Algèbre générale

Jean-Romain Heu

2021

Introduction

Ce polycopié contient les définitions et propriétés du cours d'algèbre. La plupart des exemples et démonstrations seront donnés en cours.

L'ensemble des documents liés à ce cours sera disponible sur le site

jeanromain.heu.free.fr.

Des tests sur les différents chapitres seront accessibles sur Moodle :

https ://moodle.insa-strasbourg.fr

Les objectifs de ce cours sont les suivants.

- ★ Acquérir les méthodes de raisonnement et la rigueur scientifique.
- ★ Maîtriser le langage mathématique et savoir rédiger une démonstration.
- ★ Développer des capacités d'abstraction.
- ★ Maîtriser un certain nombre d'outils mathématiques indispensables pour la suite des études.

Afin d'atteindre ces objectifs, il est absolument nécessaire d'apprendre le cours, d'en étudier les démonstrations et les exemples et de préparer les exercices avant d'aller en travaux dirigés.

Le programme du cours est le suivant.

1. Logique, langage mathématique et raisonnements
2. Arithmétique
3. Ensembles et applications
4. Le corps des nombres complexes
5. Groupes, anneaux, corps
6. L'anneau des matrices

Le cours d'algèbre du second semestre sera consacré aux espaces vectoriels, à l'algèbre linéaire et aux équations différentielles.

I. Logique, langage mathématique et raisonnement

1 Éléments de logique

Définition

Une **proposition logique** est un énoncé mathématique auquel on peut attribuer une valeur de vérité, soit « vrai » soit « faux ».

Exemples « $2 < 3$ », « l'ensemble $\{3, a, 53\}$ possède 7 éléments », « 49 est un nombre premier », « $\cos^2(1) + \sin^2(1) = 1$ », « π est un nombre entier » sont des propositions logiques.

1.1 Connecteurs logiques

Les connecteurs logiques sont des opérations permettant de créer de nouvelles propositions à partir de propositions existantes.

La négation

Soit P une proposition. La négation de P, ou « non P », notée $\neg P$ est la proposition qui est vraie si P est fausse et fausse si P est vraie. On peut décrire la proposition $\neg P$ à l'aide d'une **table de vérité**.

P	$\neg P$
V	F
F	V

La conjonction (et)

La conjonction de deux propositions P et Q est la proposition « P et Q » notée également $P \wedge Q$ qui est vraie si P et Q le sont et qui est fausse sinon.

P	Q	P et Q
V	V	V
V	F	F
F	V	F
F	F	F

La disjonction (ou)

La disjonction de deux propositions P et Q est la proposition « P ou Q » notée également $P \vee Q$ qui est vraie si l'une au moins des deux propositions l'est et qui est fausse sinon.

P	Q	P ou Q
V	V	V
V	F	V
F	V	V
F	F	F

L'implication

Soient P et Q deux propositions. L'implication de P vers Q est la proposition $(\neg P)$ ou Q. On la note $P \Rightarrow Q$ et on la lit « P implique Q ».

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

★ L'implication $P \Rightarrow Q$ ne dit rien sur les valeurs de vérité de P et Q. Elle n'exprime rien de plus qu'un lien entre les deux propositions. Par exemple, $3 = 8$ et $4 = 9$ sont des propositions fausses mais l'implication $(3 = 8) \Rightarrow (4 = 9)$ est parfaitement vraie. En effet si on suppose que $3 = 8$, on en déduit facilement que $4 = 9$ en ajoutant 1 aux deux membres de l'égalité.

★ On appelle **réciproque** de l'implication $P \Rightarrow Q$, la proposition $Q \Rightarrow P$. Sa valeur de vérité est en général indépendante de celle de $P \Rightarrow Q$.
Par exemple, l'implication $(x = 2) \Rightarrow (x^2 = 4)$ est toujours vraie. Mais sa réciproque $(x^2 = 4) \Rightarrow (x = 2)$ est fausse si on considère le cas $x = -2$.

Propriété

★ **Modus ponens** : soient P et Q des propositions logiques. Alors l'implication $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ est une **tautologie**, *i.e.* une proposition de valeur de vérité toujours vraie.

Cette proposition correspond au raisonnement logique le plus élémentaire : si P est vraie et si l'implication $P \Rightarrow Q$ l'est aussi, alors on peut en déduire que Q est vraie.

★ **Transitivité de l'implication** : soient P, Q et R des propositions logiques. La proposition

$$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow [P \Rightarrow R]$$

est également une tautologie : si $P \Rightarrow Q$ et $Q \Rightarrow R$ sont vraies, alors $P \Rightarrow R$ est vraie.

L'équivalence

L'équivalence de deux propositions P et Q est la proposition $(P \Rightarrow Q$ et $Q \Rightarrow P)$. On la note $P \Leftrightarrow Q$ et on la lit « P équivaut à Q ».

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Exercice À l'aide de tous ces connecteurs logiques, on peut définir d'autres propositions logiques. Soient par exemple deux propositions P et Q. Posons R la proposition

$$(P \wedge \neg Q) \Rightarrow (\neg Q \Rightarrow \neg P).$$

Calculer la table de vérité de R et reconnaître ainsi la proposition R.

P	Q	$\neg Q$	$\neg P$	$P \wedge \neg Q$	$\neg Q \Rightarrow \neg P$	R
V	V					
V	F					
F	V					
F	F					

On dispose d'un certain nombre de règles permettant de simplifier les propositions logiques. Nous noterons $P \cong Q$ pour dire que les propositions P et Q ont la même table de vérité.

Propriété

Soient P et Q deux propositions logiques.

★ $\neg(\neg P) \cong P$, $\quad P \wedge P \cong P$, $\quad P \vee P \cong P$.

★ $(P \Rightarrow Q) \cong (\neg Q \Rightarrow \neg P)$.
On dit que $\neg Q \Rightarrow \neg P$ est la **contraposée** de $P \Rightarrow Q$.

★ **Lois de Morgan** :
$\neg(P \text{ ou } Q) \cong (\neg P \text{ et } \neg Q)$
$\neg(P \text{ et } Q) \cong (\neg P \text{ ou } \neg Q)$.

★ **Négation de l'implication** : $\neg(P \Rightarrow Q) \cong (P \text{ et } \neg Q)$.

Exercice Simplifier la proposition R en utilisant ces règles.

À retenir

★ Comprendre et interpréter les propositions définies à l'aide de connecteurs logiques.
★ Être capable d'en déterminer la véracité.
★ Ne pas confondre contraposée et réciproque.
★ Savoir définir la négation d'une proposition.
★ Connaître les règles de simplification des propositions.

1.2 Quantificateurs

On peut avoir besoin d'utiliser des propositions contenant une ou plusieurs variables. Une telle proposition logique est appelée prédicat.

Exemples « Pour tout nombre entier relatif x, le nombre x^2 est positif », « il existe un nombre entier relatif dont le carré vaut 4 » sont des prédicats.

Symboles

- ★ Le symbole $\forall$ signifie « pour tout ». Par exemple, le prédicat ci-dessus s'écrit : $\forall x \in \mathbf{Z}, x^2 \geq 0$.
- ★ Le symbole $\exists$ signifie « il existe ». Le deuxième prédicat ci-dessus s'écrit : $\exists x \in \mathbf{Z}, x^2 = 4$.
- ★ Le symbole $\exists!$ signifie « il existe un unique ». Par exemple $\exists! x \in \mathbf{Z}, x^2 = 4$ est un prédicat de valeur de vérité fausse, mais $\exists! x \in \mathbf{N}, x^2 = 4$ est de valeur de vérité vraie.

Remarques Les symboles $\forall$ et $\exists$ sont respectivement un A et un E retournés, initiales des mots allemands « Alle » (tous) et « Existieren ».

Les variables apparaissant après ces symboles sont muettes, leurs écritures pourraient être remplacées par n'importe quels autres symboles :

$$\exists x \in \mathbf{N}, x^2 - 5x + 6 = 0 \quad \text{et} \quad \exists y \in \mathbf{N}, y^2 - 5y + 6 = 0$$

sont deux écritures d'un même prédicat.

Dans un prédicat faisant intervenir plusieurs variables, l'ordre des quantificateurs est important. On ne peut pas intervertir un $\forall$ et un $\exists$. Par contre, on peut intervertir deux $\forall$ ou deux $\exists$ successifs.

Par exemple, $\forall x \in \mathbf{N}, \exists y \in \mathbf{Z},\ x + y = 0$ et $\exists y \in \mathbf{Z}, \forall x \in \mathbf{N},\ x + y = 0$ ne sont pas les mêmes prédicats. Il est important de noter que dans ce premier exemple, la variable y dépend de x (pour éviter les erreurs, on devrait la noter y_x), ce qui n'est plus le cas dans le second exemple. Par contre, $\exists x \in \mathbf{Z}, \exists y \in \mathbf{R},\ x + y^2 = 0$ et $\exists y \in \mathbf{R}, \exists x \in \mathbf{Z},\ x + y^2 = 0$ représentent le même prédicat. Ici, on peut dire que y et x dépendent chacun l'un de l'autre. Cette proposition s'exprime en fait plus clairement sous la forme $\exists (x, y) \in \mathbf{Z} \times \mathbf{R},\ x + y^2 = 0$.

Propriété

Soit $P(x)$ un prédicat dépendant d'une variable x. Alors

- ★ $\neg(\forall x, P(x)) \ \cong \ (\exists x, \neg P(x))$
- ★ $\neg(\exists x, P(x)) \ \cong \ (\forall x, \neg P(x))$

2 Axiomes

Au XIXème siècle, les mathématiciens se sont retrouvés coincés face à un grand nombre de problèmes. L'une des raisons principales de leurs échecs est le fait que les mathématiques ne reposaient alors pas sur des bases solides. Les objets et concepts étaient définis de manière imprécise alors que les problèmes mathématiques nécessitaient une rigueur plus grande qu'auparavant. Les mathématiciens ont donc commencé à s'intéresser à la structure de leur langage et ils ont choisi comme notion de base la notion d'ensemble. Ils ont ainsi construit de manière axiomatique la théorie des ensembles et toutes les autres théories mathématiques reposent sur le langage de la théorie des ensembles.

Un axiome est une proposition logique à laquelle on attribue la valeur de vérité Vrai. Les valeurs de toutes les autres propositions logiques que l'on peut formuler doivent se déduire de ces axiomes. Un théorème est une proposition logique dont on a déduit des axiomes que sa valeur de vérité est vrai.

Nous ne détaillerons pas l'axiomatique de la théorie des ensembles. Pour nous, un ensemble sera simplement une collection d'objets appelés éléments. Nous en reparlerons au chapitre 2. Donnons juste un exemple simplifié d'une définition axiomatique : la définition de l'ensemble des entiers naturels.

Définition de N

Il existe un ensemble $\mathbf{N}$ appelé ensemble des entiers naturels tel que

- ★ $\mathbf{N}$ est non vide ;
- ★ tout entier n admet un successeur noté $s(n)$;
- ★ deux entiers qui ont même successeur sont égaux ;
- ★ il existe un entier, noté 0, qui n'est le successeur d'aucun entier ;
- ★ toute partie A de $\mathbf{N}$ contenant 0 et stable par successeur ($s(A) \subset A$) est égale à $\mathbf{N}$.

À partir de ces axiomes, on peut définir naturellement une notion d'ordre sur $\mathbf{N}$, une addition, une multiplication, et finalement retrouver l'ensemble des entiers naturels tel que nous nous le représentons.

Définition

★ On définit récursivement une **relation d'ordre** sur les entiers naturels de la façon suivante :

$$\forall n \in \mathbf{N}, \forall m \in \mathbf{N}, \quad n \leqslant m \text{ si } (n = m \text{ ou } s(n) \leqslant m)$$

★ On définit l'**addition** des entiers naturels à partir des deux axiomes suivants :

- ⋆ $\forall n \in \mathbf{N}, \quad n + 0 = 0 + n = n$;
- ⋆ $\forall n \in \mathbf{N}, \forall m \in \mathbf{N}, \quad n + s(m) = s(n) + m.$

★ On définit la **multiplication** des entiers naturels à partir des deux axiomes suivants :

- ⋆ $\forall n \in \mathbf{N}, \quad n \times 0 = 0 \times n = 0$;
- ⋆ $\forall n \in \mathbf{N}, \forall m \in \mathbf{N}, \quad n \times s(m) = n \times m + n.$

De telles définitions peuvent s'interpréter de manière algorithmique et permettent ainsi de définir pour l'ordinateur les opérations arithmétiques de base.

On peut ensuite démontrer des théorèmes. Quelques exemples :

Théorème

★ $\mathbf{N}$ est infini.

★ $\mathbf{N}$ est archimédien : $\forall A \in \mathbf{N}, \ \forall a \in \mathbf{N}^*, \ \exists n \in \mathbf{N}, \ \ an > A.$

★ Toute partie non vide de $\mathbf{N}$ contient un plus petit élément :

$$\forall F \subset \mathbf{N}, \ F \neq \emptyset \Rightarrow \exists m \in F, \ \forall n \in F, \ n \geq m.$$

À retenir

★ Savoir interpréter des propositions définies à l'aide de quantificateurs.

★ Être capable d'exprimer leurs négations.

★ Faire la différence entre un axiome et un théorème.

★ Être capable de déduire des théorèmes d'un système axiomatique.

3 Raisonnements

Nous présentons ici les différents types de raisonnements permettant de démontrer des théorèmes ainsi que la manière de rédiger ces raisonnements.

3.1 Raisonnements primaires

Commençons par considérer les quantificateurs apparaîssant dans une proposition.

Proposition du type $\forall x, P(x)$

Démontrer que la proposition "pour tout x, la propriété $P(x)$ est vraie" revient en théorie à montrer un grand nombre de propriétés (autant qu'il y a de valeurs possibles pour x). Il est parfois possible de le faire mais c'est souvent fastidieux voire impossible. Pour éviter cela, il suffit de considérer un élément x quelconque et de vérifier pour cet x que la propriété est vraie. Ainsi une démonstration d'une telle proposition commence toujours par

« Soit x. »

Puis une suite de raisonnements permet de montrer que la propriété $P(x)$ est vraie. Enfin on conclut par

« x étant quelconque, nous avons bien montré que la propriété est vraie pour tout x. »

Exemple Démontrer : $\forall x \in \mathbf{R}_+, \quad \frac{x}{2x+1} < 1$.

Soit $x \in \mathbf{R}_+$. Comme x est positif, on peut écrire $x \leqslant 2x$. Donc $x < 2x + 1$. Enfin, comme $2x + 1$ est également positif, on peut diviser par ce nombre sans changer le sens de l'inégalité : $\frac{x}{2x+1} < 1$.
Le nombre x étant quelconque, nous avons bien démontré que pour tout réel positif x, $\frac{x}{2x+1} < 1$.

Proposition du type $\exists x, P(x)$

Ce type de proposition est en général plus difficile à démontrer. Soit on dispose d'un argument général assurant l'existence d'un tel x, soit il faut déterminer précisemment un tel élément x. Dans ce second cas, on commence par une analyse du problème. On suppose qu'on dispose d'un élément x vérifiant $P(x)$ puis à l'aide d'une suite de raisonnements, on détermine les valeurs possibles pour x. Enfin on effectue une synthèse qui sera la démonstration de la proposition. On prend une des valeurs de x que l'on a trouvées et on vérifie que la propriété $P(x)$ est vraie.

Exemple Démontrer : $\exists x \in \mathbf{R}, \quad \frac{1}{x-2} > \frac{3}{x+1}$.

Posons $x = \frac{21}{10}$. Alors $x - 2 = \frac{1}{10}$ et $\frac{1}{x-2} = 10$. D'autre part, $x + 1 = \frac{31}{10}$ et $\frac{3}{x+1} = \frac{30}{31}$. On obtient bien $\frac{1}{x-2} > \frac{3}{x+1}$. Nous avons donc bien démontré l'existence d'un nombre réel satisfaisant l'inégalité.
Remarque : pour que la démonstration soit valable, il n'est pas utile de préciser comment x a été trouvé. Dans le cas présent, nous avons choisi une valeur de x légèrement supérieure à 2 afin que $\frac{1}{x-2}$ soit élevé.

Une autre démonstration est possible en utilisant des propriétés analytiques des fonctions. On peut faire l'étude de la fonction f définie sur $\mathbf{R} \setminus \{-1, 2\}$ par $f(x) = \frac{1}{x-2} - \frac{3}{x+1}$ et déduire de son tableau de variation qu'elle est strictement positive sur $]2, \frac{7}{2}[$. Ainsi, pour tout x appartenant à cet intervalle, $\frac{1}{x-2} > \frac{3}{x+1}$. En particulier, il existe bien un réel x satisfaisant l'inégalité.

Proposition du type $\exists! x, P(x)$

La démonstration se divise en deux parties : <u>existence</u> et <u>unicité</u>. Tout d'abord, on démontre l'existence d'un tel x comme ci-dessus. Puis on démontre son unicité. Pour cela, on considère deux éléments quelconques x et y tels que $P(x)$ et $P(y)$ soient vraies. Puis on démontre que $x = y$. Cela prouve que toutes les solutions du problème sont égales. Comme il en existe une, elle est unique.

Exemple Démontrer : $\exists! x \in \mathbf{R}_+, \quad x^2 = 2$.

<u>Existence</u> : posons $x = \sqrt{2}$. Alors x est bien un réel positif et $x^2 = \sqrt{2}^2 = 2$. L'existence est ainsi démontrée.

<u>Unicité</u> : considérons deux nombres réels positifs x et y tels que $x^2 = 2$ et $y^2 = 2$. Montrons que $x = y$. On a $x^2 = y^2$, donc $x^2 - y^2 = 0$. On factorise : $(x - y)(x + y) = 0$. Donc $x - y = 0$ ou $x + y = 0$.

Or x et y sont des nombres positifs par hypothèse, et même strictement positifs car leur carré vaut 2. Donc $x + y > 0$. Finalement il reste $x - y = 0$, donc $x = y$: il ne peut y avoir qu'un seul nombre positif dont le carré vaut 2.

Proposition du type $P \Rightarrow Q$

Pour démontrer directement une telle proposition, on suppose que P est vraie. Puis on en déduit que Q est également vraie.

Exemple Démontrer l'implication : $\forall x \in \mathbf{R}, \quad \sqrt{x-3} = \sqrt{1-x} \Rightarrow x = 2$.

Soit x un nombre réel quelconque. Supposons que $\sqrt{x-3} = \sqrt{1-x}$. Alors en élevant au carré des deux côtés de l'égalité, on obtient $x - 3 = 1 - x$. On en déduit bien que $x = 2$ et l'implication est ainsi démontrée.

Remarque : avec notre démonstration, nous n'avons pas résolu l'équation $\sqrt{x-3} = \sqrt{1-x}$. Pour ce faire, il faut encore vérifier que le candidat $x = 2$ satisfait bien l'équation. En l'occurrence, il y a un problème puisque $2 - 3 < 0$ et ainsi $\sqrt{2-3}$ n'est pas défini.

Notre implication nous a permis de démontrer que s'il existe une solution à l'équation, alors c'est nécessairement $x = 2$. Mais rien ne garantit dans notre preuve que c'est bien une solution. Ici, l'équation proposée ne possède aucune solution.

Proposition du type $P \Leftrightarrow Q$

Pour démontrer une équivalence, on utilise une double implication. On démontre $P \Rightarrow Q$ comme ci-dessus puis on démontre $Q \Rightarrow P$. Enfin on conclut $P \Leftrightarrow Q$.

Exemple Démontrer l'équivalence : $\forall x \in \mathbf{R},\ \sqrt{x-3} = \sqrt{5-x} \Leftrightarrow x = 4$.
Cette fois-ci, on nous demande de résoudre complètement l'équation. On raisonne par double implication en commençant par chercher des candidats puis en les vérifiant.

Soit x un nombre réel quelconque.
$\Rightarrow$: Supposons que $\sqrt{x-3} = \sqrt{5-x}$. Alors en élevant au carré des deux côtés de l'égalité, on obtient $x - 3 = 5 - x$. On en déduit bien que $x = 4$ et la première implication est ainsi démontrée : $\sqrt{x-3} = \sqrt{5-x} \Rightarrow x = 4$.

$\Leftarrow$: Supposons maintenant $x = 4$. Alors $4 - 3 \geqslant 0$ et $5 - 4 \geqslant 0$. Leur racines carrées sont donc bien définies et on a $\sqrt{4-3} = 1 = \sqrt{5-4}$. Ainsi $x = 4 \Rightarrow \sqrt{x-3} = \sqrt{5-x}$.

Par double implication, nous avons démontré l'équivalence $\sqrt{x-3} = \sqrt{5-x} \Leftrightarrow x = 4$ pour tout nombre réel x.

3.2 Démonstrations

Le langage des mathématiques est avant tout pour nous la langue française. Les symboles mathématiques ne servent qu'à abréger les expressions. Une démonstration doit donc être rédigée. En particulier, toutes les assertions mathématiques doivent être reliées par des connecteurs logiques de la langue. Par exemple : donc, or, si, alors, mais, cependant, de plus...

Raisonnement direct

C'est le mode de raisonnement le plus classique. Il consiste à partir des hypothèses, puis à l'aide d'implications successives, à aboutir au résultat recherché.

L'exemple le plus célèbre est le suivant :
Tous les hommes sont mortels. (hypothèse)
Or Socrate est un homme. (hypothèse)
Donc Socrate est mortel. (conclusion)

Raisonnement par contraposée

Lorsque l'on doit démontrer une implication de la forme $P \Rightarrow Q$, on peut très bien démontrer sa contraposée $\neg Q \Rightarrow \neg P$ qui lui est équivalente. On suppose donc $\neg Q$ et on montre $\neg P$. On peut alors conclure que $P \Rightarrow Q$ est vrai.

Exemple Démontrer : $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad x + y \geqslant 0 \Rightarrow (x \geqslant 0 \text{ ou } y \geqslant 0)$.

Commençons par traduire l'énoncé : si la somme de deux nombres réels est positive, alors au moins l'un des deux est positif.

Raisonnons par contraposée et démontrons que si deux nombres sont strictement négatifs, alors leur somme le sera aussi : $\forall x \in \mathbf{R}, \forall y \in \mathbf{R}, \quad (x < 0 \text{ et } y < 0) \Rightarrow x + y < 0$.

Soient x et y des réels. Supposons $x < 0$ et $y < 0$. Alors, en additionnant, $x + y < 0$. Notre résultat est donc démontré. Et par contraposée, la proposition intiale l'est également.

Raisonnement par l'absurde

Raisonner par l'absurde pour démontrer une proposition consiste à supposer que la proposition est fausse. En partant de cette hypothèse, on effectue une suite de raisonnements qui doit aboutir à une absurdité, c'est-à-dire une proposition dont on sait qu'elle est fausse. On peut alors conclure que l'hypothèse de départ est fausse et donc que la proposition à démontrer est vraie.

Exemple Démontrer qu'il n'existe pas de triangle rectangle équilatéral.

L'énoncé exclut de fait le cas pathologique d'un triangle réduit à un point. Supposons par l'absurde qu'il existe un triangle rectangle équilatéral. Notons alors a, b et c les longueurs de ses côtés, a étant celle de l'hypoténuse. Alors, d'après le théorème de Pythagore, $a^2 = b^2 + c^2$. Or le triangle est équilatéral donc $a = b = c$. On obtient ainsi $a^2 = a^2 + a^2 = 2a^2$. Comme $a \neq 0$, on en déduit $1 = 2$. Nous avons donc abouti à une absurdité. Notre hypothèse initiale est ainsi infirmée et il ne peut pas exister de triangle rectangle équilatéral.

Raisonnement avec disjonction de cas

Si un énoncé est de la forme $\forall x \in E, P(x)$ avec $E = A \cup B$, la disjonction de cas consiste à démontrer les propositions $\forall x \in A, P(x)$ et $\forall x \in B, P(x)$. Il peut y avoir bien sûr plus de deux cas, l'important étant de bien couvrir l'ensemble des cas possibles.

Exemple Démontrer : $\forall x \in \mathbf{R}, \ x - 1 < |x| + 2$.

Soit $x \in \mathbf{R}$. On distingue deux cas : $x \geqslant 0$ et $x < 0$.

Si $x \geqslant 0$, alors $|x| = x$. Comme $-1 < 2$, on déduit $x - 1 < x + 2$, donc $x - 1 < |x| + 2$.

Si $x < 0$, alors $x - 1 < 0$. Et comme $|x| \geqslant 0$, on a $|x| + 2 > 0$. On en déduit encore $x - 1 < |x| + 2$.

Ainsi, dans les deux cas, on démontre que $x - 1 < |x| + 2$ et le résultat est donc démontré pour tout nombre réel x.

Raisonnement par récurrence

Le raisonnement par récurrence repose sur le dernier axiome de Péano. On souhaite démontrer une proposition de la forme $\forall n \in \mathbf{N}, P(n)$. Le raisonnement s'effectue en deux étapes :

- ★ Initialisation : on démontre la proposition $P(0)$,
- ★ Hérédité : on démontre $\forall n \in \mathbf{N}, P(n) \Rightarrow P(n+1)$. Autrement dit, on choisit n quelconque et on suppose $P(n)$ vraie. On montre alors que $P(n+1)$ est vraie.

On peut alors conclure par récurrence que $P(n)$ est vrai pour tout n.

Il faut savoir adapter ce raisonnement. On doit parfois effectuer l'initialisation pour plusieurs valeurs de n ou utiliser une **récurrence forte** pour l'hérédité.

Exemples Pour $n \in \mathbf{N}^*$, on définit sur $\mathbf{R}$ la fonction f_n par $f_n(x) = x^n$. Démontrer, par récurrence sur n, que sa dérivée est définie sur $\mathbf{R}$ par $f_n'(x) = nx^{n-1}$.

Initialisation : soit $n = 1$. La fonction f_1 est définie par $f_1(x) = x^1 = x$. Sa dérivée en un point x_0 est définie par la limite de son taux d'accroissement (si elle existe) : $f_1'(x_0) = \lim_{x\to x_0} \frac{f_1(x)-f_1(x_0)}{x-x_0} = \lim_{x\to x_0} \frac{x-x_0}{x-x_0} = 1$. Ainsi la dérivée de f_1 est donnée par $f_1(x) = 1 = 1 \cdot x^0$. Le résultat est démontré au rang $n = 1$.

Hérédité : soit $n \in \mathbf{N}^*$. Supposons la propriété vraie pour n : $f_n'(x) = nx^{n-1}$. Démontrons alors qu'elle est vraie au rang $n+1$: $f_{n+1}'(x) = (n+1)x^n$. Utilisons la propriété de la dérivée d'un produit : $(fg)' = f'g + fg'$. Ici $f_{n+1}(x) = x^{n+1} = x \cdot x^n$. Donc $f_{n+1} = f_1 f_n$. Or nous avons déjà calculé la dérivée de f_1 et nous connaissons celle de f_n par hypothèse de récurrence. Ainsi $f_{n+1}' = f_1' f_n + f_1 f_n'$ et on obtient pour tout x : $f_{n+1}'(x) = 1 \cdot x^n + x \cdot nx^{n-1} = (n+1)x^n$. La propriété est donc vérifiée au rang $n+1$ si elle l'est au rang n.

Par récurrence nous avons bien démontré la propriété pour tout entier $n \geqslant 1$.

On définit $u_1 = 1$, et pour tout $n \geqslant 1$, u_{n+1} est la moyenne des n premiers termes de la suite. Démontrer, à l'aide d'une récurrence forte sur n que pour tout $n \in \mathbf{N}^*$, $u_n = 1$.

Initialisation : $u_1 = 1$ par définition, donc le résultat est vérifié pour $n = 1$.

Hérédité : soit $n \geqslant 1$. Supposons que pour tout entier k tel que $1 \leqslant k \leqslant n$, $u_k = 1$. Montrons alors que $u_{n+1} = 1$. Par définition, $u_{n+1} = \frac{1}{n}\sum_{k=1}^{n} u_k$. Or par hypothèse de récurrence, chacun des termes de cette somme vaut 1. Ainsi $u_{n+1} = \frac{1}{n}\sum_{k=1}^{n} 1 = \frac{n}{n} = 1$.

La proposition est ainsi démontrée par récurrence.

À retenir

- ★ Connaître les différents types de raisonnements.
- ★ Être capable de construire un raisonnement élaboré.
- ★ Savoir rédiger une démonstration.
- ★ Savoir rédiger une démonstration !

II. Arithmétique

L'un des objectifs de ce chapitre est de montrer comment une théorie mathématique se construit et d'illustrer les différents types de raisonnements vus dans le premier chapitre.

1 Divisibilité

Définition : divisibilité

Soient d et n des nombres entiers. On dit que d **divise** n et on note $d|n$ si $\exists k \in \mathbf{Z},\ n = dk$.
On dit aussi que d est un **diviseur** de n et que n est un **multiple** de d.

Exemple 28 est un multiple de -7 car $28 = (-7)\times(-4)$. 0 est le multiple de tout entier n puisqu'on peut écrire $0 = n\times 0$. En revanche 0 n'est le diviseur d'aucun entier n hormis 0 puisque, par exemple, $0 = 0\times 15$.

Propriété

Soient a, b et d des nombres entiers.

- ⊛ Si $d \mid a$ et $a \mid d$, alors $a = \pm d$: si a et d sont multiples l'un de l'autre, alors $a = \pm d$.
- ⊛ Si $d \mid a$, alors $d \mid ab$: si d divise un nombre, il divise tous ses multiples.
- ⊛ Si $d \mid a$ et $d \mid b$, alors $d \mid a+b$: si deux nombres sont multiples de d, leur somme est aussi multiple de d.
- ⊛ Si $d \mid a$ et $a \mid b$, alors $d \mid b$: la divisibilité est transitive.

Définition : primalité

On appelle **nombre premier** tout nombre entier naturel ayant exactement deux diviseurs positifs : 1 et lui-même.
On notera $\mathbf{P}$ leur ensemble.

Attention, 1 n'est pas un nombre premier !

Théorème de la division euclidienne

Soient a et b des nombres entiers avec $b \neq 0$. Alors

$$\exists! n \in \mathbf{Z},\ \exists! r \in \mathbf{N},\quad a = nb + r \quad \text{et} \quad 0 \leqslant r < |b|.$$

Cette égalité est appelée **division euclidienne** de a par b ; n est le **quotient** de la division et r en est le **reste**.

Exemples Retournons à l'école élémentaire et effectuons la division de 197 par 27.
Combien de fois faut-il prendre 27 pour arriver à 197 ? On essaie : $27\times 3 = 81$, $27\times 6 = 162$. Il reste de la place pour approcher 197 : $27\times 7 = 189$. Cette fois c'est bon, le prochain multiple sera strictement supérieur à 197. Il ne reste qu'à calculer le reste : $197 - 27\times 7 = 8$ donc $197 = 27\times 7 + 8$ avec $0 \leqslant 8 < 27$.

Avec des nombres négatifs, c'est un peu moins naturel. Divisons -23 par -7 : $-23 = 4\times(-7) + 5$ avec $0 \leqslant 5 < |-7|$.

Généralisons l'idée proposée dans l'exemple pour en faire une démonstration.

Démonstration : Nous rédigeons la preuve pour les entiers positifs. Soient a et b dans $\mathbf{N}$ avec $b \neq 0$.

Existence : montrons l'existence de deux entiers n et r tels que $a = nb + r$ et $0 \leqslant r < b$.
• Posons $A = \{m \in \mathbf{N} \mid a < mb\}$.
Comme $\mathbf{N}$ est archimédien et $b \neq 0$, on sait qu'il existe $m \in \mathbf{N}$ tel que $bm > a$. On en déduit ainsi que A est non vide.
• Comme A est une partie non vide de $\mathbf{N}$, il admet un minimum que nous notons m. Cela signifie que $m \in A$ et $m - 1 \notin A$.
• Posons $n = m - 1$; c'est bien un entier positif car m ne peut pas être nul. Nous posons ensuite $r = a - nb$. Nous avons donc trivialement $a = nb + r$. Il ne reste plus qu'à montrer $0 \leqslant r < b$.
• Comme $m \in A$, $a < mb$
et comme $m - 1 \notin A$, $(m-1)b \leqslant a$.
Autrement dit, $nb \leqslant a < (n+1)b$.
Soustrayons nb : $0 \leqslant a - nb < b$, c'est-à-dire $0 \leqslant r < b$.
• On a finalement bien montré qu'il existait $n \in \mathbf{N}$ et $r \in \mathbf{N}$ tels que $a = nb + r$ et $0 \leq r < b$.

Unicité : montrons que le couple (n, r) de la division de a par b est unique. Pour cela, considérons deux couples solutions et montrons qu'ils sont égaux.
• Soient n et r des entiers tels que $a = nb + r$ avec $0 \leqslant r < b$;
et soient m et s tels que $a = mb + s$ avec $0 \leqslant s < b$.
Montrons que $n = m$ et $r = s$.
• On obtient donc $mb + s = nb + r$.
Regroupons certains termes et factorisons par b : $b(m - n) = r - s$.
Ainsi $r - s$ est un multiple de b.
Or $-b < -s \leqslant 0$ et $0 \leq r < b$. Donc, en additionnant ces inégalités, $-b < r - s < b$.
• Ainsi $r - s$ est un multiple de b strictement compris entre $-b$ et b.
Nécessairement $r - s = 0$. Donc $r = s$.
Finalement $a = nb = mb$. On en déduit $n = m$ car $b \neq 0$.
• Ainsi $n = m$ et $r = s$ ce qui démontre l'unicité du couple (n, r).

Exercice Rédiger la preuve pour les cas $a < 0$ ou $b < 0$. On pourra essayer de se ramener au cas déjà traité en commençant par diviser $|a|$ par $|b|$.

Définition : nombres premiers entre eux

On dit que deux entiers a et b sont **premiers entre eux** s'ils n'ont aucun diviseur commun hormis 1 et -1 :

$$\forall d \in \mathbf{N},\ (d|a \text{ et } d|b) \implies d = 1.$$

Théorème de Bézout

Soient a et b deux entiers premiers entre eux. Alors il existe des entiers u et v tels que

$$au + bv = 1.$$

Démonstration : Soient a et b des entiers premiers entre eux. En particulier, ils sont non nuls.
• Soit $A = \{au + bv \mid u \in \mathbf{Z}, v \in \mathbf{Z}\} \cap \mathbf{N}^*$ l'ensemble de tous les entiers strictement positifs s'écrivant sous la forme $au + bv$ où u et v sont des entiers. Nous allons démontrer que 1 appartient à cet ensemble.
L'ensemble A est non vide car $a\times 1 + b\times 0$ ou $a\times(-1) + b\times 0$ en est un élément.
Ainsi A est une partie non vide de $\mathbf{N}$ et il possède donc un minimum que nous notons m. Montrons que $m = 1$.
• Comme $m \in A$, il existe des entiers relatifs u et v tels que $m = au + bv$.
Effectuons la division euclidienne de a par m (possible car $m \neq 0$) : il existe des entiers n et r tels que $a = nm + r$ avec $0 \leqslant r < m$. Alors $a = n(au + bv) + r$.
Donc $r = a(1 - nu) + b(-nv)$. Ainsi r est de la forme $au' + bv'$.
Or, $r < m$ et $m = \min(A)$. Donc $r \notin A$. Finalement, r est un nombre positif de la forme $au' + bv'$ qui n'appartient pas à A. Ce ne peut être que 0 : $r = 0$. Donc $a = nm$ et m divise a.
• En effectuant la division euclidienne de b par m, on montre de même que m divise b.
• Or a et b sont supposés premiers entre eux. Donc comme m est un entier positif qui divise a et b, on déduit que $m = 1$.
• On peut donc conclure que $au + bv = 1$ avec u et v dans $\mathbf{Z}$.

Exercice Démontrer la réciproque du théorème de Bézout.

Définition du pgcd

On appelle **plus grand commun diviseur** (PGCD) de deux entiers a et b le plus grand nombre entier naturel qui divise à la fois a et b :

$$d = \text{PGCD}(a,b) \text{ si } d|a \text{ et } d|b \text{ et } (\forall d' \in \mathbf{N}, d'|a \text{ et } d'|b \implies d'|d).$$

Par définition, deux entiers sont premiers entre eux si et seulement si leur pgcd est 1.

Exercice Démontrer la version forte du théorème de Bézout :

$$\forall a \in \mathbf{Z}, \forall b \in \mathbf{Z}, \exists u \in \mathbf{Z}, \exists v \in \mathbf{Z},\ au + bv = \text{PGCD}(a,b).$$

L'algorithme d'Euclide permet de déterminer ce PGCD et de trouver des coefficients u et v vérifiant l'égalité ci-dessus.

Théorème : lemme d'Euclide et lemme de Gauss

Soit p un nombre premier et soient a et b dans $\mathbf{Z}$.
Si p divise le produit ab, alors p divise a ou p divise b :

$$\forall p \in \mathbf{P},\ \forall (a,b) \in \mathbf{Z} \times \mathbf{Z},\quad p|ab \implies (\ p|a \text{ ou } p|b\ ).$$

Soient α et β des nombres premiers entre eux et γ un entier tel que $\alpha|\beta\gamma$. Alors $\alpha|\gamma$.

Démonstration : Démontrons le lemme d'Euclide.
- Soit p un nombre premier et soient a et b des entiers tels que $p|ab$.
Il existe donc un entier k tel que $ab = kp$.
- Distinguons deux cas : soit p divise a, soit il ne le divise pas.
  - Si p divise a, alors il n'y a rien de plus à démontrer.
  - Si p ne divise pas a : comme p est premier, ses seuls diviseurs sont p et 1. Donc, si p ne divise pas a, le seul diviseur commun à a et p est 1 : ils sont premiers entre eux.
    Nous pouvons donc appliquer le théorème de Bézout : il existe deux entiers u et v tels que $up + va = 1$.
    On multiplie par b : $upb + vab = b$. Or $ab = kp$, et on obtient $p(ub + kv) = b$.
    Comme $ub + kv$ est un entier, on en déduit que p divise b.
- Nous avons donc bien démontré que dans chacun des cas, p divise a ou p divise b.

Exercice Montrer de manière analogue le **lemme de Gauss**.

Théorème fondamental de l'arithmétique

Tout nombre entier naturel non nul se décompose en un produit fini de nombres premiers :

$$\forall n \in \mathbf{N}^*, \exists k \in \mathbf{N}, \exists p_1, \ldots, p_k \in \mathbf{P},\ n = \prod_{i=1}^{k} p_i.$$

Cette décomposition est unique à l'ordre des facteurs près.

Démonstration :

Existence : Montrons par récurrence sur n que n se décompose en un produit de facteurs premiers.
• Initialisation : le nombre 1 peut s'écrire sous la forme d'un produit vide de nombres premiers (*i.e.* avec $k = 0$). Le nombre 2 est premier et se décompose naturellement en $2 = \prod_{i=1}^{1} p$ avec $p = 2$.
• Hérédité : soit $n \geqslant 2$. Supposons le résultat vrai pour tout les entiers m jusqu'à $n-1$. Montrons alors qu'il est vrai pour n.
Distinguons deux cas : n est premier ou il ne l'est pas.
– Si n est premier, alors le résultat est évident.
– Si n n'est pas premier, alors il existe des entiers m_1 et m_2 tels que $m_1 < n$, $m_2 < n$ et $n = m_1 m_2$.
On peut alors appliquer l'hypothèse de récurrence à m_1 et m_2. Ils se décomposent en un produit de nombres premiers :
$\exists, i, j \geqslant 0, \exists q_1, \ldots, q_i, r_1, \ldots, r_j \in \mathbf{P}$,
$m_1 = \prod_{l=1}^{i} q_l, \quad m_2 = \prod_{l=1}^{j} r_l$.
Alors $n = m_1 m_2 = \prod_{l=1}^{i} q_l \prod_{l=1}^{j} r_l$.
Ce dernier terme est encore un produit de nombres premiers. Le résultat est donc encore vrai pour n.
• On a ainsi montré par récurrence que tout nombre entier strictement positif s'écrit comme produit de nombres premiers.

Unicité : soit $n \in \mathbf{N}^*$.
• Supposons que l'on puisse écrire n comme produit de nombres premiers de deux manières :
$\exists k \in \mathbf{N}, \exists p_1, \ldots, p_k \in \mathbf{P},\ n = \prod_{i=1}^{k} p_i$ et
$\exists j \in \mathbf{N}, \exists q_1, \ldots, q_j \in \mathbf{P},\ n = \prod_{i=1}^{j} q_i$.
• Soit $p \in \mathbf{P}$. Notons α le nombre de fois où p apparaît dans la première décomposition de n (α peut être nul). Notons de même β le nombre d'apparitions de p dans la seconde décomposition de n. Montrons que $\alpha = \beta$.
• On regroupe tous les facteurs p dans la première factorisation de n : $n = p^\alpha m$ où m est le produit de tous les autres facteurs premiers. Comme p ne divise aucun de ces facteurs, p ne divise pas m (c'est une conséquence du lemme d'Euclide). On peut en déduire que p^α divise n mais que $p^{\alpha+1}$ ne divise pas n.
• De même, à partir de la seconde factorisation, on montre que p^β divise n mais que $p^{\beta+1}$ ne divise pas n. Comme α et β vérifient la même propriété, on en déduit que $\alpha = \beta$.
• Ainsi, tout nombre premier apparaît le même nombre de fois dans chaque décomposition de n en facteurs premiers. Cela revient à dire que ces décompositions sont les mêmes, à l'ordre des facteurs près.

Théorème

L'ensemble $\mathbf{P}$ des nombres premiers est infini.

Démonstration :
• Supposons par l'absurde que l'ensemble des nombres premiers est fini. Notons n leur nombre et notons $p_1, p_2, \ldots, p_n$ les nombres premiers (par hypothèse, il n'y en a pas d'autres).
• Posons alors $N = 1 + \prod_{i=1}^{n} p_i$. D'après le théorème précédent, comme $N \geqslant 2$, il admet une décomposition en facteurs premiers. En particulier N admet un diviseur premier.
• Notons-le p ; c'est un des nombres premiers p_i de notre liste. Il divise donc trivialement le produit $\prod_{i=1}^{n} p_i$. Or il divise aussi $N = 1 + \prod_{i=1}^{n} p_i$. Il divise donc leur différence, donc p divise 1. Or 1 n'est divisible par aucun nombre premier. On aboutit donc à une absurdité.
• On peut ainsi conclure que l'ensemble des nombres premiers est infini.

À retenir

- ★ Connaître toutes les définitions de cette partie.
- ★ Connaître tous les théorèmes (hypothèses + conclusion) de cette partie et en comprendre les démonstrations.
- ★ Être capable de les utiliser dans des problèmes d'arithmétique.
- ★ Savoir appliquer l'algorithme d'Euclide.

2 Congruences

Pour toute cette partie, on se donne un nombre entier n non nul.

Définition

Soient a et b deux nombres entiers. On dit que a et b sont **congrus modulo** n si $n|(a-b)$.
On note $a \equiv b \mod n$ ou encore $a \equiv b[n]$.

Avec les mêmes notations, a est congru à b modulo n si a est égal à b à un multiple de n près :

$$a \equiv b[n] \text{ ssi } \exists k \in \mathbf{Z},\ a = b + kn.$$

Propriété

Soient a, b et c des nombres entiers. Alors

- ★ $a \equiv a \mod n$;
- ★ si $a \equiv b \mod n$, alors $b \equiv a \mod n$;
- ★ si $a \equiv b \mod n$ et $b \equiv c \mod n$, alors $a \equiv c \mod n$.

La relation de congruence est ainsi réflexive, symétrique et transitive. On dit qu'elle définit une **relation d'équivalence**. Cela signifie qu'elle possède les propriétés fondamentales de l'égalité, qui permettent entre autres de résoudre des équations.

Définition

Soit $a \in \mathbf{Z}$. On note $\bar{a}$ l'ensemble des entiers congrus à a modulo n :

$$\bar{a} = \{a + kn \mid k \in \mathbf{Z}\} = \{\dots a - 3n, a - 2n, a - n, a, a + n, a + 2n, \dots\}.$$

Cet ensemble est appelé **classe de congruence** modulo n de a.

Remarques Deux entiers congrus modulo n définissent la même classe d'équivalence : $a \equiv b \mod n \implies \bar{a} = \bar{b}$.
On dit alors que a et b sont deux **représentants** de cette classe.

L'ensemble $\mathbf{Z}$ est l'union disjointe des classes de congruence $\bar{0}$, $\bar{1}, \dots, \overline{n-1}$: $\mathbf{Z} = \bigsqcup_{k=0}^{n-1} \bar{k}$.

Définition

On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des classes de congruence modulo n :

$$\mathbf{Z}/n\mathbf{Z} = \{\bar{k}\ ;\ k = 0 \dots n-1\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Définition

On peut munir $\mathbf{Z}/n\mathbf{Z}$ d'une **addition** $\bar{+}$ et d'une **multiplication** $\bar{\times}$ définies par

$$\forall \bar{a} \in \mathbf{Z}/n\mathbf{Z}, \quad \forall \bar{b} \in \mathbf{Z}/n\mathbf{Z} \qquad \bar{a} \bar{+} \bar{b} = \overline{a+b} \quad \text{et} \quad \bar{a} \bar{\times} \bar{b} = \overline{ab}.$$

Remarques Ces définitions sont rigoureuses dans le sens où elles ne dépendent en fait pas des représentants a et b des classes d'équivalence.
On dit que l'addition et la multiplication sur $\mathbf{Z}$ passent au quotient $\mathbf{Z}/n\mathbf{Z}$.

Plutôt qu'écrire $3 + 6 \equiv 2 \mod 7$, on préfère écrire : dans $\mathbf{Z}/7\mathbf{Z}$, $\bar{3} \bar{+} \bar{6} = \bar{2}$.
Et lorsque le contexte est clair, on ne note plus les éléments et les opérations de $\mathbf{Z}/n\mathbf{Z}$ avec des barres.

Exemples 1. Déterminer l'inverse de $\bar{6}$ dans $\mathbf{Z}/14\mathbf{Z}$.
On se place dans $\mathbf{Z}/14\mathbf{Z}$ et on cherche à résoudre $\bar{6}\bar{x} = \bar{1}$. (Il est hors de question d'écrire des fractions du type $\bar{1}/\bar{6}$, cela n'a aucun sens !) La méthode la moins subtile mais parfaitement efficace consiste en une disjonction de cas ultime : on teste toutes les valeurs possibles pour $\bar{x}$. On dresse le tableau suivant :

$\bar{x}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$
$\bar{6}\bar{x}$	$\bar{0}$	$\bar{6}$	$\overline{12}$	$\bar{4}$	$\overline{10}$	$\bar{2}$	$\bar{8}$	$\bar{0}$	$\bar{6}$	$\overline{12}$	$\bar{4}$	$\overline{10}$	$\bar{2}$	$\bar{8}$

Nous avons testé les 14 valeurs possibles pour $\bar{x}$ mais aucune ne satisfait $\bar{6}\bar{x} = \bar{1}$. Notre problème n'a donc pas de solution.

2. Calculer 3^{1234} modulo 14.
La réponse est simple : il s'agit de $\bar{3}^{1234}$. Mais on nous demande implicitement de trouver le représentant situé entre $\bar{0}$ et $\bar{13}$. Pour cela, la meilleure méthode consiste à calculer doucement les puissances de 3 en les réduisant modulo 14 à chaque étape : on calcule chaque puissance en multipliant la précédente par 3 et en réduisant le résultat module 14. Ainsi, dans $\mathbf{Z}/14\mathbf{Z}$, $3^2 = 9$, $3^3 = 27 = 13$, $3^4 = 3 \times 3^3 = 3 \times 13 = 39 = 11$, etc :

3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	$\cdots$
3	9	13	11	5	1	3	9	13	$\cdots$

En continuant on voit le cycle $3, 9, 13, 11, 5, 1$ se répéter. En particulier on a obtenu $3^6 = 1$. Divisons 1234 par 6 : $1234 = 205 \times 6 + 4$. Comme la multiplication est compatible avec le calcul modulo 14, on peut écrire : dans $\mathbf{Z}/14\mathbf{Z}$, $3^{1234} = 3^{205 \times 6 + 4} = (3^6)^{205} \times 3^4 = 1^{205} \times 11$. Conclusion : $3^{1234} = 11 \mod 14$.

À retenir

- ★ Comprendre ce qu'est une classe de congruence.
- ★ Savoir raisonner et calculer dans $\mathbf{Z}/n\mathbf{Z}$: calcul de puissance, résolution d'équations, etc.
- ★ Éviter certaines erreurs : les fractions n'ont aucun sens dans $\mathbf{Z}/n\mathbf{Z}$; $\bar{a}\bar{b} = \bar{0} \not\Rightarrow (\bar{a} = \bar{0} \text{ ou } \bar{b} = 0)$.

III. Ensembles et applications

1 Ensembles

La définition du concept d'ensemble repose sur une liste d'axiomes. Pour nous, un ensemble sera simplement une collection d'objets appelés éléments. Cette collection n'a pas d'ordre et chaque élément ne peut y apparaître qu'une fois :

$$\{3, 1, 7, 2\} = \{1, 2, 3, 7\} = \{7, 3, 1, 3, 2, 7\}.$$

La notation $a \in E$ se lit « a est un élément de E » ou bien « a appartient à E ».

1.1 Écriture d'un ensemble

Il y a plusieurs manières de définir des ensembles. Un ensemble peut être défini de manière **explicite** par la simple donnée de ces éléments :

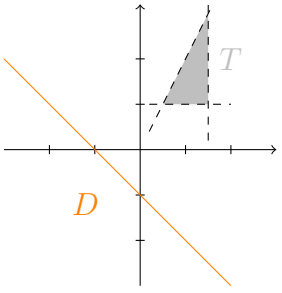
$$E = \{3, 5, 8, 2\}, \qquad F = \{\cos, 2, a, \{3, 8\}\}.$$

Mais avant même de pouvoir définir ces ensembles, il faut disposer d'ensembles de référence. Ceux-ci sont définis de manière axiomatique ou construits à partir d'autres à l'aide de relations d'équivalence (voir chapitre 3). Introduisons les notations usuelles de certains de ces ensembles :

- $\emptyset$ désigne l'ensemble vide, *i.e.* l'ensemble ne contenant aucun élément.
- $\mathbf{N}$ désigne l'ensemble des entiers naturels : 0, 1, 2.
- $\mathbf{Z}$ désigne l'ensemble des entiers relatifs : -7, -2, 0, 1, 8.
- $\mathbf{Q}$ désigne l'ensemble des nombres rationnels : $\frac{5}{7}$, 0, $-\frac{1}{3}$, 7.
- $\mathbf{R}$ désigne l'ensemble des nombre réels : π, -4, $0.534652\cdots$, $\ln(2)$.
- $\mathbf{C}$ désigne l'ensemble des nombres complexes : i, 0, $3\mathrm{i} - 2$, $\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$.

On peut ensuite définir des sous-ensembles particuliers de ces ensembles. Un ensemble peut être défini de manière **implicite**, à partir d'une propriété. Quelques exemples :

- L'ensemble des nombres entiers qui sont des carrés est l'ensemble $\{x \in \mathbf{N} \mid \exists y \in \mathbf{N}, x = y^2\}$.
- L'ensemble $\mathbf{P}$ des nombres premiers.
- L'ensemble des solutions d'une équation de la forme $f(x) = 0$ est l'ensemble $\{x \mid f(x) = 0\}$.
- L'ensemble $D = \{(x, y) \in \mathbf{R}^2 \mid x + y + 1 = 0\}$ désigne, dans le plan, la droite d'équation $x + y + 1 = 0$. Il s'agit de la droite de pente -1 passant par le point $(0, -1)$.
- L'ensemble $T = \{(x, y) \in \mathbf{R}^2 \mid y \leqslant 2x,\ y \geqslant 1 \text{ et } x \leqslant \frac{3}{2}\}$ est représenté dans le plan par un triangle.



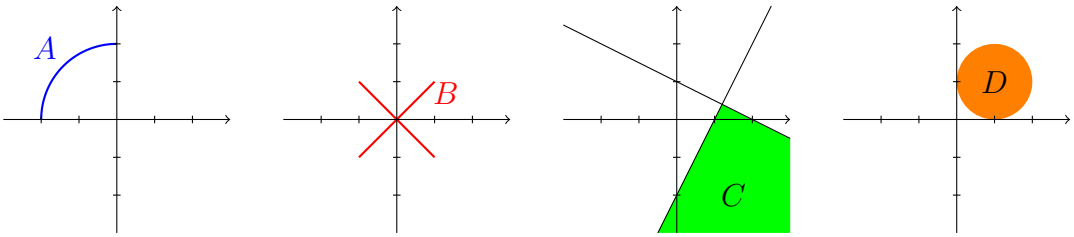
Attention : les éléments de D et T sont des couples de réels. On peut écrire $(x, y) \in T$, mais écrire $x \in T$ ou $y \in T$ n'a ici aucun sens.

Parmi les ensembles définis implicitement, on trouve les ensembles définis de manière **paramétrique**, c'est-à-dire en considérant un ensemble d'éléments dépendant d'un ou plusieurs paramètres. Quelques exemples :

- L'ensemble des carrés d'entiers peut être défini de manière paramétrique : c'est l'ensemble $\{z^2 \ ; \ z \in \mathbf{N}\}$.
- L'ensemble $\{\cos(x) \ ; \ x \in \mathbf{R}\}$ est en fait l'intervalle $[-1, 1]$.
- L'ensemble $\{\cos(x) \ ; \ x \in \mathbf{Z}\}$ est bien plus compliqué à décrire.
- L'ensemble D peut se paramétrer : si $\vec{u}$ est un vecteur directeur de la droite, alors $D = \{(0, -1) + t\vec{u} \ ; \ t \in \mathbf{R}\}$. Avec $\vec{u} = (1, -1)$, $D = \{(t, -1 - t) \ ; \ t \in \mathbf{R}\}$.
- L'ensemble T peut aussi se paramétrer. Comme il s'agit d'un objet de « dimension 2 », il faudra deux paramètres : $T = \{(a, b) \ ; \ a \in [\frac{1}{2}, \frac{3}{2}] \text{ et } b \in [1, 2a]\}$.

Il faut savoir jongler avec ces deux manières de définir les ensembles. Selon les situations, une définition est meilleure qu'une autre. Le cercle unité dans le plan, par exemple, admet deux définitions très différentes. On peut le définir implicitement comme l'ensemble $\{(x, y) \in \mathbf{R}^2 \mid x^2 + y^2 = 1\}$ et de manière paramétrique comme l'ensemble $\{(\cos(t), \sin(t)), t \in \mathbf{R}\}$.

Exercice Définir mathématiquement les parties du plan ci-dessous :



$A =$

$B =$

$C =$

$D =$

1.2 Comparaisons d'ensemble

Définition

Soient A et B deux ensembles. On dit que A est **inclus** dans B et on note $A \subset B$ si tout élément de A est élément de B :

$$\forall x \in A,\ x \in B.$$

On dit que A et B sont **égaux** et on note $A = B$ s'ils ont les mêmes éléments :

$$\forall x,\ x \in A \Leftrightarrow x \in B.$$

Si A est inclus dans B, on dit aussi que A est une **partie** de B. On dit que deux ensembles sont **différents** s'ils ne sont pas égaux.

Exemples Pour tout ensemble A, $\emptyset \subset A$. $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

Remarques Pour démontrer l'inclusion $A \subset B$, on montre que tout élément de A est dans B. Une telle preuve commence donc toujours par « Soit $x \in A$ » et se termine par « Donc $x \in B$. Ainsi tout élément de A est aussi élément de B, donc $A \subset B$ ».

On peut vérifier que $A = B$ si et seulement si $A \subset B$ et $B \subset A$. Ainsi, pour démontrer que deux ensembles A et B sont égaux, on raisonne souvent par **double inclusion** : on montre $A \subset B$ puis $B \subset A$.

Exemple Notons $A = \{(x, y) \in \mathbf{R}^2 \mid x + y + 1 = 0\}$ et $B = \{(t, -1 - t)\ ;\ t \in \mathbf{R}\}$. Montrons $A = B$.

Montrons $B \subset A$: soit (x, y) un élément de B.
Alors, par définition, on peut l'écrire sous la forme $(x, y) = (t, -1 - t)$ avec $t \in \mathbf{R}$.
Alors $x + y + 1 = t + (-1 - t) + 1 = 0$.
Donc (x, y) satisfait la propriété de A. Donc $(x, y) \in A$.
Donc tout élément de B est aussi dans A : $B \subset A$.

Montrons $A \subset B$: soit $(x, y) \in A$.
Alors, par définition, $x + y + 1 = 0$.
Posons $t = x$.
Alors $t \in \mathbf{R}$ et $t + y + 1 = 0$. Donc $y = -1 - t$.
Finalement $(x, y) = (t, -1 - t)$: on reconnaît un élément de B. Donc $(x, y) \in B$. Donc $A \subset B$.

Par double inclusion, nous avons montré $A = B$.

Définition

Soient A et B deux ensembles.
On dit que A et B sont **disjoints** s'ils n'ont aucun élément en commun, *i.e.* si $A \cap B = \emptyset$:

$$\forall x,\ x \in A \Rightarrow x \notin B.$$

Attention : ne pas confondre disjoint et différent.

Définition

Soit E un ensemble. On appelle **ensemble des parties** de E l'ensemble noté $\mathcal{P}(E)$ défini par

$$\mathcal{P}(E) = \{A \mid A \subset E\}.$$

Exemple Soit $E = \{a, b, c\}$.
Alors $\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Il contient huit éléments.

1.3 Opérations sur les ensembles

Définition

Soient A et B deux ensembles. On appelle **union** de A et B et on note $A \cup B$ l'ensemble contenant les éléments de A et de B :

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

On appelle **intersection** de A et B et on note $A \cap B$ l'ensemble contenant les éléments qui appartiennent à la fois à A et à B :

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

Propriété

Soient A, B et C des parties d'un ensemble E.

- ★ Commutativité : $A \cup B = B \cup A$ et $A \cap B = B \cap A$.
- ★ Associativité : $A \cup (B \cup C) = (A \cup B) \cup C$ et $A \cap (B \cap C) = (A \cap B) \cap C$.
- ★ Distributivité : $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Définition

Soient A une partie d'un ensemble E. On appelle **complémentaire** de A dans E l'ensemble noté $\bar{A}$ contenant les éléments de E qui n'appartiennent pas à A :

$$\bar{A} = \{x \in E \mid x \notin A\}.$$

Définition

Soient A et B deux parties d'un ensemble E. On appelle **différence** de A et B et on note $A \setminus B$ l'ensemble contenant les éléments qui appartiennent à A mais pas à B :

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

Remarques

$A \setminus B = A \cap \bar{B}$.

Dans les ensembles de nombres, la notation * permet d'exclure 0 de l'ensemble :

$$\mathbf{N}^* = \mathbf{N} \setminus \{0\}, \quad \mathbf{Z}^* = \mathbf{Z} \setminus \{0\}, \quad \mathbf{R}^* = \mathbf{R} \setminus \{0\}, \quad \text{etc.}$$

Définition

Un **couple** (x, y) est un objet mathématique formé à partir de deux autres objets x et y et qui possède la propriété suivante

$$(x, y) = (x', y') \iff x = x' \text{ et } y = y'.$$

Soient E et F des ensembles. On appelle **produit cartésien** de E et F l'ensemble des couples (x, y) formés à partir des éléments x de E et y de F :

$$E \times F = \{(x, y) \ ; \ x \in E, y \in F\}.$$

Remarques

★ Le produit cartésien $E \times E$ se note aussi E^2.

★ On peut étendre la notion de couple : si $E_1, \ldots, E_n$ sont des ensembles, on peut définir des n-**uplets** $(x_1, \ldots, x_n)$ avec pour tout i, $x_i \in E_i$. L'ensemble de ces n-uplets est le produit cartésien $E_1 \times E_2 \times \cdots \times E_n$.

★ Le produit cartésien $E \times \cdots \times E$ des n-uplets d'éléments de E se note E^n.

À retenir

★ Savoir lire et interpréter les notations ensemblistes.

★ Savoir définir mathématiquement des ensembles.

★ Être capable de paramétrer des sous-ensembles simples du plan : droites, polygones, cercles, disques, etc.

★ Être capable de démontrer des inclusions ou des égalités d'ensembles.

2 Applications

2.1 Définition

Définition

Soient E et F deux ensembles.

★ Une **application** f de E vers F est la donnée d'une partie Γ de $E \times F$ telle que

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

★ Si $(x,y) \in \Gamma$, on dit que y est **l'image** de x par f et on note $y = f(x)$. L'ensemble E est **l'ensemble de départ** de f et F est son **ensemble d'arrivée**. L'ensemble Γ est appelé **graphe** de f.

★ On note l'application f sous la forme

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

★ On note $\mathcal{F}(E,F)$ ou F^E l'ensemble des applications de E vers F.

Remarques Pour nous, les termes « fonction » et « application » seront synonymes. Il existe quelques différences subtiles entre ces deux notions, mais nous les ignorerons.

Soient f et g deux applications. On dit qu'elles sont égales et on note $f = g$ si elles ont le même ensemble de départ E, le même ensemble d'arrivée F et si $\forall x \in E,\ f(x) = g(x)$.

Définition

Soient E et F des ensembles.

· On appelle application **identité** de E l'application

$$\begin{array}{rccc} \mathrm{id}_E: & E & \to & E \\ & x & \mapsto & x \end{array}$$

· Soit $a \in F$.

On appelle application **constante** égale à a l'application

$$\begin{array}{rccc} a: & E & \to & F \\ & x & \mapsto & a \end{array}$$

· Soit A une partie de E. On appelle fonction **indicatrice** de A l'application

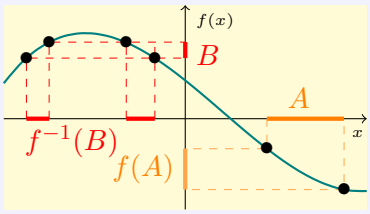
$$\begin{array}{rccc} \mathbf{1}_A: & E & \to & \mathbf{R} \\ & x & \mapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{array}$$

Exercice Montrer que $\mathbf{1}_A \times \mathbf{1}_B = \mathbf{1}_{A \cap B}$.

2.2 Images et antécédents

Définition

Soit f une application de E vers F.
Soit $A \subset E$. L'**image** de A par f est l'ensemble $f(A) = \{f(x) \mid x \in A\}$.
L'image de E est appelée image de f.



Soit $B \subset F$. L'**image réciproque** de B par f est l'ensemble $f^{-1}(B) = \{x \in E \mid f(x) \in B\}$.
Soit $y \in F$. On appelle **antécédent** de y tout élément x de E tel que $f(x) = y$, *i.e.* tel que $x \in f^{-1}(\{y\})$.

2.3 Restriction, prolongement, composition

Définition

Soit E et F des ensembles et $f \in \mathcal{F}(E, F)$. Soit $A \subset E$.

★ On appelle **restriction** de f à A l'application

$$\begin{array}{rccc} f|_A : & A & \to & F \\ & x & \mapsto & f(x). \end{array}$$

★ Soit $g \in \mathcal{F}(A, F)$. On dit que f est un **prolongement** de g si $f|_A = g$, autrement dit si f et g coïncident sur A.

Définition

Soient E, F et G des ensembles et soient $f : E \to F$ et $g : F \to G$ des applications. On appelle **composée** de f et g l'application notée $g \circ f$ définie de E vers G par $g \circ f(x) = g(f(x))$:

$$\begin{array}{rccc} g \circ f : & E & \to & G \\ & x & \mapsto & g(f(x)). \end{array}$$

Propriété

Soient E, F, G et H des ensembles et soient $f \in \mathcal{F}(E, F)$, $g \in \mathcal{F}(F, G)$ et $h \in \mathcal{F}(G, H)$. La composition des applications est associative :

$$(h \circ g) \circ f = h \circ (g \circ f).$$

On peut ainsi noter sans ambiguïté cette composée $h \circ g \circ f$.

2.4 Injections, surjections et bijections

Définition

Soient E et F des ensembles et $f \in \mathcal{F}(E, F)$.

★ L'application f est **injective** si deux éléments quelconques distincts de E ont des images distinctes par f :

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

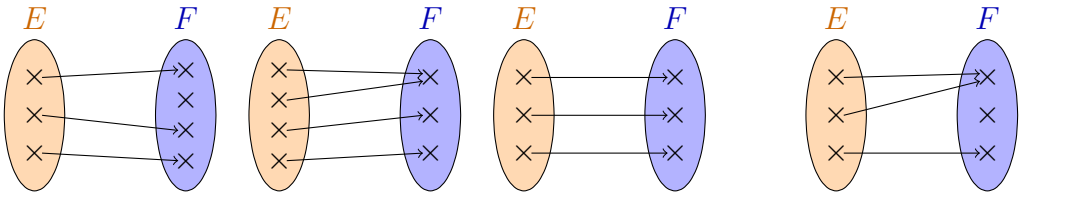
★ L'application f est **surjective** si l'image de E par f est l'ensemble F :

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

★ L'application f est **bijective** si elle est injective et surjective :

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

Autrement dit, f est surjective si tout élément de F admet un antécédent par f, et f est bijective si tout élément de F admet un et un seul antécédent par f.



Injection Surjection Bijection Ni injection, ni surjection

Définition

Soit f une bijection de E vers F.
On appelle **bijection réciproque** de f l'application, notée f^{-1}, définie de F vers E qui à chaque élément de F associe son unique antécédent par f.

C'est l'unique application telle que $f^{-1} \circ f = \mathrm{id}_E$ et $f \circ f^{-1} = \mathrm{id}_F$.

Propriété

★ Si une application est strictement monotone, alors elle est injective.

★ La composée de deux injections/surjections/bijection est une injection/surjection/bijection.

★ Si une application f admet une application réciproque g ($f \circ g = \mathrm{id}$ et $g \circ f = \mathrm{id}$), alors f est une bijection et $g = f^{-1}$.

Exemple Soit $f : \mathbf{R} \to]0, \frac{5}{2}[$ définie par $f(x) = \frac{5}{2+\mathrm{e}^x}$. Montrer que f est une bijection.

Première preuve :

Montrons que f est injective : soient x et x' dans $\mathbf{R}$ tels que $f(x) = f(x')$. Alors $\frac{5}{2+\mathrm{e}^x} = \frac{5}{2+\mathrm{e}^{x'}}$.
Donc $2 + \mathrm{e}^x = 2 + \mathrm{e}^{x'}$, donc $\mathrm{e}^x = \mathrm{e}^{x'}$.
Enfin, en passant au logarithme, on déduit $x = x'$.
Donc f est injective.

Montrons que f est surjective : soit $y \in]0, \frac{5}{2}[$.
Comme $0 < y < \frac{5}{2}$, $2 < \frac{5}{y}$ et donc $\frac{5}{y} - 2 > 0$.
On peut ainsi définir $x = \ln(\frac{5}{y} - 2)$.
Alors $f(x) = f(\ln(\frac{5}{y} - 2)) = \frac{5}{2+(\frac{5}{y}-2)} = y$.
Ainsi tout élément y de $]0, \frac{5}{2}[$ admet un antécédent $x \in \mathbf{R}$ par f, donc f est surjective.

Comme f est injective et surjective, elle est bijective.

Deuxième preuve utilisant des arguments d'analyse :

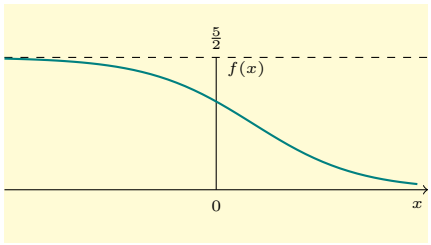
Montrons que f est injective : la fonction f est dérivable sur $\mathbf{R}$ et sa dérivée est définie par $f'(x) = -\frac{5\mathrm{e}^x}{(2+\mathrm{e}^x)^2}$.
Cette dérivée est strictement négative sur $\mathbf{R}$, donc f est strictement décroissante sur $\mathbf{R}$. En particulier, elle est injective.

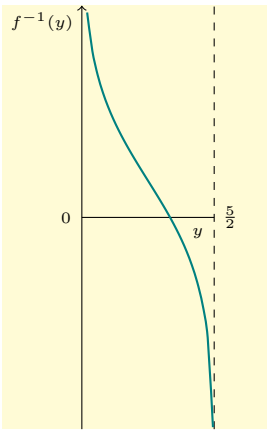
Montrons que f est surjective : la fonction f tend vers 0 en $+\infty$ et tend vers $\frac{5}{2}$ en $-\infty$. Comme c'est une application continue, on déduit du théorème des valeurs intermédiaires qu'elle prend toutes les valeurs de $]0, \frac{5}{2}[$.
Elle est donc surjective.

Troisième preuve utilisant les bijections réciproques :

On décompose f en une composée d'applications élémentaires. Chacune de ces applications est une bijection dont on connaît la bijection réciproque. On en déduit que f est une bijection et on construit sa bijection réciproque en composant (à l'envers) les bijections réciproques élémentaires.

$$
\begin{array}{ccccccccccc}
f : & \mathbf{R} & \xrightarrow{\exp} & \mathbf{R}_+^* & \xrightarrow{+2} &]2,+\infty[& \xrightarrow{\frac{1}{\bullet}} &]0,\frac{1}{2}[& \xrightarrow{\times 5} &]0,\frac{5}{2}[\\
 & x & \longrightarrow & \exp(x) & \longrightarrow & 2+\exp(x) & \longrightarrow & \frac{1}{2+\exp(x)} & \longrightarrow & 5\times\frac{1}{2+\exp(x)} \\
f^{-1} : & \ln(\frac{5}{y}-2) & \xleftarrow{\ln} & \frac{5}{y}-2 & \xleftarrow{-2} & \frac{5}{y} & \xleftarrow{\frac{1}{\bullet}} & \frac{y}{5} & \xleftarrow{\div 5} & y
\end{array}
$$





À retenir

- ★ Ne pas confondre fonction et images d'une fonction.
- ★ Savoir déterminer les images et images réciproques d'une application.
- ★ Connaître et maîtriser la composition des applications.
- ★ Être capable de déterminer et de démontrer le caractère injectif, surjectif ou bijectif d'une application.
- ★ Être capable de définir la bijection réciproque d'une bijection.

3 Cardinal d'un ensemble

3.1 Ensembles finis

Le cardinal d'un ensemble est le nombre d'éléments qu'il possède. Donner le cardinal d'un ensemble revient donc à compter ses éléments. Mathématiquement, cela implique l'utilisation de l'ensemble $\mathbf{N}$. On peut définir la notion de cardinal de la manière suivante.

Définition

Soit E un ensemble non vide et $n \in \mathbf{N}^*$.
On dit que E est de **cardinal fini** n s'il existe une bijection de $\{1, \dots, n\}$ vers E. On note alors $\text{Card}(E) = n$.

Le cardinal de l'ensemble vide est 0.

Exemples $\text{Card}(\{2, 8, 3\}) = 3, \quad \text{Card}(\{0, \{7, 9, 2\}\} = 2.$

Remarques Pour que cette définition ait un sens, il ne faut pas que deux entiers distincts puissent être le cardinal d'un même ensemble. Cela ne peut pas arriver grâce à la propriété suivante (qui se démontre par récurrence sur n) :

Propriété : soient $(n, m) \in \mathbf{N}^2$. Il existe une bijection de $\{1, \dots, n\}$ vers $\{1, \dots, m\}$ si et seulement si $n = m$.

On l'aura compris, la notion de cardinal est intrinsèquement liée aux bijections, ce que résume la propriété suivante.

Propriété du cardinal

Soient E et F deux ensembles de cardinal fini.
Ils ont le même cardinal si et seulement s'il existe une bijection de E vers F.

Propriété

Soit E et F des ensembles de cardinaux finis n et m. On note $\text{Bij}(E)$ l'ensemble des bijections de E vers E. Alors

$$\text{Card}(\mathcal{P}(E)) = 2^n, \quad \text{Card}(E \times F) = nm, \quad \text{Card}(F^E) = m^n, \quad \text{Card}(\text{Bij}(E)) = n!$$

3.2 Ensemble infinis et dénombrabilité

Définition

Soit E un ensemble.
On dit que E est de **cardinal infini** s'il n'est pas de cardinal fini.

Exemples $\mathbf{N}$, $\mathbf{R}$, $\mathbf{P}$ et l'ensemble des nombres pairs sont des ensembles infinis.

La propriété du cardinal est-elle satisfaite par les ensembles infinis : peut-on toujours mettre en bijection deux ensembles infinis ? La réponse est non ! Cela signifie qu'il existe plusieurs infinis de tailles différentes. Cette découverte étonnante est due à Georg Cantor dans les années 1870.

Définition

Soit E un ensemble infini. On dit que E est **dénombrable** s'il existe une bijection de $\mathbf{N}$ vers E.

L'infini de $\mathbf{N}$ est en quelque sorte le plus petit des infinis. Un ensemble est dénombrable s'il a le même infini que $\mathbf{N}$, autrement dit, si on peut énumérer ses éléments.

Exemples $\mathbf{P}$, $\mathbf{Z}$ et $\mathbf{Q}$ sont des ensembles dénombrables.

Propriété

L'ensemble $\mathbf{R}$ des nombres réels n'est pas dénombrable.

Cela signifie que l'infini de $\mathbf{R}$ est plus grand que l'infini de $\mathbf{N}$.

Propriété

Il existe une bijection de $\mathcal{P}(\mathbf{N})$ vers $\mathbf{R}$. Il existe une bijection de $\mathbf{R}^2$ vers $\mathbf{R}$.

Autrement dit, $\mathbf{R}$, $\mathbf{R}^2$ et $\mathcal{P}(\mathbf{N})$ ont le même cardinal infini !

À retenir

- ★ Retenir que la notion de cardinal est liée au concept de bijection.
- ★ Être capable de mettre en bijection des ensembles ayant même cardinal.
- ★ Savoir ce qu'est un ensemble dénombrable.
- ★ Savoir que $\mathbf{N}$, $\mathbf{Z}$ et $\mathbf{Q}$ sont dénombrables alors que $\mathbf{R}$ et $\mathbf{C}$ ne le sont pas.

IV. Le corps des nombres complexes

1 Définitions

1.1 Construction de C

Définition

On définit sur $\mathbf{R}^2$ l'addition et la multiplication suivantes

$$\forall (x,y),(x',y') \in \mathbf{R}^2, \quad (x,y)+(x',y') = (x+x', y+y');$$

$$\forall (x,y),(x',y') \in \mathbf{R}^2, \quad (x,y)\times(x',y') = (xx'-yy', xy'+x'y).$$

On appelle **corps des nombres complexes** l'ensemble $\mathbf{R}^2$ muni de ces deux opérations et on le note $\mathbf{C}$.

Notations : on pose $\mathrm{i} = (0,1)$ et pour $x \in \mathbf{R}$, on note simplement x l'élément $(x,0)$ de $\mathbf{C}$. Le nombre i satisfait : $\mathrm{i}^2 = -1$.
Et pour tous x et y dans $\mathbf{R}$, on obtient $x + \mathrm{i}\times y = (x,0)+(0,1)\times(y,0) = (x,y)$.

Cette écriture $x + \mathrm{i}y$ s'appelle **écriture algébrique** d'un nombre complexe. C'est l'écriture standard des nombres complexes. Elle est pertinente car elle se prête aux manipulations algébriques de manière naturelle. Les opérations s'effectuent formellement (développements, factorisations, etc) , simplement en utilisant la règle $\mathrm{i}^2 = -1$:

$$(x+\mathrm{i}y)+(x'+\mathrm{i}y') = (x+x')+\mathrm{i}(y+y').$$
$$(x+\mathrm{i}y)\times(x'+\mathrm{i}y') = xx'+x\mathrm{i}y+\mathrm{i}yx'+\mathrm{i}y\mathrm{i}y' = (xx'-yy')+\mathrm{i}(xy'+x'y).$$

La plupart des raisonnements algébriques classiques sur $\mathbf{R}$ seront encore possibles dans $\mathbf{C}$. Cela repose sur les propriétés élémentaires suivantes satisfaites par nos nouvelles lois.

- ★ L'addition et la multiplication dans $\mathbf{C}$ sont **associatives** et **commutatives**.
- ★ La multiplication est **distributive** par rapport à l'addition.
- ★ Le nombre complexe 1 est l'**élément neutre** de la multiplication : $\forall z \in \mathbf{C},\ z\times 1 = z$.
- ★ Tout nombre non nul admet un unique **inverse** : $\forall z \in \mathbf{C}^*,\ \exists! z' \in \mathbf{C},\ zz' = 1$.
  On note alors $z' = \frac{1}{z}$.

Ces propriétés confèrent à $\mathbf{C}$ une structure de **corps** (*cf.* chapitre suivant).

Attention : $\frac{1}{z}$ et $\frac{1}{x+\mathrm{i}y}$ ne sont que des notations pas très explicites. Si on veut identifier ces nombres précisément, il faut les écrire sous forme algébrique. Pour cela, on manipule l'expression en introduisant astucieusement l'expression conjuguée (voir plus loin) du nombre à inverser :

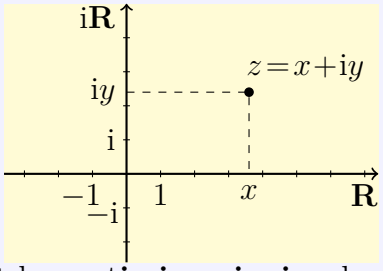
$$\frac{1}{x+\mathrm{i}y} = \frac{x-\mathrm{i}y}{(x+\mathrm{i}y)(x-\mathrm{i}y)} = \frac{x-\mathrm{i}y}{x^2+y^2} = \tfrac{x}{x^2+y^2} - \mathrm{i}\tfrac{y}{x^2+y^2}.$$

1.2 Représentation des nombres complexes

Comme $\mathbf{R}^2$ est en bijection naturelle avec le plan cartésien, tout nombre complexe est naturellement associé à un point du plan.

Définition

On dit qu'un point M du plan, d'abscisse x et d'ordonnée y, a pour **affixe** le nombre complexe $z = x + \mathrm{i}y$.



On dit que x est la **partie réelle** de z et y est la **partie imaginaire** de z. On note $x = \Re e(z)$ et $y = \Im m(z)$.
Les nombres de la forme $\mathrm{i}y$ avec $y \in \mathbf{R}$ sont appelés nombres **imaginaires purs**.

1.3 Nombre conjugué

Définition

Soit $z = x + \mathrm{i}y \in \mathbf{C}$. On appelle **nombre conjugué** de z le nombre complexe

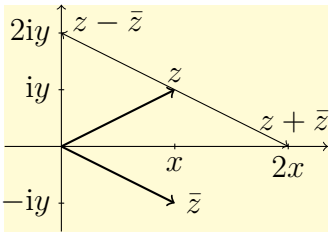
$$\bar{z} = x - \mathrm{i}y.$$

Propriété

Soient z, z_1, z_2 des nombres complexes.

- ★ $\bar{\bar{z}} = z$;
- ★ $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
- ★ $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$;
- ★ $\overline{\frac{1}{z}} = \frac{1}{\bar{z}}$;
- ★ $z + \bar{z} = 2\Re e(z)$; $\quad z - \bar{z} = 2\mathrm{i}\Im m(z)$;
- ★ si $z = x + \mathrm{i}y$, alors $z\bar{z} = x^2 + y^2 \in \mathbf{R}_+$.

Remarques Soient M le point d'affixe z et M' le point d'affixe $\bar{z}$. Alors M et M' sont symétriques par rapport à l'axe réel.



1.4 Écriture polaire, module et argument

Définition

Soit $\theta \in \mathbf{R}$. On définit l'exponentielle du nombre complexe $\mathrm{i}\theta$ comme étant le nombre complexe

$$\mathrm{e}^{\mathrm{i}\theta} = \cos(\theta) + \mathrm{i}\sin(\theta).$$

Propriété

Soient θ, θ_1 et θ_2 dans $\mathbf{R}$. Alors

$$\mathrm{e}^{\mathrm{i}\theta_1}\mathrm{e}^{\mathrm{i}\theta_2} = \mathrm{e}^{\mathrm{i}(\theta_1+\theta_2)}, \qquad \frac{1}{\mathrm{e}^{\mathrm{i}\theta}} = \mathrm{e}^{-\mathrm{i}\theta} \quad \text{et} \quad \overline{\mathrm{e}^{\mathrm{i}\theta}} = \mathrm{e}^{-\mathrm{i}\theta}.$$

Propriété

Soit $z \in \mathbf{C}^*$. Il existe $r \in \mathbf{R}_+^*$ et $\theta \in \mathbf{R}$ tels que

$$z = r\mathrm{e}^{\mathrm{i}\theta}.$$

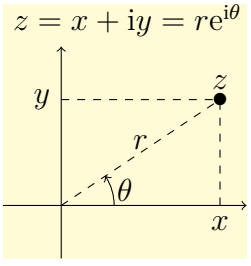
Cette égalité est appelée **écriture polaire** de z. Le nombre r est appelé **module** de z et le nombre θ est appelé **argument** de z. On note $|z| = r$ et $\arg(z) = \theta$.

Le module d'un nombre z est unique. L'argument d'un nombre z non nul est unique modulo 2π, c'est-à-dire

$$\theta_1 = \arg(z) \text{ et } \theta_2 = \arg(z) \implies \exists k \in \mathbf{Z},\ \theta_2 - \theta_1 = 2k\pi.$$

Le module de 0 est 0, mais on considère que 0 n'a pas d'argument.

Si M est le point d'affixe z, alors $|z|$ est la norme du vecteur $\overrightarrow{OM}$ et $\arg(z)$ est l'angle entre l'axe réel Ox et la demi-droite $[OM)$.



Propriété : liens entre les deux écritures

Soit $z \in \mathbf{C}$ d'écritures algébrique et polaire $z = x + \mathrm{i}y = r\mathrm{e}^{\mathrm{i}\theta}$. Alors

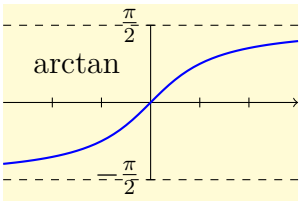
$$x = r\cos(\theta) \quad \text{et} \quad y = r\sin(\theta).$$

Propriété (suite)

$$|z| = r = \sqrt{x^2+y^2} \quad \text{et} \quad \arg(z) = \begin{cases} \arctan(\frac{y}{x}) & \text{si } x > 0 \\ \pi + \arctan(\frac{y}{x}) & \text{si } x < 0 \\ \frac{\pi}{2} & \text{si } x = 0 \text{ et } y > 0 \\ -\frac{\pi}{2} & \text{si } x = 0 \text{ et } y < 0 \end{cases}$$

Remarques

★ La fonction **tangente** est l'application de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ vers $\mathbf{R}$ qui à un angle associe la pente de la demi-droite correspondante. C'est une bijection. On appelle **arctangente** sa bijection réciproque.



★ Mis à part certains angles remarquables, on a rarement accès à une forme polaire très explicite : $\sqrt{3} - \mathrm{i} = 2\mathrm{e}^{-\mathrm{i}\frac{\pi}{6}}$, $9 + 4\mathrm{i} = \sqrt{97}\ \mathrm{e}^{\mathrm{i}\arctan(4/9)}$.

★ Pour tout $z \in \mathbf{C}$, $z\bar{z} = |z|^2$.

★ Le module permet de définir une **distance** sur $\mathbf{C}$:
pour z et z' dans $\mathbf{C}$, $|z - z'|$ représente la distance euclidienne dans le plan complexe entre les points d'affixes z et z'.

Propriété

Soient z_1, $z_2 \in \mathbf{C}$. Alors

★ $|z_1 z_2| = |z_1||z_2|$;

★ $|z_1| = |\bar{z}_1|$;

★ inégalité triangulaire : $|z_1 + z_2| \leq |z_1| + |z_2|$;

★ $\arg(z_1) = -\arg(\bar{z}_1) \mod 2\pi$;

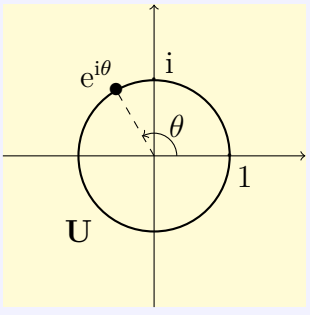
★ $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2) \mod 2\pi$.

Définition

On note $\mathbf{U}$ l'ensemble des nombres complexes dont le module est 1 :

$$\mathbf{U} = \{z \in \mathbf{C} \mid |z| = 1\} = \{\mathrm{e}^{\mathrm{i}\theta} \ ; \ \theta \in \mathbf{R}\}.$$

Dans le plan complexe l'ensemble $\mathbf{U}$ correspond au cercle unité.



2 Propriétés des nombres complexes

2.1 Racines de polynômes

Théorème fondamental de l'algèbre

Tout polynôme non constant à coefficients complexes admet une racine complexe.

Démonstration : Malgré son nom, ce théorème est en grande partie un théorème d'analyse reposant sur des propriétés de $\mathbf{R}$ et $\mathbf{C}$. Les résultats d'analyse nécessaires n'étant pas encore connus, nous ne pouvons donner qu'une idée de la preuve.

Soit P un polynôme non constant de $\mathbf{C}[X]$. Soit $r \geqslant 0$ et définissons l'application :

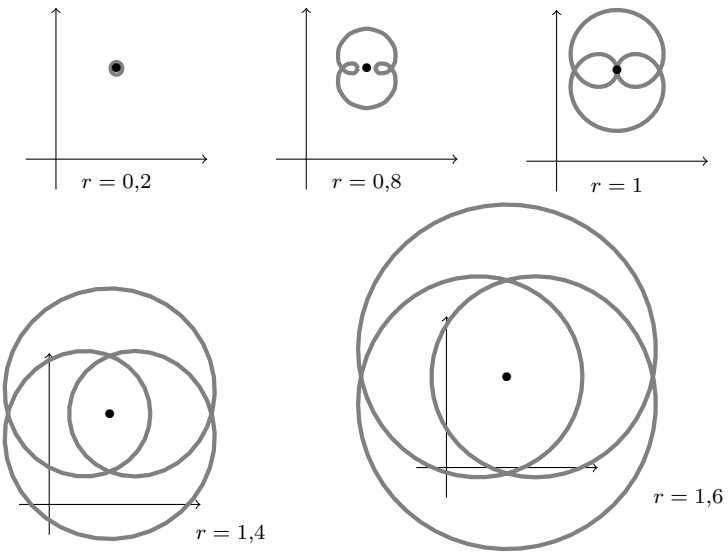
$$\begin{array}{rccc} f_r : & [0,2\pi] & \to & \mathbf{C} \\ & \theta & \mapsto & P(r\mathrm{e}^{\mathrm{i}\theta}). \end{array}$$

Cette application est continue et comme $f_r(0) = f_r(2\pi) = P(r)$, son image dans $\mathbf{C}$ est une courbe **continue** et **fermée**.
Pour $r = 0$, f_0 est constante et la courbe associée est simplement le point $\{P(0)\}$.
Lorsqu'on augmente r, cela revient à augmenter le module des nombres $r\mathrm{e}^{\mathrm{i}\theta}$ dont on considère l'image par P. Or on peut montrer que si $|z| \to +\infty$, alors $|P(z)| \to +\infty$. En effet, si on pose $P = a_n X^n + \cdots + a_1 X + a_0$ (avec $n \geqslant 1$ car P est non constant), alors d'après l'inégalité triangulaire :

$$|P(z)| \geqslant |a_n||z|^n - \sum_{k=0}^{n-1} |a_k||z|^k.$$

Le terme de droite diverge vers $+\infty$ quand $|z|$ tend vers $+\infty$, donc il en est de même pour $|P(z)|$.

Revenons à nos courbes. Cette dernière propriété signifie que lorsque r devient grand, les points de la courbe de f_r sont tous de module élevé. Regardons ce que cela donne sur un exemple. Nous avons pris $P = X^3 - X + 2 + 3\mathrm{i}$.



On comprend ainsi ce qu'il se passe. Lorsqu'on augmente r, nos courbes s'écartent de plus en plus de $P(0)$ tout en tournant autour de lui. Leur ensemble va recouvrir le plan complexe. En particulier, l'une d'elle passera par l'origine. Donc il existe r et θ tel que $P(r\mathrm{e}^{\mathrm{i}\theta}) = 0$. Autrement dit, le polynôme P admet une racine dans $\mathbf{C}$.
Sur notre exemple, on voit qu'une des racines de P aura un module compris entre 1 et 1,4. Et on comprend que notre argument repose sur une version généralisée du **théorème des valeurs intermédiaires**.

Corollaire

Tout polynôme de degré n à coefficients complexes peut s'écrire comme un produit de n polynômes de degré 1 à coefficients complexes.

Tout polynôme de degré n à coefficients complexes possède au plus n racines complexes.

Remarques Déterminer les racines d'un polynôme est crucial dans un grand nombre de problèmes mathématiques et scientifiques. On sait d'après le théorème ci-dessus qu'un polynôme quelconque possède toujours des racines. Encore faut-il réussir à les déterminer. Il existe des méthodes générales pour trouver toutes les racines des polynômes de degré 1, 2, 3 et 4. À partir du degré 5, on ne possède plus de méthode générale, mais pire, Évariste Galois a démontré qu'une telle méthode ne pouvait pas exister. À part pour certains polynômes particuliers, la seule méthode dont nous disposons en pratique est l'approximation numérique des racines. Cela mériterait un chapitre entier de cours mais ce sera pour une autre fois.

Regardons les quelques méthodes simples que nous connaissons.

Racines carrées

Définition

Soit $\omega \in \mathbf{C}$. Une racine carrée de ω est un nombre complexe z tel que $z^2 = \omega$. Autrement dit, c'est une racine du polynôme $X^2 - \omega$.

Remarques La notation $\sqrt{\omega}$ est interdite car ambiguë (ω possède deux racines carrées). Elle ne peut être utilisée que pour les nombres réels positifs et désigne dans ce cas l'unique racine positive du nombre.

Propriété

Soit $\omega \in \mathbf{C}$ de forme polaire $\omega = re^{i\theta}$.
Les racines carrées de ω sont les nombres complexes

$$z_1 = \sqrt{r}\ e^{i\frac{\theta}{2}} \quad \text{et} \quad z_2 = -\sqrt{r}\ e^{i\frac{\theta}{2}}.$$

En pratique, on ne dispose pas toujours de la forme polaire d'un nombre complexe. Il est néanmoins possible de déterminer ses racines carrées à partir de son écriture algébrique. Nous présentons la méthode à gauche et sa mise en œuvre sur l'exemple $\omega = 2 - 6i$.

Soit $\omega = a + \mathrm{i}b$.
On cherche les nombres complexes $x + \mathrm{i}y$ tels que $(x + \mathrm{i}y)^2 = a + \mathrm{i}b$.
En développant puis en identifiant parties réelle et imaginaire, on obtient un système à deux équations : $x^2 - y^2 = a$ et $2xy = b$.
Pour simplifier la résolution on ajoute la condition $|(x + \mathrm{i}y)^2| = |\omega|$, *i.e.* $x^2 + y^2 = |\omega|$.
En lui ajoutant et en lui soustrayant l'équation $x^2 - y^2 = a$, on obtient $x = \pm\sqrt{\frac{|\omega|+a}{2}}$ et $y = \pm\sqrt{\frac{|\omega|-a}{2}}$.
Parmi les 4 couples (x, y) ainsi obtenus, seuls deux vérifient l'équation $2xy = b$ (il suffit d'étudier les signes de x et y).
On obtient ainsi les deux solutions $x+\mathrm{i}y$ recherchées.

Soit $\omega = 2 - 6\mathrm{i}$.
On cherche des réels x et y tels que $(x+\mathrm{i}y)^2 = 2-6\mathrm{i}$.
Après développement et identification, on obtient $x^2 - y^2 = 2$ (1) et $2xy = -6$ (2).
De plus, on doit avoir $|x + \mathrm{i}y|^2 = |2 - 6\mathrm{i}|$, donc $x^2 + y^2 = \sqrt{40}$ (3).
En additionnant (1) et (3), on obtient $2x^2 = \sqrt{40}+2$, donc $x = \pm\sqrt{\sqrt{10}+1}$.
En soustrayant (1) à (3), on obtient $2y^2 = \sqrt{40} - 2$, donc $y = \pm\sqrt{\sqrt{10}-1}$.
Nous savons que ω possède deux racines carrées dans $\mathbf{C}$, mais nous avons obtenu 4 racines carrées potentielles. Or, d'après (2), $xy < 0$. On en déduit que x et y sont de signes opposés. Donc les racines carrées de ω sont

$$\sqrt{\sqrt{10}+1}-\mathrm{i}\sqrt{\sqrt{10}-1} \quad \text{et} \quad -\sqrt{\sqrt{10}+1}+\mathrm{i}\sqrt{\sqrt{10}-1}.$$

Racines d'un polynôme de degré 2

Propriété

Soient a, b et c dans $\mathbf{C}$ avec $a \neq 0$ et soit $P = aX^2 + bX + c$ un polynôme.
Soit $\Delta = b^2 - 4ac$ et soit δ une racine carrée de Δ.
Alors les racines de P sont les nombres complexes

$$z_1 = \frac{-b + \delta}{2a} \quad \text{et} \quad z_2 = \frac{-b - \delta}{2a}.$$

Remarques

★ Si P est à coefficients réels, son discriminant est un nombre réel. S'il est positif, on retrouve des expressions bien connues.
S'il est négatif, ses racines carrées sont $\pm\mathrm{i}\sqrt{-\Delta}$ et les racines de P sont $\frac{-b\pm\mathrm{i}\sqrt{-\Delta}}{2a}$.

★ Si $\Delta = 0$, alors $z_1 = z_2$ et on dit que P possède une **racine double**.

Exemples Soit $P = \mathrm{i}X^2 - X + 2$. Son **discriminant** est $\Delta = (-1)^2 - 8\mathrm{i} = 1 - 8\mathrm{i}$.
Les racines carrées de Δ sont $\delta = \sqrt{\frac{\sqrt{65}+1}{2}} - \mathrm{i}\sqrt{\frac{\sqrt{65}-1}{2}}$ et $-\delta$.
Les racines de P sont donc

$$\frac{1 + \sqrt{\frac{\sqrt{65}+1}{2}} - \mathrm{i}\sqrt{\frac{\sqrt{65}-1}{2}}}{2\mathrm{i}} \quad \text{et} \quad \frac{1 - \sqrt{\frac{\sqrt{65}+1}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{65}-1}{2}}}{2\mathrm{i}}.$$

Soit $Q = X^2 + 2X + \mathrm{i}$. Son discriminant est $\Delta = 4 - 4\mathrm{i} = 4\sqrt{2}\ \mathrm{e}^{-\mathrm{i}\frac{\pi}{4}}$. Les racines carrées de Δ sont $\delta = 2\sqrt[4]{2}\ \mathrm{e}^{-\mathrm{i}\frac{\pi}{8}}$ et $-\delta$. Les racines de Q sont donc

$$-1 + \sqrt[4]{2}\ \mathrm{e}^{-\mathrm{i}\frac{\pi}{8}} \quad \text{et} \quad -1 - \sqrt[4]{2}\ \mathrm{e}^{-\mathrm{i}\frac{\pi}{8}}.$$

Racines n-ièmes

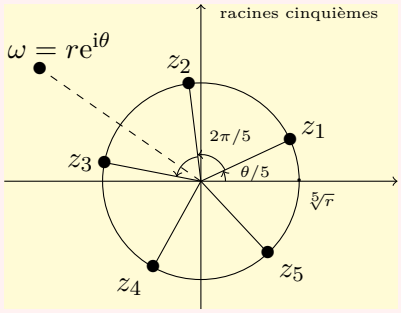
Définition

Soit $\omega \in \mathbf{C}$ et $n \geq 1$. Une racine n-ième de ω est un nombre complexe z tel que $z^n = \omega$. Autrement dit, c'est une racine du polynôme $X^n - \omega$.

Propriété

Soit $\omega \in \mathbf{C}$ de forme polaire $\omega = r\mathrm{e}^{\mathrm{i}\theta}$ et $n \geq 1$. Alors les racines n-ièmes de ω sont les n nombres complexes définis pour $k = 0, \ldots, n-1$ par

$$z_k = \sqrt[n]{r}\ \mathrm{e}^{\mathrm{i}\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)}.$$



2.2 Trigonométrie

L'utilisation de l'exponentielle complexe permet de simplifier certains calculs de trigonométrie.

Propriété Formules d'Euler et de Moivre

Soient $x \in \mathbf{R}$ et $n \in \mathbf{N}$. Alors

$$\cos(x) = \frac{\mathrm{e}^{\mathrm{i}x} + \mathrm{e}^{-\mathrm{i}x}}{2} \quad \text{et} \quad \sin(x) = \frac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}}.$$

$$(\cos(x) + \mathrm{i}\sin(x))^n = \cos(nx) + \mathrm{i}\sin(nx).$$

Avant de parler de linéarisation, rappelons quelques formules algébriques.

Propriété : binôme de Newton

Soient x et y deux nombres complexes et n un entier naturel. Alors

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

Propriété : somme des termes d'une suite géométrique

Soit z un nombre complexe tel que $z \neq 1$ et soit n un entier naturel. Alors

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

Cette formule découle de la formule suivante : pour tous a, b dans $\mathbf{C}$,

$$\begin{aligned} a^n - b^n &= (a-b)\sum_{k=0}^{n-1} b^k a^{n-1-k} \\ &= (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2 b^{n-3} + ab^{n-2} + b^{n-1}). \end{aligned}$$

De manière générale, **linéariser** une expression mathématique signifie l'exprimer comme une somme de termes d'ordre 1, c'est-à-dire sans exposants. En trigonométrie, linéariser une expression faisant intervenir des produits et des puissances de cosinus, sinus et tangente signifie l'exprimer comme une somme de cosinus, sinus et tangente. Par exemple l'égalité $\cos^2(x) = \dfrac{\cos(2x)+1}{2}$ est une linéarisation de $\cos^2(x)$. L'intérêt est que les expressions linéarisées sont en général plus facile à manipuler et à intégrer.

Pour linéariser une fonction trigonométrique, on remplace les cosinus et sinus par des exponentielles complexes à l'aide des formules d'Euler ; puis on développe les produits et puissances avec la formule du binôme de Newton ; enfin on regroupe les exponentielles de manière à faire réapparaître des cosinus et sinus.

Exemple Linéariser $\sin^3(x)$:

$$\begin{aligned} (\sin(x))^3 &= \left(\frac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}}\right)^3 = \frac{1}{-8\mathrm{i}}(\mathrm{e}^{3\mathrm{i}x} - 3\mathrm{e}^{\mathrm{i}x} + 3\mathrm{e}^{-\mathrm{i}x} - \mathrm{e}^{-3\mathrm{i}x}) \\ &= -\frac{1}{4}\left(\frac{\mathrm{e}^{3\mathrm{i}x} - \mathrm{e}^{-3\mathrm{i}x}}{2\mathrm{i}} - 3\frac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}}\right) = -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x). \end{aligned}$$

Cette linéarisation permet par exemple de déterminer une primitive de $\sin^3$:

$$\int \sin^3(x)\mathrm{d}x = \int -\frac{1}{4}\sin(3x) + \frac{3}{4}\sin(x)\ \mathrm{d}x = \frac{1}{12}\cos(3x) - \frac{3}{4}\cos(x).$$

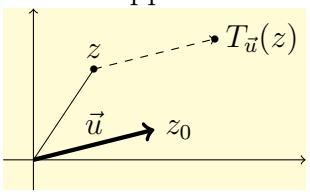
2.3 Transformations géométriques

Comme le plan est en bijection naturelle avec l'ensemble des nombres complexes, il est possible de voir les transformations du plan comme des applications de $\mathbf{C}$ dans $\mathbf{C}$. Pour les transformations usuelles, leur écriture complexe a le mérite d'être très simple.

Translations

Soit $\vec{u}$ un vecteur de $\mathbf{R}^2$. La translation de vecteur $\vec{u}$ est l'application du plan dans lui-même qui envoie tout point A sur le point B tel que $\overrightarrow{AB} = \vec{u}$.
Soit z_0 l'affixe de $\vec{u}$. Alors la translation de vecteur $\vec{u}$ correspond à l'application

$$\begin{array}{rccc} T_{\vec{u}} : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & z + z_0 \end{array}$$

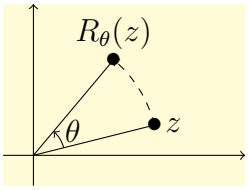


Remarque : $T_{\vec{u}}$ est une bijection et $T_{\vec{u}}^{-1} = T_{-\vec{u}}$.

Rotations

Soit $\theta \in \mathbf{R}$. La rotation d'angle θ et de centre 0 est l'application du plan dans lui-même qui envoie tout point A sur le point B tel que $OA = OB$ et $AOB = \theta$.
Alors la rotation d'angle θ correspond à l'application

$$\begin{array}{rccc} R_\theta : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & \mathrm{e}^{\mathrm{i}\theta} z \end{array}$$



Remarque : R_θ est une bijection et $R_\theta^{-1} = R_{-\theta}$.
De manière générale, $R_{\theta+\theta'} = R_\theta \circ R_{\theta'}$.

Soit Ω un point d'affixe z_0. Alors la rotation d'angle θ et de centre Ω correspond à l'application

$$\begin{array}{rccc} R_{\Omega,\theta} : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & z_0 + \mathrm{e}^{\mathrm{i}\theta}(z - z_0) \end{array}$$

On remarque que $R_{\Omega,\theta} = T_{\overrightarrow{O\Omega}} \circ R_\theta \circ T_{\overrightarrow{\Omega O}}$.

Propriété

Soient a et b dans $\mathbf{C}$ et $\varphi : z \mapsto az + b$. Si $|a| = 1$ mais $a \neq 1$, φ est une rotation du plan.
Son centre Ω est l'unique **point fixe** de φ : $\varphi(z_\Omega) = z_\Omega$.
Son angle de rotation est l'argument de a.

Exemple Étudions l'application $\varphi : z \mapsto -\mathrm{i}z + 2 - 3\mathrm{i}$.
La forme polaire de $-\mathrm{i}$ et $\mathrm{e}^{-\mathrm{i}\frac{\pi}{2}}$. On en déduit une décomposition de φ en transformations élémentaires : $\varphi = T_{2-3\mathrm{i}} \circ R_{-\frac{\pi}{2}}$. Si on écrit $\varphi(z) = -\mathrm{i}(z+2\mathrm{i}+3)$, on obtient une autre décomposition : $\varphi = R_{-\frac{\pi}{2}} \circ T_{3+2\mathrm{i}}$.

La composée d'une rotation et d'une translation est une rotation. Cherchons maintenant ses caractéristiques. Son angle de rotation est l'argument de $-\mathrm{i}$, donc $-\frac{\pi}{2}$.

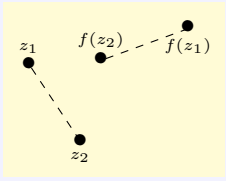
Cherchons son centre. Soit $z \in \mathbf{C}$. C'est un point de fixe de φ si $\varphi(z) = z$ ssi $-\mathrm{i}z + 2 - 3\mathrm{i} = z$ ssi $z(1 + \mathrm{i}) = 2 - 3\mathrm{i}$ ssi $z = \frac{2-3\mathrm{i}}{1+\mathrm{i}} = -\frac{1}{2} - \frac{5}{2}\mathrm{i}$.

Ainsi φ est la rotation de centre $-\frac{1}{2} - \frac{5}{2}\mathrm{i}$ et d'angle $-\frac{\pi}{2}$. On peut vérifier qu'on a bien $\varphi(z) = -\mathrm{i}(z + \frac{1}{2} + \frac{5}{2}\mathrm{i}) - \frac{1}{2} - \frac{5}{2}\mathrm{i}$.

Définition

On appelle **isométrie du plan** toute application f du plan qui préserve les distances. En notation complexe, il s'agit des applications $f : \mathbf{C} \to \mathbf{C}$ vérifiant

$$\forall (z_1, z_2) \in \mathbf{C}^2, \quad |f(z_2) - f(z_1)| = |z_2 - z_1|.$$



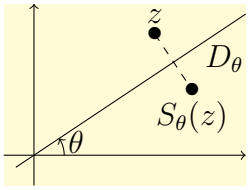
Une isométrie du plan est complètement définie si on connaît ses images de trois points non alignés. Cette propriété permet de caractériser toutes les isométries du plan :

Théorème

Les isométries du plan sont les translations, les rotations, les symétries axiales et les symétrie glissées (c'est-à-dire les composées d'une symétrie et d'une translation).

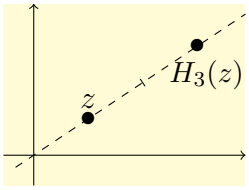
Les **symétries axiales** peuvent également être exprimées sous forme complexe en utilisant la conjugaison.

Si on sort du cadre des isométries, d'autres transformations géométriques s'expriment naturellement en complexe. Citons simplement les **homothéties** qui permettent de grossir ou de réduire les distances tout en préservant les angles et les formes.



$S_\theta(z) = \mathrm{e}^{2\mathrm{i}\theta}\bar{z}$

Symétrie orthogonale d'axe D_θ



$H_3(z) = 3z$

Homothétie de centre O, de rapport 3

À retenir

- ★ Maîtriser écriture algébrique, écriture polaire et point de vue géométrique, et savoir passer de l'un à l'autre.
- ★ Savoir extraire les racines carrées d'un nombre complexe sous forme algébrique et polaire et les racines n-ièmes sous forme polaire.
- ★ Savoir déterminer les racines d'un polynôme de degré 2.
- ★ Connaître les formules d'Euler.
- ★ Savoir caractériser les rotations et translations du plan.

V. Groupes, anneaux et corps

1 Loi de composition

Définition

Soit E un ensemble. On appelle **loi de composition interne** dans E toute application de $E \times E$ vers E.
Nous noterons de telles applications non pas sous la forme $f(x, y)$ mais à l'aide d'un symbole sous la forme $x * y$.

Exemples L'addition est une loi de composition interne dans $\mathbf{N}$. La soustraction et la multiplication sont des lois internes dans $\mathbf{Z}$. La division en est une dans $\mathbf{R}^*$.

Définition

Soit E un ensemble muni d'une loi de composition interne notée $*$. On dit que

- ★ La loi $*$ est **associative** si : $\forall (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z$
- ★ La loi $*$ est **commutative** si : $\forall (x, y) \in E^2,\ x * y = y * x$

2 Groupes

Définition

Soit G un ensemble muni d'une loi de composition interne notée $*$. On dit que le couple $(G, *)$ est un **groupe** si

- ★ la loi $*$ est associative ;
- ★ G possède un élément neutre : $\exists e \in G, \forall x \in G,\ x * e = e * x = x$;
- ★ tout élément de G admet un inverse : $\forall x \in G, \exists y \in G,\ x * y = y * x = e$.

Si de plus la loi $*$ est commutative, on dit que le groupe $(G, *)$ est **commutatif** ou encore **abélien**.

Exemples Les exemples ci-dessous sont des groupes de référence à connaître !
⋆ $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$ et $(\mathbf{R}^2, +)$ sont des groupes.
⋆ $(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$ et $(\mathbf{C}^*, \times)$ sont des groupes.
⋆ Soit E un ensemble. Alors $(\mathrm{Bij}(E), \circ)$ est un groupe.

Voici un autre exemple. On définit sur $\mathbf{Z}$ la loi $*$ par : $\forall (n,m) \in \mathbf{Z}$, $n*m = n+m-n\times m$. $(\mathbf{Z},*)$ est-il un groupe ?

★ La loi $*$ est bien une loi interne à $\mathbf{Z}$: pour tous entiers n et m, $n*m$ est encore un entier.

★ Montrons que la loi $*$ est associative : soient n, m et p des entiers. Alors

$$(n*m)*p = (n+m+nm)*p = (n+m-nm)+p-(n+m-nm)p = n+m+p-nm-np-mp+nmp.$$

De même, on trouve $n*(m*p) = n*(m+p-mp) = n+m+p-nm-np-mp+nmp$. Ainsi $(n*m)*p = n*(m*p)$. Remarquons que la loi $*$ est également commutative puisque $n*m = m*n = n+m-nm$.

★ L'entier 0 est élément neutre pour la loi $*$: pour tout entier n, $n*0 = n+0-n\times 0 = n$. Et par commutativité, $0*n = n$ également.

★ On remarque que 0 a pour inverse 0 pour la loi $*$ puisque $0*0 = 0$. De même, 2 a pour inverse 2 puisque $2*2 = 2+2-2\times 2 = 0$. Mais tous les entiers ne possèdent pas d'inverse pour notre loi. Par exemple, pour tout entier n, $1*n = 1+n-1\times n = 1 \neq 0$. Donc 1 n'a pas d'inverse pour la loi $*$.

Conclusion : $(\mathbf{Z},*)$ n'est pas un groupe puisque la propriété des inverses n'est pas satisfaite.

Remarques Dire qu'un ensemble G est un groupe n'a pas de sens si on ne précise pas pour quelle loi. Un groupe est un couple, c'est un ensemble muni d'une loi.

Très souvent, on n'utilise pas le symbole de la loi du groupe et on se contente de noter xy le produit $x*y$. De même, pour $x \in G$, on notera x^{-1} l'inverse de x et pour $n \in \mathbf{Z}$, on notera x^n pour le produit $x*\cdots*x$ ou $x^{-1}*\cdots*x^{-1}$ selon le signe de n, x^0 étant égal à l'élément neutre e.

Attention, si le groupe n'est pas commutatif, on ne peut pas simplifier certaines expressions : $xyx \neq x^2y$, $xyx^{-1}y^{-1} \neq e$. Si $xy = zx$, on ne peut pas déduire $y = z$.

Lorsqu'un groupe est commutatif, on note souvent sa loi avec le symbole $+$. Dans ce cas, on note $-x$ l'inverse de x et pour $n \in \mathbf{Z}$, nx désigne l'élément $\pm(x+\cdots+x)$ selon le signe de n.

Propriété

Soit $(G,\cdot)$ un groupe d'élément neutre e. Alors

★ L'élément neutre e est unique.

★ Pour tout x dans G, son inverse est unique.

★ L'inverse de e est e.

★ L'inverse de xy est $y^{-1}x^{-1}$.

★ Pour tous x, y et z dans G, $xy = xz \implies y = z$ et $yx = zx \implies y = z$.

Remarques Historiquement, la notion de groupe a été introduite par Évariste Galois au XIXème siècle dans le cadre de la résolution des équations polynomiales. On sait, depuis longtemps, déterminer explicitement les racines des polynômes de degré 2, 3 et 4 grâce à des formules (méthodes du discriminant, de Cardan, etc). Galois a démontré, grâce à la notion de groupe, qu'à partir du degré 5, de telles formules ne pouvaient pas exister et qu'il n'existe donc pas de méthode générale pour résoudre les équations polynomiales.

Les groupes sont aussi énormément utilisés pour faire de la géométrie. Le groupe des isométries permet de faire de la géométrie euclidienne, le groupe affine, de la géométrie

affine, les groupes projectifs de la géométrie projective, etc. Ils ont permis notamment de comprendre et classer les différents pavages du plan ou les polyèdres réguliers.

En dehors des mathématiques, les groupes ou des structures analogues interviennent dans de nombreux domaines de la physique. Citons la crystallographie, la relativité restreinte, la mécanique quantique,...

Mentionnons enfin le Monstre qui est un groupe fini à
808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000 éléments. Il a été découvert afin de répondre à un problème de mathématiques compliqué mais il intervient également dans des problèmes de symétrie en physique mathématique.

3 Sous-groupes

Définition

Soit $(G, *)$ un groupe et $H \subset G$. On dit que H est un **sous-groupe** de G si $(H, *)$ est un groupe, c'est-à-dire si la restriction de la loi $*$ au sous-ensemble H confère à H une structure de groupe.

Cette propriété implique notamment que H est stable par la loi $*$. Mathématiquement, la définition de sous-groupe se traduit ainsi :

Définition

Soit $(G, *)$ un groupe d'élément neutre e et soit $H \subset G$. L'ensemble H est un sous-groupe de G si

- ★ $\forall x \in H, \forall y \in H,\ x * y \in H$;
- ★ $e \in H$;
- ★ $\forall x \in H,\ x^{-1} \in H$.

Exemples

- ★ Le groupe tout entier G et $\{e\}$ sont des sous-groupes triviaux de $(G, *)$.
- ★ $(\mathbf{Q}^*, \times)$ est un groupe et $\mathbf{Q}^* \subset \mathbf{R}^*$, donc $\mathbf{Q}^*$ est un sous-groupe de $(\mathbf{R}^*, \times)$.
- ★ L'ensemble des nombres pairs est un sous-groupe de $(\mathbf{Z}, +)$: en effet, la somme de deux nombres pairs est un nombre pair ; l'élément neutre de $\mathbf{Z}$ est 0 et il est pair ; l'opposé d'un nombre pair est encore un nombre pair. Les propriétés du groupe $(\mathbf{Z}, +)$ sont donc stables dans l'ensemble des nombres pairs et ce dernier est donc un sous-groupe.
- ★ Soit $D = \{\ (x, y) \mid y = 3x\ \}$. Montrons que D est un sous-groupe de $(\mathbf{R}^2, +)$.
  - ⋆ Montrons que D est stable pour $+$: soient (x, y) et (x', y') dans D. Alors $y = 3x$ et $y' = 3x'$. Donc $(y + y') = 3(x + x')$. Ainsi $(x + x', y + y')$ est aussi un élément de D. Donc $(x, y) + (x', y') \in D$.
  - ⋆ L'élément neutre de $(\mathbf{R}^2, +)$ est $(0, 0)$. Il vérifie $0 = 3 \times 0$, donc $(0, 0) \in D$.
  - ⋆ Soit $(x, y) \in D$. Alors $y = 3x$. Donc $-y = 3 \times (-x)$. Donc $(-x, -y) \in D$. Donc D est stable par inversion.
- ★ L'ensemble Isom des isométries du plan est un sous-groupe de $(\mathrm{Bij}(\mathbf{R}^2), \circ)$: en effet, la composée de deux isométries est encore une isométrie, l'application identité est une isométrie et la bijection réciproque d'une isométrie est encore une isométrie.

Propriété

Soient H et K des sous-groupes d'un groupe $(G, *)$. Alors $H \cap K$ est un sous-groupe de $(G, *)$.

Remarques En général $H \cup K$ n'est pas un sous-groupe.

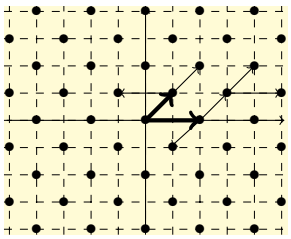
Définition

Soit $(G, *)$ un groupe et $A \subset G$. On appelle **sous-groupe engendré par** A le plus petit sous-groupe (pour l'inclusion) de G contenant A. On le note $<A>$.
Si $<A> = G$, on dit que l'ensemble A engendre le groupe G.

Remarques Le sous-groupe engendré est l'ensemble des éléments que l'on peut obtenir en utilisant les éléments de A, la loi $*$ et les inverses.
L'ensemble A n'est a priori pas un sous-groupe de G. Si A est un sous-groupe, le sous-groupe qu'il engendre est trivialement A lui-même.

Exemples ★ Dans $(\mathbf{Z}, +)$, le sous-groupe $<\{2\}>$ engendré par 2 est le sous-groupe des nombres pairs : avec 2, l'addition et la soustraction, on peut obtenir tous les nombres pairs mais aucun nombre impair.
Avec les nombres 2 et 3, l'addition et la soustraction, on peut obtenir tous les nombres entiers. Donc les nombres 2 et 3 engendrent $(\mathbf{Z}, +)$: $<\{2, 3\}> = \mathbf{Z}$.

★ Dans $(\mathbf{R}^2, +)$, quel est le sous-groupe engendré par les vecteurs $(2, 0)$ et $(1, 1)$? Graphiquement, on additionnant ou soustrayant ces vecteurs autant de fois qu'on le souhaite, on obtient ce qu'on appelle un réseau. Il s'agit ici du réseau des points à coordonnées entières et de même parité :



$$<\{(2,0),(1,1)\}> = \{(a,b) \in \mathbf{Z}^2 \mid a-b \text{ est pair}\}.$$

Démontrons-le :

Notons $H = \{(a,b) \in \mathbf{Z}^2 \mid a-b \text{ est pair}\}$. Soit $(a,b) \in H$. Montrons qu'il est engendré par $(2,0)$ et $(1,1)$. Notons $a-b = 2k$ avec $k \in \mathbf{Z}$. Alors on peut écrire $(a,b) = (a-b,0) + (b,b) = k \times (2,0) + b \times (1,1)$. Autrement dit, (a,b) peut être obtenu en additionnant (ou soustrayant selon les signes de k et b) k fois $(2,0)$ et b fois $(1,1)$. Il appartient bien au sous-groupe engendré par ces deux vecteurs. On en déduit que $H \subset <\{(2,0),(1,1)\}>$.
Montrons maintenant que H est un sous-groupe de $(\mathbf{R}^2, +)$: H est stable par addition car si $(a,b) \in \mathbf{Z}^2$ et $(c,d) \in \mathbf{Z}^2$ avec $a-b$ et $c-d$ pairs, alors $(a+c, b+d) \in \mathbf{Z}^2$ avec $(a+c)-(b+d)$ pair. Le vecteur nul est bien dans H, et l'opposé $(-a,-b)$ d'un vecteur (a,b) de H est encore à coordonnées entières avec $(-a)-(-b)$ pair. Donc H est bien un sous-groupe. De plus il contient les vecteurs $(2,0)$ et $(1,1)$. Il contient donc le plus petit sous-groupe qui les contient. Donc $<\{(2,0),(1,1)\}> \subset H$.
Par double inclusion, on peut conclure.

★ Toute translation dans le plan peut être obtenue comme la composée de deux rotations : la translation de vecteur $\overrightarrow{O\Omega}$ est, par exemple, la composée des rotations $R_{O,\pi}$ et $R_{I,\pi}$ où I est le milieu du segment $[O\Omega]$. Il est alors possible de démontrer que le sous-groupe engendré par l'ensemble des rotations du plan est l'ensemble des isométries directes du plan :

$$<\{R_{\Omega,\theta}\ ;\ \Omega \in \mathbf{R}^2, \theta \in \mathbf{R}\}> = Isom_+ = \{\text{rotations et translations du plan}\}.$$

4 Morphismes de groupes

Un morphisme, du grec *morphos*, la forme, est une application qui préserve la structure.

Définition

Soient $(G, *)$ et $(F, \circledast)$ des groupes et $f : G \to F$ une application. On dit que f est un **morphisme de groupes** si f préserve les structures des groupes :

- ★ $\forall x \in G, \forall y \in G,\ f(x * y) = f(x) \circledast f(y)$;
- ★ $f(e_G) = e_F$;
- ★ $\forall x \in G,\ f(x^{-1}) = f(x)^{-1}$.

Remarques Pour montrer que f est un morphisme de groupes, il suffit en fait de vérifier la première condition. Elle implique en effet les deux autres conditions.

Exemples Soit $f : (\mathbf{C}^*, \times) \to (\mathbf{R}, +)$ défini par $f(x) = \ln(|z|)$. Montrons que c'est un morphisme de groupes.

Soient z et z' dans $\mathbf{C}^*$. Alors $f(z \times z') = \ln(|zz'|) = \ln(|z| \cdot |z'|) = \ln(|z|) + \ln(|z'|) = f(z) + f(z')$.

Donc f est bien un morphisme de groupe pour les lois $\times$ et $+$.

Soit $g : (\mathbf{R}^2, +) \to (\text{Isom}, \circ)$ l'application qui à un vecteur $\vec{u}$ de $\mathbf{R}^2$ associe la translation de vecteur $\vec{u}$: $g(\vec{u}) = T_{\vec{u}}$. Montrons que g est un morphisme de groupes.

Soient $\vec{u}$ et $\vec{v}$ des vecteurs de $\mathbf{R}^2$. Alors $g(\vec{u} + \vec{v}) = T_{\vec{u}+\vec{v}}$. D'autre part, si on compose la translation de vecteur $\vec{u}$ avec la translation de vecteur $\vec{v}$, on obtient la translation de vecteur $\vec{v} + \vec{u}$. Ainsi $T_{\vec{u}} \circ T_{\vec{v}} = T_{\vec{u}+\vec{v}}$. Finalement, $g(\vec{u} + \vec{v}) = g(\vec{u}) \circ g(\vec{v})$ et g est bien un morphisme de groupes.

Définition

L'ensemble des morphismes de $(G, *)$ dans $(F, \times)$ se note $\text{Hom}(G, F)$.
Si $f \in \text{Hom}(G, G)$, on dit que f est un **endomorphisme**.
Si $f \in \text{Hom}(G, F)$ est une bijection, on dit que f est un **isomorphisme** de groupes.

Propriété

La composée de deux morphismes de groupes est un morphisme de groupes.

Définition

Soit $f \in \text{Hom}(G, F)$. On appelle **noyau** de f l'ensemble

$$\text{Ker}(f) = f^{-1}(\{e_F\}) = \{x \in G \mid f(x) = e_F\}.$$

Propriété

Soit $f \in \mathrm{Hom}(G, F)$. Alors

- ★ $\mathrm{Ker}(f)$ est un sous-groupe de $(G, *)$;
- ★ $\mathrm{Im}(f)$ est un sous-groupe de $(F, \times)$;
- ★ le morphisme f est injectif si et seulement si $\mathrm{Ker}(f) = \{e_G\}$.

Exemples Reprenons les morphismes f et g définis plus haut et cherchons leurs noyaux ; le noyau de f est l'ensemble des éléments z de $\mathbf{C}^*$ qui sont envoyés sur l'élément neutre 0 de $(\mathbf{R}, +)$. Soit $z \in G$. Alors

$$z \in \mathrm{Ker}(f) \Leftrightarrow f(z) = 0 \Leftrightarrow \ln(|z|) = 0 \Leftrightarrow |z| = 1.$$

Ainsi $\mathrm{Ker}(f)$ est l'ensemble des nombres complexes de module 1 : $\mathrm{Ker}(f) = \mathbf{U}$. Il s'agit bien d'un sous-groupe de $(\mathbf{C}^*, \times)$. En particulier, $\mathrm{Ker}(f) \neq \{1\}$ et f n'est pas injectif.

Le noyau de g est l'ensemble des vecteurs $\vec{u}$ de $\mathbf{R}^2$ qui sont envoyés sur l'élément neutre id de Isom. Autrement dit, $\vec{u} \in \mathrm{Ker}(g)$ si et seulement si $T_{\vec{u}} = \mathrm{id}$. Or la seule translation égale à l'application identité est la translation de vecteur nul. Donc $\vec{u} \in \mathrm{Ker}(g)$ si et seulement si $\vec{u} = \vec{0}$ et on conclut que $\mathrm{Ker}(g) = \{\vec{0}\}$. En particulier, le morphisme g est injectif.

5 Groupes finis

Un groupe fini est un groupe de cardinal fini. Ces groupes ont été largement étudiés et classifiés. Il existe en effet de nombreuses propriétés qui ne dépendent que du cardinal du groupe et non de son contenu explicite. Voilà une de ces propriétés générales.

Théorème de Lagrange

Soit $(G, *)$ un groupe fini et H un sous-groupe de G.
Alors le cardinal de H divise le cardinal de G.

Démonstration : Notons k le cardinal de H. Soit $x \in G$ et soit $A_x = \{xh; h \in H\}$.
Montrons que $\mathrm{Card}(A_x) = \mathrm{Card}(H)$: soient h_1 et h_2 deux éléments distincts de H. Si $xh_1 = xh_2$, alors comme on est dans un groupe on peut en déduire $h_1 = h_2$, ce qui est faux. Donc $xh_1 \neq xh_2$. Ainsi les k éléments xh pour h variant dans H sont deux à deux distincts et donc A_x contient k éléments : $\mathrm{Card}(A_x) = \mathrm{Card}(H)$.
Montrons maintenant que si x et y sont dans G, alors $A_x = A_y$ ou A_x et A_y sont disjoints. Soient donc x et y dans G. Supposons que A_x et A_y ne sont pas disjoints. Il existe donc un élément commun à ces deux ensembles. On a donc h_1 et h_2 dans H tels que $xh_1 = yh_2$. Donc $x = yh_2h_1^{-1}$. Considérons un élément quelconque de A_x. Il est de la forme xh avec $h \in H$. Or $xh = yh_2h_1^{-1}h$. Comme H est un sous-groupe de G, $h_2h_1^{-1}h \in H$ et donc $yh_2h_1^{-1}h \in A_y$. On a ainsi démontré que $xh \in A_y$ pour tout $h \in H$. Donc $A_x \subset A_y$. On montre de la même manière que $A_y \subset A_x$. Ainsi, si A_x et A_y ne sont pas disjoints, alors $A_x = A_y$.
Remarquons avant de conclure que puisque $e \in H$, $xe = x \in A_x$. Ainsi tout élément de G est dans l'un des ensembles A_x. Nous pouvons désormais conclure : tout élément de G est dans une certaine partie A_x de G. Chacune de ces parties est de cardinal k. Et ces différentes parties sont deux à deux disjointes. On en déduit que G se découpe en un certain nombre de parties A_x toutes de même cardinal k. Donc k divise n.

Définition

Soit $(G, *)$ un groupe de cardinal fini. Soit H un sous-groupe de G et $x \in G$.
On appelle **ordre** de H le cardinal de H. On appelle **ordre** de x le cardinal du sous-groupe $< x >$ engendré par x.

Propriété

Soit x un élément d'un groupe $(G, *)$. L'ordre de x est le plus petit entier positif d non nul tel que $x^d = e$.
Le sous-groupe engendré par x est alors l'ensemble $\{x, x^2, x^3, \ldots, x^{d-1}, x^d\}$.
Et d'après le théorème de Lagrange, l'ordre d de x divise le cardinal de G.

Démonstration : Soit $x \in G$. Montrons d'abord qu'un tel entier d existe. Soit $E = \{x^k; k \in \mathbf{N}^*\}$. C'est une partie de G. Or G est fini et E est indexé par un ensemble infini. Nécessairement il existe deux indices i et j distincts tels que $x^i = x^j$. Supposons $j > i$. On obtient alors $x^{j-i} = e$. Ainsi, il existe bien une puissance non nulle de x qui vaut e. On note alors d le plus petit entier non nul tel que $x^d = e$.

Posons maintenant $H = \{x, x^2, x^3, \ldots, x^{d-1}, x^d\}$. Montrons que $H = <x>$.
Montrons déjà que H est un sous-groupe de $(G, *)$. Comme $x^d = e$, $e \in H$. Soit $1 \leq i \leq d$ et x^i un élément de H. Alors $x^i x^{d-i} = x^d = e$. Donc l'inverse de x^i est x^{d-i}, c'est bien un élément de H. Enfin, soient x^i et x^j avec $1 \leq i, j \leq d$ des élément de H. Alors $x^i x^j = x^{i+j}$. Si $1 \leq i + j \leq d$, alors $x^i x^j \in H$. Si $d + 1 \leq i + j \leq 2d$, alors $x^{i+j} = x^{i+j-d} x^d = x^{i+j-d}$ avec $1 \leq i + j - d \leq d$. Donc $x^i x^j \in H$ dans tous les cas.
Ainsi, H est bien un sous-groupe. C'est donc un sous-groupe de G contenant x et ainsi $<x> \subset H$.

Enfin, le sous-groupe engendré par x contient nécessairement x et toutes ses puissances. En particulier, $H \subset <x>$.
Donc $H = <x>$.

Propriété

Soit $n \in \mathbf{N}$, $(G, *)$ un groupe de cardinal n et $x \in G$. Alors $x^n = e$.

Définition

Un groupe fini est **cyclique** s'il existe un élément de G qui engendre G :

$$\exists x \in G, \ <x> = G.$$

Si n est le cardinal de G, cela signifie qu'il existe un élément d'ordre n.

6 Structures de groupes sur $\mathbf{Z}/n\mathbf{Z}$

On a vu que l'on pouvait munir l'ensemble $\mathbf{Z}/n\mathbf{Z}$ de l'addition et de la multiplication usuelles. Obtient-on ainsi des groupes ?

Propriété

Soit $n \in \mathbf{Z}^*$. $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe commutatif.

Il est cyclique : $\mathbf{Z}/n\mathbf{Z} = <\bar{1}>$.

Exemple Dans $(\mathbf{Z}/20\mathbf{Z}, +)$, l'opposé de $\overline{15}$ est $-\overline{15} = \overline{5}$ et $\overline{15}$ est d'ordre 4 car $\overline{15} + \overline{15} \neq \overline{0}$, $\overline{15} + \overline{15} + \overline{15} \neq \overline{0}$ et $\overline{15} + \overline{15} + \overline{15} + \overline{15} = \overline{0}$.

En revanche $(\mathbf{Z}/n\mathbf{Z}, \times)$ n'est clairement pas un groupe car $\bar{0}$ n'a pas d'inverse. Mais on peut retirer $\bar{0}$ et se demander si $((\mathbf{Z}/n\mathbf{Z})^*, \times)$ est un groupe.

Propriété

Soit $p \geqslant 2$. $((\mathbf{Z}/p\mathbf{Z})^*, \times)$ est un groupe si et seulement si p est un nombre premier.

Il est de cardinal $p-1$.

Démonstration : Soit p un nombre premier. Montrons alors que $((\mathbf{Z}/p\mathbf{Z})^*, \times)$ est un groupe.

- ★ Il faut d'abord vérifier que la loi $\times$ est bien interne à $(\mathbf{Z}/p\mathbf{Z})^*$. C'est une conséquence du lemme d'Euclide : soient $\bar{a}$ et $\bar{b}$ tels que $\bar{a}\bar{b} = \bar{0}$ dans $\mathbf{Z}/p\mathbf{Z}$. Cela signifie que ab est un multiple de p. Or p est premier, donc a ou b est un multiple de p. Ainsi, dans $\mathbf{Z}/p\mathbf{Z}$, $\bar{a}\bar{b} = \bar{0} \implies \bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Par contraposée, si $\bar{a}$ et $\bar{b}$ sont non nuls, alors $\bar{a}\bar{b}$ est également non nul. Donc $(\mathbf{Z}/p\mathbf{Z})^*$ est stable par produit.
- ★ On sait que la loi $\times$ est associative.
- ★ $\bar{1}$ est clairement élément neutre.
- ★ Soit $\bar{a} \in (\mathbf{Z}/p\mathbf{Z})^*$. Montrons qu'il possède un inverse. C'est une conséquence du théorème de Bézout. Comme $\bar{a} \neq \bar{0}$, a et p sont premiers entre eux, il existe u et v dans $\mathbf{Z}$, tels que $au + vp = 1$. Alors, modulo p, $\bar{a}\bar{u} = \bar{1}$. Donc $\bar{u}$ est l'inverse de $\bar{a}$.

Nous avons bien un groupe.

Si p n'est pas un nombre premier, alors le premier point n'est pas satisfait. On peut factoriser p en $p = ab$ avec $a < p$ et $b < p$. Alors $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$ mais $\bar{a}\bar{b} = \bar{0}$. Donc $(\mathbf{Z}/p\mathbf{Z})^*$ n'est pas stable par produit.

Remarques Nous disposons ainsi d'une méthode pour déterminer l'inverse d'un nombre modulo p : l'égalité de Bézout que l'on sait obtenir avec l'algorithme d'Euclide.

Exemple Soit $\bar{5} \in (\mathbf{Z}/17\mathbf{Z})^*$. Déterminer son inverse.

On applique l'algorithme d'Euclide à 5 et 17 et on trouve l'égalité de Bézout : $5 \cdot 7 - 17 \cdot 2 = 1$. Donc, dans $\mathbf{Z}/17\mathbf{Z}$, $\bar{5} \cdot \bar{7} = \bar{1}$ et $\bar{7}$ est donc l'inverse de $\bar{5}$.

Déterminer l'ordre de $\bar{5}$ dans $(\mathbf{Z}/17\mathbf{Z})^*$ ainsi que le sous-groupe qu'il engendre.

Nous allons appliquer les résultats de la partie précédente. Tout d'abord on sait que l'ordre de $\bar{5}$ divise le cardinal du groupe, c'est-à-dire 16. Cet ordre peut donc être égal à 1, 2, 4, 8 ou 16. Calculons les puissances de 5 modulo 17 jusqu'à ce qu'on obtienne 1 : dans $\mathbf{Z}/17\mathbf{Z}$, $\bar{5}^2 = \bar{8}$, $\bar{5}^3 = \bar{6}$, $\bar{5}^4 = \overline{13}$, $\bar{5}^5 = \bar{3}$, $\bar{5}^6 = \overline{15}$, $\bar{5}^7 = \bar{7}$, $\bar{5}^8 = \bar{1}$. Donc $\bar{5}$ est d'ordre 8 et $<\{\bar{5}\}> = \{\bar{5}, \bar{8}, \bar{6}, \overline{13}, \bar{3}, \overline{15}, \bar{7}, \bar{1}\}$. Remarquons qu'on retrouve bien l'inverse de $\bar{5}$, il s'agit de la dernière puissance calculée avant d'obtenir $\bar{1}$.

Corollaire : petit théorème de Fermat

Soit p un nombre premier et soit a un nombre entier premier avec p.
Alors $a^{p-1} \equiv 1 \mod p$.

Terminons par un résultat peu important dans le cadre de ce cours mais important pour certaines applications arithmétiques.

Propriété

Soit p un nombre premier.
Alors $((\mathbf{Z}/p\mathbf{Z})^*, \times)$ est un groupe cyclique.

Il s'agit d'une propriété absolument non triviale. Un point important de la démonstration est que l'on prouve l'existence d'un élément engendrant $(\mathbf{Z}/p\mathbf{Z})^*$ mais qu'on ne donne aucune méthode pour trouver un tel élément explicitement. Si une telle méthode existait, beaucoup de systèmes cryptographiques s'effondreraient.

Démonstration : Nous donnons les étapes de la preuve.

- ★ Si q est un nombre premier et d tels que q^d divise $p-1$. Montrons qu'il existe un élément d'ordre q^d. D'après le petit théorème de Fermat, on a pour tout x dans $(\mathbf{Z}/p\mathbf{Z})^*$, $x^{p-1}=1$, donc $\left(x^{\frac{p-1}{q^d}}\right)^{q^d}=1$. On en déduit que tous les éléments de la forme $x^{\frac{p-1}{q^d}}$ ont leur ordre qui divise q^d. Comme q est premier, leur ordre est une puissance de q. Si aucun d'entre eux n'était d'ordre q^d, alors on en déduirait que pour tout x, $\left(x^{\frac{p-1}{q^d}}\right)^{q^{d-1}}=1$. Cela signifierait que tous les éléments de $(\mathbf{Z}/p\mathbf{Z})^*$ seraient racines du polynôme $X^{\frac{p-1}{q}}-1$. Or, comme $(\mathbf{Z}/p\mathbf{Z},+,\times)$ est un anneau intègre, on sait que ce polynôme ne peut avoir qu'au plus $\frac{p-1}{q}$ racines dans $\mathbf{Z}/p\mathbf{Z}$ (voir plus bas le théorème de la section 8.1). On obtient donc une contradiction et il y a nécessairement un élément d'ordre q^d.
- ★ Propriété valable dans tout groupe commutatif : si x est un élément d'ordre a et y un élément d'ordre b avec a et b premiers entre eux, alors xy est d'ordre ab.
- ★ Si on combine les deux dernières propriétés, on montre facilement en partant de la décomposition en facteurs premiers de $p-1$ qu'il existe un élément d'ordre $p-1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$.

7 Le groupe des permutations

Fixons un entier $n \in \mathbf{N}^*$ pour toute cette partie.

Définition

On note $\mathfrak{S}_n$ l'ensemble des bijections de $\{1,\dots,n\}$. Une telle bijection est appelée **permutation** de $\{1,\dots,n\}$.

On munit $\mathfrak{S}_n$ de la composition des applications. Alors $(\mathfrak{S}_n,\circ)$ est un groupe fini de cardinal $n!$ appelé **groupe des permutation**.

Notation : prenons $n=5$. Soit $\sigma \in \mathfrak{S}_5$ la permutation que nous notons

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}.$$

C'est la permutation définie par $\sigma(1)=4$, $\sigma(2)=2$, $\sigma(3)=5$, $\sigma(4)=1$ et, nécessairement, $\sigma(5)=3$.

Définition

On appelle **identité** la permutation $\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$.
C'est simplement l'application identité de $\{1,\dots,n\}$. La permutation id est l'élément neutre de $(\mathfrak{S}_n,\circ)$.

On appelle **transposition** toute permutation qui échange deux éléments et laisse tous les autres invariants. Pour $i,j \in \{1,\dots,n\}$ avec $i \neq j$, on note $\tau_{i,j}$ la transposition définie par

$$\tau_{i,j}(i)=j, \tau_{i,j}(j)=i \text{ et } \forall k \neq i,j, \tau_{i,j}(k)=k.$$

Les transpositions sont, après l'identité, les permutations les plus simples. Ce sont des éléments d'ordre 2 du groupe des permutations. Elles suffisent à décrire le groupe tout entier :

Propriété

L'ensemble des transpositions de $\mathfrak{S}_n$ engendre $\mathfrak{S}_n$. Cela signifie que toute permutation peut s'écrire comme un produit de transpositions.

Démonstration : Soit $n \geq 2$ et $\sigma \in \mathfrak{S}_n$. Montrons que σ peut s'écrire comme un produit de transpositions.

Si $\sigma = Id$, on peut l'écrire $\sigma = \tau_{1,2}\tau_{1,2}$ ou simplement dire que c'est un produit de 0 transpositions. Le résultat est donc le résultat est vrai pour id.

Supposons maintenant que $\sigma \neq \text{id}$. Posons $k = \max\{j \mid \sigma(j) \neq j\}$. C'est le plus grand entier modifié par σ. Nécessairement, $k \geq 2$ et $\sigma(k) < k$. Posons alors $\tau = \tau_{\sigma(k),k}$ et $\tilde{\sigma} = \tau\sigma$. Alors $\forall j > k$, $\tilde{\sigma}(j) = \tau\sigma(j) = \tau(j) = j$. Et $\tilde{\sigma}(k) = \tau\sigma(k) = k$. Ainsi $\tilde{\sigma}$ fixe tous les entiers à partir de k. Si on pose $k' = \max\{j \mid \tilde{\sigma}(j) \neq j\}$, alors $k' < k$.

On a donc un moyen d'augmenter le nombre d'entiers fixés par une permutation. En procédant récursivement, on peut, en multipliant à chaque étape par une transposition bien choisie, arriver à fixer tous les entiers de 1 à n, *i.e.* obtenir l'identité. On montre ainsi qu'il existe des transpositions $\tau^{(1)}, \ldots, \tau^{(r)}$ telles que $\tau^{(r)} \cdots \tau^{(1)}\sigma = \text{id}$. Alors $\sigma = \tau^{(1)} \cdots \tau^{(r)}$ et peut donc s'écrire comme un produit de transpositions.

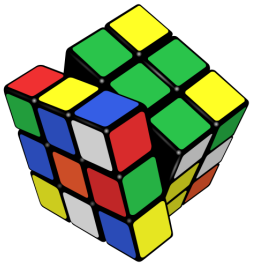
Exemple ★ Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \in \mathfrak{S}_5$. Déterminer son inverse, son ordre et le décomposer en un produit de transpositions.

L'inverse de σ est simplement sa bijection réciproque, il suffit de « lire » σ dans l'autre sens : $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$.

Pour l'ordre de σ, on calcule ses puissances jusqu'à ce qu'on obtienne l'identité : $\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, $\sigma^3 = \sigma \circ \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix}$, $\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \text{id}$. Donc σ est d'ordre 4 et engendre le sous-groupe $\{\sigma, \sigma^2, \sigma^3, \sigma^4 = \text{id}\}$. Remarquons que 4 divise bien le cardinal 120 du groupe et que σ^3 est bien l'inverse de σ. Notons enfin que l'ordre de σ exprime bien ce que fait σ : cette permutation fait « tourner » les éléments selon un cycle de longueur 4 : $1 \to 4 \to 3 \to 5 \to 1$. Il est donc logique qu'en itérant 4 fois σ, on retrouve l'identité.

Appliquons l'algorithme de la démonstration pour décomposer σ en permutations : $\tau_{15}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$, $\tau_{34}\tau_{15}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$, $\tau_{13}\tau_{34}\tau_{15}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$. Donc $\tau_{13}\tau_{34}\tau_{15}\sigma = \text{id}$ et on obtient $\sigma = \tau_{15}\tau_{34}\tau_{13}$. Ce n'est pas la seule décomposition de σ. En s'y prenant autrement, on peut obtenir par exemple $\sigma = \tau_{13}\tau_{14}\tau_{35}$.

★ Le groupe des permutations permet entre autres de modéliser et coder certains problèmes. Regardons par exemple le cas du Rubik's cube. Cet objet est formé de 27 petits cubes, dont 20 peuvent être déplacés en faisant pivoter une des faces (le cube central et les milieux des faces restent fixés). On peut ainsi décrire une configuration du cube comme une permutation des 20 petits cubes par rapport à leur position initiale. Une configuration est donc un élément de $\mathfrak{S}_{20}$. Tous les éléments de $\mathfrak{S}_{20}$ ne correspondent pas à une configuration possible du cube : par exemple, un coin du cube ne pourra jamais se retrouver au milieu d'une arête. Pour décrire l'ensemble des configurations possibles, on commence par remarquer qu'il n'y a que 6 mouvements élémentaires possibles : faire pivoter d'un quart de tour l'une des 6 faces du cube. Tous les autres déplacements sont des composées de ces déplacements simples. Chacun de ces mouvements élémentaires est décrit par une permutation d'ordre 4. Finalement, l'ensemble des configurations possibles du cube est le sous-groupe engendré par ces 6 permutations élémentaires.



L'étude algébrique de ce sous-groupe a permis de déterminer le nombre total de configurations différentes : 43 252 003 274 489 856 000 configurations ! L'étude a également permis de trouver et de coder des algorithmes de résolution du cube et même d'obtenir les théorèmes suivants : toute configuration du cube peut être ramenée à la position initiale en utilisant au plus 20 rotations de faces ! Et il existe des configurations qui ne peuvent être résolues en moins de 18 rotations. Mais ces derniers résultats sont théoriques et ne fournissent pas de méthodes explicites.

8 Autres structures algébriques

Si on ajoute une seconde loi, on peut considérer de nouvelles structures algébriques.

8.1 Anneaux

Définition

Soit E un ensemble muni de deux lois de composition internes $*$ et $\circ$. On dit que $*$ est **distributive** par rapport à $\circ$ si

$$\forall x \in E, \forall y \in E, \forall z \in E \quad x*(y\circ z) = (x*y)\circ(x*z) \text{ et } (y\circ z)*x = (y*x)\circ(z*x).$$

Définition

Soit A un ensemble muni de deux lois de composition internes $+$ et $*$. On dit que $(A, +, *)$ est un **anneau** si

- ★ $(A, +)$ est un groupe commutatif ;
- ★ la loi $*$ est associative ;
- ★ la loi $*$ est distributive par rapport à la loi $+$.

Remarques On n'impose presque rien à la loi $*$: elle peut être non commutative et ne pas avoir d'élément neutre. Si elle en a un, on le note souvent 1 et on dit que A est **unitaire**. Mais on n'exige pas que les éléments de A aient un inverse.

Exemples

- ★ $(\mathbf{Z}, +, \times)$ et $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ sont des anneaux commutatifs.
- ★ $(\mathcal{F}(\mathbf{R}, \mathbf{R}), +, \times)$ est un anneau commutatif.
- ★ Si pour $n \in \mathbf{N}^*$ on note G l'ensemble des endomorphismes du groupe $(\mathbf{R}^n, +)$, alors $(G, +, \circ)$ est un anneau non commutatif [1].

La propriété suivante, satisfaite dans $\mathbf{Z}$ ou $\mathbf{R}$, ne l'est pas dans tous les anneaux.

Définition

Soit $(A, +, \cdot)$ un anneau. On dit que c'est un anneau **intègre** si

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

1. Cet anneau est isomorphe à l'anneau $\mathcal{M}_n(\mathbf{R})$ des matrices, étudié au chapitre suivant. Cela traduit le fait que les matrices permettent de représenter les endomorphismes de $\mathbf{R}^n$.

Exemple L'anneau $(\mathbf{Z}/4\mathbf{Z}, +, \times)$ n'est pas intègre car $\bar{2} \times \bar{2} = \bar{0}$ alors que $\bar{2} \neq \bar{0}$. On a déjà vu que $\mathbf{Z}/p\mathbf{Z}$ est intègre si et seulement si p est un nombre premier (ou $p = 1$).

Théorème

Soit $(A, +, \cdot)$ un anneau intègre, soit $n \in \mathbf{N}$ et soit P un polynôme de degré n à coefficients dans A. Alors P admet au plus n racines dans A.

Démonstration : Démontrons le résultat par récurrence sur n.

Soit P un polynôme de degré $n = 0$. Donc P est un polynôme constant non nul. Donc P n'a pas de racine et le résultat est vérifié.

Soit $n \geq 1$. Supposons maintenant le résultat vrai pour les polynômes de degré $n-1$. Soit P un polynôme de degré n. Si P n'a pas de racine, le résultat est vérifié. Supposons que P a une racine a dans A. Alors, par définition, on peut factoriser P par $(X - a)$: $P = (X - a)Q$ où Q est un polynôme de degré $n - 1$. Supposons que P a une autre racine b distincte de a. Cela signifie que $(b - a)Q(b) = 0$. Comme A est intègre, on déduit que $b - a = 0$ ou $Q(b) = 0$. Or $b - a \neq 0$ donc $Q(b) = 0$. Ainsi, toute racine de P distincte de a est nécessairement racine de Q. Or par hypothèse de récurrence, Q a au plus $n - 1$ racines dans A. Donc, en ajoutant a, on déduit que P a au plus n racines dans K.

Le résultat est ainsi démontré par récurrence.

Les propriétés suivantes sont vraies dans tout anneau.

Propriété : binôme de Newton et somme géométrique

Soit $(A, +, \cdot)$ un anneau.
Soient x et y dans A tels que $xy = yx$ et soit n un entier naturel. Alors

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

Avec les mêmes hypothèses, $\quad x^n - y^n = (x - y) \sum_{k=0}^{n-1} y^k x^{n-1-k}$

$$= (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + x^2 y^{n-3} + xy^{n-2} + y^{n-1}).$$

En particulier, si l'anneau est unitaire, alors pour $x \in A$ et $n \in \mathbf{N}$

$$1 - x^{n+1} = (1 - x) \sum_{k=0}^{n} x^k = (1 - x)(1 + x + x^2 + \cdots + x^{n-1} + x^n).$$

8.2 Corps

Définition

Soit K un ensemble muni de deux lois de composition internes $+$ et $\cdot$.
On dit que $(K, +, \cdot)$ est un **corps** si $(K, +, \cdot)$ est un anneau unitaire commutatif et si tout élément de $K \setminus \{0_K\}$ admet un inverse pour la loi $\cdot$.

Remarques Autrement dit, $(K, +, \cdot)$ est un corps si $(K, +, \cdot)$ est un anneau et si $(K^*, \cdot)$ est un groupe commutatif.

On peut montrer qu'un corps est en particulier un anneau intègre.

Le corps est une structure dans laquelle beaucoup de raisonnements classiques restent valables. Il est indispensable pour définir les notions d'espaces vectoriels et de matrices.

Exemples ★ $(\mathbf{Q}, +, \times), (\mathbf{R}, +, \times)$, et $(\mathbf{C}, +, \times)$ sont des corps.
★ Si p est un nombre premier, $(\mathbf{Z}/p\mathbf{Z}, +, \times)$ est un corps.

8.3 Espaces vectoriels

L'espace vectoriel est la structure la plus importante à connaître, elle sera étudiée au second semestre.

Définition

Soit E un ensemble et $\mathbf{K}$ un corps. On munit E d'une loi interne $+$ et d'une loi externe : $\cdot : \mathbf{K} \times E \to E$. On dit que E est un **$\mathbf{K}$-espace vectoriel** si

★ $(E, +)$ est un groupe commutatif,

★ Pour tous λ et μ dans $\mathbf{K}$, pour tous x et y dans E :

$$\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y, \qquad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x.$$

$$(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x), \qquad 1_{\mathbf{K}} \cdot x = x.$$

Exemples ★ L'ensemble $\mathbf{R}^3$ des vecteurs de l'espace muni de l'addition des vecteurs et de la multiplication par un scalaire réel est un $\mathbf{R}$-espace vectoriel.

Cela signifie que l'on sait additionner des vecteurs, les multiplier par un nombre réel et que toutes ces opérations ont des propriétés algébriques satisfaisantes.

★ L'ensemble $\mathcal{F}(\mathbf{R}, \mathbf{R})$ des fonctions réelles est également un $\mathbf{R}$-espace vectoriel pour les lois usuelles.

De manière analogue à ce que nous avons vu avec les groupes, nous définirons les notions de sous-espace vectoriel, de sous-espace engendré et de morphisme d'espace vectoriel (également appelé application linéaire).

À retenir

★ Maîtriser les notions de groupe, sous-groupe et morphisme.

★ Savoir déterminer l'ordre d'un élément et le sous-groupe qu'il engendre.

★ Savoir raisonner algébriquement dans $\mathbf{Z}/n\mathbf{Z}$ et dans $\mathfrak{S}_n$.

★ Connaître les définitions des anneaux et des corps.

VI. L'anneau des matrices

Introduction. On s'intéresse à une population exposée à un virus extérieur (un virus transmis par des insectes par exemple). Le but de notre étude est de répondre à ces questions : la population est-elle menacée d'extinction ? Ou au contraire, le virus disparaîtra-t-il ? Ou encore, la population continuera-t-elle à se développer tout en ayant toujours une certaine proportion d'individus malades ?

Les hypothèses concernant le virus sont les suivantes.

★ Il n'est pas contagieux entre individus.
★ Il ne se transmet pas aux descendants.
★ Les individus malades ne peuvent pas se reproduire.
★ Après avoir été infecté, un individu peut résister au virus et redevenir sain, mais s'il contracte finalement la maladie, il ne pourra plus guérir.

Les données annuelles sont les suivantes.

★ $\nu = \frac{1}{9}$ est le taux de natalité chez les individus qui ne sont pas malades.
★ $\tau = \frac{1}{3}$ est la probabilité d'être infecté.
★ $\gamma_S = \frac{1}{3}$ est la probabilité qu'une personne infectée redevienne saine.
★ $\gamma_M = \frac{1}{3}$ est la probabilité qu'une personne infectée contracte la maladie.
★ $\mu = \frac{2}{3}$ est le taux de mortalité chez les personnes malades.

Initialement, il y avait 1600 personnes dans la population et toutes étaient saines.

Nous noterons S_n, I_n et M_n le nombre de personnes saines, infectées et malades à l'année n. D'après les données ci-dessus, on peut décrire l'évolution de la population par le système suivant.

$$\left\{\begin{array}{rcll} S_{n+1} & = & S_n + \nu(S_n + I_n) + \gamma_S I_n - \tau S_n & = \frac{7}{9}S_n + \frac{4}{9}I_n + 0M_n \\ I_{n+1} & = & I_n - \gamma_S I_n - \gamma_M I_n + \tau S_n & = \frac{1}{3}S_n + \frac{1}{3}I_n + 0M_n \\ M_{n+1} & = & (1-\mu)M_n + \gamma_M I_n & = 0S_n + \frac{1}{3}I_n + \frac{1}{3}M_n \end{array}\right.$$

Nous verrons que toutes les données du problème sont contenues dans la **matrice** $\begin{bmatrix} \frac{7}{9} & \frac{4}{9} & 0 \\ \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$. Nous répondrons dans ce chapitre aux questions posées plus haut en nous intéressant aux propriétés de cette matrice.

Les matrices sont devenues un objet mathématique aussi basique que peuvent l'être les nombres ou les fonctions. Elles interviennent en mathématique dans des domaines aussi divers que les équations différentielles, les probabilités ou la géométrie.

C'est un des rares outils mathématique que l'on maîtrise très bien. Pour cette raison, dès qu'on le peut, on modélise un problème à l'aide de matrices. C'est ainsi qu'elles interviennent de manière fondamentale en mécanique, en mécanique quantique, en biologie dans les problèmes d'évolution de populations, en informatique dans tous les problèmes de graphes, etc.

1 Généralités

On considère un ensemble $\mathbf{A}$ muni d'une addition et d'une multiplication avec de bonnes propriétés (associativité, commutativité, distributivité). Nous ne travaillerons essentiellement qu'avec les corps $\mathbf{R}$ ou $\mathbf{C}$, mais cet ensemble $\mathbf{A}$ peut très bien être $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$, un anneau de polynômes ou un anneau de fonctions.

Soient n et p des entiers strictement positifs.

Définition

Une **matrice** M à coefficients dans $\mathbf{A}$ et à n lignes et p colonnes est un élément de $\mathbf{A}^{np}$ que l'on représente sous la forme d'un tableau :

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1p} \\ m_{21} & m_{22} & \cdots & m_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{np} \end{bmatrix}.$$

On note également $M = (m_{ij})_{i \leqslant n, j \leqslant p}$.

On note $\mathcal{M}_{n,p}(\mathbf{A})$ l'ensemble des matrices à coefficients dans $\mathbf{A}$ à n lignes et p colonnes.

Définition

- ★ On appelle **matrice nulle** de $\mathcal{M}_{n,p}(\mathbf{A})$ la matrice dont tous les coefficients sont nuls.
- ★ Si $n = p$, on dit que M est une **matrice carrée**. L'ensemble des matrices carrées de taille n est noté $\mathcal{M}_n(\mathbf{A})$ (ou encore $\mathcal{M}(n, \mathbf{A})$).
- ★ Si $p = 1$, la matrice M n'a qu'une colonne. On parle alors de **vecteur colonne**. De même, si $n = 1$, on parle de **vecteur ligne**.

Les vecteurs colonnes et les vecteurs lignes de taille n sont naturellement associés à des éléments de $\mathbf{A}^n$.

Définition : addition des matrices

Soient $M = (a_{ij})_{i \leqslant n, j \leqslant p} \in \mathcal{M}_{n,p}(\mathbf{A})$ et $N = (b_{ij})_{i \leqslant n, j \leqslant p} \in \mathcal{M}_{n,p}(\mathbf{A})$.
On définit la **somme** de ces deux matrices par

$$M + N = (a_{ij} + b_{ij})_{i \leqslant n, j \leqslant p} \in M_{n,p}(A).$$

Définition : multiplication des matrices

Soient $A = (a_{ij})_{i\leqslant n, j\leqslant p} \in \mathcal{M}_{n,p}(\mathbf{A})$ et $B = (b_{ij})_{i\leqslant p, j\leqslant q} \in \mathcal{M}_{p,q}(\mathbf{A})$.
On définit le **produit** de ces deux matrices par

$$AB = (c_{ij})_{i\leqslant n, j\leqslant q} \in \mathcal{M}_{n,q}(\mathbf{A}),$$

avec pour tous i et j

$$c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}.$$

Définition : multiplication scalaire

Soit $M = (m_{ij})_{i\leqslant n, j\leqslant p} \in \mathcal{M}_{n,p}(\mathbf{A})$ et $a \in \mathbf{A}$. On définit pour M la **multiplication par le scalaire** a par

$$aM = (am_{ij})_{i\leqslant n, j\leqslant p} \in \mathcal{M}_{n,p}(A).$$

Exemple $\begin{bmatrix} 2 & 1 \\ -5 & 3 \\ 6 & 4 \end{bmatrix} + \begin{bmatrix} 0 & -4 \\ 7 & 9 \\ 8 & 9 \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ 2 & 12 \\ 14 & 13 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & -1 \end{bmatrix} \cdot \begin{bmatrix} 4 & 1 \\ 2 & 2 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 8 & 13 \\ 5 & 1 \end{bmatrix}$, $7 \begin{bmatrix} 2 \\ -5 \\ 6 \end{bmatrix} = \begin{bmatrix} 14 \\ -35 \\ 42 \end{bmatrix}$.

Propriété

- ★ L'addition des matrices est associative et commutative.
- ★ Le couple $(\mathcal{M}_{n,p}(\mathbf{A}), +)$ est un groupe. Muni en plus de la multiplication scalaire, c'est un $\mathbf{A}$-espace-vectoriel si $\mathbf{A}$ est un corps.
- ★ La multiplication des matrices est associative mais **non commutative**.
- ★ La multiplication est distributive par rapport à l'addition.
- ★ la multiplication n'est **pas intègre** : si $AB = 0$, on ne peut pas déduire en général que $A = 0$ ou $B = 0$.

Remarques

- ★ Le produit de deux matrices carrées de taille n est une matrice carrée de taille n. Pour une matrice carrée M et un entier k dans $\mathbf{N}^*$, on notera M^k le produit $M \cdots M$ où M apparaît k fois dans le produit.
- ★ Pour $\mathbf{A} = \mathbf{R}$, le produit d'un vecteur ligne de taille n par un vecteur colonne de taille n est simplement le produit scalaire usuel de ces deux vecteurs de $\mathbf{R}^n$.
- ★ Le produit d'une matrice carrée de taille n par un vecteur colonne de taille n est un vecteur colonne de taille n.

Définition

Soit $M = (m_{i,j})_{i\leq n, j\leq p} \in \mathcal{M}_{n,p}(\mathbf{A})$. On appelle **transposée** de M la matrice notée ${}^tM$ appartenant à $\mathcal{M}_{p,n}(\mathbf{A})$ et définie par

$$ {}^tM = (\ell_{i,j})_{i\leq p, j\leq n} \quad \text{avec} \quad \forall i,j,\ \ell_{i,j} = m_{j,i}. $$

Propriété

Soient A, B et C des matrices telles que $A+B$ et AC soient bien définies et soit $a \in \mathbf{A}$. Alors

- ★ ${}^t({}^tA) = A$
- ★ ${}^t(A+B) = {}^tA + {}^tB$
- ★ ${}^t(AC) = {}^tC\,{}^tA$
- ★ ${}^t(aA) = a\,{}^tA$

Exemples Soit $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$ et $X = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$.

Alors $AX = \begin{bmatrix} 8 \\ 17 \\ 26 \end{bmatrix}$, ${}^tX = \begin{bmatrix} 0 & 1 & 2 \end{bmatrix}$, ${}^tA = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$, ${}^tX\,{}^tA = \begin{bmatrix} 8 & 17 & 26 \end{bmatrix} = {}^t(AX)$.

2 L'anneau des matrices

Soit $n \in \mathbf{N}^*$. On note $\mathcal{M}_n(\mathbf{A})$ l'ensemble $\mathcal{M}_{n,n}(\mathbf{A})$ des matrices carrées de taille n à coefficients dans $\mathbf{A}$. La loi $\times$ est interne à $\mathcal{M}_n(\mathbf{A})$. Muni de cette loi associative et distributive, et si $\mathbf{A}$ est un corps, le groupe $(\mathcal{M}_n(\mathbf{A}), +)$ devient un **anneau** $(\mathcal{M}_n(\mathbf{A}), +, \times)$.

Définition

La **matrice identité** de taille n est la matrice $I_n = (e_{i,j}) \in \mathcal{M}_n(\mathbf{A})$ définie par

$$ \forall i \leqslant n,\ \ e_{i,i} = 1 \quad \text{et} \quad \forall j \neq i,\ \ e_{i,j} = 0 \quad : \qquad I_n = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}. $$

Propriété

- ★ La matrice nulle est **l'élément absorbant** de l'anneau :
  $\forall A \in \mathcal{M}_n(\mathbf{A}),\ A \times 0 = 0 \times A = 0$.
- ★ La matrice identité en est **l'élément unité** :
  $\forall A \in \mathcal{M}_n(\mathbf{A}),\ A \times I_n = I_n \times A = A$.

Parmi les matrices carrées, citons un certain nombres de matrices particulières.

Définition

Soit $M = (m_{ij}) \in \mathcal{M}_n(\mathbf{A})$.
C'est une **matrice diagonale** si $\forall i \neq j, \quad m_{ij} = 0$.
C'est une **matrice triangulaire supérieure** si $\forall i > j, \quad m_{ij} = 0$.
C'est une **matrice triangulaire inférieure** si $\forall i < j, \quad m_{ij} = 0$.
C'est une **matrice symétrique** si $M = {}^tM$.
C'est une **matrice antisymétrique** si $M = -{}^tM$.

Remarques Les ensembles de matrices diagonales, triangulaires supérieures et triangulaires inférieures sont des sous-anneaux de $\mathcal{M}_n(\mathbf{A})$: ils sont stables par addition, opposé et multiplication.

Exemple $\begin{bmatrix} 3 & 0 & 0 \\ 1 & 2 & 0 \\ 2 & 4 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 & 0 & 0 \\ 3 & 4 & 0 \\ 9 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 21 & 0 & 0 \\ 13 & 8 & 0 \\ 71 & 16 & 5 \end{bmatrix}$, mais $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 9 & 0 \\ 3 & 0 & 5 \end{bmatrix} \cdot \begin{bmatrix} 7 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 0 \end{bmatrix} = \begin{bmatrix} 12 & 14 & 7 \\ 23 & 20 & 29 \\ 26 & 18 & 3 \end{bmatrix}$.

3 Le groupe des matrices inversibles

3.1 Définitions

Définition

Soit $M \in \mathcal{M}_n(\mathbf{A})$. On dit que M est **inversible** s'il existe $N \in \mathcal{M}_n(\mathbf{A})$ telle que $MN = NM = I_n$.

On note $\mathrm{GL}_n(\mathbf{A})$ (ou $\mathrm{GL}(n, \mathbf{A})$) l'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbf{A})$.

Propriété

$(\mathrm{GL}_n(\mathbf{A}), \times)$ est un groupe appelé **groupe linéaire**.

Propriété

Soit $\mathbf{A}$ un corps, soient A et B dans $\mathrm{GL}_n(\mathbf{A})$ et soit $a \neq 0$. Alors

- ★ $AB \in \mathrm{GL}_n(\mathbf{A})$ et $(AB)^{-1} = B^{-1}A^{-1}$;
- ★ ${}^tA$ est inversible et $({}^tA)^{-1} = {}^t(A^{-1})$;
- ★ $(A^{-1})^{-1} = A$;
- ★ aA est inversible et $(aA)^{-1} = \frac{1}{a}A^{-1}$.

Propriété

Soit $A \in \mathcal{M}_n(\mathbf{A})$.
Alors A est inversible si et seulement si $\forall Y \in \mathbf{A}^n, \exists! X \in \mathbf{A}^n, \quad AX = Y$.

Nous verrons que cette proposition signifie que tout système linéaire défini par une matrice carrée inversible admet une unique solution.

Propriété

Soient A et B dans $\mathcal{M}_n(\mathbf{A})$ telles que $A \neq 0$, $B \neq 0$ et $AB = 0$. Alors A et B sont non inversibles.

Exemple Soit A une matrice telle que $A^2 = I_n$. Alors, par définition, A est inversible et $A^{-1} = A$. D'autre part, $A^2 - I_n = 0$, donc $(A - I_n)(A + I_n) = 0$ (cette factorisation est possible car A et I_n commutent). D'après la propriété précédente, si $A \neq \pm I_n$, on peut en déduire que $A - I_n$ et $A + I_n$ ne sont pas des matrices inversibles. Tout cela est par exemple vérifié par $A = \begin{bmatrix} 2 & 1 \\ -3 & -2 \end{bmatrix}$.

Propriété

Soit $A \in \mathcal{M}_n(\mathbf{A})$.
Supposons que A admet un inverse à droite, c'est-à-dire qu'il existe B dans $\mathcal{M}_n(A)$ tel que $AB = I_n$. Alors A est inversible et $A^{-1} = B$.

De même, si A admet un inverse à gauche C, *i.e.* $CA = I_n$, alors A est inversible et $A^{-1} = C$.

Voici une propriété permettant de simplifier les calculs de puissance matricielle.

Propriété

Soient A, D et P des matrices telles que P est inversible et $A = PDP^{-1}$. Alors, pour tout entier n, $A^n = PD^nP^{-1}$.

Exemple Soient $A = \begin{bmatrix} -7 & 10 \\ -5 & 8 \end{bmatrix}$ et $P = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$. Alors P est inversible d'inverse $P^{-1} = \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix}$ et $P^{-1}AP = \begin{bmatrix} 3 & 0 \\ 0 & -2 \end{bmatrix}$. On obtient une matrice diagonale dont les puissances sont triviales à calculer. On dit qu'on a **diagonalisé** A. En multipliant par P à droite et par P^{-1} à gauche, on obtient $A = PDP^{-1}$ et ainsi :

$$A^n = PD^nP^{-1} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3^n & 0 \\ 0 & (-2)^n \end{bmatrix} \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -(-2)^{n+1} - 3^n & (-2)^{n+1} + 2 \cdot 3^n \\ (-2)^n - 3^n & -(-2)^n + 2 \cdot 3^n \end{bmatrix}.$$

La matrice P n'a pas été choisie au hasard. C'est elle qui permet de transformer A en une matrice diagonale. On peut interpréter l'opération $A \to P^{-1}AP$ comme un changement de repère permettant d'observer A de manière plus simple. En particulier ici, il est bien plus simple de calculer ses puissances dans ce nouveau repère. Toutes ces considérations (et notamment la façon de trouver la matrice P) seront étudiées dans le cours d'algèbre linéaire.

3.2 Inversion d'une matrice

Nous présentons ici la méthode la plus classique pour inverser une matrice. Elle consiste à effectuer une série d'opérations sur les lignes [2] de la matrice considérée jusqu'à ce qu'on obtienne la matrice identité. Si on effectue en parallèle les mêmes opérations en partant de la matrice identité, alors la matrice obtenue à la fin est l'inverse de la matrice considérée.

Les opérations autorisées sont les suivantes :

Multiplication par un scalaire : $L_i \leftarrow \lambda L_i$, avec $\lambda \in A^\times$;

Combinaison linéaire de lignes : $L_i \leftarrow L_i + \mu L_j$, avec $\mu \in A$ et $j \neq i$;

Échange de lignes : $L_i \leftrightarrow L_j$;

Présentons la méthode sur un exemple. Afin de transformer la matrice de départ en la matrice identité, nous allons faire apparaître successivement des zéros pour la transformer en une matrice triangulaire supérieure, puis diagonale. Enfin, en multipliant les lignes par des scalaires, nous obtiendrons la matrice identité.

Inversons la matrice $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 3 \\ 2 & 1 & -1 \end{bmatrix}$:

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ \underline{1} & 1 & 3 & 0 & 1 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 \end{array}\right] \quad L_2 \leftarrow L_2 - L_1$$

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & -1 & 1 & 0 \\ \underline{2} & 1 & -1 & 0 & 0 & 1 \end{array}\right] \quad L_3 \leftarrow L_3 - 2L_1$$

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & -1 & 1 & 0 \\ 0 & \underline{-1} & -1 & -2 & 0 & 1 \end{array}\right] \quad L_2 \leftrightarrow L_3$$

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & \underline{-1} & -2 & 0 & 1 \\ 0 & 0 & 3 & -1 & 1 & 0 \end{array}\right] \quad L_2 \leftarrow L_2 + L_3/3$$

$$\left[\begin{array}{ccc|ccc} 1 & \underline{1} & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & -\frac{7}{3} & \frac{1}{3} & 1 \\ 0 & 0 & 3 & -1 & 1 & 0 \end{array}\right] \quad L_1 \leftarrow L_1 + L_2$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{4}{3} & \frac{1}{3} & 1 \\ 0 & \underline{-1} & 0 & -\frac{7}{3} & \frac{1}{3} & 1 \\ 0 & 0 & \underline{3} & -1 & 1 & 0 \end{array}\right] \quad \begin{array}{l} L_2 \leftarrow -L_2 \\ L_3 \leftarrow L_3/3 \end{array}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{4}{3} & \frac{1}{3} & 1 \\ 0 & 1 & 0 & \frac{7}{3} & -\frac{1}{3} & -1 \\ 0 & 0 & 1 & -\frac{1}{3} & \frac{1}{3} & 0 \end{array}\right]$$

Ainsi, l'inverse de la matrice $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 3 \\ 2 & 1 & -1 \end{bmatrix}$ est la matrice $A^{-1} = \begin{bmatrix} -\frac{4}{3} & \frac{1}{3} & 1 \\ \frac{7}{3} & -\frac{1}{3} & -1 \\ -\frac{1}{3} & \frac{1}{3} & 0 \end{bmatrix}$.

Bien sûr, il n'est pas certain que la matrice considérée soit inversible. La méthode permet également de répondre à ce problème. Si on arrive à obtenir la matrice identité après différentes opérations, cela prouve que la matrice est inversible et on a obtenu son inverse. Si au cours de la méthode, on a réussi à faire apparaître **une ligne de zéros**, cela prouve que la matrice n'est pas inversible et il est inutile de continuer les calculs.

2. Comme l'inverse d'une matrice M est égale à la transposée de l'inverse de ${}^tM$, il est possible de raisonner sur ${}^tM$. Or toute opération sur les lignes de ${}^tM$ revient à faire l'opération correspondante sur les colonnes de M. Il est donc possible d'inverser M en agissant exclusivement sur les colonnes de M.

4 Quelques applications

4.1 Systèmes linéaires

Un système linéaire est un système d'équations de la forme

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & y_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & y_2 \\ \vdots & & \vdots & & & & \vdots & \vdots & \vdots \\ a_{p1}x_1 & + & a_{p2}x_2 & + & \cdots & + & a_{pn}x_n & = & y_p \end{cases}$$

On dit que ce système est à p équations et n inconnues. On peut l'écrire matriciellement sous la forme

$$AX = Y,$$

avec $A = (a_{ij})_{i,j} \in \mathcal{M}_{p,n}(\mathbf{R})$, $X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ et $Y = \begin{bmatrix} y_1 \\ \vdots \\ y_p \end{bmatrix}$.

S'il y a autant d'équations que d'inconnues, *i.e.* $n = p$, alors la matrice A est une matrice carrée. Si celle-ci est inversible, alors le système possède une unique solution donnée par

$$X = A^{-1}Y.$$

Ainsi, résoudre un système revient à inverser une matrice. Si la matrice A n'est pas inversible, alors le système aura une infinité de solutions ou aucune. En raisonnant sur la matrice A il est possible de préciser tout cela. Lorsque le système n'est pas donné par une matrice carrée, il existe des moyens de se ramener à une matrice carrée.

Exemple Fixons a, b et c et résolvons le système linéaire $\begin{cases} x & + & y & + & z & = & a \\ x & + & 2y & + & 3z & = & b \\ x & - & y & - & 2z & = & c \end{cases}$ en utilisant la méthode du pivot de Gauss :

$$\begin{cases} x & +y & +z & = & a \\ x & +2y & +3z & = & b \\ x & -y & -2z & = & c \end{cases} \quad \begin{matrix} L_2 \leftarrow L_2 - L_1 \\ L_3 \leftarrow L_1 - L_3 \end{matrix} \quad \begin{cases} x & +y & & = & 4a & -2b & -c \\ & y & & = & 5a & -3b & -2c \\ & & -z & = & 3a & -2b & -c \end{cases} \quad L_1 \leftarrow L_1 - L_2$$

$$\begin{cases} x & +y & +z & = & a \\ & y & +2z & = & -a & +b \\ & 2y & +3z & = & a & & -c \end{cases} \quad L_3 \leftarrow L_3 - 2L_2 \quad \begin{cases} x & & & = & -a & +b & +c \\ & y & & = & 5a & -3b & -2c \\ & & -z & = & 3a & -2b & -c \end{cases} \quad L_3 \leftarrow -L_3$$

$$\begin{cases} x & +y & +z & = & a \\ & y & +2z & = & -a & +b \\ & & -z & = & 3a & -2b & -c \end{cases} \quad \begin{matrix} L_1 \leftarrow L_1 + L_3 \\ L_2 \leftarrow L_2 + 2L_3 \end{matrix} \quad \begin{cases} x & & & = & -a & +b & +c \\ & y & & = & 5a & -3b & -2c \\ & & z & = & -3a & +2b & +c \end{cases}$$

Matriciellement, le système s'écrit $A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$ avec $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & -1 & -2 \end{bmatrix}$. Nos calculs ci-dessus reviennent en fait à inverser la matrice A et nous avons obtenu $A^{-1} = \begin{bmatrix} -1 & 1 & 1 \\ 5 & -3 & -2 \\ -3 & 2 & 1 \end{bmatrix}$. La solution est bien $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = A^{-1} \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. L'intérêt ici de la notation matricielle est qu'elle est plus synthétique que l'écriture explicite des équations du système. Cela est particulièrement pertinent pour la résolution informatique des systèmes linéaires.

4.2 Applications linéaires

Une **application linéaire** de $\mathbf{R}^n$ vers $\mathbf{R}^p$ est un morphisme de groupe pour l'addition. C'est une application de la forme

$$\varphi(x_1, \ldots, x_n) = (a_{11}x_1 + \cdots + a_{1n}x_n, \quad \ldots \quad , a_{p1}x_1 + \cdots + a_{pn}x_n).$$

On peut représenter une telle application à l'aide de matrices, sous la forme

$$\varphi(X) = AX,$$

où $A = (a_{i,j})_{i,j} \in \mathcal{M}_{p,n}(\mathbf{R})$ et $X \in \mathcal{M}_{n,1}(\mathbf{R})$.

De telles applications jouent un rôle fondamental en mathématiques et seront étudiées en détail plus tard. L'intérêt principal de l'écriture matricielle est que la composition d'applications linéaires est donnée par un produit matriciel : si φ et ψ sont données par les matrices M et N, alors $\psi \circ \varphi$ est une application linéaire de matrice NM.

Exemple Dans le plan $\mathbf{R}^2$, la rotation de centre O et d'angle θ est définie en coordonnées cartésiennes par $r_\theta(x, y) = (\cos(\theta)x - \sin(\theta)y \ , \ \sin(\theta)x + \cos(\theta)y)$. Il s'agit ainsi d'une application linéaire qu'on peut représenter à l'aide de la matrice

$$R_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

On peut alors vérifier que $R_\theta R_{\theta'} = R_{\theta+\theta'}$ et $R_\theta^{-1} = R_{-\theta}$.

4.3 Matrice d'adjacence

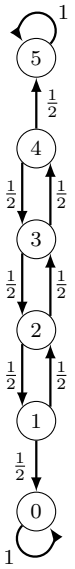
Un graphe est un ensemble de sommets reliés entre eux par des arêtes. Ces dernières peuvent être orientées. Notons $s_1, \ldots, s_n$ les sommets du graphe et a_{ij} l'arête éventuelle allant du sommet s_i vers le sommet s_j. Notons A l'ensemble des arêtes du graphe. On appelle **matrice d'adjacence** du graphe la matrice $M = (m_{ij})_{i,j} \in \mathcal{M}_n$ définie par $m_{ij} = 1$ si $a_{ij} \in A$ et $m_{ij} = 0$ sinon.

Cette matrice décrit entièrement le graphe considéré. Elle possède, entre autre, la propriété suivante : si $k \in \mathbf{N}^*$, et si on note $M^k = (m_{ij}^{(k)})_{i,j}$, alors $m_{ij}^{(k)}$ est égal au nombre de chemins reliant le sommet s_i au sommet s_j via k arêtes.

Il est possible d'attribuer aux arêtes des poids, voire des probabilités. La matrice d'adjacence peut alors être améliorée en la matrice constituée par ces poids ou probabilités. Là encore, les puissance de cette matrice donnent un certain nombre de propriétés du graphe.

Exemple Deux joueurs jouent à pile ou face. Le premier possède 2 euros et le second 3 euros. À chaque manche, le perdant paye un euro au gagnant. Le jeu s'arrête lorsqu'un des joueurs est ruiné.

Le problème peut être modélisé par le graphe ci-contre, chaque sommet correspondant à la fortune du premier joueur et les arêtes aux probabilités de passer d'un état à un autre après une manche. La matrice du graphe, appelée matrice de transition, est



$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Alors M^{15} est la matrice de transition du graphe en 15 étapes. Elle permet de décrire les probabilités de se retrouver dans chaque état après 15 étapes. Numériquement on obtient

$$M^{15} \approx \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0,79 & 0 & 0,02 & 0 & 0,01 & 0,18 \\ 0,57 & 0,02 & 0 & 0,03 & 0 & 0,38 \\ 0,38 & 0 & 0,03 & 0 & 0,02 & 0,57 \\ 0,18 & 0,01 & 0 & 0,02 & 0 & 0,79 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Cela nous permet de conclure que, partant avec 2 euros, le premier joueur a, après 15 manches, 57% de chances d'être ruiné et 38% de chances de gagner la partie.

À retenir

- ★ Savoir additionner et multiplier des matrices.
- ★ Savoir déterminer si une matrice est inversible et calculer son inverse.
- ★ Connaître les définitions des matrices transposées, diagonales, triangulaires, symétriques et antisymétriques.
- ★ Savoir raisonner algébriquement dans l'anneau des matrices.
- ★ Comprendre l'importance des matrices diagonales et l'intérêt de la diagonalisation ($A = P^{-1}DP$).
- ★ Savoir traduire matriciellement des systèmes linéaires ou des applications linéaires.