Algèbre générale

Jean-Romain Heu

2017

Introduction

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

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

jeanromain.heu.free.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.
- Maîtriser des concepts abstraits.
- Maîtriser un certain nombre d'outils mathématiques indispensables.

Afin d'atteindre ces objectifs, il est absolument nécessaire d'apprendre son cours et de préparer ses exercices avant d'aller en travaux dirigés.

Le programme de ce cours est le suivant.

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

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

Chapitre 1

Logique, langage mathématique et raisonnement

1.1 Éléments de logique

Définition 1.1.1. *Une proposition logique est un énoncé mathématique auquel on peut attribuer une valeur de vérité, soit « vrai » soit « faux ».*

Exemple 1.1.1. *« $2 < 3$ », « 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.*

1.1.1 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. Sa table de vérité est

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. Sa table de vérité est

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 $P \implies Q$ et on la lit « P implique Q ». Sa table de vérité est

P	Q	$P \implies Q$
V	V	V
V	F	F
F	V	V
F	F	V

On appelle **réciproque** de l'implication $P \implies Q$, la proposition $Q \implies P$.

Proposition 1.1.1. *Soient P, Q et R des propositions logiques.*
Alors la proposition $[(P \implies Q) \wedge (Q \implies R)] \implies [P \implies R]$ *est une* **tautologie**, i.e. *une proposition de valeur de vérité toujours vraie.*

Autrement dit, si $P \implies Q$ *et* $Q \implies R$ *sont vraies, alors* $P \implies R$ *est vraie.*
On dit que l'implication est **transitive**.

L'équivalence

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

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

Avec ces connecteurs logiques, on peut construire d'autres propositions logiques. Soient par exemple deux propositions P et Q. Posons R la proposition

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

Il est alors possible de déterminer la table de vérité de R, voire de simplifier l'expression de R.

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.

Proposition 1.1.2. *Soient* P *et* Q *deux propositions logiques.*

- $\neg(\neg P) \cong P$
- $(P \implies Q) \cong (\neg Q \implies \neg P)$.
  On dit que $\neg Q \implies \neg P$ *est la* **contraposée** *de* $P \implies Q$.
- *Lois de Morgan :*
  $\neg(P \text{ ou } Q) \cong (\neg P \text{ et } \neg Q)$
  $\neg(P \text{ et } Q) \cong (\neg P \text{ ou } \neg Q)$.

1.1.2 Quantificateurs

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

Exemple 1.1.2. *« 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.

Remarque 1.1.1. *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 $\exists (x, y) \in \mathbf{Z} \times \mathbf{R},\ x + y^2 = 0$.

Proposition 1.1.3. *Soit $P(x)$ un prédicat dépendant d'une variable x. Alors*

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

1.2 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.

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.

On peut ensuite démontrer des théorèmes. Quelques exemples :

Théorème 1.2.1. $\mathbf{N}$ *est infini.*

Théorème 1.2.2. $\mathbf{N}$ *est archimédien :* $\forall A \in \mathbf{N}, \forall a \in \mathbf{N}^*, \exists n \in \mathbf{N}, \quad an > A.$

Théorème 1.2.3. *Toute partie non vide de* $\mathbf{N}$ *contient un plus petit élément :*

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

1.3 Raisonnements

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

1.3.1 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. »

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.

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

La démonstration se divise en deux parties : existence et unicité. 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.

Proposition du type $P \implies Q$

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

Proposition du type $P \Leftrightarrow Q$

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

1.3.2 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 $P \implies Q$, on peut très bien démontrer sa contraposée $\neg Q \implies \neg P$ qui lui est équivalente. On suppose donc $\neg Q$ et on montre $\neg P$. On peut alors conclure que $P \implies Q$ est vrai.

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.

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.

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 $\forall n \in \mathbf{N}, P(n) \implies P(n+1)$. 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.

Chapitre 2

Arithmétique

L'un des objectifs de ce chapitre est d'illustrer les différents types de raisonnements vus dans le premier chapitre.

2.1 Divisibilité

Définition 2.1.1. *Soient d et n des entiers naturels. On dit que d* **divise** *n et on note $d|n$ si $\exists k \in \mathbf{N},\ n = dk$.*
On dit aussi que d est un **diviseur** *de n et que n est un* **multiple** *de d.*

Définition 2.1.2. *On appelle* **nombre premier** *tout nombre entier naturel ayant exactement deux diviseurs : 1 et lui-même.*
On notera $\mathcal{P}$ leur ensemble.

Attention, 1 n'est pas premier !

Théorème 2.1.1. *Soient a et b des entiers naturels avec $b \neq 0$. Il existe un unique couple d'entiers $(n, r) \in \mathbf{N} \times \mathbf{N}$ tel que $a = nb + r$ et $0 \leqslant r < b$.*
Cette égalité est appelée **division euclidienne** *de a par b ; n est le quotient de la division et r en est le reste.*

Démonstration :
Soient a et b dans $\mathbf{N}$ tels que $b \neq 0$.
Existence : montrons l'existence de deux entiers n et r tels que $a = nb + r$ et $0 \leqslant r < b$.
• Soit $A = \{m \in \mathbf{N} \mid mb > a\}$.
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 que A est non vide.
• Comme A est une partie non vide de $\mathbf{N}$, il admet un minimum que nous notons n_A. Ainsi $n_A \in A$ et $n_A - 1 \notin A$. Posons $n = n_A - 1$ (n est positif car n_A ne peut pas être nul). Et posons ensuite $r = a - nb$.
• Il reste à montrer $0 \leqslant r < b$. Comme n_A est dans A, $a < n_A b$ et comme $n_A - 1$ n'y est pas, $(n_A - 1)b \leqslant a$.

Autrement dit, $nb \leqslant a < (n+1)b$. Ainsi $0 \leqslant a - nb < b$, 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) obtenu est unique.
• Soient n, r, m et s des entiers tels que $a = nb + r = mb + s$ avec $0 \leqslant r < b$ et $0 \leqslant s < b$. Montrons que $n = m$ et $r = s$.
• On a $b(m-n) = r-s$. Donc $r-s$ est un multiple de b. Or $-b < -s \leqslant 0$ et $0 \leq r < b$. Donc $-b < r-s < b$. Ainsi $r - s$ est un multiple de b strictement compris entre $-b$ et b. Nécessairement $r - s = 0$. Donc $r = s$. Finalement $a = nb = mb$, donc $n = m$ car $b \neq 0$.
• Ainsi $n = m$ et $r = s$ ce qui démontre l'unicité du couple (n, r).

Définition 2.1.3. *On dit que deux entiers naturels a et b sont premiers entre eux s'ils n'ont aucun diviseur commun hormis 1 :*

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

Théorème 2.1.2. de Bézout.
Soient a et b deux entiers naturels premiers entre eux. Alors il existe des entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration :
• Soient a et b des entiers naturels premiers entre eux.
• Soit $A = \{au + bv \mid u \in \mathbf{Z}, v \in \mathbf{Z}\}$. Montrer que l'on peut trouver u et v tels que $au + bv = 1$ revient à montrer que $1 \in A$.
• Soit $A' = A \cap \mathbf{N}^*$ l'ensemble des entiers strictement positifs appartenant à A.
Comme $a \times 1 + b \times 0 = a \in A'$, on déduit que A' est non vide.
• Étant une partie non vide de $\mathbf{N}$, A' possède un minimum que nous notons c. Nous allons montrer que $c = 1$. Pour cela, nous allons montrer que c divise à la fois a et b.
• Comme c est dans A, il existe des entiers relatifs u et v tels que $c = au + bv$.
• Effectuons la division euclidienne de a par c (possible car $c \neq 0$) : il existe des entiers n et d tels que $a = nc + d$ avec $0 \leqslant d < c$. Alors $a - d = nc = n(au + bv)$. Donc $d = a(1 - nu) + b(-nv)$. Ainsi d est de la forme $au' + bv'$, c'est un élément de A.
• De plus d est positif. Or $d < c$ et c est le minimum de A'. Donc d ne peut appartenir à A'. Le seul élément positif de A qui n'est pas dans A' est 0. Donc $d = 0$.
• Donc $a = nc$ et c divise a.

• En effectuant la division euclidienne de b par c, on montre de même que c divise b.

• Or a et b sont supposés premiers entre eux. Donc comme c est un entier positif qui divise a et b, on déduit que $c = 1$.
• On peut donc conclure que $au + bv = 1$ avec u et v dans $\mathbf{Z}$.

Exercice : démontrer la réciproque du théorème de Bézout.

Définition 2.1.4. *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 :*

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

Exercice : démontrer la version forte du théorème de Bézout :

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

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

Théorème 2.1.3. (Lemme d'Euclide)

Soit p un nombre premier et soient $a, b \in N$. Si p divise le produit ab, alors p divise a ou p divise b :

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

Démonstration :
• Soit p un nombre premier et soient a et b des entiers naturels 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, alors comme p est premier, a et p sont premiers entre eux. D'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $up + va = 1$.
• Alors $upb + vab = b$ puis en remplaçant ab par kp, $p(ub + kv) = b$.
• 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 la même manière le **lemme de Gauss**.
Soient a, b et c des entiers tels que $a|bc$ et $PGCD(a, b) = 1$ (a et b premiers entre eux). Alors $a|c$.

Théorème 2.1.4. fondamental de l'arithmétique.

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

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

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.
• Soit $n \in \mathbf{N}^*$.
• Si $n = 1$, on peut écrire n sous la forme d'un produit vide de nombres premiers (*i.e.* avec $k = 0$).
• Si $n = 2$, n est premier et se décompose naturellement en $n = \prod_{i=1}^{1} p$ avec $p = 2$.
• Supposons maintenant le résultat vrai pour tout entier m tel que $m < n$. Distinguons deux cas : soit n est premier soit 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 : $\exists, i, j \geqslant 0, \exists q_1, \ldots, q_i, r_1, \ldots, r_j \in \mathcal{P},\ \ m_1 = \prod_{l=1}^{i} q_l,\ \ m_2 = \prod_{l=1}^{j} r_l$. Alors

$$n = m_1 m_2 = \prod_{l=1}^{i} q_l \prod_{l=1}^{j} r_l.$$

Ce dernier terme est un produit de nombre premier. 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 : $\exists k \in \mathbf{N}, \exists p_1, \ldots, p_k \in \mathcal{P},\ n = \prod_{i=1}^{k} p_i$ et $\exists j \in \mathbf{N}, \exists q_1, \ldots, q_j \in \mathcal{P},\ n = \prod_{i=1}^{j} q_i$.
• Soit $p \in \mathcal{P}$. 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 peut écrire $n = p^\alpha m$ où m est le produit de tous les facteurs premiers différents de p de la première décomposition de n. 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 peut pas diviser pas n.
• De même, 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 bien 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 2.1.5. *L'ensemble $\mathcal{P}$ 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_j ; c'est un des nombres premiers définis initialement.
• Alors p_j divise $1 + \prod_{i=1}^{n} p_i$. Or p_j divise clairement $\prod_{i=1}^{n} p_i$ puisqu'il est un des termes de ce produit.
• On en déduit que p_j divise 1. Or 1 n'est divisible par aucun nombre premier. On aboutit donc à une absurdité.
• On peut conclure que l'ensemble des nombres premiers est infini.

2.2 Congruences

Définition 2.2.1. *Soit n un entier et soient a et b deux entiers relatifs. On dit que a et b sont* **congrus modulo** *n si $n|a-b$.*

On note $a \equiv b \mod n$ ou encore $a \equiv b[n]$.

Proposition 2.2.1. *Avec les mêmes notations, a est congru à b modulo n si a est égal à b à un multiple de n près :*

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

Proposition 2.2.2. *Soient n, a, b et c des entiers relatifs. 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* $a \equiv c \mod n$.

On dit que la relation de congruence est une **relation d'équivalence**.

Définition 2.2.2. *Soit $n \in \mathbf{Z}$ et $a \in \mathbf{Z}$. 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.

Proposition 2.2.3. *Soient n, a et b des entiers tels que $a \equiv b \mod n$. Alors $\bar{a} = \bar{b}$.*

On dit que a et b sont des représentants de la classe de congruence $\bar{a}$.

Si $n \neq 0$, l'ensemble $\mathbf{Z}$ est l'union disjointe des classes de congruence $\bar{0}$, $\bar{1}, \dots, \overline{n-1}$:

$$\mathbf{Z} = \bigsqcup_{k=0}^{n-1} \bar{k}.$$

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

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

Proposition 2.2.4. *On peut munir $\mathbf{Z}/n\mathbf{Z}$ d'une addition $\bar{+}$ et d'une multiplication $\bar{\times}$ définies par*

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

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 $\mathbf{Z}/n\mathbf{Z}$.

Remarque : 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.

Chapitre 3

Ensembles et applications

3.1 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".

3.1.1 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 : $i, 0, 3i - 2, e^{\frac{2i\pi}{3}}$.

À partir de ces ensembles, on peut définir des sous-ensembles particuliers. 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 $\mathcal{P}$ des nombres premiers,
- l'ensemble des solutions d'une équation de la forme $f(x) = 0$ est l'ensemble $\{x \mid f(x) = 0\}$.

Parmi ces 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 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.

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 $\{(x, y) \mid x^2 + y^2 = 1\}$ et de manière paramétrique comme l'ensemble $\{(\cos(t), \sin(t)), t \in \mathbf{R}\}$.

3.1.2 Comparaisons d'ensemble

Définition 3.1.1. *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.

Exemple 3.1.1. *Pour tout ensemble A, $\emptyset \subset A$.*

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

Remarque 3.1.1. *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 $x \in B$ » puis la conclusion.*

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 $B \subset A$.

Définition 3.1.2. *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 à ne pas confondre disjoint et différent.

Définition 3.1.3. *Soit E un ensemble. On appelle* **ensemble des parties** *de E l'ensemble noté $\mathcal{P}(E)$ défini par*

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

Autrement dit, $A \in \mathcal{P}(E) \Leftrightarrow A \subset E$.

3.1.3 Opérations sur les ensembles

Définition 3.1.4. *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 :*

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

Définition 3.1.5. *Soient A et B deux ensembles. 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 :*

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

Proposition 3.1.1. *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 : $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Définition 3.1.6. *Soient A une partie d'un ensemble E. On appelle* **complémentaire** *de A dans E et on note $\bar{A}$ l'ensemble contenant des éléments de E qui n'appartiennent pas à A :*

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

Définition 3.1.7. *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 :*

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

On remarque que $A \setminus B = A \cap \bar{B}$.

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

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

Définition 3.1.8. *Un* **couple** (x, y) *est un objet mathématique formé à partir de deux autres objets* x *et* y *et qui possède la propriété suivante*

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

Définition 3.1.9. *Soient* E *et* F *des ensembles. On appelle produit cartésien de* E *et* F *l'ensemble des couples* (x, y) *avec* x *dans* E *et* y *dans* F *:*

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

Remarque 3.1.2.

- *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*.*

3.2 Applications

3.2.1 Définition

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

Définition 3.2.1. *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*
$$\forall x \in E, \exists! y \in F,\ (x, y) \in \Gamma.$$
- *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.*

Définition 3.2.2. *Soit E et F des ensembles.*

On appelle application **identité** *de E l'application*
$$\begin{array}{rccc} Id_E: & E & \to & E \\ & x & \mapsto & x. \end{array}$$

Soit $a \in F$. On appelle fonction **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*
$$\begin{array}{rccc} \mathbf{1}_A: & E & \to & \mathbf{R} \\ & x & \mapsto & \begin{cases} 1 & si\ x \in A \\ 0 & si\ x \notin A \end{cases}. \end{array}$$

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

3.2.2 Images et antécédents

Définition 3.2.3. *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 3.2.4. *Soit f une application de E vers F.*
Soit $A \subset E$.
On appelle **image** *de A par f l'ensemble $f(A) = \{f(x) \mid x \in A\}$.*
L'image de E est appelée image de f.

Soit $B \subset F$.
On appelle **image réciproque** *de B par f 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 $x \in f^{-1}(\{y\})$.*

3.2.3 Restriction, prolongement, composition

Définition 3.2.5. *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 3.2.6. *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 $\forall x \in E,\ g \circ f(x) = g(f(x))$:*

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

Proposition 3.2.1. *Soient E, F, G et H des ensembles et soient $f \in \mathcal{F}(E, F)$, $g \in \mathcal{F}(F, G)$ et $f \in \mathcal{F}(G, H)$. La composition des applications est associative :*

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

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

3.2.4 Injections, surjections et bijections

Définition 3.2.7. *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.

Définition 3.2.8. *Soit f une bijection de E vers F.*
On appelle **bijection réciproque** *de f l'unique application notée f^{-1} telle que $f^{-1} \circ f = Id_E$ et $f \circ f^{-1} = Id_F$.*
C'est l'application qui à chaque élément de F associe son unique antécédent par f.

Remarque 3.2.1. *On peut montrer qu'une application est une bijection en montrant qu'elle admet une fonction réciproque.*

Proposition 3.2.2. *La composée de deux bijections est une bijection.*

3.3 Cardinal d'un ensemble

3.3.1 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 3.3.1. *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 $\{1, \ldots, n\}$ vers E.*
On note $\mathrm{Card}(E) = n$.
Le cardinal de l'ensemble vide est 0.

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.

Proposition 3.3.1. *Soient $(n, m) \in \mathbf{N}^2$.*
Il existe une bijection de $\{1, \ldots, n\}$ vers $\{1, \ldots, m\}$ si et seulement si $n = m$.

Et de manière générale :

Proposition 3.3.2. *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.

Exemple 3.3.1. $\mathrm{Card}(\{2, 8, 3\}) = 3$, $\mathrm{Card}(\{0, \{7, 9, 2\}\} = 2$.

Proposition 3.3.3. *Soit E et F des ensembles de cardinaux finis n et m.*
Alors

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

3.3.2 Ensemble infinis et dénombrabilité

Définition 3.3.2. *Soit E un ensemble.*
On dit que E est de cardinal infini s'il n'est pas de cardinal fini.

Exemple 3.3.2. $\mathbf{N}, \mathbf{R}, \mathcal{P}$ *et l'ensemble des nombres pairs sont des ensembles infinis.*

La propriété 3.3.2 s'applique-t-elle aux ensembles infinis ? Deux ensembles infinis sont-ils nécessairement en bijection ? Nous allons voir que 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 3.3.3. *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.

Exemple 3.3.3. $\mathcal{P}, \mathbf{Z}$ *et* $\mathbf{Q}$ *sont des ensembles dénombrables.*

Proposition 3.3.4. *L'ensemble des nombres réels* $\mathbf{R}$ *n'est pas dénombrable.*

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

Proposition 3.3.5. *Il existe une bijection de* $\mathcal{P}(\mathbf{N})$ *vers* $\mathbf{R}$*. Autrement dit,* $\mathbf{R}$ *et* $\mathcal{P}(\mathbf{N})$ *ont le même cardinal infini.*

Proposition 3.3.6. *Il existe une bijection de* $\mathbf{R}$ *vers* $\mathbf{R}^2$*. Autrement dit,* $\mathbf{R}$ *et* $\mathbf{R}^2$ *ont le même cardinal infini.*

Chapitre 4

Nombres complexes

4.1 Définitions

4.1.1 Construction de C

Définition 4.1.1. *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* $\mathbf{C}$.

Proposition 4.1.1. *L'addition et la multiplication sont associatives et commutatives. La multiplication est distributive par rapport à l'addition.*

Le nombre complexe $(1,0)$ *est l'élément neutre de la multiplication :* $\forall z \in \mathbf{C},\ z\times(1,0) = z$.

Proposition 4.1.2. *Soit* $z \neq (0,0)$. *Alors il existe un unique nombre complexe* z' *tel que* $zz' = (1,0)$. *On note alors* $z' = \frac{1}{z}$.

Définition 4.1.2. *Tout nombre complexe est naturellement associé à un point du plan. On dit qu'un point* M *du plan, d'abscisse* x *et d'ordonnée* y, *a pour* **affixe** *le nombre complexe* $z = (x,y)$.

4.1.2 Écriture algégrique et conjugué

Définition 4.1.3. *On note* i *l'élément* $(0,1)$ *de* $\mathbf{C}$.
Pour $x \in \mathbf{R}$*, on note simplement* x *l'élément* $(x,0)$ *de* $\mathbf{C}$.
Ainsi, pour tous x, y *dans* $\mathbf{R}$*,* $x + \mathrm{i}y$ *représente l'élément* (x,y) *de* $\mathbf{C}$.

Pour tout nombre complexe z*, l'écriture* $z = x + \mathrm{i}y$ *est* **l'écriture algébrique** *de* z.
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**.

Définition 4.1.4. *Soit* $z = x + \mathrm{i}y \in \mathbf{C}$*. On appelle nombre conjugué de* z *le nombre complexe*

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

Proposition 4.1.3. *Soient* z, z_1, z_2 *des nombres complexes.*

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

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.

4.1.3 Écriture polaire, module et argument

Définition 4.1.5. *Soit* $\theta \in \mathbf{R}$*. On définit l'exponentielle du nombre complexe* $i\theta$ *comme étant le nombre complexe*

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

Proposition 4.1.4. *Soient* $\theta_1, \theta_2 \in \mathbf{R}$*. Alors* $\mathrm{e}^{\mathrm{i}\theta_1}\mathrm{e}^{\mathrm{i}\theta_2} = \mathrm{e}^{\mathrm{i}(\theta_1+\theta_2)}$ *et* $\dfrac{1}{\mathrm{e}^{\mathrm{i}\theta}} = \mathrm{e}^{-\mathrm{i}\theta}$.

Proposition 4.1.5. *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 $\vec{OM}$ et $\arg(z)$ est l'angle entre l'axe réel Ox et la demi-droite $[OM)$.

Proposition 4.1.6. *Soit $z \in \mathbf{C}$ d'écriture algébrique $z = x + iy$. Alors*

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

On remarque que $z\bar{z} = |z|^2$.

Proposition 4.1.7. *Le module est une distance sur $\mathbf{C}$. Pour $z, z' \in \mathbf{C}$, $|z - z'|$ représente la distance euclidienne dans le plan complexe entre les points d'affixes z et z'.*

Proposition 4.1.8. *Soient $z_1, z_2 \in \mathbf{C}$.*

- $|z_1 z_2| = |z_1||z_2|$;
- $|z_1| = |\bar{z}_1|$;
- *inégalité triangulaire :* $|z_1 + z_2| \leq |z_1| + |z_2|$;
- $\arg(z_1) = -\arg(\bar{z}_1)$;
- $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$.

Définition 4.1.6. *On note $\mathbf{U}$ l'ensemble des nombres complexes dont le module est 1 :*

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

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

4.2 Propriétés des nombres complexes

4.2.1 Racines de polynômes

Théorème 4.2.1. fondamental de l'algèbre
Tout polynôme non constant à coefficients complexes admet une racine complexe.

Corollaire 4.2.2.
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.

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.

Racine carrée

Définition 4.2.1. *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 $X^2 - \omega$.*

Remarque 4.2.1. *La notation $\sqrt{\omega}$ est interdite car ambiguë. Elle ne peut être utilisée que pour les nombres réels positifs et désigne dans ce cas l'unique racine positive du nombre.*

Proposition 4.2.3. *Soit $z \in \mathbf{C}$ de forme polaire $z = r\mathrm{e}^{\mathrm{i}\theta}$.*
Les racines carrées de z sont les nombres complexes

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

En pratique, on ne dispose pas toujours de la forme trigonométrique d'un nombre complexe. Il est néanmoins possible de déterminer ses racines carrées à partir de son écriture algébrique. Voilà la méthode.

Soit $z = a + \mathrm{i}b$. On cherche les nombres complexes $x + \mathrm{i}y$ tels que $(x + \mathrm{i}y)^2 = a + \mathrm{i}b$. En 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 $|(x+\mathrm{i}y)^2| = |z| = \sqrt{a^2 + b^2}$. On résout le système $x^2 - y^2 = a$, $x^2 + y^2 = |z|$ et on obtient $x = \pm\sqrt{\frac{|z|+a}{2}}$ et $y = \pm\sqrt{\frac{|z|-a}{2}}$. Parmi les 4 couples (x, y) ainsi obtenus, seuls deux vérifient l'équation $2xy = b$. On obtient ainsi les deux solutions $x + \mathrm{i}y$ recherchées.

Racines d'un polynôme de degré 2

Proposition 4.2.4. *Soient $a, b, c \in \mathbf{C}$ avec $a \neq 0$ et $P = aX^2 + bX + c$ un polynôme.*
Soit $\Delta = b^2 - 4ac$ et soit δ une racine carrée de Δ.
Les racines de P sont les nombres complexes

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

Remarque 4.2.2.

- *Si P est à coefficients réels, on retrouve les expressions bien connues dépendant du signe de Δ.*
- *Si $\Delta = 0$, alors $z_1 = z_2$ et on dit que P possède une racine double.*

Racines n-ièmes

Définition 4.2.2. *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 $X^n - \omega$.*

Proposition 4.2.5. *Soit $z \in \mathbf{C}$ de forme polaire $z = r\mathrm{e}^{\mathrm{i}\theta}$ et $n \geq 1$.*
Les racines n-ième de z sont les n nombres complexes définis pour $k = 0, \ldots, n-1$ par

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

4.2.2 Trigonométrie

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

Proposition 4.2.6. *Soient $x \in \mathbf{R}$ et $n \in \mathbf{N}$. Alors*

$$\cos(x) = \frac{\mathrm{e}^{\mathrm{i}x} + \mathrm{e}^{-\mathrm{i}x}}{2}, \qquad \sin(x) = \frac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}}.$$

Formule de Moivre *:*

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

Avant de parler de linéarisation, rappelons quelques formules algébriques.

Proposition 4.2.7. binôme de Newton

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

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

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 $a, b \in \mathbf{C}$,

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

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 leurs expressions avec l'exponentielle complexe, on développe les produits et puissances avec la formule du binôme de Newton, puis on regroupe les exponentielles de manière à faire réapparaître des cosinus et sinus.

Par exemple $(\sin(x))^3 = (\dfrac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}})^3 = \dfrac{1}{-8\mathrm{i}}(\mathrm{e}^{3\mathrm{i}x} - 3\mathrm{e}^{\mathrm{i}x} + 3e^{-\mathrm{i}x} - \mathrm{e}^{-3\mathrm{i}x}) = -\dfrac{1}{4}(\dfrac{\mathrm{e}^{3\mathrm{i}x} - \mathrm{e}^{-3\mathrm{i}x}}{2\mathrm{i}} - 3\dfrac{\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}}{2\mathrm{i}}) = -\dfrac{1}{4}\sin(3x) + \dfrac{3}{4}\sin(x)$.

4.2.3 Transformations géométriques

On a vu qu'il y avait une bijection naturelle entre le plan usuel et l'ensemble des nombres complexes. Il est donc 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.

Translation

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 $\vec{AB} = \vec{u}$. 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 $T_{\vec{u}}^{-1} = T_{-\vec{u}}$.

Rotation

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 $R_{\Omega,\theta} = T_{\vec{O\Omega}} \circ R_\theta \circ T_{\vec{\Omega O}}$.

Symétrie

Soit $\theta \in \mathbf{R}$ et D la droite du plan passant par 0 et d'angle θ. La symétrie orthogonale par rapport à la droite D correspond à l'application

$$\begin{array}{rccc} S_D : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & \mathrm{e}^{2\mathrm{i}\theta} \overline{z} \end{array}$$

Théorème 4.2.8. *On appelle* **isométrie** *du plan toute application f du plan qui préserve les distances :* $\forall (z_1, z_2) \in \mathbf{C}^2$, $|f(z_2) - f(z_1)| = |z_2 - z_1|$.

Les translations, les rotations, les symétries et les symétrie glissées (c'est-à-dire la composée d'une symétrie et d'une translation) forment l'ensemble des isométries du plan.

Homothétie

Soit $\lambda \in \mathbf{R}$. L'homothétie de rapport λ et de centre O est l'application du plan dans lui-même qui envoie tout point A sur le point B tel que O, A et B sont alignés et $OB = \lambda OA$.
L'homothétie de rapport λ correspond à l'application

$$\begin{array}{rccc} H_\lambda : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & \lambda z \end{array}$$

Soit Ω un point d'affixe z_0. Alors l'homothétie de rapport λ et de centre Ω correspond à l'application

$$\begin{array}{rccc} H_{\Omega,\lambda} : & \mathbf{C} & \to & \mathbf{C} \\ & z & \mapsto & z_0 + \lambda(z - z_0) \end{array}$$

On remarque encore que $H_{\Omega,\lambda} = T_{\vec{O\Omega}} \circ H_\lambda \circ T_{\vec{\Omega O}}$.

Similitude

Soient $\theta \in \mathbf{R}$ et $\lambda \in \mathbf{R}$. La similitude d'angle θ et de rapport λ est la composée d'une rotation d'angle θ et de centre O avec l'homothétie de rapport λ et de centre O. Elle correspond donc à l'application

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

Plus généralement, toute application affine de $\mathbf{C}$, c'est-à-dire de la forme $z \mapsto az + b$ avec $a, b \in \mathbf{C}$, $a \neq 0$, peut s'écrire comme une composée d'une rotation, d'une homothétie et d'une translation.

Chapitre 5

Groupes

5.1 Loi de composition

Définition 5.1.1. *Soit E un ensemble. On appelle loi de composition interne 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 $x * y$.

Exemple 5.1.1. *L'addition, la soustraction, la multiplication et la division dans les ensembles de nombres sont des lois de composition internes.*

Définition 5.1.2. *Soit E un ensemble muni d'une loi de composition interne notée $*$. On dit que*

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

5.2 Groupes

5.2.1 Généralités

Définition 5.2.1. *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**.

Remarque 5.2.1. *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 $y = z$.

Lorqu'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.

Exemple 5.2.1. *$(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$ 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.

Proposition 5.2.1. *Soit $(G, *)$ 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, $xy = xz \implies y = z$.*

Remarque 5.2.2. *Historiquement, la notion de groupe a été introduite par Évariste Galois au XIXème siècle dans le cadre de la résolution des équations polynômiales. On sait obtenir les racines des polynômes de degré 2 grâce à des formules bien connues. Il existe également des formules plus compliquées pour déterminer les racines des polynômes de degré 3 et 4. Galois a démontré, grâce à la théorie des groupes, 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 polynômiales.*

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.

5.2.2 Sous-groupes

Définition 5.2.2. *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 5.2.3. *Soit $(G, *)$ un groupe d'élément neutre e et soit $H \subset G$. L'ensemble H est un sous-groupe de G si*

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

Exemple 5.2.2. *L'ensemble des nombres pairs est un sous-groupe de $(\mathbf{Z}, +)$. Le groupe tout entier G et $\{e\}$ sont des sous-groupes de $(G, *)$.*

Proposition 5.2.2. *Soient H et K des sous-groupes d'un groupe $(G, *)$. Alors $H \cap K$ est un sous-groupe de $(G, *)$.*

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

Définition 5.2.4. *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.

Exemple 5.2.3. *Dans $(\mathbf{Z}, +)$, le sous-groupe $< \{2\} >$ engendré par 2 est le sous-groupe des nombres pairs.*
Les nombres 2 et 3 engendrent $(\mathbf{Z}, +)$: $< \{2, 3\} >= \mathbf{Z}$.

5.2.3 Morphismes

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

Définition 5.2.5. *Soient $(G, *)$ et $(F, \times)$ des groupes et $f : G \to F$ une application. On dit que f est un* **morphisme de groupes** *si f préserve la structure de groupe, c'est-à-dire si*

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

Remarque 5.2.3. *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.*

Définition 5.2.6. *L'ensemble des morphismes de $(G, *)$ dans $(F, \times)$ se note* $\mathrm{Hom}(G, F)$.
Si $f \in \mathrm{Hom}(G, G)$, on dit que f est un **endomorphisme**.
Si $f \in \mathrm{Hom}(G, F)$ est une bijection, on dit que f est un **isomorphisme** *de groupes.*

Proposition 5.2.3. *La composée de deux morphismes de groupes est un morphisme de groupes.*

Définition 5.2.7. *Soit $f \in \mathrm{Hom}(G, F)$. On appelle* **noyau** *de f l'ensemble*

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

Proposition 5.2.4. *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* $\mathrm{Ker}(f) = \{e_G\}$.

5.3 Groupes finis

Théorème 5.3.1. 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 $\text{Card}(A_x) = \text{Card}(H)$: 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 : $\text{Card}(A_x) = \text{Card}(H)$.
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 5.3.1. *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.*

D'après le théorème de Lagrange, l'ordre d'un élément de G divise le cardinal de G.

Proposition 5.3.2. *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 $\{x, x^2, x^3, \ldots, x^{d-1}, x^d\}$.

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 $H =< x >$.

Proposition 5.3.3. *Soit $n \in \mathbf{N}$, $(G, *)$ un groupe de cardinal n et $x \in G$.*
Alors $x^n = e$.

Définition 5.3.2. *On dit qu'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.

5.4 Deux exemples

5.4.1 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 ?

Proposition 5.4.1. *Soit $n \in \mathbf{Z}^*$.*
$(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe commutatif.

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

Pour $(\mathbf{Z}/n\mathbf{Z}, \times)$, la réponse est clairement non 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.

Proposition 5.4.2. *$((\mathbf{Z}/n\mathbf{Z})^*, \times)$ est un groupe si et seulement si n est un nombre premier.*

Il est de cardinal $n - 1$.

Corollaire 5.4.3. Petit théorème de Fermat.
Soit p un nombre premier et soit a un nombre entier premier avec p.
Alors $a^{p-1} \equiv 1[p]$.

Proposition 5.4.4. *Soit p un nombre premier.*
Alors $((\mathbf{Z}/p\mathbf{Z})^*, \times)$ est un groupe cyclique.

5.4.2 Le groupe des permutations

Définition 5.4.1. *Soit $n \in \mathbf{N}^*$. On note $\mathfrak{S}_n$ l'ensemble des bijections de $\{1, \ldots, n\}$. Une telle bijection est appelée* **permutation** *de $\{1, \ldots, n\}$.*

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 5.4.2. *Soit $n \in \mathbf{N}^*$.*
On appelle **identité** *la permutation $Id = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$.*

C'est simplement l'application identité de $\{1, \ldots, n\}$. 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 $i, j \in \{1, \ldots, n\}$ 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 des éléments d'ordre 2 du groupe des permutations.

Proposition 5.4.5. *L'ensemble des transpositions de $\mathfrak{S}_n$ engendre $\mathfrak{S}_n$.*

Autrement dit, 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 $\sigma \neq Id$. 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 $\tau^{(r)} \cdots \tau^{(1)}\sigma = Id$. Alors $\sigma = \tau^{(1)} \cdots \tau^{(r)}$ et peut donc s'écrire comme un produit de transpositions.

5.5 Anneaux, corps, espaces vectoriels

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

5.5.1 Anneaux

Définition 5.5.1. *Soit E un ensemble muni de deux lois de composition internes $*$ et $\circ$. On dit que $*$ est* **distributive** *par rapport à $\circ$ si*

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

Définition 5.5.2. *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 $+$.*

Remarque : 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, les éléments de A n'ont pas nécessairement d'inverse.

Exemple 5.5.1.
$(\mathbf{Z}, +, \times)$ 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.

La propriété suivante, classique dans $\mathbf{Z}$ ou $\mathbf{R}$, n'est pas satisfaite en général dans un anneau.

Définition 5.5.3. *Soit $(A, +, \cdot)$ un anneau. On dit que c'est un anneau* **intègre** *si*

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

Les propriétés suivantes sont en revanche vraies dans tout anneau.

Proposition 5.5.1. *Soit $(A, +, \cdot)$ un anneau.*

Formule du binôme de Newton *: 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,

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} y^k x^{n-1-k} = (x-y)(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\cdots+x^2y^{n-3}+xy^{n-2}+y^{n-1}).$$

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

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

5.5.2 Corps

Définition 5.5.4. *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 $\cdot$.*

Remarque 5.5.1. *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.

Exemple 5.5.2. *$(\mathbf{Q},+,\times), (\mathbf{R},+,\times)$, et $(\mathbf{C},+,\times)$ sont des corps.*

Si p est un nombre premier, $(\mathbf{Z}/p\mathbf{Z},+,\times)$ est un corps.

Théorème 5.5.2. *Soit $(K,+,\cdot)$ un corps, soit $n \in \mathbf{N}$ et soit P un polynôme de degré n à coefficients dans K.*

Alors P admet au plus n racines dans K.

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 $\mathbf{K}$. Alors on peut factoriser P par $(X-a)$: $P = (X-a)Q$ où Q est un polynôme de degré $n-1$ (nous verrons cela au chapitre 8). Supposons que P a une autre racine b distincte de a. Cela signifie que $(b-a)Q(b) = 0$. Or $b - a \neq 0$. Comme K est un corps, $b-a$ est donc inversible. On en déduit $Q(b) = 0$. 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 K. Donc, en ajoutant a, on déduit que P a au plus n racines dans K.

Le résultat est ainsi démontré par récurrence.

5.5.3 Espace vectoriel

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

Définition 5.5.5. *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* **K-espace vectoriel** *si*

- $(E, +)$ *est un groupe commutatif,*
- *Pour tous λ et μ dans $\mathbf{K}$, pour tous x et y dans E :*

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

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

Exemple 5.5.3. *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).

Chapitre 6

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** $\begin{pmatrix} \frac{7}{9} & \frac{4}{9} & 0 \\ \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$. 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.

6.1 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 6.1.1. *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 :*

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

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 6.1.2. *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 6.1.3. *On appelle* **matrice nulle** *de $\mathcal{M}_{n,p}(\mathbf{A})$ la matrice $M = (m_{ij})_{i \leqslant n, j \leqslant p}$ telle que pour tous i et j, $m_{ij} = 0$.*

Définition 6.1.4.
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 l'***addition** *de ces deux matrices par*

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

Définition 6.1.5.
Soient $M = (a_{ij})_{i \leqslant n, j \leqslant p} \in M_{n,p}(A)$ et $N = (b_{ij})_{i \leqslant p, j \leqslant q} \in M_{p,q}(A)$.
On définit le **produit** *de ces deux matrices par*

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

avec pour tous i et j

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

Définition 6.1.6. *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*

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

Proposition 6.1.1.

- *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 $B = 0$.*

Remarque 6.1.1.

- *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 6.1.7. *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*

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

Proposition 6.1.2. *Soient A, B et C des matrices telles que $A + B$ et AC soient bien définies et soit $a \in \mathbf{A}$. Alors*

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

6.2 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 6.2.1. *On appelle* **matrice identité** *de taille n la matrice de $\mathcal{M}_n(\mathbf{A})$ définie par*

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Proposition 6.2.1.

- *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 6.2.2. *Soit $M = (a_{ij}) \in \mathcal{M}_n(A)$.*
On dit que M est une **matrice diagonale** *si $\forall i \neq j,\ a_{ij} = 0$.*
On dit que M est une **matrice triangulaire supérieure** *si $\forall i > j,\ a_{ij} = 0$.*
On dit que M est une **matrice triangulaire inférieure** *si $\forall i < j,\ a_{ij} = 0$.*
On dit que M est une **matrice symétrique** *si $M = {}^tM$.*
On dit que M est une **matrice antisymétrique** *si $M = -{}^tM$.*

Remarque 6.2.1. *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.*

6.3 Le groupe des matrices inversibles

6.3.1 Définitions

Définition 6.3.1. *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 $\mathcal{M}_n(\mathbf{A})$.

Proposition 6.3.1. *$(\mathrm{GL}_n(\mathbf{A}), \times)$ est un groupe.*

Proposition 6.3.2. *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 $(aA)^{-1} = \frac{1}{a}A^{-1}$.*

Proposition 6.3.3. *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.

Proposition 6.3.4. *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 $A^{-1} = C$.*

Proposition 6.3.5. *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.*

6.3.2 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 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 : $L_i \leftrightarrow L_j$;

Comme l'inverse d'une matrice M est égal 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.

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 $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 3 \\ 2 & 1 & -1 \end{pmatrix}$:

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

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

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

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

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

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

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

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

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 ou une colonne de zéros, cela signifie que la matrice considérée n'est pas inversible et il est inutile de continuer les calculs, ils n'aboutiront pas.

6.4 Quelques applications

6.4.1 Systèmes linéaires

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

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

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

$$AX = Y,$$

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

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.

6.4.2 Applications linéaires

Une application linéaire de $\mathbf{R}^n$ vers $\mathbf{R}^p$ 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.

Contentons-nous d'un exemple classique.

Dans le plan $\mathbf{R}^2$, la rotation de centre O et d'angle θ est une application linéaire donnée par la matrice

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

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

6.4.3 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 $M^k = (m_{ij}^{(k)})_{ij}$, 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.

Chapitre 7

Polynômes

Dans tout ce chapitre, $\mathbf{K}$ désignera un corps commutatif. Nous travaillerons essentiellement dans $\mathbf{R}$ ou $\mathbf{C}$, mais $\mathbf{K}$ peut aussi bien désigner $\mathbf{Q}$ ou $\mathbf{Z}/p\mathbf{Z}$ avec p un nombre premier. Beaucoup de résultats seront valables si $\mathbf{K}$ est simplement un anneau.

7.1 L'anneau des polynômes

On note $\mathbf{K}^{\mathbf{N}}$ l'ensemble des suites à valeurs dans $\mathbf{K}$.

Définition 7.1.1. *On appelle* **polynôme** *à coefficients dans* $\mathbf{K}$ *toute suite* $(a_k)_{k\in\mathbf{N}}$ *de* $\mathbf{K}^{\mathbf{N}}$ *nulle à partir d'un certain rang, c'est-à-dire telle qu'il existe* $n \in \mathbf{N}$ *avec pour tout* $k > n$, $a_k = 0$.

Un tel polynôme P *est alors noté*

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_{k=0}^{n} a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X^1 + a_0 X^0.$$

Le symbole X *est appelé* **indeterminée** *du polynôme. Les* a_k *sont appelés* **coefficients** *de* P.

L'ensemble des polynômes à coefficients dans $\mathbf{K}$ *est noté* $\mathbf{K}[X]$.

Parmi les polynômes, citons le **polynôme nul**, noté simplement 0, dont tous les coefficients sont nuls, et de manière générale, les **polynômes constants** qui sont de la forme $P = a_0 X^0$.

Définition 7.1.2. *On définit sur* $\mathbf{K}[X]$ *une* **addition**.
Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ *et* $Q = \sum_{k=0}^{+\infty} b_k X^k$ *dans* $\mathbf{K}[X]$. *Alors*

$$P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k.$$

Définition 7.1.3. *On définit sur* $\mathbf{K}[X]$ *une* **multiplication**.
Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ *et* $Q = \sum_{k=0}^{+\infty} b_k X^k$ *dans* $\mathbf{K}[X]$. *Alors*

$$PQ = \sum_{k=0}^{+\infty} c_k X^k,$$

avec pour tout k *dans* $\mathbf{N}$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

Proposition 7.1.1.
Le triplet $(\mathbf{K}[X], +, \times)$ *est un anneau commutatif et intègre.*

Le polynôme nul en est l'élément absorbant et le polynôme constant 1 en est l'élément neutre.

L'ensemble $(\mathbf{K}[X])^\times$ *des polynômes inversibles est l'ensemble* $\mathbf{K}^*$ *des polynômes constants non nuls.*

Définition 7.1.4. *Soit* $(\mathbf{A}, +, *)$ *un anneau muni d'une "bonne" multiplication scalaire* $\mathbf{K} \times \mathbf{A} \to \mathbf{A}$. *Soit* $x \in \mathbf{A}$.
On appelle **morphisme d'évaluation** *en* x *l'application*

$$\begin{array}{rccc} \varphi_x : & \mathbf{K}[X] & \to & \mathbf{A} \\ & P = \sum a_k X^k & \to & P(x) = \sum a_k x^k. \end{array}$$

Exemple 7.1.1. *Le polynôme* $X^2 - 2X + 3$ *peut être évalué en* $z = 1 + i \in \mathbf{C}$, *mais aussi en* $5 \in \mathbf{Z}$, *en* $\left(\begin{smallmatrix} 2 & 3 \\ -1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(\mathbf{Z})$ *ou encore en* $\overline{3} \in \mathbf{Z}/5\mathbf{Z}$.

Définition 7.1.5. *Soit* $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbf{K}[X]$ *un polynôme non nul. On appelle* **degré** *de* P *l'entier positif défini par*

$$\deg(P) = \max\{k \in \mathbf{N} \mid a_k \neq 0\}.$$

Si P *est le polynôme nul, on pose* $\deg(P) = -\infty$.

Soit P *un polynôme de degré* $n \in \mathbf{N}$. *Son coefficient* a_n *est appelé* **coefficient dominant**. *Si* $a_n = 1$, *on dit que* P *est* **unitaire**.

Proposition 7.1.2. *Soient* P *et* Q *dans* $\mathbf{K}[X]$.

- $\deg(PQ) = \deg(P) + \deg(Q)$.
- *Si* $\deg(P) \neq \deg(Q)$, *alors* $\deg(P+Q) = \max(\deg(P), \deg(Q))$.
- *Si* $\deg(P) = \deg(Q)$, *alors* $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.

7.2 Arithmétique des polynômes

Définition 7.2.1. *Soient P et Q dans $\mathbf{K}[X]$. On dit que Q* **divise** *P et on note $Q|P$ si $\exists R \in \mathbf{K}[X],\ P = QR$.*

Définition 7.2.2. *On appelle* **polynôme irréductible** *tout polynôme P non constant dont les seuls diviseurs, à un multiple scalaire près, sont les polynômes 1 et P.*

Exemple 7.2.1. *Les polynômes de degré 1 sont toujours irréductibles.*
Le polynôme $X^2 + 1$ est irréductible dans $\mathbf{R}[X]$ mais pas dans $\mathbf{C}[X]$.
Le polynôme $X^3 - 2$ est irréductible dans $\mathbf{Q}[X]$.

Théorème 7.2.1. Division euclidienne des polynômes

Soient P_1 et P_2 dans $\mathbf{K}[X]$ avec $P_2 \neq 0$. Il existe un unique couple de polynômes $(Q, R) \in \mathbf{K}[X]^2$ tel que $P_1 = QP_2 + R$ et $\deg(R) < \deg(P_2)$.

Le polynôme Q est le quotient de la division et R en est le reste.

Définition 7.2.3. *On dit que deux polynômes P et Q de $\mathbf{K}(X]$ sont* **premiers entre eux** *s'ils n'ont aucun diviseur commun hormis les polynômes constants non nuls :*

$$\forall R \in \mathbf{K}[X],\ (R|P \text{ et } R|Q) \implies R \in \mathbf{K}^*.$$

Théorème 7.2.2. de Bézout.
Soient P et Q deux polynômes premiers entre eux. Alors il existe des polynômes U et V tels que

$$PU + QV = 1.$$

La réciproque de ce théorème est vraie.

Définition 7.2.4. *On appelle* **plus grand commun diviseur** *(PGCD) de deux polynômes P et Q le polynôme unitaire de degré maximal qui divise à la fois P et Q.*

Comme pour les nombres entiers, on a une version forte du théorème de Bezout :

$$\forall P \in \mathbf{K}[X], \forall Q \in \mathbf{K}[X], \exists U \in \mathbf{K}[X], \exists V \in \mathbf{K}[X],\ PU+QV = \mathrm{PGCD}(P,Q).$$

Le PGCD et la relation de Bézout s'obtiennent avec l'algorithme d'Euclide, c'est-à-dire avec des divisions euclidiennes successives de polynômes.

Théorème 7.2.3. Lemme de Gauss

Soit P un polynôme irréductible et soient A et B dans $\mathbf{K}[X]$. Si P divise le produit AB, alors P divise A ou P divise B.

Soient P et Q des polynômes premiers entre eux et soit $A \in \mathbf{K}[X]$. Si P divise AQ, alors P divise A.

Théorème 7.2.4. Décomposition des polynômes en facteurs irréductibles

Tout polynôme P non nul de $\mathbf{K}[X]$ se décompose en un produit fini de polynômes irréductibles : il existe un entier naturel n, des polynômes irréductibles $P_1, \ldots, P_n$ et $a \in \mathbf{K}^*$ tel que

$$P = a \prod_{i=1}^{n} P_i.$$

Si on impose aux polynômes P_i d'être unitaires, alors cette décomposition est unique à l'ordre des facteurs près.

7.3 Racines d'un polynôme

Définition 7.3.1. *Soit $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$. On dit que α est une* **racine** *de P si le polynôme $X - \alpha$ divise P.*

Proposition 7.3.1. *Un élément α de $\mathbf{K}$ est racine d'un polynôme P si et seulement si $P(\alpha) = 0$.*

Définition 7.3.2. *Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$ une racine de P et $m \in \mathbf{N}^*$. On dit que α est une racine d'***ordre** *m (ou de* **multiplicité** *m) si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P.*

Si α est une racine de multiplicité 1, on dit que c'est une **racine simple**, *si elle est de multiplicité 2, on parle de* **racine double**.

Définition 7.3.3. *Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbf{K}[X]$.*

On appelle **polynôme dérivé** *de P, le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ (si $n = 0$, on définit simplement $P' = 0$).*

On note P'', $P^{(3)}$,..., $P^{(j)}$ les polynômes dérivés successifs de P.

Proposition 7.3.2. *Soit $a \in \mathbf{K}$. Alors a est une racine multiple de P si et seulement si a est racine de P et P'.*

Plus précisément, a est racine de multiplicité m si et seulement si a est racine des polynômes P, P', P'', ...,$P^{(m-1)}$ mais n'est pas racine de $P^{(m)}$.

Définition 7.3.4. *Soit $P \in \mathbf{K}[X]$. On dit que P est scindé si on peut l'écrire comme un produit de polynômes de degré 1.*

Exemple 7.3.1. *Le polynôme $X^2 - 1 = (X - 1)(X + 1)$ est scindé dans $\mathbf{R}[X]$ et $\mathbf{Q}[X]$.*
Le polynôme $X^2 + 1$ n'est pas scindé dans $\mathbf{R}[X]$ mais est scindé dans $\mathbf{C}[X]$.

Proposition 7.3.3. *Un polynôme P de degré $n \in \mathbf{N}$ a au plus n racines dans $\mathbf{K}$ comptées avec multiplicité.*

Il est scindé si et seulement s'il possède exactement n racines dans $\mathbf{K}$ comptées avec multiplicités.

Proposition 7.3.4. Relations entre racines et coefficients

Soit $n \in \mathbf{N}$ et $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbf{K}[X]$ de degré n. On le suppose unitaire et scindé sur K. Notons alors $\sigma_1, \ldots, \sigma_n$ ses n racines dans K.

Alors

$$\forall k \in \{0, 1, \ldots, n\}, \quad a_{n-k} = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} \sigma_{i_1} \sigma_{i_2} \cdots \sigma_{i_k}.$$

En particulier,

$$a_0 = (-1)^n \prod_{i=1}^{n} \sigma_i, \quad \text{et} \quad a_{n-1} = -\sum_{i=1}^{n} \sigma_i.$$

7.4 Polynômes irréductibles de $\mathbf{R}[X]$ et $\mathbf{C}[X]$

7.4.1 Polynômes à coefficients complexes

Théorème 7.4.1. Théorème fondamental de l'algèbre *Tout polynôme non constant de $\mathbf{C}[X]$ a une racine dans $\mathbf{C}$.*

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 :

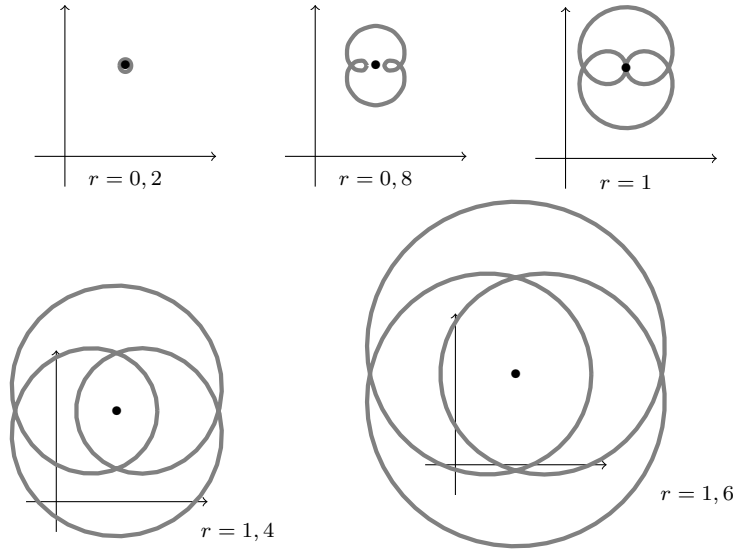
$$\begin{array}{rccc} f_r : & [0, 2\pi] & \to & \mathbf{C} \\ & \theta & \mapsto & P(r\mathrm{e}^{\mathrm{i}\theta}). \end{array}$$

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 $P = X^3 - X + 2 + 3i$.



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 $P(re^{i\theta}) = 0$. 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 7.4.2. *Les polynômes irréductibles de* $\mathbf{C}[X]$ *sont les polynômes de degré 1.*

Corollaire 7.4.3. *Tout polynôme de* $\mathbf{C}[X]$ *est scindé.*

Tout polynôme à coefficients complexes se décompose en un produit de polynômes de degré 1.

7.4.2 Polynômes à coefficients réels

Proposition 7.4.4. *Soit* $P \in \mathbf{C}[X]$ *un polynôme dont tous les coefficients sont réels. Si* $\alpha \in \mathbf{C}$ *est racine de* P*, alors* $\bar{\alpha}$ *est aussi racine de* P*.*

Proposition 7.4.5. *Les polynômes irréductibles de* $\mathbf{R}[X]$ *sont les polynômes de degré 1 et les polynômes de degré 2 n'ayant pas de racine dans* $\mathbf{R}$*,* i.e. *dont le discriminant est strictement négatif.*

Corollaire 7.4.6. *Tout polynôme à coefficients réels se décompose en un produit de polynômes de degré 1 et de polynômes de degré 2 dont le discriminant est strictement négatif.*

En particulier, tout polynôme réel de degré impair possède une racine réelle.

7.4.3 Autres polynômes

Dans $\mathbf{Q}[X]$ ou $\mathbf{Z}/p\mathbf{Z}[X]$ avec p premier, les choses ne sont pas aussi simples que dans $\mathbf{R}[X]$ ou $\mathbf{C}[X]$.

Proposition 7.4.7. *Pour tout entier $n \in \mathbf{N}^*$, il existe dans chacun de ces deux anneaux de polynômes un polynôme irréductible de degré n.*

En pratique, il est souvent difficile de montrer qu'un polynôme de $\mathbf{Q}[X]$ ou $\mathbf{Z}/p\mathbf{Z}$ est irréductible. Il existe cependant quelques critères comme le critère d'Eisenstein par exemple. Mentionnons le critère simple suivant.

Proposition 7.4.8. *Soit $P \in \mathbf{K}[X]$ de degré 2 ou 3. Alors P est irréductible si et seulement s'il n'a pas de racine dans $\mathbf{K}$.*

Exemple 7.4.1. *$X^4 - 4$ n'a pas de racine dans $\mathbf{Q}$ mais n'est pas irréductible puisque $X^4 - 4 = (X^2 - 2)(X^2 + 2)$.*

$X^4 + 1$ est irréductible sur $\mathbf{Q}$. Sa décomposition dans $\mathbf{R}[X]$ est $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$ et sa décomposition dans $\mathbf{C}$ est $X^4 + 1 = \prod_{i=0}^{3}(X - e^{i\frac{\pi+2i}{4}})$.

7.5 Applications

Les fonctions polynomiales sont les fonctions les plus simples, celles que l'on maîtrise le mieux et que l'on sait calculer sans difficultés. C'est pourquoi elles jouent un rôle central dans l'approximation des fonctions.

7.5.1 Interpolation de Lagrange

Considérons une fonction f dont on connaît les valeurs en n points : $\forall i \leq n, \ \ f(x_i) = y_i$. On cherche à approcher f par une fonction polynomiale. Le principe de l'interpolation est de chercher un polynôme qui coïncide avec f en les x_i. Le théorème ci-dessous fournit un tel polynôme.

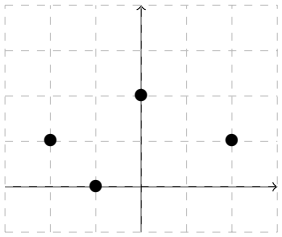
Théorème 7.5.1. *Soit $n \in \mathbf{N}^*$ et soient $x_1, \ldots, x_n$ des nombres réels distincts. Soient $y_1, \ldots, y_n$ des nombres réels.*

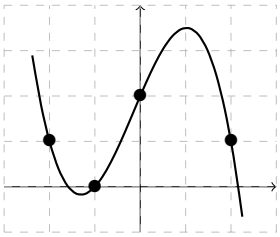
Alors il existe un unique polynôme P de degré au plus $n-1$ tel que $\forall i \leq n, \ \ P(x_i) = y_i$.

Ce polynôme est le polynôme

$$P = \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}.$$

Exemple 7.5.1. *Quel est le polynôme de degré minimal qui interpole les points ci-dessous ?*





Réponse : il s'agit du polynôme

$$\begin{aligned} P &= 1 \cdot \frac{X+1}{-2+1} \cdot \frac{X-0}{-2-0} \cdot \frac{X-2}{-2-2} + 0 \cdot \frac{X+2}{-1+2} \cdot \frac{X-0}{-1-0} \cdot \frac{X-2}{-1-2} \\ &\quad +2 \cdot \frac{X+2}{0+2} \cdot \frac{X+1}{0+1} \cdot \frac{X-2}{0-2} + 1 \cdot \frac{X+2}{2+2} \cdot \frac{X+1}{2+1} \cdot \frac{X-0}{2-0} \\ &= -\tfrac{7}{12}X^3 - \tfrac{1}{4}X^2 + \tfrac{7}{3}X + 2. \end{aligned}$$

7.5.2 Approximation locale

L'étude locale d'une fonction consiste à décrire le comportement de la fonction au voisinage direct d'un certain point. Par exemple, on peut considérer que la fonction $x \to e^x$ est proche de la fonction $x \to 1+x$ au voisinage de $x = 0$ car cette droite est la tangente à la fonction exp en $x = 0$.

On peut affiner cela et l'idée est d'approcher localement les fonctions par des fonctions polynomiales. Cela repose sur la remarque suivante.

Si P est un polynôme de degré n, alors pour tout x dans $\mathbf{R}$

$$P(x) = P(0)+P'(0)x+\frac{P''(0)}{2}x^2+\frac{P^{(3)}(0)}{3!}x^3+\cdots+\frac{P^{(n)}(0)}{n!}x^n = \sum_{k=0}^{n}\frac{P^{(k)}(0)}{k!}x^k.$$

Et plus généralement, pour $a \in \mathbf{R}$

$$\begin{aligned} P(x) &= P(a) + P'(a)(x-a) + \frac{P''(a)}{2}(x-a)^2 + \frac{P^{(3)(a)}}{3!}(x-a)^3 + \cdots + \frac{P^{(n)(a)}}{n!}(x-a)^n \\ &= \sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}(x-a)^k. \end{aligned}$$

Théorème 7.5.2. Formule de Taylor.

Soit $n \in \mathbf{N}^*$ et f une fonction réelle n fois dérivable en 0. Alors pour tout x au voisinage de 0

$$f(x) = f(0) + f'(0)x + \frac{f''(0)}{2}x^2 + \frac{f^{(3)}(0)}{3!}x^3 + \cdots + \frac{f^{(n)}(0)}{n!}x^n + R_n(x),$$

où R_n est une fonction (appelée reste) qui est négligeable devant x^n au voisinage de 0 : $\lim_{x\to 0}\frac{R_n(x)}{x^n} = 0$.

Si f est n fois dérivable en un point $a \in \mathbf{R}$, alors au voisinage de a

$$f(x) = f(a)+f'(a)(x-a)+\frac{f''(a)}{2}(x-a)^2+\frac{f^{(3)}(a)}{3!}(x-a)^3+\cdots+\frac{f^{(n)}(a)}{n!}(x-a)^n+R_n(x),$$

où R_n est une fonction négligeable devant $(x-a)^n$ au voisinage de a.

Autrement dit, cela signifie que la fonction polynomiale $\sum_{k=0}^{n}\frac{f^{(k)}(0)}{k!}x^k$ constitue une bonne approximation de la fonction f au voisinage de 0.

7.6 Le corps des fractions rationnelles

Nous ne considérons ici que les corps $\mathbf{R}$ et $\mathbf{C}$ et nous contenterons d'une présentation succinte des fractions rationnelles.

Le corps des fractions rationnelles sur $\mathbf{K}$ est en un sens le plus petit corps contenant l'ensemble des polynômes de $\mathbf{K}[X]$. On peut le définir rigoureusement à l'aide d'une relation d'équivalence parfaitement analogue à celle qui permet de construire $\mathbf{Q}$ à partir de $\mathbf{Z}$. Cela nous permet de définir l'ensemble suivant.

Définition 7.6.1. *Une* **fraction rationnelle** *sur* $\mathbf{K}$ *est le quotient* $F = \frac{P}{Q}$ *de deux polynômes* P *et* Q *de* $\mathbf{K}[X]$ *avec* $Q \neq 0$.

On dit que la fraction $\frac{P}{Q}$ *est sous* **forme irréductible** *si les polynômes* P *et* Q *sont premiers entre eux.*

Si la fraction est sous forme irréductible, on appelle **racines** *de* F *les racines de* P *et* **pôles** *de* F *les racines de* Q.

L'ensemble des fractions rationnelles sur $\mathbf{K}$ *est noté* $\mathbf{K}(X)$.

Proposition 7.6.1. *On peut munir* $\mathbf{K}(X)$ *d'une addition et une multiplication naturelles. Alors* $(\mathbf{K}(X), +, \times)$ *est un corps commutatif.*

Les fractions rationnelles interviennent beaucoup en tant que fonctions réelles ou complexes. Pour résoudre un grand nombre de problèmes avec ces fonctions, il est nécessaire de savoir les décomposer en une somme de fractions rationnelles simples. Ces décompositions reposent sur la décomposition en facteurs irréductibles des polynômes.

Théorème 7.6.2. *Soit $F \in \mathbf{C}(X)$ de forme irréductible $F = \frac{P}{Q}$.*
Soit $Q = u\prod_{i=1}^{k}(X-\alpha_i)^{n_i}$ la décomposition en facteurs irréductibles de Q, les α_i étant les racines de Q dans $\mathbf{C}$ et les n_i leurs multiplicités.

Alors il existe des nombres complexes $\lambda_{i,j}$ et un polynôme E tels que

$$\frac{P}{Q} = E + \sum_{i=1}^{k}\left(\frac{\lambda_{i,1}}{X-\alpha_i} + \frac{\lambda_{i,2}}{(X-\alpha_i)^2} + \cdots + \frac{\lambda_{i,n_i}}{(X-\alpha_i)^{n_i}}\right).$$

Cette décomposition est unique.

- Le polynôme E est le quotient de la division euclidienne de P par Q.
- Si α_1 est une racine simple de Q, on écrit $Q = (X-\alpha_1)Q_1$ et $\lambda_{1,1} = \frac{P(\alpha_1)}{Q_1(\alpha_1)} = \frac{P(\alpha_1)}{Q'(\alpha_1)}$.
- Pour les pôles d'ordre supérieur à 2, il existe des méthodes un peu plus techniques pour obtenir les $\lambda_{i,j}$ correspondant.
- Pour décomposer une fraction rationnelle de $\mathbf{R}(X)$, on commence par la décomposer dans $\mathbf{C}(X)$, puis on regroupe les termes conjugués.

Exemple 7.6.1.
En utilisant le fait que $\frac{2X^2-1}{X^4+2X^3+X^2} = \frac{2X^2-1}{X^2(X+1)^2} = \frac{1}{(X+1)^2} - \frac{2}{X+1} - \frac{1}{X^2} + \frac{2}{X}$, on montre (en reconnaissant une somme télescopique)

$$\sum_{k=1}^{n}\frac{2k^2-1}{k^4+2k^3+k^2} = \sum_{k=1}^{n}\left(\frac{1}{(k+1)^2} - \frac{1}{k^2}\right) + \left(\frac{2}{k} - \frac{2}{k+1}\right)$$

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

En utilisant le fait que

$$\frac{8X^2+4X}{X^4-1} = \frac{-1-2i}{X-i} + \frac{-1+2i}{X+i} + \frac{3}{X-1} + \frac{-1}{X+1} = \frac{4}{X^2+1} + \frac{-2X}{X^2+1} + \frac{3}{X-1} + \frac{-1}{X+1}$$

on déduit qu'une primitive de cette fonction rationnelle est

$$4\mathrm{Arctan}(X) - \ln(X^2+1) + 3\ln(X-1) - \ln(X+1).$$