de L_0 tous les multiples de 2 qui sont différents de 2, ce qui donne la liste $L_1 = (2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25)$;
- 3 est nécessairement premier et en supprimant de L_1 tous les multiples de 3 qui sont différents de 3, on obtient la liste $L_2 = (2, 3, 5, 7, 11, 13, 17, 19, 23, 25)$;
- 5 est nécessairement premier et en supprimant de L_2 tous les multiples de 5 qui sont différents de 5, on obtient la liste $L_3 = (2, 3, 5, 7, 11, 13, 17, 19, 23)$;
- 7 est nécessairement premier et en supprimant de L_3 tous les multiples de 7 qui sont différents de 7, on obtient la liste $L_4 = (2, 3, 5, 7, 11, 13, 17, 19, 23)$. Tous les éléments de cette liste sont premiers puisque $7 > \sqrt{25}$.

Les résultats qui suivent sont élémentaires, mais souvent utiles.

Lemme 24.1 Soit p un entier naturel premier. Pour tout entier naturel non nul n , on a soit p qui divise n , soit p qui est premier avec n .

Démonstration. Comme $\delta = p \wedge n$ divise p , on a soit $\delta = p$ et p divise n , soit $\delta = 1$ et p est premier avec n . ■

Lemme 24.2 Deux nombres premiers distincts sont premiers entre eux.

Démonstration. Soient p, q deux nombres premiers. Si $\delta = p \wedge q \neq 1$, le lemme précédent nous dit que p divise q et q divise p , donc $p = q$. ■

Lemme 24.3 *Un entier $p \geq 2$ est premier si, et seulement si, il est premier avec tout entier compris entre 1 et $p - 1$.*

Démonstration. Si p est premier, comme il ne divise pas $k \in \{1, \dots, p - 1\}$, il est premier avec k .

Réciproquement si p n'est pas premier, il s'écrit alors $p = ab$ avec $a \geq 2$, $b \geq 2$ et p n'est pas premier avec $a \in \{2, \dots, p - 1\}$. ■

Le théorème de Gauss nous donne le résultat suivant qui nous sera utile pour prouver l'unicité (à l'ordre près) de la décomposition en facteurs premiers d'un entier $n \geq 2$.

Lemme 24.4 *Soit p un nombre premier et r un entier naturel supérieur ou égal à 2. Si p divise le produit $n_1 n_2 \cdots n_r$ de r entiers naturels non nuls, alors p divise l'un des n_k .*

Démonstration. On procède par récurrence sur $n \geq 2$.

Si p divise $n_1 n_2$, on a soit p qui divise n_1 , soit p qui est premier avec n_1 et il va alors diviser n_2 (théorème de Gauss).

Supposons le résultat acquis au rang $n - 1 \geq 2$. Si p divise $n_1 n_2 \cdots n_r$, on a soit p qui divise n_1 , soit p qui est premier avec n_1 et il va alors diviser $n_2 \cdots n_r$ et l'un des n_k où k est compris entre 2 et n . ■

Dans le cas où tous les n_k sont égaux à un même entier n , on a :

$$(p \text{ premier divise } n^r) \Rightarrow (p \text{ divise } n)$$

Exercice 24.3 *Soient $p \geq 2$ un nombre premier et n, m des entiers naturels non nuls. Montrer que p divise n ou p^m est premier avec n .*

Solution 24.3 *Si p divise n c'est fini. Sinon p est premier avec n et le théorème de Bézout nous dit qu'il existe deux entiers relatifs u et v tels que $up + vn = 1$. On a alors $1 = (up + vn)^m = u^m p^m + v_n n$, ce qui signifie que p^m et n sont premiers entre eux.*

Exercice 24.4 *Soient a et b deux entiers relatifs non nuls. Montrer que :*

$$(a^2 + b^2) \wedge (ab) = (a \wedge b)^2.$$

Solution 24.4 *Soient $\delta = a \wedge b$ et p, q premiers entre eux tels que $a = \delta p$ et $b = \delta q$. On a :*

$$\begin{aligned} \delta' &= (a^2 + b^2) \wedge (ab) = (\delta^2 (p^2 + q^2)) \wedge (\delta^2 (pq)) \\ &= \delta^2 ((p^2 + q^2) \wedge (pq)). \end{aligned}$$

Il s'agit alors de montrer que $\delta' = (p^2 + q^2) \wedge (pq) = 1$ si $p \wedge q = 1$ (on s'est ramené en fait au cas où a et b sont premiers entre eux). Supposons que $\delta' \geq 2$, il admet alors un diviseur premier $d \geq 2$ et d qui divise pq (pq est multiple de δ') va diviser p ou q . Mais d divise p entraîne d divise p^2 avec d diviseur de $p^2 + q^2$ ($p^2 + q^2$ est multiple de δ'), donc d premier divise q^2 , il divise donc q , ce qui est impossible (p et q premiers entre eux ne peuvent avoir $d \geq 2$ comme diviseur commun). Comme p et q jouent des rôles analogues, d ne divise pas q . On a donc nécessairement $\delta' = 1$.

Exercice 24.5 *Soient a et b deux entiers relatifs non nuls et n un entier naturel non nul. Montrer que :*

$$a^n \wedge b^n = (a \wedge b)^n \text{ et } a^n \vee b^n = (a \vee b)^n.$$

Solution 24.5 Soient $\delta = a \wedge b$ et p, q premiers entre eux tels que $a = \delta p$ et $b = \delta q$. On a :

$$a^n \wedge b^n = (\delta^n p^n) \wedge (\delta^n q^n) = \delta^n (p^n \wedge q^n)$$

et $(a \wedge b)^n = \delta^n$. Il s'agit alors de montrer que $\delta' = p^n \wedge q^n = 1$ si $p \wedge q = 1$ (on s'est ramené en fait au cas où a et b sont premiers entre eux). Supposons que $\delta' \geq 2$, il admet alors un diviseur premier $d \geq 2$ et d qui divise p^n et q^n va diviser p et q ce qui est impossible. On a donc nécessairement $\delta' = 1$.

Pour ce qui est du ppcm, on a :

$$a^n \vee b^n = \frac{|a|^n |b|^n}{a^n \wedge b^n} = \frac{(|a| |b|)^n}{(a \wedge b)^n} = (a \vee b)^n.$$

Par exemple, on a :

$$125 \wedge 27 = 5^3 \wedge 3^3 = 5 \wedge 3 = 1.$$

On peut déduire de l'exercice précédent que deux entiers relatifs non nuls a et b sont premiers entre eux si, et seulement si, a^n et b^n sont premiers entre eux, quel que soit l'entier $n \geq 1$.

Exercice 24.6 Soient a, b, c, d des entiers relatifs non nuls. Montrer que si $a \wedge b = c \wedge d = 1$, alors $(ac) \wedge (bd) = (a \wedge d)(b \wedge c)$.

Solution 24.6 En notant $\delta_1 = a \wedge d$ et $\delta_2 = b \wedge c$, on a $a = \delta_1 p_1$, $d = \delta_1 q_1$, $b = \delta_2 p_2$ et $c = \delta_2 q_2$ avec $p_1 \wedge q_1 = p_2 \wedge q_2 = 1$, ce qui donne :

$$(ac) \wedge (bd) = \delta_1 \delta_2 ((p_1 q_2) \wedge (p_2 q_1)).$$

Si $\delta' = ((p_1 q_2) \wedge (p_2 q_1)) \geq 2$, il admet alors un diviseur premier p qui divise $p_1 q_2$ et $p_2 q_1$ et on a quatre possibilités :

- soit p divise p_1 et q_1 , ce qui est impossible puisque $p_1 \wedge q_1 = 1$;
- soit p divise q_2 et p_2 , ce qui est impossible puisque $p_2 \wedge q_2 = 1$;
- soit p divise p_1 et p_2 et il divise alors a et b ce qui est impossible puisque $a \wedge b = 1$;
- soit p divise q_2 et q_1 et il divise alors c et d ce qui est impossible puisque $c \wedge d = 1$.

La seule possibilité est donc $\delta' = 1$.

24.2 L'ensemble \mathcal{P} des nombres premiers est infini

On peut montrer de nombreuses manières que l'ensemble \mathcal{P} des nombres premiers est infini.

La démonstration élémentaire qui suit, conséquence de l'existence de diviseurs premiers pour $n \geq 2$, est due à Euclide.

Théorème 24.3 (Euclide) L'ensemble \mathcal{P} des nombres premiers est infini.

Démonstration. On sait déjà que \mathcal{P} est non vide (il contient 2). Supposons que \mathcal{P} soit fini avec :

$$\mathcal{P} = \{p_1, \dots, p_r\}.$$

L'entier $n = p_1 \cdots p_r + 1$ qui est supérieur 2 admet un diviseur premier $p_k \in \mathcal{P}$. L'entier p_k divise alors $n = p_1 \cdots p_r + 1$ et $p_1 \cdots p_r$, il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion \mathcal{P} est infini. ■

Remarque 24.2 En rangeant les nombres premiers dans l'ordre croissant, on constate que les entiers $n_r = p_1 \cdots p_r + 1$ sont premiers pour r compris entre 1 et 5 ($n_1 = 3$, $n_2 = 7$, $n_3 = 31$, $n_4 = 211$, $n_5 = 2311$). Pour $r = 6$, $n_6 = 30031 = 59 \times 509$ n'est pas premier. On ne sait pas si la suite $(n_r)_{r \geq 1}$ contient une infinité de nombres premiers.

Exercice 24.7 Montrer que pour tout entier naturel n , on peut trouver un nombre premier p plus grand que n . Conclure.

Solution 24.7 Pour tout $n \in \mathbb{N}$, l'entier $m = n! + 1 \geq 2$ admet un diviseur premier p_n . Si $p_n < n$ alors p_n est un diviseur de $n!$, donc de $1 = m - n!$, ce qui est impossible. On peut donc construire une suite strictement croissante $(p_n)_{n \in \mathbb{N}}$ de nombres premiers, ce qui implique que \mathcal{P} est infini.

Exercice 24.8 On note :

$$\mathcal{P}_1 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} ; p = 4n + 3\}$$

$$\mathcal{P}_2 = \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} ; p = 6n + 5\}$$

Montrer, en s'inspirant de la démonstration du théorème d'Euclide, que \mathcal{P}_1 [resp. \mathcal{P}_2] est infini et conclure.

Solution 24.8 On remarque qu'un nombre premier différent de 2 est nécessairement impair et son reste dans la division euclidienne par 4 [resp. par 6] ne peut être que 1 ou 3 [resp. 1, 3 ou 5].

Supposons que \mathcal{P}_1 [resp. \mathcal{P}_2] soit fini et notons $p_1 = 3$ [resp. $p_1 = 5$] $< p_2 < \cdots < p_r$ tous ses éléments. L'entier :

$$m = 4p_1 \cdots p_r - 1 = 4(p_1 \cdots p_r - 1) + 3$$

$$\text{resp. } m = 6p_1 \cdots p_r - 1 = 6(p_1 \cdots p_r - 1) + 5$$

qui est de la forme $4n + 3$ [resp. $6n + 5$] avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r ($m > 4p_k - 1 > p_k$ puisque $p_k \geq 3$) [resp. $m > 6p_k - 1 > p_k$ puisque $p_k \geq 5$]. Comme m est impair [resp. impair non multiple de 3 puisque congru à 5 modulo 3] ses diviseurs premiers sont de la forme $4k + 1$ avec $k \in \mathbb{N}^*$ ou $4k + 3$ avec $k \in \mathbb{N}$ [resp. $6k + 1$ avec $k \in \mathbb{N}^*$ ou $6k + 5$ avec $k \in \mathbb{N}$] et ils ne peuvent pas être tous de la forme $4k + 1$ [resp. $6k + 1$] sans quoi m serait aussi de cette forme, donc congru à 1 modulo 4 [resp. modulo 6] ce qui contredit le fait qu'il est congru à 3 [resp. à 5] (ou à -1) modulo 4 [resp. modulo 6]. L'entier m a donc un diviseur p_k dans \mathcal{P}_1 [resp. dans \mathcal{P}_2] et comme p_k divise $p_1 \cdots p_r$, il va aussi diviser -1 , ce qui est impossible avec p_k premier. L'ensemble \mathcal{P}_1 [resp. \mathcal{P}_2] est donc infini.

De $\mathcal{P}_1 \subset \mathcal{P}$ [resp. $\mathcal{P}_2 \subset \mathcal{P}$] on déduit que \mathcal{P} est infini.

Remarque 24.3 De manière plus générale on peut montrer que si a et b sont deux entiers premiers entre eux alors il existe une infinité de nombres premiers de la forme $an + b$ (théorème de Dirichlet).

Pour tout réel $x \geq 2$, on désigne par $\pi(x)$ le cardinal de l'ensemble des nombres premiers contenus dans l'intervalle $[0, x]$, soit :

$$\pi(x) = \text{card}(\mathcal{P} \cap [0, x])$$

Du théorème d'Euclide on déduit que :

$$\lim_{x \rightarrow +\infty} \pi(x) = +\infty.$$

Le théorème des nombres premiers (conjecturé par Gauss, puis montré par Hadamard et de la Vallée-Poussin) nous dit plus précisément que :

$$\pi(x) \underset{x \rightarrow +\infty}{\sim} \frac{x}{\ln(x)}.$$

En désignant par li la fonction logarithme intégral définie par :

$$\forall x \geq e, \text{li}(x) = \int_e^x \frac{dt}{\ln(t)}$$

on a aussi :

$$\pi(x) \underset{x \rightarrow +\infty}{\sim} \text{li}(x).$$

Exercice 24.9 Montrer que $\text{li}(x) \underset{x \rightarrow +\infty}{\sim} \frac{x}{\ln(x)}$.

Solution 24.9 Une intégration par parties donne :

$$\text{li}(x) = \left[\frac{t}{\ln(t)} \right]_e^x + \int_e^x \frac{dt}{\ln^2(t)} = \frac{x}{\ln(x)} - 1 + \int_e^x \frac{dt}{\ln^2(t)}$$

avec :

$$\begin{aligned} \varphi(x) &= \int_e^x \frac{dt}{\ln^2(t)} = \int_e^{\sqrt{x}} \frac{dt}{\ln^2(t)} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2(t)} \\ &\leq \frac{\sqrt{x} - e}{\ln^2(e)} + 4 \frac{x - \sqrt{x}}{\ln^2(x)} \leq \sqrt{x} + 4 \frac{x}{\ln^2(x)} \end{aligned}$$

(pour $t \geq \sqrt{x}$, on a $\ln(t) \geq \ln(\sqrt{x}) = \frac{\ln(x)}{2}$) et :

$$0 < \frac{\varphi(x)}{\frac{x}{\ln(x)}} \leq \frac{\ln(x)}{\sqrt{x}} + \frac{4}{\ln(x)} \xrightarrow{x \rightarrow +\infty} 0$$

ce qui donne l'équivalence $\text{li}(x) \underset{x \rightarrow +\infty}{\sim} \frac{x}{\ln(x)}$.

Les exercices qui suivent nous donne une première idée de la répartition des nombres premiers.

Exercice 24.10 On note :

$$2 = p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots$$

la suite infinie des nombres premiers rangée dans l'ordre croissant.

1. Montrer que :

$$\forall n \geq 1, 2n - 1 \leq p_n \leq 2^{2^{n-1}}.$$

2. En déduire que $\pi(x) > \ln(\ln(x))$.

Solution 24.10

1. On procède par récurrence sur $n \geq 1$.

Pour $n = 1$ et $n = 2$, le résultat est évident.

On le suppose acquis pour tout entier k compris entre 1 et $n \geq 2$. Comme pour $n \geq 2$, p_n est impair, l'entier $p_n + 1$ est pair donc non premier et $p_{n+1} \geq p_n + 2$. Avec l'hypothèse de récurrence, on déduit donc que :

$$p_{n+1} \geq p_n + 2 \geq 2n + 1.$$

Si p est un diviseur premier du produit $p_1 \cdots p_n + 1$, on a nécessairement $p \geq p_{n+1}$ (sinon $p = p_k$ où k est compris entre 1 et n , donc p divise $p_1 \cdots p_n$ et 1, ce qui est impossible). On a donc :

$$p_{n+1} \leq p \leq p_1 \cdots p_n + 1 \leq 2^1 \cdots 2^{2^{n-1}} + 1,$$

soit :

$$p_{n+1} \leq 2^{1+2+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \leq 2^{2^n}.$$

2. Pour tout réel $x \geq 2$, la partie entière m de $\ln(\ln(x))$ est telle que :

$$-1 \leq m \leq \ln(\ln(x)) < m + 1$$

et l'entier naturel $n = m + 1$ est tel que :

$$n - 1 \leq \ln(\ln(x)) < n$$

ce qui équivaut à :

$$e^{e^{n-1}} \leq x < e^{e^n}$$

La fonction π étant croissante, on a :

$$n = \pi(p_n) \leq \pi(2^{2^{n-1}}) \leq \pi(e^{2^{n-1}}) \leq \pi(x)$$

soit :

$$\pi(x) \geq n > \ln(\ln(x))$$

Exercice 24.11 Montrer que pour tout entier naturel $n \geq 2$, on peut trouver n entiers naturels consécutifs non premiers (la distribution des nombres premiers n'est pas régulière).

Solution 24.11 Les n entiers $m_k = (n+1)! + k$ où k est compris entre 2 et $n+1$ sont non premiers puisque m_k est divisible par k qui est compris entre 2 et $n+1 < m_k$.

24.3 Décomposition en facteurs premiers

Le théorème qui suit est parfois appelé « théorème fondamental de l'arithmétique ».

Théorème 24.4 Tout entier naturel $n \geq 2$ se décompose de manière unique sous la forme :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad (24.1)$$

où les p_k sont des nombres premiers vérifiant :

$$2 \leq p_1 < p_2 < \cdots < p_r$$

et les α_k sont des entiers naturels non nuls.

Démonstration. On démontre tout d'abord l'existence d'une telle décomposition par récurrence sur $n \geq 2$.

Pour $n = 2$, on a déjà la décomposition.

Supposons le résultat acquis pour tout entier k compris entre 2 et $n \geq 2$. Si $n+1$ est premier, on a déjà la décomposition, sinon on écrit $n+1 = ab$ avec a et b compris entre 2 et n et il suffit d'utiliser l'hypothèse de récurrence pour a et b .

L'unicité d'une telle décomposition peut aussi se montrer par récurrence sur $n \geq 2$. Le résultat est évident pour $n = 2$. Supposons le acquis pour tout entier k compris entre 2 et $n \geq 2$. Si $n+1$ a deux décompositions :

$$n+1 = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s},$$

où les p_j [resp. q_i] sont premiers deux à deux distincts et les α_j [resp. β_i] entiers naturels non nuls. L'entier p_1 est premier et divise le produit $q_1^{\beta_1} \cdots q_s^{\beta_s}$, il divise donc nécessairement l'un des q_k . L'entier q_k étant également premier la seule possibilité est $p_1 = q_k$. En simplifiant par p_1 on se ramène à la décomposition d'un entier inférieur ou égal à n et il suffit alors d'utiliser l'hypothèse de récurrence pour conclure. ■

L'écriture (24.1) est la décomposition en facteurs premiers de l'entier n .

Le théorème précédent se traduit en disant que l'anneau \mathbb{Z} des entiers relatifs est factoriel.

En fait, de manière plus générale, on peut montrer qu'un anneau euclidien (c'est le cas de \mathbb{Z} ou de $\mathbb{K}[x]$) est principal et en conséquence factoriel.

L'unicité dans la décomposition en facteurs premiers peut être utilisée pour montrer que \mathbb{Q} (ou \mathbb{N}^2) est dénombrable.

Exercice 24.12 On désigne par f l'application définie sur $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ par :

$$\forall (n, m) \in \mathbb{N}^2, f(n, m) = 2^n 3^m$$

Montrer que f est injective. Il résulte que \mathbb{N}^2 est dénombrable.

Solution 24.12 L'égalité $f(n, m) = f(n', m')$ avec (n, m) et (n', m') dans \mathbb{N}^2 équivaut à $2^n 3^m = 2^{n'} 3^{m'}$ et l'unicité de la décomposition en facteurs premiers d'un entier naturel non nul nous dit que $(n, m) = (n', m')$. L'application f est donc injective de \mathbb{N}^2 dans \mathbb{N} et bijective de \mathbb{N}^2 dans $f(\mathbb{N}^2) \subset \mathbb{N}$.

Exercice 24.13 Soient $p > q \geq 2$ deux nombres premiers. Montrer que $\frac{\ln(p)}{\ln(q)}$ est irrationnel.

Solution 24.13 Supposons que $\frac{\ln(p)}{\ln(q)} = \frac{\alpha}{\beta}$ avec α, β entiers naturels non nuls premiers entre eux. On a alors $\ln(p^\alpha) = \ln(q^\beta)$ et $p^\alpha = q^\beta$, ce qui est impossible du fait de l'unicité de la décomposition en facteurs premiers.

Exercice 24.14 Soient $p_1 < p_2 < \cdots < p_r$ des nombres premiers. Montrer que les réels $\ln(p_1), \ln(p_2), \dots, \ln(p_r)$ sont \mathbb{Q} -libres dans \mathbb{R} .

Solution 24.14 Supposons qu'il existe des rationnels $\frac{\alpha_1}{\beta_1}, \dots, \frac{\alpha_r}{\beta_r}$ tels que $\sum_{k=1}^r \frac{\alpha_k}{\beta_k} \ln(p_k) = 0$.

En notant $\beta = \prod_{k=1}^r \beta_k$, on a $\sum_{k=1}^r \beta \frac{\alpha_k}{\beta_k} \ln(p_k) = 0$, soit $\sum_{k=1}^r \gamma_k \ln(p_k) = 0$, où les γ_k sont des entiers relatifs, ce qui équivaut à $\prod_{k=1}^r p_k^{\gamma_k} = 1$ et les γ_k sont nécessairement tous nuls puisque les p_k sont premiers distincts (unicité de la décomposition en facteurs premiers).

Exercice 24.15 Soit $n \geq 2$ un entier sans facteur carré, c'est-à-dire que n a une décomposition en facteurs premiers de la forme $n = \prod_{k=1}^r p_k$ où les p_k sont premiers deux à deux distincts. Montrer que \sqrt{n} est irrationnel.

Solution 24.15 Si \sqrt{n} est rationnel, il s'écrit alors $\sqrt{n} = \frac{a}{b}$, où a, b sont deux entiers naturels non nuls premiers entre eux. On a $a^2 = nb^2$ et si p est un diviseur premier de a (on a bien $a \geq 2$ puisque $\sqrt{n} > 1$), p^2 divise nb^2 en étant premier avec b^2 (a et b sont premiers entre eux), il divise n (théorème de Gauss), ce qui contredit le fait que n est sans facteur carré. Donc \sqrt{n} est irrationnel.

Exercice 24.16 Soit n un entier de la forme $n = 2^m + 1$ avec $m \geq 0$. Montrer que si n est premier alors $m = 0$ ou m est une puissance de 2 (ce qui revient à dire que $n = 2^{2^p} + 1$ est un nombre de Fermat).

Solution 24.16 Si $m = 0$, alors $n = 2$ est premier.

Si $m = 1 = 2^0$, alors $n = 3$ est premier.

On suppose que $m \geq 2$. La décomposition en facteurs premiers de m permet d'écrire que $m = 2^p(2q+1)$ où p et q sont des entiers naturels.

Si q est non nul, on a alors :

$$\begin{aligned} n &= (2^{2^p})^{2q+1} + 1 = a^{2q+1} + 1 \\ &= (a+1) \sum_{k=0}^{2q} (-1)^k a^{2q-k} = (a+1)b \end{aligned}$$

avec $a+1 = 2^{2^p} + 1 \geq 3$ et :

$$b = \frac{n}{a+1} = \frac{a \cdot a^{2q} + 1}{a+1} > 1$$

($a \geq 2$ et $q \geq 1$), donc n n'est pas premier.

Exercice 24.17 Soit $p = 2^m - 1$ un nombre premier de MERSENNE (donc m est premier). Montrer que $q = 2^{m-1}p$ est un nombre parfait, c'est-à-dire qu'il est égal à la somme de ses diviseurs stricts (i. e. différents de q).

Solution 24.17 L'entier $q = 2^{m-1}p$ est décomposé en facteurs premiers et ses diviseurs stricts sont les 2^k avec k compris entre 0 et $m-1$ et les $2^k p$ avec k compris entre 0 et $m-2$. La somme de ses diviseurs stricts est :

$$\begin{aligned} S &= \sum_{k=0}^{m-1} 2^k + p \sum_{k=0}^{m-2} 2^k \\ &= 2^m - 1 + p(2^{m-1} - 1) = p + p(2^{m-1} - 1) = q \end{aligned}$$

Si $n = \prod_{k=1}^r p_k^{\alpha_k}$ est un entier décomposé en produit de facteurs premiers, alors les diviseurs de n sont de la forme $d = \prod_{k=1}^r p_k^{\gamma_k}$ où les γ_k sont des entiers naturels tels que $\gamma_k \leq \alpha_k$ pour tout k compris entre 1 et r . Il y a donc $\prod_{k=1}^r (\alpha_k + 1)$ diviseurs positifs possibles de n .

La décomposition en facteurs premiers peut être utilisée pour calculer le pgcd et le ppcm de deux entiers naturels supérieur ou égal à 2.

Tout est basé sur le lemme qui suit.

Lemme 24.5 Soient n, m deux entiers naturels supérieur ou égal à 2 et :

$$n = \prod_{k=1}^r p_k^{\alpha_k}, \quad m = \prod_{k=1}^r p_k^{\beta_k}$$

leurs décompositions en facteurs premiers avec les p_k premiers deux à deux distincts et les α_k, β_k entiers naturels (certains de ces entiers pouvant être nuls). On a alors :

$$(a \text{ divise } b) \Leftrightarrow (\forall k \in \{1, 2, \dots, r\}, \alpha_k \leq \beta_k)$$

Démonstration. Dire que n divise m équivaut à dire qu'il existe un entier $q \geq 1$ tel que $m = qn$ et en écrivant $q = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ où les γ_k sont des entiers naturels, on a :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} = p_1^{\alpha_1 + \gamma_1} \cdots p_r^{\alpha_r + \gamma_r}.$$

L'unicité de la décomposition en facteurs premiers de m nous dit alors que :

$$\forall k \in \{1, 2, \dots, r\}, \beta_k = \alpha_k + \gamma_k \geq \alpha_k.$$

■

Théorème 24.5 Soient n, m deux entiers naturels supérieur ou égal à 2 et :

$$n = \prod_{k=1}^r p_k^{\alpha_k}, \quad m = \prod_{k=1}^r p_k^{\beta_k}$$

leurs décompositions en facteurs premiers avec les p_k premiers deux à deux distincts et les α_k, β_k entiers naturels (certains de ces entiers pouvant être nuls). On a alors :

$$n \wedge m = \prod_{k=1}^r p_k^{\min(\alpha_k, \beta_k)}, \quad n \vee m = \prod_{k=1}^r p_k^{\max(\alpha_k, \beta_k)}.$$

Démonstration. L'entier $\delta = \prod_{k=1}^r p_k^{\min(\alpha_k, \beta_k)}$ divise n et m d'après le lemme précédent.

Si d est un diviseur de n et m , il s'écrit sous la forme $d = \prod_{k=1}^r p_k^{\gamma_k}$ où les γ_k sont des entiers naturels tels que $\gamma_k \leq \alpha_k$ et $\gamma_k \leq \beta_k$ pour tout k compris entre 1 et r , on a donc $\gamma_k \leq \min(\alpha_k, \beta_k)$ pour tout k compris entre 1 et r et d divise δ . Donc δ est bien le pgcd de n et m .

Pour ce qui est du ppcm, on a :

$$n \vee m = \frac{nm}{n \wedge m} = \prod_{k=1}^r p_k^{\alpha_k + \beta_k - \min(\alpha_k, \beta_k)}$$

avec :

$$\alpha_k + \beta_k - \min(\alpha_k, \beta_k) = \max(\alpha_k, \beta_k)$$

pour tout k compris entre 1 et r . ■

Le résultat précédent se généralise au calcul du pgcd et du ppcm de $p \geq 2$ entiers naturels.

Exercice 24.18 On note $2 = p_1 < p_2 < \cdots < p_n < \cdots$ la suite infinie des nombres premiers et on se propose de montrer la divergence de la série $\sum_{n=1}^{+\infty} \frac{1}{p_n}$. Pour ce faire, on introduit la suite $(u_n)_{n \geq 1}$ définie par :

$$\forall n \geq 1, u_n = \frac{1}{\prod_{k=1}^n \left(1 - \frac{1}{p_k}\right)}.$$

1. Montrer que, pour tout $n \geq 1$, on a :

$$u_n = \sum_{k \in E_n} \frac{1}{k}$$

où E_n est l'ensemble des entiers naturels non nuls qui ont tous leurs diviseurs premiers dans $\mathcal{P}_n = \{p_1, \dots, p_n\}$.

2. En déduire que, pour tout $n \geq 1$, on a :

$$u_n \geq \sum_{k=1}^{p_n} \frac{1}{k}.$$

3. En déduire que la série $\sum \ln \left(1 - \frac{1}{p_n}\right)$ est divergente et conclure.

4. Quelle est la nature de la série $\sum \frac{1}{p_n^\alpha}$ où α est un réel ?

5. Quelle est le rayon de convergence de la série entière $\sum \frac{z^{p_n}}{p_n}$.

Solution 24.18

1. Pour $n \geq 1$, on a :

$$\begin{aligned} u_n &= \prod_{k=1}^n \frac{1}{1 - \frac{1}{p_k}} = \prod_{k=1}^n \left(\sum_{i=0}^{+\infty} \frac{1}{p_k^i} \right) = \sum_{i_1 \geq 0, i_2 \geq 0, \dots, i_n \geq 0}^{+\infty} \frac{1}{p_1^{i_1} p_2^{i_2} \dots p_n^{i_n}} \\ &= \sum_{k \in E_n} \frac{1}{k}. \end{aligned}$$

2. Résulte du fait que E_n contient $\{1, 2, \dots, p_n\}$, la série étant à termes positifs.

3. La suite $\left(\sum_{k=1}^{p_n} \frac{1}{k} \right)_{n \geq 1}$ étant extraite de la suite divergente vers l'infini $\left(\sum_{k=1}^n \frac{1}{k} \right)_{n \geq 1}$, on a

$$\lim_{n \rightarrow +\infty} \sum_{k=1}^{p_n} \frac{1}{k} = +\infty, \text{ donc } \lim_{n \rightarrow +\infty} u_n = +\infty \text{ et } \lim_{n \rightarrow +\infty} \prod_{k=1}^n \left(1 - \frac{1}{p_k}\right) = 0, \text{ ce qui entraîne :}$$

$$\lim_{n \rightarrow +\infty} \ln \left(\prod_{k=1}^n \left(1 - \frac{1}{p_k}\right) \right) = \lim_{n \rightarrow +\infty} \sum_{k=1}^n \ln \left(1 - \frac{1}{p_k}\right) = -\infty$$

La série $\sum \ln \left(1 - \frac{1}{p_n}\right)$ est donc divergente. Cette série étant à termes négatifs avec

$$\ln \left(1 - \frac{1}{p_n}\right) \underset{+\infty}{\sim} -\frac{1}{p_n}, \text{ on en déduit la divergence de } \sum \frac{1}{p_n}.$$

On a aussi la courte démonstration suivante :

Si $\sum_{n=1}^{+\infty} \frac{1}{p_n} < +\infty$ il existe alors un entier $r \geq 1$ tel que :

$$R_r = \sum_{n=r+1}^{+\infty} \frac{1}{p_n} < \frac{1}{2}.$$

On note $P = p_1 \cdots p_r$. Pour tout $n \geq 1$, les diviseurs premiers de $1 + nP$ sont dans $\{p_k \mid k \geq r+1\}$ (pour $1 \leq k \leq r$, le nombre premier p_k divisant P ne peut diviser $1 + nP$) et on a :

$$1 + nP = p_{r+1}^{m_1} \cdots p_{r+s_n}^{m_{s_n}}$$

avec $s_n \geq 1$, $m_j \geq 0$ pour j compris entre 1 et s_n et $m_{s_n} \geq 1$. On en déduit que pour tout $N \geq 1$, on a :

$$\sum_{n=1}^N \frac{1}{1+nP} = \sum_{n=1}^N \prod_{k=1}^{s_n} \frac{1}{p_{r+k}^{m_k}} < \sum_{j=1}^{+\infty} \left(\sum_{k=1}^{+\infty} \frac{1}{p_{r+k}} \right)^j < \sum_{j=1}^{+\infty} \left(\frac{1}{2} \right)^j$$

en contradiction avec $\sum_{n=1}^{+\infty} \frac{1}{1+nP} = +\infty$.

4. Pour $\alpha \leq 0$, on a $\frac{1}{p_n^\alpha} \geq 1$ et la série $\sum \frac{1}{p_n^\alpha}$ diverge puisque son terme général ne tend pas vers 0.

Pour $0 < \alpha \leq 1$, on a $\frac{1}{p_n^\alpha} \geq \frac{1}{p_n}$ et la série $\sum \frac{1}{p_n^\alpha}$ diverge.

Pour $\alpha > 1$, on a pour tout $n \geq 1$:

$$S_n = \sum_{k=1}^n \frac{1}{p_k^\alpha} \leq \sum_{k=1}^{p_n} \frac{1}{k^\alpha} < \sum_{k=1}^{+\infty} \frac{1}{k^\alpha} < +\infty$$

donc la suite des sommes partielles $(S_n)_{n \geq 1}$ est majorée et la série $\sum \frac{1}{p_n^\alpha}$ converge.

5. La série $\sum \frac{z^{p_n}}{p_n}$ diverge pour $z = 1$, son rayon de convergence est donc $R \leq 1$.

Pour $|z| < 1$ et $n \geq 1$, on a $p_n \geq n$ et :

$$\left| \frac{z^{p_n}}{p_n} \right| \leq |z^{p_n}| \leq |z^n|$$

avec $\sum_{n=1}^{+\infty} |z^n| < +\infty$, donc $\sum_{n=1}^{+\infty} \left| \frac{z^{p_n}}{p_n} \right| < +\infty$ et $R \geq 1$. On a donc $R = 1$.

Un théorème de Mertens nous dit que pour tout réel $x \geq 2$, on a :

$$\sum_{p_n \leq x} \frac{1}{p_n} = C + \ln(\ln(x)) + O\left(\frac{1}{\ln(x)}\right)$$

où $C \simeq 0.261$.

On a aussi :

$$\sum_{p_n \leq x} \frac{1}{p_n} = \ln(x) + O(1).$$

24.4 Valuation p -adique

Pour tout nombre premier p et tout entier naturel non nul n , on note $\nu_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers avec $\nu_p(n) = 0$ si p ne figure pas dans cette décomposition et $\nu_p(1) = 0$. Cet entier $\nu_p(n)$ est appelé la valuation p -adique de n .

On a donc :

$$\nu_p(n) = \max \{k \in \mathbb{N} \mid p^k \text{ divise } n\}$$

et :

$$\nu_p(n) \neq 0 \Leftrightarrow (p \text{ divise } n).$$

La décomposition en facteurs premiers de n peut donc s'écrire sous la forme :

$$n = \prod_{p \in \mathcal{D}_n \cap \mathcal{P}} p^{\nu_p(n)}$$

où \mathcal{D}_n désigne l'ensemble des diviseurs positifs de n , ce qui peut aussi s'écrire $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$, le produit étant fini puisque $\nu_p(n) = 0$ si p ne divise pas n .

On peut remarquer que si m est le nombre de zéros qui terminent l'écriture décimale d'un entier $n \geq 2$, alors n est divisible par 10^m et pas par 10^{m+1} et en conséquence, $m = \min(\nu_2(n), \nu_5(n))$.

Théorème 24.6

1. Si p est un nombre premier et n, m sont deux entiers naturels non nuls, alors :

$$\begin{cases} \nu_p(nm) = \nu_p(n) + \nu_p(m) \\ \nu_p(n+m) \geq \min(\nu_p(n), \nu_p(m)) \end{cases}$$

l'égalité étant réalisée dans la deuxième formule si $\nu_p(n) \neq \nu_p(m)$.

2. Soient n, m deux entiers naturels non nuls.

(a) n divise m si, et seulement si, $\nu_p(n) \leq \nu_p(m)$ pour tout $p \in \mathcal{P}$.

(b) Pour tout $p \in \mathcal{P}$, on a :

$$\begin{cases} \nu_p(n \wedge m) = \min(\nu_p(n), \nu_p(m)) \\ \nu_p(n \vee m) = \max(\nu_p(n), \nu_p(m)) \end{cases}$$

Démonstration.

1. On a :

$$nm = \prod_{q \in \mathcal{P}} q^{\nu_q(n) + \nu_q(m)}$$

ce qui entraîne $\nu_p(nm) = \nu_p(n) + \nu_p(m)$ pour tout $p \in \mathcal{P}$ et en supposant que $\nu_p(n) \leq \nu_p(m)$:

$$\begin{aligned} n + m &= p^{\nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)} \\ &= p^{\nu_p(n)} \left(\prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m) - \nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)} \right) \end{aligned}$$

ce qui entraîne $\nu_p(n+m) \geq \nu_p(n) = \min(\nu_p(n), \nu_p(m))$. Si $\nu_p(n) \leq \nu_p(m)$, alors $\prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(n)} + p^{\nu_p(m) - \nu_p(n)} \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(m)}$ ne peut pas être divisible par p et $\nu_p(n+m) = \nu_p(n)$.

2.

- (a) C'est le lemme 24.5.
- (b) C'est le théorème 24.5.

■

Exercice 24.19 On se donne un entier $n \geq 2$ et un nombre premier p .

1. Déterminer, pour tout entier naturel non nul k , le nombre n_k de multiples de p^k compris entre 1 et n .
2. Montrer que :

$$\nu_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right]$$

(formule de Legendre).

3. Donner un équivalent de $\nu_p(n!)$ quand n tend vers l'infini.
4. Déterminer le nombre de zéros qui terminent l'écriture décimale de $100!$

Solution 24.19

1. Les multiples de p^k compris entre 1 et n sont les entiers $m = p^k q$ où q est un entier compris entre 1 et $\frac{n}{p^k}$, il y en a $n_k = \left[\frac{n}{p^k} \right]$. Pour $p^k > n$, on a $n_k = 0$.
2. L'ensemble $E_n = \{1, 2, \dots, n\}$ peut être partitionné sous la forme :

$$E_n = \bigcup_{k=0}^{+\infty} (P_k \cap E_n)$$

où P_0 est l'ensemble des entiers non multiples de p et, pour $k \geq 1$, P_k est l'ensemble des entiers multiples de p^k et non multiples de p^{k+1} . Pour tout $k \geq 0$ et tout $m \in P_k$, on a $\nu_p(m) = k$. De plus, pour $k \geq 1$, $P_k \cap E_n$ est formé de l'ensemble des entiers compris entre 1 et n qui sont multiples de p^k privé du sous-ensemble formé des multiples de p^{k+1} et donc $\text{card}(P_k \cap E_n) = n_k - n_{k+1}$.

On en déduit que :

$$\begin{aligned} \nu_p(n!) &= \sum_{m=1}^n \nu_p(m) = \sum_{k=0}^{+\infty} \sum_{m \in P_k \cap E_n} \nu_p(m) \\ &= \sum_{k=0}^{+\infty} k \text{card}(P_k \cap E_n) = \sum_{k=0}^{+\infty} k (n_k - n_{k+1}) \end{aligned}$$

cette somme étant en réalité finie. Précisément on a $n_k = 0$ dès que $p^k > n$, soit $k > \frac{\ln(n)}{\ln(p)}$. On a donc, en posant $q = \left\lceil \frac{\ln(n)}{\ln(p)} \right\rceil$ et en effectuant un changement d'indice :

$$\begin{aligned}\nu_p(n!) &= \sum_{k=1}^q k(n_k - n_{k+1}) = \sum_{k=1}^q kn_k - \sum_{k=1}^q kn_{k+1} \\ &= \sum_{k=1}^q kn_k - \sum_{j=2}^{q+1} (j-1)n_j \\ &= n_1 + \sum_{k=2}^q (kn_k - (k-1)n_k) - qn_{q+1} \\ &= \sum_{k=1}^q n_k = \sum_{k=1}^{+\infty} n_k = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.\end{aligned}$$

3. Avec les notations précédentes, on a pour tout entier k compris entre 1 et $q_n = \left\lceil \frac{\ln(n)}{\ln(p)} \right\rceil$:

$$\left\lfloor \frac{n}{p^k} \right\rfloor \leq \frac{n}{p^k} < \left\lfloor \frac{n}{p^k} \right\rfloor + 1$$

et :

$$\nu_p(n!) = \sum_{k=1}^{q_n} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{q_n} \frac{n}{p^k} < \nu_p(n!) + q_n$$

ou encore :

$$\frac{\nu_p(n!)}{n} \leq \sum_{k=1}^{q_n} \frac{1}{p^k} < \frac{\nu_p(n!)}{n} + \frac{q_n}{n}$$

avec :

$$0 < \frac{q_n}{n} \leq \frac{1}{\ln(p)} \frac{\ln(n)}{n} \xrightarrow{n \rightarrow +\infty} 0$$

ce qui donne :

$$\lim_{n \rightarrow +\infty} \left(\sum_{k=1}^{q_n} \frac{1}{p^k} - \frac{\nu_p(n!)}{n} \right) = 0$$

et tenant compte de $\lim_{n \rightarrow +\infty} q_n = +\infty$, on a :

$$\lim_{n \rightarrow +\infty} \sum_{k=1}^{q_n} \frac{1}{p^k} = \sum_{k=0}^{+\infty} \frac{1}{p^k} - 1 = \frac{1}{1 - \frac{1}{p}} - 1 = \frac{1}{p-1}$$

et $\lim_{n \rightarrow +\infty} \frac{\nu_p(n!)}{n} = \frac{1}{p-1}$, soit $\nu_p(n!) \underset{n \rightarrow +\infty}{\sim} \frac{n}{p-1}$.

4. Si m est le nombre de zéros qui terminent l'écriture décimale de $n!$ où $n = 100$, alors $n!$ est divisible par 10^m et pas par 10^{m+1} et donc :

$$m = \min(\nu_2(n!), \nu_5(n!)).$$

On a :

$$\nu_2(100!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{100}{2^k} \right\rfloor = \sum_{k=1}^q \left\lfloor \frac{100}{2^k} \right\rfloor$$

avec $q = \left\lfloor \frac{\ln(100)}{\ln(2)} \right\rfloor = 6$ et :

$$\nu_5(100!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{100}{5^k} \right\rfloor = \sum_{k=1}^{q'} \left\lfloor \frac{100}{5^k} \right\rfloor$$

avec $q' = \left\lfloor \frac{\ln(100)}{\ln(5)} \right\rfloor = 2$ ce qui donne :

$$\nu_5(100!) = \frac{100}{5} + \frac{100}{25} = 24 < \frac{100}{2} < \nu_2(100!)$$

et $m = 24$, ce qui est confirmé par Maple :

```
100! = 93 326 215 443 944 152 681 699 238 856 266 700 490 715 968 264 38
621 468 592 963 895 217 599 993 229 915 608 941 463 976 156 518
286 253 697 920 827 223 758 251 185 210 916 864
000 000 000 000 000 000 000 000
```

On peut remarquer que $\nu_2(100!) \simeq 100$ et $\nu_5(100!) \simeq 25$.

Exercice 24.20 Pour tout entier naturel n supérieur ou égal à 2, on note $H_n = \sum_{k=1}^n \frac{1}{k}$.

1. Soit p un entier naturel non nul. Montrer que $H_{2p} = \frac{1}{2}H_p + \frac{a}{2b+1}$ où a, b sont des entiers naturels avec a non nul.
2. Montrer par récurrence que pour tout entier naturel non nul H_n est le quotient d'un entier impair par un entier pair et qu'en conséquence ce n'est pas un entier.

Solution 24.20

1. On a :

$$H_{2p} = \sum_{k=1}^p \frac{1}{2k} + \sum_{k=0}^{p-1} \frac{1}{2k+1} = \frac{1}{2}H_p + \frac{N}{D}$$

avec $D = \text{ppcm}(1, 3, \dots, 2p-1)$ qui est impair et N entier naturel non nul.

2. On a $H_2 = \frac{3}{2} \notin \mathbb{N}$. Supposons le résultat acquis au rang $n \geq 2$. Si $n = 2p$, on a alors :

$$\begin{aligned} H_{n+1} &= H_n + \frac{1}{2p+1} = \frac{2a+1}{2b} + \frac{1}{2p+1} \\ &= \frac{(2a+1)(2p+1) + 2b}{2b(2p+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + b + p + 2ap$ et $b' = b(2p+1)$. Si $n = 2p+1$, on a alors :

$$\begin{aligned} H_{n+1} &= H_{2(p+1)} = \frac{c}{2d+1} + \frac{1}{2}H_{p+1} \\ &= \frac{c}{2d+1} + \frac{1}{2} \frac{2a+1}{2b} = \frac{4bc + (2d+1)(2a+1)}{4b(2d+1)} = \frac{2a'+1}{2b'} \end{aligned}$$

avec $a' = a + d + 2ad + 2bc$ et $b' = b(2d+1)$.

Dans tous les cas, H_n est le quotient d'un entier impair par un entier pair et en conséquence, ce n'est pas un entier.

Exercice 24.21 Soient $m < n$ deux entiers naturels non nuls et :

$$H_{m,n} = \sum_{k=m}^n \frac{1}{k}.$$

1. Montrer que :

$$r = \max_{m \leq k \leq n} \nu_2(k) \neq 0.$$

2. On veut montrer qu'il existe un unique entier k compris entre m et n tel que $r = \nu_2(k)$. Pour ce faire on raisonne par l'absurde en supposant que $r = \nu_2(k_1) = \nu_2(k_2)$ avec $m \leq k_1 < k_2 \leq n$.

(a) Montrer que $r = \nu_2(k_3)$ avec $k_1 < k_3 = \frac{k_1 + k_2}{2} < k_2$.

(b) Montrer que la suite $(k_j)_{j \geq 2}$ définie par $k_{j+1} = \frac{k_1 + k_j}{2}$ est une suite strictement décroissante d'entiers naturels non nuls vérifiant $r = \nu_2(k_j)$ pour tout $j \geq 2$ et conclure.

3. Montrer qu'il existe un entier impair s tel que :

$$\text{ppcm}(m, m+1, \dots, n) = 2^r s.$$

4. On désigne par k l'unique entier compris entre m et n tel que $r = \nu_2(k)$.

(a) Montrer qu'il existe un entier impair n_k tel que :

$$\frac{1}{k} = \frac{n_k}{2^r s}.$$

(b) Montrer que pour tout entier j compris entre m et n et différent de k , il existe un entier pair n_j tel que :

$$\frac{1}{j} = \frac{n_j}{2^r s}.$$

(c) En déduire que $H_{m,n}$ s'écrit comme le quotient d'un entier impair par un entier pair et donc qu'il n'est pas entier.

Solution 24.21

1. Du fait que l'un des deux entiers m ou $m+1$ est pair, on déduit que pour $m < n$ on a $r = \max_{m \leq k \leq n} \nu_2(k) \neq 0$.

2. L'ensemble $\{m, \dots, n\}$ étant fini il existe au moins un entier k compris entre m et n tel que $r = \nu_2(k)$ et il s'agit ici de montrer que cet entier est unique. On suppose donc qu'il existe deux entiers $k_1 < k_2$ compris entre m et n tels que $r = \nu_2(k_1) = \nu_2(k_2)$. On a alors $k_1 = 2^r q_1$ et $k_2 = 2^r q_2$ avec q_1 et q_2 impairs.

(a) L'entier $k_3 = \frac{k_1 + k_2}{2}$, milieu de l'intervalle $[k_1, k_2]$, est compris entre m et n et il s'écrit :

$$k_3 = 2^{r-1} (q_1 + q_2),$$

avec $q_1 + q_2$ pair. On a donc $\nu(k_3) \geq r$ et comme on a aussi $\nu_2(k_3) \leq r = \max_{m \leq k \leq n} \nu_2(k)$, on a nécessairement $\nu_2(k_3) = r$.

(b) En itérant la construction précédente, on peut construire une suite strictement décroissante d'entiers $(k_j)_{j \geq 2}$ telle que $k_{j+1} = \frac{k_1 + k_j}{2}$, $m \leq k_1 < k_j \leq n$ et $r = \nu_2(k_1) = \nu_2(k_j)$, ce qui est impossible. On peut donc conclure qu'il existe un unique entier k compris entre m et n tel que $r = \nu_2(k)$.

3. En utilisant les décompositions en facteurs premiers de tous les entiers compris entre m et n , on a :

$$\text{ppcm}(m, m+1, \dots, n) = 2^r s,$$

où s est un entier impair.

4. Pour tout entier j compris entre m et n , on peut écrire :

$$\frac{1}{j} = \frac{1}{2^{\nu_2(j)} q_j},$$

où q_j est impair et divise s . Soit en écrivant $s = q_j p_j$ avec p_j impair :

$$\frac{1}{j} = \frac{2^{r-\nu_2(j)} p_j}{2^r s}.$$

(a) Pour $j = k$ on a $r = \nu_2(k)$ et :

$$\frac{1}{k} = \frac{n_k}{2^r s},$$

avec $n_k = p_k$ impair.

(b) Pour $j \neq k$, on a $\nu_2(j) < r$ et :

$$\frac{1}{j} = \frac{n_j}{2^r s},$$

avec $n_j = 2^{r-\nu_2(j)} p_j$ pair.

(c) En écrivant que :

$$H_{m,n} = \frac{1}{k} + \sum_{\substack{j=m \\ j \neq k}}^n \frac{1}{j} = \frac{n_k}{2^r s} + \frac{u}{2^r s} = \frac{n_k + u}{2^r s},$$

avec n_k impair et u pair, on déduit que $H_{m,n}$ est le quotient d'un entier impair par un entier pair. En conséquence $H_{m,n}$ n'est pas un entier.

Exercice 24.22 Soit $n \geq 3$ un entier.

Si $a < b$ sont des réels strictement positifs, on notera $\prod_{a \leq p \leq b} p$ le produit des nombres premiers compris entre a et b , avec la convention que ce produit vaut 1 s'il n'y a pas de nombres premiers compris entre a et b . On utilise la même notation avec les inégalités $a < p \leq b$, $a \leq p < b$ ou $a < p < b$.

1. Montrer que, pour tout réel $x > 0$, $[2x] - 2[x]$ vaut 0 ou 1.

2. Montrer que tous les facteurs premiers de C_{2n}^n sont compris entre 2 et $2n$.

3. Calculer $\nu_p(C_{2n}^n)$ pour tout nombre premier p .

4. Montrer que si p est un nombre premier vérifiant $\sqrt{2n} < p < 2n$, alors $\nu_p(C_{2n}^n)$ vaut 0 ou 1.

5. Montrer que si p est un nombre premier vérifiant $\frac{2}{3}n < p < n$, alors $\nu_p(C_{2n}^n) = 0$.

6. Montrer que si p est un nombre premier vérifiant $2 \leq p \leq \sqrt{2n}$, on a alors, en notant $m_p = \nu_p(C_{2n}^n)$, $p^{m_p} \leq 2n$.
7. Dédurre de ce qui précède que :

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p$$

Solution 24.22

1. Des encadrements :

$$\begin{cases} [2x] \leq 2x < [2x] + 1 \\ [x] \leq x < [x] + 1 \end{cases}$$

on déduit que :

$$[2x] - 2[x] > 2x - 1 - 2x = -1$$

soit $[2x] - 2[x] \geq 0$ et :

$$[2x] - 2[x] < 2x - 2x + 2 = 2$$

soit $[2x] - 2[x] \leq 1$. On a donc bien $[2x] - 2[x] \in \{0, 1\}$.

2. Si p est un diviseur premier de C_{2n}^n , il divise aussi $(2n)! = (n!)^2 C_{2n}^n$ et en conséquence il divise l'un des entiers m compris entre 1 et $2n$, il est donc nécessairement compris entre 2 et $2n$.

3. On a :

$$\nu_p((2n)!) = \nu_p((n!)^2 C_{2n}^n) = 2\nu_p(n!) + \nu_p(C_{2n}^n)$$

et en utilisant la formule de Legendre (exercice précédent) :

$$\begin{aligned} \nu_p(C_{2n}^n) &= \nu_p((2n)!) - 2\nu_p(n!) \\ &= \sum_{k=1}^{+\infty} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right). \end{aligned}$$

4. Si p est un nombre premier vérifiant $\sqrt{2n} < p < 2n$, on a alors pour tout $k \geq 2$:

$$0 < \frac{n}{p^k} < \frac{2n}{p^k} \leq \frac{2n}{p^2} < 1$$

et $\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] = 0$, ce qui donne :

$$\nu_p(C_{2n}^n) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] \in \{0, 1\}$$

5. Pour $n \geq 5$, on a $\sqrt{2n} < \frac{2}{3}n$ (c'est équivalent à $\sqrt{2n} > 3$ ou encore à $2n > 9$), donc si p est un nombre premier tel que $\frac{2}{3}n < p \leq n$, on a $\nu_p(C_{2n}^n) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right]$ avec :

$$\begin{cases} 2 \leq \frac{2n}{p} < 3 \\ 1 \leq \frac{n}{p} < \frac{3}{2} \end{cases}$$

ce qui donne :

$$\nu_p(C_{2n}^n) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] = 2 - 2 = 0.$$

Pour $n = 2$, le seul nombre premier vérifiant $\frac{2}{3}2 < p \leq 2$ est $p = 2$ et :

$$\nu_2(C_4^2) = \nu_2(6) = 1.$$

Pour $n = 3$, le seul nombre premier vérifiant $\frac{2}{3}3 < p \leq 3$ est $p = 3$ et :

$$\nu_3(C_6^3) = \nu_3(20) = 0.$$

Pour $n = 4$, le seul nombre premier vérifiant $\frac{2}{3}4 < p \leq 4$ est $p = 3$ et :

$$\nu_3(C_8^4) = \nu_3(65) = 0.$$

On peut aussi dire directement que si $\frac{2}{3}n < p \leq n$ avec $n \geq 3$, alors $p > \frac{2}{3}3 = 2$, soit $p \geq 3$, donc $p^2 \geq 3p > 2n$ et pour tout $k \geq 2$:

$$\frac{n}{p^k} < \frac{2n}{p^k} \leq \frac{2n}{p^2} < 1$$

ce qui donne $\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] = 0$ et :

$$\nu_p(C_{2n}^n) = \left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] = 2 - 2 = 0$$

puisque $2 \leq \frac{2n}{p} < 3$ et $1 \leq \frac{n}{p} < \frac{3}{2}$.

6. En notant, pour tout entier $k \geq 1$, $a_k = \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right]$, on a :

$$m_p = \nu_p(C_{2n}^n) = \sum_{k=1}^{+\infty} a_k$$

cette somme étant finie et les a_k valant 0 ou 1. Si tous les a_k sont nuls, alors $m_p = 0$ et $p^{m_p} = 1 \leq 2n$. Sinon, il y en a seulement un nombre fini qui valent 1 et on désigne par r le grand indice tel que $a_r = 1$. On a alors :

$$m_p = \sum_{k=1}^r a_k \leq r.$$

Si $p^{m_p} > 2n$, on a alors $\frac{2n}{p^k} \leq \frac{2n}{p^{m_p}} < 1$ pour tout $k \geq m_p$ et $a_k = 0$, ce qui impose $r < m_p$ ($r \geq m_p$ donnerait $a_r = 0$, alors que $a_r = 1$) en contradiction avec $m_p \leq r$. On a donc $p^{m_p} \leq 2n$.

7. Comme les facteurs premiers de C_{2n}^n sont compris entre 2 et $2n$ avec $\nu_p(C_{2n}^n) \in \{0, 1\}$ pour $\sqrt{2n} < p < 2n$, on a :

$$C_{2n}^n = \prod_{2 \leq p \leq \sqrt{2n}} p^{m_p} \prod_{\sqrt{2n} < p \leq 2n} p^{m_p}$$

avec $m_p = \nu_p(C_{2n}^n)$ et $p^{m_p} \leq 2n$ pour $2 \leq p \leq \sqrt{2n}$, $m_p \in \{0, 1\}$ pour $\sqrt{2n} < p \leq 2n$. Comme il y a au plus $[\sqrt{2n}]$ nombres premiers entre 2 et $\sqrt{2n}$ avec $[\sqrt{2n}] \leq \sqrt{2n}$, on déduit que :

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq 2n} p^{m_p}.$$

De plus on a vu que $m_p = 0$ pour $\frac{2}{3}n < p \leq n$, ce qui donne :

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{m_p} \prod_{n < p \leq 2n} p^{m_p} \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p$$

24.5 Le postulat de Bertrand

On se propose ici de montrer le résultat suivant postulé par J. Bertrand en 1845 : si n est un entier supérieur ou égal à 2, il existe des nombres premiers compris entre n et $2n$.

La démonstration de ce lemme utilise la majoration :

$$\forall n \geq 2, C_{2n}^n \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p$$

établie avec l'exercice 24.22 et les lemmes techniques qui suivent.

Lemme 24.6 Pour tout entier $r \geq 1$, on a :

$$\frac{2^{2r}}{2r} \leq C_{2r+1}^r \leq 2^{2r}$$

et $\prod_{r+2 \leq p \leq 2r+1} p$ divise C_{2r+1}^r .

Démonstration. Pour $r \geq 1$, on a :

$$\begin{aligned} 2^{2r+1} &= (1+1)^{2r+1} = \sum_{k=0}^{2r+1} C_{2r+1}^k \\ &\geq C_{2r+1}^r + C_{2r+1}^{r+1} = 2C_{2r+1}^r \end{aligned}$$

et $C_{2r+1}^r \leq 2^{2r}$.

Pour k compris entre 1 et r , on a :

$$\begin{aligned} C_{2r}^k &= \frac{(2r)!}{k!(2r-k)!} = \frac{2r-k+1}{k} \frac{(2r)!}{(k-1)!(2r-(k-1))!} \\ &= \frac{2r-k+1}{k} C_{2r}^{k-1} \geq \frac{k+1}{k} C_{2r}^{k-1} > C_{2r}^{k-1} \end{aligned}$$

Il en résulte que $C_{2r}^r > C_{2r}^k$ pour tout k compris entre 1 et $r-1$, cette inégalité étant encore valable pour $k=0$. Et avec $C_{2r}^{r+k} = C_{2r}^{r-k}$ pour k compris entre 0 et r , on déduit que $C_{2r}^r > C_{2r}^k$ pour tout $k \neq r$ compris entre 0 et $2r$.

De ces inégalités, on déduit que :

$$\begin{aligned} 2^{2r} &= (1+1)^{2r} = C_{2r}^0 + C_{2r}^r + \sum_{\substack{k=1 \\ k \neq r}}^{2r} C_{2r}^k \\ &< C_{2r}^0 + C_{2r}^r + (2r-1)C_{2r}^r = 1 + 2rC_{2r}^r \end{aligned}$$

soit $2^{2r} \leq 2rC_{2r}^r$, ou encore $\frac{2^{2r}}{2r} \leq C_{2r}^r$.

S'il n'y a pas de nombres premiers compris entre $r+2$ et $2r+1$, alors $\prod_{r+2 \leq p \leq 2r+1} p = 1$ divise C_{2r+1}^r . Sinon, soit p un nombre premier compris entre $r+2$ et $2r+1$. Cet entier p divise $(2r+1)! = r!(r+1)!C_{2r+1}^r$ et comme $p \geq r+2$, il ne peut diviser le produit $r!(r+1)!$ formé d'entiers tous strictement inférieurs à $r+2$ (sinon il diviserait l'un d'eux), il est donc premier avec $r!(r+1)!$ et va diviser C_{2r+1}^r (théorème de Gauss). L'entier C_{2r+1}^r est donc divisible par tous les nombres premiers compris entre $r+2$ et $2r+1$, en conséquence, il est divisible par leur produit. On a donc en particulier $\prod_{r+2 \leq p \leq 2r+1} p \leq C_{2r+1}^r$. ■

Lemme 24.7 Pour tout entier $m \geq 2$, on a :

$$\prod_{2 \leq p \leq m+1} p \leq 4^m.$$

Démonstration. On procède par récurrence sur $m \geq 2$. Pour $m=2$, on a :

$$\prod_{2 \leq p \leq m+1} p = 2 \cdot 3 < 4^2.$$

Supposons le résultat acquis jusqu'au rang $m-1 \geq 2$.

Si m est impair, alors $m+1$ est pair différent de 2 et :

$$\prod_{2 \leq p \leq m+1} p = \prod_{2 \leq p \leq m} p \leq 4^{m-1} < 4^m.$$

Si m est pair, il s'écrit $m=2r$ avec $r \geq 2$ (puisque $m \geq 3$) et :

$$\begin{aligned} \prod_{2 \leq p \leq m+1} p &= \prod_{2 \leq p \leq 2r+1} p = \prod_{2 \leq p \leq r+1} p \prod_{r+2 \leq p \leq 2r+1} p \\ &\leq 4^r C_{2r+1}^r \leq 4^r 2^{2r} = 4^{2r} = 4^m. \end{aligned}$$

■

Lemme 24.8 Pour tout entier $n \geq 3$, on a :

$$C_{2n}^n \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}} \prod_{n < p \leq 2n} p$$

et :

$$2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}} \prod_{n < p \leq 2n} p. \quad (24.2)$$

Démonstration. Pour $n \geq 3$, en notant $m = \left\lfloor \frac{2n}{3} \right\rfloor$, on a $m \leq \frac{2n}{3} < m+1$ et :

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{2 \leq p \leq m+1} p \leq 4^m \leq 4^{\frac{2n}{3}}$$

ce qui donne :

$$C_{2n}^m \leq (2n)^{\sqrt{2n}} \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p C_{2n}^m \leq (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}} \prod_{n < p \leq 2n} p$$

En utilisant l'inégalité $\frac{2^{2n}}{2n} \leq C_{2n}^m$, on en déduit que :

$$2^{2n} = 4^n \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2n}{3}} \prod_{n < p \leq 2n} p$$

et :

$$4^{\frac{n}{3}} = 2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}} \prod_{n < p \leq 2n} p.$$

■

Lemme 24.9 En désignant par f et g les fonctions définies pour $x \geq 3$ par :

$$f(x) = \frac{\ln(x)}{x} \text{ et } g(x) = \frac{\ln(2)}{6} \frac{x}{1+x}.$$

il existe un entier $n_0 > 3$ tel que $f(x) < g(x)$ pour tout $x \geq n_0$.

Démonstration. Comme $\lim_{x \rightarrow +\infty} \frac{\ln(x)}{x} = 0$ et $\lim_{x \rightarrow +\infty} g(x) = \frac{\ln(2)}{6} > 0$, l'existence de x_0 tel que $f(x_0) = g(x_0)$ est assurée. En dessinant les graphes de f et g sur $[3, 35]$, on voit que x_0 est unique et localisé entre 30 et 31.

La fonction $h = g - f$ est dérivable sur $]0, +\infty[$ avec :

$$h'(x) = \frac{\ln(2)}{6} \frac{1}{(1+x)^2} + \frac{1}{x^2} (\ln(x) - 1) > 0$$

pour $x \geq 3$. Cette fonction est donc strictement croissante sur $[3, +\infty]$ et avec :

$$h(30) \simeq -1.5753 \times 10^{-3} < 0, \quad h(31) \simeq 1.1406 \times 10^{-3} > 0$$

on déduit du théorème des valeurs intermédiaires que h s'annule en un point $x_0 \in]30, 31[$ et $h(x) > 0$ pour tout $x > x_0$. La valeur $n_0 = 31$ convient. ■

Théorème 24.7 (Bertrand) Si n est un entier supérieur ou égal à 2, il existe alors des nombres premiers compris entre n et $2n$.

Démonstration. Pour $n = 2$, c'est clair.

Supposons que, pour $n \geq 3$, il n'existe pas de nombres premiers compris entre n et $2n$. A fortiori, il n'en existe pas entre $n+1$ et $2n$ et $\prod_{n < p \leq 2n} p = 1$. De l'inégalité (24.2), on déduit alors

que $2^{\frac{2n}{3}} \leq (2n)^{1+\sqrt{2n}}$, ce qui entraîne :

$$\frac{2n}{3} \ln(2) \leq (1 + \sqrt{2n}) \ln(2n)$$

ou encore :

$$\frac{2n}{6} \ln(2) \leq (1 + \sqrt{2n}) \ln(\sqrt{2n})$$

encore équivalent à :

$$g(\sqrt{2n}) = \frac{\ln(2)}{6} \frac{\sqrt{2n}}{1 + \sqrt{2n}} \leq f(\sqrt{2n}) = \frac{\ln(\sqrt{2n})}{\sqrt{2n}}$$

et nécessairement $\sqrt{2n} < n_0 = 31$, soit $2n < 31^2 = 961$ ou encore $n \leq \frac{960}{2} = 480$.

On donc ainsi montré que pour tout entier $n > 480$, il existe des nombres premiers entre n et $2n$.

Pour les entiers compris entre 2 et 480, il n'est pas nécessaire de considérer tous les cas. On peut remarquer que la suite strictement croissante de nombres premiers :

$$(p_k)_{1 \leq k \leq 11} = (2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631)$$

est telle que $p_k < p_{k+1} < 2p_k$. Il en résulte que tout intervalle $]n, 2n]$ avec $2 \leq n \leq 480$ contient l'un de ces nombres premiers. En effet, en désignant pour $n \geq 2$, par k le plus grand indice tel que $p_k \leq n$, on a $p_k \leq n < p_{k+1} < 2p_k \leq 2n$ et $p_{k+1} \in]n, 2n]$. ■

24.6 Les théorèmes de Fermat et de Wilson

Le lemme qui suit nous donne une démonstration relativement simple du « petit » théorème de Fermat.

Lemme 24.10 *Un entier naturel $p \geq 2$ est premier si, et seulement si, pour tout entier k compris entre 1 et $p-1$, p divise $C_p^k = \frac{p!}{k!(p-k)!}$.*

Démonstration. Si $p \geq 2$ est premier, comme il divise $p! = k!(p-k)!C_p^k$ et est premier avec $k!(p-k)!$ (sinon il diviserait ce produit et donc l'un des entiers j compris entre 1 et $p-1$, ce qui est impossible), il divise C_p^k (théorème de Gauss).

Réciproquement, supposons que p divise C_p^k pour tout entier k compris entre 1 et $p-1$.

Pour tout k compris entre 1 et $p-1$, on a :

$$C_{p-1}^{k-1} + C_{p-1}^k = C_p^k$$

(triangle de Pascal) et avec $C_p^k \equiv 0$ modulo p , on déduit que $C_{p-1}^k \equiv -C_{p-1}^{k-1}$ modulo p et par récurrence finie sur k compris entre 1 et $p-1$, on déduit que C_{p-1}^k est congru à $(-1)^k$ modulo p . En effet, pour $k=1$, on a $C_{p-1}^1 \equiv -C_{p-1}^0 = -1$ modulo p et en supposant le résultat acquis pour $k-1$ compris entre 1 et $p-2$, on a $C_{p-1}^k \equiv -C_{p-1}^{k-1} \equiv -(-1)^{k-1} = (-1)^k$.

Si p n'est pas premier, il admet un diviseur d compris entre 2 et $p-1$ et on a :

$$C_p^d = \frac{p}{d} C_{p-1}^{d-1} = q C_{p-1}^{d-1}$$

où q est un entier compris entre 2 et $p-1$, avec $C_p^d \equiv 0$ modulo p et $C_{p-1}^{d-1} \equiv (-1)^{d-1}$ modulo p , ce qui donne $q(-1)^{d-1} \equiv 0$ modulo p , encore équivalent à dire que p divise $q(-1)^{d-1}$ avec $2 \leq |q(-1)^{d-1}| \leq p-1$, ce qui est impossible.

Donc p est premier. ■

Théorème 24.8 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif n on a :*

$$n^p \equiv n \pmod{p}.$$

Démonstration. On démontre tout d'abord ce résultat sur les entiers naturels par récurrence sur $n \geq 0$. Pour $n = 0$ le résultat est évident. On le supposant acquis pour $n \geq 0$, on a :

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} C_p^k n^k + 1 \equiv n^p + 1 \equiv n+1 \pmod{p}.$$

Pour $n < 0$, on a $(-n)^p \equiv -n$ modulo p . Si $p = 2$ alors $-n \equiv n$ modulo 2 et $(-n)^2 = n^2$. Pour $p \geq 3$, p est impair et $(-n)^p = -n^p$ est congru à $-n$ modulo p , donc n^p est congru à n modulo p . ■

On peut aussi déduire du lemme 24.10 que si p est premier, alors pour tout couple (a, b) d'entiers relatifs, on a :

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p \equiv a^p + b^p \pmod{p}.$$

Par récurrence sur l'entier $n \geq 1$, on déduit alors que pour tout n -uplet (a_1, \dots, a_n) d'entiers relatifs, on a :

$$(a_1 + \dots + a_n)^p \equiv a_1^p + \dots + a_n^p \pmod{p}.$$

Prenant tous les a_k égaux à 1, on en déduit que n^p est congru à n modulo p . Ce résultat est encore valable pour $n = 0$ et $n < 0$.

Théorème 24.9 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif n non multiple de p , on a :*

$$n^{p-1} \equiv 1 \pmod{p}.$$

Démonstration. L'entier premier p divise $n^p - n = n(n^{p-1} - 1)$ et est premier avec n si n n'est pas un multiple de p , il divise donc $n^{p-1} - 1$. ■

Remarque 24.4 *Connaissant les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et le théorème de Lagrange pour les groupes finis, on peut donner la démonstration suivante du théorème de Fermat : pour p premier, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps, donc $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times = \frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$ est un groupe d'ordre $p-1$ et tout élément de ce groupe a un ordre qui divise $p-1$, ce qui entraîne $a^{p-1} = 1$ dans ce groupe.*

Si p est un entier pour lequel il existe un entier n compris entre 1 et $p-1$ tel que n^{p-1} ne soit pas congru à 1 modulo p , alors p n'est pas premier puisque n^{p-1} est congru à 1 modulo p pour p premier et $1 \leq n \leq p-1$ d'après le théorème de Fermat.

La réciproque du théorème de Fermat est fausse. On peut en fait montrer que pour $p \geq 2$, la condition $n^{p-1} \equiv 1 \pmod{p}$ pour tout n premier avec p est équivalente à p premier ou $p = \prod_{k=1}^r p_k$ avec $r \geq 3$, $3 \leq p_1 < \dots < p_r$ premiers tels que pour tout k compris entre 1 et r , $p_k - 1$ divise $p - 1$ (un tel entier est appelé nombre de Carmichael ou nombre pseudo-premier). Par exemple 561, 1105, 1729, sont des nombres de Carmichael.

En 1999, Alford, Granville et Pomerance ont montré qu'il y a une infinité de nombres de Carmichael.

Exercice 24.23 Calculer le reste dans la division euclidienne de 5^{2008} par 11.

Solution 24.23 Comme 11 est premier le théorème de Fermat nous dit que 5^{10} est congru à 1 modulo 11. On effectue alors la division euclidienne de 2008 par 10, soit $2008 = 200 \times 10 + 8$ et on déduit que 5^{2008} est congru à 5^8 modulo 11. Enfin avec $5^2 \equiv 3$, $5^4 \equiv 9 \equiv -2$, $5^8 \equiv 4$ modulo 11, on déduit que $5^{2008} \equiv 4$ modulo 11, ce qui signifie que 4 est le reste dans la division euclidienne de 5^{2008} par 11.

Le principe de l'exercice précédent est le suivant.

On cherche le reste dans la division euclidienne de a^b par p , où $p \geq 3$ est premier.

On effectue la division euclidienne de b par $p-1$, soit $b = q(p-1) + r$ avec $0 \leq r \leq p-2$ et on a $a^b = (a^{p-1})^q a^r$ avec $a^{p-1} \equiv 1 \pmod{p}$ si p ne divise pas a , ce qui donne $a^b \equiv a^r \pmod{p}$ (on a diminué b). Ensuite $a \equiv s \pmod{p}$ avec $1 \leq s \leq p-1$ (on a diminué a) et $a^b \equiv s^r \pmod{p}$. On se débrouille pour construire un exercice où s^r est facile à calculer.

Exercice 24.24 Soit $p \geq 7$ un nombre premier. Montrer que $p^4 - 1$ est divisible par 240.

Solution 24.24 Comme $240 = 2^4 \cdot 3 \cdot 5$, il suffit de montrer que $p^4 - 1$ est multiple de 2^4 , 3 et 5.

Comme p est premier différent de 3 et 5, le petit théorème de Fermat nous dit que $p^4 - 1$ est congru à 0 modulo 5 et p^3 congru à p , modulo 3, donc p^4 est congru à p^2 qui est lui-même congru à 1 modulo 3. L'entier $p^4 - 1$ est donc multiple de 3 et 5.

D'autre part, on a $p^4 - 1 = (p-1)(p^3 + p^2 + p + 1)$ avec p congru à 1 ou 3 modulo 4, puisque p est premier différent de 2.

Si p est congru à 1 modulo 4, alors $p-1$ est congru à 0 modulo 4, donc multiple de 4, et $p^3 + p^2 + p + 1$ est congru à 0, modulo 4, donc lui aussi multiple de 4 et $p^4 - 1$ est multiple de 16.

Si p est congru à 3 modulo 4, il s'écrit alors $p = 3 + 4q$ avec $q \geq 1$ et :

$$p^4 - 1 = 432q + 864q^2 + 768q^3 + 256q^4 + 80$$

chaque coefficient de ce polynôme étant multiple de 16, il en résulte que $p^4 - 1$ est multiple de 16. D'où le résultat annoncé.

Exercice 24.25 Soit $n \geq 2$. Montrer que $n^5 - n$ est divisible par 30.

Solution 24.25 Comme $n(n-1)$ est pair et $n(n-1)(n+1)$ est multiple de 3 (n est congru à $-1, 0$ ou 1 modulo 3) $m = n^5 - n = n(n-1)(n+1)(n^2+1)$ est divisible par 2 et 3, donc par 6. Le théorème de Fermat nous dit que $m = n^5 - n$ est divisible par 5, donc m est divisible par $30 = 6 \times 5$ puisque 6 est premier avec 5.

Lemme 24.11 Soit $p \geq 5$ un nombre premier. Pour tout entier k compris entre 1 et $p-1$, il existe un unique entier r compris entre 1 et $p-1$ tel que kr soit congru à 1 modulo p .

Démonstration. Pour $k = 1$, on peut prendre $r = 1$.

Tout entier k compris entre 2 et $p-1$ étant premier avec p , il existe deux entiers relatifs u et v tels que $ku + pv = 1$ et ku est congru à 1 modulo p (on peut aussi utiliser le théorème de Fermat : comme k est premier avec p , k^{p-1} est congru à 1 modulo p et $u = k^{p-2}$ convient). En effectuant la division euclidienne de u par p , on a $u = qp + r$ avec r compris entre 0 et $p-1$ et kr est congru à ku , donc à 1, modulo p , ce qui exclu la valeur $r = 0$.

Supposons que l'on ait trouvé un autre entier $s \neq r$ vérifiant la même condition que r . On peut supposer que $s > r$. On a alors $kr \equiv ks \equiv 1$ modulo p avec r, s compris entre 1 et $p-1$, ce qui implique que $k(s-r) \equiv 0$ modulo p , donc p divise $k(s-r)$ en étant premier avec k et en conséquence il doit diviser $s-r$ avec $1 \leq s-r \leq p-1$, ce qui est impossible. L'entier r est donc unique. ■

Dans le lemme précédent, on aura $k = r$, si, et seulement si, $k^2 - 1 = (k-1)(k+1)$ est divisible par p , donc p doit diviser $k-1$ ou $k+1$, ce qui n'est possible que si $k = 1$ ou $k = p-1$.

Théorème 24.10 (Wilson) *Un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-1)!$ est congru à -1 modulo p .*

Démonstration. Si p n'est pas premier il s'écrit $p = ab$ avec a et b entiers compris entre 2 et $p-1$. L'entier a est alors un diviseur de $(p-1)!$ et de p qui divise $(p-1)! + 1$, donc a divise $(p-1)! + 1$ et a divise 1, ce qui est impossible.

Soit $p \geq 2$ un nombre premier. Pour $p = 2$, $(p-1)! + 1 = 2$ est congru à 0 modulo 2 et pour $p = 3$, $(p-1)! + 1 = 3$ est congru à 0 modulo 3.

Pour $p \geq 5$, en utilisant le lemme précédent, on partitionne l'ensemble $E = \{2, 3, \dots, p-2\}$ en deux sous-ensembles E_1 et E_2 à $\frac{p-3}{2}$ éléments de sorte que :

$$\forall k \in E_1, \exists r \in E_2 \mid kr \equiv 1 \pmod{p}$$

et on a alors :

$$(p-1)! = 1 \cdot \left(\prod_{k \in E_1} k \right) \left(\prod_{r \in E_2} r \right) (p-1) \equiv p-1 \equiv -1 \pmod{p}$$

■

Exercice 24.26 *Montrer qu'un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo p .*

Solution 24.26 *Pour $p \geq 2$, on a $(p-1)! = (p-1)(p-2)! \equiv -(p-2)! \pmod{p}$, avec la convention $0! = 1$. Le résultat se déduit alors du théorème de Wilson.*

24.7 Les anneaux $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ et la fonction indicatrice d'Euler

Les démonstrations des propositions qui suivent sont faites au paragraphe 25.3.

Théorème 24.11 *Pour $n \geq 2$ il y a équivalence entre :*

1. n est premier ;
2. \mathbb{Z}_n est un corps ;
3. \mathbb{Z}_n est un intègre.

Ce résultat nous permet de retrouver le petit théorème de Fermat.

On peut également en déduire le théorème de Wilson.

Le résultat qui suit donne une généralisation du petit théorème de Fermat.

Définition 24.2 On dit que deux polynômes P et Q à coefficients entiers sont congrus modulo un nombre premier p s'ils sont de mêmes degré et tous leurs coefficients sont égaux modulo p (ce qui se traduit aussi par $P = Q$ dans l'anneau $\mathbb{Z}_p[X]$ des polynômes à coefficients dans le corps $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$).

Théorème 24.12 p est premier si, et seulement si, il existe un entier relatif n premier avec p tel que $(X + n)^p$ soit congru à $X^p + n$ modulo p .

Démonstration. On sait que si p est premier, alors pour tout entier k compris entre 1 et $p-1$, p divise $C_p^k = \frac{p!}{k!(p-k)!}$ (lemme 24.10), ce qui implique en utilisant la formule du binôme de Newton que, pour tout $n \in \mathbb{Z}$, $(X + n)^p$ est congru à $X^p + n^p$ modulo p et le théorème de Fermat nous dit que n^p est congru à n modulo p .

Si $(X + n)^p$ est congru à $X^p + n$ modulo p , on a alors $C_p^k n^k \equiv 0$ modulo p pour tout k compris entre 1 et $p-1$ et $n^p \equiv n$ modulo p . Comme p est premier avec n et divise $C_p^k n^k$, pour k compris entre 1 et $p-1$, il va diviser C_p^k (théorème de Gauss). On déduit alors du lemme 24.10 que p est premier. ■

Le calcul de $\varphi(n)$ pour $n \geq 2$, où φ est la fonction indicatrice d'Euler, peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Théorème 24.13 (chinois) Les entiers n et m sont premiers entre eux si, et seulement si, les anneaux \mathbb{Z}_{nm} et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.

Corollaire 24.2 Si n et m sont deux entiers naturels non nuls premiers entre eux, alors $\varphi(nm) = \varphi(n) \varphi(m)$.

Lemme 24.12 Soient p un nombre premier et α un entier naturel non nul. On a :

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}.$$

Théorème 24.14 Si $n \geq 1$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $2 \leq p_1 < \dots < p_r$ premiers et les α_i entiers naturels non nuls, alors :

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

De ce résultat on déduit que pour tout $n \geq 3$, $\varphi(n)$ est un entier pair. On déduit également que $\varphi(n)$ est compris entre 1 et n .

Exercice 24.27 Soient p et q deux nombres premiers distincts et $n = pq$. Montrer que si a et b sont deux entiers naturels tels que $ab \equiv 1 \pmod{\varphi(n)}$, alors pour tout entier relatif c , on a $c^{ab} \equiv c \pmod{n}$. Ce résultat est à la base du système cryptographique R.S.A.

Solution 24.27 Si $ab \equiv 1 \pmod{\varphi(n)}$, il existe alors un entier relatif k tel que :

$$ab = 1 + k\varphi(n) = 1 + k(p-1)(q-1).$$

Si c est un entier relatif premier avec p , on a alors $c^{p-1} \equiv 1 \pmod{p}$ (théorème de Fermat) et :

$$c^{ab} = c^{k(p-1)(q-1)} \equiv c \pmod{p}.$$

Si l'entier relatif c n'est pas premier avec p , c est nécessairement un multiple de p (qui est premier) et :

$$c^{ab} \equiv 0 \equiv c \pmod{p}.$$

De manière analogue, on a $c^{ab} \equiv c \pmod{q}$ et avec p et q premiers entre eux il en résulte que $c^{ab} \equiv c \pmod{pq}$.

Exercice 24.28 Soit p un nombre premier impair.

1. En utilisant l'application $x \mapsto x^2$ de \mathbb{Z}_p^\times dans \mathbb{Z}_p^\times , montrer qu'il y a exactement $\frac{p-1}{2}$ carrés dans \mathbb{Z}_p^\times .
2. Montrer que l'ensemble des carrés de \mathbb{Z}_p^\times est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \bar{1}$.
3. En déduire que $\overline{(-1)}$ est un carré dans \mathbb{Z}_p si, et seulement si, p est congru à 1 modulo 4.
4. En déduire qu'il existe une infinité de nombres premiers de la forme $4n+1$.

Solution 24.28

1. L'application $\varphi : x \mapsto x^2$ est un morphisme de groupes de \mathbb{Z}_p^\times dans \mathbb{Z}_p^\times de noyau $\ker(\varphi) = \{ \overline{(-1)}, \bar{1} \}$ ($x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$ et $-1 \neq 1$ dans le corps \mathbb{Z}_p pour $p \geq 3$ premier). On a donc $\text{card}(\text{Im}(\varphi)) = \text{card}\left(\mathbb{Z}_p^\times / \{ \overline{(-1)}, \bar{1} \}\right) = \frac{p-1}{2}$, ce qui signifie qu'il y a exactement $\frac{p-1}{2}$ carrés dans \mathbb{Z}_p^\times (comme $\bar{0}$ est un carré, il y a exactement $\frac{p+1}{2}$ carrés dans \mathbb{Z}_p).
2. Si $x \in \mathbb{Z}_p^\times$ est un carré, il existe $y \in \mathbb{Z}_p^\times$ tel que $x = y^2$ et $x^{\frac{p-1}{2}} = y^{p-1} = \bar{1}$. Donc les carrés de \mathbb{Z}_p^\times sont racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \bar{1}$. Comme il y a $\frac{p-1}{2}$ carrés et au plus $\frac{p-1}{2}$ racines du polynôme P dans \mathbb{Z}_p^\times , on en déduit l'ensemble $\text{Im}(\varphi)$ des carrés de \mathbb{Z}_p^\times est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \bar{1}$.
3. On a :

$$\begin{aligned} \left(\overline{(-1)} \in \text{Im}(\varphi) \right) &\Leftrightarrow \left(\overline{(-1)}^{\frac{p-1}{2}} = \bar{1} \right) \Leftrightarrow \left(\frac{p-1}{2} \equiv 0 \pmod{2} \right) \\ &\Leftrightarrow (p \equiv 1 \pmod{4}) \end{aligned}$$

4. Supposons qu'il y a un nombre fini d'entiers premiers de la forme $4n+1$. On désigne par m le plus grand de ces entiers et par $p \geq 3$ un diviseur premier de $N = (m!)^2 + 1$, on a alors $p > m$ et $\overline{(m!)^2} = \overline{(-1)}$, donc $\overline{(-1)}$ est un carré dans \mathbb{Z}_p et est premier de la forme $4n+1$, ce qui contredit $p > m$.

Les anneaux $\mathbb{Z}/n\mathbb{Z}$

25.1 Congruences dans \mathbb{Z} . Anneaux $\mathbb{Z}/n\mathbb{Z}$

On rappelle que si n est un entier naturel et a, b deux entiers relatifs, on dit que a et b sont congrus modulo n , si $b - a$ est un multiple de n , ce qui se note $a \equiv b \pmod{n}$ (voir le paragraphe 23.2).

Cette relation de congruence modulo n est une relation d'équivalence sur \mathbb{Z} et pour tout entier relatif a , on note :

$$\begin{aligned}\bar{a} &= \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{b \in \mathbb{Z} \mid n \text{ divise } b - a\} \\ &= \{b = a + qn \mid q \in \mathbb{Z}\} = a + n\mathbb{Z}\end{aligned}$$

sa classe d'équivalence modulo n .

L'ensemble de toutes ces classes d'équivalence modulo n est noté $\frac{\mathbb{Z}}{n\mathbb{Z}}$. C'est l'ensemble quotient de \mathbb{Z} par le sous-groupe $n\mathbb{Z}$. On dit aussi que c'est l'ensemble des classes résiduelles modulo n .

Pour simplifier, on note :

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{a} \mid a \in \mathbb{Z}\}.$$

Dans le cas particulier où $n = 0$, la congruence modulo 0 est tout simplement la relation d'égalité et pour tout entier relatif a , on a :

$$\bar{a} = a + 0\mathbb{Z} = \{a\}$$

de sorte que :

$$\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\}$$

est en bijection avec \mathbb{Z} . On identifie alors \mathbb{Z}_0 à \mathbb{Z} .

Dans le cas particulier où $n = 1$, deux entiers relatifs quelconques sont toujours congrus modulo 1 et pour tout entier relatif a , on a :

$$\bar{a} = a + \mathbb{Z} = \mathbb{Z}$$

de sorte que :

$$\mathbb{Z}_1 = \{\mathbb{Z}\} = \{\bar{0}\}$$

est identifié à $\{0\}$.

Théorème 25.1 *Pour tout entier naturel non nul n , on a :*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Cet ensemble est donc de cardinal égal à n et il est en bijection avec l'ensemble de tous les restes modulo n .

Démonstration. Le théorème de division euclidienne nous permet d'écrire tout entier relatif a sous la forme $a = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne que $\overline{a} = \overline{r}$. On a donc $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Pour montrer que cet ensemble est de cardinal égal à n , il nous reste à montrer que tous ses éléments sont distincts. Si $\overline{r} = \overline{s}$ avec r et s compris entre 0 et $n-1$, on a alors $s - r = qn$ avec $q \in \mathbb{Z}$ et l'encadrement $0 \leq |s - r| = |q|n \leq n-1$ dans \mathbb{N} impose $q = 0$, ce qui équivaut à $r = s$. ■

Considérant qu'un anneau a au moins deux éléments et que $\mathbb{Z}_1 = \{\overline{0}\}$, on suppose dans ce qui suit que $n \geq 2$.

La compatibilité de la relation de congruence modulo n avec l'addition et la multiplication sur \mathbb{Z} (voir le paragraphe 23.2) va nous permettre de transporter la structure d'anneau de \mathbb{Z} à \mathbb{Z}_n , un tel prolongement étant unique.

On désigne par π_n la surjection canonique de \mathbb{Z} sur \mathbb{Z}_n , c'est l'application qui associe à tout entier relatif sa classe modulo n .

Tout antécédent par π_n d'un élément x de \mathbb{Z}_n est appelé un représentant de x .

Théorème 25.2 *Il existe une unique structure d'anneau commutatif unitaire sur \mathbb{Z}_n telle que la surjection canonique π_n soit un morphisme d'anneaux.*

Démonstration. On vérifie tout d'abord qu'on définit deux opérations internes sur \mathbb{Z}_n avec :

$$\forall (x, y) \in \mathbb{Z}_n^2, \begin{cases} x + y = \overline{a + b} \\ xy = \overline{ab} \end{cases}$$

où $a \in \mathbb{Z}$ est un représentant de x et $b \in \mathbb{Z}$ un représentant de y . En effet, si a' est un autre représentant de x et b' un représentant de y , on a alors $a \equiv a'$ et $b \equiv b'$ modulo n , ce qui entraîne $a + b \equiv a' + b'$ et $ab \equiv a'b'$ modulo n , soit $\overline{a + b} = \overline{a' + b'}$ et $\overline{ab} = \overline{a'b'}$, ce qui prouve que ces définitions de $x + y$ et xy ne dépendent pas des choix des représentants de x et y .

On vérifie ensuite facilement que ces deux lois confèrent à \mathbb{Z}_n une structure d'anneau commutatif unitaire et que π_n est bien un morphisme d'anneaux.

Réciproquement s'il existe une structure d'anneau commutatif unitaire sur \mathbb{Z}_n qui fait de π_n un morphisme d'anneaux, on a alors pour tous $x = \pi_n(a)$, $y = \pi_n(b)$ dans \mathbb{Z}_n :

$$\begin{cases} x + y = \pi_n(a) + \pi_n(b) = \pi_n(a + b) = \overline{a + b} \\ xy = \pi_n(a) \pi_n(b) = \pi_n(ab) = \overline{ab} \end{cases}$$

ce qui prouve l'unicité. ■

25.2 Groupes cycliques

L'entier n est toujours supposé au moins égal à 2.

Si G est un groupe ayant un nombre fini d'éléments son cardinal est appelé l'ordre de G .

On rappelle que si G est un groupe et a un élément de G , on définit alors le sous-groupe de G engendré par a par :

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$$

dans le cas où la loi est notée multiplicativement ou :

$$\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$$

dans le cas où la loi est notée additivement.

On dit que a est d'ordre fini dans G si ce groupe $\langle a \rangle$ est fini et l'ordre de a est alors l'ordre de $\langle a \rangle$ (voir le paragraphe ??).

Définition 25.1 On dit qu'un groupe G est monogène s'il est engendré par l'un de ses éléments, c'est-à-dire s'il existe a dans G tel que $G = \langle a \rangle$. Un groupe monogène fini est dit cyclique.

Remarque 25.1 Un groupe cyclique est nécessairement commutatif.

Remarque 25.2 Un groupe cyclique engendré par un élément $a \neq 1$ (le neutre de G) a au moins deux éléments, 1 et a .

Exemple 25.1 Tout élément x de \mathbb{Z}_n s'écrivant :

$$x = \bar{k} = \underbrace{\bar{1} + \cdots + \bar{1}}_{k \text{ fois}} = k\bar{1}$$

avec $\bar{k} = \bar{0}$ si, et seulement si, k est multiple de n . Il en résulte que $(\mathbb{Z}_n, +)$ est un groupe cyclique d'ordre (ou de cardinal) n . En fait, à isomorphisme près, c'est le seul.

Exemple 25.2 Le groupe :

$$\left\langle e^{\frac{2i\pi}{n}} \right\rangle = \left\{ e^{\frac{2ik\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$$

des racines n -ièmes de l'unité est cyclique d'ordre n .

Exemple 25.3 Si θ est un réel tel que $\frac{\theta}{2\pi}$ n'est pas rationnel, alors le groupe :

$$\langle e^{i\theta} \rangle = \{e^{ik\theta} \mid k \in \mathbb{Z}\}$$

est monogène infini puisque $e^{ik\theta} \neq 1$ pour tout $k \in \mathbb{Z}$.

Théorème 25.3 Tout groupe cyclique d'ordre n est isomorphe à \mathbb{Z}_n .

Démonstration. Soit $G = \langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$ un groupe cyclique d'ordre n . L'application $\varphi_a : k \mapsto a^k$ réalise un morphisme surjectif de groupes de $(\mathbb{Z}, +)$ sur (G, \cdot) de noyau $\ker(\varphi_a) = n\mathbb{Z}$ (par définition de l'ordre de a).

Si j, k sont deux entiers relatifs tels que $j \equiv k \pmod{n}$ on a alors $k - j = qn$ et $a^k = a^j a^{qn} = a^j$. On peut donc définir l'application $\overline{\varphi}_a$ de \mathbb{Z}_n dans G par $\overline{\varphi}_a : \bar{k} \mapsto a^k$.

On vérifie facilement que $\overline{\varphi}_a$ est un morphisme de groupes surjectif de $(\mathbb{Z}_n, +)$ sur (G, \cdot) de noyau $\ker(\overline{\varphi}_a) = \{\bar{0}\}$. Cette application réalise donc un isomorphisme de groupes de $(\mathbb{Z}_n, +)$ sur (G, \cdot) . ■

Dans le cas où n est premier, on a le résultat plus précis suivant qui est une conséquence du théorème de Lagrange (théorème 20.12).

Théorème 25.4 Soit p un nombre premier. Tout groupe G d'ordre p est cyclique, donc isomorphe à \mathbb{Z}_p .

Démonstration. Tout élément de $G \setminus \{1\}$ est d'ordre p (puisque son ordre divise p et est différent de 1), il en résulte que G est cyclique d'ordre p , donc isomorphe à \mathbb{Z}_p . ■

Le résultat qui suit nous dit que les sous groupes d'un groupe cyclique sont cycliques.

Théorème 25.5 *Tous les sous groupes de \mathbb{Z}_n sont cycliques d'ordre qui divise n . Réciproquement pour tout diviseur d de n , il existe un unique sous groupe de G d'ordre d , c'est le groupe cyclique engendré par $q = \frac{n}{d}$:*

$$H = \langle \bar{q} \rangle = \{ \bar{0}, \bar{q}, \dots, (d-1)\bar{q} \}.$$

Démonstration. Soit H un sous-groupe de \mathbb{Z}_n . Le théorème de Lagrange nous dit que son ordre d est un diviseur de n . On note $q = \frac{n}{d}$.

Pour tout \bar{a} dans H , on a $d\bar{a} = \bar{0}$, soit $da = kn$, ou encore $a = kq$, c'est-à-dire que $\bar{a} = k\bar{q}$ est dans le sous-groupe $\langle \bar{q} \rangle$ de \mathbb{Z}_n engendré par \bar{q} . On a donc $H \subset \langle \bar{q} \rangle$, ce qui entraîne $\text{card}(\langle \bar{q} \rangle) \geq d$. Mais $d\bar{q} = \bar{n} = \bar{0}$ nous dit que \bar{q} est d'ordre au plus égal à d . En définitive, $\langle \bar{q} \rangle$ est d'ordre d , donc égal à H . Un sous-groupe d'ordre d de \mathbb{Z}_n , s'il existe, est donc unique.

Réciproquement, soit d un diviseur de n , $q = \frac{n}{d}$ et $H = \langle \bar{q} \rangle$ le sous groupe de \mathbb{Z}_n engendré par \bar{q} . Si δ est l'ordre de H , on a $\delta\bar{q} = \bar{0}$, soit $\delta q = kn = kqd$ et $\delta = kd \geq d$. Mais on a aussi $d\bar{q} = \bar{0}$, ce qui entraîne $\delta \leq d$ et donc $\delta = d$.

Il existe donc un unique sous-groupe d'ordre d de \mathbb{Z}_n , c'est $\langle \bar{q} \rangle$. ■

25.3 Fonction indicatrice d'Euler

Définition 25.2 *On dit qu'un élément \bar{a} de \mathbb{Z}_n est inversible s'il existe \bar{b} dans \mathbb{Z}_n tel que $\bar{a}\bar{b} = \bar{1}$.*

On note \mathbb{Z}_n^* l'ensemble des éléments inversibles de \mathbb{Z}_n . C'est un groupe pour la loi multiplicative.

Théorème 25.6 *Soit a un entier relatif. Les propriétés suivantes sont équivalentes :*

1. \bar{a} est inversible dans \mathbb{Z}_n ;
2. a est premier avec n ;
3. \bar{a} est un générateur de $(\mathbb{Z}_n, +)$.

Démonstration. Dire que \bar{a} est inversible dans \mathbb{Z}_n équivaut à dire qu'il existe \bar{b} dans \mathbb{Z}_n tel que $\bar{a}\bar{b} = \bar{1}$, encore équivalent à dire qu'il existe b, q dans \mathbb{Z} tels que $ab + qn = 1$, ce qui équivaut à dire que a et n sont premiers entre eux (théorème de Bézout).

En traduisant le fait que \bar{a} est inversible dans \mathbb{Z}_n par l'existence d'un entier relatif b tel que $\bar{a}\bar{b} = \bar{b}\bar{a} = \bar{1}$, on déduit que cela équivaut à dire que $\bar{1}$ est dans le groupe engendré par \bar{a} et donc que ce groupe est \mathbb{Z}_n . ■

Définition 25.3 *On appelle fonction indicatrice d'Euler la fonction qui associe à tout entier naturel non nul n , le nombre, noté $\varphi(n)$, d'entiers compris entre 1 et n qui sont premiers avec n .*

Le théorème précédent nous dit que pour tout entier $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$ (ou de n'importe quel groupe cyclique d'ordre n) ou encore que c'est le nombre d'éléments inversibles de \mathbb{Z}_n .

Du théorème de Lagrange, on déduit immédiatement le résultat suivant.

Théorème 25.7 (Euler) *Pour tout entier relatif a premier avec n , on a $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Démonstration. Si a est premier avec n , alors \bar{a} appartient à \mathbb{Z}_n^* qui est un groupe d'ordre $\varphi(n)$ et en conséquence son ordre divise $\varphi(n)$ (théorème de Lagrange), ce qui entraîne $\bar{a}^{\varphi(n)} = \bar{1}$, ou encore $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Si n est premier, alors tout entier compris entre 1 et $n-1$ est premier avec n , ce qui implique que $\varphi(n) = n-1$ et le théorème d'Euler devient le petit théorème de Fermat.

Théorème 25.8 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif a on a :*

$$a^p \equiv a \pmod{p}.$$

Démonstration. Le théorème d'Euler nous dit que $a^{p-1} \equiv 1 \pmod{p}$ si a est premier avec p , c'est-à-dire si a n'est pas multiple de p , ce qui entraîne $a^p \equiv a \pmod{p}$. Pour a multiple de p , on a $a^p \equiv a \equiv 0 \pmod{p}$. ■

La réciproque de ce théorème est fautive comme nous le montrera l'étude des nombres de Carmichael au paragraphe ?? . Par exemple on a $a^{561} \equiv a \pmod{561}$ pour tout entier relatif a avec $561 = 3 \cdot 11 \cdot 17$ non premier.

Le théorème de Fermat peut être utilisé pour calculer des congruences avec des grands nombres. Si p est un nombre premier impair, n, m deux entiers naturels, l'entier n n'étant pas multiple de p , en effectuant les divisions euclidiennes par p et par $p-1$, on $n = qp + r$, $m = q'(p-1) + s$ avec $1 \leq r \leq p-1$, $0 \leq s \leq p-2$ et :

$$n^m \equiv r^s \pmod{p}$$

Par exemple on a $2003^{2003} \equiv 4 \pmod{5}$. En effet $2003 = 5 \cdot 400 + 3$ et $2003 = 4 \cdot 500 + 3$.

Dans le cas où n est premier tous les éléments de $\mathbb{Z}_n \setminus \{\bar{0}\}$ sont inversibles et en conséquence \mathbb{Z}_n est un corps. En fait on a le résultat plus précis suivant.

Théorème 25.9 *Pour $n \geq 2$ il y a équivalence entre :*

1. n est premier ;
2. \mathbb{Z}_n est un corps ;
3. \mathbb{Z}_n est un intègre.

Démonstration. On vient de voir que pour n premier \mathbb{Z}_n est un corps.

De manière générale, tout corps est intègre.

Supposons \mathbb{Z}_n intègre et soit d un diviseur de n différent de n dans \mathbb{N} . Il existe donc un entier q compris entre 2 et n tel que $n = qd$ et dans \mathbb{Z}_n on a $\bar{q}\bar{d} = \bar{0}$ avec $\bar{d} \neq \bar{0}$, ce qui impose $\bar{q} = \bar{0}$, donc $q = n$ et $d = 1$. L'entier n est donc premier. ■

Remarque 25.3 *L'implication (3) \Rightarrow (2) est aussi conséquence du fait que tout anneau unitaire fini et intègre est un corps (théorème de Wedderburn). Si A est un anneau fini intègre, alors pour tout $a \in A \setminus \{0\}$ l'application $x \mapsto ax$ est injective de A dans A , donc bijective, ce qui entraîne l'existence de $a' \in A$ tel que $aa' = e$ (e est le neutre pour la multiplication).*

Ce résultat nous permet de retrouver le petit théorème de Fermat.

On peut également en déduire le théorème de Wilson.

Théorème 25.10 (Wilson) *Un entier n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.*

Démonstration. Si n est premier alors \mathbb{Z}_n est un corps commutatif et tout élément \bar{k} de \mathbb{Z}_n^* est racine du polynôme $X^{n-1} - \bar{1}$, on a donc $X^{n-1} - \bar{1} = \prod_{k=1}^{n-1} (X - \bar{k})$ dans $\mathbb{Z}_n[X]$ et en évaluant ce polynôme en $\bar{0}$, il vient $-\bar{1} = \prod_{k=1}^{n-1} (-\bar{k}) = (-1)^{n-1} \overline{(n-1)!}$. Pour $n = 2$, on a $-\bar{1} = \bar{1}$ et pour $n \geq 2$ premier on a n impair et $-\bar{1} = \overline{(n-1)!}$ dans \mathbb{Z}_n .

Réciproquement si $n \geq 2$ est tel que $\overline{(n-1)!} = -\bar{1}$ dans \mathbb{Z}_n , alors tout diviseur d de n compris entre 1 et $n-1$ divisant $(n-1)! = -1 + kn$ va diviser -1 , ce qui donne $d = 1$ et l'entier n est premier. ■

Le calcul de $\varphi(n)$ pour $n \geq 2$ peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Théorème 25.11 (chinois) *Les entiers n et m sont premiers entre eux si, et seulement si, les anneaux \mathbb{Z}_{nm} et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.*

Démonstration. Pour tout entier relatif k , on note \bar{k} sa classe modulo nm , \dot{k} sa classe modulo n et \ddot{k} sa classe modulo m .

Le produit cartésien $\mathbb{Z}_n \times \mathbb{Z}_m$ est naturellement muni d'une structure d'anneau commutatif unitaire avec les lois $+$ et \cdot définies par :

$$\begin{cases} \left(\dot{j}, \ddot{k} \right) + \left(\dot{j}', \ddot{k}' \right) = \left(\dot{j} + \dot{j}', \ddot{k} + \ddot{k}' \right) \\ \left(\dot{j}, \ddot{k} \right) \cdot \left(\dot{j}', \ddot{k}' \right) = \left(\dot{j} \cdot \dot{j}', \ddot{k} \cdot \ddot{k}' \right) \end{cases}$$

Supposons n et m premiers entre eux. L'application $\varphi : k \mapsto \left(\dot{k}, \ddot{k} \right)$ est un morphisme d'anneaux de \mathbb{Z} dans $\mathbb{Z}_n \times \mathbb{Z}_m$ et son noyau est formé des entiers divisibles par n et m donc par nm puisque ces entiers sont premiers entre eux, il se factorise donc en un morphisme injectif d'anneaux de \mathbb{Z}_{nm} dans $\mathbb{Z}_n \times \mathbb{Z}_m$ par $\bar{\varphi} : \bar{k} \mapsto \left(\dot{k}, \ddot{k} \right)$. Ces deux anneaux ayant même cardinal, l'application $\bar{\varphi}$ réalise en fait un isomorphisme d'anneaux de \mathbb{Z}_{nm} dans $\mathbb{Z}_n \times \mathbb{Z}_m$.

Si n et m ne sont pas premiers entre eux les groupes additifs \mathbb{Z}_{nm} et $\mathbb{Z}_n \times \mathbb{Z}_m$ ne peuvent être isomorphes puisque $\bar{1}$ est d'ordre nm dans \mathbb{Z}_{nm} et tous les éléments de $\mathbb{Z}_n \times \mathbb{Z}_m$ ont un ordre qui divise le ppcm de n et m qui est strictement inférieur à nm . ■

Corollaire 25.1 *Si n et m sont deux entiers naturels non nuls premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$.*

Démonstration. On utilise les notations de la démonstration précédente.

La restriction de l'isomorphisme $\bar{\varphi}$ à \mathbb{Z}_{nm}^* réalise un isomorphisme de groupes multiplicatifs de \mathbb{Z}_{nm}^* sur $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$, ce qui entraîne :

$$\varphi(nm) = \text{card}(\mathbb{Z}_{nm}^*) = \text{card}(\mathbb{Z}_n^*) \text{card}(\mathbb{Z}_m^*) = \varphi(n)\varphi(m).$$

■

Le calcul de $\varphi(n)$ est alors ramené à celui de $\varphi(p^\alpha)$ où p est un nombre premier et α un entier naturel non nul.

Lemme 25.1 *Soient p un nombre premier et α un entier naturel non nul. On a :*

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}.$$

Démonstration. Si p est premier, alors un entier k compris entre 1 et p^α n'est pas premier avec p^α si et seulement si il est divisible par p , ce qui équivaut à $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, il y a donc $p^{\alpha-1}$ possibilités. On en déduit alors que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}.$$

■

Théorème 25.12 Si $n \geq 1$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $2 \leq p_1 < \dots < p_r$ premiers et les α_i entiers naturels non nuls, alors :

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i-1} (p_i - 1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Démonstration. En utilisant les résultats précédents, on a :

$$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r \varphi(p^{\alpha_i}) = \prod_{i=1}^r (p_i - 1) p_i^{\alpha_i-1} = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

■

De ce résultat on déduit que pour tout $n \geq 3$, $\varphi(n)$ est un entier pair. En effet, pour $n = 2^\alpha$ avec $\alpha \geq 2$, on a $\varphi(n) = 2^{\alpha-1}$ qui est pair et pour $n = 2^\alpha \prod_{i=1}^r p_i^{\alpha_i} = p_1^{\alpha_1} m$ avec $\alpha \geq 0$, $r \geq 1$, tous les p_i étant premiers impairs, on a $\varphi(n) = (p_1 - 1) p_1^{\alpha_1-1} \varphi(m)$ qui est pair.

On déduit également que $\varphi(n)$ est compris entre 1 et n (ce qui se voit aussi avec la définition). En fait on a le résultat plus précis suivant.

Théorème 25.13 Pour tout entier $n \geq 2$, on a :

$$\forall n \geq 2, \sqrt{n} - 1 < \varphi(n) < n.$$

Démonstration. L'inégalité $\varphi(n) < n$ est une conséquence immédiate de la définition.

Pour montrer l'autre inégalité on procède en plusieurs étapes.

On s'intéresse d'abord aux valeurs n comprises entre 2 et 7. Pour ces valeurs, on a $\varphi(2) = 1 > \sqrt{2} - 1$, $\varphi(5) = 4 > \sqrt{5} - 1$ et $\varphi(3) = \varphi(4) = \varphi(6) = 2 > \sqrt{k} - 1$ pour $k = 3, 4, 6$.

On s'intéresse ensuite aux entiers de la forme $n = \prod_{i=1}^r p_i$ avec $3 \leq p_1 < \dots < p_r$ premiers.

Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \prod_{i=1}^r \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $p(p-3) \geq 0$, soit $p^2 - 3p + 1 > 0$ ou encore $(p-1)^2 p$, c'est-à-dire $p-1 > \sqrt{p}$. On en déduit donc que $\varphi(n) > \sqrt{n}$.

Considérons le cas de n impair supérieur ou égal à 7. Il s'écrit $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $3 \leq p_1 < \dots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r . En posant $m = \prod_{i=1}^r p_i$, on a :

$$\varphi(n) = \frac{n}{m} \prod_{i=1}^r \varphi(p_i) = \frac{n}{m} \varphi(m)$$

et :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}} > 1,$$

ce qui donne $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha$ avec $\alpha \geq 3$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}-1} = \left(\sqrt{2}\right)^{\alpha-2} > 1$$

et $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha 3^\beta$ avec $\alpha \geq 1$, $\beta \geq 1$ et $(\alpha, \beta) \neq (1, 1)$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}} 3^{\frac{\beta}{2}-1} = \left(\sqrt{2}\right)^\alpha \left(\sqrt{3}\right)^{\beta-2} > 1$$

(pour $\beta \geq 2$ il n'y a pas de problème et pour $\beta = 1$ on a $\alpha \geq 2$ et $(\sqrt{2})^\alpha (\sqrt{3})^{-1} \geq \frac{2}{\sqrt{3}} > 1$),
ce qui donne $\varphi(n) > \sqrt{n}$.

Enfin, si n est pair supérieur ou égal à 7, il s'écrit $n = 2^{\alpha_1} \prod_{i=2}^r p_i^{\alpha_i}$ avec $3 \leq p_2 < \dots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r . En posant $m = 2 \prod_{i=2}^r p_i$, on a ::

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}},$$

avec :

$$\frac{\varphi(m)}{\sqrt{m}} = \frac{1}{\sqrt{2}} \prod_{i=2}^r \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $\frac{p-1}{\sqrt{p}} > 1$, donc $\frac{\varphi(m)}{\sqrt{m}} > \frac{p_2-1}{\sqrt{2}\sqrt{p_2}}$ et pour $p_2 \geq 5$, on a $\frac{p_2-1}{\sqrt{2}\sqrt{p_2}} > 1$. Il reste à étudier le cas $p_2 = 3$, soit $n = 2^{\alpha_1} 3^{\alpha_2} r$, avec $r = \prod_{i=3}^r p_i^{\alpha_i}$ où $5 \leq p_3 < \dots < p_r$ sont premiers.

Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \frac{\varphi(2^{\alpha_1} 3^{\alpha_2})}{\sqrt{2^{\alpha_1} 3^{\alpha_2}}} \frac{\varphi(r)}{\sqrt{r}} > 1$$

d'après ce qui précède.

On a donc ainsi montré que $\varphi(n) > \sqrt{n}$ pour tout $n \geq 7$. ■

Utilisation des congruences et des anneaux $\mathbb{Z}/n\mathbb{Z}$

26.1 Équations diophantiennes $ax \equiv b \pmod{n}$

Soient n un entier supérieur ou égal à 2, a un entier supérieur ou égal à 1 et b un entier relatif. On veut résoudre dans \mathbb{Z} l'équation diophantienne :

$$ax \equiv b \pmod{n} \quad (26.1)$$

Dans le cas où $b = 1$, cette équation a des solutions si, et seulement si \bar{a} est inversible dans \mathbb{Z}_n , ce qui équivaut à dire que a est premier avec n . Dans ce cas l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$ de (26.1). Si $x \in \mathbb{Z}$ est une autre solution, alors $a(x - x_0)$ est divisible par n qui est premier avec a et le théorème de Gauss nous dit que n doit diviser $x - x_0$. Réciproquement on vérifie facilement que pour tout $k \in \mathbb{Z}$, $x_0 + kn$ est solution de (26.1). En définitive, dans le cas où a et n sont premiers entre eux, l'ensemble des solutions de $ax \equiv 1 \pmod{n}$ est :

$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Dans le cas où les entiers a et n sont premiers entre eux et b est un entier relatif quelconque, pour toute solution particulière u_0 de l'équation $ax \equiv 1 \pmod{n}$ l'entier $x_0 = bu_0$ est solution de (26.1). Comme précédemment, on en déduit que l'ensemble des solutions de (26.1) est :

$$S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Considérons maintenant le cas général.

On note δ le pgcd de a et n et on a $a = \delta a'$, $n = \delta n'$ avec a' et n' premiers entre eux.

Théorème 26.1 *L'équation diophantienne (26.1) a des solutions entières si, et seulement si, δ divise b . Dans ce cas, l'ensemble des solutions de cette équation est :*

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 est une solution particulière de $a'x \equiv 1 \pmod{n'}$

Démonstration. Si l'équation (26.1) admet une solution $x \in \mathbb{Z}$ alors $\delta n'$ divise $\delta a' - b$ et δ divise b .

Si b est un multiple de δ , il s'écrit $b = \delta b'$ et toute solution de $a'x \equiv b' \pmod{n'}$ est aussi solution de (26.1).

On a vu que les solutions de $a'x \equiv b' \pmod{n'}$ sont de la forme $x = b'x'_0 + kn'$ où x'_0 est une solution de $a'x \equiv 1 \pmod{n'}$ et k est un entier relatif. Réciproquement on vérifie facilement que pour tout entier $k \in \mathbb{Z}$, $x = b'x'_0 + kn'$ est solution de (26.1). ■

26.2 Équations diophantiennes $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$

On s'intéresse ici aux système d'équations diophantiennes :

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad (26.2)$$

où n, m sont deux entiers naturels supérieur ou égal à 2.

Théorème 26.2 (chinois) *Soient n, m deux entier supérieur ou égal à 2 premiers entre eux. Quels que soient les entiers relatifs a et b le système (26.2) a une infinité de solutions dans \mathbb{Z} .*

Démonstration. Comme n et m sont premiers entre eux on peut trouver une infinité de couples d'entiers relatifs (u, v) tels que :

$$nu + mv = 1.$$

En posant $x = bnu + amv$ on obtient une infinité de solutions de (26.2). ■

Ce théorème peut aussi s'exprimer en disant que le morphisme d'anneaux introduit dans la démonstration du théorème 25.11, $\varphi : k \mapsto \begin{pmatrix} \cdot & \cdot \\ k & k \end{pmatrix}$, est surjectif de \mathbb{Z} dans $\mathbb{Z}_n \times \mathbb{Z}_m$. Son noyau étant $nm\mathbb{Z}$, on retrouve l'isomorphisme de \mathbb{Z}_{nm} sur $\mathbb{Z}_n \times \mathbb{Z}_m$.

Dans le cas où n et m sont premiers entre eux on vient de voir que si (u_0, v_0) est solution de $nu + mv = 1$ (un tel couple peut être obtenu par l'algorithme d'Euclide) alors $x_0 = bnu_0 + amv_0$ est une solution particulière de (26.2). À partir d'une telle solution on déduit toutes les autres. En effet, si $x \in \mathbb{Z}$ est solution de (26.2) alors x est congru à x_0 modulo n et modulo m , soit :

$$x - x_0 = pn = qm.$$

Mais m est premier avec n , le théorème de Gauss nous dit alors que m divise p . On a donc $x = x_0 + knm$ avec $k \in \mathbb{Z}$. Et réciproquement on vérifie que pour tout entier relatif k , $x_0 + knm$ est solution de (26.2). En définitive, si n et m sont premiers entre eux, alors l'ensemble des solutions de (26.2) est :

$$S = \{x_0 + knm \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de (26.2).

Dans le cas général où m et n ne sont pas nécessairement premiers entre eux on note δ le pgcd de n et m , $n = \delta n'$, $m = \delta m'$ avec n', m' premiers entre eux et on note μ le ppcm de n et m .

Théorème 26.3 *L'équation diophantienne (26.2) a des solutions entières si, et seulement si, $a - b$ est multiple de δ . Dans ce cas, l'ensemble des solutions de (26.2) est :*

$$S = \{x_0 + k\mu \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Démonstration. Si $x \in \mathbb{Z}$ est une solution de (26.2) alors δ qui divise n et m va diviser $x - a$ et $x - b$, il divise donc $a - b$.

Réciproquement, supposons que $a - b$ est multiple de δ , c'est à dire que $b - a = \delta c'$. Les entiers n' et m' étant premiers entre eux, le théorème de Bézout nous dit qu'il existe des entiers u_0 et v_0 tels que $n'u_0 + m'v_0 = 1$. En posant :

$$x_0 = bn'u_0 + am'v_0,$$

on a :

$$\begin{aligned} x_0 &= b(1 - m'v_0) + am'v_0 = b - m'v_0(b - a) \\ &= b - m'v_0\delta c' = b - mv_0c' \equiv b \pmod{m}. \end{aligned}$$

De manière analogue on voit que x_0 est congru à a modulo n . L'entier x_0 est donc une solution de (26.2).

Si $x \in \mathbb{Z}$ est solution de (26.2) alors x est congru à x_0 modulo n et modulo m , soit :

$$x - x_0 = pn = qm = p\delta n' = q\delta m'.$$

Il en résulte que $\frac{x - x_0}{\delta}$ est un entier et :

$$\frac{x - x_0}{\delta} = pn' = qm'.$$

Comme m' est premier avec n' , le théorème de Gauss nous dit que m' doit diviser p . On a donc :

$$\frac{x - x_0}{\delta} = kn'm'$$

avec $k \in \mathbb{Z}$. Ce qui peut aussi s'écrire :

$$x - x_0 = knm' = k \frac{nm}{\delta} = k\mu$$

avec $k \in \mathbb{Z}$.

Réciproquement on vérifie facilement que pour tout entier relatif k , $x_0 + k\mu$ est solution de (26.2). En définitive, l'ensemble des solutions de (26.2) est :

$$S = \{x_0 + k\mu \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation. ■

26.3 Critères de divisibilité

Les anneaux $\mathbb{Z}/n\mathbb{Z}$ peuvent être utilisés pour obtenir des critères de divisibilité des entiers par 2, 3, 5, 9 et 11.

Soit a un entier naturel non nul d'écriture décimale $a = \overline{a_p \cdots a_1 a_0}^{10}$, où les a_k sont des entiers compris entre 0 et 9, le coefficient a_p étant non nul.

- Comme 10 est congru à 0 modulo 2 (resp. modulo 5) on déduit que a est congru à a_0 modulo 2 (resp. modulo 5) et donc a est divisible par 2 (resp. par 5) si et seulement si son chiffre des unités a_0 est pair, c'est-à-dire égal à 0, 2, 4, 6 ou 8 (resp. multiple de 5, c'est-à-dire égal à 0 ou 5).

- Du fait que 10 est congru à 1 modulo 3 (resp. modulo 9) on déduit que 10^k est congru à 1 modulo 3 (resp. modulo 9) pour tout entier k et a est congru à $\sum_{k=0}^p a_k$ modulo 3 (resp. modulo 9). Donc a est divisible par 3 (resp. par 9) si et seulement si la somme de ses chiffres est divisible par 3 (resp. par 9).
- Enfin du fait que 10 est congru à -1 modulo 11 on déduit que 10^k est congru à $(-1)^k$ modulo 11 pour tout entier k et a est congru à $\sum_{k=0}^p (-1)^k a_k$ modulo 11. Donc a est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

En remplaçant 10 par une base $b \geq 2$, on a de manière plus générale les résultats suivants, où on a noté $a = \overline{a_p \cdots a_1 a_0}^b$ l'écriture en base b d'un entier a (les a_k sont compris entre 0 et $b-1$ et a_p est non nul) :

- si d est un diviseur de b alors a est divisible par d si, et seulement si a_0 est divisible par d ;
- si d est un diviseur de $b-1$ alors a est divisible par d si, et seulement si $\sum_{k=0}^p a_k$ est divisible par d ;
- a est divisible par $b+1$ si, et seulement si $\sum_{k=0}^p (-1)^k a_k$ est divisible par $b+1$.

Cinquième partie
Problèmes d'algèbre

Les anneaux considérés sont toujours supposés unitaires.

Le théorème de d'Alembert-Gauss

27.1 Énoncé

Le but de cet problème est de montrer le théorème fondamental de l'algèbre : tout polynôme complexe non constant a au moins une racine.

On se donne un polynôme $P(z) = \sum_{k=0}^n a_k z^k$ de degré $n \geq 1$ avec $a_n = 1$.

1. Montrer que $\lim_{|z| \rightarrow +\infty} |P(z)| = +\infty$.

2. Montrer qu'il existe $z_0 \in \mathbb{C}$ tel que $|P(z_0)| = \inf_{z \in \mathbb{C}} |P(z)|$.

3. On suppose que $P(z_0) \neq 0$ et on définit le polynôme Q par $Q(z) = \frac{P(z+z_0)}{P(z_0)}$.

(a) Montrer que :

$$\forall z \in \mathbb{C}, |Q(z)| \geq 1.$$

(b) Montrer qu'il existe un entier p compris entre 1 et n et une fonction ε définie sur \mathbb{C} tels que $b_p \neq 0$, $\lim_{z \rightarrow 0} \varepsilon(z) = 0$ et $Q(z) = 1 + b_p z^p (1 + \varepsilon(z))$.

(c) Justifier l'existence d'un réel $r > 0$ tel que $|\varepsilon(z)| < \frac{1}{2}$ pour tout $z \in \mathbb{C}$ tel que $|z| < r$.

(d) On note $b_p = r_p e^{i\theta_p}$ avec $r_p > 0$ et $0 \leq \theta_p < 2\pi$.

i. Montrer que pour tout $z = \rho e^{-i\frac{\theta_p + \pi}{p}}$ avec $0 < \rho < r$, on a :

$$|Q(z)| \leq |1 - r_p \rho^p| + \frac{1}{2} r_p \rho^p.$$

ii. En déduire qu'il existe $z_1 \in \mathbb{C}$ tel que $|Q(z_1)| < 1$.

iii. Conclure.

27.2 Solution

1. Pour tout $z \in \mathbb{C}^*$, on a :

$$|P(z)| = |z|^n \left| \frac{a_0}{z^n} + \dots + \frac{a_{n-1}}{z} + 1 \right|$$

avec $\lim_{|z| \rightarrow +\infty} \left| \frac{a_{n-k}}{z^k} \right| = 0$ pour $k = 1, \dots, n$. D'où le résultat.

2. De $\lim_{|z| \rightarrow +\infty} |P(z)| = +\infty$, on déduit qu'il existe $R > 0$ tel que :

$$|z| > R \Rightarrow |P(z)| > |P(0)|$$

Sur le compact $K = \{|z| \leq R\}$, la fonction continue $|P|$ est minorée et atteint sa borne inférieure, il existe donc $z_0 \in K$ tel que $|P(z_0)| = \inf_{z \in K} |P(z)|$. On a alors, pour tout $z \in \mathbb{C}$, soit $z \in K$ et $|P(z)| \geq |P(z_0)|$, soit $z \notin K$, donc $|z| > R$ et $|P(z)| > |P(0)| \geq |P(z_0)|$. Dans tous les cas, $|P(z)| \geq |P(z_0)|$ et $|P(z_0)| = \inf_{z \in \mathbb{C}} |P(z)|$.

3.

- (a) Résulte de :

$$\forall z \in \mathbb{C}, |P(z + z_0)| \geq |P(z_0)|.$$

- (b) On a $Q \in \mathbb{C}[z]$ avec $Q(0) = 1$ et $\deg(Q) = n$, donc :

$$Q(z) = 1 + b_p z^p + \dots + b_n z^n$$

avec $1 \leq p \leq n$ et $b_p \neq 0$, ce qui s'écrit :

$$Q(z) = 1 + b_p z^p (1 + \varepsilon(z))$$

avec $\lim_{z \rightarrow 0} \varepsilon(z) = 0$.

- (c) Par définition de la limite nulle.

(d)

- i. Pour $z = \rho e^{-i\frac{\theta_p + \pi}{p}}$, on a :

$$\begin{aligned} |Q(z)| &= |1 + b_p z^p (1 + \varepsilon(z))| \\ &\leq |1 + b_p z^p| + r_p \rho^p |\varepsilon(z)| \end{aligned}$$

Si de plus $\rho = |z| < r$, alors $|\varepsilon(z)| < \frac{1}{2}$ et :

$$|Q(z)| \leq |1 + b_p z^p| + r_p \rho^p \frac{1}{2}$$

avec :

$$b_p z^p = r_p e^{i\theta_p} \left(\rho e^{-i\frac{\theta_p + \pi}{p}} \right)^p = r_p \rho^p e^{-i\pi} = -r_p \rho^p.$$

- ii. On a $\lim_{\rho \rightarrow 0} (1 - r_p \rho^p) = 1$, donc $1 - r_p \rho^p > 0$ pour ρ assez petit et pour un tel choix :

$$|Q(z)| \leq 1 - r_p \rho^p + \frac{1}{2} r_p \rho^p = 1 - \frac{1}{2} r_p \rho^p < 1.$$

- iii. C'est contradictoire avec $|Q(z)| \geq 1$. Donc $P(z_0) = 0$ et le théorème de d'Alembert-Gauss est démontré.

La forme quadratique $Tr(M^2)$ sur $\mathcal{M}_n(\mathbb{R})$

28.1 Énoncé

Exercice 28.1 Soient $E = \mathcal{M}_n(\mathbb{R})$ l'espace vectoriel des matrices carrées à coefficients réels d'ordre $n \geq 2$ et q l'application définie sur E par :

$$\forall M \in E, q(M) = Tr(M^2).$$

1. En notant $M = ((x_{ij}))_{1 \leq i, j \leq n}$ un élément de E , donner une expression de q .
2. Montrer que q est une forme quadratique sur E .
3. Donner une expression la forme polaire φ de q .
4. Effectuer une réduction de q en combinaison linéaire de carrés de formes linéaires indépendantes dans le dual E^* .
5. Déterminer le rang, le noyau et la signature de q .
6. Soient $E_1 = \{M \in E \mid {}^tM = M\}$ le sous-espace vectoriel de E formé des matrices symétriques et $E_2 = \{M \in E \mid {}^tM = -M\}$ le sous-espace vectoriel de E formé des matrices antisymétriques.
 - (a) Donner la dimension de E_1 en précisant une base.
 - (b) Que dire des termes diagonaux d'une matrice $M = ((x_{ij}))_{1 \leq i, j \leq n} \in E_2$?
 - (c) Donner la dimension de E_2 en précisant une base.
 - (d) Montrer que $E = E_1 \oplus E_2$.
 - (e) Montrer que $E_2 \subset E_1^\perp$, où E_1^\perp désigne l'orthogonal de E_1 relativement à φ .
 - (f) Déterminer E_1^\perp .
7. Montrer que la restriction de q à E_1 est définie positive et que la restriction de q à E_2 est définie négative.

28.2 Solution

1. Le coefficient d'indice (i, i) de $P = M^2$, pour i compris entre 1 et n , est :

$$p_{ii} = \sum_{k=1}^n x_{ik}x_{ki}$$

et donc :

$$\begin{aligned} q(M) &= Tr(M^2) = \sum_{i=1}^n p_{ii} = \sum_{i=1}^n \sum_{k=1}^n x_{ik} x_{ki} \\ &= \sum_{i=1}^n x_{ii}^2 + 2 \sum_{1 \leq i < j \leq n} x_{ij} x_{ji}. \end{aligned}$$

2. On peut dire que q est un polynôme homogène de degré en $((x_{ij}))_{1 \leq i, j \leq n}$.
Ou alors, en désignant par φ l'application définie par :

$$\forall (M, N) \in E^2, \varphi(M, N) = Tr(MN)$$

vérifier que :

- φ est symétrique puisque $Tr(MN) = Tr(NM)$ pour toutes matrices M, N dans E .
- φ est bilinéaire puisque l'application trace est une forme linéaire et, à N fixé, l'application $M \mapsto MN$ est linéaire de E dans E , ce qui entraîne que pour tout N fixé, dans E l'application $M \mapsto Tr(MN)$ est linéaire comme composée d'applications linéaires. La symétrie nous dit que φ est en fait bilinéaire et cette application étant à valeurs réelles, c'est bien une forme bilinéaire symétrique.
- Pour tout $M \in E$, $q(M) = \varphi(M, M)$.

En conséquence q est une forme quadratique.

3. Ce qui précède nous dit que l'application $\varphi : (M, N) \mapsto Tr(MN)$ est la forme polaire de q .
4. Pour $1 \leq i < j \leq n$, on a :

$$2x_{ij}x_{ji} = \frac{1}{2}(x_{ij} + x_{ji})^2 - \frac{1}{2}(x_{ij} - x_{ji})^2,$$

ce qui donne la réduction de Gauss :

$$\begin{aligned} q(M) &= \sum_{i=1}^n x_{ii}^2 + \frac{1}{2} \sum_{1 \leq i < j \leq n} (x_{ij} + x_{ji})^2 - \frac{1}{2} \sum_{1 \leq i < j \leq n} (x_{ij} - x_{ji})^2 \\ &= \sum_{i=1}^n L_{ii}^2(M) + \frac{1}{2} \sum_{1 \leq i < j \leq n} L_{ij}^2(M) - \frac{1}{2} \sum_{1 \leq i < j \leq n} L_{ji}^2(M) \end{aligned}$$

où les formes linéaires L_{ij} pour $1 \leq i, j \leq n$ sont définies par :

$$\begin{cases} L_{ii}(M) = x_{ii} & (1 \leq i \leq n) \\ L_{ij}(M) = x_{ij} + x_{ji} & (1 \leq i < j \leq n) \\ L_{ji}(M) = x_{ij} - x_{ji} & (1 \leq i < j \leq n) \end{cases}$$

L'algorithme de Gauss nous assure que ces formes sont linéairement indépendantes dans le dual E^* .

5. Le rang de q est :

$$\begin{aligned} rg(q) &= card\{L_{ii} \mid 1 \leq i \leq n\} + card\{L_{ij} \mid 1 \leq i < j \leq n\} + card\{L_{ji} \mid 1 \leq i < j \leq n\} \\ &= n + 2\{(i, j) \in \mathbb{N}^2 \mid 1 \leq i < j \leq n\} = n + 2card(X) \end{aligned}$$

avec :

$$X = \{(1, 2), \dots, (1, n)\} \cup \{(2, 3), \dots, (2, n)\} \cup \dots \cup \{(n-1, n)\}$$

ce qui donne :

$$\text{card}(X) = (n-1) + (n-2) + \dots + 2 + 1 = \frac{n(n-1)}{2}$$

et $\text{rg}(q) = n + n(n-1) = n^2 = \dim(E)$.

La forme q est donc non dégénérée et $\ker(q) = \{0\}$.

La signature de q est

$$\text{sign}(q) = \left(n + \frac{n(n-1)}{2}, \frac{n(n-1)}{2} \right) = \left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2} \right).$$

6.

- (a) Une matrice symétrique est uniquement déterminée par son triangle supérieur large (i. e. avec la diagonale comprise), ce qui signifie que $\dim(E_1) = \frac{n(n+1)}{2}$.

On peut aussi dire qu'une matrice symétrique s'écrit :

$$M = \sum_{1 \leq i \leq j \leq n} a_{ij} E_{ij}$$

où les matrices E_{ij} sont définies par :

pour $1 \leq i \leq n$, E_{ii} a tous ses coefficients nuls sauf celui d'indice (i, i) qui vaut 1 ;

pour $1 \leq i < j \leq n$, E_{ij} a tous ses coefficients nuls sauf ceux d'indice (i, j) et (j, i) qui valent 1.

Le système $\{E_{ij} \mid 1 \leq i \leq j \leq n\}$ engendre E_1 et on vérifie facilement qu'il est libre, c'est donc une base de E_1 . On retrouve que :

$$\dim(E_1) = \text{card} \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i \leq j \leq n\} = \frac{n(n+1)}{2}.$$

- (b) De ${}^t M = -M$, on déduit que $x_{ii} = -x_{ii}$ pour tout i compris entre 1 et n . En conséquence, tous les termes diagonaux de $M \in E_2$ sont nuls.
- (c) Comme en **a.** on vérifie que $\dim(E_2) = \frac{n(n-1)}{2}$, une base étant donnée par la famille de matrices $\{F_{ij} \mid 1 \leq i < j \leq n\}$, où :
- pour $1 \leq i < j \leq n$, F_{ij} a tous ses coefficients nuls sauf ceux d'indice (i, j) et (j, i) qui valent respectivement 1 et -1 .
- (d) Si $M \in E_1 \cap E_2$, on a alors $M = {}^t M = -M$, ce qui implique $M = 0$. On a donc $E_1 \cap E_2 = \{0\}$ avec :

$$\dim(E) = n^2 = \frac{n(n-1)}{2} + \frac{n(n+1)}{2} = \dim(E_1) + \dim(E_2)$$

et en conséquence $E = E_1 \oplus E_2$.

- (e) Pour $(M, N) \in E_2 \times E_1$, on a :

$${}^t(MN) = {}^t N {}^t M = -NM,$$

c'est-à-dire que $MN \in E_2$ et $\varphi(M, N) = \text{Tr}(MN) = 0$, ce qui signifie que $M \in E_1^\perp$.

(f) Comme φ est non dégénérée, on a :

$$\dim(E_1^\perp) = \dim(E) - \dim(E_1) = \frac{n(n-1)}{2} = \dim(E_2)$$

et ce qui précède nous dit que $E_1^\perp = E_2$.

7. Pour $M \in E_1$, on a ${}^tM = M$ et :

$$L_{ji}(M) = x_{ij} - x_{ji} = 0 \quad (1 \leq i < j \leq n)$$

et la décomposition de Gauss donne :

$$q(M) = \sum_{i=1}^n L_{ii}^2(M) + \frac{1}{2} \sum_{1 \leq i < j \leq n} L_{ij}^2(M) \geq 0$$

avec $q(M) = 0$ si, et seulement si, $L_{ii}(M) = x_{ii} = 0$ pour $1 \leq i \leq n$ et $L_{ij}(M) = x_{ij} + x_{ji} = 2x_{ij} = 0$ pour $1 \leq i < j \leq n$, ce qui équivaut à $M = 0$.

La restriction de q à E_1 est donc définie positive.

De même, pour $M \in E_2$, on a ${}^tM = -M$, soit $x_{ij} = -x_{ji}$ pour tous i, j , ce qui entraîne $L_{ii}(M) = x_{ii} = 0$ pour $1 \leq i \leq n$ et $L_{ij}(M) = x_{ij} + x_{ji} = 0$ pour $1 \leq i < j \leq n$. La décomposition de Gauss donne alors :

$$q(M) = -\frac{1}{2} \sum_{1 \leq i < j \leq n} L_{ji}^2(M) \leq 0$$

avec $q(M) = 0$ si, et seulement si, $L_{ji}(M) = x_{ij} - x_{ji} = 2x_{ij} = 0$ pour $1 \leq i < j \leq n$, ce qui équivaut à $M = 0$.

La restriction de q à E_2 est donc définie négative.

Décomposition d'un entier en carrés.

Entiers de Gauss

29.1 Énoncé

Pour tout nombre complexe $z = x + iy$, on note $\bar{z} = x - iy$ le complexe conjugué de z et $|z| = \sqrt{z\bar{z}}$ le module de z .

– I – Le théorème des deux carrés

On note Σ_2 l'ensemble des entiers naturels qui s'écrivent comme somme de deux carrés, soit :

$$\Sigma_2 = \{n \in \mathbb{N} \mid n = a^2 + b^2 \text{ où } (a, b) \in \mathbb{Z}^2\}.$$

On peut remarquer qu'un entier n est dans Σ_2 si, et seulement si, il existe un nombre complexe $z = a + ib$ avec $(a, b) \in \mathbb{Z}^2$ tel que $n = |z|^2$.

1. Montrer que Σ_2 est stable pour le produit, c'est-à-dire que le produit de deux entiers naturels qui sont somme de deux carrés est encore somme de deux carrés.
Il suffit donc, pour décrire Σ_2 , de s'occuper des nombres premiers qui peuvent s'écrire comme somme de deux carrés.
2. Montrer que si $n \in \Sigma_2$ est impair, il est alors congru à 1 modulo 4.
3. Soit p un nombre premier dans Σ_2 . Montrer que p est soit égal à 2, soit congru à 1 modulo 4.
4. Soit p un nombre premier congru à 1 modulo 4. Montrer qu'il existe un entier naturel non nul r tel que p divise $1 + r^2$ (on peut utiliser le théorème de Wilson). Ce résultat est-il encore vrai pour p premier congru à 3 modulo 4 ?
5. Soient x un réel et $n \geq 1$ un entier. Montrer qu'il existe un couple d'entiers $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que :

$$1 \leq q \leq n \text{ et } |qx - p| \leq \frac{1}{n+1}.$$

6. Soient x et λ deux réels avec $\lambda > 1$ non entier. Montrer qu'il existe un couple d'entiers $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que :

$$1 \leq q < \lambda \text{ et } |qx - p| < \frac{1}{\lambda}.$$

7. Soient r et n deux entiers naturels non nuls tels que n divise $1 + r^2$. Montrer que n est somme de deux carrés (on peut utiliser la question précédente avec $x = \frac{r}{n}$ et $\lambda = \sqrt{n}$).

8. Soient p, q deux entiers naturels non nuls premiers entre eux et n un entier naturel non nul. Montrer que si n divise $p^2 + q^2$, il est alors somme de deux carrés.
9. Soit p un nombre premier. Montrer que p est somme de deux carrés si, et seulement si, il est égal à 2 ou congru à 1 modulo 4 (théorème de Fermat).
10. On propose ici une autre démonstration du résultat précédent. Compte tenu de **I.3**, il suffit de montrer qu'un nombre premier congru à 1 modulo 4 est dans Σ_2 . On se donne donc un nombre premier p congru à 1 modulo 4.
 - (a) Montrer qu'il existe un entier r compris entre 2 et $p - 1$ tel que p divise $r^2 + 1$.
 - (b) Montrer que si $r < \sqrt{p}$, alors $p = r^2 + 1$.
 - (c) On suppose que $\sqrt{p} < r$.
 - i. En désignant par $(r_k)_{0 \leq k \leq n}$ la suite des restes successifs qui apparaissent dans l'algorithme d'Euclide pour le calcul de $p \wedge r$ où $r_0 = r$, $r_{n-1} = p \wedge r$ et $r_n = 0$, montrer que, pour tout k compris entre 0 et $n - 1$, il existe un entier w_k compris entre 1 et $p - 1$ tel que $r_k \equiv rw_k$ modulo p .
 - ii. Montrer qu'il existe un entier k compris entre 1 et $n - 1$ tel que $p = r_k^2 + w_k^2$.
11. Soit n un entier naturel non nul somme de deux carrés. Montrer que si p est un diviseur premier de n congru à 3 modulo 4, alors l'exposant de p dans la décomposition de n en facteurs premiers est nécessairement pair.
12. Dédurre de ce qui précède qu'un entier naturel non nul n est somme de deux carrés si, et seulement si, les éventuels diviseurs premiers de n congrus à 3 modulo 4 qui apparaissent dans sa décomposition en facteurs premiers y figurent avec un exposant pair.
13. Montrer que $n = 3240$ est dans Σ_2 et donner une décomposition de n en somme de deux carrés.
14. Montrer que si n est somme de deux carrés, $n = a^2 + b^2$, avec a et b premiers entre eux, alors n n'a pas de diviseur premier congru à 3 modulo 4. La réciproque est-elle vraie ?

– II – Les entiers de Gauss

On désigne par $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss défini par :

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}.$$

1.

- (a) Montrer que $\mathbb{Z}[i]$ est un sous anneau de \mathbb{C} stable par l'opération de conjugaison complexe.
- (b) Montrer que l'anneau $\mathbb{Z}[i]$ est contenu dans tout sous anneau de \mathbb{C} qui contient i . L'anneau $\mathbb{Z}[i]$ est donc le plus petit sous anneau (unitaire) de \mathbb{C} (pour l'ordre de l'inclusion) qui contient i , on dit que c'est le sous anneau de \mathbb{C} engendré par i .
- (c) Montrer que $\mathbb{Z}[i]$ est égal à l'intersection de tous les sous anneaux de \mathbb{C} qui contiennent i .

2. Déterminer l'ensemble $\mathbb{Z}[i]^\times$ des éléments inversibles de $\mathbb{Z}[i]$.

3. Soient u, v dans $\mathbb{Z}[i]$.

- (a) Montrer que si u/v dans $\mathbb{Z}[i]$, alors $|u|^2$ divise $|v|^2$ dans \mathbb{N} et, pour $v \neq 0$, $|u| \leq |v|$.

- (b) Montrer que si u/v dans $\mathbb{Z}[i]$ et $|u| = |v|$, alors u et v sont associés et v/u .
 (c) Montrer que si u/v et v/u dans $\mathbb{Z}[i]$, alors $|u| = |v|$. La réciproque est-elle vraie ?
 4. Soit (u, v) dans $\mathbb{Z}[i] \times \mathbb{Z}[i]^*$. Montrer qu'il existe un couple (q, r) dans $\mathbb{Z}[i]^2$ tel que :

$$u = qv + r \text{ avec } |r| < |v|$$

- ($\mathbb{Z}[i]$ est un anneau euclidien). Un tel couple (q, r) est-il unique ?
 5. Montrer que $\mathbb{Z}[i]$ est un anneau principal.
 6. Soit u irréductible dans $\mathbb{Z}[i]$ et v, w dans $\mathbb{Z}[i]$. Montrer que si u divise vw alors u divise v ou u divise w .
 7. Soit p un nombre premier.
 (a) Montrer que si $p = 2$, il est alors réductible dans $\mathbb{Z}[i]$.
 (b) Montrer que si p est impair congru à 3 modulo 4, il est alors irréductible dans $\mathbb{Z}[i]$.
 (c) Montrer que si p est impair congru à 1 modulo 4, il est alors réductible dans $\mathbb{Z}[i]$.
 On a donc montré que p est réductible dans $\mathbb{Z}[i]$ si, et seulement si, il est somme de deux carrés d'entiers naturels.
 8. Montrer que si $u \in \mathbb{Z}[i]$ est tel que $|u|^2$ soit premier dans \mathbb{N} , alors u est irréductible dans $\mathbb{Z}[i]$.
 9. Montrer que les éléments irréductibles de $\mathbb{Z}[i]$ sont les entiers de Gauss associés à un entier naturel premier congru à 3 modulo 4 et les entiers de Gauss u tels que $|u|^2$ soit premier dans \mathbb{N} .

– III – Le théorème des quatre carrés

On note Σ_4 l'ensemble des entiers naturels qui s'écrivent comme somme de quatre carrés, soit :

$$\Sigma_4 = \{n \in \mathbb{N} \mid n = a^2 + b^2 + c^2 + d^2 \text{ où } (a, b, c, d) \in \mathbb{Z}^4\}.$$

On peut remarquer qu'un entier n est dans Σ_4 si, et seulement si, il existe deux nombres complexes $u = a + ib$ et $v = c + id$ avec $(a, b, c, d) \in \mathbb{Z}^4$ tels que :

$$n = \det \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} = |u|^2 + |v|^2.$$

Pour tout nombre premier p , on note \mathbb{F}_p le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ des classes résiduelles modulo p .

- Montrer que Σ_4 est stable pour le produit, c'est-à-dire que le produit de deux entiers naturels qui sont somme de quatre carrés est encore somme de quatre carrés.
 Dans les deux questions qui suivent, p désigne un nombre premier impair.
- Déterminer le nombre de carrés dans \mathbb{F}_p , c'est-à-dire le cardinal de l'ensemble :

$$C = \{x^2 \mid x \in \mathbb{F}_p\}.$$

- Montrer que pour tous u, v dans \mathbb{F}_p^* et w dans \mathbb{F}_p , l'équation $ux^2 + vy^2 = w$ a une solution (x, y) dans \mathbb{F}_p^2 .

(c) Montrer qu'il existe des entiers relatifs r et s compris entre $-\frac{p-1}{2}$ et $\frac{p-1}{2}$ tels que p divise $1 + r^2 + s^2$.

3. On se propose dans cette question de montrer que p est somme de quatre carrés.

On note :

$$E = \{k \in \{1, \dots, p-1\} \mid kp \in \Sigma_4\}.$$

(a) Montrer que E est non vide.

(b) On désigne par m le plus petit élément de E . Montrer que m est impair.

(c) On suppose que $m > 1$ et on désigne par a, b, c, d des entiers relatifs tels que :

$$mp = a^2 + b^2 + c^2 + d^2.$$

On désigne par r_1, r_2, r_3, r_4 les représentants respectifs de $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ dans l'anneau quotients $\frac{\mathbb{Z}}{m\mathbb{Z}}$ des classes résiduelles modulo m tels que $|r_k| \leq \frac{m-1}{2}$ pour tout k compris entre 1 et 4 (est impair) et on note :

$$n = r_1^2 + r_2^2 + r_3^2 + r_4^2.$$

i. Montrer qu'il existe un entier q compris entre 1 et $m-1$ tels que $n = qm$.

ii. Montrer qu'il existe des entiers x_1, x_2, x_3, x_4 tous divisibles par m tels que :

$$m^2 qp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

iii. En déduire que $qp \in \Sigma_4$ et conclure.

4. Montrer que tout entier naturel est somme de quatre carrés, c'est-à-dire que $\Sigma_4 = \mathbb{N}$ (théorème de Lagrange).

Les anneaux $\mathbb{Z}[i\sqrt{n}]$ pour $n \geq 2$

On se donne un entier naturel $n \geq 2$ et on note :

$$\mathbb{Z}[i\sqrt{n}] = \{a + ib\sqrt{n} \mid (a, b) \in \mathbb{Z}^2\}$$

(pour $n = 1$, il s'agit des entiers de Gauss déjà étudiés).

On rappelle qu'un idéal I d'un anneau A est principal s'il existe $a \in A$ tel que :

$$I = aA = \{ab \mid b \in A\}.$$

On dit que l'anneau A est principal si tous ses idéaux sont principaux.

On rappelle que l'anneau A est euclidien, s'il existe une fonction $N : A^* \rightarrow \mathbb{N}$ (appelée stathme) telle que pour tout couple (a, b) d'éléments de A^* , il existe un couple (q, r) dans A^2 tel que $a = bq + r$ avec $r = 0$ ou $N(r) < N(b)$.

On rappelle que l'anneau A est dit factoriel si pour tout $a \in A^*$ il existe une unité $u \in A^\times$ et des éléments irréductibles p_1, \dots, p_r tels que $a = u \prod_{k=1}^r p_k$, cette décomposition étant unique à

permutation et aux inversibles près, c'est-à-dire que si $a = u \prod_{k=1}^r p_k = v \prod_{k=1}^s q_k$, où u, v sont des unités et $p_1, \dots, p_r, q_1, \dots, q_s$ des éléments irréductibles, alors $r = s$ et il existe une permutation σ de l'ensemble $\{1, 2, \dots, r\}$ telle que, pour tout k compris entre 1 et r , p_k et $q_{\sigma(k)}$ soient associés.

1.
 - (a) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous anneau de \mathbb{C} stable par l'opération de conjugaison complexe.
 - (b) Montrer que l'anneau $\mathbb{Z}[i\sqrt{n}]$ est contenu dans tout sous anneau de \mathbb{C} qui contient $i\sqrt{n}$. L'anneau $\mathbb{Z}[i\sqrt{n}]$ est donc le plus petit sous anneau (unitaire) de \mathbb{C} (pour l'ordre de l'inclusion) qui contient $i\sqrt{n}$, on dit que c'est le sous anneau de \mathbb{C} engendré par $i\sqrt{n}$.
 - (c) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est égal à l'intersection de tous les sous anneaux de \mathbb{C} qui contiennent $i\sqrt{n}$.
2. Déterminer l'ensemble $\mathbb{Z}[i\sqrt{n}]^\times$ des éléments inversibles de $\mathbb{Z}[i\sqrt{n}]$.
3. Soient u, v dans $\mathbb{Z}[i\sqrt{n}]$.
 - (a) Montrer que si u/v dans $\mathbb{Z}[i\sqrt{n}]$, alors $|u|^2$ divise $|v|^2$ dans \mathbb{N} et, pour $v \neq 0$, $|u| \leq |v|$.
 - (b) Montrer que si u/v dans $\mathbb{Z}[i\sqrt{n}]$ et $|u| = |v|$, alors u et v sont associés et v/u .
 - (c) Montrer que si u/v et v/u dans $\mathbb{Z}[i\sqrt{n}]$, alors $|u| = |v|$. La réciproque est-elle vraie ?
4. Montrer que si $u \in \mathbb{Z}[i\sqrt{n}]$ est tel que $|u|^2$ soit premier dans \mathbb{N} , alors u est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.
5. Montrer que tout élément u non nul et non inversible dans $\mathbb{Z}[i\sqrt{n}]$ se décompose en produit de facteurs irréductibles, c'est-à-dire qu'il existe un entier $r \geq 1$, des éléments v_1, \dots, v_r deux à deux distincts (si $r \geq 2$) irréductibles dans $\mathbb{Z}[i\sqrt{n}]$ et des entiers naturels non nuls $\alpha_1, \dots, \alpha_r$, tels que $u = \pm \prod_{k=1}^r p_k^{\alpha_k}$.
6. On suppose ici que $n \geq 3$ est impair.
 - (a) Montrer que 2 , $1 + i\sqrt{n}$ et $1 - i\sqrt{n}$ sont irréductibles dans $\mathbb{Z}[i\sqrt{n}]$.
 - (b) Montrer que $1 + n$ s'écrit de deux manières différentes comme produit de facteurs irréductibles (permutations mises à part). L'anneau $\mathbb{Z}[i\sqrt{n}]$ n'est donc pas factoriel pour $n \geq 3$ impair.
 - (c) Soit u irréductible dans $\mathbb{Z}[i\sqrt{n}]$ divisant le produit vw où v, w sont dans $\mathbb{Z}[i\sqrt{n}]$. Peut-on affirmer que u divise v ou w ?
7. Montrer qu'un anneau euclidien est principal.
8. Soit A un anneau principal. Montrer directement (sans utiliser l'implication A principal, donc factoriel) que si un élément u irréductible dans A divise le produit vw de deux éléments de A , alors il divise v ou w .
9. On suppose que $n \geq 3$.
 - (a) Montrer que $i\sqrt{n}$, est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.
 - (b) Montrer (sans utiliser l'implication A principal, donc factoriel) que $\mathbb{Z}[i\sqrt{n}]$ n'est ni euclidien ni principal (on distinguera les cas n pair et n impair).
10. Montrer que $\mathbb{Z}[i\sqrt{n}]$ est principal pour $n = 1$ ou $n = 2$.

29.2 Solution

– I – Le théorème des deux carrés

On peut remarquer que Σ_2 est non vide, puisqu'il contient $0, 1, 2 = 1^2 + 1^2$ et plus généralement tous les entiers carrés $n = a^2 + 0$.

1. Soient $n = a^2 + b^2$ et $m = c^2 + d^2$ où a, b, c, d sont des entiers relatifs. En écrivant que $n = |u|^2$ et $m = |v|^2$ où, $u = a + ib$ et $v = c + id$, on a :

$$\begin{aligned} nm &= |uv|^2 = |(ac - bd) + (ad + bc)i|^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

(identité de Lagrange), c'est-à-dire que nm est somme de deux carrés d'entiers.

2. Si n est un entier impair qui s'écrit $n = a^2 + b^2$ avec a et b entiers, alors ces deux entiers sont de parité différente. Comme a et b jouent des rôles symétriques, on peut supposer que $n = 2p$ et $b = 2q + 1$ et on a $n = 4p^2 + (2q + 1)^2 = 4k' + 1$, c'est-à-dire que n est congru à 1 modulo 4.
3. On a $2 = 1^2 + 1^2 \in \Sigma_2$. Si p est premier différent de 2, il est nécessairement impair et si de plus il est dans Σ_2 , il est alors congru à 1 modulo 4.
4. Comme $p \geq 3$ est congru à 1 modulo 4, il s'écrit $p = 4q + 1$ avec $q \geq 1$ et $m = \frac{p-1}{2} = 2q$ est un entier pair non nul.
Avec $2m = p - 1 \equiv -1 \pmod{p}$, on déduit que $m + 1 \equiv -m \pmod{p}$ et pour tout entier k compris entre 1 et $m - 1$:

$$m + k + 1 \equiv -m + k = -(m - k) \pmod{p}$$

de sorte que :

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot \dots \cdot m \cdot (m+1) \cdot \dots \cdot (m+m) \\ &\equiv m! (-1)^m m \cdot (m-1) \cdot \dots \cdot 1 = (m!)^2 \pmod{p} \end{aligned}$$

(m est pair).

D'autre part, le théorème de Wilson nous dit que $(p-1)! \equiv -1 \pmod{p}$ si p est premier. On a donc $(m!)^2 \equiv -1 \pmod{p}$, ce qui signifie que p divise $r^2 + 1$ où $r = m!$

Dire que $p \equiv 3 \pmod{4}$ revient à dire qu'il existe un entier $n \geq 0$ tel que $p = 4n + 3$.

On a alors $r = \frac{p-1}{2} = 2n + 1$ et si $x \in \mathbb{Z}_p^*$ est tel que $x^2 = -\bar{1}$, il vient $x^{p-1} = x^{2r} = (-\bar{1})^{2n+1} = -\bar{1}$, ce qui contredit le théorème de Fermat qui nous dit que $x^{p-1} = \bar{1}$ pour tout $x \in \mathbb{Z}_p^*$ (on a $-\bar{1} \neq \bar{1}$ puisque $p \geq 2$).

En définitive, on a montré qu'un entier premier p est congru à 1 modulo 4, si, et seulement si, $-\bar{1}$ est un carré dans \mathbb{Z}_p^* .

5. En désignant par $[t]$ la partie entière du réel t ($[t] \leq t < [t] + 1$), on a :

$$E = \{kx - [kx] \mid 0 \leq k \leq n\} \cup \{1\} \subset [0, 1]$$

et il existe au moins deux éléments distincts de E qui ont un écart au plus égal à $\frac{1}{n+1}$.

En effet, si ce n'est pas le cas, les $n+2$ éléments de E sont deux à deux distincts et en les rangeant dans l'ordre croissant :

$$t_0 = 0 < t_1 < \dots < t_n < t_{n+1} = 1$$

on a :

$$1 = m([0, 1]) \geq m\left(\bigcup_{k=0}^n [t_k, t_{k+1}]\right) = \bigcup_{k=0}^n m([t_k, t_{k+1}]) > (n+1) \frac{1}{n+1} = 1$$

ce qui est impossible. Si ces deux éléments sont $x_k = kx - [kx]$, où k est compris entre 0 et n et $x_{n+1} = 1$, on a alors :

$$|kx - [kx] - 1| = |qx - p| \leq \frac{1}{n+1}$$

où on a posé $q = k \in \{1, \dots, n\}$ ($k = 0$ donne $|x_k - x_{n+1}| = 1 > \frac{1}{n+1}$ puisque $n \geq 1$) et $p = [kx] + 1 \in \mathbb{Z}$. Sinon il s'agit de $x_k = kx - [kx]$ et $x_j = jx - [jx]$ avec $0 \leq k < j \leq n$ et on a :

$$|jx - [jx] - (kx - [kx])| = |qx - p| \leq \frac{1}{n+1}$$

où on a posé $q = j - k \in \{1, \dots, n\}$ et $p = [kx] - [jx] \in \mathbb{Z}$.

6. On désigne par n la partie entière de λ et on a $n < \lambda < n+1$ (λ n'est pas entier) et en désignant par (p, q) un couple d'entiers dans $\mathbb{Z} \times \mathbb{N}^*$ tels que $1 \leq q \leq n$ et $|qx - p| \leq \frac{1}{n+1}$, on a $1 \leq q < \lambda$ et $|qx - p| < \frac{1}{\lambda}$.

7. Si n est un carré, il est alors somme de deux carrés. Sinon le réel $\lambda = \sqrt{n}$ n'est pas entier et en notant $x = \frac{r}{n}$, on peut trouver un couple d'entiers (u, v) tel que $1 \leq v < \lambda$ et :

$$|vx - u| = \left|v \frac{r}{n} - u\right| < \frac{1}{\lambda} = \frac{1}{\sqrt{n}}$$

ou encore :

$$1 \leq v < \sqrt{n} \text{ et } |vr - un| < \sqrt{n}.$$

En posant $w = vr - un \in \mathbb{Z}$, on a $w^2 \leq n$ et $1 \leq v^2 + w^2 < 2n$ avec :

$$v^2 + w^2 = v^2 + (vr - un)^2 \equiv v^2 + v^2 r^2 = v^2 (1 + r^2) \pmod{n}$$

et $1 + r^2 \equiv 0 \pmod{n}$, ce qui donne $v^2 + w^2 \equiv 0 \pmod{n}$, soit $v^2 + w^2 = kn$ avec $1 \leq v^2 + w^2 < 2n$, ce qui impose $k = 1$, c'est-à-dire que $v^2 + w^2 = n$.

8. Si p et q sont premiers entre eux, le théorème de Bézout nous dit qu'il existe deux entiers u, v tels que $up + vq = 1$. Si n divise $p^2 + q^2$, il divise aussi :

$$\begin{aligned} (u^2 + v^2)(p^2 + q^2) &= |(u + iv)(p - iq)|^2 = |(up + vq) + i(vp - uq)|^2 \\ &= |1 + i(vp - uq)|^2 = 1 + (vp - uq)^2 \end{aligned}$$

et en conséquence n est somme de deux carrés.

9. On a déjà vu que $2 \in \Sigma_2$ et que tout nombre premier impair appartenant à Σ_2 est congru à 1 modulo 4.

Réciproquement soit p un nombre premier impair congru à 1 modulo 4. On a vu en **I.4** qu'on peut trouver un entier r tel que p divise $1 + r^2$. La question précédente nous dit alors que p est somme de deux carrés.

En définitive, on a montré, pour p premier impair, l'équivalence entre les propositions :

- p est somme de deux carrés ;
- p est congru à 1 modulo 4 ;
- $\overline{-1}$ est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

10.

- (a) Comme p est congru à 1 modulo 4, il existe un entier x tel que $x^2 + 1$ soit divisible par p et en désignant par r le représentant de \bar{x} dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ compris entre 0 et $p - 1$, l'entier $r^2 + 1$ est divisible par p . Les cas $r = 0$ et $r = 1$ étant impossibles puisque p est premier impair, on a en fait $2 \leq r \leq p - 1$.
- (b) Si $r < \sqrt{p}$, on a alors $r^2 < p$, soit $r^2 \leq p - 1$ et $r^2 + 1 = qp \leq p$, soit $r^2 + 1 = p$ et p est somme de deux carrés (par exemple $p = 5$ et $r = 2$).
- (c) On suppose donc que $\sqrt{p} \leq r$. Comme p est premier, \sqrt{p} n'est pas entier et on, a $\sqrt{p} < r$.
- i. L'algorithme d'Euclide, pour le calcul de $p \wedge r = 1$ (p premier est premier avec r compris entre 2 et $p - 1$) consiste à utiliser les suites d'entiers $(r_k)_{0 \leq k \leq n}$ et $(q_k)_{1 \leq k \leq n}$ définies par :

$$\begin{cases} r_{-1} = p = q_1 r_0 + r_1 \quad (0 < r_1 < r_0 = r) \\ r_0 = q_2 r_1 + r_2 \quad (0 < r_2 < r_1) \\ r_1 = q_3 r_2 + r_3 \quad (0 < r_3 < r_2) \\ \vdots \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad (0 < r_{n-1} < r_{n-2}) \\ r_{n-2} = q_n r_{n-1} + r_n \quad (r_n = 0) \end{cases}$$

et on a $r_{n-1} = p \wedge r = 1$. Pour tout k compris entre 0 et $n - 1$, il existe des entiers u_k et v_k tels que $r_k = pu_k + rv_k$ (on le vérifie par récurrence finie sur k), soit $r_k \equiv rv_k$ modulo p et en désignant par w_k le représentant modulo p de v_k qui est compris entre 0 et $p - 1$, on a encore $r_k \equiv rw_k$ modulo p . Comme $0 = r_n < r_{n-1} < \dots < r_1 < r < p$, on $w_k \neq 0$ pour k compris entre 0 et $n - 1$ (sinon p divise r_k).

- ii. De plus avec $1 = r_{n-1} < \sqrt{p} < r_0 = r$ et \sqrt{p} non entier, on déduit qu'il existe un entier k compris entre 1 et $n - 1$ tel que $r_k < \sqrt{p} < r_{k-1}$. Pour un tel k , on a :

$$r_k^2 + w_k^2 \equiv r^2 w_k^2 + w_k^2 = w_k^2 (r^2 + 1) \equiv 0 \pmod{p}$$

c'est-à-dire que p divise $r_k^2 + w_k^2$ avec :

$$2 \leq r_k^2 + w_k^2 < p + p = 2p$$

et nécessairement, $p = r_k^2 + w_k^2$.

11. Soit n un entier naturel non nul somme de deux carrés, $n = a^2 + b^2$ avec $(a, b) \in \mathbb{N}^2$. En désignant par δ le pgcd de a et b , on a $a = \delta\alpha$, $b = \delta\beta$ avec α et β premiers entre eux et $n = \delta^2(\alpha^2 + \beta^2)$. Si p est un diviseur premier de n congru à 3 modulo 4, on a alors $n = p^m q$ où $m \geq 1$ et q est premier avec p . Si p divise $\alpha^2 + \beta^2$, il est alors somme de deux carrés, ce qui est impossible pour $p \equiv 3$ modulo 4 (question I.2). Donc p ne divise pas $\alpha^2 + \beta^2$ et divise δ^2 donc δ . La décomposition de δ en facteurs premier contient donc p avec un exposant $r \geq 1$ et celle de n contient p avec un exposant $2r$.

12. On rappelle qu'un nombre premier impair est congru à 1 ou 3 modulo 4.

La condition nécessaire vient d'être montré.

Réciproquement supposons $n = 2^{m_1} p_2^{m_2} \cdots p_r^{m_r} q_1^{2r_1} \cdots q_s^{2r_s}$, où $m_1 \geq 0$, les p_j sont des nombres premiers congrus à 1 modulo 4 (s'il en existe) et les q_j des nombres premiers congrus à 3 modulo 4 (s'il en existe). Comme 1, 2, les p_j et les q_j^2 sont dans Σ_2 qui est stable par multiplication, on en déduit que $n \in \Sigma_2$.

13. Par exemple $3240 = 2^3 \cdot 3^4 \cdot 5$ est somme de deux carrés. On a :

$$\begin{aligned} 3240 &= |(1+i)^3 * (1+2i)|^2 * 9^2 \\ &= |-6-2i|^2 * 9^2 = 6^2 * 9^2 + 2^2 * 9^2 \\ &= 54^2 + 18^2 \end{aligned}$$

14. Si $n = a^2 + b^2$ avec a et b premiers entre eux, alors tout diviseur premier impair p de n divise $a^2 + b^2$ et il est alors somme de deux carrés (question **I.8**) et donc congru à 1 modulo 4 (question **I.9**).

La réciproque est fausse comme le montre l'exemple de :

$$n = 45 = 5 \cdot 3^2 = 3^2 + 6^2.$$

– II – Les entiers de Gauss

1.

- (a) Pour tout $u = a + ib \in \mathbb{Z}[i]$, on a $\bar{u} = a - ib \in \mathbb{Z}[i]$, donc $\mathbb{Z}[i]$ stable par conjugaison. On a $1 = 1 + i \cdot 0 \in \mathbb{Z}[i]$. Pour $u = a + ib$ et $v = c + id$, où a, b, c, d sont des entiers relatifs, on a :

$$\begin{cases} u - v = (a - c) + (b - d)i \in \mathbb{Z}[i] \\ uv = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i] \end{cases}$$

- (b) Si un anneau A contient i , il contient également 1 (il s'agit d'anneaux unitaires) et en conséquence il contient tout élément de la forme $a + ib$ avec $(a, b) \in \mathbb{Z}^2$. On a donc $\mathbb{Z}[i] \subset A$.

- (c) En désignant par $(A_i)_{i \in I}$ la famille de tous les sous anneaux de \mathbb{C} qui contiennent i , on a $A = \bigcap_{i \in I} A_i \subset \mathbb{Z}[i]$ puisque $\mathbb{Z}[i]$ est l'un de ces sous-anneaux et $\mathbb{Z}[i] \subset A$ puisque A est un anneau. On a donc bien $\mathbb{Z}[i] = A$.

2. Si $u = a + ib$ est inversible dans $\mathbb{Z}[i]$, il existe alors $v \in \mathbb{Z}[i]$ tel que $uv = 1$ et $|u|^2 |v|^2 = 1$ avec $|u|^2 = a^2 + b^2 \in \mathbb{N}$ et $|v|^2 \in \mathbb{N}$, ce qui impose $|u|^2 = |v|^2 = 1$. On a donc $a^2 + b^2 = 1$ avec $(a^2, b^2) \in \mathbb{N}^2$, ce qui équivaut à $(a^2, b^2) = (1, 0)$ ou $(a^2, b^2) = (0, 1)$ ou encore à $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$. On a donc $\mathbb{Z}[i]^\times \subset \{-1, 1, -i, i\}$. L'inclusion réciproque se vérifiant facilement. En définitive, on a :

$$\mathbb{Z}[i]^\times = \{u \in \mathbb{Z}[i] \mid |u| = 1\} = \{-1, 1, -i, i\}.$$

On peut remarquer que le groupe $\mathbb{Z}[i]^\times$ est le cyclique d'ordre 4 formé des racines 4-ième de l'unité et qu'il est isomorphe à $\frac{\mathbb{Z}}{4\mathbb{Z}}$.

3.

(a) Dire que u/v dans $\mathbb{Z}[i]$ signifie qu'il existe $q \in \mathbb{Z}[i]$ tel que $v = qu$, ce qui entraîne $|v|^2 = |q|^2 |u|^2$ avec $|q|^2 \in \mathbb{N}$ et $|u|^2$ divise $|v|^2$ dans \mathbb{N} . De plus, pour v non nul, on a $q \neq 0$, donc $|q|^2 \geq 1$ dans \mathbb{N} et $|v|^2 \geq |u|^2$, ce qui revient à dire que $|u| \leq |v|$.

(b) Si $u = 0$ ou $v = 0$ alors $u = v = 0$ et u, v sont bien associés.

On suppose donc que $u \neq 0$ et $v \neq 0$. On a $v = qu$ dans $\mathbb{Z}[i]^*$ avec $|u| = |v|$, donc $|q| = 1$ dans $\mathbb{Z}[i]$, ce qui équivaut à dire que $q \in \mathbb{Z}[i]^\times$. Il en résulte que u et v sont associés, ce qui entraîne que v divise u .

(c) Dire que u/v et v/u dans $\mathbb{Z}[i]$ équivaut à dire que u et v sont associés dans $\mathbb{Z}[i]$, soit $v = qu$ avec $q \in \{-1, 1, -i, i\}$, ce qui entraîne $|u| = |v|$ (on peut aussi utiliser la question précédente en permutant les rôles de u et v).

La réciproque est fautive. En effet, pour $u = 2+i$ et $v = \bar{u} = 2-i$, on a $|u| = |v| = \sqrt{5}$ et u, v ne sont pas associés puisque $\frac{u}{v} = \frac{2+i}{2-i} = \frac{3}{5} + \frac{4}{5}i \notin \mathbb{Z}[i]$.

4. Soit $z = \frac{u}{v} = x + iy$ avec $(x, y) \in \mathbb{R}^2$. En utilisant la partition $\mathbb{R} = \bigcup_{n \in \mathbb{Z}} \left[n - \frac{1}{2}, n + \frac{1}{2} \right]$, on peut trouver un unique couple (a, b) d'entiers relatifs tels que :

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2} \right] \times \left[b - \frac{1}{2}, b + \frac{1}{2} \right]$$

et en notant $q = a + ib$, on a $q \in \mathbb{Z}[i]$ et :

$$\begin{aligned} \left| \frac{u}{v} - q \right|^2 &= |(x-a) + i(y-b)|^2 \\ &= (x-a)^2 + (y-b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1 \end{aligned}$$

ou encore $|u - qv| < |v|$. En posant $r = u - qv$, on a bien $r \in \mathbb{Z}[i]$ et $|r| < |v|$.

Un tel couple n'est pas unique comme le montre l'exemple de $(u, v) = (14, 4)$. On a $14 = 3 \cdot 4 + 2 = 4 \cdot 4 + (-2)$ avec $|2| = |-2| < |4|$.

5. Soit I un idéal de $\mathbb{Z}[i]$. Si $I = \{0\}$, il est principal. On suppose que $I \neq \{0\}$ et on pose :

$$n = \inf \{ |u|^2 \mid u \in I \setminus \{0\} \}.$$

Cette borne inférieure existe puisque $P = \{ |u|^2 \mid u \in I \setminus \{0\} \}$ est une partie non vide de \mathbb{N}^* et de plus elle est atteinte, c'est-à-dire qu'il existe u_0 dans $I \setminus \{0\}$ tel que $n = |u_0|^2$. En effectuant la division euclidienne d'un élément u de I par u_0 , on a $u = qu_0 + r$ avec $r \in \mathbb{Z}[i]$ tel que $|r| < |u_0|$, ce qui entraîne $r = 0$ puisque u_0 est de module minimal dans $I \setminus \{0\}$. Tout élément u de I s'écrit donc $u = qu_0$ et $I \subset u_0 \mathbb{Z}[i]$. Comme par ailleurs $u_0 \mathbb{Z}[i] \subset I$ puisque I est un idéal, on a $I = u_0 \mathbb{Z}[i]$.

En définitive, $\mathbb{Z}[i]$ est principal.

En fait, de manière plus générale, tout anneau euclidien est principal.

6. Comme $\mathbb{Z}[i]$ est principal, l'idéal $u\mathbb{Z}[i] + v\mathbb{Z}[i]$ est engendré par un élément δ (un pgcd de u et v), soit $u\mathbb{Z}[i] + v\mathbb{Z}[i] = \delta\mathbb{Z}[i]$. De $u \in \delta\mathbb{Z}[i]$, on déduit que δ divise u , donc δ est soit inversible, soit associé à u , puisque u est irréductible. Dans le cas où δ est inversible, on a $\delta\mathbb{Z}[i] = \mathbb{Z}[i]$, donc $1 \in u\mathbb{Z}[i] + v\mathbb{Z}[i]$, soit $1 = \alpha u + \beta v$ avec α, β dans $\mathbb{Z}[i]$ et u divise $w = \alpha u w + \beta v w$. Dans le cas où δ est associé à u , on a $\delta\mathbb{Z}[i] = u\mathbb{Z}[i]$, donc

$v \in u\mathbb{Z}[i]$ et u divise v .

Par récurrence, on déduit que si u irréductible divise un produit $\prod_{k=1}^r v_k$, il divise alors l'un des v_k .

7.

- (a) On a $2 = (1+i)(1-i)$ avec $1 \pm i$ non inversible ($|1 \pm i| = \sqrt{2} \neq 1$), donc 2 est réductible dans $\mathbb{Z}[i]$.
- (b) Soit p premier impair congru à 3 modulo 4. Si $p = u_1 u_2$ avec $|u_k| = |a_k + ib_k| > 1$, pour $k = 1, 2$, dans $\mathbb{Z}[i]$, on a alors $p^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$ dans \mathbb{N}^* et $a_1^2 + b_1^2$ est un entier compris entre 2 et $p^2 - 1$ (puisque $a_k^2 + b_k^2 \geq 2$) qui divise p^2 , ce qui impose $a_1^2 + b_1^2 = p$ en contradiction avec p congru à 3 modulo 4 puisque dans ce cas p n'est pas somme de deux carrés.
- (c) Si p est premier impair congru à 1 modulo 4, il est alors somme de deux carrés, soit $p = a^2 + b^2 = uv$ avec $u = a + ib$, $v = \bar{u}$ et $|u| = |v| = \sqrt{p} > 1$ dans $\mathbb{Z}[i]$, ce qui signifie que u et v ne sont pas inversibles et p est réductible dans $\mathbb{Z}[i]$.

8. Supposons que $|u|^2$ soit premier dans \mathbb{N} . Si $u = vw$ dans $\mathbb{Z}[i]$, on a alors $p = |u|^2 = |v|^2 |w|^2$ dans \mathbb{N} avec p premier, ce qui implique $|v|^2 = 1$ ou $|w|^2 = 1$, soit v ou w inversible dans $\mathbb{Z}[i]$. L'entier de Gauss u est donc irréductible dans $\mathbb{Z}[i]$.

9. On a déjà montré que les entiers naturels premiers congrus à 3 modulo 4 et les entiers de Gauss u tels que $|u|^2$ soit premier dans \mathbb{N} sont irréductibles de $\mathbb{Z}[i]$.

Réciproquement, soit u irréductible de $\mathbb{Z}[i]$. L'entier de Gauss u divise $u\bar{u} = |u|^2$ dans $\mathbb{Z}[i]$. En utilisant la décomposition en facteurs premiers de $|u|^2$ dans \mathbb{N} , on déduit que u divise un des facteurs premiers p de cet entier $|u|^2$. On a donc $p = uv$ avec $p \geq 2$ premier dans \mathbb{N} et $v \in \mathbb{Z}[i]$. Si v est inversible, u est alors associé à p , donc p est premier irréductible $\mathbb{Z}[i]$, c'est-à-dire congru à 3 modulo 4. Sinon, on a $|v| > 1$ et de $p^2 = |u|^2 |v|^2$ dans \mathbb{N} , avec $2 \leq |u|^2 < p^2$, on déduit que $|u|^2 = p$.

Les éléments irréductibles de $\mathbb{Z}[i]$ sont donc les entiers de Gauss associés à un entier naturel premier congru à 3 modulo 4 et les entiers de Gauss u tels que $|u|^2$ soit premier dans \mathbb{N} .

– III – Le théorème des quatre carrés

1. Soient $n = a^2 + b^2 + b^2 + c^2$ et $m = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ où a, b, \dots, δ sont des entiers relatifs. En écrivant que $n = \det \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ et $m = \det \begin{pmatrix} u' & v' \\ -\bar{v}' & \bar{u}' \end{pmatrix}$ où $u = a + ib$, $v = c + id$,

$u' = \alpha + i\beta$, $v' = \gamma + i\delta$, on a :

$$\begin{aligned} nm &= \det \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \begin{pmatrix} u' & v' \\ -\bar{v}' & \bar{u}' \end{pmatrix} = \det \begin{pmatrix} uu' - v\bar{v}' & uv' + v\bar{u}' \\ -\bar{u}v' - \bar{v}u' & \bar{u}\bar{u}' - \bar{v}\bar{v}' \end{pmatrix} \\ &= \det \begin{pmatrix} uu' - v\bar{v}' & uv' + v\bar{u}' \\ -(\bar{u}v' + \bar{v}u') & \bar{u}\bar{u}' - \bar{v}\bar{v}' \end{pmatrix} = |uu' - v\bar{v}'|^2 + |uv' + v\bar{u}'|^2 \\ &= |(a + ib)(\alpha + i\beta) - (c + id)(\gamma - i\delta)|^2 \\ &\quad + |(a + ib)(\gamma + i\delta) + (c + id)(\alpha - i\beta)|^2 \\ &= |(a\alpha - b\beta - c\gamma - d\delta) + i(a\beta + b\alpha - d\gamma + c\delta)|^2 \\ &\quad + |(a\gamma - b\delta + c\alpha + d\beta) + i(b\gamma + a\delta + d\alpha - c\beta)|^2 \\ &= (a\alpha - b\beta - c\gamma - d\delta)^2 + (a\beta + b\alpha + c\delta - d\gamma)^2 \\ &\quad + (a\gamma - b\delta + c\alpha + d\beta)^2 + (a\delta + b\gamma - c\beta + d\alpha)^2 \end{aligned}$$

c'est-à-dire que nm est somme de quatre carrés d'entiers.

Comme on peut changer b, c, d en $-b, -c, -d$ sans modifier n , cette identité s'écrit aussi :

$$\begin{aligned} nm &= (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - b\alpha - c\delta + d\gamma)^2 \\ &\quad + (a\gamma + b\delta - c\alpha - d\beta)^2 + (a\delta - b\gamma + c\beta - d\alpha)^2 \end{aligned}$$

2.

- (a) En utilisant le fait que l'application $x \mapsto x^2$ est un morphisme du groupe multiplicatif \mathbb{F}_p^* sur lui-même de noyau $\{\overline{-1}, \overline{1}\}$ à deux éléments ($\overline{-1} \neq \overline{1}$ dans \mathbb{F}_p puisque $p \geq 3$) et d'image le groupe multiplicatif C^* des carrés de \mathbb{F}_p^* , on déduit que C^* est isomorphe

au groupe quotient $\frac{\mathbb{F}_p^*}{\{\overline{-1}, \overline{1}\}}$ et $\text{card}(C^*) = \text{card}\left(\frac{\mathbb{F}_p^*}{\{\overline{-1}, \overline{1}\}}\right) = \frac{p-1}{2}$. Comme $C =$

$C^* \cup \{\overline{0}\}$, on en déduit que $\text{card}(C) = \frac{p-1}{2} + 1 = \frac{p+1}{2}$.

- (b) Pour u, v dans \mathbb{F}_p^* et w dans \mathbb{F}_p , les ensembles $A = \{ux^2 \mid x \in \mathbb{F}_p\}$ et $B = \{w - vy^2 \mid y \in \mathbb{F}_p\}$ sont en bijection avec C (puisque u et v sont non nuls et \mathbb{F}_p est un corps) et donc ont le même nombre d'éléments, soit $\frac{p+1}{2}$. Ces ensembles ne peuvent donc être disjoints dans \mathbb{F}_p qui est de cardinal p , c'est-à-dire qu'il existe x, y dans \mathbb{F}_p tels que $ux^2 = w - vy^2$.

- (c) Prenant $(u, v, w) = (\overline{1}, \overline{1}, \overline{-1})$ dans la question précédente, on peut trouver x, y dans \mathbb{F}_p tels que $x^2 + y^2 = \overline{-1}$ et en écrivant que :

$$\mathbb{F}_p = \left\{ \overline{-\frac{p-1}{2}}, \dots, \overline{-1}, \overline{0}, \overline{1}, \dots, \overline{\frac{p-1}{2}} \right\}$$

on peut écrire que $x = \bar{r}$ et $y = \bar{s}$ avec r et s compris entre $-\frac{p-1}{2}$ et $\frac{p-1}{2}$. L'égalité $\overline{1} + x^2 + y^2 = \overline{0}$ dans \mathbb{F}_p se traduit alors en disant que p divise $1 + r^2 + s^2$.

3.

- (a) Si r et s sont des entiers compris entre $-\frac{p-1}{2}$ et $\frac{p-1}{2}$ tels que p divise $1 + r^2 + s^2$, il existe alors un entier k tel que $kp = 1 + r^2 + s^2$, ce qui entraîne $kp \in \Sigma_4$, $k \geq 1$ et :

$$kp \leq 1 + 2\frac{(p-1)^2}{4} < 1 + \frac{p^2}{2} < p^2$$

donc $k < p$ et k est dans E .

- (b) m est le plus petit entier compris entre 1 et $p-1$ tel que mp s'écrive $mp = a^2 + b^2 + c^2 + d^2$ où $(a, b, c, d) \in \mathbb{Z}^4$. Si m est pair, les entiers a, b, c, d sont soit de même parité, soit deux d'entre eux sont pairs et les deux autres impairs. On aurait alors $mp = \sum_{k=1}^4 x_k^2$ où les x_k sont des entiers qui sont de même parités ou tels que x_1, x_2 soient pairs et x_3, x_4 impairs. Dans ces deux cas, on peut écrire que :

$$\frac{m}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 \in \Sigma_4$$

ce qui contredit le caractère minimal de m . L'entier m est donc impair.

(c)

- i. Il est clair que $n \geq 0$. Si $n = 0$, alors tous les r_k sont nuls, ce qui signifie que les entiers a, b, c, d sont tous divisibles par m et il existe des entiers q_1, q_2, q_3, q_4 tels que :

$$mp = m^2 (q_1^2 + q_2^2 + q_3^2 + q_4^2)$$

ce qui donne $p = mu$ et m divise p avec p premier et $2 \leq m \leq p-1$, ce qui est impossible. On a donc $n \geq 1$.

Par ailleurs, comme $|r_k| \leq \frac{m-1}{2}$ pour tout k compris entre 1 et 4, on a :

$$n \leq 4 \left(\frac{m-1}{2}\right)^2 = (m-1)^2 < m^2$$

et :

$$\begin{aligned} n &= r_1^2 + r_2^2 + r_3^2 + r_4^2 \\ &\equiv a^2 + b^2 + c^2 + d^2 = mp \equiv 0 \pmod{m} \end{aligned}$$

c'est-à-dire que m divise n . On a donc $1 \leq n = qm < m^2$ et $q < m$.

- ii. Les entiers mp et $n = qm$ étant sommes de deux carrés, il en est de même du produit m^2qp . Plus précisément, avec :

$$\begin{cases} mp = a^2 + b^2 + c^2 + d^2 \\ qm = r_1^2 + r_2^2 + r_3^2 + r_4^2 \end{cases}$$

on a :

$$m^2qp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

où :

$$\begin{cases} x_1 = ar_1 + br_2 + cr_3 + dr_4 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m} \\ x_2 = ar_2 - br_1 - cr_4 + dr_3 \equiv ab - ba - cd + dc \equiv 0 \pmod{m} \\ x_3 = ar_3 + br_4 - cr_1 - dr_2 \equiv ac + bd - ca - db \equiv 0 \pmod{m} \\ x_4 = ar_4 - br_3 + cr_2 - dr_1 \equiv ad - bc + cb - da \equiv 0 \pmod{m} \end{cases}$$

c'est-à-dire que tous les r_k sont divisibles par m .

- iii. On a donc $x_k = my_k$ pour tout k compris entre 1 et 4 et :

$$m^2qp = m^2 (y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

ce qui donne $qp = y_1^2 + y_2^2 + y_3^2 + y_4^2 \in \Sigma_4$ avec $1 \leq q \leq m-1 \leq p-1$, ce qui contredit le caractère minimal de m .

On a donc $m = 1$ et $p \in \Sigma_4$.

4. Comme tout entier naturel est produit de nombres premiers et Σ_4 qui contient 0, 1 et tous les nombres premiers est stable par le produit, on déduit que $\Sigma_4 = \mathbb{N}$.

– IV – Les anneaux $\mathbb{Z}[i\sqrt{n}]$ pour $n \geq 2$

1.

- (a) Pour tout $u = a + ib\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$, on a $\bar{u} = a - ib\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$, donc $\mathbb{Z}[i\sqrt{n}]$ stable par conjugaison.

On a $1 = 1 + i \cdot 0 \cdot \sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$. Pour $u = a + ib\sqrt{n}$ et $v = c + id\sqrt{n}$, où a, b, c, d sont des entiers relatifs, on a :

$$\begin{cases} u - v = (a - c) + (b - d)i\sqrt{n} \in \mathbb{Z}[i\sqrt{n}] \\ uv = (ac - bdn) + (ad + bc)i\sqrt{n} \in \mathbb{Z}[i\sqrt{n}] \end{cases}$$

- (b) Si un anneau A contient $i\sqrt{n}$, il contient également 1 (il s'agit d'anneaux unitaires) et en conséquence il contient tout élément de la forme $a + ib\sqrt{n}$ avec $(a, b) \in \mathbb{Z}^2$. On a donc $\mathbb{Z}[i\sqrt{n}] \subset A$.
- (c) En désignant par $(A_i)_{i \in I}$ la famille de tous les sous anneaux de \mathbb{C} qui contiennent $i\sqrt{n}$, on a $A = \bigcap_{i \in I} A_i \subset \mathbb{Z}[i\sqrt{n}]$ puisque $\mathbb{Z}[i\sqrt{n}]$ est l'un de ces sous-anneaux et $\mathbb{Z}[i\sqrt{n}] \subset A$ puisque A est un anneau. On a donc bien $\mathbb{Z}[i\sqrt{n}] = A$.

2. Si $u = a + ib\sqrt{n}$ est inversible dans $\mathbb{Z}[i\sqrt{n}]$, il existe alors $v \in \mathbb{Z}[i\sqrt{n}]$ tel que $uv = 1$ et $|u|^2 |v|^2 = 1$ avec $|u|^2 = a^2 + nb^2 \in \mathbb{N}$ et $|v|^2 \in \mathbb{N}$, ce qui impose $|u|^2 = |v|^2 = 1$. On a donc $a^2 + nb^2 = 1$ avec $(a^2, b^2) \in \mathbb{N}^2$ et $n \geq 2$, ce qui équivaut à $b = 0$ et $a = \pm 1$. On a donc $\mathbb{Z}[i\sqrt{n}]^\times \subset \{-1, 1\}$. L'inclusion réciproque étant vérifiée pour tout anneau unitaire. On a donc :

$$\mathbb{Z}[i\sqrt{n}]^\times = \{u \in \mathbb{Z}[i\sqrt{n}] \mid |u| = 1\} = \{-1, 1\}.$$

3.

- (a) Dire que u/v dans $\mathbb{Z}[i\sqrt{n}]$ signifie qu'il existe $q \in \mathbb{Z}[i\sqrt{n}]$ tel que $v = qu$, ce qui entraîne $|v|^2 = |q|^2 |u|^2$ avec $|q|^2 \in \mathbb{N}$ et $|u|^2$ divise $|v|^2$ dans \mathbb{N} . De plus, pour v non nul, on a $q \neq 0$, donc $|q|^2 \geq 1$ dans \mathbb{N} et $|v|^2 \geq |u|^2$, ce qui revient à dire que $|u| \leq |v|$.
- (b) Si $u = 0$ ou $v = 0$ alors $u = v = 0$ et u, v sont bien associés.
On suppose donc que $u \neq 0$ et $v \neq 0$. On a $v = qu$ dans $\mathbb{Z}[i\sqrt{n}]^*$ avec $|u| = |v|$, donc $|q| = 1$ dans $\mathbb{Z}[i\sqrt{n}]$, ce qui équivaut à dire que $q \in \mathbb{Z}[i\sqrt{n}]^\times$. Il en résulte que u et v sont associés, ce qui entraîne que v divise u .
- (c) Dire que u/v et v/u dans $\mathbb{Z}[i\sqrt{n}]$ équivaut à dire que u et v sont associés dans $\mathbb{Z}[i\sqrt{n}]$, soit $v = \pm u$, ce qui entraîne $|u| = |v|$.
La réciproque est fautive. En effet, pour $u = 1 + i\sqrt{n}$ et $v = \bar{u} = 1 - i\sqrt{n}$, on a $|u| = |v| = \sqrt{n+1}$ et u, v ne sont pas associés puisque :

$$\frac{u}{v} = \frac{1 + i\sqrt{n}}{1 - i\sqrt{n}} = \frac{(1 + i\sqrt{n})^2}{1 + n} = \frac{1 - n}{1 + n} + \frac{2}{n + 1}i\sqrt{n} \notin \mathbb{Z}[i\sqrt{n}]$$

pour $n \geq 2$ ($\frac{2}{n+1} \notin \mathbb{Z}$).

4. Supposons que $|u|^2$ soit premier dans \mathbb{N} . Si $u = vw$ dans $\mathbb{Z}[i\sqrt{n}]$, on a alors $p = |u|^2 = |v|^2 |w|^2$ dans \mathbb{N} avec p premier, ce qui implique $|v|^2 = 1$ ou $|w|^2 = 1$, soit v ou w inversible dans $\mathbb{Z}[i\sqrt{n}]$. L'élément u est donc irréductible dans $\mathbb{Z}[i\sqrt{n}]$.
5. On procède par récurrence sur l'entiers $|u|^2 \geq 2$ (u est non nul et non inversible).
Si $|u|^2 = 2$, alors u est irréductible (2 est premier) et on a une décomposition avec $r = 1$.
Supposons le résultat acquis pour tous les éléments u de $\mathbb{Z}[i\sqrt{n}]$ tels que $|u|^2 \leq m - 1$ où $m \geq 3$ et soit $u \in \mathbb{Z}[i\sqrt{n}]$ tel que $|u|^2 = m$. Si u est irréductible c'est terminé avec $r = 1$. Sinon il existe v, w non inversibles dans $\mathbb{Z}[i\sqrt{n}]$ tels que $u = vw$ et on a $m = |u|^2 = |v|^2 |w|^2$ avec $|v|^2 \geq 2$ et $|w|^2 \geq 2$ dans \mathbb{N} , ce qui entraîne $2 \leq |v|^2 \leq m - 1$, $2 \leq |w|^2 \leq m - 1$ et v, w se décomposent en produit de facteurs irréductibles, ce qui donne une décomposition pour u .

6.

(a)

- i. Supposons que $2 = vw$ avec v, w non inversibles dans $\mathbb{Z}[i\sqrt{n}]$. On a alors $4 = |v|^2 |w|^2$ avec $|v|^2 \geq 2$ et $|w|^2 \geq 2$ dans \mathbb{N} , ce qui implique $|v|^2 = |w|^2 = 2$ ($|v|^2 = 1$ est exclu puisque v n'est pas inversible et $|v|^2 = 4$ donne $|w|^2 = 1$ qui est également exclu). En écrivant $v = a + ib\sqrt{n}$, on a alors $a^2 + nb^2 = 2$ avec $n \geq 3$, ce qui impose $b = 0$ et $a^2 = 2$ avec a entier, ce qui est impossible.
- ii. Supposons que $1 + i\sqrt{n} = vw$ avec v, w non inversibles dans $\mathbb{Z}[i\sqrt{n}]$. On a alors $1 + n = |v|^2 |w|^2$ avec $|v|^2 \geq 2$ et $|w|^2 \geq 2$ dans \mathbb{N} , ce qui implique $|v|^2 \leq n$ et $|w|^2 \leq n$. En écrivant $v = a + ib\sqrt{n}$, on a alors $a^2 + nb^2 \leq n$ avec $n \geq 3$. Pour $b \neq 0$, on a alors $a^2 + n \leq a^2 + nb^2 \leq n$ ce qui impose $a = 0$ et $nb^2 \leq n$ donne $b^2 = 1$, soit $|v| = 1$ qui contredit v non inversible. Pour $b = 0$, on a alors $aw = a(c + id\sqrt{n}) = 1 + i\sqrt{n}$ qui donne $ac = 1$ et $v = a = \pm 1$ qui contredit encore v non inversible.
- iii. $1 - i\sqrt{n}$ est également irréductible comme conjugué de $1 + i\sqrt{n}$.

(b) L'entier $n + 1 \geq 4$ étant pair s'écrit $n + 1 = 2^\alpha m$ avec $\alpha \geq 1$ et $m \geq 1$ impair.Si $m = 1$, alors :

$$1 + n = 2^\alpha = (1 + i\sqrt{n})(1 - i\sqrt{n})$$

ce qui donne deux décompositions différentes de $1 + n$.Si $m \geq 3$, il est alors non inversible dans $\mathbb{Z}[i\sqrt{n}]$ et en le décomposant en facteurs irréductibles dans $\mathbb{Z}[i\sqrt{n}]$, on a :

$$\begin{aligned} 1 + n &= (1 + i\sqrt{n})(1 - i\sqrt{n}) \\ &= 2^\alpha m = 2^\alpha \prod_{k=2}^r p_k^{\alpha_k} \end{aligned}$$

les p_k étant irréductibles dans $\mathbb{Z}[i\sqrt{n}]$ et différents de $1 \pm i\sqrt{n}$ (si par exemple, l'un des p_k vaut $1 + i\sqrt{n}$, $1 - i\sqrt{n}$ sera alors divisible par 2, ce qui contredit le fait qu'il est irréductible), ce qui donne deux décompositions différentes de $1 + n$.

(c) Prenons $u = 2$ qui est irréductible. Il divise $1 + n = (1 + i\sqrt{n})(1 - i\sqrt{n})$ qui est un entier pair et pourtant ne divise ni $v = 1 + i\sqrt{n}$, ni $w = 1 - i\sqrt{n}$ puisque v et w sont irréductibles.

En fait l'unicité dans la décomposition en facteurs irréductibles dans un anneau intègre équivaut à la propriété de Gauss : « u irréductible divise vw entraîne u divise v ou u divise w ».

7. Soit I un idéal de A . Si $I = \{0\}$, il est principal. On suppose que $I \neq \{0\}$ et on pose :

$$n = \inf \{N(u) \mid u \in I \setminus \{0\}\}.$$

Cette borne inférieure existe puisque $P = \{N(u) \mid u \in I \setminus \{0\}\}$ est une partie non vide de \mathbb{N} et de plus elle est atteinte, c'est-à-dire qu'il existe u_0 dans $I \setminus \{0\}$ tel que $n = N(u_0)$. En effectuant la division euclidienne d'un élément u de I par u_0 , on a $u = qu_0 + r$ avec q, r dans A et $r = 0$ ou $N(r) < N(u_0)$, ce qui entraîne $r = 0$ puisque u_0 est de stathme minimal dans $I \setminus \{0\}$. Tout élément u de I s'écrit donc $u = qu_0$ et $I \subset u_0A$. Comme par ailleurs $u_0A \subset I$ puisque I est un idéal, on a $I = u_0A$.

En définitive, A est principal.

8. Comme l'anneau A est principal, l'idéal $uA + vA$ est engendré par un élément δ (un pgcd de u et v dans A), soit $uA + vA = \delta A$. De $u \in \delta A$, on déduit que δ divise u , donc δ est soit inversible, soit associé à u , puisque u est irréductible. Dans le cas où δ est inversible, on a $\delta A = A$, donc $1 \in uA + vA$, soit $1 = \alpha u + \beta v$ avec α, β dans A et u divise $w = \alpha u + \beta v$. Dans le cas où δ est associé à u , on a $\delta A = uA$, donc $v \in uA$ et u divise v .

Par récurrence, on déduit que si u irréductible divise un produit $\prod_{k=1}^r v_k$, il divise alors l'un des v_k .

9.

- (a) Si $i\sqrt{n} = uv$ avec u, v non inversibles, en écrivant que $u = a + ib\sqrt{n}$, on déduit que $n = |i\sqrt{n}|^2$ est divisible par $a^2 + nb^2 \geq 2$. Si $b = 0$, en écrivant que $v = c + id\sqrt{n}$, on a alors :

$$i\sqrt{n} = ac + iad\sqrt{n}$$

et $ad = 1$, soit $|a| = 1$ qui contredit $a^2 + nb^2 \geq 2$. Si $b \neq 0$, on a alors $nb^2 \leq a^2 + nb^2 \leq n$ ce qui entraîne $|b| = 1$ et $a = 0$, soit $u = \pm 1$, en contradiction avec u inversible. Donc $i\sqrt{n}$ est irréductible dans $\mathbb{Z}[i\sqrt{n}]$.

- (b) Il suffit de montrer que $\mathbb{Z}[i\sqrt{n}]$ n'est pas principal.

Pour $n \geq 3$ impair, on a vu en **I.6c** que $\mathbb{Z}[i\sqrt{n}]$ ne satisfait pas à la condition de Gauss, il ne peut donc être principal.

Si $n \geq 4$ est pair, il s'écrit $n = 2m$ avec $m \geq 2$. Avec :

$$2(m + i\sqrt{n}) = n + 2i\sqrt{n} = i\sqrt{n}(2 - i\sqrt{n})$$

on déduit que l'irréductible $i\sqrt{n}$ divise le produit $2(m + i\sqrt{n})$ sans diviser $v = 2$ ou $m + i\sqrt{n}$. En effet, les multiples de $i\sqrt{n}$ sont de la forme :

$$i\sqrt{n}(a + ib\sqrt{n}) = -nb + ia\sqrt{n} = -2mb + ia\sqrt{n}$$

et les égalités $-2mb = 2$ ou $-2mb = m$ sont impossibles.

10. Pour $n = 1$, c'est déjà fait en partie **II**.

Pour $n = 2$, c'est la même démonstration.

Soient u, v non nuls dans $\mathbb{Z}[i\sqrt{2}]$ et $z = \frac{u}{v} = x + iy\sqrt{2}$ avec $(x, y) \in \mathbb{R}^2$. En utilisant

la partition $\mathbb{R} = \bigcup_{n \in \mathbb{Z}} \left[n - \frac{1}{2}, n + \frac{1}{2} \right]$, on peut trouver un unique couple (a, b) d'entiers relatifs tels que :

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2} \right] \times \left[b - \frac{1}{2}, b + \frac{1}{2} \right]$$

et en notant $q = a + ib\sqrt{2}$, on a $q \in \mathbb{Z}[i\sqrt{2}]$ et :

$$\begin{aligned}\left|\frac{u}{v} - q\right|^2 &= \left|(x - a) + i(y - b)\sqrt{2}\right|^2 \\ &= (x - a)^2 + 2(y - b)^2 \leq \frac{1}{4} + \frac{2}{4} < 1\end{aligned}$$

ou encore $|u - qv| < |v|$. En posant $r = u - qv$, on a bien $r \in \mathbb{Z}[i\sqrt{2}]$ et $|r| < |v|$.

Nombres de Fibonacci

30.1 Énoncé

On définit la suite de Fibonacci $(u_n)_{n \in \mathbb{N}}$ par :

$$\begin{cases} u_0 = 0, u_1 = 1 \\ \forall n \in \mathbb{N}^*, u_{n+1} = u_{n-1} + u_n \end{cases}$$

1. Montrer que pour tout $n \in \mathbb{N}^*$, u_n est un entier naturel non nul.
2. Montrer que l'ensemble E des suites réelles $x = (x_n)_{n \in \mathbb{N}}$ qui vérifient la relation de récurrence :

$$\forall n \in \mathbb{N}^*, x_{n+1} = x_{n-1} + x_n \quad (30.1)$$

est un espace vectoriel de dimension 2.

3. Soit r un réel non nul. Montrer que la suite $x = (r^n)_{n \in \mathbb{N}}$ est dans E si, et seulement si, r est racine du polynôme :

$$P(X) = X^2 - X - 1.$$

4. Montrer que P a deux racines réelles distinctes $r_1 < r_2$ et déterminer ces dernières.
5. Montrer que si u est la suite des nombres de Fibonacci, alors :

$$\forall n \in \mathbb{N}, u_n = \frac{1}{\sqrt{5}} (r_2^n - r_1^n). \quad (30.2)$$

6. Lorsque n tend vers l'infini, donner un équivalent simple de u_n en fonction de r_2 (r_2 est le nombre d'or).
7. Montrer de deux manières différentes que :

$$\forall n \in \mathbb{N}, u_{n+2} = 1 + \sum_{k=0}^n u_k.$$

8. Montrer que :

$$\forall n \in \mathbb{N}^*, u_{n-1}u_{n+1} - u_n^2 = (-1)^n \quad (30.3)$$

des deux manières suivantes :

- (a) en utilisant la formule (30.2) ;
- (b) en raisonnant par récurrence.

9. Montrer que, pour tout $n \in \mathbb{N}^*$, u_{n-1} et u_n sont premiers entre eux.
 10. Soient $m \geq n$ dans \mathbb{N} . Montrer que :

$$u_{m-n} = (-1)^n (u_m u_{n+1} - u_{m+1} u_n).$$

des deux manières suivantes :

- (a) en utilisant la formule (30.2);
 (b) en raisonnant par récurrence.
11. Pour tout $n \in \mathbb{N}^*$, on note $A_n = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}$.
 (a) Montrer que A_n est inversible dans $\mathcal{M}_2(\mathbb{Z})$.
 (b) Montrer que pour tout $n \in \mathbb{N}^*$ on a $A_n A_1 = A_{n+1}$ et retrouver la formule (30.3).
 (c) Montrer que pour tout n, m dans \mathbb{N}^* on a $A_n A_m = A_{n+m}$.
 (d) Montrer que pour tout n, m dans \mathbb{N}^* on a

$$u_{n+m} = u_m u_{n-1} + u_n u_{m+1} = u_m u_{n+1} + u_n u_{m-1}. \quad (30.4)$$

12. Soient n, m dans \mathbb{N}^* . Montrer que si m est un multiple de n alors u_m est multiple de u_n .
 13. Soient n, m dans \mathbb{N}^* .

- (a) Montrer que si $d \in \mathbb{N}^*$ est un diviseur commun à n et m , alors u_d est un diviseur commun à u_n et u_m .
 (b) En déduire que $u_{n \wedge m}$ divise $u_n \wedge u_m$.

14. Montrer que pour n, q dans \mathbb{N}^* on a :

$$\begin{cases} u_{qn} \equiv q u_n u_{n+1}^{q-1} (u_n^2) \\ u_{qn+1} \equiv u_{n+1}^q (u_n^2) \end{cases}$$

15. Soient n, m dans \mathbb{N}^* .

- (a) Montrer que $u_n \wedge u_m = u_n \wedge u_{m+n}$.
 (b) Montrer que $u_n \wedge u_m = u_n \wedge u_{m+qn}$ pour tout $q \geq 0$.
 (c) Montrer que :

$$u_n \wedge u_m = u_{n \wedge m}$$

(on peut raisonner par récurrence sur $s = n + m$).

16. Soient $m \geq n \geq 3$ dans \mathbb{N} . Montrer que m est un multiple de n si, et seulement si, u_m est multiple de u_n .
 17. Soient $m \geq n \geq 3$ dans \mathbb{N} . Montrer que m est multiple de nu_n si, et seulement si, u_m est multiple de u_n^2 .

30.2 Solution

1. On a $u_0 = 0$ et on vérifie facilement par récurrence sur $n \geq 1$ que $u_n \in \mathbb{N}^*$ pour tout $n \in \mathbb{N}^*$.
2. Il est facile de vérifier que E est un sous-espace vectoriel de l'espace des suites réelles. En effet la suite nulle vérifie la relation de récurrence (30.1) et si x, y vérifient cette relation, pour tous réels λ, μ , on a pour tout entier $n \geq 1$:

$$\begin{aligned}\lambda x_{n+1} + \mu y_{n+1} &= \lambda(x_{n-1} + x_n) + \mu(y_{n-1} + y_n) \\ &= (\lambda x_{n-1} + \mu y_{n-1}) + (\lambda x_n + \mu y_n)\end{aligned}$$

ce qui signifie que $\lambda x + \mu y \in E$.

L'application $\varphi : x \mapsto (x_0, x_1)$ est linéaire de E dans \mathbb{R}^2 et elle est bijective du fait qu'une suite x vérifiant (30.1) est uniquement déterminée par ses valeurs initiales x_0 et x_1 . L'application φ réalise donc un isomorphisme de E sur \mathbb{R}^2 et E est de dimension 2.

3. Dire que la suite $x = (r^n)_{n \in \mathbb{N}}$ est dans E équivaut à dire que :

$$\forall n \in \mathbb{N}^*, r^{n-1}(r^2 - r - 1) = 0$$

encore équivalent à dire que r est racine de P puisque $r \neq 0$.

4. Le discriminant de P est $\delta = 5$, il a donc deux racines réelles données par :

$$r_1 = \frac{1 - \sqrt{5}}{2} \text{ et } r_2 = \frac{1 + \sqrt{5}}{2}.$$

5. Les suites $x = (r_1^n)_{n \in \mathbb{N}}$ et $y = (r_2^n)_{n \in \mathbb{N}}$ sont dans E et linéairement indépendantes. En effet si $\lambda x + \mu y = 0$ (i. e. $\lambda r_1^n + \mu r_2^n = 0$ pour tout $n \in \mathbb{N}$) on a en particulier $\lambda + \mu = 0$, donc $\mu = -\lambda$ et $\lambda r_1 + \mu r_2 = 0$, soit $\lambda(r_1 - r_2) = 0$ et $\lambda = \mu = 0$ puisque $r_1 \neq r_2$. Ces deux suites forment donc une base de E . Il existe donc deux réels α et β uniquement déterminés tels que $u = \alpha x + \beta y$. Les réels α et β sont solutions du système linéaire :

$$\begin{cases} \alpha + \beta = 0 \\ \alpha r_1 + \beta r_2 = 1 \end{cases}$$

ce qui donne :

$$\alpha = \frac{1}{r_1 - r_2} = -\frac{1}{\sqrt{5}} \text{ et } \beta = -\alpha = \frac{1}{\sqrt{5}}.$$

On a donc :

$$\forall n \in \mathbb{N}, u_n = \frac{1}{\sqrt{5}}(r_2^n - r_1^n).$$

6. De $\frac{u_n}{r_2^n} = \frac{1}{\sqrt{5}} \left(1 - \left(\frac{r_1}{r_2}\right)^n\right)$ avec $\lim_{n \rightarrow +\infty} \left(\frac{r_1}{r_2}\right)^n = 0$ (on a $0 < \frac{r_1}{r_2} < 1$), on déduit que :

$$u_n \underset{n \rightarrow +\infty}{\sim} \frac{r_2^n}{\sqrt{5}} = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^n.$$

7. On peut procéder par récurrence sur $n \geq 0$. Pour $n = 0$, on a $u_2 = 1 = u_0 + 1$ et en supposant le résultat acquis au rang $n \geq 0$:

$$\begin{aligned}u_{n+3} &= u_{n+1} + u_{n+2} = u_{n+1} + 1 + \sum_{k=0}^n u_k \\ &= 1 + \sum_{k=0}^{n+1} u_k.\end{aligned}$$

On peut aussi utiliser la formule (30.2). Pour tout $n \in \mathbb{N}$ on a :

$$\begin{aligned} \sum_{k=0}^n u_k &= \frac{1}{\sqrt{5}} \left(\sum_{k=0}^n r_2^k - \sum_{k=0}^n r_1^k \right) \\ &= \frac{1}{\sqrt{5}} \left(\frac{1 - r_2^{n+1}}{1 - r_2} - \frac{1 - r_1^{n+1}}{1 - r_1} \right) \\ &= \frac{1}{\sqrt{5}} \frac{(1 - r_2^{n+1})(1 - r_1) - (1 - r_1^{n+1})(1 - r_2)}{(1 - r_2)(1 - r_1)} \\ &= \frac{1}{\sqrt{5}} \frac{(r_2 - r_1) - (r_2^{n+1} - r_1^{n+1}) + r_1 r_2 (r_2^n - r_1^n)}{1 - (r_1 + r_2) + r_1 r_2} \end{aligned}$$

avec :

$$r_1 + r_2 = 1, \quad r_1 r_2 = -1, \quad r_2 - r_1 = \sqrt{5}$$

ce qui donne :

$$\sum_{k=0}^n u_k = (u_n + u_{n+1}) - 1 = u_{n+2} - 1.$$

8.

(a) Pour tout $n \in \mathbb{N}^*$, on a :

$$\begin{aligned} u_{n-1}u_{n+1} - u_n^2 &= \frac{1}{5} \left((r_2^{n-1} - r_1^{n-1})(r_2^{n+1} - r_1^{n+1}) - (r_2^n - r_1^n)^2 \right) \\ &= -\frac{1}{5} (r_1 r_2)^{n-1} (r_2^2 + r_1^2 - 2r_1 r_2) \\ &= -\frac{1}{5} (r_1 r_2)^{n-1} (r_2 - r_1)^2 \end{aligned}$$

avec $r_1 r_2 = -1$ et $r_1 - r_2 = -\sqrt{5}$, ce qui donne :

$$u_{n-1}u_{n+1} - u_n^2 = -\frac{1}{5} (-1)^{n-1} (\sqrt{5})^2 = (-1)^n.$$

(b) En désignant par $(\delta_n)_{n \in \mathbb{N}^*}$ la suite définie par :

$$\forall n \in \mathbb{N}^*, \quad \delta_n = u_{n-1}u_{n+1} - u_n^2,$$

on a $\delta_1 = -1$ et pour $n \geq 2$:

$$\begin{aligned} \delta_n &= u_{n-1}(u_{n-1} + u_n) - u_n(u_{n-2} + u_{n-1}) \\ &= -(u_{n-2}u_n - u_{n-1}^2) = -\delta_{n-1}. \end{aligned}$$

On en déduit alors par récurrence sur $n \geq 1$ que :

$$\forall n \in \mathbb{N}^*, \quad \delta_n = (-1)^{n-1} \delta_1 = (-1)^n.$$

9. Le résultat précédent et le théorème de Bézout nous disent que pour tout $n \in \mathbb{N}^*$, u_{n-1} et u_n sont premiers entre eux.

10.

(a) Pour $m \geq n$ dans \mathbb{N} , on a :

$$u_{m-n} = \frac{1}{\sqrt{5}} (r_2^{m-n} - r_1^{m-n})$$

et

$$\begin{aligned} u_m u_{n+1} - u_{m+1} u_n &= \frac{1}{5} ((r_2^m - r_1^m) (r_2^{n+1} - r_1^{n+1}) - (r_2^{m+1} - r_1^{m+1}) (r_2^n - r_1^n)) \\ &= \frac{1}{5} (r_2 - r_1) (r_2^{m-n} - r_1^{m-n}) r_1^n r_2^n \\ &= \frac{1}{5} \sqrt{5} (r_2^{m-n} - r_1^{m-n}) (-1)^n = (-1)^n u_{m-n}. \end{aligned}$$

(b) On peut aussi procéder par récurrence sur $m \geq n$ à n fixé dans \mathbb{N} .

Pour $m = n$ et $m = n + 1$ le résultat est vrai. Supposons le acquis pour les entiers $n, n + 1, \dots, m \geq n + 1$. On a alors :

$$u_{m+1-n} = u_{m-n-1} + u_{m-n}$$

avec :

$$u_{m-n} = (-1)^n (u_m u_{n+1} - u_{m+1} u_n)$$

et :

$$u_{m-1-n} = (-1)^n (u_{m-1} u_{n+1} - u_m u_n)$$

ce qui donne :

$$\begin{aligned} u_{m+1-n} &= (-1)^n (u_{n+1} (u_m + u_{m-1}) - (u_m + u_{m+1}) u_n) \\ &= (-1)^n (u_{m+1} u_{n+1} - u_{m+2} u_n) \end{aligned}$$

soit le résultat au rang $m + 1$.

11.

(a) Pour tout $n \in \mathbb{N}^*$ on a :

$$\det(A_n) = u_{n-1} u_{n+1} - u_n^2 = (-1)^n$$

ce qui implique que la matrice A_n est inversible dans $\mathcal{M}_2(\mathbb{Z})$.

(b) Pour tout $n \in \mathbb{N}^*$ on a :

$$A_n A_1 = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} u_{n+2} & u_{n+1} \\ u_{n+1} & u_n \end{pmatrix} = A_{n+1}$$

et :

$$\det(A_{n+1}) = \det(A_n) \det(A_1) = -\det(A_n).$$

On en déduit alors par récurrence sur $n \geq 1$ que :

$$\det(A_n) = u_{n-1} u_{n+1} - u_n^2 = (-1)^n.$$

(c) On déduit du résultat précédent, par récurrence sur $m \geq 0$, n étant donné dans \mathbb{N}^* que $A_n A_m = A_{n+m}$.

Le résultat est vrai pour $m = 0$ et $m = 1$ et en le supposant vrai pour $m \geq 1$, on a :

$$A_n A_{m+1} = A_n A_m A_1 = A_{n+m} A_1 = A_{n+m+1}.$$

(d) De :

$$\begin{aligned} A_n A_m &= \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} u_{m+1} & u_m \\ u_m & u_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} u_m u_n + u_{m+1} u_{n+1} & u_m u_{n+1} + u_n u_{m-1} \\ u_m u_{n-1} + u_n u_{m+1} & u_m u_n + u_{m-1} u_{n-1} \end{pmatrix} \\ &= A_{n+m} = \begin{pmatrix} u_{n+m+1} & u_{n+m} \\ u_{n+m} & u_{n+m-1} \end{pmatrix} \end{aligned}$$

on déduit que :

$$u_{n+m} = u_m u_{n-1} + u_n u_{m+1} = u_m u_{n+1} + u_n u_{m-1}$$

(la dernière égalité peut aussi se déduire du fait que $u_{n+m} = u_{m+n}$).

12. Il s'agit de montrer que si $m = qn$ avec $q \geq 1$, alors u_m est multiple de u_n .

On procède par récurrence sur $q \geq 1$.

Pour $q = 1$, c'est évident.

En supposant le résultat acquis pour $q \geq 1$, en écrivant que :

$$u_{(q+1)n} = u_{qn+n} = u_{qn} u_{n-1} + u_n u_{qn+1}$$

on déduit que $u_{(q+1)n}$ est aussi multiple de u_n .

13.

(a) Si $d \in \mathbb{N}^*$ est un diviseur commun à n et m , on a alors $n = q_1 d$ et $m = q_2 d$ et le résultat précédent nous dit que u_d divise u_n et u_m .

(b) Comme $d = m \wedge n$ divise n et m , $u_d = u_{m \wedge n}$ divise u_n et u_m ainsi que leur pgcd $u_n \wedge u_m$.

14. On procède par récurrence sur $q \geq 1$ à n fixé dans \mathbb{N}^* .

Pour $q = 1$, le résultat est évident.

En le supposant vrai pour $q \geq 1$, on a :

$$\begin{aligned} u_{(q+1)n} &= u_{qn} u_{n-1} + u_n u_{qn+1} \equiv q u_n u_{n+1}^{q-1} u_{n-1} + u_n u_{qn+1} \pmod{u_n^2} \\ &\equiv q u_n u_{n-1} u_{n+1}^{q-1} + u_n u_{n+1}^q \pmod{u_n^2} \end{aligned}$$

avec $u_{n+1} = u_{n-1} + u_n \equiv u_{n-1}$ modulo u_n , ce qui donne $u_n u_{n-1} \equiv u_n u_{n+1}$ modulo u_n^2 et :

$$u_{(q+1)n} \equiv q u_n u_{n+1}^q + u_n u_{n+1}^q = (q+1) u_n u_{n+1}^q \pmod{u_n^2}$$

De manière analogue, on a :

$$\begin{aligned} u_{(q+1)n+1} &= u_{qn+1+n} = u_{qn+1} u_{n+1} + u_n u_{qn} \\ &\equiv u_{n+1}^q u_{n+1} + u_n q u_n u_{n+1}^{q-1} = u_{n+1}^{q+1} + q u_n^2 u_{n+1}^{q-1} \\ &\equiv u_{n+1}^{q+1} \pmod{u_n^2} \end{aligned}$$

15.

- (a) Soit $\delta = u_n \wedge u_m$. Comme δ divise u_n et u_m il divise u_{m+n} d'après la formule (30.4) et δ va diviser le pgcd de u_{m+n} et u_n . En notant δ' ce pgcd, il divise u_{m+n} et u_n donc $u_m u_{n-1}$ toujours d'après la formule (30.4). Comme u_n et u_{n-1} sont premiers entre eux, δ' est nécessairement premier avec u_{n-1} (un diviseur commun à δ' et u_{n-1} est aussi diviseur commun à u_n et u_{n-1} puisque δ' divise u_n) et le théorème de Gauss nous dit que δ' va diviser u_m . Donc δ' va diviser δ .

En définitive, $\delta = u_n \wedge u_m = u_n \wedge u_{m+n}$.

- (b) Par récurrence, on déduit que $u_n \wedge u_m = u_n \wedge u_{m+qn}$ pour tout $q \geq 0$.
En effet, c'est vrai pour $q = 0$ et $q = 1$ et supposant que c'est vrai pour $q \geq 1$, on a :

$$u_n \wedge u_m = u_n \wedge u_{m+qn} = u_n \wedge u_{m+qn+n} = u_n \wedge u_{m+(q+1)n}.$$

- (c) On raisonne par récurrence sur $s = n + m$.

Pour $s = 2$, on a $n = m = 1$ et le résultat est évident.

Supposons le résultat acquis pour tous les couples (n, m) d'entiers naturels non nuls tels que $n + m < s$, où $s \geq 2$. Soient n, m dans \mathbb{N}^* tels que $n + m = s$ et $d \in \mathbb{N}^*$ est un diviseur commun à u_n et u_m . Du fait de la commutativité du pgcd, on peut supposer que $m \geq n$. Par division euclidienne, on a $m = qn + r$ avec $0 \leq r < n$ et :

$$u_n \wedge u_m = u_n \wedge u_{qn+r} = u_n \wedge u_r$$

avec $n + r < m + r \leq m + n = s$. L'hypothèse de récurrence nous dit alors que $u_n \wedge u_r = u_{n \wedge r}$ avec $n \wedge r = n \wedge m$ (théorème 23.9). On a donc $u_n \wedge u_m = u_{n \wedge m}$.

16. On a déjà vu que si m est un multiple de n alors u_m est multiple de u_n (question 12).
Réciproquement supposons que $m \geq n \geq 3$ et u_m multiple de u_n . On a alors $u_n = u_n \wedge u_m = u_{n \wedge m}$ avec $n \wedge m \leq n$. Comme la suite $(u_n)_{n \geq 3}$ est strictement croissante avec $u_n > 1 = u_1$ pour $n \geq 3$, on a nécessairement $n \wedge m = n$, ce qui signifie que n divise m .
17. Supposons que m soit un multiple de nu_n , soit $m = qnu_n$. On a alors :

$$u_m = u_{(qu_n)n} \equiv (qu_n) u_n u_{n+1}^{q-1} = qu_n^2 u_{n+1}^{q-1} \equiv 0 \pmod{u_n^2}$$

et u_m est multiple de u_n^2 .

Réciproquement, supposons que u_m soit multiple de u_n^2 , il est alors multiple de u_n et m est multiple de n (question 16), soit $m = qn$. On a alors :

$$u_{qn} \equiv qu_n u_{n+1}^{q-1} \pmod{u_n^2}$$

et qu_{n+1}^{q-1} est multiple de u_n , c'est-à-dire que u_n qui est premier avec u_{n+1} divise qu_{n+1}^{q-1} , le théorème de Gauss nous dit alors que u_n divise q , soit $q = q'u_n$ et $m = q'nu_n$ est multiple de nu_n .

Infinitude de l'ensemble des nombres premiers

31.1 Énoncé

On se propose avec ce problème de donner plusieurs démonstration du théorème d'Euclide sur l'infinitude de l'ensemble \mathcal{P} des nombres premiers (partie **II**), puis d'en déduire quelques conséquences (partie **III**).

– I – Les nombres de Fermat

On appelle nombre de Fermat tout entier de la forme :

$$F_n = 2^{2^n} + 1$$

où n est un entier naturel.

1. Montrer que pour tout $n \in \mathbb{N}$, F_{n+1} et F_n sont premiers entre eux.
2. Montrer que pour $n \neq m$ dans \mathbb{N} , F_n et F_m sont premiers entre eux.
3. Montrer que pour $n \neq m$ dans \mathbb{N} et p dans \mathbb{N}^* , F_n^p et F_m^p sont premiers entre eux.
4. On considère la suite d'entiers naturels $(G_n)_{n \in \mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N}, G_n = 2^{3^n} + 1.$$

- (a) Montrer que dans cette suite, seul G_0 est premier.
- (b) Montrer que, pour $n \in \mathbb{N}$, G_n est divisible par 3^{n+1} .
5. Soient $m \geq 1$ et $a \geq 2$ deux entiers. Montrer que si $p = a^m + 1$ est premier, alors a est pair et il existe un entier $n \geq 0$ tel que $m = 2^n$, c'est-à-dire que $p = 2^{2^n} b^{2^{2^n}} + 1$ avec $b \geq 1$ et dans le cas où $b = 1$, p est un nombre de Fermat premier (par exemple pour $n = 0, 1, 2, 3, 4$). Comme pour les nombre de Fermat, on peut vérifier que pour tout entier pair $a \geq 2$, les entiers $u_n = a^{2^n} + 1$ sont deux à deux premiers entre eux.
6. Soit p un diviseur premier d'un nombre de Fermat F_n avec $n \geq 0$. Montrer que p est soit égal à F_n , soit de la forme $p = 2^{n+1}q + 1$, où q admet un diviseur premier impair.
7. Montrer que, pour tout $n \geq 2$, le chiffre des unités de F_n est égal à 7.

– II – Infinitude de l'ensemble \mathcal{P} des nombres premiers

On se propose ici de donner plusieurs démonstration du théorème d'Euclide sur l'infinitude de l'ensemble \mathcal{P} des nombres premiers.

Pour tout entier naturel non nul p , on note $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Preuve 1 Rappeler la démonstration d'Euclide de l'infinitude de l'ensemble \mathcal{P} des nombres premiers.

Preuve 2 Montrer que pour tout entier naturel n , on peut trouver un nombre premier p plus grand que n . Conclure.

Pour les questions **3. 4. 5. 6. 7.** et **8.** on suppose que \mathcal{P} est fini et on note $p_1 = 2 < \dots, < p_r$ tous ses éléments (p_r et donc le plus grand nombre premier).

Pour tout réel x , on note $[x]$ sa partie entière.

Preuve 3 Pour tout entier k compris entre 1 et r , on note $n = \prod_{k=1}^r p_k = p_k q_k$. En utilisant les diviseurs premiers de $S = \sum_{k=1}^r q_k$, montrer qu'on aboutit à une contradiction et conclure.

Preuve 4 En utilisant la décomposition en facteurs premiers, montrer que pour tout entier $n \geq 1$ on a $2^n \leq (n+1)^r$ et conclure.

Preuve 5 Soit n un entier naturel non nul.

(a) Soit m un entier compris entre 1 et p_r^n . Montrer que si $m = \prod_{k=1}^r p_k^{\alpha_k}$ est la décomposition

en nombres premiers de m , alors $\alpha_k \leq \left\lfloor n \frac{\ln(p_r)}{\ln(p_k)} \right\rfloor$.

(b) En déduire que $p_r^n \leq n^r \left(\frac{\ln(p_r)}{\ln(2)} + 1 \right)^r$ et conclure.

Preuve 6

(a) Montrer, le plus simplement possible, que la série $\sum \frac{1}{n^2}$ est convergente de somme $S \in]0, 2[$.

(b) Pour $n > \prod_{k=1}^r p_k$, on partitionne l'ensemble $E = \{1, 2, \dots, n\}$ en distinguant les entiers compris entre 1 et n qui sont sans facteurs carrés (i. e. de la forme $\prod_{k=1}^r p_k^{\varepsilon_k}$ où $(\varepsilon_1, \dots, \varepsilon_r) \in \{0, 1\}^r$) de ceux qui sont divisibles par le carré d'un nombre premier, soit $E = E_1 \cup E_2$, où :

$$E_1 = \left\{ m \in E \mid m = \prod_{k=1}^r p_k^{\varepsilon_k} \text{ où } (\varepsilon_1, \dots, \varepsilon_r) \in \{0, 1\}^r \right\}$$

$$E_2 = \{ m \in E \mid \exists p_k \in \mathcal{P} \text{ tel que } p_k^2 \text{ divise } m \}$$

i. Montrer que, pour k compris entre 1 et r , il y a au plus $\left\lfloor \frac{n}{p_k^2} \right\rfloor$ entiers m dans E divisibles par p_k^2 .

ii. En déduire que $n < 2^r + n(S-2)$ et conclure.

Preuve 7

- (a) Soient x un réel strictement supérieur à 1, n un entier naturel compris entre 1 et x et $n = \prod_{k=1}^r p_k^{\alpha_k}$ la décomposition en facteurs premiers de n où les α_k sont des entiers positifs ou nuls. Montrer que pour tout k compris entre 1 et r , on a :

$$\alpha_k \leq \left\lfloor \frac{\ln(x)}{\ln(p_k)} \right\rfloor.$$

- (b) En déduire que pour tout réel $x > 1$, on a :

$$x < \left(\frac{\ln(2x)}{\ln(2)} \right)^r + 1$$

et conclure.

Preuve 8 Montrer que si p est un diviseur premier de $m = 2^{p_r} - 1$, alors $\bar{2}$ est d'ordre p_r dans le groupe multiplicatif \mathbb{Z}_p^* et conclure.

Preuve 9

- (a) Soit p un nombre premier impair. On se propose de montrer que $-\bar{1}$ est un carré dans \mathbb{Z}_p si, et seulement si, p est congru à 1 modulo 4.
- i. Montrer que si $p \equiv 3 \pmod{4}$, alors $-\bar{1}$ n'est pas un carré dans \mathbb{Z}_p (ce qui revient à dire que l'équation $x^2 + \bar{1} = 0$ n'a pas de solutions dans \mathbb{Z}_p).
 - ii. Montrer que si $p \equiv 1 \pmod{4}$, alors l'équation $x^2 + \bar{1} = 0$ a deux solutions dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ qui sont $\overline{-r!}$ et $\overline{r!}$ où $r = \frac{p-1}{2}$ ($-\bar{1}$ est alors un carré dans \mathbb{Z}_p).

- (b) On note :

$$\begin{aligned} \mathcal{P}_1 &= \{p \in \mathcal{P} \mid \exists n \in \mathbb{N} ; p = 4n + 3\} \\ \mathcal{P}_2 &= \{p \in \mathcal{P} \mid \exists n \in \mathbb{N}^* ; p = 4n + 1\} \end{aligned}$$

- i. Montrer que \mathcal{P}_1 est infini. Conclure.
- ii. Montrer que \mathcal{P}_2 est infini. Conclure.

De manière plus générale on peut montrer que si a et b sont deux entiers premiers entre eux alors il existe une infinité de nombres premiers de la forme $an + b$ (théorème de Dirichlet).

Preuve 10

- (a) Montrer que si on dispose d'une suite $(u_n)_{n \in \mathbb{N}}$ strictement croissante d'entiers naturels différents de 0 et 1 et deux à deux premiers entre eux, on peut alors en déduire que \mathcal{P} infini.
- (b) En utilisant les nombres de Fermat, montrer que \mathcal{P} infini.
- (c) Soient a, b deux entiers naturels non nuls premiers entre eux avec $b > a$. On définit la suite $(u_n)_{n \in \mathbb{N}}$ par :

$$\begin{cases} u_0 = b \\ \forall n \geq 1, u_n - a = u_{n-1} (u_{n-1} - a) \end{cases}$$

- i. Montrer que $(u_n)_{n \in \mathbb{N}}$ est une suite strictement croissante d'entiers naturels différents de 0 et 1.
- ii. Montrer que pour tous $m > n \geq 0$, on a :

$$u_m \equiv a \pmod{u_n}$$

- iii. Montrer que, pour tout $n \geq 0$, u_n est premier avec a .
 - iv. Montrer que les u_n sont deux à deux premiers entre eux. Conclure.
 - v. Que retrouve-t-on pour $(a, b) = (2, 3)$.
- (d) Soit a un entiers naturel impair supérieur ou égal à 3. On définit la suite $(u_n)_{n \in \mathbb{N}}$ par :

$$\begin{cases} u_0 = a \\ \forall n \geq 1, u_n = u_{n-1}^2 - 2 \end{cases}$$

- i. Montrer que $(u_n)_{n \in \mathbb{N}}$ est une suite strictement croissante d'entiers naturels impairs.
- ii. Montrer que, pour tout entier naturel n , on a :

$$\begin{cases} u_{n+1} \equiv -2 \pmod{u_n} \\ \forall m \geq n+2, u_m \equiv 2 \pmod{u_n} \end{cases}$$

- iii. Montrer que les u_n sont deux à deux premiers entre eux. Conclure.

Preuves 11 Connaissez vous d'autres démonstrations du théorème d'Euclide ?

– III – Quelques applications

1. On note $2 = p_1 < p_2 < \dots < p_n < \dots$ la suite infini des nombres premiers et on se propose de montrer que $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$. Pour ce faire, on raisonne par l'absurde en supposant que la série à termes positifs $\sum \frac{1}{p_n}$ est convergente. Pour tout $n \geq 1$, on note :

$$R_n = \sum_{k=n+1}^{+\infty} \frac{1}{p_k}$$

le reste d'ordre n de cette série.

- (a) Montrer qu'il existe un entier $r \geq 1$ tel que :

$$\forall n \geq r, 0 < R_n < \frac{1}{2}.$$

On note $\mathcal{P}_1 = \{p_1, \dots, p_r\}$ et $\mathcal{P}_2 = \{p_k \mid k \geq r+1\}$.

- (b) Pour tout entier naturel non nul N , on partitionne l'ensemble $E = \{1, 2, \dots, N\}$ en distinguant les entiers compris entre 1 et N qui ont tous leurs diviseurs premiers dans \mathcal{P}_1 de ceux qui ont au moins un diviseur dans \mathcal{P}_2 , soit $E = E_1 \cup E_2$, où :

$$E_1 = \left\{ n \in E \mid n = \prod_{k=1}^r p_k^{\alpha_k} \text{ où } (\alpha_1, \dots, \alpha_r) \in \mathbb{N}^r \right\}$$

$$E_2 = \{n \in E \mid \exists p_k \in \mathcal{P}_2 \text{ qui divise } n\}$$

- i. En écrivant tout entier n dans E_1 sous la forme $n = pq^2$ où p, q sont deux entiers naturels non nul, l'entier p étant égal à 1 ou sans facteurs carrés (i. e. $p = \prod_{k=1}^r p_k^{\varepsilon_k}$ où $(\varepsilon_1, \dots, \varepsilon_r) \in \{0, 1\}^r$), montrer que :

$$N_1 \leq 2^r \left[\sqrt{N} \right]$$

($[\cdot]$ désigne la partie entière).

- ii. Montrer que pour tout p_k dans \mathcal{P}_2 , il y a au plus $\left[\frac{N}{p_k} \right]$ entiers n dans E divisibles par p_k et en déduire que :

$$N_2 < \frac{N}{2}.$$

- iii. Montrer que pour N assez grand, on a $N_1 + N_2 < N$ et conclure.

Si Q est un polynôme à coefficients entiers relatifs de degré supérieur ou égal à 1 et p un nombre premier, on dit que p divise Q s'il existe un entier relatif a tel que p divise $Q(a)$.

2. On se propose de montrer dans cette question le théorème de Schur suivant : tout polynôme non constant à coefficients entiers relatifs admet une infinité de diviseurs premiers.
- (a) Montrer que tout polynôme à coefficients entiers relatifs non constant admet des diviseurs premiers.
- (b) Montrer que tout polynôme Q à coefficients entiers relatifs non constant tel que $Q(0) = 0$ admet une infinité des diviseurs premiers.
- (c) Soit :

$$Q(X) = \sum_{k=0}^n a_k X^k$$

un polynôme à coefficients entiers relatifs de degré $n \geq 1$ non nul en 0.

On suppose que l'ensemble des diviseurs premiers de Q est fini et on le note :

$$\mathcal{P}_Q = \{p_1, \dots, p_r\}.$$

On note aussi $m = \prod_{k=1}^r p_k$.

- i. Montrer qu'il existe un polynôme $R(X) = \sum_{k=1}^n b_k X^k$ de degré n dans $\mathbb{Z}[X]$ tel que $Q(a_0 m X) = a_0 (1 + R(X))$, chaque coefficient b_k , pour k compris entre 1 et r , étant divisible par m .
- ii. En utilisant les diviseurs premiers de $1 + R$, montrer qu'on aboutit à une contradiction et conclure.
3. En utilisant le polynôme $Q(X) = 4X^2 + 1$, retrouver le fait qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Pour tout entier naturel $n \in \mathbb{N}^*$, on note $\omega_n = \exp\left(\frac{2i\pi}{n}\right)$ et on définit le polynôme cyclotomique Φ_n par :

$$\Phi_n(X) = \prod_{\substack{k=1 \\ k \wedge n = 1}}^n (X - \omega_n^k)$$

(les ω_n^k pour k premier avec n et $1 \leq k \leq n$ sont les racines primitives n -ième de l'unité). Pour tout entier naturel $n \in \mathbb{N}^*$, on note \mathcal{D}_n l'ensemble des diviseurs de n dans \mathbb{N}^* .

On admet les résultats suivants :

— pour tout $n \in \mathbb{N}^*$ on a :

$$X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d(X)$$

— pour tout $n \in \mathbb{N}^*$, Φ_n est un polynôme à coefficients entiers.

Soient $n \geq 2$ un entier naturel et p un nombre premier ne divisant pas n . On se propose de montrer dans les deux questions qui suivent que p divise Φ_n si, et seulement si, p est congru à 1 modulo n .

4. On se donne un entier $n \geq 2$ et un nombre premier p qui divise Φ_n .

(a) Montrer qu'il existe un entier naturel a tel que l'ordre d de \bar{a} dans le groupe multiplicatif \mathbb{Z}_p^* soit un diviseur de n .

(b) Montrer que si $d = n$, alors p est congru à 1 modulo n .

(c) On suppose que $d < n$.

i. Montrer que $a^n - 1$ est divisible par p^2 .

ii. Montrer que, pour tout entier $m \geq 1$, on a :

$$\Phi_m(a + p) \equiv \Phi_m(a) \pmod{p}.$$

iii. Montrer que $(a + p)^n - 1$ est divisible par p^2 .

iv. Montrer que $na^{n-1}p$ est divisible par p^2 et que si on suppose de plus p est premier avec n , on aboutit alors à une contradiction.

(d) Conclure.

5. Montrer que si p est un nombre premier congru à 1 modulo n , alors p divise Φ_n .

6. Dédurre de ce qui précède, le cas particulier suivant du théorème de Dirichlet : pour tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $1 + kn$ où $k \in \mathbb{N}^*$.

31.2 Solution

– I – Les nombres de Fermat

1. On a :

$$F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (F_n - 1)^2 + 1.$$

Le pgcd de F_n et F_{n+1} divise F_n et $F_{n+1} = F_n^2 - 2F_n + 2$, il divise donc 2 et comme il divise F_n qui est impair ce pgcd vaut 1, c'est-à-dire que F_n et F_{n+1} sont premiers entre eux.

2. On vérifie tout d'abord par récurrence, que pour tout $n \geq 0$, on a $F_{n+1} = \prod_{k=0}^n F_k + 2$.

Pour $n = 0$, on a :

$$F_1 = 2^2 + 1 = 5 = F_0 + 2.$$

En supposant le résultat acquis pour $n - 1 \geq 0$, on a :

$$F_{n+1} = F_n(F_n - 2) + 2 = F_n \prod_{k=0}^{n-1} F_k + 2 = \prod_{k=0}^n F_k + 2.$$

Supposons que $m > n$.

On a :

$$\begin{aligned} F_m &= \prod_{k=0}^{m-1} F_k + 2 = F_n \prod_{\substack{k=0 \\ k \neq n}}^{m-1} F_k + 2 \\ &= qF_n + 2 \end{aligned}$$

Le pgcd de F_n et F_m divise alors 2 et comme il divise F_n qui est impair ce pgcd vaut 1, c'est-à-dire que F_n et F_m sont premiers entre eux.

3. Avec $F_n^p \wedge F_m^p = (F_n \wedge F_m)^p$ pour tout $p \geq 1$, on déduit pour $n \neq m$ F_n^p et F_m^p sont premiers entre eux.

4.

(a) On a $G_0 = 3$ qui est premier. En utilisant l'identité :

$$a^3 + 1 = (a + 1)(a^2 - a + 1)$$

on a, pour tout $n \in \mathbb{N}$:

$$\begin{aligned} G_{n+1} &= 2^{3^{n+1}} + 1 = (2^{3^n})^3 + 1 \\ &= (2^{3^n} + 1) \left((2^{3^n})^2 - 2^{3^n} + 1 \right) \\ &= G_n \left((2^{3^n})^2 - 2^{3^n} + 1 \right) = G_n q_n \end{aligned}$$

avec $G_n \geq 2$ et $q_n = (2^{3^n})^2 - 2^{3^n} + 1 \geq 2$ pour tout $n \in \mathbb{N}$. Il en résulte que G_{n+1} n'est pas premier.

(b) On a $G_0 = 3$ et $G_1 = 9 = 3^2$.Avec $2^{3^n} \equiv (-1)^{3^n}$ modulo 3 et 3^n impair, on déduit que $2^{3^n} \equiv -1$ modulo 3 et :

$$q_n = (2^{3^n})^2 - 2^{3^n} + 1 \equiv (-1)^2 - (-1) + 1 = 3 \equiv 0 \pmod{3}$$

c'est-à-dire que q_n est divisible par 3 et en supposant que G_n est divisible par 3^{n+1} , on déduit que G_{n+1} est divisible par 3^{n+2} . On a donc ainsi montré par récurrence que pour tout $n \in \mathbb{N}$, G_n est divisible par 3^{n+1} .

5. Supposons que a soit impair, on a donc $a \geq 3$ et $a^m + 1$ est un nombre pair supérieur ou égal à 4, il ne peut être premier. L'entier a est donc nécessairement pair.

En utilisant la décomposition en facteurs premiers, on a $m = 2^n(2q + 1)$ où n et q sont deux entiers naturels. Supposons $q \geq 1$, on a alors :

$$\begin{aligned} a^m + 1 &= (a^{2^n})^{2q+1} + 1 = b^{2q+1} + 1 \\ &= (b + 1)(b^{2q} - b^{2q-1} + b^{2q-2} - \dots + 1) \\ &= (b + 1) \sum_{k=0}^{2q} (-1)^k b^{2q-k} = (b + 1) S \end{aligned}$$

avec $b + 1 = a^{2^n} + 1 \geq 2$ et $S = \frac{a^m + 1}{b + 1} = \frac{b^{2q+1} + 1}{b + 1} \geq 2$ (c'est équivalent à $b(b^{2q} - 2) \geq 1$ qui est vérifié puisque $b = a^{2^n} \geq a \geq 2$ et $q \geq 1$) et l'entier $a^m + 1$ n'est pas premier.

6. Supposons que $F_n = 2^{2^n} + 1 = pq_n$ avec p premier et q_n entier naturel non nul. Comme F_n est impair, on a nécessairement $p \geq 3$. On a alors $\overline{F_n} = \overline{0}$ dans $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

On a donc $\overline{2^{2^n}} = -\overline{1}$ dans \mathbb{Z}_p et $\overline{2^{2^{n+1}}} = (\overline{2^{2^n}})^2 = (-\overline{1})^2 = \overline{1}$ et l'ordre de $\overline{2}$ dans le groupe multiplicatif \mathbb{Z}_p^* est un diviseur de 2^{n+1} , donc de la forme 2^k avec $1 \leq k \leq n + 1$, mais avec $\overline{2^{2^n}} = -\overline{1} \neq \overline{1}$ (puisque $p \neq 2$) on déduit que cet ordre est exactement 2^{n+1} .

Par ailleurs, on sait que l'ordre d'un élément dans un groupe divise l'ordre du groupe (théorème de Lagrange), donc 2^{n+1} est un diviseur de $p - 1 = \text{card}(\mathbb{Z}_p^*)$, ce qui peut se traduire par $p - 1$ congru à 0 modulo 2^{n+1} ou encore p congru à 1 modulo 2^{n+1} .

Dire que p est congru à 1 modulo 2^{n+1} signifie qu'il existe un entier $q \geq 1$ tel que $p = 2^{n+1}q + 1$. Si q n'admet aucun diviseur premier impair, il est de la forme $q = 2^m$ avec

$m \geq 0$ et $p = 2^{n+1+m} + 1$ est premier, ce qui impose que $n + 1 + m = 2^r$ (question **I.5.**), c'est-à-dire que $p = 2^{2^r} + 1$ est un nombre de Fermat et $p = F_n$ puisque deux nombres de Fermat distincts sont premiers entre eux.

Pour $n = 0, 1, 2, 3, 4$, on vérifie que F_n est premier.

Pour $n = 5$, les diviseurs premiers de F_5 sont de la forme $p = 2^6 q + 1$. Les valeurs possibles de q , non puissance de 2, sont $q = 3, 5, 7, 9, 10, \dots$ et on vérifie que pour $q = 10$, $p = 641$ est un diviseur premier de F_5 , donc F_5 n'est pas premier.

7. Pour $n = 2$, on a $F_2 = 17$. En supposant que, pour $n \geq 2$, F_n est congru à 7 modulo 10 (équivalent à dire que 7 est le chiffre des unités de F_n), on a :

$$F_{n+1} = (F_n - 1)^2 + 1 \equiv 6^2 + 1 = 37 \equiv 7 \pmod{10}.$$

– II – Infinitude de l'ensemble \mathcal{P} des nombres premiers

Preuve 1 On sait déjà que \mathcal{P} est non vide (il contient 2). Supposons que \mathcal{P} soit fini avec :

$$\mathcal{P} = \{p_1, \dots, p_r\}.$$

L'entier $n = p_1 \cdots p_r + 1$ est supérieur ou égal à 2, il admet donc un diviseur premier $p_k \in \mathcal{P}$. L'entier p_k divise alors $n = p_1 \cdots p_r + 1$ et $p_1 \cdots p_r$, il divise donc la différence qui est égale à 1, ce qui est impossible. En conclusion \mathcal{P} est infini.

Preuve 2 Pour tout $n \in \mathbb{N}$, l'entier $m = n! + 1 \geq 2$ admet un diviseur premier p_n . Si $p_n < n$ alors p_n est un diviseur de $n!$, donc de $1 = m - n!$, ce qui est impossible. On a donc ainsi une suite strictement croissante $(p_n)_{n \in \mathbb{N}}$ de nombres premiers, ce qui implique que \mathcal{P} est infini.

Preuve 3 Si p est un diviseur premier de S , c'est l'un des p_k avec k compris entre 1 et r . En remarquant que pour j compris entre 1 et r différent de k , $q_j = \frac{n}{p_j}$ est divisible par p_k , on déduit que p_k va diviser $q_k = S - \sum_{\substack{j=1 \\ j \neq k}}^r q_j$ et pourtant $q_k = \frac{n}{p_k}$ n'est pas divisible par p_k (p_k est premier avec tous les p_j pour $j \neq k$, donc avec leur produit n_k). On aboutit donc ainsi à une contradiction. Il en résulte que \mathcal{P} est infini.

Preuve 4 Tout entier m compris entre 1 et 2^n s'écrit $m = \prod_{k=1}^r p_k^{\alpha_k}$, où les α_k sont des entiers positifs ou nuls. Pour k compris entre 1 et r , on a $p_k^{\alpha_k} \leq m \leq 2^n$ et nécessairement $\alpha_k \leq n$ (si $\alpha_k > n$, alors $p_k^{\alpha_k} \geq 2^{\alpha_k} > 2^n$) et donc :

$$E = \{1, 2, \dots, 2^n\} \subset F = \left\{ \prod_{k=1}^r p_k^{\alpha_k} \mid (\alpha_1, \dots, \alpha_r) \in \{0, 1, \dots, n\}^r \right\}$$

ce qui entraîne :

$$2^n = \text{card}(E) \leq \text{card}(F) = (n+1)^r$$

l'entier naturel non nul n étant quelconque, ce qui est en contradiction avec $\lim_{n \rightarrow +\infty} \frac{2^n}{(n+1)^r} = +\infty$.

Il en résulte que \mathcal{P} est infini.

Preuve 5

(a) De $p_k^{\alpha_k} \leq m = \prod_{j=1}^r p_j^{\alpha_j} \leq p_r^n$, on déduit que $\alpha_k \ln(p_k) \leq n \ln(p_r)$ et :

$$\alpha_k \leq n \frac{\ln(p_r)}{\ln(p_k)} \leq n \frac{\ln(p_r)}{\ln(2)} < \left[n \frac{\ln(p_r)}{\ln(2)} \right] + 1$$

$$\text{et } \alpha_k \leq \left[n \frac{\ln(p_r)}{\ln(2)} \right].$$

(b) On a donc :

$$\{1, 2, \dots, p_r^n\} \subset \left\{ \prod_{k=1}^r p_k^{\alpha_k} \mid 0 \leq \alpha_1, \dots, \alpha_r \leq \left[n \frac{\ln(p_r)}{\ln(2)} \right] \right\}$$

et :

$$\begin{aligned} p_r^n &\leq \left(\left[n \frac{\ln(p_r)}{\ln(2)} \right] + 1 \right)^r \leq \left(n \frac{\ln(p_r)}{\ln(2)} + 1 \right)^r = n^r \left(\frac{\ln(p_r)}{\ln(2)} + \frac{1}{n} \right)^r \\ &\leq n^r \left(\frac{\ln(p_r)}{\ln(2)} + 1 \right)^r \end{aligned}$$

ou encore :

$$\frac{p_r^n}{n^r} \leq \left(\frac{\ln(p_r)}{\ln(2)} + 1 \right)^r$$

l'entier $n \geq 1$ étant quelconque, ce qui est incompatible avec $\lim_{n \rightarrow +\infty} \frac{p_r^n}{n^r} = +\infty$.

Il en résulte que \mathcal{P} est infini.

Preuve 6

(a) Pour tout $k \geq 2$, on a :

$$\frac{1}{k^2} < \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}$$

et pour $n \geq 2$:

$$S_n = \sum_{k=1}^n \frac{1}{k^2} < 1 + \sum_{k=2}^n \left(\frac{1}{k-1} - \frac{1}{k} \right) = 2 - \frac{1}{n}$$

avec $\lim_{n \rightarrow +\infty} \left(2 - \frac{1}{n} \right) = 2$. Il en résulte que la suite croissante $(S_n)_{n \geq 1}$ est majorée par 2, elle est donc convergente de limite $S \leq 2$.

En écrivant, pour tout $n \geq 2$, que :

$$\begin{aligned} \frac{1}{n^2} &= \left(\frac{1}{n^2} - \frac{1}{n(n-1)} \right) + \frac{1}{n(n-1)} \\ &= \left(\frac{1}{n-1} - \frac{1}{n} \right) - \frac{1}{n^2(n-1)} \end{aligned}$$

on a :

$$\begin{aligned} S &= \sum_{n=1}^{+\infty} \frac{1}{n^2} = 1 + \sum_{n=2}^{+\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) - \sum_{n=2}^{+\infty} \frac{1}{n^2(n-1)} \\ &= 2 - \sum_{n=2}^{+\infty} \frac{1}{n^2(n-1)} = 2 - T < 2. \end{aligned}$$

(b)

- i. Si $m \in E$ est divisible par p_k^2 , on a alors $m = p_k^2 q_k \leq n$ et $q_k = \frac{m}{p_k^2} \leq \frac{n}{p_k^2} < \left\lfloor \frac{n}{p_k^2} \right\rfloor + 1$, soit $q_k \leq \left\lfloor \frac{n}{p_k^2} \right\rfloor$. Il y a donc un maximum de $\left\lfloor \frac{n}{p_k^2} \right\rfloor$ possibilités pour q_k et pour un tel m .
- ii. En écrivant que :

$$E_2 = \bigcup_{k=1}^r \{m \in E \mid m \text{ est divisible par } p_k^2\}$$

on déduit que :

$$\begin{aligned} \text{card}(E_2) &\leq \sum_{k=1}^r \left\lfloor \frac{n}{p_k^2} \right\rfloor \leq \sum_{k=1}^r \frac{n}{p_k^2} = n \sum_{k=1}^r \frac{1}{p_k^2} \\ &< n \sum_{n=2}^{+\infty} \frac{1}{n^2} = n(S-1). \end{aligned}$$

D'autre part, avec :

$$E_1 \subset \left\{ \prod_{k=1}^r p_k^{\varepsilon_k} \text{ où } (\varepsilon_1, \dots, \varepsilon_r) \in \{0, 1\}^r \right\}$$

on déduit que :

$$\text{card}(E_1) \leq \text{card}(\{0, 1\}^r) = 2^r.$$

On a donc, pour tout entier $n > \prod_{k=1}^r p_k$:

$$n = \text{card}(E_1) + \text{card}(E_2) < 2^r + n(S-1)$$

soit :

$$0 < 2^r + n(S-2)$$

avec $S-2 < 0$, ce qui est impossible pour n assez grand.

Il en résulte que \mathcal{P} est infini.

Preuve 7

- (a) Soit x un réel strictement supérieur à 1 et n un entier naturel non nul tel que $n \leq x$. On a la décomposition en facteurs premiers $n = \prod_{k=1}^r p_k^{\alpha_k}$, où les α_k sont des entiers positifs ou nuls. Pour tout k compris entre 1 et r , on a $p_k^{\alpha_k} \leq n \leq x$ et

$$\alpha_k \leq \frac{\ln(x)}{\ln(p_k)} \leq \frac{\ln(x)}{\ln(p_1)} = \frac{\ln(x)}{\ln(2)} < \left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil + 1$$

soit :

$$\alpha_k \leq \left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil$$

puisque α_k est entier.

- (b) Pour $x > 1$, on a $[x] = \text{card}(E_x)$, où :

$$E_x = \{n \in \mathbb{N} \mid 1 \leq n \leq x\}.$$

Un entier naturel n étant uniquement déterminé par sa décomposition en facteurs premiers $\prod_{k=1}^r p_k^{\alpha_k}$ où les entiers α_k sont compris entre 0 et $\left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil$ si n est compris entre 1 et x , on a :

$$E_x \subset F_x = \left\{ \prod_{k=1}^r p_k^{\alpha_k} \mid 0 \leq \alpha_1, \dots, \alpha_r \leq \left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil \right\}$$

avec :

$$\begin{aligned} \text{card}(F_x) &= \text{card} \left\{ (\alpha_1, \dots, \alpha_r) \in \mathbb{N}^r \mid 0 \leq \alpha_k \leq \left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil \right\} \\ &= \left(\left\lceil \frac{\ln(x)}{\ln(2)} \right\rceil + 1 \right)^r \leq \left(\frac{\ln(x)}{\ln(2)} + 1 \right)^r = \left(\frac{\ln(2x)}{\ln(2)} \right)^r \end{aligned}$$

ce qui donne :

$$[x] = \text{card}(E_x) \leq \text{card}(F_x) \leq \left(\frac{\ln(2x)}{\ln(2)} \right)^r$$

et :

$$x < [x] + 1 \leq \left(\frac{\ln(2x)}{\ln(2)} \right)^r + 1$$

soit :

$$\frac{x}{(\ln(2x))^r} < \frac{1}{(\ln(2))^r} + \frac{1}{(\ln(2x))^r} < 2 \frac{1}{(\ln(2))^r}$$

en contradiction avec $\lim_{x \rightarrow +\infty} \frac{x}{(\ln(2x))^r} = +\infty$.

On en déduit que \mathcal{P} est infini.

Preuve 8 Si p est un diviseur premier de $m = 2^{p_r} - 1 \geq 2$, on a alors $m \equiv 0$ modulo p , soit $\bar{2}^{p_r} = \bar{1}$ dans \mathbb{Z}_p et l'ordre de $\bar{2}$ dans le groupe multiplicatif \mathbb{Z}_p^* est un diviseur de p_r et comme p_r est premier, cet ordre est exactement p_r (on a $\bar{2} \neq \bar{1}$ dans \mathbb{Z}_p).

Par ailleurs, on sait que l'ordre d'un élément dans un groupe divise l'ordre du groupe (théorème de Lagrange), donc p_r est un diviseur de $p - 1 = \text{card}(\mathbb{Z}_p^*)$ et $p_r < p$, ce qui contredit le fait que p_r est le plus grand nombre premier.

L'ensemble \mathcal{P} est donc infini.

Preuve 9

(a) On remarque qu'un nombre premier différent de 2 est nécessairement impair et son reste dans la division euclidienne par 4 ne peut être que 1 ou 3.

i. Dire $p \equiv 3 \pmod{4}$ revient à dire qu'il existe un entier $n \geq 0$ tel que $p = 4n + 3$.

On a alors $r = \frac{p-1}{2} = 2n + 1$ et si $x \in \mathbb{Z}_p^*$ est tel que $x^2 = -\bar{1}$, il vient $x^{p-1} = x^{2r} = (-\bar{1})^{2n+1} = -\bar{1}$, ce qui contredit le théorème de Fermat qui nous dit que $x^{p-1} = \bar{1}$ pour tout $x \in \mathbb{Z}_p^*$ (on a $-\bar{1} \neq \bar{1}$ puisque $p \geq 2$).

ii. Le théorème de Wilson nous dit que $(p-1)! = -\bar{1}$ dans \mathbb{Z}_p^* puisque p est premier. Par ailleurs, pour $k = 1, \dots, r$, on a :

$$r + k \equiv -r + k - 1 \pmod{p}$$

(c'est équivalent à $2r = p - 1 \equiv -1 \pmod{p}$), soit :

$$r + k \equiv -(r - (k - 1)) \pmod{p}$$

et :

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot \dots \cdot r \cdot (r+1) \cdot \dots \cdot (r+r) \\ &\equiv r! (-1)^r r (r-1) \cdot \dots \cdot 1 = (-1)^r (r!)^2 \pmod{p} \end{aligned}$$

Pour $p \equiv 1 \pmod{4}$, on a $p = 4n + 1$ avec $n \geq 1$ et $r = \frac{p-1}{2} = 2n$, de sorte que $(-1)^r = 1$ et $(p-1)! \equiv (r!)^2 \pmod{p}$, ce qui donne $\overline{r!}^2 = -\bar{1}$ d'après le théorème de Wilson. Donc $-\bar{1}$ est un carré dans \mathbb{Z}_p^* . Comme $-\overline{r!}$ est aussi solution de $x^2 + \bar{1} = 0$ avec $-\overline{r!} \neq \overline{r!}$ puisque $p \neq 2$, on a ainsi les deux seules solutions possibles.

(b)

i. Supposons que \mathcal{P}_1 soit fini et notons $3 = p_1 < p_2 < \dots < p_r$ tous ses éléments. L'entier :

$$m = 4p_1 \cdot \dots \cdot p_r - 1 = 4(p_1 \cdot \dots \cdot p_r - 1) + 3$$

qui est de la forme $4n + 3$ avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r ($m > 4p_k - 1 > p_k$ puisque $p_k \geq 3$). Comme m est impair, ses diviseurs premiers sont de la forme $4k + 1$ avec $k \in \mathbb{N}^*$ ou $4k + 3$ avec $k \in \mathbb{N}$ et ils ne peuvent pas être tous de la forme $4k + 1$, sans quoi m serait aussi de cette forme, donc congru à 1 modulo 4, ce qui contredit le fait qu'il est congru à 3 (ou à -1) modulo 4. L'entier m a donc un diviseur p_k dans \mathcal{P}_2 et comme p_k divise $p_1 \cdot \dots \cdot p_r$, il va aussi diviser -1 , ce qui est impossible avec p_k premier. L'ensemble \mathcal{P}_1 est donc infini.

De $\mathcal{P}_1 \subset \mathcal{P}$, on déduit que \mathcal{P} est infini.

ii. Supposons que \mathcal{P}_2 soit fini et notons $5 = p_1 < p_2 < \dots < p_r$ tous ses éléments. L'entier :

$$m = 4p_1^2 \cdot \dots \cdot p_r^2 + 1$$

qui est de la forme $4n + 1$ avec $n \geq 2$ n'est pas premier puisque strictement supérieur à tous les p_k pour k compris entre 1 et r . Comme m est impair, ses diviseurs premiers sont de la forme $4k + 1$ avec $k \in \mathbb{N}^*$ ou $4k + 3$ avec $k \in \mathbb{N}$. Si

p est un diviseur premier de m , on a alors $m = a^2 + 1 = pq$ et $\bar{a}^2 = -\bar{1}$ dans \mathbb{Z}_p^* , c'est-à-dire que $-\bar{1}$ est un carré dans \mathbb{Z}_p^* et p est nécessairement de la forme $4k+1$ avec $k \in \mathbb{N}^*$, donc p est l'un des p_k dans \mathcal{P}_2 et comme p_k divise $p_1 \cdots p_r$, il va aussi diviser 1 puisqu'il divise m , ce qui est impossible. L'ensemble \mathcal{P}_2 est donc infini. De $\mathcal{P}_2 \subset \mathcal{P}$, on déduit que \mathcal{P} est infini.

Preuve 10

- (a) En désignant, pour tout entier naturel n , par p_n un diviseur premier de u_n , on a $p_n \neq p_m$ pour tous $n \neq m$ puisque u_n et u_m sont premiers entre eux et donc ne peuvent avoir un diviseur premier en commun. La suite $(p_n)_{n \in \mathbb{N}}$ nous fournit donc une infinité de nombres premiers.
- (b) Résulte du fait que la suite $(F_n)_{n \in \mathbb{N}}$ des nombres de Fermat est strictement croissante dans $\mathbb{N} \setminus \{0, 1\}$ et que deux nombres de Fermat distincts sont premiers entre eux.
- (c)

- i. On vérifie facilement par récurrence que $(u_n)_{n \in \mathbb{N}}$ est une suite d'entiers naturels et que $u_n > a \geq 1$ pour tout $n \in \mathbb{N}$. En effet, $u_0 = b > a$ avec $b \in \mathbb{N}$ et supposant le résultat acquis au rang $n-1$, on a $u_n = a + u_{n-1}(u_{n-1} - a) \in \mathbb{N}$ et :

$$u_n - a = u_{n-1}(u_{n-1} - a) > 0.$$

On en déduit que pour tout $n \geq 1$, on a :

$$u_n - u_{n-1} = a + u_{n-1}(u_{n-1} - a - 1) \geq a > 0$$

($u_{n-1} > a$ dans \mathbb{N} équivaut à $u_{n-1} \geq a+1$), c'est-à-dire que $(u_n)_{n \in \mathbb{N}}$ est strictement croissante à valeurs dans $\mathbb{N} \setminus \{0, 1\}$.

- ii. On procède par récurrence sur $m > n$, à $n \geq 0$ fixé.
Pour $m = n+1$, on a :

$$u_{n+1} - a = u_n(u_n - a) \equiv 0 \pmod{u_n}$$

et supposant le résultat acquis au rang $m-1 > n$, on a :

$$u_m - a = u_{m-1}(u_{m-1} - a) \equiv 0 \pmod{u_n}.$$

Prenant $n = 0$, on déduit que $u_m \equiv a \pmod{u_0}$ pour tout $m \geq 1$, soit $u_m \equiv a \pmod{b}$ pour tout $m \geq 1$.

- iii. Pour $n = 0$, on a $u_0 = b$ qui est premier avec a par hypothèse.
Supposons le résultat acquis au rang $n-1 \geq 1$ et soit $\delta = u_n \wedge a$. Si $\delta \geq 2$, il admet alors un diviseur premier p qui divise u_n et a . Avec $u_n - a = u_{n-1}(u_{n-1} - a)$, on déduit que p divise $u_{n-1}(u_{n-1} - a)$ et en conséquence divise u_{n-1} ou $u_{n-1} - a$ et encore $u_{n-1} = (u_{n-1} - a) + a$, mais p ne peut diviser u_{n-1} et a qui sont premiers entre eux. On a donc $\delta = 1$.
- iv. Pour $m > n \geq 0$, on a $u_m = qu_n + a$ ($u_m \equiv a \pmod{u_n}$) avec $0 \leq a < u_n$, c'est-à-dire que a est le reste dans la division euclidienne de u_m par u_n et :

$$u_m \wedge u_n = u_n \wedge a = 1$$

On en déduit que \mathcal{P} est infini.

v. Pour $(a, b) = (2, 3)$, la suite $(u_n)_{n \in \mathbb{N}}$ est solution de l'équation récurrente :

$$\begin{cases} u_0 = 3 \\ \forall n \geq 1, u_n - 2 = u_{n-1}(u_{n-1} - 2) \end{cases}$$

ou encore :

$$\begin{cases} u_0 = 3 \\ \forall n \geq 1, u_n = (u_{n-1} - 1)^2 + 1 \end{cases}$$

On sait que la suite $(F_n)_{n \in \mathbb{N}}$ des nombres de Fermat est aussi solution de cette équation. On retrouve donc le fait que deux nombres de Fermat distincts sont premiers entre eux.

En notant $v_n = u_n - F_n$, on a :

$$\begin{cases} v_0 = 0 \\ \forall n \geq 1, v_n = (v_{n-1} - 1)^2 + 1 \end{cases}$$

et par récurrence $v_n = 2$ pour tout $n \geq 1$. On a donc :

$$\begin{cases} u_0 = F_0 = 3 \\ \forall n \geq 1, u_n = F_n + 2 \end{cases}$$

(d)

- i. On vérifie facilement par récurrence que $(u_n)_{n \in \mathbb{N}}$ est une suite d'entiers naturels impairs tous différents de 1. En effet, $u_0 = a$ est impair avec $a \geq 3$ et supposant le résultat acquis au rang $n - 1$, $u_n = u_{n-1}^2 - 2$ est un entier impair et :

$$u_n \geq 9 - 2 \geq 3.$$

On en déduit que pour tout $n \geq 1$, on a :

$$u_n - u_{n-1} = u_{n-1}(u_{n-1} - 1) - 2 \geq 6 - 2 > 0$$

c'est-à-dire que $(u_n)_{n \in \mathbb{N}}$ est strictement croissante.

- ii. Par définition de u_n , on a $u_{n+1} \equiv -2 \pmod{u_n}$ et :

$$u_{n+2} = u_{n+1}^2 - 2 \equiv (-2)^2 - 2 = 2 \pmod{u_n}.$$

En supposant que $u_m \equiv 2 \pmod{u_n}$ pour $m \geq n + 2$, on a :

$$u_{m+1} = u_m^2 - 2 \equiv (-2)^2 - 2 = 2 \pmod{u_n}.$$

On a donc ainsi vérifié par récurrence, que pour tout $m \geq n + 2$, on a $u_m \equiv 2 \pmod{u_n}$.

- iii. Pour $m > n \geq 0$, on a $u_m = qu_n + r$ avec $r = \pm 2$ ($u_m \equiv \pm 2 \pmod{u_n}$), il en résulte que :

$$u_m \wedge u_n = u_n \wedge (\pm 2) = 1$$

puisque u_n est impair.

On en déduit que \mathcal{P} est infini.

1.

- (a) La quantité R_n étant le reste d'ordre n de la série à termes positifs convergente $\sum \frac{1}{p_n}$, on a $\lim_{n \rightarrow +\infty} R_n = 0$ et il existe un entier $n_0 \geq 1$ tel que :

$$\forall n \geq n_0, 0 < R_n < \frac{1}{2}.$$

- (b) Les ensembles \mathcal{P}_1 et \mathcal{P}_2 formant une partition de l'ensemble \mathcal{P} des nombres premiers, on peut faire la partition indiquée de E .

- i. La décomposition en facteurs premiers de tout entier $n \in E_1$, peut s'écrire sous la forme :

$$n = \prod_{k=1}^r p_k^{\alpha_k} = \prod_{k=1}^r p_k^{\varepsilon_k} \prod_{k=1}^r p_k^{2\beta_k} = pq^2$$

où, pour tout k compris entre 1 et r , on a posé :

$$\varepsilon_k = \begin{cases} 0 & \text{si } \alpha_k \text{ est pair} \\ 1 & \text{si } \alpha_k \text{ est impair} \end{cases}$$

$p = \prod_{k=1}^r p_k^{\varepsilon_k}$, $q = \prod_{k=1}^r p_k^{\beta_k}$. Le nombre maximum de choix possibles pour p est :

$$\text{card}(\{0, 1\}^r) = 2^r$$

et avec $q^2 \leq n \leq N$, on déduit que $q \leq \sqrt{N} < \left[\sqrt{N} \right] + 1$, soit $q \leq \left[\sqrt{N} \right]$ et il y a un maximum de $\left[\sqrt{N} \right]$ choix possibles pour q . On en déduit donc que :

$$N_1 \leq 2^r \left[\sqrt{N} \right].$$

- ii. Si $n \in E_2$, il existe un nombre premier $p_k \in \mathcal{P}_2$ qui divise n , c'est-à-dire que $n = p_k q$ et $q = \frac{n}{p_k} \leq \frac{N}{p_k} < \left[\frac{N}{p_k} \right] + 1$, soit $q \leq \left[\frac{N}{p_k} \right]$ et il y a un maximum de $\left[\frac{N}{p_k} \right]$ choix possibles pour q , donc pour n . Pour p_k grand, on a en fait $\left[\frac{N}{p_k} \right] = 0$. On en déduit alors que :

$$N_2 \leq \left[\frac{N}{p_{r+1}} \right] + \left[\frac{N}{p_{r+2}} \right] + \dots$$

soit :

$$N_2 \leq \sum_{k=r+1}^{+\infty} \left[\frac{N}{p_k} \right] \leq \sum_{k=r+1}^{+\infty} \frac{N}{p_k} = N \sum_{k=r+1}^{+\infty} \frac{1}{p_k} < \frac{N}{2}.$$

- iii. On a donc :

$$N_1 + N_2 < 2^r \left[\sqrt{N} \right] + \frac{N}{2}$$

avec :

$$2^r \left[\sqrt{N} \right] \leq 2^r \sqrt{N} < \frac{N}{2}$$

pour N assez grand (précisément $N > 2^{2r+2}$ convient), ce qui donne $N_1 + N_2 < N$ en contradiction avec $N = N_1 + N_2$.

En définitive, $\sum_{n=1}^{+\infty} \frac{1}{p_n} = +\infty$.

2.

(a) Soit :

$$Q(X) = \sum_{k=0}^n a_k X^k$$

un polynôme à coefficients entiers relatifs de degré $n \geq 1$.

Les équations $Q(x) = -1$, $Q(x) = 0$ et $Q(x) = 1$ n'ayant qu'un nombre fini de solutions dans \mathbb{Z} , il existe un entier naturel a tel que $|Q(k)| \geq 2$ pour tout entier relatif $k \geq a$.

En particulier $Q(a)$ admet des diviseurs premiers.

(b) Si $Q(0) = 0$, on a alors $Q(X) = XR(X)$ avec R non nul dans $\mathbb{Z}[X]$ et pour tout nombre premier p , $Q(p) = pR(p)$ est divisible par p . Donc Q admet une infinité de diviseurs premiers.

(c)

i. On a :

$$Q(a_0 m X) = \sum_{k=0}^n a_k a_0^k m^k X^k = a_0 \left(1 + \sum_{k=1}^n a_k a_0^{k-1} m^k X^k \right)$$

ii. Le polynôme $1 + R$ qui est non constant à coefficients entiers admet des diviseurs premiers. Si p est l'un d'eux il existe un entier a tel que p divise $1 + R(a)$ et p divise $Q(a_0 m a) = a_0 (1 + R(a))$, c'est-à-dire que p est un diviseur premier de Q , c'est donc l'un des p_k . L'entier p divise alors m et comme m divise tous les coefficients b_k , p va diviser $R(a)$. On est donc dans la situation où p premier divise les entiers $R(a)$ et $1 + R(a)$, ce qui entraîne que p divise 1, soit une impossibilité.

En conclusion Q admet une infinité de diviseurs premiers.

3. Le polynôme $Q(X) = 4X^2 + 1$ admettant une infinité de nombres premiers, on peut donc trouver une suite strictement croissante $(p_n)_{n \in \mathbb{N}}$ de nombres premiers et une suite $(a_n)_{n \in \mathbb{N}}$ d'entiers relatifs tels que pour tout $n \in \mathbb{N}$, p_n divise $4a_n^2 + 1$. On a alors $4\overline{a_n}^2 = -1$ dans \mathbb{Z}_{p_n} et p_n est nécessairement congru à 1 modulo 4, c'est-à-dire que p_n est de la forme $4k + 1$.

On a dispose ainsi d'une infinité de nombres premiers congrus à 1 modulo 4.

4.

- (a) Dire que p divise Φ_n équivaut à dire qu'il existe un entier relatif a tel que p divise $\Phi_n(a)$, ce qui revient à dire que $\overline{\Phi_n(a)} = \bar{0}$ dans \mathbb{Z}_p . Avec $\bar{a}^n - \bar{1} = \prod_{d \in \mathcal{D}_n} \overline{\Phi_d(a)}$, on déduit que $\bar{a}^n = \bar{1}$ dans \mathbb{Z}_p et l'ordre d de a dans le groupe multiplicatif \mathbb{Z}_p^* est un diviseur de n , soit $d \in \mathcal{D}_n$.
- (b) Si $d = n$, alors n est un diviseur de $p - 1 = \text{card}(\mathbb{Z}_p^*)$ et $p = 1 + kn$ avec $k \in \mathbb{Z}$.
- (c)

i. Si $d < n$, de :

$$\bar{0} = \bar{a}^d - \bar{1} = \prod_{\delta \in \mathcal{D}_d} \overline{\Phi_\delta(a)}$$

dans le corps \mathbb{Z}_p , on déduit qu'il existe $\delta \in \mathcal{D}_d$ tel que $\overline{\Phi_\delta(a)} = \bar{0}$, ce qui équivaut à dire que $\Phi_\delta(a)$ est divisible par p . L'entier p divise donc $\Phi_n(a)$ et $\Phi_\delta(a)$ où δ est un diviseur de n (δ divise d qui divise n) tel que $\delta < n$, ce qui entraîne que :

$$a^n - 1 = \prod_{d' \in \mathcal{D}_n} \Phi_{d'}(a) = \Phi_\delta(a) \Phi_n(a) \prod_{d' \in \mathcal{D}_n - \{\delta, n\}} \Phi_{d'}(a)$$

est divisible par p^2 .

- ii. Pour tout entier $m \geq 1$ et tout entier k compris entre 1 et $\varphi(m) = \deg(\Phi_m)$, on a :

$$(a + p)^k = a^k + \sum_{j=1}^k C_k^j a^{k-j} p^j \equiv a^k \pmod{p}$$

et en conséquence :

$$\Phi_m(a + p) \equiv \Phi_m(a) \pmod{p}.$$

- iii. Avec :

$$(a + p)^n - 1 = \Phi_\delta(a + p) \Phi_n(a + p) \prod_{d' \in \mathcal{D}_n - \{\delta, n\}} \Phi_{d'}(a + p)$$

et :

$$\Phi_m(a + p) \equiv \Phi_m(a) \equiv 0 \pmod{p}$$

pour $m = \delta$ et $m = n$, on déduit que $(a + p)^n - 1$ est divisible par p^2 .

- iv. De ce qui précède, on déduit que $(a + p)^n - a^n$ est divisible par p^2 et il existe un entier q tel que :

$$p^2 q = (a + p)^n - a^n = na^{n-1}p + \sum_{k=2}^n C_n^k a^{n-k} p^k = na^{n-1}p + p^2 r$$

ce qui entraîne que $na^{n-1}p$ est divisible par p^2 et donc que na^{n-1} est divisible par p . Comme p est premier avec n , on en déduit que a^{n-1} est divisible par p , soit $\bar{a}^{n-1} = \bar{0}$ dans le corps \mathbb{Z}_p et $\bar{a} = \bar{0}$, ce qui contredit $\bar{a}^n = \bar{1}$. On ne peut donc avoir $d < n$.

- (d) On a donc $d = n$ et p est congru à 1 modulo n .

5. Réciproquement si p est congru à 1 modulo n , alors n est un diviseur de l'ordre $p - 1$ du groupe cyclique \mathbb{Z}_p^* et il existe dans \mathbb{Z}_p^* un élément \bar{a} d'ordre n . De $\bar{0} = \bar{a}^n - \bar{1} = \prod_{d \in \mathcal{D}_n} \overline{\Phi_d(a)}$, on déduit qu'il existe $d \in \mathcal{D}_n$ tel que $\overline{\Phi_d(a)} = \bar{0}$. Si $d < n$, de $\bar{a}^d - \bar{1} = \prod_{\delta \in \mathcal{D}_d} \overline{\Phi_\delta(a)}$, on déduit que $\bar{a}^d = \bar{1}$, ce qui n'est pas compatible avec la définition de l'ordre n de \bar{a} . On a donc $d = n$ et $\overline{\Phi_n(a)} = \bar{0}$, ce qui équivaut à dire que p divise $\Phi_n(a)$.
6. Pour $n = 1$, c'est l'infinitude de l'ensemble des nombres premiers. Comme, pour tout $n \geq 2$, Φ_n admet une infinité de diviseurs premiers, il y en a une infinité qui ne divisent pas n et de tels diviseurs sont nécessairement congrus à 1 modulo p d'après ce qui précède. On déduit donc qu'il existe une infinité de nombres premiers de la forme $1 + kn$ où $k \in \mathbb{N}^*$.

Le théorème de Fermat pour $n = 2$ et $n = 4$

32.1 Énoncé

– I –

On cherche tous les solutions dans \mathbb{N}^3 de l'équation de Fermat :

$$x^2 + y^2 = z^2. \quad (32.1)$$

1. Montrer que si $(x, y, z) \in \mathbb{N}^3$ est solution de (32.1), alors x et y ne peuvent être tous les deux impairs.
2. Montrer que si $(x, y, z) \in \mathbb{N}^3$ est une solution non triviale de (32.1) alors $x \wedge y = y \wedge z = x \wedge z$. En déduire qu'il existe $\delta \in \mathbb{N}^*$ et x', y', z' dans \mathbb{N} deux à deux premiers entre eux solution de (32.1) tels que $x = \delta x', y = \delta y', z = \delta z'$.
3. Soit $(x, y, z) \in \mathbb{N}^3$ une solution non triviale de (32.1) avec x, y, z deux à deux premiers entre eux (on peut toujours se ramener au cas où x, y, z sont positifs).

(a) Montrer que x et y sont de parités différentes.

On suppose que x est pair et y impair (x et y jouent des rôles symétriques).

- (b) Montrer qu'il existe deux entiers u et v premiers entre eux tels que $y = u - v$ et $z = u + v$.
- (c) Montrer que u et v sont les carrés de deux entiers premiers entre eux. On note $u = n^2$ et $v = m^2$.
- (d) En déduire que :

$$x = 2nm, \quad y = n^2 - m^2, \quad z = n^2 + m^2.$$

(e) En déduire toutes les solutions de (32.1).

– II –

On s'intéresse à l'équation :

$$x^4 + y^4 = z^2. \quad (32.2)$$

On suppose que l'équation admet des solutions (x, y, z) dans \mathbb{N}^3 avec $z \neq 0$.

1. Montrer que l'équation (32.2) admet une solution (x, y, z) dans \mathbb{N}^3 avec $z > 0$ minimal, $x > 0$ et $y > 0$.

2. Montrer que x et y sont premiers entre eux puis que x, y et z sont deux à deux premiers entre eux.
3. Montrer que l'on peut supposer x pair et qu'il existe alors deux entiers a et b premiers entre eux tels que :

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad z = a^2 + b^2.$$

4. Montrer que a est impair et b est pair.
5. Montrer qu'il existe deux entiers u et v premiers entre eux tels que :

$$b = 2uv, \quad y = u^2 - v^2, \quad a = u^2 + v^2.$$

En notant que $x^2 = 4uv(u^2 + v^2)$ montrer qu'il existe des entiers naturels r, s, t tels que :

$$u = r^2, \quad v = s^2, \quad a = t^2.$$

Montrer que r et s sont non nuls et que $0 < t < z$.

6. Dédurre de ce qui précède que l'équation (32.2) n'a pas de solution (x, y, z) dans \mathbb{N}^3 telle que $x \neq 0$ et $y \neq 0$.

32.2 Solution

– I –

1. Si x et y sont impairs, ils sont congrus à 1 ou -1 modulo 4, on a donc dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$, $\bar{x}^2 = \bar{y}^2 = \bar{2}$, ce qui est impossible puisque les carrés dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$ sont $\bar{0}$ et $\bar{1}$.
2. Soient $\delta_1 = x \wedge y$, $\delta_2 = y \wedge z$ et $\delta_3 = x \wedge z$. On a $\delta_1 \neq 0$ puisque $(x, y) \neq (0, 0)$. Avec $a^2 \wedge b^2 = (a \wedge b)^2$ (exercice ??) et $a \wedge b = a \wedge (a + b)$ (exercice 23.21), on déduit que :

$$\delta_3^2 = x^2 \wedge z^2 = x^2 \wedge (x^2 + y^2) = x^2 \wedge y^2 = \delta_1^2$$

et :

$$\delta_2^2 = y^2 \wedge z^2 = y^2 \wedge (x^2 + y^2) = y^2 \wedge x^2 = \delta_1^2$$

ce qui donne $\delta_1 = \delta_2 = \delta_3$ puisque tous ces entiers sont positifs. On peut alors écrire, on note δ ce pgcd commun, $x = \delta x'$, $y = \delta y'$, $z = \delta z'$ avec x', y', z' deux à deux premiers entre eux et (32.1) avec $\delta \neq 0$ nous donne $(x')^2 + (y')^2 = (z')^2$.

3.
 - (a) On a déjà vu que x et y ne peuvent être tous deux impairs et comme ils sont premiers entre eux, ils ne peuvent être tous deux pairs.
 - (b) On a $x = 2a$ et $y = 2b + 1$ et (32.1) s'écrit :

$$4a^2 + (2b + 1)^2 = z^2$$

et z est nécessairement impair. On définit donc des entiers en notant $u = \frac{y + z}{2}$, $v = \frac{z - y}{2}$ et on a $y = u - v$, $z = u + v$. Le pgcd δ de u et v divisant y et z divise aussi leur pgcd qui vaut 1. On a donc $\delta = 1$.

(c) Avec les notations précédentes, on a :

$$uv = \frac{z^2 - y^2}{4} = \frac{x^2}{4} = a^2$$

les entiers u et v étant premiers entre eux, ce qui impose que ces entiers sont des carrés. En effet, si u n'est pas un carré, il est différent de 1 et sa décomposition en facteurs premiers nous donne $u = p^{2\alpha+1}q$ avec p premier ne divisant ni q ni v (u et v sont premiers entre eux, ce qui donne $a^2 = p^{2\alpha+1}r$ avec p ne divisant pas r , ce qui est impossible. On a donc $u = n^2$ et $v = m^2$ avec n, m premiers entre eux puisque $1 = n^2 \wedge m^2 = (n \wedge m)^2$.

(d) On a donc :

$$\begin{cases} y = u - v = n^2 - m^2, \\ z = u + v = n^2 + m^2, \\ x^2 = 4a^2 = 4uv = 4n^2m^2 \end{cases}$$

avec $x \geq 0$, ce qui donne :

$$x = 2nm, \quad y = n^2 - m^2, \quad z = n^2 + m^2$$

où n, m sont des entiers naturels premiers entre eux.

(e) Ce qui précède nous dit que si $(x, y, z) \in \mathbb{N}^3$ est solution non triviale de (32.1), il existe alors un entier naturel non nul δ et des entiers naturels n, m premiers entre eux tels que :

$$(x, y, z) = (2\delta nm, \delta(n^2 - m^2), \delta(n^2 + m^2))$$

Réciproquement, on a bien :

$$4\delta^2 n^2 m^2 + \delta^2 (n^2 - m^2)^2 = \delta^2 (n^2 + m^2)^2$$

et $\delta = 0$ nous donne la solution triviale.

Toutes les solutions dans \mathbb{N}^3 sont donc les triplets (x, y, z) avec (x, y) ou (y, z) de la forme $(2\delta nm, \delta(n^2 - m^2))$ où $\delta \in \mathbb{N}$ et n, m sont premiers entre dans \mathbb{N} avec $n > m$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ et les nombres de Carmichael

33.1 Énoncé

Pour tout entier naturel $n \geq 2$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo n , \mathbb{Z}_n^* le groupe multiplicatif des éléments inversibles de cet anneau et $\varphi(n)$ le nombre d'éléments de \mathbb{Z}_n^* (indicateur d'Euler).

On pose $\varphi(1) = 1$.

Si k est un entier relatif, on note $\bar{k} = k + n\mathbb{Z}$ la classe de k dans \mathbb{Z}_n .

Pour tout couple (a, b) d'entiers relatifs, on note $a \wedge b$ le pgcd de a et b et $a \vee b$ leur ppcm.

– I – Préliminaires sur les groupes finis

Pour cette partie, les groupes sont notés multiplicativement et on note 1 l'élément neutre.

Si G est un groupe, pour tout a dans G , on note $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ le sous groupe de G engendré par a .

Si $\langle a \rangle$ est infini, on dit alors que a est d'ordre infini dans G , sinon on dit que a est d'ordre fini dans G et l'ordre de a est $\theta(a) = \text{card}(\langle a \rangle)$.

1. Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.
2. Soit G un groupe fini. Montrer que si x est un élément de G d'ordre p , y un élément de G d'ordre q , avec p et q premiers entre eux et $xy = yx$, alors xy est d'ordre pq . Si p et q ne sont pas premiers entre eux, xy est-il d'ordre $p \vee q$.
3. Donner un exemple de groupe dans lequel on peut trouver deux éléments d'ordre fini dont le produit est d'ordre infini.
4. Soit G un groupe commutatif fini d'ordre $n \geq 2$.
 - (a) Montrer que si p et q sont deux entiers naturels non nuls, alors il existe deux entiers p' et q' premiers entre eux tels que p' divise p , q' divise q et $p \vee q = p'q'$.
 - (b) Montrer qu'il existe un élément de G dont l'ordre est égal au ppcm m des ordres de tous les éléments de G .
 - (c) Montrer que m a les mêmes facteurs premiers que n .
 - (d) En déduire que pour tout diviseur premier p de n il existe dans G un élément d'ordre p .
5. Montrer que tout sous groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif \mathbb{K} est cyclique.

6. Soit G un groupe tel que tout élément de G soit d'ordre au plus égal à 2.

(a) Montrer que G est commutatif.

(b) On suppose de plus que G est fini. Montrer que $\text{card}(G) = 2^n$.

7. Soit $G = \langle a \rangle$ un groupe cyclique d'ordre $n \geq 2$.

(a) Soit $x = a^k \in H$. Montrer que l'ordre de x est égal à $\frac{n}{n \wedge k}$.

(b) Montrer que si H est un sous-groupe de G non réduit à $\{1\}$, alors $H = \langle a^p \rangle$ où p divise n et H est cyclique d'ordre $\frac{n}{p}$.

(c) Montrer que pour tout diviseur q de n , il existe un unique sous groupe de G d'ordre q , c'est le groupe cyclique $H = \langle a^p \rangle$ avec $p = \frac{n}{q}$.

– II – Quelques propriétés de la fonction indicatrice d'Euler

1. Montrer que pour tout entier naturel $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$.

2. Montrer que pour tout entier naturel $n \geq 2$, $\varphi(n)$ est le nombre d'entiers compris entre 1 et n premiers avec n .

3. Soit $n \geq 2$. Montrer que si k est un entier relatif premier avec n , alors $k^{\varphi(n)} \equiv 1 \pmod{n}$ (théorème d'Euler).

4. Soit $n \geq 2$. Montrer que n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$ (théorème de Wilson).

5. Soit p un nombre premier strictement plus grand que 3. On note $S_p = \sum_{k=1}^{p-1} \frac{1}{k}$ et pour tout

entier k compris entre 1 et $p-1$, $p_k = \prod_{\substack{j=1 \\ j \neq k, j \neq p-k}}^{p-1} j$.

(a) Montrer que :

$$\sum_{k=1}^{p-1} p_k = 2 \frac{(p-1)!}{p} S_p.$$

(b) Montrer que pour tout entier k compris entre 1 et $p-1$, $\overline{p_k} = \left(\overline{k}^{-1}\right)^2$ dans \mathbb{Z}_p .

(c) En déduire que $\sum_{k=1}^{p-1} p_k$ est divisible par p .

(d) En écrivant $S_p = \frac{a}{b}$ avec a et b premiers entre eux, montrer que p^2 divise a .

6. Soient p un nombre premier et α un entier naturel non nul. Montrer que :

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}.$$

7. Montrer que si n et m sont deux entiers naturels non nuls premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$.

8. Montrer que si $n \geq 1$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $2 \leq p_1 < \dots < p_r$ premiers et les α_i entiers naturels non nuls, alors :

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

9. Soient p et q deux nombres premiers distincts et $n = pq$. Montrer que si a et b sont deux entiers naturels tels que $ab \equiv 1 \pmod{\varphi(n)}$, alors pour tout entier relatif c , on a $c^{ab} \equiv c \pmod{n}$.
10. On veut montrer dans cette question que :

$$\forall n \geq 2, \quad \varphi(n) > \sqrt{n} - 1.$$

- (a) Montrer le résultat pour $n = 2, 3, 4, 5, 6$.
- (b) Montrer le résultat pour $n = \prod_{i=1}^r p_i$ avec $3 \leq p_1 < \dots < p_r$ premiers.
- (c) Montrer le résultat pour n impair supérieur ou égal à 7.
- (d) Montrer le résultat pour $n = 2^\alpha$ avec $\alpha \geq 3$.
- (e) Montrer le résultat pour $n = 2^\alpha 3^\beta$ avec $\alpha \geq 1, \beta \geq 1$ et $(\alpha, \beta) \neq (1, 1)$.
- (f) Montrer le résultat pour n pair supérieur ou égal à 7.
11. Pour tout entier $n \geq 2$, on note \mathcal{D}_n l'ensemble des diviseurs positifs de n et pour tout $d \in \mathcal{D}_n$, on note :

$$S_d = \left\{ k \in \{1, \dots, n\} \mid k \wedge n = \frac{n}{d} \right\}.$$

- (a) Montrer que les S_d , pour d décrivant \mathcal{D}_n , forment une partition de $\{1, \dots, n\}$.
- (b) Montrer que pour tout $d \in \mathcal{D}_n$ on a $\text{card}(S_d) = \varphi(d)$.
- (c) En déduire la formule de Möbius :

$$n = \sum_{d \in \mathcal{D}_n} \varphi(d).$$

12. Pour tout entier $n \geq 2$, on désigne par Φ_n le n -ième polynôme cyclotomique défini par :

$$\Phi_n(X) = \prod_{k \in S_n} (X - \omega_n^k),$$

où S_n est l'ensemble des entiers k compris entre 1 et n premier avec n et $\omega_n = e^{\frac{2i\pi}{n}}$. Pour $n = 1$, on note $\Phi_1(X) = X - 1$.

- (a) Montrer que $X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d$, où \mathcal{D}_n est l'ensemble des diviseurs positifs de n .
- (b) En déduire la formule de Möbius $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

– III – Quelques propriétés de Z_n^*

1. Pour tout entier $n \geq 2$, on note G_n le groupe des automorphismes du groupe additif \mathbb{Z}_n .

- (a) Montrer que pour tout $x \in \mathbb{Z}_n^*$ l'application $\sigma(x)$ définie sur \mathbb{Z}_n par :

$$\forall y \in \mathbb{Z}_n, \quad \sigma(x)(y) = xy$$

est un automorphisme du groupe additif \mathbb{Z}_n .

- (b) Montrer que l'application σ réalise un isomorphisme de (\mathbb{Z}_n^*, \cdot) sur (G_n, \circ) .

2. Soit p un nombre premier. On désigne toujours par \mathcal{D}_{p-1} l'ensemble des diviseurs positifs de $p-1$ et pour tout $d \in \mathcal{D}_{p-1}$, on note $\psi(d)$ le nombre d'éléments d'ordre d dans \mathbb{Z}_p^* .

- (a) Montrer que :

$$p-1 = \sum_{d \in \mathcal{D}_{p-1}} \psi(d).$$

- (b) Soit $d \in \mathcal{D}_{p-1}$. Montrer que si $\psi(d) > 0$, alors $\psi(d) = \varphi(d)$.

- (c) Montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$ et en déduire que \mathbb{Z}_p^* est cyclique (on retrouve donc un cas particulier du résultat de I.5.).

3. Soient p un nombre premier impair et α un entier supérieur ou égal à 2. On se propose dans cette question de montrer que le groupe multiplicatif $\mathbb{Z}_{p^\alpha}^*$ est cyclique (voir aussi le livre d'algèbre de Perrin-Riou).

- (a) Montrer que pour tout entier k compris entre 1 et $p-1$, C_p^k est divisible par p .

- (b) Montrer qu'il existe une suite d'entiers naturels non nuls $(\lambda_k)_{k \in \mathbb{N}}$ tous premiers avec p tels que :

$$\forall k \in \mathbb{N}, \quad (1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

- (c) Montrer que la classe résiduelle modulo p^α , $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^*$.

- (d) Soit $x = k + p\mathbb{Z}$ un générateur du groupe cyclique \mathbb{Z}_p^* . Montrer que $y = k^{p^{\alpha-1}} + p^\alpha \mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^*$.

- (e) Déduire de ce qui précède que $\mathbb{Z}_{p^\alpha}^*$ est cyclique.

4. Montrer que \mathbb{Z}_2^* et $\mathbb{Z}_{2^2}^*$ sont cycliques.

5. Dans cette question on s'intéresse au groupe multiplicatif $\mathbb{Z}_{2^\alpha}^*$ pour $\alpha \geq 3$.

- (a) Montrer qu'il existe une suite $(\lambda_k)_{k \in \mathbb{N}}$ d'entiers impairs tels que :

$$\forall k \in \mathbb{N}, \quad 5^{2^k} = 1 + \lambda_k 2^{k+2}.$$

- (b) Montrer que la classe résiduelle de 5 modulo 2^α est d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^*$.

- (c) On désigne par ψ l'application qui à toute classe résiduelle modulo 2^α , $k + 2^\alpha \mathbb{Z}$, associe la classe résiduelle modulo 4, $k + 4\mathbb{Z}$. Montrer que cette application est bien définie, qu'elle induit un morphisme surjectif de groupes multiplicatifs de $\mathbb{Z}_{2^\alpha}^*$ sur \mathbb{Z}_4^* et que son noyau est un groupe cyclique d'ordre $2^{\alpha-2}$.

- (d) Montrer que l'application :

$$\begin{aligned} \pi : \mathbb{Z}_{2^\alpha}^* &\rightarrow \mathbb{Z}_4^* \times \ker(\psi) \\ x &\mapsto (\psi(x), \psi(x)x) \end{aligned}$$

est un isomorphisme de groupes. En déduire que $\mathbb{Z}_{2^\alpha}^*$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Le groupe $\mathbb{Z}_{2^\alpha}^*$ est-il cyclique ?

– IV – Nombres de Carmichael

Un théorème de Fermat nous dit que si p est premier et k premier avec p , alors $k^{p-1} \equiv 1 \pmod{p}$ (théorème d'Euler II.3. avec n premier). Dans cette partie on s'intéresse à la réciproque de ce résultat. Que peut-on dire de n tel que $k^{n-1} \equiv 1 \pmod{n}$ pour tout k premier avec n ?

On appelle nombre de Carmichael tout entier $n \geq 2$ non premier tel que :

$$\forall x \in \mathbb{Z}_n^*, \quad x^{n-1} = \bar{1}.$$

1. Montrer qu'un nombre de Carmichael est impair.
2. Soit $n = \prod_{i=1}^r p_i$ avec $r \geq 2$, $3 \leq p_1 < \dots < p_r$ premiers tels que pour tout i compris entre 1 et r , $p_i - 1$ divise $n - 1$. Montrer que n est un nombre de Carmichael.
3. Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $r \geq 2$, $3 \leq p_1 < \dots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r un nombre de Carmichael.
 - (a) On suppose qu'il existe un indice i compris entre 1 et r tel que $\alpha_i \geq 2$.
 - i. Montrer qu'il existe un entier relatif p tel que la classe modulo $p_i^{\alpha_i}$, $p + p_i^{\alpha_i}\mathbb{Z}$, soit d'ordre p_i dans $\mathbb{Z}_{p_i^{\alpha_i}}^*$ et qu'il existe un entier relatif q premier avec n solution du système de congruence :

$$\begin{cases} q \equiv p \pmod{p_i^{\alpha_i}} \\ q \equiv 1 \pmod{p_j^{\alpha_j}} \quad (1 \leq j \neq i \leq r). \end{cases}$$

- ii. En déduire que p_i divise $n - 1$ et conclure.

- (b) Montrer que $n = \prod_{i=1}^r p_i$ avec $p_i - 1$ divisant $n - 1$ pour tout i compris entre 1 et r .

- (c) Montrer que $r \geq 3$.

On a donc montré le résultat suivant pour $n \geq 2$: la condition $k^{n-1} \equiv 1 \pmod{n}$ pour tout k premier avec n est équivalente à n premier ou $n = \prod_{i=1}^r p_i$ avec $r \geq 3$, $3 \leq p_1 < \dots < p_r$ premiers tels que pour tout i compris entre 1 et r , $p_i - 1$ divise $n - 1$. Par exemple 561, 1105, 1729, sont des nombres de Carmichael (il y en a une infinité).

33.2 Solution

– I – Préliminaires sur les groupes finis

1. Le groupe additif $G = \frac{\mathbb{Z}}{2\mathbb{Z}}[X]$ (ou $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$ avec p premier, ou $\prod_{p \in \mathcal{P}} \frac{\mathbb{Z}}{p\mathbb{Z}}$) est infini et tous ses éléments sont d'ordre 2.

Si on définit sur le corps \mathbb{Q} des rationnels la relation d'équivalence $r \sim s$ si et seulement si $r - s \in \mathbb{Z}$, alors le groupe quotient $\frac{\mathbb{Q}}{\mathbb{Z}}$ pour cette relation d'équivalence est infini et tous ses éléments sont d'ordre fini ($q \frac{\overline{p}}{q} = \overline{0}$).

Si E est un ensemble infini, alors $(\mathcal{P}(E), \Delta)$ où Δ est l'opérateur de différence symétrique est infini et tous les éléments sont d'ordre 1 ou 2 puisque $A\Delta A = \emptyset$.

2. On a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$ puisque x et y commutent. L'ordre r de xy est donc un diviseur de pq .

L'égalité $(xy)^r = x^r y^r = 1$ entraîne $y^r = (x^r)^{-1} \in \langle x \rangle \cap \langle y \rangle = H$. Le groupe H étant contenu dans les groupes $\langle x \rangle$ et $\langle y \rangle$ a un ordre qui divise p et q et ces entiers étant premiers entre eux, on a nécessairement $H = \{1\}$. On a donc $y^r = x^r = 1$ et r est un multiple de p et q , donc de pq puisque p et q sont premiers entre eux. On peut donc conclure à l'égalité $r = pq$.

Une autre solution consiste à dire que si $(xy)^r = 1$, alors $(xy)^{rp} = 1$ avec $x^{rp} = 1$ et x, y qui commutent, donc $y^{rp} = 1$ et q divise rp , il divise donc r puisqu'il est premier avec p . De même p divise r . Donc pq divise r et pq est l'ordre de xy puisque $(xy)^{pq} = 1$.

Si p et q ne sont pas premiers entre eux, l'ordre de xy n'est pas nécessairement le ppcm des ordres de x et y . En prenant x d'ordre $p \geq 2$ dans G et $y = x^{-1}$ qui est également d'ordre p , on $xy = 1$ d'ordre $1 \neq \text{ppcm}(p, p) = p$.

3. Le produit de deux réflexions vectorielles $\sigma_{\mathcal{D}}$ et $\sigma_{\mathcal{D}'}$ d'axes \mathcal{D} et \mathcal{D}' faisant un angle α est une rotation d'angle 2α . Chaque réflexion est d'ordre 2 et la composée $\sigma_{\mathcal{D}} \circ \sigma_{\mathcal{D}'}$ est d'ordre infini si $\frac{2\pi}{2\alpha} \notin \mathbb{Q}$.

On peut aussi considérer la composée de deux symétries centrales dans le plan de centre O_1 et O_2 distincts, cette composée est la translation de vecteur $\overrightarrow{2O_1O_2}$ qui est d'ordre infini dans le groupe des bijections du plan.

4. (a) On a les décompositions en facteurs premiers :

$$p = \prod_{i=1}^r p_i^{\alpha_i}, \quad q = \prod_{i=1}^r p_i^{\beta_i}$$

avec $2 \leq p_1 < \dots < p_r$ premiers et les α_i, β_i positifs ou nuls pour $1 \leq i \leq r$. On pose alors :

$$p' = \prod_{\substack{i=1 \\ \alpha_i > \beta_i}}^r p_i^{\alpha_i}, \quad q' = \prod_{\substack{i=1 \\ \alpha_i \leq \beta_i}}^r p_i^{\beta_i}$$

(p' ou q' est égal à 1 si la condition $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée) et on a p' divise p , q' divise q , $p \vee q = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)} = p'q'$, $p' \wedge q' = 1$.

- (b) Soit μ le plus grand des ordres des éléments de G (l'exposant de G) et x un élément d'ordre μ dans G . Nous allons montrer que μ est multiple de l'ordre de tout élément de G , en conséquence c'est le ppcm de ces ordres. Soit donc y un élément de G et p son ordre. En désignant par μ' et p' des entiers premiers entre eux tels que μ' divise μ , p' divise p et $\mu \vee p = \mu'p'$, on a $x' = x^{\frac{\mu}{\mu'}}$ d'ordre μ' , $y' = y^{\frac{p}{p'}}$ d'ordre p' et le produit $x'y'$ est d'ordre $\mu'p' = \mu \vee p$ (le groupe G est commutatif et les ordres μ' et p' sont premiers entre eux). Ce qui entraîne $\mu \vee p \leq \mu$ et $\mu = \mu \vee p$ est un multiple de p . En définitive μ est le ppcm m des ordres des éléments de G et il existe un élément x de G d'ordre m .

- (c) Soit $\{x_1, \dots, x_p\}$ un système de générateurs de G (qui est fini) et $H = \prod_{i=1}^p \langle x_i \rangle$. Du fait que G est commutatif, l'application $\psi : H \rightarrow G$ définie par :

$$\forall y = (y_1, \dots, y_p) \in H, \quad \psi(y) = \prod_{i=1}^p y_i$$

est un morphisme de groupes et ce morphisme est surjectif puisque $\{x_1, \dots, x_p\}$ engendrent G . Ce morphisme surjectif induit alors un isomorphisme du groupe quotient $\frac{H}{\ker(\psi)}$ sur G , ce qui entraîne $\text{card}(H) = \text{card}(\ker(\psi)) \text{card}(G)$ et $n = \text{card}(G)$

divise $\text{card}(H) = \prod_{i=1}^p r_i$ où, pour i compris entre 1 et p , r_i est l'ordre de x_i . Le ppcm

m des ordres des éléments de G étant multiple de chaque r_i , m^p est multiple de $\prod_{i=1}^p r_i$

donc de n , ce qui entraîne que m a les mêmes facteurs premiers que n .

Autre solution : il existe $x \in G$ d'ordre m , donc m divise n et les facteurs premiers de m sont des facteurs premiers de n . Le théorème de Sylow nous dit que si p est un diviseur premier de n , il existe alors un sous-groupe H de G d'ordre p et H est cyclique, soit $H = \langle a \rangle$ avec a d'ordre p dans G , donc p divise m .

Voir le théorème de décomposition des groupes abéliens sous la forme : $\mathbb{Z}^r \times \frac{\mathbb{Z}}{q_1 \mathbb{Z}} \times \dots$

- (d) Si p est un diviseur premier de n , c'est également un diviseur premier de m et $m = pr$. En désignant par x un élément de G d'ordre m et en posant $y = x^r$ on dispose d'un élément d'ordre p dans G (c'est le premier théorème de Sylow, voir Schwarz).

5. Soit G un sous groupe d'ordre n de \mathbb{K}^* . Il existe dans G (commutatif) un élément x d'ordre $m \leq n$ égal au ppcm des ordres des éléments de G . L'ordre de tout élément de G divisant m , on déduit que tout $y \in G$ est racine du polynôme $P(X) = X^m - 1$, ce qui donne n racines de P dans \mathbb{K} , mais sur un corps commutatif un polynôme de degré m a au plus m racines¹, on a donc $n \leq m$. En définitive $m = n$ et G ayant un élément d'ordre n est cyclique.

6. (a) Si tous les éléments de G sont d'ordre au plus égal à 2, alors pour tout $x \in G$, on a $x^2 = 1$ et $x = x^{-1}$. Pour x, y dans G , on a alors $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$, c'est-à-dire que G est commutatif.

- (b) On suppose de plus que G est fini. Si G est réduit à $\{1\}$ alors $\text{card}(G) = 1 = 2^0$. Si G n'est pas réduit à $\{1\}$, il existe $x \in G \setminus \{1\}$ tel que $\langle x \rangle = \{1, x\}$ et le groupe quotient $\frac{G}{\langle x \rangle}$ est de cardinal strictement inférieur à 2 avec tous ses éléments d'ordre au plus égal à 2. On conclut alors par récurrence sur l'ordre de G . En supposant le résultat acquis pour les groupes d'ordre strictement inférieur à $\text{card}(G)$, on a $\text{card}\left(\frac{G}{\langle x \rangle}\right) = 2^p$ et $\text{card}(G) = 2^{p+1}$.

Autre solution : ppcm {ordre des éléments de G } = 2 qui a les mêmes facteurs premiers que n , donc $n = 2^m$ (4.c.).

Autre solution : si p est un diviseur premier de n , alors il existe x d'ordre p dans G (4.d.), mais x est d'ordre 1 ou 2, donc $p = 2$ et $n = 2^m$.

7. (a) Soit $x = a^k \in H$. On note $d = n \wedge k$, $n = dn'$, $k = dk'$ avec k' et n' premiers entre eux. On a $x^{n'} = a^{kn'} = a^{\frac{k}{d}n} = a^{\frac{k'}{d}n} = a^{k'n} = 1$, ce qui entraîne que n' est un multiple de l'ordre m de x . D'autre part, avec $1 = x^m = a^{km}$ on déduit que $n = dn'$ divise $km = dk'm$ et n' divise $k'm$ avec n' et k' premiers entre eux, ce qui entraîne que n' divise m . On a donc $m = n' = \frac{n}{n \wedge k}$.

1. Ce résultat est faux sur un corps non commutatif, voir par exemple le corps des quaternions.

- (b) Si H n'est pas réduit à $\{1\}$, il existe k compris entre 1 et $n-1$ tel que $a^k \in H$ et on peut poser :

$$p = \min \{k \in \{1, \dots, n-1\} \mid a^k \in H\}.$$

En écrivant, pour tout $x = a^k \in H$, $k = pq + r$ avec $0 \leq r \leq p-1$ (division euclidienne), on a $a^r = a^k (a^{pq})^{-1} \in H$ et nécessairement $r = 0$. On a donc $H \subset \langle a^p \rangle \subset H$, soit $H = \langle a^p \rangle$. Avec $a^n = 1 \in H$ on déduit que n est multiple de p et l'ordre de H est égal à $\frac{n}{n \wedge p} = \frac{n}{p}$.

- (c) Si q est un diviseur de n , on pose $H = \langle a^p \rangle$ où $p = \frac{n}{q}$ et H est un sous-groupe cyclique de G d'ordre $\frac{n}{p} = q$. Réciproquement si H est un sous-groupe de G d'ordre q , c'est nécessairement $H = \langle a^p \rangle$ avec $p = \frac{n}{q}$ (question précédente).

– II – Quelques propriétés de la fonction indicatrice d'Euler

1. Dire que \bar{k} est inversible dans \mathbb{Z}_n équivaut à dire qu'il existe $\bar{u} \in \mathbb{Z}_n$ tel que $\bar{k}\bar{u} = \bar{1}$ encore équivalent à dire qu'il existe $u \in \mathbb{Z}$ tel que $u\bar{k} = \bar{1}$, soit à dire que $\bar{1}$ est dans le groupe engendré par \bar{k} et donc que ce groupe est \mathbb{Z}_n . Donc $\bar{k} \in \mathbb{Z}_n^*$ si et seulement si \bar{k} est générateur du groupe additif \mathbb{Z}_n . Il en résulte que $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$.
2. Dire que \bar{k} est inversible dans \mathbb{Z}_n équivaut à dire qu'il existe $\bar{u} \in \mathbb{Z}_n$ tel que $\bar{k}\bar{u} = \bar{1}$ encore équivalent à dire qu'il existe deux entiers relatifs u et v tels que $ku + nv = 1$ équivalent à dire que k et n sont premiers entre eux (théorème de Bézout). En considérant que chaque classe modulo n a un unique représentant compris entre 1 et n , on déduit que $\varphi(n)$ est le nombre d'entiers compris entre 1 et n premiers avec n .²
3. Si k est premier avec n , alors \bar{k} appartient à \mathbb{Z}_n^* qui est d'ordre $\varphi(n)$ et $\bar{k}^{\varphi(n)} = \bar{1}$, c'est-à-dire que $k^{\varphi(n)} \equiv 1 \pmod{n}$.
4. Si n est premier alors \mathbb{Z}_n est un corps commutatif et tout élément a de \mathbb{Z}_n^* est racine du polynôme $X^{n-1} - \bar{1}$, on a donc $X^{n-1} - \bar{1} = \prod_{a \in \mathbb{Z}_n^*} (X - a) = \prod_{k=1}^{n-1} (X - \bar{k})$ dans $\mathbb{Z}_n[X]$ et en évaluant ce polynôme en $\bar{0}$, il vient $-\bar{1} = \prod_{k=1}^{n-1} (-\bar{k}) = (-1)^{n-1} \overline{(n-1)!}$. Pour $n = 2$, on a $-\bar{1} = \bar{1}$ et pour $n \geq 2$ premier on a n impair et $-\bar{1} = \overline{(n-1)!}$ dans \mathbb{Z}_n . Réciproquement si $n \geq 2$ est tel que $\overline{(n-1)!} = -\bar{1}$ dans \mathbb{Z}_n , alors tout diviseur d de n compris entre 1 et $n-1$ divisant $(n-1)! = -1 + kn$ va diviser -1 , ce qui donne $d = 1$ et l'entier n est premier.
5. (a) On a :

$$\sum_{k=1}^{p-1} p_k = \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} = \frac{(p-1)!}{p} \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) = 2 \frac{(p-1)!}{p} S_p.$$

- (b) Pour k compris entre 1 et $p-1$, on a, en utilisant le théorème de Wilson :

$$k(p-k)p_k = (p-1)! \equiv -1 \pmod{p},$$

ce qui donne $k^2 p_k \equiv 1 \pmod{p}$ ou encore $\overline{p_k} = \left(\bar{k}^{-1}\right)^2$ dans \mathbb{Z}_n .

2. $\frac{\varphi(n)}{n}$ est la probabilité pour qu'un entier k pris au hasard entre 1 et n soit premier avec n .

(c) L'application $x \mapsto x^{-1}$ réalisant une permutation de \mathbb{Z}_n^* , on a :

$$\sum_{k=1}^{p-1} \overline{p_k} = \sum_{k=1}^{p-1} \left(\overline{k}^{-1} \right)^2 = \sum_{x \in \mathbb{Z}_n^*} (x^{-1})^2 = \sum_{y \in \mathbb{Z}_n^*} (y)^2 = \sum_{j=1}^{p-1} \overline{j}^2 = \overline{\sum_{j=1}^{p-1} j^2},$$

avec $\sum_{j=1}^{p-1} j^2 = \frac{p(p-1)(2p-1)}{6} \in \mathbb{N}$ et p premier strictement plus grand que 3, ce qui entraîne que 6 divise $p(p-1)(2p-1)$ en étant premier avec p , donc 6 divise $(p-1)(2p-1)$ (théorème de Gauss) et $\frac{(p-1)(2p-1)}{6} \in \mathbb{N}$, ce qui permet de conclure à :

$$\sum_{k=1}^{p-1} \overline{p_k} = \overline{\sum_{j=1}^{p-1} j^2} = \overline{0}$$

dans \mathbb{Z}_n .

(d) L'égalité $\sum_{k=1}^{p-1} p_k = 2 \frac{(p-1)!}{p} S_p$ avec $S_p = \frac{a}{b}$, s'écrit :

$$pb \sum_{k=1}^{p-1} p_k = 2a(p-1)!$$

et du fait que p divise $\sum_{k=1}^{p-1} p_k$, on déduit que p^2 divise $2a(p-1)!$. L'entier p étant premier impair est premier avec $2(p-1)!$, on déduit avec le théorème de Gauss que p^2 divise a .

6. Si p est premier, alors un entier k compris entre 1 et p^α n'est pas premier avec p^α si et seulement si il est divisible par p , ce qui équivaut à $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, il y a donc $p^{\alpha-1}$ possibilités. On en déduit alors que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}.$$

7. Le théorème chinois nous dit que si n et m sont deux entiers premiers entre eux alors les anneaux \mathbb{Z}_{nm} et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes, un isomorphisme étant réalisé par :

$$\forall \overline{k} \in \mathbb{Z}_{nm}, f(\overline{k}) = \left(\overset{\cdot}{\overline{k}}, \overset{\cdot\cdot}{\overline{k}} \right),$$

où on a noté $\overset{\cdot}{\overline{k}}$ la classe de k modulo nm , $\overset{\cdot\cdot}{\overline{k}}$ la classe de k modulo n et \overline{k} la classe de k modulo m . La restriction de f à \mathbb{Z}_{nm}^* réalise un isomorphisme de groupes multiplicatifs de \mathbb{Z}_{nm}^* sur $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$, ce qui entraîne :

$$\varphi(nm) = \text{card}(\mathbb{Z}_{nm}^*) = \text{card}(\mathbb{Z}_n^*) \text{card}(\mathbb{Z}_m^*) = \varphi(n) \varphi(m).$$

8. En utilisant les résultats des questions précédentes, on a :

$$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r \varphi(p^{\alpha_i}) = \prod_{i=1}^r (p_i - 1) p_i^{\alpha_i - 1} = n \prod_{i=1}^r \left(1 - \frac{1}{p_i} \right).$$

9. Si $ab \equiv 1 \pmod{\varphi(n)}$, il existe alors un entier relatif k tel que :

$$ab = 1 + k\varphi(n) = 1 + k(p-1)(q-1).$$

Si c est un entier relatif premier avec p , on a alors $c^{p-1} \equiv 1 \pmod{p}$ (théorème de Fermat) et :

$$c^{ab} = c^{k(p-1)(q-1)} \equiv c \pmod{p}.$$

Si l'entier relatif c n'est pas premier avec p , c'est nécessairement un multiple de p (qui est premier) et :

$$c^{ab} \equiv 0 \equiv c \pmod{p}.$$

De manière analogue, on a $c^{ab} \equiv c \pmod{q}$ et avec p et q premiers entre eux il en résulte que $c^{ab} \equiv c \pmod{pq}$.³

10. (a) On a $\varphi(2) = 1 > \sqrt{2} - 1$, $\varphi(5) = 4 > \sqrt{5} - 1$ et $\varphi(3) = \varphi(4) = \varphi(6) = 2 > \sqrt{k} - 1$ pour $k = 3, 4, 6$.

- (b) Si $n = \prod_{i=1}^r p_i$ avec $3 \leq p_1 < \dots < p_r$ premiers, on a alors :

$$\frac{\varphi(n)}{\sqrt{n}} = \prod_{i=1}^r \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $p(p-3) \geq 0$, soit $p^2 - 3p + 1 > 0$ ou encore $(p-1)^2 > p$, c'est-à-dire $p-1 > \sqrt{p}$. On en déduit donc que $\varphi(n) > \sqrt{n}$.

- (c) Si n est un nombre impair supérieur ou égal à 7, il s'écrit $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec $3 \leq p_1 < \dots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r . En posant $m = \prod_{i=1}^r p_i$, on a :

$$\varphi(n) = \frac{n}{m} \prod_{i=1}^r \varphi(p_i) = \frac{n}{m} \varphi(m)$$

et :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}} > 1,$$

ce qui donne $\varphi(n) > \sqrt{n}$.

- (d) Si $n = 2^\alpha$ avec $\alpha \geq 3$, on a alors :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}-1} = (\sqrt{2})^{\alpha-2} > 1$$

et $\varphi(n) > \sqrt{n}$.

- (e) Si $n = 2^\alpha 3^\beta$ avec $\alpha \geq 1$, $\beta \geq 1$ et $(\alpha, \beta) \neq (1, 1)$, on a alors :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}} 3^{\frac{\beta}{2}-1} = (\sqrt{2})^\alpha (\sqrt{3})^{\beta-2} > 1$$

(pour $\beta \geq 2$ il n'y a pas de problème et pour $\beta = 1$ on a $\alpha \geq 2$ et $(\sqrt{2})^\alpha (\sqrt{3})^{-1} \geq \frac{2}{\sqrt{3}} > 1$), ce qui donne $\varphi(n) > \sqrt{n}$.

3. Ce résultat est à la base du système cryptographique R.S.A.

- (f) Si n est pair, il s'écrit $n = 2^{\alpha_1} \prod_{i=2}^r p_i^{\alpha_i}$ avec $3 \leq p_2 < \dots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r . En posant $m = 2 \prod_{i=2}^r p_i$, on a ::

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}},$$

avec :

$$\frac{\varphi(m)}{\sqrt{m}} = \frac{1}{\sqrt{2}} \prod_{i=2}^r \frac{p_i - 1}{\sqrt{p_i}}.$$

Pour $p \geq 3$, on a $\frac{p-1}{\sqrt{p}} > 1$, donc $\frac{\varphi(m)}{\sqrt{m}} > \frac{p_2 - 1}{\sqrt{2}\sqrt{p_2}}$ et pour $p_2 \geq 5$, on a $\frac{p_2 - 1}{\sqrt{2}\sqrt{p_2}} > 1$.

Il reste à étudier le cas $p_2 = 3$, soit $n = 2^{\alpha_1} 3^{\alpha_2} r$, avec $r = \prod_{i=3}^r p_i^{\alpha_i}$ où $5 \leq p_3 < \dots < p_r$ sont premiers. Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \frac{\varphi(2^{\alpha_1} 3^{\alpha_2})}{\sqrt{2^{\alpha_1} 3^{\alpha_2}}} \frac{\varphi(r)}{\sqrt{r}} > 1$$

d'après ce qui précède. On a donc ainsi montré que $\varphi(n) > \sqrt{n}$ pour tout $n \geq 7$.

11. (a) Il est clair que $S_d \cap S_{d'} = \emptyset$ pour $d \neq d'$ dans \mathcal{D}_n . Si k est un entier compris entre 1 et n , en notant δ le pgcd de k et n , $k = \delta k'$ et $n = \delta d$ avec k' et d premiers entre eux, on a $k \wedge n = \delta = \frac{n}{d}$ et $k \in S_d$ avec $d \in \mathcal{D}_n$. On a donc la partition :

$$\{1, \dots, n\} = \bigcup_{d \in \mathcal{D}_n} S_d.$$

- (b) Un entier k compris entre 1 et n est dans S_d si et seulement si il s'écrit $k = \frac{n}{d} k'$ avec k' compris entre 1 et d premier avec d . On a donc :

$$\text{card}(S_d) = \text{card} \{k' \in \{1, \dots, d\} \mid k' \wedge d = 1\} = \varphi(d).$$

- (c) Des deux questions précédentes, on déduit que $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

12. (a) Les S_d , pour $d \in \mathcal{D}_n$ formant une partition de $\{1, \dots, n\}$, on a :

$$X^n - 1 = \prod_{k=1}^n (X - \omega_n^k) = \prod_{d \in \mathcal{D}_n} \prod_{k \in S_d} (X - \omega_n^k),$$

avec :

$$\prod_{k \in S_d} (X - \omega_n^k) = \prod_{\substack{k'=1 \\ k' \wedge d=1}}^d \left(X - \left(e^{\frac{2i\pi}{n}} \right)^{k' \frac{n}{d}} \right) = \prod_{\substack{k'=1 \\ k' \wedge d=1}}^d (X - \omega_d^{k'}) = \Phi_d(X)$$

($k \in S_d$ s'écrit $k = k' \frac{n}{d}$ avec k' compris entre 1 et d premier avec d), ce qui donne :

$$X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d(X).$$

- (b) Chaque polynôme Φ_d étant de degré $\varphi(d)$, en posant $\varphi(1) = 1$, on déduit du résultat précédent que $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

– III – Quelques propriétés de \mathbb{Z}_n^*

1. (a) Pour y, z dans \mathbb{Z}_n , on a :

$$\sigma(x)(y+z) = x(y+z) = xy + xz = \sigma(x)(y) + \sigma(x)(z),$$

c'est-à-dire que $\sigma(x)$ est un morphisme de groupes additifs.

Si $y \in \ker(\sigma(x))$, alors $xy = \bar{0}$ et $y = x^{-1}xy = \bar{0}$, c'est-à-dire que $\sigma(x)$ est injectif et donc bijectif puisque \mathbb{Z}_n est fini. On a donc bien $\sigma(x) \in \text{Aut}(\mathbb{Z}_n) = G_n$.

Ou bien : $(\sigma(x) \circ \sigma(x^{-1}))(y) = (\sigma(x^{-1}) \circ \sigma(x))(y) = y$ et automorphisme.

- (b) Pour x, x' dans \mathbb{Z}_n^* et y dans \mathbb{Z}_n , on a :

$$\sigma(xx')(y) = x(x'y) = (\sigma(x) \circ \sigma(x'))(y).$$

On a donc $\sigma(xx') = \sigma(x) \circ \sigma(x')$ et σ est un morphisme de groupes.

Si $\sigma(x) = I_d$, on a $\sigma(x)(\bar{1}) = \bar{1}$, soit $x = x\bar{1} = \bar{1}$, donc σ est injective.

Si $u \in G_n$ et $\bar{k} = u(\bar{1})$, alors pour tout $\bar{j} \in \mathbb{Z}_n$, on a :

$$u(\bar{j}) = u(j\bar{1}) = ju(\bar{1}) = j\bar{k} = \bar{j}\bar{k} = \sigma(\bar{k})\bar{j}.$$

L'application σ est donc surjective. En définitive σ réalise un isomorphisme de groupes de (\mathbb{Z}_n^*, \cdot) sur $(\text{Aut}(\mathbb{Z}_n), \circ)$.

2. (a) Du fait que tout élément de \mathbb{Z}_p^* a un ordre qui divise $p-1$, on déduit que $p-1 = \sum_{d \in \mathcal{D}_{p-1}} \psi(d)$.

- (b) Dire que $\psi(d) > 0$ équivaut à dire qu'il existe dans \mathbb{Z}_p^* au moins un élément x d'ordre d et le groupe $G = \{\bar{1}, x, \dots, x^{d-1}\}$ est alors formé de d solutions distinctes de l'équation $X^d - \bar{1} = \bar{0}$, or cette équation a au plus d solutions dans le corps commutatif \mathbb{Z}_p , il en résulte que G est exactement l'ensemble de toutes les solutions de cette équation. On déduit donc que les éléments d'ordre d dans \mathbb{Z}_p^* sont les générateurs du groupe cyclique G et on sait qu'il y a $\varphi(d)$ tels générateurs. On a donc $\psi(d) = \varphi(d)$ si $\psi(d) > 0$.

- (c) On a $p-1 = \sum_{d \in \mathcal{D}_{p-1}} \psi(d) = \sum_{d \in \mathcal{D}_{p-1}} \varphi(d)$ avec $\psi(d) = 0$ ou $\psi(d) = \varphi(d)$, ce qui entraîne que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$. En particulier, on a $\psi(p-1) > 0$, c'est-à-dire qu'il existe dans \mathbb{Z}_p^* des éléments d'ordre $p-1$ et ce groupe est alors cyclique d'ordre $p-1$.

3. (a) On a $C_p^k = \frac{p!}{k!(p-k)!}$ et p divise $k!(p-k)!C_p^k = p!$. Tout entier j compris entre 1 et $p-1$ étant premier avec p , on déduit du théorème de Gauss que p divise C_p^k si k est compris entre 1 et $p-1$.

- (b) On procède par récurrence sur $k \geq 0$. Pour $k = 0$, on prend $\lambda_0 = 1$. Pour $k = 1$, on a :

$$(1+p)^p = 1 + p^2 + \sum_{k=2}^p C_p^k p^k,$$

avec $C_p^k p^k$ divisible par p^3 pour k compris entre 2 et p si $p \geq 3$, ce qui donne :

$$(1+p)^p = 1 + p^2 + \nu p^3 = 1 + \lambda_1 p^2$$

avec $\lambda_1 = 1 + \nu p$ premier avec p . En supposant le résultat acquis pour $k \geq 1$, on a :

$$(1+p)^{p^{k+1}} = (1 + \lambda_k p^{k+1})^p = 1 + \lambda_k p^{k+2} + \sum_{j=2}^p C_p^j \lambda_k^j p^{j(k+1)},$$

avec $C_p^j \lambda_k^j p^{j(k+1)}$ divisible par p^{k+3} , pour j compris entre 2 et p , ce qui donne :

$$(1+p)^{p^{k+1}} = 1 + p^{k+2} (\lambda_k + \nu p) = 1 + \lambda_{k+1} p^{k+2},$$

avec $\lambda_{k+1} = \lambda_k + \nu p$ premier avec p si λ_k est premier avec p .

(c) $1+p$ étant premier avec p^α , on a bien $\overline{1+p} \in \mathbb{Z}_{p^\alpha}^*$ et avec :

$$\begin{cases} (1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \pmod{p^\alpha} \\ (1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \not\equiv 1 \pmod{p^\alpha} \end{cases}$$

($\lambda_{\alpha-2}$ est premier avec p , donc $\lambda_{\alpha-2} p^{\alpha-1}$ ne peut être divisible par p^α) on déduit que $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^*$.

(d) La classe modulo p , $x = k + p\mathbb{Z}$ est d'ordre $p-1$ dans \mathbb{Z}_p^* et du fait que $p^{\alpha-1} - 1$ est divisible par $p-1$ pour $\alpha \geq 2$, on déduit que $k^{p^{\alpha-1}-1} \equiv 1 \pmod{p}$ et $k^{p^{\alpha-1}} \equiv k \pmod{p}$, ce qui entraîne que la classe modulo p de $j = k^{p^{\alpha-1}}$ est d'ordre $p-1$ dans \mathbb{Z}_p^* . D'autre part avec :

$$j^{p-1} = k^{(p-1)p^{\alpha-1}} = k^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

on déduit que $y = j + p^\alpha \mathbb{Z} = k^{p^{\alpha-1}} + p^\alpha \mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^*$ (si $j^r \equiv 1 \pmod{p^\alpha}$ avec $r \geq 1$, alors p^α et donc p divise $j^r - 1$ ce qui entraîne $j^r \equiv 1 \pmod{p}$ et r est multiple de $p-1$).

(e) Dans $\mathbb{Z}_{p^\alpha}^*$ on a $x = \overline{1+p}$ d'ordre $p^{\alpha-1}$ et un élément y d'ordre $p-1$ avec $p-1$ et $p^{\alpha-1}$ premiers entre eux, il en résulte que $z = xy$ est d'ordre $\text{ppcm}(p-1, p^{\alpha-1}) = (p-1)p^{\alpha-1} = \varphi(p^\alpha)$ dans $\mathbb{Z}_{p^\alpha}^*$. En conséquence $\mathbb{Z}_{p^\alpha}^*$ est cyclique d'ordre $\mathbb{Z}_{p^\alpha}^*$.

4. On a $\mathbb{Z}_2^* = \{\overline{1}\}$ et $\mathbb{Z}_4^* = \{\overline{1}, \overline{-1}\} \approx \mathbb{Z}_2$.

5. (a) On procède par récurrence sur $k \geq 0$. Pour $k = 0$, on a $5 = 1 + 2^2$ et $\lambda_0 = 1$. Pour $k = 1$, on a $5^2 = 1 + 3 * 2^3$ et $\lambda_1 = 3$. En supposant le résultat acquis pour $k \geq 1$, on a :

$$5^{2^{k+1}} = (1 + \lambda_k 2^{k+2})^2 = 1 + \lambda_{k+1} 2^{k+3},$$

avec $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} = \lambda_k (1 + \lambda_k 2^{k+1})$ impair si λ_k l'est.

(b) On a $5^{2^{\alpha-2}} = 1 + \lambda_{\alpha-2} 2^\alpha \equiv 1 \pmod{2^\alpha}$ et $5^{2^{\alpha-3}} = 1 + \lambda_{\alpha-3} 2^{\alpha-1} \not\equiv 1 \pmod{2^\alpha}$ du fait que $\lambda_{\alpha-3} \equiv 1 \pmod{2}$. On a donc $5 + 2^\alpha \mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^*$ et $H = \langle 5 + 2^\alpha \mathbb{Z} \rangle$ est un sous-groupe cyclique d'ordre $2^{\alpha-2}$ de $\mathbb{Z}_{2^\alpha}^*$, il est donc isomorphe à $\mathbb{Z}_{2^{\alpha-2}}$.

(c) Si $k \equiv k' \pmod{2^\alpha}$ alors 2^α divise $k - k'$ et $k \equiv k' \pmod{4}$ ($\alpha \geq 2$), donc l'application ψ est bien définie. Dire que $k + 2^\alpha \mathbb{Z}$ est inversible dans \mathbb{Z}_{2^α} équivaut à dire que k est premier avec 2^α et donc avec 4, c'est-à-dire que ψ envoie $\mathbb{Z}_{2^\alpha}^*$ dans \mathbb{Z}_4^* . Il est facile de vérifier que ψ est un morphisme de groupes multiplicatifs. Si $x = k + 4\mathbb{Z}$ est inversible

dans \mathbb{Z}_4 alors $k \equiv 1 \pmod{4}$ ou $k \equiv -1 \pmod{4}$ et $x = \psi(y)$ avec $y = 1 + 2^\alpha \mathbb{Z}$ ou $y = -1 + 2^\alpha \mathbb{Z}$ dans $\mathbb{Z}_{2^\alpha}^*$, c'est-à-dire que ψ est surjective. Par passage au quotient ψ induit alors un isomorphisme de $\frac{\mathbb{Z}_{2^\alpha}^*}{\ker(\psi)}$ sur \mathbb{Z}_4^* , il en résulte que :

$$\text{card}(\mathbb{Z}_{2^\alpha}^*) = \text{card}(\ker(\psi)) \text{card}(\mathbb{Z}_4^*) = 2 \text{card}(\ker(\psi))$$

et $\text{card}(\ker(\psi)) = 2^{\alpha-2}$. Avec $5 + 2^\alpha \mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\ker(\psi)$ ($5 \equiv 1 \pmod{4}$) on déduit que $\ker(\psi)$ est cyclique d'ordre $2^{\alpha-2}$ engendré par $5 + 2^\alpha \mathbb{Z}$.

- (d) Pour $x \in \mathbb{Z}_{2^\alpha}^*$, on a $\psi(x) \in \mathbb{Z}_4^* = \{\bar{1}, \bar{-1}\}$. Si $\psi(x) = \bar{1}$, alors $\psi(x)x = x \in \ker(\psi)$ et si $\psi(x) = \bar{-1}$, alors $\psi(x)x = -x$ et $\psi(\psi(x)x) = -\psi(x) = \bar{1}$ et $\psi(x)x \in \ker(\psi)$. Du fait que ψ est un morphisme de groupes multiplicatifs, on déduit qu'il en est de même de π .

Si $x \in \ker(\pi)$, alors $\psi(x) = \bar{1}$ et $\psi(x)x = \bar{1}$, donc $x = \bar{1}$ et π est injectif. Ces deux groupes ayant même cardinal, on déduit que π est un isomorphisme. En résumé $\mathbb{Z}_{2^\alpha}^*$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ pour $\alpha \geq 3$ et $\mathbb{Z}_{2^\alpha}^*$ n'est pas cyclique puisqu'il n'y a pas d'élément d'ordre $2^{\alpha-1}$ dans $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$.

– IV – Nombres de Carmichael

- Si n est pair, alors $n-1$ est impair et $(\bar{-1})^{n-1} = \bar{-1}$ ($n \neq 2$) et n n'est pas un nombre de Carmichael.
- Soit $x = \bar{k} \in \mathbb{Z}_n^*$ avec k entier relatif premier avec n . Pour tout i compris entre 1 et r , l'entier k est premier avec p_i et le théorème de Fermat nous dit que $k^{p_i-1} \equiv 1 \pmod{p_i}$, ce qui entraîne $k^{n-1} \equiv 1 \pmod{p_i}$ puisque $n-1$ est multiple de p_i-1 . On a donc p_i qui divise $k^{n-1} - 1$ pour tout i compris entre 1 et r , les p_i étant premiers et distincts, il en résulte que $n = \prod_{i=1}^r p_i$ divise $k^{n-1} - 1$, soit $\bar{k}^{n-1} = \bar{1}$ dans \mathbb{Z}_n^* et donc n est un nombre de Carmichael.
- (a) i. Le groupe multiplicatif $\mathbb{Z}_{p_i^{\alpha_i}}^*$ est d'ordre $\varphi(p_i^{\alpha_i}) = (p_i-1)p_i^{\alpha_i-1}$ et pour $\alpha_i \geq 2$, p_i est un diviseur premier de l'ordre de ce groupe, on sait alors qu'il existe dans $\mathbb{Z}_{p_i^{\alpha_i}}^*$ un élément $x = p + p_i^{\alpha_i} \mathbb{Z}$ d'ordre p_i . D'autre part le théorème chinois nous dit que l'application :

$$t + n\mathbb{Z} \mapsto (t + p_1^{\alpha_1} \mathbb{Z}, \dots, t + p_r^{\alpha_r} \mathbb{Z})$$

réalise un isomorphisme d'anneaux de \mathbb{Z}_n sur $\prod_{i=1}^r \mathbb{Z}_{p_i^{\alpha_i}}$ et ce isomorphisme induit

un isomorphisme de groupes de \mathbb{Z}_n^* sur $\prod_{i=1}^r \mathbb{Z}_{p_i^{\alpha_i}}^*$, en conséquence l'élément

$(1 + p_1^{\alpha_1} \mathbb{Z}, \dots, 1 + p_i^{\alpha_i} \mathbb{Z}, \dots, 1 + p_r^{\alpha_r} \mathbb{Z}) \in \prod_{i=1}^r \mathbb{Z}_{p_i^{\alpha_i}}^*$ a un unique antécédent $q + n\mathbb{Z}$ dans \mathbb{Z}_n^* , ce qui se traduit par l'existence d'un entier relatif q premier avec n et solution de :

$$\begin{cases} q \equiv p \pmod{p_i^{\alpha_i}} \\ q \equiv 1 \pmod{p_j^{\alpha_j}} \end{cases} \quad (1 \leq j \neq i \leq r).$$

- L'entier q étant premier avec n , la classe résiduelle $x = q + n\mathbb{Z}$ est dans \mathbb{Z}_n^* et $x^{n-1} = \bar{1}$, c'est-à-dire que $q^{n-1} \equiv 1 \pmod{n}$, ce qui donne $q^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}$ d'après le théorème chinois, soit $p^{n-1} \equiv 1 \pmod{p_i^{\alpha_i}}$ puisque $q \equiv p \pmod{p_i^{\alpha_i}}$. En conséquence l'ordre p_i de $p + p_i^{\alpha_i} \mathbb{Z}$ dans $\mathbb{Z}_{p_i^{\alpha_i}}^*$ divise $n-1$, ce qui est en contradiction

avec p_i premier divisant n . En conclusion il ne peut pas exister d'indice i tel que $\alpha_i \geq 2$ si n est un nombre de Carmichael. On a donc $n = \prod_{i=1}^r p_i$.

- (b) Pour tout i compris entre 1 et r le groupe multiplicatif $\mathbb{Z}_{p_i}^*$ est cyclique d'ordre $p_i - 1$, il existe donc un élément $k_i + p_i\mathbb{Z}$ d'ordre $p_i - 1$ dans $\mathbb{Z}_{p_i}^*$ et en désignant par k un entier relatif premier avec n solution de :

$$\begin{cases} k \equiv k_i \pmod{p_i} \\ k \equiv 1 \pmod{p_j} \quad (1 \leq j \neq i \leq r) \end{cases}$$

(conséquence du théorème chinois), on a $k^{n-1} \equiv 1 \pmod{n}$ (n est un nombre de Carmichael et $k + n\mathbb{Z}$ est dans \mathbb{Z}_n^*), donc $k^{n-1} \equiv 1 \pmod{p_i}$, soit $k_i^{n-1} \equiv 1 \pmod{p_i}$ puisque $k \equiv k_i \pmod{p_i}$ et l'ordre de $k_i + p_i\mathbb{Z}$ dans $\mathbb{Z}_{p_i}^*$ qui est égal à $p_i - 1$ divise $n - 1$.

- (c) Supposons que $n = p_1 p_2$ avec $3 \leq p_1 < p_2$ premiers tels que $p_i - 1$ divise $n - 1$ pour $i = 1, 2$. En écrivant que $n - 1 = (p_1 - 1) + p_1(p_2 - 1)$, on déduit que $n - 1$ ne peut être divisible par $p_2 - 1$, en effet si $p_2 - 1$ divise $n - 1$ il divise $p_1 - 1$ avec $p_1 < p_2$, ce qui est impossible. En conséquence un nombre de Carmichael a au moins trois facteurs premiers.

Sous-groupes de $\mathcal{L}(E)$

On désigne par \mathbb{K} un corps commutatif, E un \mathbb{K} -espace vectoriel de dimension $n \geq 1$, $\mathcal{L}(E)$ la \mathbb{K} -algèbre des endomorphismes de E , $GL(E)$ le groupe des automorphismes de E , $\mathcal{M}_n(\mathbb{K})$ la \mathbb{K} -algèbre des matrices carrées d'ordre $n \geq 1$ à coefficients dans \mathbb{K} et $GL_n(\mathbb{K})$ le groupe multiplicatif des matrices carrées d'ordre $n \geq 1$ à coefficients dans \mathbb{K} qui sont inversibles.

Bibliographie

- [1] J. M. ARNAUDIES, J. LELONG-FERRAND — *Cours de Mathématiques. Tomes 1 à 4.* Dunod (1974).
- [2] M. AUDIN — *Géométries. De la licence à l'agrégation.* Belin (1998).
- [3] O. BORDELLES — *Thèmes d'arithmétique.* Ellipses (2006).
- [4] A. BOUVIER, D. RICHARD — *Groupes.* Hermann (1974).
- [5] M. CONDAMINE — *Algèbre. Terminale C-D-E.* Delagrave (1971).
- [6] J. M. DE KONINCK, A. MERCIER. *Introduction à la théorie des nombres.* Modulo. (1994).
- [7] M. DEMAZURE. *Cours d'algèbre.* Cassini. (1997).
- [8] C. DESCHAMPS, A. WARUSFEL. *Mathématiques tout en un. Série E. Ramis. Volumes 1 et 2.* Dunod. (1999).
- [9] R. DESCOMBES — *Éléments de théorie des nombres.* P. U. F. (1986).
- [10] J. DIEUDONNE. *Algèbre linéaire et géométrie élémentaire.* Hermann. (1968).
- [11] D. DUVERNEY. *Théorie des nombres.* Dunod. (1998).
- [12] F. R. GANTMACHER. *Théorie des matrices (Vol. 1 et 2).* Dunod (1966).
- [13] R. GOBLOT. *Algèbre commutative.* Masson (1996).
- [14] B. GOSTIAUX. *Cours de Mathématiques Spéciales. Volumes 1 à 4.* P. U. F. (1995).
- [15] X. GOURDON. *Les Maths en tête. Algèbre.* Ellipses.
- [16] A. GRAMAIN — *Géométrie élémentaire.* Hermann (1997).
- [17] F. GRAMAIN. *Nombres premiers et polynômes irréductibles.* Revue des Mathématiques Spéciales (Octobre 2000).
- [18] G. H. HARDY, E. M. WRIGHT. *An introduction to the theory of numbers.* Oxford (1979).
- [19] Y. HELLEGOUARCH — *Invitation aux mathématiques de Fermat-Wiles.* Masson (1997).
- [20] R. A. HORN, C. A. JOHNSON. *Matrix analysis.* Cambridge University Press (1985).
- [21] S. LANG. *Structures algébriques.* InterEditions (1976).
- [22] S. LANG. *Algèbre linéaire 1.* InterEditions (1976).
- [23] S. LANG. *Algèbre linéaire 2.* InterEditions (1976).
- [24] S. LANG — *Algèbre.* Dunod (2004).
- [25] J. LELONG-FERRAND. *Les fondements de la géométrie.* Presses universitaires de France (1985).
- [26] F. LIRET, D. MARTINAIS. *Cours de mathématiques. Analyse 1-ère et 2-ème année. Algèbre 1-ère et 2-ème année.* Dunod.
- [27] D. J. MERCIER. *Cours de géométrie, préparation au CAPES et à l'agrégation.* Publibook (2004).

- [28] R. MNEIMNE — *Eléments de géométrie (actions de groupes)*. Cassini (1997).
- [29] D. PERRIN — *Cours d'algèbre*. Ellipses (1996).
- [30] E. RAMIS, C. DESCHAMPS, J. ODOUX. *Cours de Mathématiques Spéciales. Volume 1 à 5*. Masson.
- [31] M. ROGALSKI. *Carrefours entre analyse algèbre et géométrie*. Ellipses (2001).
- [32] P. SAMUEL — *Théorie algébrique des nombres*. Hermann (1971).
- [33] L. SCHWARTZ — *Mathématiques pour la licence. Algèbre*. Dunod (1998).
- [34] A. SZPIRGLAS — *Exercices d'algèbre*. Cassini (2001).
- [35] P. TAUVEL. *Agrégation interne de Mathématiques. Cours de géométrie*. Masson.
- [36] P. TAUVEL. *Algèbre pour l'agrégation interne*. Masson.
- [37] C. TISSERON — *Géométries affine, projective et euclidienne*. Hermann (1983).
- [38] A. TISSIER. *Agrégation interne de Mathématiques. Mathématiques générales*. Bréal. (1991).
- [39] J. TRIGNAN — *La géométrie des nombres complexes*. Bréal (1983).