ALGÈBRE 1

COURS DE MATHÉMATIQUES

PREMIER SEMESTRE – LMD

Université Ferhat Abbas, Sétif 1

Faculté des Sciences

Département de Mathématiques

À la découverte de l'algèbre

La première année d'études supérieures pose les bases des mathématiques. Pourquoi se lancer dans une telle expédition ? Déjà parce que les mathématiques vous offriront un langage unique pour accéder à une multitude de domaines scientifiques. Mais aussi parce qu'il s'agit d'un domaine passionnant ! Nous vous proposons de partir à la découverte des maths, de leur logique et de leur beauté.
Dans vos bagages, des objets que vous connaissez déjà : les entiers, les fonctions... Ces notions en apparence simples et intuitives seront abordées ici avec un souci de rigueur, en adoptant un langage précis et en présentant les preuves. Vous découvrirez ensuite de nouvelles théories (les espaces vectoriels, les équations différentielles,...).

Ce tome d'algèbre 1 est consacré à l'algèbre générale. La première partie débute par la logique et les ensembles, qui sont des fondamentaux en mathématiques. Ensuite vous étudierez des ensembles particuliers : les nombres complexes, les entiers ainsi que les polynômes. Cette partie se termine par l'étude de quelques structures algébrique élémentaires , comme celles des groupe et anneaux .

Les efforts que vous devrez fournir sont importants : tout d'abord comprendre le cours, ensuite connaître par cœur les définitions, les théorèmes, les propositions... sans oublier de travailler les exemples et les démonstrations, qui permettent de bien assimiler les notions nouvelles et les mécanismes de raisonnement. Enfin, vous devrez passer autant de temps à pratiquer les mathématiques : il est indispensable de résoudre activement par vous-même des exercices, sans regarder les solutions. Pour vous aider, vous trouverez sur le site Exo7 toutes les vidéos correspondant à ce cours, ainsi que des exercices corrigés.
Au bout du chemin, le plaisir de découvrir de nouveaux univers, de chercher à résoudre des problèmes... et d'y parvenir. Bonne route !

Le contenue de ce livre est issu d'un large travail collectif. Les auteurs sont :

- Arnaud Bodin
- Niels Borne
- Marc Bourdon
- Guoting Chen
- Gilles Costantini
- Laura Desideri
- Abdellah Hanani
- Jean-Louis Rouget

Nous remercions l'équipe d'Exo7 qui a gracieusement mis les fichiers sources à la disposition du public. Les chapitres dans cet ouvrage ont étés partiellement éditer et compiler par Professeur El-Bachir pour couvrir le contenue du module d'algèbre 1 offert durant le premier semestre du programme de LMD du département de mathématiques de l'université Ferhat Abbas , Sétif, Algérie.

Sommaire

Chapitre 1
Logique et raisonnements

1.1. Motivation

- Il est important d'avoir un ***langage rigoureux***. La langue française est souvent ambigüe. Prenons l'exemple de la conjonction « *ou* » ; au restaurant « *fromage ou dessert* » signifie l'un ou l'autre mais pas les deux. Par contre si dans un jeu de carte on cherche « *les as ou les cœurs* » alors il ne faut pas exclure l'as de cœur. Autre exemple : que répondre à la question « *As-tu* 10 *euros en poche ?* » si l'on dispose de 15 euros ?
- Il y a des notions difficiles à expliquer avec des mots : par exemple la continuité d'une fonction est souvent expliquée par « *on trace le graphe sans lever le crayon* ». Il est clair que c'est une définition peu satisfaisante. Voici la définition mathématique de la continuité d'une fonction $f : I \to \mathbb{R}$ en un point $x_0 \in I$:

  $$\forall \epsilon > 0 \quad \exists \delta > 0 \quad \forall x \in I \quad (|x - x_0| < \delta \implies |f(x) - f(x_0)| < \epsilon).$$

  C'est le but de ce chapitre de rendre cette ligne plus claire ! C'est la ***logique***.
- Enfin les mathématiques tentent de ***distinguer le vrai du faux***. Par exemple « *Est-ce qu'une augmentation de* 20%*, puis de* 30% *est plus intéressante qu'une augmentation de* 50% *?* ». Vous pouvez penser « *oui* » ou « *non* », mais pour en être sûr il faut suivre une démarche logique qui mène à la conclusion. Cette démarche doit être convaincante pour vous mais aussi pour les autres. On parle de ***raisonnement***.

Les mathématiques sont un langage pour s'exprimer rigoureusement, adapté aux phénomènes complexes, qui rend les calculs exacts et vérifiables. Le raisonnement est le moyen de valider — ou d'infirmer — une hypothèse et de l'expliquer à autrui.

1.2. Logique

Assertions

Une **assertion** est une phrase soit vraie, soit fausse, pas les deux en même temps.
Exemples :

- « *Il pleut.* »
- « *Je suis plus grand que toi.* »
- « $2+2=4$ »
- « $2\times 3=7$ »
- « *Pour tout* $x\in\mathbb{R}$*, on a* $x^2\geqslant 0$. »
- « *Pour tout* $z\in\mathbb{C}$*, on a* $|z|=1$. »

Si P est une assertion et Q est une autre assertion, nous allons définir de nouvelles assertions construites à partir de P et de Q.

L'opérateur logique « *et* »

L'assertion « P ***et*** Q » est vraie si P est vraie et Q est vraie. L'assertion « P *et* Q » est fausse sinon.
On résume ceci en une **table de vérité** :

$P \setminus Q$	V	F
V	V	F
F	F	F

FIGURE 1.1 – Table de vérité de « P *et* Q »

Par exemple si P est l'assertion « *Cette carte est un as* » et Q l'assertion « *Cette carte est cœur* » alors l'assertion « P *et* Q » est vraie si la carte est l'as de cœur et est fausse pour toute autre carte.

L'opérateur logique « *ou* »

L'assertion « P ***ou*** Q » est vraie si l'une (au moins) des deux assertions P ou Q est vraie. L'assertion « P *ou* Q » est fausse si les deux assertions P et Q sont fausses.
On reprend ceci dans la table de vérité :

$P \setminus Q$	V	F
V	V	V
F	V	F

FIGURE 1.2 – Table de vérité de « P *ou* Q »

Si P est l'assertion « *Cette carte est un as* » et Q l'assertion « *Cette carte est cœur* » alors l'assertion « P *ou* Q » est vraie si la carte est un as ou bien un cœur (en particulier elle est vraie pour l'as de cœur).

Remarque.
Pour définir les opérateurs « *ou* », « *et* » on fait appel à une phrase en français utilisant les mots *ou*, *et* ! Les tables de vérités permettent d'éviter ce problème.

La négation « *non* »

L'assertion « ***non*** P » est vraie si P est fausse, et fausse si P est vraie.

P	V	F
non P	F	V

FIGURE 1.3 – Table de vérité de « *non* P »

L'implication $\Longrightarrow$

La définition mathématique est la suivante :

L'assertion « *(non P) ou Q* » est notée « $P \Longrightarrow Q$ ».

Sa table de vérité est donc la suivante :

$P \setminus Q$	V	F
V	V	F
F	V	V

FIGURE 1.4 – Table de vérité de « $P \Longrightarrow Q$ »

L'assertion « $P \Longrightarrow Q$ » se lit en français « P *implique* Q ».
Elle se lit souvent aussi « *si P est vraie alors Q est vraie* » ou « *si P alors Q* ».
Par exemple :

- « $0 \leqslant x \leqslant 25 \Longrightarrow \sqrt{x} \leqslant 5$ » est vraie (prendre la racine carrée).
- « $x \in]-\infty, -4[\Longrightarrow x^2 + 3x - 4 > 0$ » est vraie (étudier le binôme).
- « $\sin(\theta) = 0 \Longrightarrow \theta = 0$ » est fausse (regarder pour $\theta = 2\pi$ par exemple).
- « $2+2=5 \Longrightarrow \sqrt{2} = 2$ » est vraie ! Eh oui, si P est fausse alors l'assertion « $P \Longrightarrow Q$ » est toujours vraie.

L'équivalence $\Longleftrightarrow$

L'**équivalence** est définie par :

« $P \Longleftrightarrow Q$ » est l'assertion « $(P \Longrightarrow Q)$ *et* $(Q \Longrightarrow P)$ ».

On dira « P *est équivalent à* Q » ou « P *équivaut à* Q » ou « P *si et seulement si* Q ». Cette assertion est vraie lorsque P et Q sont vraies ou lorsque P et Q sont fausses. La table de vérité est :

$P \setminus Q$	V	F
V	V	F
F	F	V

FIGURE 1.5 – Table de vérité de « $P \iff Q$ »

Exemples :

- Pour $x, x' \in \mathbb{R}$, l'équivalence « $x \cdot x' = 0 \iff (x = 0$ *ou* $x' = 0)$ » est vraie.
- Voici une équivalence *toujours fausse* (quelque soit l'assertion P) : « $P \iff non(P)$ ».

On s'intéresse davantage aux assertions vraies qu'aux fausses, aussi dans la pratique et en dehors de ce chapitre on écrira « $P \iff Q$ » ou « $P \implies Q$ » uniquement lorsque ce sont des assertions vraies. Par exemple si l'on écrit « $P \iff Q$ » cela sous-entend « $P \iff Q$ *est vraie* ». Attention rien ne dit que P et Q soient vraies. Cela signifie que P et Q sont vraies en même temps ou fausses en même temps.

Proposition 1.
Soient P, Q, R trois assertions. Nous avons les équivalences (vraies) suivantes :

1. $P \iff$ non(non(P))
2. (P et Q) $\iff$ (Q et P)
3. (P ou Q) $\iff$ (Q ou P)
4. non(P et Q) $\iff$ (non P) ou (non Q)
5. non(P ou Q) $\iff$ (non P) et (non Q)
6. $\big(P$ et (Q ou $R)\big) \iff (P$ et $Q)$ ou (P et $R)$
7. $\big(P$ ou (Q et $R)\big) \iff (P$ ou $Q)$ et (P ou $R)$
8. « $P \implies Q$ » $\iff$ « non(Q) $\implies$ non(P) »

Démonstration. Voici des exemples de démonstrations :

4. Il suffit de comparer les deux assertions « *non*(P *et* Q) » et « (*non* P) *ou* (*non* Q) » pour toutes les valeurs possibles de P et Q. Par exemple si P est vrai et Q est vrai alors « P *et* Q » est vrai donc « *non*(P *et* Q) » est faux ; d'autre part (non P) est faux, (non Q) est faux donc « (*non* P) *ou* (*non* Q) » est faux. Ainsi dans ce premier cas les assertions sont toutes les deux fausses. On dresse ainsi les deux tables de vérités et comme elles sont égales les deux assertions sont équivalentes.

$P \setminus Q$	V	F
V	F	V
F	V	V

FIGURE 1.6 – Tables de vérité de « *non*$(P$ *et* $Q)$ » et de « $($*non* $P)$ *ou* $($*non* $Q)$ »

6. On fait la même chose mais il y a trois variables : P, Q, R. On compare donc les tables de vérité d'abord dans le cas où P est vrai (à gauche), puis dans le cas où P est faux (à droite). Dans les deux cas les deux assertions « $\big(P$ *et* $(Q$ *ou* $R)\big)$ » et « $(P$ *et* $Q)$ *ou* $(P$ *et* $R)$ » ont la même table de vérité donc les assertions sont équivalentes.

$Q \setminus R$	V	F
V	V	V
F	V	F

$Q \setminus R$	V	F
V	F	F
F	F	F

8. Par définition, l'implication « $P \implies Q$ » est l'assertion « *(non P) ou Q* ». Donc l'implication « *non*$(Q) \implies$ *non*(P) » est équivalente à « *non*$($*non*$(Q))$ *ou non*(P) » qui équivaut encore à « Q *ou non*(P) » et donc est équivalente à « $P \implies Q$ ». On aurait aussi pu encore une fois dresser les deux tables de vérité et voir qu'elles sont égales.

□

Quantificateurs

Le quantificateur $\forall$: « *pour tout* »

Une assertion P peut dépendre d'un paramètre x, par exemple « $x^2 \geqslant 1$ », l'assertion $P(x)$ est vraie ou fausse selon la valeur de x.
L'assertion

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

est une assertion vraie lorsque les assertions $P(x)$ sont vraies pour tous les éléments x de l'ensemble E.
On lit « *Pour tout x appartenant à E,* $P(x)$ », sous-entendu « *Pour tout x appartenant à E,* $P(x)$ *est vraie* ».
Par exemple :

- « $\forall x \in [1, +\infty[\quad (x^2 \geqslant 1)$ » est une assertion vraie.
- « $\forall x \in \mathbb{R} \quad (x^2 \geqslant 1)$ » est une assertion fausse.
- « $\forall n \in \mathbb{N} \quad n(n+1)$ *est divisible par* 2 » est vraie.

Le quantificateur $\exists$: « *il existe* »

L'assertion

$$\exists x \in E \quad P(x)$$

est une assertion vraie lorsque l'on peut trouver au moins un x de E pour lequel $P(x)$ est vraie. On lit « *il existe x appartenant à E tel que $P(x)$ (soit vraie)* ».
Par exemple :

- « $\exists x \in \mathbb{R} \quad (x(x-1) < 0)$ » est vraie (par exemple $x = \frac{1}{2}$ vérifie bien la propriété).
- « $\exists n \in \mathbb{N} \quad n^2 - n > n$ » est vraie (il y a plein de choix, par exemple $n = 3$ convient, mais aussi $n = 10$ ou même $n = 100$, un seul suffit pour dire que l'assertion est vraie).
- « $\exists x \in \mathbb{R} \quad (x^2 = -1)$ » est fausse (aucun réel au carré ne donnera un nombre négatif).

La négation des quantificateurs

La négation de « $\forall x \in E \quad P(x)$ » est « $\exists x \in E \quad$ *non* $P(x)$ » .

Par exemple la négation de « $\forall x \in [1, +\infty[\quad (x^2 \geqslant 1)$ » est l'assertion « $\exists x \in [1, +\infty[\quad (x^2 < 1)$ ». En effet la négation de $x^2 \geqslant 1$ est non$(x^2 \geqslant 1)$ mais s'écrit plus simplement $x^2 < 1$.

La négation de « $\exists x \in E \quad P(x)$ » est « $\forall x \in E \quad$ *non* $P(x)$ ».

Voici des exemples :

- La négation de « $\exists z \in \mathbb{C} \quad (z^2 + z + 1 = 0)$ » est « $\forall z \in \mathbb{C} \quad (z^2 + z + 1 \neq 0)$ ».
- La négation de « $\forall x \in \mathbb{R} \quad (x + 1 \in \mathbb{Z})$ » est « $\exists x \in \mathbb{R} \quad (x + 1 \notin \mathbb{Z})$ ».
- Ce n'est pas plus difficile d'écrire la négation de phrases complexes. Pour l'assertion :
$$\forall x \in \mathbb{R} \quad \exists y > 0 \quad (x + y > 10)$$
sa négation est
$$\exists x \in \mathbb{R} \quad \forall y > 0 \quad (x + y \leqslant 10).$$

Remarques

L'ordre des quantificateurs est très important. Par exemple les deux phrases logiques
$$\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \quad (x + y > 0) \qquad \text{et} \qquad \exists y \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad (x + y > 0).$$
sont différentes. La première est vraie, la seconde est fausse. En effet une phrase logique se lit de gauche à droite, ainsi la première phrase affirme « *Pour tout réel x, il existe un réel y (qui peut donc dépendre de x) tel que $x + y > 0$.* » (par exemple on peut prendre $y = |x| + 1$). C'est donc une phrase vraie. Par contre la deuxième se lit : « *Il existe un réel y, tel que pour tout réel x, $x + y > 0$.* » Cette phrase est fausse, cela ne peut pas être le même y qui convient pour tous les x !
On retrouve la même différence dans les phrases en français suivantes. Voici une phrase vraie « *Pour toute personne, il existe un numéro de téléphone* », bien sûr le numéro dépend de la personne. Par contre cette phrase est fausse : « *Il existe un numéro, pour toutes les personnes* ». Ce serait le même numéro pour tout le monde !

Terminons avec d'autres remarques.

- Quand on écrit « $\exists x \in \mathbb{R} \quad (f(x) = 0)$ » cela signifie juste qu'il existe un réel pour lequel f s'annule. Rien ne dit que ce x est unique. Dans un premier temps vous pouvez lire la phrase ainsi : « *il existe* au moins *un réel* x *tel que* $f(x) = 0$ ». Afin de préciser que f s'annule en une unique valeur, on rajoute un point d'exclamation :
$$\exists ! \, x \in \mathbb{R} \quad (f(x) = 0).$$
- Pour la négation d'une phrase logique, il n'est pas nécessaire de savoir si la phrase est fausse ou vraie. Le procédé est algorithmique : on change le « *pour tout* » en « *il existe* » et inversement, puis on prend la négation de l'assertion P.
- Pour la négation d'une proposition, il faut être précis : la négation de l'inégalité stricte « $<$ » est l'inégalité large « $\geqslant$ », et inversement.
- Les quantificateurs ne sont pas des abréviations. Soit vous écrivez une phrase en français : « *Pour tout réel* x*, si* $f(x) = 1$ *alors* $x \geqslant 0$. » , soit vous écrivez la phrase logique :
$$\forall x \in \mathbb{R} \quad (f(x) = 1 \implies x \geqslant 0).$$
Mais surtout n'écrivez pas « $\forall x$ *réel, si* $f(x) = 1 \implies$ *x positif ou nul* ». Enfin, pour passer d'une ligne à l'autre d'un raisonnement, préférez plutôt « *donc* » à « $\implies$ ».
- Il est défendu d'écrire $\nexists, \not\Longrightarrow$. Ces symboles n'existent pas !

Mini-exercices.

1. Écrire la table de vérité du « *ou exclusif* ». (C'est le *ou* dans la phrase « *fromage ou dessert* », l'un ou l'autre mais pas les deux.)
2. Écrire la table de vérité de « *non (P et Q)* ». Que remarquez vous ?
3. Écrire la négation de « $P \implies Q$ ».
4. Démontrer les assertions restantes de la proposition 1.
5. Écrire la négation de « $\big(P$ *et* $(Q$ *ou* $R)\big)$ ».
6. Écrire à l'aide des quantificateurs la phrase suivante : « *Pour tout nombre réel, son carré est positif* ». Puis écrire la négation.
7. Mêmes questions avec les phrases : « *Pour chaque réel, je peux trouver un entier relatif tel que leur produit soit strictement plus grand que* 1 ». Puis « *Pour tout entier n, il existe un unique réel* x *tel que* $\exp(x)$ *égale n* ».

1.3. Raisonnements

Voici des méthodes classiques de raisonnements.

Raisonnement direct

On veut montrer que l'assertion « $P \implies Q$ » est vraie. On suppose que P est vraie et on montre qu'alors Q est vraie. C'est la méthode à laquelle vous êtes le plus habitué.

Exemple 1.
Montrer que si $a, b \in \mathbb{Q}$ alors $a+b \in \mathbb{Q}$.

Démonstration. Prenons $a \in \mathbb{Q}$, $b \in \mathbb{Q}$. Rappelons que les rationnels $\mathbb{Q}$ sont l'ensemble des réels s'écrivant $\frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.
Alors $a = \frac{p}{q}$ pour un certain $p \in \mathbb{Z}$ et un certain $q \in \mathbb{N}^*$. De même $b = \frac{p'}{q'}$ avec $p' \in \mathbb{Z}$ et $q' \in \mathbb{N}^*$. Maintenant

$$a+b = \frac{p}{q} + \frac{p'}{q'} = \frac{pq'+qp'}{qq'}.$$

Or le numérateur $pq'+qp'$ est bien un élément de $\mathbb{Z}$; le dénominateur qq' est lui un élément de $\mathbb{N}^*$. Donc $a+b$ s'écrit bien de la forme $a+b = \frac{p''}{q''}$ avec $p'' \in \mathbb{Z}, q'' \in \mathbb{N}^*$. Ainsi $a+b \in \mathbb{Q}$. □

Cas par cas

Si l'on souhaite vérifier une assertion $P(x)$ pour tous les x dans un ensemble E, on montre l'assertion pour les x dans une partie A de E, puis pour les x n'appartenant pas à A. C'est la méthode de **disjonction** ou du **cas par cas**.

Exemple 2.
Montrer que pour tout $x \in \mathbb{R}$, $|x-1| \leqslant x^2 - x + 1$.

Démonstration. Soit $x \in \mathbb{R}$. Nous distinguons deux cas.
Premier cas : $x \geqslant 1$. Alors $|x-1| = x-1$. Calculons alors $x^2 - x + 1 - |x-1|$.

$$\begin{aligned} x^2 - x + 1 - |x-1| &= x^2 - x + 1 - (x-1) \\ &= x^2 - 2x + 2 \\ &= (x-1)^2 + 1 \geqslant 0. \end{aligned}$$

Ainsi $x^2 - x + 1 - |x-1| \geqslant 0$ et donc $x^2 - x + 1 \geqslant |x-1|$.
Deuxième cas : $x < 1$. Alors $|x-1| = -(x-1)$. Nous obtenons $x^2 - x + 1 - |x-1| = x^2 - x + 1 + (x-1) = x^2 \geqslant 0$. Et donc $x^2 - x + 1 \geqslant |x-1|$.
Conclusion. Dans tous les cas $|x-1| \leqslant x^2 - x + 1$. □

Contraposée

Le raisonnement par **contraposition** est basé sur l'équivalence suivante (voir la proposition 1) :

L'assertion « $P \implies Q$ » est équivalente à « $non(Q) \implies non(P)$ ».

Donc si l'on souhaite montrer l'assertion « $P \implies Q$ », on montre en fait que si non(Q) est vraie alors non(P) est vraie.

Exemple 3.
Soit $n \in \mathbb{N}$. Montrer que si n^2 est pair alors n est pair.

Démonstration. Nous supposons que n n'est pas pair. Nous voulons montrer qu'alors n^2 n'est pas pair. Comme n n'est pas pair, il est impair et donc il existe $k \in \mathbb{N}$ tel que $n = 2k+1$. Alors $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2\ell+1$ avec $\ell = 2k^2+2k \in \mathbb{N}$. Et donc n^2 est impair.
Conclusion : nous avons montré que si n est impair alors n^2 est impair. Par contraposition ceci est équivalent à : si n^2 est pair alors n est pair. □

Absurde

Le **raisonnement par l'absurde** pour montrer « $P \implies Q$ » repose sur le principe suivant : on suppose à la fois que P est vraie et que Q est fausse et on cherche une contradiction. Ainsi si P est vraie alors Q doit être vraie et donc « $P \implies Q$ » est vraie.

Exemple 4.
Soient $a, b \geqslant 0$. Montrer que si $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a = b$.

Démonstration. Nous raisonnons par l'absurde en supposant que $\frac{a}{1+b} = \frac{b}{1+a}$ **et** $a \neq b$. Comme $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a(1+a) = b(1+b)$ donc $a + a^2 = b + b^2$ d'où $a^2 - b^2 = b - a$. Cela conduit à $(a-b)(a+b) = -(a-b)$. Comme $a \neq b$ alors $a - b \neq 0$ et donc en divisant par $a-b$ on obtient $a + b = -1$. La somme des deux nombres positifs a et b ne peut être négative. Nous obtenons une contradiction.
Conclusion : si $\frac{a}{1+b} = \frac{b}{1+a}$ alors $a = b$. □

Dans la pratique, on peut choisir indifféremment entre un raisonnement par contraposition ou par l'absurde. Attention cependant de bien préciser quel type de raisonnement vous choisissez et surtout de ne pas changer en cours de rédaction !

Contre-exemple

Si l'on veut montrer qu'une assertion du type « $\forall x \in E \quad P(x)$ » est vraie alors pour chaque x de E il faut montrer que $P(x)$ est vraie. Par contre pour montrer que cette assertion est fausse alors il suffit de trouver $x \in E$ tel que $P(x)$ soit fausse. (Rappelez-vous la négation de « $\forall x \in E \quad P(x)$ » est « $\exists x \in E \quad non\ P(x)$ ».) Trouver un tel x c'est trouver un **contre-exemple** à l'assertion « $\forall x \in E \quad P(x)$ ».

Exemple 5.
Montrer que l'assertion suivante est fausse « *Tout entier positif est somme de trois carrés* ».
(Les carrés sont les 0^2, 1^2, 2^2, 3^2,... Par exemple $6 = 2^2 + 1^2 + 1^2$.)

Démonstration. Un contre-exemple est 7 : les carrés inférieurs à 7 sont 0, 1, 4 mais avec trois de ces nombres on ne peut faire 7. □

Récurrence

Le **principe de récurrence** permet de montrer qu'une assertion $P(n)$, dépendant de n, est vraie pour tout $n \in \mathbb{N}$. La démonstration par récurrence se déroule en trois étapes : lors de l'***initialisation*** on prouve $P(0)$. Pour l'étape d'***hérédité***, on suppose $n \geqslant 0$ donné avec $P(n)$ vraie, et on démontre alors que l'assertion $P(n+1)$ au rang suivant est vraie. Enfin dans la ***conclusion***, on rappelle que par le principe de récurrence $P(n)$ est vraie pour tout $n \in \mathbb{N}$.

Exemple 6.
Montrer que pour tout $n \in \mathbb{N}$, $2^n > n$.

Démonstration. Pour $n \geqslant 0$, notons $P(n)$ l'assertion suivante :

$$2^n > n.$$

Nous allons démontrer par récurrence que $P(n)$ est vraie pour tout $n \geqslant 0$.
Initialisation. Pour $n = 0$ nous avons $2^0 = 1 > 0$. Donc $P(0)$ est vraie.
Hérédité. Fixons $n \geqslant 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie.

$$\begin{aligned} 2^{n+1} = 2^n + 2^n &> n + 2^n \qquad \text{car par } P(n) \text{ nous savons } 2^n > n, \\ &> n + 1 \qquad \text{car } 2^n \geqslant 1. \end{aligned}$$

Donc $P(n+1)$ est vraie.
Conclusion. Par le principe de récurrence $P(n)$ est vraie pour tout $n \geqslant 0$, c'est-à-dire $2^n > n$ pour tout $n \geqslant 0$. □

Remarques :

- La rédaction d'une récurrence est assez rigide. Respectez scrupuleusement la rédaction proposée : donnez un nom à l'assertion que vous souhaitez montrer (ici $P(n)$), respectez les trois étapes (même si souvent l'étape d'initialisation est très facile). En particulier méditez et conservez la première ligne de l'hérédité « Fixons $n \geqslant 0$. Supposons que $P(n)$ soit vraie. Nous allons montrer que $P(n+1)$ est vraie. »
- Si on doit démontrer qu'une propriété est vraie pour tout $n \geqslant n_0$, alors on commence l'initialisation au rang n_0.
- Le principe de récurrence est basé sur la construction de l'ensemble $\mathbb{N}$. En effet un des axiomes pour définir $\mathbb{N}$ est le suivant : « *Soit A une partie de $\mathbb{N}$ qui contient 0 et telle que si $n \in A$ alors $n+1 \in A$. Alors $A = \mathbb{N}$* ».

Mini-exercices.

1. (Raisonnement direct) Soient $a, b \in \mathbb{R}_+$. Montrer que si $a \leqslant b$ alors $a \leqslant \frac{a+b}{2} \leqslant b$ et $a \leqslant \sqrt{ab} \leqslant b$.
2. (Cas par cas) Montrer que pour tout $n \in \mathbb{N}$, $n(n+1)$ est divisible par 2 (distinguer les n pairs des n impairs).
3. (Contraposée ou absurde) Soient $a, b \in \mathbb{Z}$. Montrer que si $b \neq 0$ alors $a + b\sqrt{2} \notin \mathbb{Q}$. (On utilisera que $\sqrt{2} \notin \mathbb{Q}$.)
4. (Absurde) Soit $n \in \mathbb{N}^*$. Montrer que $\sqrt{n^2+1}$ n'est pas un entier.
5. (Contre-exemple) Est-ce que pour tout $x \in \mathbb{R}$ on a $x < 2 \implies x^2 < 4$?
6. (Récurrence) Montrer que pour tout $n \geqslant 1$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.
7. (Récurrence) Fixons un réel $x \geqslant 0$. Montrer que pour tout entier $n \geqslant 1$, $(1+x)^n \geqslant 1 + nx$.

Ensembles, applications et relations

Chapitre 2

2.1. Ensembles

Définir des ensembles

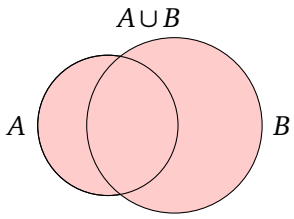
- On va définir informellement ce qu'est un ensemble : un **ensemble** est une collection d'éléments.
- Exemples :
$$\{0,1\}, \quad \{\text{rouge}, \text{noir}\}, \quad \{0,1,2,3,\ldots\} = \mathbb{N}.$$
- Un ensemble particulier est l'**ensemble vide**, noté $\varnothing$ qui est l'ensemble ne contenant aucun élément.
- On note
$$\boxed{x \in E}$$
si x est un élément de E, et $x \notin E$ dans le cas contraire.
- Voici une autre façon de définir des ensembles : une collection d'éléments qui vérifient une propriété.
- Exemples :
$$\{x \in \mathbb{R} \mid |x-2| < 1\}, \quad \{z \in \mathbb{C} \mid z^5 = 1\}, \quad \{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\} = [0,1].$$

Inclusion, union, intersection, complémentaire, différence

- L'**inclusion**. $E \subset F$ si tout élément de E est aussi un élément de F. Autrement dit : $\forall x \in E\ (x \in F)$. On dit alors que E est un **sous-ensemble** de F ou une **partie** de F.
- L'**égalité**. $E = F$ si et seulement si $E \subset F$ et $F \subset E$.
- **Ensemble des parties** de E. On note $\mathscr{P}(E)$ l'ensemble des parties de E. Par exemple si $E = \{1,2,3\}$:
$$\mathscr{P}(\{1,2,3\}) = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}.$$
- **Union**. Pour $A, B \subset E$,

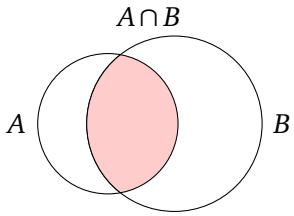
$$\boxed{A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}}$$

Le « *ou* » n'est pas exclusif : x peut appartenir à A et à B en même temps.



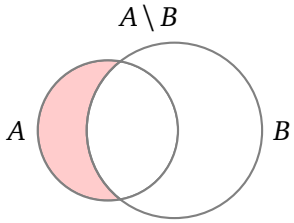
- **Intersection**.

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



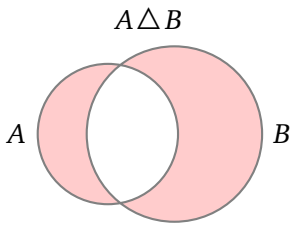
- **Différence.** Pour $A, B \subset E$, la différence A moins B, dénotée $A \setminus B$, qui est l'ensemble de tous les éléments appartenant à A mais pas à B

$$\boxed{A \setminus B = \{x \in E | x \in A \textbf{ et } x \notin B\}}$$



- **Différence symétrique.** Pour $A, B \subset E$, la différence symétrique entre A et B est

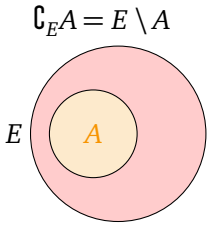
$$\boxed{A \triangle B = (A \setminus B) \cup (B \setminus A)}$$



- **Complémentaire**. Si $A \subset E$,

$$\boxed{\complement_E A = E \setminus A = \{x \in E \mid x \notin A\}}$$

On le note aussi $E \setminus A$ et juste $\complement A$ s'il n'y a pas d'ambiguïté (et parfois aussi A^c ou $\overline{A}$).



Considérons les ensembles suivants :
(a) Si X est un univers et $A \subset X$, alors $A \setminus \varnothing = A$ et $A \setminus X = \varnothing$.
(b) Si $X = \mathbb{R}$, $A = (0,1)$ et $B = (\frac{1}{3}, 5]$, alors $A \setminus B = (0, \frac{1}{3}]$.
(c) Si $X = \mathbb{R}^2$, $A = \{(x,0) : x \in \mathbb{R}\}$ et $B = \{(x,1) : x \in \mathbb{R}\}$, alors $A \setminus B = A$.

Règles de calculs

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

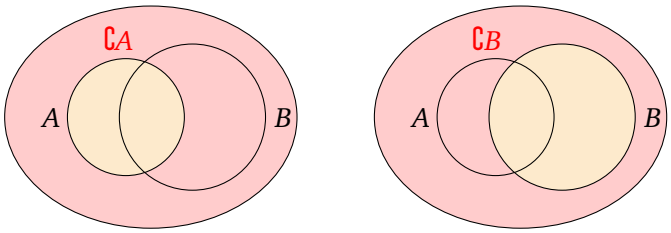
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap B) \cap C$ (on peut donc écrire $A \cap B \cap C$ sans ambigüité)
- $A \cap \varnothing = \varnothing$, $A \cap A = A$, $A \subset B \iff A \cap B = A$

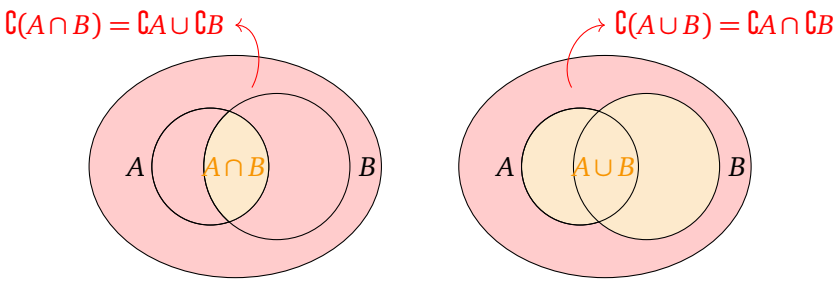
- $A \cup B = B \cup A$
- $A \cup (B \cup C) = (A \cup B) \cup C$ (on peut donc écrire $A \cup B \cup C$ sans ambiguïté)
- $A \cup \varnothing = A$, $A \cup A = A$, $A \subset B \iff A \cup B = B$

- $\boxed{A \cap (B \cup C) = (A \cap B) \cup (A \cap C)}$
- $\boxed{A \cup (B \cap C) = (A \cup B) \cap (A \cup C)}$

- $\complement\big(\complement A\big) = A$ et donc $A \subset B \iff \complement B \subset \complement A$
- $\complement(A \cap B) = \complement A \cup \complement B$
- $\complement(A \cup B) = \complement A \cap \complement B$

Voici les dessins pour les deux dernières assertions.





Les preuves sont pour l'essentiel une reformulation des opérateurs logiques, en voici quelques-unes :

- Preuve de $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$: $x\in A\cap(B\cup C)\iff x\in A$ et $x\in(B\cup C)\iff x\in A$ et $(x\in B$ ou $x\in C)\iff(x\in A$ et $x\in B)$ ou $(x\in A$ et $x\in C)\iff(x\in A\cap B)$ ou $(x\in A\cap C)\iff x\in(A\cap B)\cup(A\cap C)$.
- Preuve de $\complement(A\cap B)=\complement A\cup\complement B$: $x\in\complement(A\cap B)\iff x\notin(A\cap B)\iff$ non$\big(x\in A\cap B\big)\iff$ non$\big(x\in A$ et $x\in B\big)\iff$ non$(x\in A)$ ou non$(x\in B)\iff x\notin A$ ou $x\notin B\iff x\in\complement A\cup\complement B$.

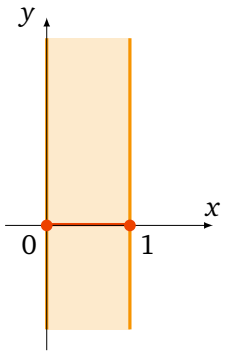
Remarquez que l'on repasse aux éléments pour les preuves.

Produit cartésien

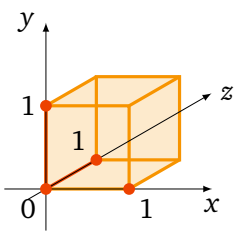
Soient E et F deux ensembles. Le **produit cartésien**, noté $E\times F$, est l'ensemble des couples (x,y) où $x\in E$ et $y\in F$.

Exemple 1.

1. Vous connaissez $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}=\big\{(x,y)\mid x,y\in\mathbb{R}\big\}$.
2. Autre exemple $[0,1]\times\mathbb{R}=\big\{(x,y)\mid 0\leqslant x\leqslant 1,y\in\mathbb{R}\big\}$



3. $[0,1]\times[0,1]\times[0,1]=\big\{(x,y,z)\mid 0\leqslant x,y,z\leqslant 1\big\}$



Cardinal

Définition 1.
Un ensemble E est **fini** s'il existe un entier $n \in \mathbb{N}$ et une bijection de E vers $\{1, 2, \dots, n\}$. Cet entier n est unique et s'appelle le **cardinal** de E (ou le **nombre d'éléments**) et est noté $\operatorname{Card} E$.

Quelques exemples :

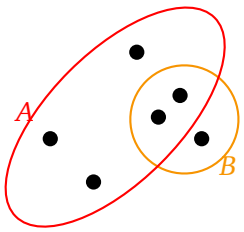
1. $E = \{\text{rouge}, \text{noir}\}$ est en bijection avec $\{1, 2\}$ et donc est de cardinal 2.
2. $\mathbb{N}$ n'est pas un ensemble fini.
3. Par définition le cardinal de l'ensemble vide est 0.

Enfin quelques propriétés :

1. Si A est un ensemble fini et $B \subset A$ alors B est aussi un ensemble fini et $\operatorname{Card} B \leqslant \operatorname{Card} A$.
2. Si A, B sont des ensembles finis disjoints (c'est-à-dire $A \cap B = \varnothing$) alors $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$.
3. Si A est un ensemble fini et $B \subset A$ alors $\operatorname{Card}(A \setminus B) = \operatorname{Card} A - \operatorname{Card} B$. En particulier si $B \subset A$ et $\operatorname{Card} A = \operatorname{Card} B$ alors $A = B$.
4. Enfin pour A, B deux ensembles finis quelconques :

$$\boxed{\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)}$$

Voici une situation où s'applique la dernière propriété :



La preuve de la dernière propriété utilise la décomposition

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

Les ensembles A et $B \setminus (A \cap B)$ sont disjoints, donc

$$\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card}\big(B \setminus (A \cap B)\big) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)$$

par la propriété 2, puis la propriété 3.

Nombres de sous-ensembles

Soit E un ensemble fini de cardinal n.

Proposition 1.
Il y a $2^{\operatorname{Card} E}$ *sous-ensembles de* E *:*

$$\boxed{\operatorname{Card} \mathscr{P}(E) = 2^n}$$

Exemple 2.
Si $E = \{1,2,3,4,5\}$ alors $\mathscr{P}(E)$ a $2^5 = 32$ parties. C'est un bon exercice de les énumérer :

- l'ensemble vide : $\varnothing$,
- 5 singletons : $\{1\}, \{2\}, \ldots$,
- 10 paires : $\{1,2\}, \{1,3\}, \ldots, \{2,3\}, \ldots$,
- 10 triplets : $\{1,2,3\}, \ldots$,
- 5 ensembles à 4 éléments : $\{1,2,3,4\}, \{1,2,3,5\}, \ldots$,
- et E tout entier : $\{1,2,3,4,5\}$.

Démonstration. Encore une récurrence sur $n = \operatorname{Card} E$.

- Si $n = 1$, $E = \{a\}$ est un singleton, les deux sous-ensembles sont : $\varnothing$ et E.
- Supposons que la proposition soit vraie pour $n \geqslant 1$ fixé. Soit E un ensemble à $n+1$ éléments. On fixe $a \in E$. Il y a deux sortes de sous-ensembles de E :
  - — les sous-ensembles A qui ne contiennent pas a : ce sont les sous-ensembles $A \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y en a 2^n.
  - — les sous-ensembles A qui contiennent a : ils sont de la forme $A = \{a\} \cup A'$ avec $A' \subset E \setminus \{a\}$. Par l'hypothèse de récurrence il y a 2^n sous-ensembles A' possibles et donc aussi 2^n sous-ensembles A.

  Le bilan : $2^n + 2^n = 2^{n+1}$ parties $A \subset E$.
- Par le principe de récurrence, nous avons prouvé que si $\operatorname{Card} E = n$ alors on a $\operatorname{Card} \mathscr{P}(E) = 2^n$.

□

Mini-exercices.

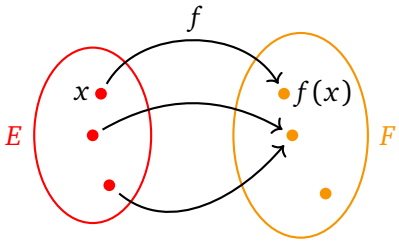
1. En utilisant les définitions, montrer : $A \neq B$ si et seulement s'il existe $a \in A \setminus B$ ou $b \in B \setminus A$.
2. Énumérer $\mathscr{P}(\{1,2,3,4\})$.
3. Montrer $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $\complement(A \cup B) = \complement A \cap \complement B$.
4. Énumérer $\{1,2,3\} \times \{1,2,3,4\}$.
5. Représenter les sous-ensembles de $\mathbb{R}^2$ suivants : $\big(]0,1[\cup [2,3[\big) \times [-1,1]$, $\big(\mathbb{R} \setminus (]0,1[\cup [2,3[\big) \times \big((\mathbb{R} \setminus [-1,1]) \cap [0,2]\big)$.

2.2. Applications

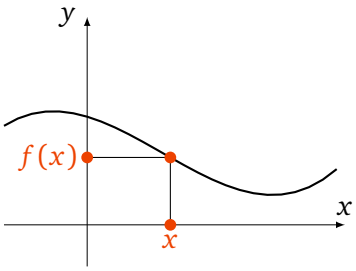
Définitions

- Une **application** (ou une **fonction**) $f : E \to F$, c'est la donnée pour chaque élément $x \in E$ d'un unique élément de F noté $f(x)$.

  Nous représenterons les applications par deux types d'illustrations : les ensembles « patates », l'ensemble de départ (et celui d'arrivée) est schématisé par un ovale ses éléments par des points. L'association $x \mapsto f(x)$ est représentée par une flèche.

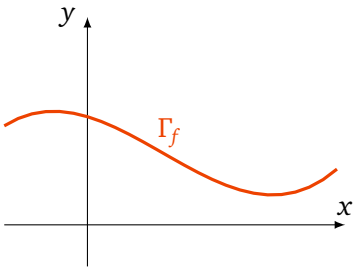


  L'autre représentation est celle des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ (ou des sous-ensembles de $\mathbb{R}$). L'ensemble de départ $\mathbb{R}$ est représenté par l'axe des abscisses et celui d'arrivée par l'axe des ordonnées. L'association $x \mapsto f(x)$ est représentée par le point $(x, f(x))$.

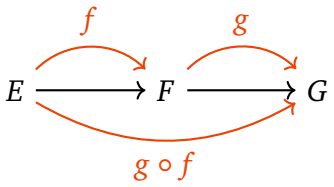


- **Égalité**. Deux applications $f, g : E \to F$ sont égales si et seulement si pour tout $x \in E$, $f(x) = g(x)$. On note alors $f = g$.
- Le **graphe** de $f : E \to F$ est

$$\boxed{\Gamma_f = \left\{\big(x, f(x)\big) \in E \times F \mid x \in E\right\}}$$



- **Composition**. Soient $f : E \to F$ et $g : F \to G$ alors $g \circ f : E \to G$ est l'application définie par $g \circ f(x) = g\big(f(x)\big)$.



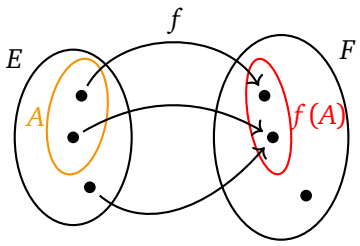
Exemple 3.

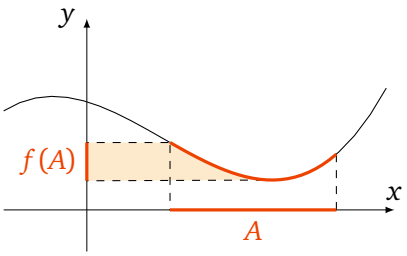
1. L'**identité**, $\mathrm{id}_E : E \to E$ est simplement définie par $x \mapsto x$ et sera très utile dans la suite.
2. Définissons f, g ainsi
$$\begin{array}{ccccc} f & : &]0,+\infty[& \longrightarrow &]0,+\infty[\\ & & x & \longmapsto & \frac{1}{x} \end{array} \quad , \quad \begin{array}{ccccc} g & : &]0,+\infty[& \longrightarrow & \mathbb{R} \\ & & x & \longmapsto & \frac{x-1}{x+1} \end{array} .$$
Alors $g \circ f :]0,+\infty[\to \mathbb{R}$ vérifie pour tout $x \in]0,+\infty[$:
$$g \circ f(x) = g\big(f(x)\big) = g\left(\frac{1}{x}\right) = \frac{\frac{1}{x}-1}{\frac{1}{x}+1} = \frac{1-x}{1+x} = -g(x).$$

Image directe, image réciproque

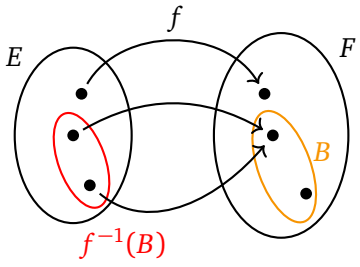
Soient E, F deux ensembles.

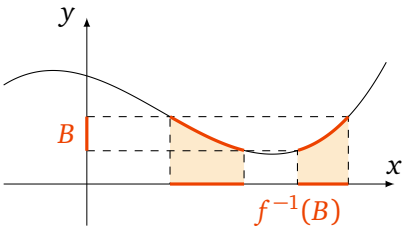
Définition 2.
Soit $A \subset E$ et $f : E \to F$, l'**image directe** de A par f est l'ensemble
$$\boxed{f(A) = \big\{f(x) \mid x \in A\big\}}$$





Définition 3.
Soit $B \subset F$ et $f : E \to F$, l'**image réciproque** de B par f est l'ensemble
$$\boxed{f^{-1}(B) = \big\{x \in E \mid f(x) \in B\big\}}$$





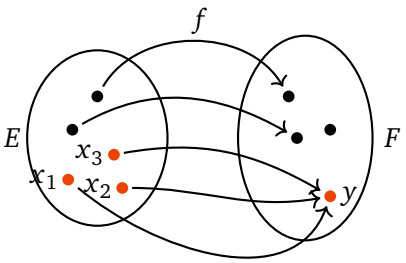
Remarque.
Ces notions sont plus difficiles à maîtriser qu'il n'y paraît !

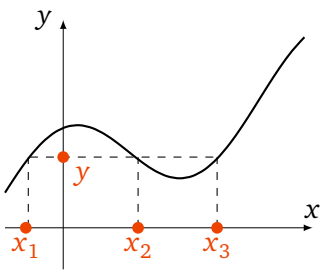
- $f(A)$ est un sous-ensemble de F, $f^{-1}(B)$ est un sous-ensemble de E.
- La notation « $f^{-1}(B)$ » est un tout, rien ne dit que f est un fonction bijective (voir plus loin). L'image réciproque existe quelque soit la fonction.
- L'image directe d'un singleton $f(\{x\}) = \{f(x)\}$ est un singleton. Par contre l'image réciproque d'un singleton $f^{-1}(\{y\})$ dépend de f. Cela peut être un singleton, un ensemble à plusieurs éléments ; mais cela peut-être E tout entier (si f est une fonction constante) ou même l'ensemble vide (si aucune image par f ne vaut y).

Antécédents

Fixons $y \in F$. Tout élément $x \in E$ tel que $f(x) = y$ est un **antécédent** de y.
En termes d'image réciproque l'ensemble des antécédents de y est $f^{-1}(\{y\})$.

Sur les dessins suivants, l'élément y admet 3 antécédents par f. Ce sont x_1, x_2, x_3.





Mini-exercices.

1. Pour deux applications $f, g : E \to F$, quelle est la négation de $f = g$?
2. Représenter le graphe de $f : \mathbb{N} \to \mathbb{R}$ définie par $n \mapsto \frac{4}{n+1}$.
3. Soient $f, g, h : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = x^2$, $g(x) = 2x + 1$, $h(x) = x^3 - 1$. Calculer $f \circ (g \circ h)$ et $(f \circ g) \circ h$.
4. Pour la fonction $f : \mathbb{R} \to \mathbb{R}$ définie par $x \mapsto x^2$ représenter et calculer les ensembles suivants : $f([0,1[)$, $f(\mathbb{R})$, $f(]-1,2[)$, $f^{-1}([1,2[)$, $f^{-1}([-1,1])$, $f^{-1}(\{3\})$, $f^{-1}(\mathbb{R} \setminus \mathbb{N})$.

2.3. Injection, surjection, bijection

Injection, surjection

Soit E, F deux ensembles et $f : E \to F$ une application.

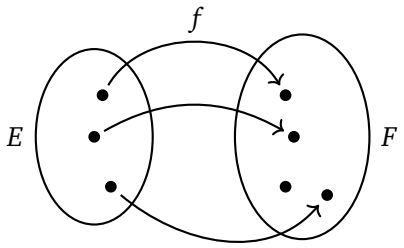
Définition 4.
f est **injective** si pour tout $x, x' \in E$ avec $f(x) = f(x')$ alors $x = x'$. Autrement dit :

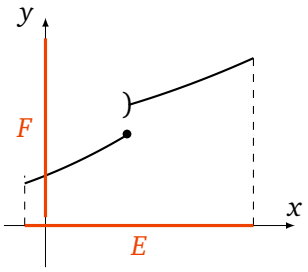
$$\boxed{\forall x, x' \in E \quad \big(f(x) = f(x') \implies x = x'\big)}$$

Définition 5.
f est **surjective** si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$. Autrement dit :

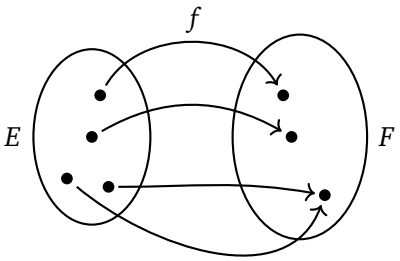
$$\boxed{\forall y \in F \quad \exists x \in E \quad \big(y = f(x)\big)}$$

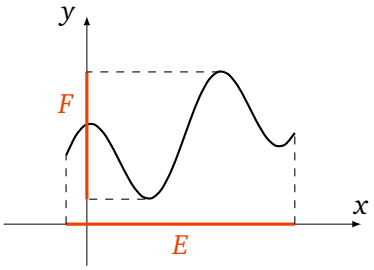
Une autre formulation : f est surjective si et seulement si $f(E) = F$.
Les applications f représentées sont injectives :





Les applications f représentées sont surjectives :

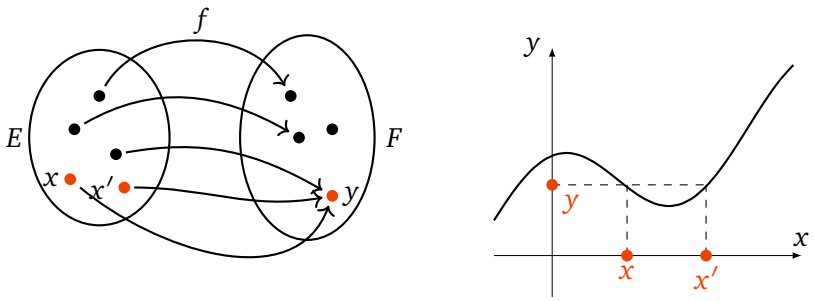




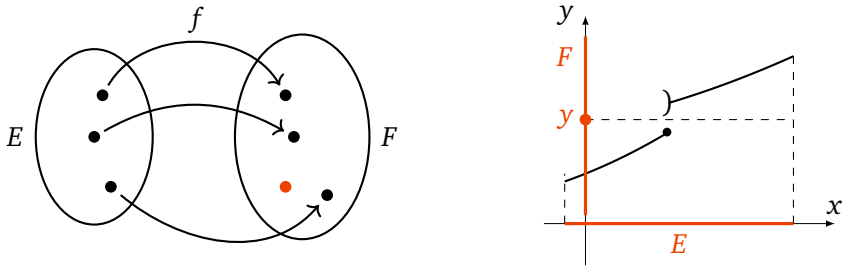
Remarque.
Encore une fois ce sont des notions difficiles à appréhender. Une autre façon de formuler l'injectivité et la surjectivité est d'utiliser les antécédents.

- f est injective si et seulement si tout élément y de F a *au plus* un antécédent (et éventuellement aucun).
- f est surjective si et seulement si tout élément y de F a *au moins* un antécédent.

Remarque.
Voici deux fonctions non injectives :



Ainsi que deux fonctions non surjectives :



Exemple 4.

1. Soit $f_1 : \mathbb{N} \to \mathbb{Q}$ définie par $f_1(x) = \frac{1}{1+x}$. Montrons que f_1 est injective : soit $x, x' \in \mathbb{N}$ tels que $f_1(x) = f_1(x')$. Alors $\frac{1}{1+x} = \frac{1}{1+x'}$, donc $1 + x = 1 + x'$ et donc $x = x'$. Ainsi f_1 est injective.

   Par contre f_1 n'est pas surjective. Il s'agit de trouver un élément y qui n'a pas d'antécédent par f_1. Ici il est facile de voir que l'on a toujours $f_1(x) \leqslant 1$ et donc par exemple $y = 2$ n'a pas d'antécédent. Ainsi f_1 n'est pas surjective.

2. Soit $f_2 : \mathbb{Z} \to \mathbb{N}$ définie par $f_2(x) = x^2$. Alors f_2 n'est pas injective. En effet on peut trouver deux éléments $x, x' \in \mathbb{Z}$ différents tels que $f_2(x) = f_2(x')$. Il suffit de prendre par exemple $x = 2$, $x' = -2$.

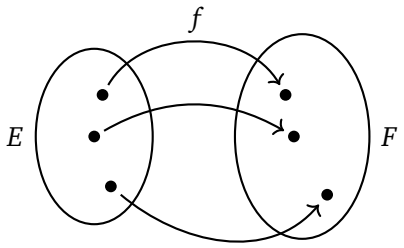
   f_2 n'est pas non plus surjective, en effet il existe des éléments $y \in \mathbb{N}$ qui n'ont aucun antécédent. Par exemple $y = 3$: si $y = 3$ avait un antécédent x par f_2, nous aurions $f_2(x) = y$, c'est-à-dire $x^2 = 3$, d'où $x = \pm\sqrt{3}$. Mais alors x n'est pas un entier de $\mathbb{Z}$. Donc $y = 3$ n'a pas d'antécédent et f_2 n'est pas surjective.

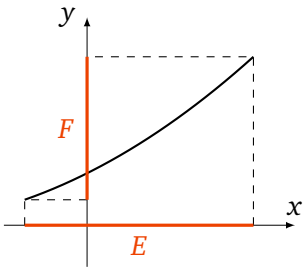
Bijection

Définition 6.
f est **bijective** si elle injective et surjective. Cela équivaut à : pour tout $y \in F$ il existe un unique $x \in E$ tel que $y = f(x)$. Autrement dit :

$$\forall y \in F \quad \exists! x \in E \quad \big(y = f(x)\big)$$

L'existence du x vient de la surjectivité et l'unicité de l'injectivité. Autrement dit, tout élément de F a un unique antécédent par f.





Proposition 2.
Soit E, F des ensembles et $f : E \to F$ une application.

1. *L'application f est bijective si et seulement si il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.*
2. *Si f est bijective alors l'application g est unique et elle aussi est bijective. L'application g s'appelle la* ***bijection réciproque*** *de f et est notée f^{-1}. De plus $\left(f^{-1}\right)^{-1} = f$.*

Remarque.

- $f \circ g = \mathrm{id}_F$ se reformule ainsi
$$\forall y \in F \quad f\big(g(y)\big) = y.$$
- Alors que $g \circ f = \mathrm{id}_E$ s'écrit :
$$\forall x \in E \quad g\big(f(x)\big) = x.$$
- Par exemple $f : \mathbb{R} \to]0, +\infty[$ définie par $f(x) = \exp(x)$ est bijective, sa bijection réciproque est $g :]0, +\infty[\to \mathbb{R}$ définie par $g(y) = \ln(y)$. Nous avons bien $\exp\big(\ln(y)\big) = y$, pour tout $y \in]0, +\infty[$ et $\ln\big(\exp(x)\big) = x$, pour tout $x \in \mathbb{R}$.

Démonstration.

1. - Sens $\Rightarrow$. Supposons f bijective. Nous allons construire une application $g : F \to E$. Comme f est surjective alors pour chaque $y \in F$, il existe un $x \in E$ tel que $y = f(x)$ et on pose $g(y) = x$. On a $f\big(g(y)\big) = f(x) = y$, ceci pour tout $y \in F$ et donc $f \circ g = \mathrm{id}_F$. On compose à droite avec f donc $f \circ g \circ f = \mathrm{id}_F \circ f$. Alors pour tout $x \in E$ on a $f\big(g \circ f(x)\big) = f(x)$ or f est injective et donc $g \circ f(x) = x$. Ainsi $g \circ f = \mathrm{id}_E$. Bilan : $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.
   - Sens $\Leftarrow$. Supposons que g existe et montrons que f est bijective.
     — f est surjective : en effet soit $y \in F$ alors on note $x = g(y) \in E$; on a bien : $f(x) = f\big(g(y)\big) = f \circ g(y) = \mathrm{id}_F(y) = y$, donc f est bien surjective.
     — f est injective : soient $x, x' \in E$ tels que $f(x) = f(x')$. On compose par g (à gauche) alors $g \circ f(x) = g \circ f(x')$ donc $\mathrm{id}_E(x) = \mathrm{id}_E(x')$ donc $x = x'$; f est bien injective.
2. - Si f est bijective alors g est aussi bijective car $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$ et on applique ce que l'on vient de démontrer avec g à la place de f. Ainsi $g^{-1} = f$.

- Si f est bijective, g est unique : en effet soit $h : F \to E$ une autre application telle que $h \circ f = \mathrm{id}_E$ et $f \circ h = \mathrm{id}_F$; en particulier $f \circ h = \mathrm{id}_F = f \circ g$, donc pour tout $y \in F$, $f\big(h(y)\big) = f\big(g(y)\big)$ or f est injective alors $h(y) = g(y)$, ceci pour tout $y \in F$; d'où $h = g$.

□

Proposition 3.
Soient $f : E \to F$ et $g : F \to G$ des applications bijectives. L'application $g \circ f$ est bijective et sa bijection réciproque est

$$\boxed{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$$

Démonstration. D'après la proposition 2, il existe $u : F \to E$ tel que $u \circ f = \mathrm{id}_E$ et $f \circ u = \mathrm{id}_F$. Il existe aussi $v : G \to F$ tel que $v \circ g = \mathrm{id}_F$ et $g \circ v = \mathrm{id}_G$. On a alors $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ \mathrm{id}_F \circ v = g \circ v = \mathrm{id}_E$. Et $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ \mathrm{id}_F \circ f = u \circ f = \mathrm{id}_E$. Donc $g \circ f$ est bijective et son inverse est $u \circ v$. Comme u est la bijection réciproque de f et v celle de g alors : $u \circ v = f^{-1} \circ g^{-1}$. □

Injection, surjection, bijection sur les ensembles finis

Proposition 4.
Soit E, F deux ensembles finis et $f : E \to F$ une application.

1. *Si f est injective alors* $\mathrm{Card}\, E \leqslant \mathrm{Card}\, F$.
2. *Si f est surjective alors* $\mathrm{Card}\, E \geqslant \mathrm{Card}\, F$.
3. *Si f est bijective alors* $\mathrm{Card}\, E = \mathrm{Card}\, F$.

Démonstration.

1. Supposons f injective. Notons $F' = f(E) \subset F$ alors la restriction $f_| : E \to F'$ (définie par $f_|(x) = f(x)$) est une bijection. Donc pour chaque $y \in F'$ est associé un unique $x \in E$ tel que $y = f(x)$. Donc E et F' ont le même nombre d'éléments. Donc $\mathrm{Card}\, F' = \mathrm{Card}\, E$. Or $F' \subset F$, ainsi $\mathrm{Card}\, E = \mathrm{Card}\, F' \leqslant \mathrm{Card}\, F$.
2. Supposons f surjective. Pour tout élément $y \in F$, il existe au moins un élément x de E tel que $y = f(x)$ et donc $\mathrm{Card}\, E \geqslant \mathrm{Card}\, F$.
3. Cela découle de (1) et (2) (ou aussi de la preuve du (1)).

□

Proposition 5.
Soit E, F deux ensembles finis et $f : E \to F$ une application. Si

$$\mathrm{Card}\, E = \mathrm{Card}\, F$$

alors les assertions suivantes sont équivalentes :

i. f *est injective,*

ii. f *est surjective,*

iii. f *est bijective.*

Démonstration. Le schéma de la preuve est le suivant : nous allons montrer successivement les implications :

$$(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$$

ce qui prouvera bien toutes les équivalences.

- $(i) \Longrightarrow (ii)$. Supposons f injective. Alors $\operatorname{Card} f(E) = \operatorname{Card} E = \operatorname{Card} F$. Ainsi $f(E)$ est un sous-ensemble de F ayant le même cardinal que F ; cela entraîne $f(E) = F$ et donc f est surjective.
- $(ii) \Longrightarrow (iii)$. Supposons f surjective. Pour montrer que f est bijective, il reste à montrer que f est injective. Raisonnons par l'absurde et supposons f non injective. Alors $\operatorname{Card} f(E) < \operatorname{Card} E$ (car au moins 2 éléments ont la même image). Or $f(E) = F$ car f surjective, donc $\operatorname{Card} F < \operatorname{Card} E$. C'est une contradiction, donc f doit être injective et ainsi f est bijective.
- $(iii) \Longrightarrow (i)$. C'est clair : une fonction bijective est en particulier injective.

□

Appliquez ceci pour montrer le **principe des tiroirs** :

Proposition 6.
Si l'on range dans k tiroirs, $n > k$ paires de chaussettes alors il existe (au moins) un tiroir contenant (au moins) deux paires de chaussettes.

Malgré sa formulation amusante, c'est une proposition souvent utile. Exemple : dans un amphi de 400 étudiants, il y a au moins deux étudiants nés le même jour !

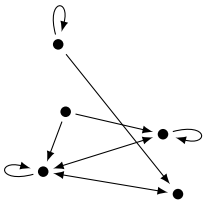
Mini-exercices.

1. Les fonctions suivantes sont-elles injectives, surjectives, bijectives ?
   - $f_1 : \mathbb{R} \to [0, +\infty[$, $x \mapsto x^2$.
   - $f_2 : [0, +\infty[\to [0, +\infty[$, $x \mapsto x^2$.
   - $f_3 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$.
   - $f_4 : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 7$.
   - $f_5 : \mathbb{R} \to [0, +\infty[$, $x \mapsto |x|$.
2. Montrer que la fonction $f :]1, +\infty[\to]0, +\infty[$ définie par $f(x) = \frac{1}{x-1}$ est bijective. Calculer sa bijection réciproque.

2.4. Relation d'équivalence

Définition

Une **relation** sur un ensemble E, c'est la donnée pour tout couple $(x, y) \in E \times E$ de « Vrai » (s'ils sont en relation), ou de « Faux » sinon.
Nous schématisons une relation ainsi : les éléments de E sont des points, une flèche de x vers y signifie que x est en relation avec y, c'est-à-dire que l'on associe « Vrai » au couple (x, y).

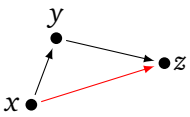


Définition 7.
Soit E un ensemble et $\mathscr{R}$ une relation, c'est une **relation d'équivalence** si :

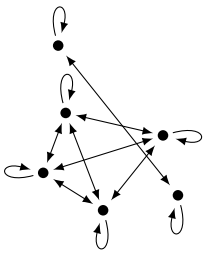
- $\forall x \in E,\ x \mathscr{R} x,$ (**réflexivité**)

- $\forall x, y \in E,\ x \mathscr{R} y \implies y \mathscr{R} x,$ (**symétrie**)

- $\forall x, y, z \in E,\ x \mathscr{R} y$ et $y \mathscr{R} z \implies x \mathscr{R} z,$ (**transitivité**)



Exemple de relation d'équivalence :



Exemples

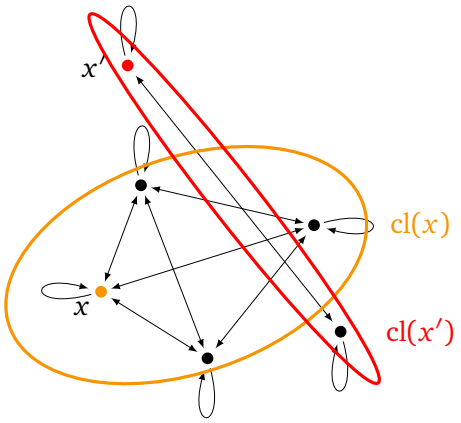
Exemple 5.
Voici des exemples basiques.

1. La relation $\mathscr{R}$ « être parallèle » est une relation d'équivalence pour l'ensemble E des droites affines du plan :
   - réflexivité : une droite est parallèle à elle-même,
   - symétrie : si D est parallèle à D' alors D' est parallèle à D,
   - transitivité : si D parallèle à D' et D' parallèle à D'' alors D est parallèle à D''.
2. La relation « être du même âge » est une relation d'équivalence.
3. La relation « être perpendiculaire » n'est pas une relation d'équivalence (ni la réflexivité, ni la transitivité ne sont vérifiées).
4. La relation $\leqslant$ (sur $E = \mathbb{R}$ par exemple) n'est pas une relation d'équivalence (la symétrie n'est pas vérifiée).

Classes d'équivalence

Définition 8.
Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E. Soit $x \in E$, la **classe d'équivalence** de x est

$$\boxed{\mathrm{cl}(x) = \{y \in E \mid y \mathscr{R} x\}}$$



$\mathrm{cl}(x)$ est donc un sous-ensemble de E, on le note aussi $\overline{x}$. Si $y \in \mathrm{cl}(x)$, on dit que y un **représentant** de $\mathrm{cl}(x)$.

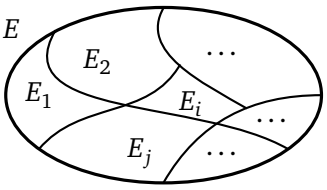
Soit E un ensemble et $\mathscr{R}$ une relation d'équivalence.

Proposition 7.
On a les propriétés suivantes :

1. $cl(x) = cl(y) \iff x \mathscr{R} y$.

2. *Pour tout $x, y \in E$, $cl(x) = cl(y)$ ou $cl(x) \cap cl(y) = \varnothing$.*
3. *Soit C un ensemble de représentants de toutes les classes alors $\{cl(x) \mid x \in C\}$ constitue une partition de E.*

Une **partition** de E est un ensemble $\{E_i\}$ de parties de E tel que $E = \bigcup_i E_i$ et $E_i \cap E_j = \varnothing$ (si $i \neq j$).



Exemples :

1. Pour la relation « être du même âge », la classe d'équivalence d'une personne est l'ensemble des personnes ayant le même âge. Il y a donc une classe d'équivalence formée des personnes de 19 ans, une autre formée des personnes de 20 ans,... Les trois assertions de la proposition se lisent ainsi :
   - On est dans la même classe d'équivalence si et seulement si on est du même âge.
   - Deux personnes appartiennent soit à la même classe, soit à des classes disjointes.
   - Si on choisit une personne de chaque âge possible, cela forme un ensemble de représentants C. Maintenant une personne quelconque appartient à une et une seule classe d'un des représentants.
2. Pour la relation « être parallèle », la classe d'équivalence d'une droite est l'ensemble des droites parallèles à cette droite. À chaque classe d'équivalence correspond une et une seule direction.

Voici un exemple que vous connaissez depuis longtemps :

Exemple 6.
Définissons sur $E = \mathbb{Z} \times \mathbb{N}^*$ la relation $\mathscr{R}$ par

$$(p,q)\mathscr{R}(p',q') \iff pq' = p'q.$$

Tout d'abord $\mathscr{R}$ est une relation d'équivalence :

- $\mathscr{R}$ est réflexive : pour tout (p,q) on a bien $pq = pq$ et donc $(p,q)\mathscr{R}(p,q)$.
- $\mathscr{R}$ est symétrique : pour tout (p,q), (p',q') tels que $(p,q)\mathscr{R}(p',q')$ on a donc $pq' = p'q$ et donc $p'q = pq'$ d'où $(p',q')\mathscr{R}(p,q)$.
- $\mathscr{R}$ est transitive : pour tout (p,q), (p',q'), (p'',q'') tels que $(p,q)\mathscr{R}(p',q')$ et $(p',q')\mathscr{R}(p'',q'')$ on a donc $pq' = p'q$ et $p'q'' = p''q'$. Alors $(pq')q'' = (p'q)q'' = q(p'q'') = q(p''q')$. En divisant par $q' \neq 0$ on obtient $pq'' = qp''$ et donc $(p,q)\mathscr{R}(p'',q'')$.

Nous allons noter $\frac{p}{q} = \mathrm{cl}(p,q)$ la classe d'équivalence d'un élément $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$. Par exemple, comme $(2,3)\mathscr{R}(4,6)$ (car $2 \times 6 = 3 \times 4$) alors les classes de $(2,3)$ et $(4,6)$ sont égales : avec notre notation cela s'écrit : $\frac{2}{3} = \frac{4}{6}$.

C'est ainsi que l'on définit les rationnels : l'ensemble $\mathbb{Q}$ des rationnels est l'ensemble de classes d'équivalence de la relation $\mathscr{R}$.
Les nombres $\frac{2}{3} = \frac{4}{6}$ sont bien égaux (ce sont les mêmes classes) mais les écritures sont différentes (les représentants sont distincts).

L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geqslant 2$ un entier fixé. Définissons la relation suivante sur l'ensemble $E = \mathbb{Z}$:

$$\boxed{a \equiv b \pmod{n} \iff a - b \text{ est un multiple de } n}$$

Exemples pour $n = 7$: $10 \equiv 3 \pmod 7$, $19 \equiv 5 \pmod 7$, $77 \equiv 0 \pmod 7$, $-1 \equiv 20 \pmod 7$.

Cette relation est bien une relation d'équivalence :

- Pour tout $a \in \mathbb{Z}$, $a - a = 0 = 0 \cdot n$ est un multiple de n donc $a \equiv a \pmod n$.
- Pour $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod n$ alors $a - b$ est un multiple de n, autrement dit il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ et donc $b - a = (-k)n$ et ainsi $b \equiv a \pmod n$.
- Si $a \equiv b \pmod n$ et $b \equiv c \pmod n$ alors il existe $k, k' \in \mathbb{Z}$ tels que $a - b = kn$ et $b - c = k'n$. Alors $a - c = (a - b) + (b - c) = (k + k')n$ et donc $a \equiv c \pmod n$.

La classe d'équivalence de $a \in \mathbb{Z}$ est notée $\overline{a}$. Par définition nous avons donc

$$\overline{a} = \mathrm{cl}(a) = \big\{b \in \mathbb{Z} \mid b \equiv a \pmod n\big\}.$$

Comme un tel b s'écrit $b = a + kn$ pour un certain $k \in \mathbb{Z}$ alors c'est aussi exactement

$$\overline{a} = a + n\mathbb{Z} = \big\{a + kn \mid k \in \mathbb{Z}\big\}.$$

Comme $n \equiv 0 \pmod n$, $n + 1 \equiv 1 \pmod n$, ... alors

$$\overline{n} = \overline{0}, \quad \overline{n+1} = \overline{1}, \quad \overline{n+2} = \overline{2}, \ldots$$

et donc l'ensemble des classes d'équivalence est l'ensemble

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \big\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\big\}}$$

qui contient exactement n éléments.
Par exemple, pour $n = 7$:

- $\overline{0} = \{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} = 7\mathbb{Z}$
- $\overline{1} = \{\ldots, -13, -6, 1, 8, 15, \ldots\} = 1 + 7\mathbb{Z}$
- ...
- $\overline{6} = \{\ldots, -8, -1, 6, 13, 20, \ldots\} = 6 + 7\mathbb{Z}$

Mais ensuite $\overline{7} = \{\ldots -7, 0, 7, 14, 21, \ldots\} = \overline{0} = 7\mathbb{Z}$. Ainsi $\mathbb{Z}/7\mathbb{Z} = \big\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{6}\big\}$ possède 7 éléments.

Remarque.
Dans beaucoup de situations de la vie courante, nous raisonnons avec les modulos. Par exemple pour l'heure : les minutes et les secondes sont modulo 60 (après 59 minutes on repart à zéro), les heures modulo 24 (ou modulo 12 sur le cadran à aiguilles). Les jours de la semaine sont modulo 7, les mois modulo 12,...

2.5. Relation d'Ordre

Nous allons voir que les réels sont ordonnés. La notion d'ordre est générale et nous allons définir cette notion sur un ensemble quelconque. Cependant gardez à l'esprit que pour nous $E = \mathbb{R}$ et $\mathscr{R} = \leqslant$.

Définition 9.
Soit E un ensemble.

1. Une **relation** binaire $\mathscr{R}$ sur E est un sous-ensemble de l'ensemble produit $E \times E$. Pour $(x, y) \in E \times E$, on dit que x est en relation avec y et on note $x \mathscr{R} y$ pour dire que $(x, y) \in \mathscr{R}$.
2. Une relation $\mathscr{R}$ est une **relation d'ordre** si
   - $\mathscr{R}$ est **réflexive** : pour tout $x \in E$, $x \mathscr{R} x$,
   - $\mathscr{R}$ est **antisymétrique** : pour tout $x, y \in E$, $(x \mathscr{R} y$ et $y \mathscr{R} x) \implies x = y$,
   - $\mathscr{R}$ est **transitive** : pour tout $x, y, z \in E$, $(x \mathscr{R} y$ et $y \mathscr{R} z) \implies x \mathscr{R} z$.

Définition 10.
Soient $\mathscr{R}$ une relation d'ordre dans un ensemble E et $x, y \in E$. On dit qu'ils x et y sont comparables si $x \mathscr{R} y$ ou $y \mathscr{R} x$. Si deux éléments quelconques de E sont comparables, on dit que E est un **ensemble totalement ordonné**. Lorsque E est totalement ordonné, on dit aussi que la relation d'ordre $\mathscr{R}$ sur E est **totale**. Un ordre qui n'est pas total est dit **partiel**.

Propriété ($\mathbb{R}$ totalement ordonné)**.**
La relation $\leqslant$ sur $\mathbb{R}$ est une relation d'ordre, et de plus, elle est totale.

Nous avons donc :

- pour tout $x \in \mathbb{R}$, $x \leqslant x$,
- pour tout $x, y \in \mathbb{R}$, si $x \leqslant y$ et $y \leqslant x$ alors $x = y$,
- pour tout $x, y, z \in \mathbb{R}$ si $x \leqslant y$ et $y \leqslant z$ alors $x \leqslant z$.

Remarque.
Pour $(x, y) \in \mathbb{R}^2$ on a par définition :

$$x \leqslant y \iff y - x \in \mathbb{R}_+$$
$$x < y \iff (x \leqslant y \text{ et } x \neq y).$$

Les opérations de $\mathbb{R}$ sont compatibles avec la relation d'ordre $\leqslant$ au sens suivant, pour des réels a, b, c, d :

$$(a \leqslant b \text{ et } c \leqslant d) \implies a + c \leqslant b + d$$
$$(a \leqslant b \text{ et } c \geqslant 0) \implies a \times c \leqslant b \times c$$
$$(a \leqslant b \text{ et } c \leqslant 0) \implies a \times c \geqslant b \times c.$$

Exemples

- la relation d'ordre usuelle sur les nombres entiers, sur les nombres réels ;
- la relation de divisibilité sur les nombres entiers, ou sur les polynômes ;
- la relation d'inclusion sur les parties d'un ensemble ;
- la relation opposée à une relation d'ordre ;
- l'ordre lexicographique sur le produit de deux ensembles ordonnés, ou sur l'ensemble des suites finies à valeurs dans un ensemble ordonné.

Minorants, plus petit élément, borne inférieure

Soient $\mathscr{R}$ une relation d'ordre sur E, S une partie de E et a un élément de E. On dit que :

- a **minore** S, ou est un **minorant** de S, si l'on a $a\mathscr{R}s$ pour tout $s \in S$.
- a **majore** S, ou est un **majorant** de S, si l'on a $s\mathscr{R}a$ pour tout $s \in S$.
- a est un **élément minimal** de S si $a \in S$ et si a est le seul élément $s \in S$ tel que $s\mathscr{R}a$.
- a est un **élément maximal** de S si $a \in S$ et si a est le seul élément $s \in S$ tel que $a\mathscr{R}s$.
- S possède un plus petit élément s'il existe un minorant de S qui est un élément de S ; on dit alors naturellement que c'est **le plus petit élément** de S et on le note éventuellement $\min(S)$.
- S possède un plus grand élément s'il existe un majorant de S qui est un élément de S ; on dit alors naturellement que c'est **le plus grand élément** de S et on le note éventuellement $\max(S)$.
- S possède une **borne inférieure** si l'ensemble des minorants de S possède un plus grand élément ; on la note alors $\inf(S)$.
- S possède une **borne supérieure** si l'ensemble des majorants de S possède un plus petit élément ; on la note alors $\sup(S)$.

Attention. Si a est un élément minimal de S, cela n'entraîne pas que a minore S, car il peut exister des éléments de S incomparables avec a. Par exemple si l'ensemble des nombres entiers $\geqslant 2$ est muni de la relation de divisibilité, les éléments minimaux sont les nombres premiers.

On définit le maximum de deux réels a et b par :

$$\max(a, b) = \begin{cases} a & \text{si } a \geqslant b \\ b & \text{si } b > a. \end{cases}$$

Exercice 1.
Comment définir $\max(a,b,c)$, $\max(a_1,a_2,\dots,a_n)$? Et $\min(a,b)$?

Ensembles bien ordonnés. On dit qu'une relation d'ordre $\preccurlyeq$ sur un ensemble E est un bon ordre, ou que l'ensemble E est bien ordonné, si toute partie non vide de E possède un plus petit élément.

Exemple fondamental : les entiers naturels. Si A et B sont des ensembles bien ordonnés, l'ordre lexicographique sur le produit $A \times B$ est bien ordonné. Un bon ordre est un ordre total ; en effet, pour $a, b \in E$, le plus petit élément de la partie non vide $\{a,b\}$ est comparable à l'autre.

Théorème (Zorn). — Soit E un ensemble muni d'une relation d'ordre $\preccurlyeq$. On suppose que toute partie totalement ordonnée de E est majorée. Alors, E possède un élément maximal.

Mini-exercices.

1. Montrer que la relation définie sur $\mathbb{N}$ par $x \mathscr{R} y \iff \frac{2x+y}{3} \in \mathbb{N}$ est une relation d'équivalence. Montrer qu'il y a 3 classes d'équivalence.
2. Dans $\mathbb{R}^2$ montrer que la relation définie par $(x,y)\mathscr{R}(x',y') \iff x+y' = x'+y$ est une relation d'équivalence. Montrer que deux points (x,y) et (x',y') sont dans une même classe si et seulement s'ils appartiennent à une même droite dont vous déterminerez la direction.
3. On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par $\overline{p}+\overline{q} = \overline{p+q}$. Calculer la table d'addition dans $\mathbb{Z}/6\mathbb{Z}$ (c'est-à-dire toutes les sommes $\overline{p}+\overline{q}$ pour $\overline{p},\overline{q} \in \mathbb{Z}/6\mathbb{Z}$). Même chose avec la multiplication $\overline{p} \times \overline{q} = \overline{p \times q}$. Mêmes questions avec $\mathbb{Z}/5\mathbb{Z}$, puis $\mathbb{Z}/8\mathbb{Z}$.

Chapitre 3

Structures algébriques

Motivation

Évariste Galois a tout juste vingt ans lorsqu'il meurt dans un duel. Il restera pourtant comme l'un des plus grands mathématiciens de son temps pour avoir introduit la notion de groupe, alors qu'il avait à peine dix-sept ans.
Vous savez résoudre les équations de degré 2 du type $ax^2 + bx + c = 0$. Les solutions s'expriment en fonction de a, b, c et de la fonction racine carrée $\sqrt{}$. Pour les équations de degré 3, $ax^3 + bx^2 + cx + d = 0$, il existe aussi des formules. Par exemple une solution de $x^3 + 3x + 1 = 0$ est $x_0 = \sqrt[3]{\frac{\sqrt{5}-1}{2}} - \sqrt[3]{\frac{\sqrt{5}+1}{2}}$. De telles formules existent aussi pour les équations de degré 4.
Une préoccupation majeure au début du XIX$^{\text{e}}$ siècle était de savoir s'il existait des formules similaires pour les équations de degré 5 ou plus. La réponse fut apportée par Galois et Abel : non il n'existe pas en général une telle formule. Galois parvient même à dire pour quels polynômes c'est possible et pour lesquels ça ne l'est pas. Il introduit pour sa démonstration la notion de groupe.

Les groupes sont à la base d'autres notions mathématiques comme les anneaux, les corps, les matrices, les espaces vectoriels,... Mais vous les retrouvez aussi en arithmétique, en géométrie, en cryptographie !

Nous allons introduire dans ce chapitre la notion de groupe, puis celle de sous-groupe. On étudiera ensuite les applications entre deux groupes : les morphismes de groupes.

3.1. Lois de composition interne

Définition 1.
Soit E un ensemble. Une **loi de composition interne** (LCI) sur E est une application $\star : E \times E \to E$. Si on la défini $(a,b) \mapsto a \star b$ on parle de la loi $\star$ et on dit que $a \star b$ est le composé de a et b pour la loi $\star$. Un ensemble E muni d'une loi de composition interne constitue une structure algébrique appelée **magma** et notée $(E, \star)$.

Remarque. On parle souvent d'opération plutôt que de loi de composition interne.

Exemples de lois de composition interne

(1) L'addition définie par $(a,b) \mapsto a+b$ est une loi de composition interne dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

(2) La multiplication définie par $(a,b) \mapsto a \times b$ est une loi de composition interne dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.

(3) La division définie par $(a,b) \mapsto a \div b$ est une loi de composition interne dans $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ et $\mathbb{C} - \{0\}$.

(4) La division $\div$ dans $\mathbb{Z} - \{0\}$ n'est pas une loi de composition interne.

(5) La composition définie par $(f,g) \mapsto f \circ g$ est une loi de composition interne sur l'ensembles de applications de E vers E.

(6) La réunion dans $\mathscr{P}(E)$, définie par $(A,B) \mapsto A \cup B$ est une loi de composition interne.

(7) L'intersection dans $\mathscr{P}(E)$, définie par $(A,B) \mapsto A \cap B$ est une loi de composition interne.

(8) La loi $\oplus$ définie sur $\mathbb{R}^2$ par $(x_1,y_1) \oplus (x_2,y_2) = (x_1+x_2, y_1+y_2)$ est une loi de composition interne.

(9) La loi $\otimes$ définie sur $\mathbb{R}^2$ par $(x_1,y_1) \otimes (x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$ est une LCI.

Propriétés usuelles des lois internes

Soit $\star$ une loi interne sur l'ensemble E.

- **Commutativité :** la loi $\star$ est **commutative** si pour tous $a, b \in E$: $a \star b = b \star a$.
- **Associativité :** la loi $\star$ est **associative** si pour tous $a, b, c \in E$: $a \star (b \star c) = (a \star b) \star c$.
- **Élément neutre :** la loi $\star$ admet un **élément neutre** $e \in E$ si pour tout $a \in E$: $a \star e = e \star a = a$.
- **Élément symétrique :** un élément $a' \in E$ est le **symétrique** de a dans E, si : $a \star a' = e = a' \star a$. Un élément qui admet un symétrique est dit **symétrisable**.

Remarque.

- Lorsque la loi est additive $+$, le symétrique est noté $-x$ et est appelé «**opposé**».
- Lorsque la loi est multiplicative $\times$, le symétrique est noté x^{-1} et est appelé «**inverse**».

Exemples

(1) La somme et le produit sur $\mathbb{C}$ (donc sur ses sous-ensembles) est associative et commutative, et admettent pour neutres respectifs 0 et 1.

(2) La différence n'est ni associative ni commutative sur $\mathbb{R}$.

(3) La loi $\circ$ (composition des fonctions de E dans E) est associative, mais n'est pas commutative (sauf si F est un singleton, auquel cas ...). Elle admet un neutre, qui est l'application Id_E .

(4) Les lois $\cup$ et $\cap$ sur $\mathscr{P}(E)$ sont associatives et commutatives. Elles admettent pour neutres respectifs $\varnothing$ et E.

(5) Les lois $\oplus$ et $\otimes$ sont associatives et commutatives sur $\mathbb{R}^2$.

(6) Dans $\mathbb{R}$, chaque élément a possède un symétrique pour l'addition qui est son opposé $-a$. Mais a n'a un symétrique pour la multiplication sauf si $a \neq 0$, son symétrique est a^{-1}.

(7) Dans $F(X,X)$, un élément f a un symétrique (pour la composition $\circ$) si et seulement si f est bijective et alors son symétrique est l'application réciproque f^{-1}.

Définition 2.
Si $\star$ est une loi de composition interne associative sur E qui admet un élément neutre, on dit que $(E,\star)$ est un **monoïde**. Si de plus $\star$ est commutative, on dit que ce monoïde est commutatif.

Proposition 1 (Unicité).
Soit $\star$ est une loi de composition interne sur E.

1. *Si $\star$ admet un élément neutre, alors ce neutre est unique.*
2. *Si $x \in E$ admet un élément symétrique, alors ce symétrique est unique.*

Définition 3 (Stabilité).
Soient E un ensemble muni d'une loi de composition interne $\star$, et F une partie de E.
On dit que F est **stable** par $\star$ si pour tous $x, y \in F$, $x \star y \in F$.
Dans ce cas on dit que $\star$ définie par restriction une loi de composition interne sut F.

Exemples

(1) Les sous-ensembles $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ de $(\mathbb{C}, +)$ sont stables par l'addition .

(2) Les sous-ensembles $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ de $(\mathbb{C}, \times)$ sont stables par la multiplication .

(3) L'ensemble des éléments $(\mathbb{R}, \times)$ est stable par la multiplication .

Définition 4 (Distributivité).
Soit E un ensemble muni de deux lois de composition internes, notées $+$ et $\star$. On dit que

$\star$ est distributive par rapport à $+$ si pour tous les éléments x, y, z de E, on a

$$x \star (y+z) = (x \star y) + (x \star z) \qquad \text{et} \qquad (x+y) \star z = (x \star z) + (y \star z).$$

Exemples

(1) Dans $\mathbb{R}$, la multiplication est distributive par rapport à l'addition .

(2) Dans $\mathbb{R}$, l'addition n'est pas distributive par rapport à la multiplication .

(3) Dans l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble E, la réunion est distributive par rapport à l'intersection et l'intersection est distributive par rapport à la réunion.

3.2. Groupe

Définition

Définition 5.
Un **groupe** $(G, \star)$ est un ensemble G auquel est associé une opération $\star$ (la **loi de composition**) vérifiant les quatre propriétés suivantes :

1. pour tout $x, y \in G$, $\quad x \star y \in G \quad$ ($\star$ est une **loi de composition interne**)
2. pour tout $x, y, z \in G$, $\quad (x \star y) \star z = x \star (y \star z) \quad$ (la loi est **associative**)
3. il existe $e \in G$ tel que $\quad \forall x \in G,\ x \star e = x \ \text{ et } \ e \star x = x \quad$ (e est l'**élément neutre**)
4. pour tout $x \in G$ il existe $x' \in G$ tel que $\quad x \star x' = x' \star x = e \quad$ (x' est l'**inverse** de x et est noté x^{-1})

Un groupe est donc un monoïde dans lequel tout élément est **symétrisable**.

Si de plus l'opération vérifie

$$\text{pour tout } x, y \in G, \qquad x \star y = y \star x,$$

on dit que G est un groupe **commutatif** (ou **abélien**).

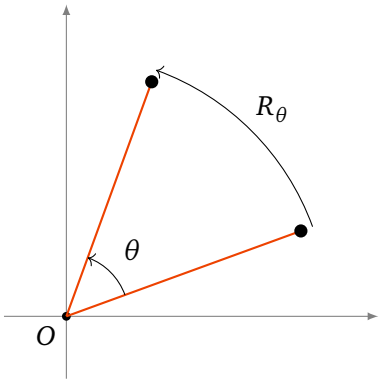
Remarque.

- L'élément neutre e est unique. En effet si e' vérifie aussi le point (3), alors on a $e' \star e = e$ (car e est élément neutre) et $e' \star e = e'$ (car e' aussi). Donc $e = e'$. Remarquez aussi que l'inverse de l'élément neutre est lui-même. S'il y a plusieurs groupes, on pourra noter e_G pour l'élément neutre du groupe G.
- Un élément $x \in G$ ne possède qu'un seul inverse. En effet si x' et x'' vérifient tous les deux le point (4) alors on a $x \star x'' = e$ donc $x' \star (x \star x'') = x' \star e$. Par l'associativité (2) et la propriété de l'élément neutre (3) alors $(x' \star x) \star x'' = x'$. Mais $x' \star x = e$ donc $e \star x'' = x'$ et ainsi $x'' = x'$.

Exemples

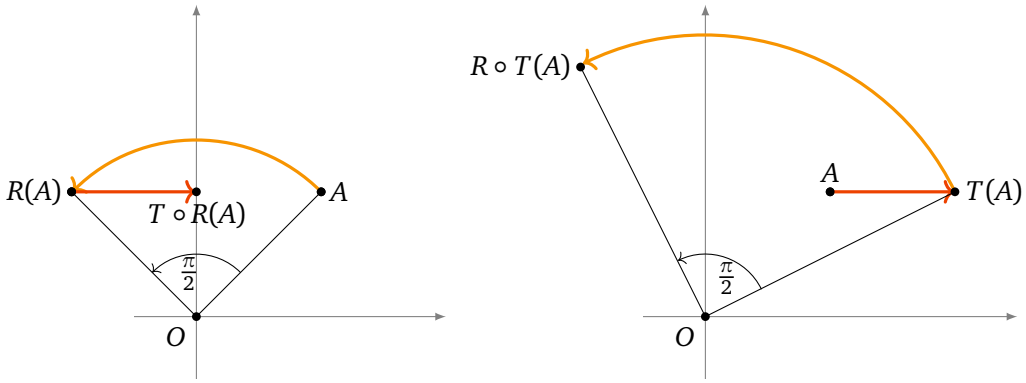
Voici des ensembles bien connus pour lesquels l'opération donnée définit une structure de groupe.

- $(\mathbb{R}^*, \times)$ est un groupe commutatif, $\times$ est la multiplication habituelle. Vérifions chacune des propriétés :
  1. Si $x, y \in \mathbb{R}^*$ alors $x \times y \in \mathbb{R}^*$.
  2. Pour tout $x, y, z \in \mathbb{R}^*$ alors $x \times (y \times z) = (x \times y) \times z$, c'est l'associativité de la multiplication des nombres réels.
  3. 1 est l'élément neutre pour la multiplication, en effet $1 \times x = x$ et $x \times 1 = x$, ceci quelque soit $x \in \mathbb{R}^*$.
  4. L'inverse d'un élément $x \in \mathbb{R}^*$ est $x' = \frac{1}{x}$ (car $x \times \frac{1}{x}$ est bien égal à l'élément neutre 1). L'inverse de x est donc $x^{-1} = \frac{1}{x}$. Notons au passage que nous avions exclu 0 de notre groupe, car il n'a pas d'inverse.
     Ces propriétés font de $(\mathbb{R}^*, \times)$ un groupe.
  5. Enfin $x \times y = y \times x$, c'est la commutativité de la multiplication des réels.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes commutatifs.
- $(\mathbb{Z}, +)$ est un groupe commutatif. Ici $+$ est l'addition habituelle.
  1. Si $x, y \in \mathbb{Z}$ alors $x + y \in \mathbb{Z}$.
  2. Pour tout $x, y, z \in \mathbb{Z}$ alors $x + (y + z) = (x + y) + z$.
  3. 0 est l'élément neutre pour l'addition, en effet $0 + x = x$ et $x + 0 = x$, ceci quelque soit $x \in \mathbb{Z}$.
  4. L'inverse d'un élément $x \in \mathbb{Z}$ est $x' = -x$ car $x + (-x) = 0$ est bien l'élément neutre 0. Quand la loi de groupe est $+$ l'inverse s'appelle plus couramment l'**opposé**.
  5. Enfin $x + y = y + x$, et donc $(\mathbb{Z}, +)$ est un groupe commutatif.
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes commutatifs.
- Soit $\mathscr{R}$ l'ensemble des rotations du plan dont le centre est à l'origine O.



  Alors pour deux rotations R_θ et $R_{\theta'}$ la composée $R_\theta \circ R_{\theta'}$ est encore une rotation de centre l'origine et d'angle $\theta + \theta'$. Ici $\circ$ est la composition. Ainsi $(\mathscr{R}, \circ)$ forme un groupe (qui est même commutatif). Pour cette loi l'élément neutre est la rotation d'angle 0 : c'est l'identité du plan. L'inverse d'une rotation d'angle θ est la rotation d'angle $-\theta$.

- Si $\mathscr{I}$ désigne l'ensemble des isométries du plan (ce sont les translations, rotations, réflexions et leurs composées) alors $(\mathscr{I}, \circ)$ est un groupe. Ce groupe n'est pas un groupe commutatif. En effet, identifions le plan à $\mathbb{R}^2$ et soit par exemple R la rotation de centre $O = (0,0)$ et d'angle $\frac{\pi}{2}$ et T la translation de vecteur $(1,0)$. Alors les isométries $T \circ R$ et $R \circ T$ sont des applications distinctes. Par exemple les images du point $A = (1,1)$ par ces applications sont distinctes : $T \circ R(1,1) = T(-1,1) = (0,1)$ alors que $R \circ T(1,1) = R(2,1) = (-1,2)$.



Voici deux exemples qui **ne sont pas** des groupes :

- $(\mathbb{Z}^*, \times)$ n'est pas un groupe. Car si 2 avait un inverse (pour la multiplication $\times$) ce serait $\frac{1}{2}$ qui n'est pas un entier.
- $(\mathbb{N}, +)$ n'est pas un groupe. En effet l'inverse de 3 (pour l'addition $+$) devrait être -3 mais $-3 \notin \mathbb{N}$.

Nous étudierons dans les sections 3.2.1 et **??** deux autres groupes très importants : les groupes cycliques $(\mathbb{Z}/n\mathbb{Z}, +)$ et les groupes de permutations $(\mathscr{S}_n, \circ)$.

Puissance

Revenons à un groupe $(G, \star)$. Pour $x \in G$ nous noterons $x \star x$ par x^2 et $x \star x \star x$ par x^3. Plus généralement nous noterons :

- $x^n = \underbrace{x \star x \star \cdots \star x}_{n \text{ fois}}$,
- $x^0 = e$,
- $x^{-n} = \underbrace{x^{-1} \star \cdots \star x^{-1}}_{n \text{ fois}}$.

Rappelez-vous que x^{-1} désigne l'inverse de x dans le groupe.

Les règles de calcul sont les mêmes que pour les puissances des nombres réels. Pour $x, y \in G$ et $m, n \in \mathbb{Z}$ nous avons :

- $x^m \star x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x \star y)^{-1} = y^{-1} \star x^{-1}$, attention à l'ordre !
- **Si** $(G, \star)$ est **commutatif** alors $(x \star y)^n = x^n \star y^n$.

Exemple des matrices 2×2

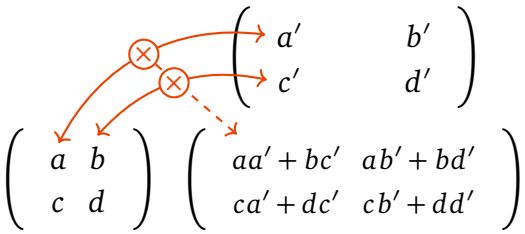
Une **matrice** 2×2 est un tableau de 4 nombres (pour nous des réels) noté ainsi :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Nous allons définir l'opération **produit** noté $\times$ de deux matrices $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$:

$$M \times M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Voici comment présenter les calculs, on place M à gauche, M' au dessus de ce qui va être le résultat. On calcule un par un, chacun des termes de $M \times M'$.
Pour le premier terme on prend la colonne située au dessus et la ligne située à gauche : on effectue les produits $a \times a'$ et $b \times c'$ qu'on additionne pour obtenir le premier terme du résultat. Même chose avec le second terme : on prend la colonne située au dessus, la ligne située à gauche, on fait les produit, on additionne : $ab' + bd'$. Idem pour les deux autres termes.



Par exemple si $M = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ et $M' = \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ alors voici comment poser les calculs ($M \times M'$ à gauche, $M' \times M$ à droite)

$$\begin{array}{cc} & \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} & \begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix} \end{array} \qquad \begin{array}{cc} & \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \end{array}$$

alors $M \times M' = \left(\begin{smallmatrix} 3 & 1 \\ -2 & -1 \end{smallmatrix}\right)$ et $M' \times M = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 1 \end{smallmatrix}\right)$. Remarquez qu'en général $M \times M' \neq M' \times M$.

Le **déterminant** d'une matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est par définition le nombre réel

$$\det M = ad - bc.$$

Proposition 2.
L'ensemble des matrices 2×2 ayant un déterminant non nul, muni de la multiplication des matrices $\times$, forme un groupe non-commutatif.

Ce groupe est noté $(\mathscr{GL}_2, \times)$.

Nous aurons besoin d'un résultat préliminaire :

Lemme 1.
$\det(M \times M') = \det M \cdot \det M'$.

Pour la preuve, il suffit de vérifier le calcul : $\big(aa'+bc'\big)\big(cb'+dd'\big)-\big(ab'+bd'\big)\big(ca'+dc'\big)=(ad-bc)(a'd'-b'c')$.
Revenons à la preuve de la proposition.

Démonstration.

1. Vérifions la loi de composition interne. Si M, M' sont des matrices 2×2 alors $M\times M'$ aussi. Maintenant si M et M' sont de déterminants non nuls alors $\det(M\times M')=\det M\cdot\det M'$ est aussi non nul. Donc si $M, M'\in\mathscr{Gl}_2$ alors $M\times M'\in\mathscr{Gl}_2$.
2. Pour vérifier que la loi est associative, c'est un peu fastidieux. Pour trois matrices M, M', M'' quelconques il faut montrer $(M\times M')\times M''=M\times(M'\times M'')$. Faites-le pour vérifier que vous maîtrisez le produit de matrices.
3. Existence de l'élément neutre. La **matrice identité** $I=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ est l'élément neutre pour la multiplication des matrices : en effet $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\times\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\times\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$.
4. Existence de l'inverse. Soit $M=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ une matrice de déterminant non nul alors $M^{-1}=\frac{1}{ad-bc}\left(\begin{smallmatrix}d&-b\\-c&a\end{smallmatrix}\right)$ est l'inverse de M : vérifiez que $M\times M^{-1}=I$ et que $M^{-1}\times M=I$.
5. Enfin nous avons déjà vu que cette multiplication n'est pas commutative.

□

Mini-exercices.

1. Montrer que $(\mathbb{R}_+^*,\times)$ est un groupe commutatif.
2. Soit $f_{a,b}:\mathbb{R}\to\mathbb{R}$ la fonction définie par $x\mapsto ax+b$. Montrer que l'ensemble $\mathscr{F}=\{f_{a,b}\mid a\in\mathbb{R}^*, b\in\mathbb{R}\}$ muni de la composition « $\circ$ » est un groupe non commutatif.
3. (Plus dur) Soit $G=]-1,1[$. Pour $x,y\in G$ on définit $x\star y=\frac{x+y}{1+xy}$. Montrer que $(G,\star)$ forme un groupe en (a) montrant que $\star$ est une loi de composition interne : $x\star y\in G$; (b) montrant que la loi est associative ; (c) montrant que 0 est élément neutre ; (d) trouvant l'inverse de x.

Soit $(G,\star)$ un groupe quelconque ; x, y, z sont des éléments de G.

4. Montrer que si $x\star y=x\star z$ alors $y=z$.
5. Que vaut $\left(x^{-1}\right)^{-1}$?
6. Si $x^n=e$, quel est l'inverse de x ?

Matrices :

7. Soient $M_1=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, $M_2=\left(\begin{smallmatrix}1&2\\1&0\end{smallmatrix}\right)$, $M_3=\left(\begin{smallmatrix}1&2\\3&4\end{smallmatrix}\right)$. Vérifier que $M_1\times(M_2\times M_3)=(M_1\times M_2)\times M_3$.
8. Calculer $(M_1\times M_2)^2$ et $M_1^2\times M_2^2$. (Rappel : $M^2=M\times M$)
9. Calculer le déterminant des M_i ainsi que leur inverse.
10. Montrer que l'ensemble des matrices 2×2 muni de l'addition $+$ définie par $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)+\left(\begin{smallmatrix}a'&b'\\c'&d'\end{smallmatrix}\right)=\left(\begin{smallmatrix}a+a'&b+b'\\c+c'&d+d'\end{smallmatrix}\right)$ forme un groupe commutatif.

3.2.1. Le groupe $\mathbb{Z}/n\mathbb{Z}$

L'ensemble et le groupe $\mathbb{Z}/n\mathbb{Z}$

Fixons $n \geqslant 1$. Rappelons que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

où $\overline{p}$ désigne la classe d'équivalence de p modulo n.
Autrement dit

$$\boxed{\overline{p} = \overline{q} \iff p \equiv q \pmod{n}}$$

ou encore $\overline{p} = \overline{q} \iff \exists k \in \mathbb{Z} \quad p = q + kn$.
On définit une **addition** sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\boxed{\overline{p} + \overline{q} = \overline{p+q}}$$

Par exemple dans $\mathbb{Z}/60\mathbb{Z}$, on a $\overline{31} + \overline{46} = \overline{31+46} = \overline{77} = \overline{17}$.

Nous devons montrer que cette addition est bien définie : si $\overline{p'} = \overline{p}$ et $\overline{q'} = \overline{q}$ alors $p' \equiv p \pmod{n}$, $q' \equiv q \pmod{n}$ et donc $p' + q' \equiv p + q \pmod{n}$. Donc $\overline{p'+q'} = \overline{p+q}$. Donc on a aussi $\overline{p'} + \overline{q'} = \overline{p} + \overline{q}$. Nous avons montré que l'addition est indépendante du choix des représentants.

Voici un exemple de la vie courante : considérons seulement les minutes d'une montre ; ces minutes varient de 0 à 59. Lorsque l'aiguille passe à 60, elle désigne aussi 0 (on ne s'occupe pas des heures). Ainsi de suite : 61 s'écrit aussi 1, 62 s'écrit aussi 2,... Cela correspond donc à l'ensemble $\mathbb{Z}/60\mathbb{Z}$. On peut aussi additionner des minutes : 50 minutes plus 15 minutes font 65 minutes qui s'écrivent aussi 5 minutes. Continuons avec l'écriture dans $\mathbb{Z}/60\mathbb{Z}$ par exemple : $\overline{135} + \overline{50} = \overline{185} = \overline{5}$. Remarquez que si l'on écrit d'abord $\overline{135} = \overline{15}$ alors $\overline{135} + \overline{50} = \overline{15} + \overline{50} = \overline{65} = \overline{5}$. On pourrait même écrire $\overline{50} = -\overline{10}$ et donc $\overline{135} + \overline{50} = \overline{15} - \overline{10} = \overline{5}$. C'est le fait que l'addition soit bien définie qui justifie que l'on trouve toujours le même résultat.

Proposition 3.
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

C'est facile. L'élément neutre est $\overline{0}$. L'opposé de $\overline{k}$ est $-\overline{k} = \overline{-k} = \overline{n-k}$. L'associativité et la commutativité découlent de celles de $(\mathbb{Z}, +)$.

Groupes cycliques de cardinal fini

Définition 6.
Un groupe $(G, \star)$ est un groupe **cyclique** s'il existe un élément $a \in G$ tel que :

$$\text{pour tout } x \in G, \text{ il existe } k \in \mathbb{Z} \text{ tel que } x = a^k$$

Autrement dit le groupe G est engendré par un seul élément a.
Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique. En effet il est engendré par $a=\overline{1}$, car tout élément $\overline{k}$ s'écrit $\overline{k}=\underbrace{\overline{1}+\overline{1}+\cdots\overline{1}}_{k \text{ fois}}=k\cdot\overline{1}$.
Voici un résultat intéressant : il n'existe, à isomorphisme près, qu'un seul groupe cyclique à n éléments, c'est $\mathbb{Z}/n\mathbb{Z}$:

Théorème 1.
Si $(G,\star)$ un groupe cyclique de cardinal n, alors $(G,\star)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

Démonstration. Comme G est cyclique alors $G=\{\ldots,a^{-2},a^{-1},e,a,a^2,a^3,\ldots\}$. Dans cette écriture il y a de nombreuses redondances (car de toute façon G n'a que n éléments). Nous allons montrer qu'en fait

$$G=\{e,a,a^2,\ldots,a^{n-1}\} \quad \text{et que} \quad a^n=e.$$

Tout d'abord l'ensemble $\{e,a,a^2,\ldots,a^{n-1}\}$ est inclus dans G. En plus il a exactement n éléments. En effet si $a^p=a^q$ avec $0\leqslant q<p\leqslant n-1$ alors $a^{p-q}=e$ (avec $p-q>0$) et ainsi $a^{p-q+1}=a^{p-q}\star a=a$, $a^{p-q+2}=a^2$ et alors le groupe G serait égal à $\{e,a,a^2,\ldots,a^{p-q-1}\}$ et n'aurait pas n éléments. Ainsi $\{e,a,a^2,\ldots,a^{n-1}\}\subset G$ et les deux ensembles ont le même nombre n d'éléments, donc ils sont égaux.
Montrons maintenant que $a^n=e$. Comme $a^n\in G$ et que $G=\{e,a,a^2,\ldots,a^{n-1}\}$ alors il existe $0\leqslant p\leqslant n-1$ tel que $a^n=a^p$. Encore une fois si $p>0$ cela entraîne $a^{n-p}=e$ et donc une contradiction. Ainsi $p=0$ donc $a^n=a^0=e$.

Nous pouvons maintenant construire l'isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$. Soit $f:\mathbb{Z}/n\mathbb{Z}\longrightarrow G$ l'application définie par $f(\overline{k})=a^k$.

- Il faut tout d'abord montrer que f est bien définie car notre définition de f dépend du représentant k et pas de la classe $\overline{k}$: si $\overline{k}=\overline{k'}$ (une même classe définie par deux représentants distincts) alors $k\equiv k'\pmod n$ et donc il existe $\ell\in\mathbb{Z}$ tel que $k=k'+\ell n$. Ainsi $f(\overline{k})=a^k=a^{k'+\ell n}=a^{k'}\star a^{\ell n}=a^{k'}\star(a^n)^\ell=a^{k'}\star e^\ell=a^{k'}=f(\overline{k'})$. Ainsi f est bien définie.
- f est un morphisme de groupes car $f(\overline{k}+\overline{k'})=f(\overline{k+k'})=a^{k+k'}=a^k\star a^{k'}=f(\overline{k})\star f(\overline{k'})$ (pour tout $\overline{k},\overline{k'}$).
- Il est clair que f est surjective car tout élément de G s'écrit a^k.
- Comme l'ensemble de départ et celui d'arrivée ont le même nombre d'éléments et que f est surjective alors f est bijective.

Conclusion : f est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(G,\star)$. □

Mini-exercices.

1. Trouver tous les sous-groupes de $(\mathbb{Z}/12\mathbb{Z},+)$.
2. Montrer que le produit défini par $\overline{p}\times\overline{q}=\overline{p\times q}$ est bien défini sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$.
3. Dans la preuve du théorème 1, montrer directement que l'application f est injective.
4. Montrer que l'ensemble $\mathbb{U}_n=\{z\in\mathbb{C}\mid z^n=1\}$ est un sous-groupe de $(\mathbb{C}^*,\times)$. Montrer

que $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Expliciter l'isomorphisme.

5. Montrer que l'ensemble $H = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\}$ est un sous-groupe de $(\mathscr{Gl}_2, \times)$ ayant 4 éléments. Montrer que H *n'est pas* isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

3.3. Structure d'anneau

Définition 7.
On appelle **anneau** un ensemble A muni de deux lois de composition internes : une addition et une multiplication, satisfaisant aux axiomes suivants :

(P1) $(A,+)$ est un groupe commutatif (Abélien). L'élément neutre pour l'addition dans un anneau A est noté 0_A et est appelé **élément nul** de A.
Explicitement, pour tout $x,y,z \in A$ on a :
(1) $(x+y)+z = x+(y+z)$;
(2) $x+y) = y+x$;
(3) $x+0_A = 0_A+x = x$;
(4) $x+(-x) = (-x)+x = 0_A$.

(P2) La multiplication $\times$ est associative sur A.
Donc pour tout $x,y,z \in A$, on a : $x \times (y \times z) = (x \times y) \times z$.

(P3) La multiplication est distributive (à gauche et à droite) par rapport à l'addition sur A et admet un neutre différent de 0_A , noté 1_A appelé **élément unité**.
Explicitement, pour tout $x,y,z \in A$, on a :
(1) $x \times (y+z) = x \times y + x \times z$ et $(x+y) \times z = x \times z + y \times z$;
(2) $a \times 1_A = 1_A \times a$.

Remarque. Soit $(A,+,\times)$ un anneau quelconque.

- On dit que des éléments a et b de A **commutent** ou sont **permutables** si l'on a $ab = ba$.
- L'addition dans un anneau est toujours commutative, cependant la multiplication ne l'est pas nécessairement. Si la multiplication est commutative dans l'anneau $(A,+,\times)$, alors l'anneau est dit **commutatif** ou **abélien**.
- Une minorité d'auteurs définissent un anneau sans exiger l'existence d'un élément neutre pour la multiplication. Cette structure, qui n'est pas l'objet du présent ouvrage, est dite **pseudo-anneau** . Lorsqu'on évoque un anneau dans ce sens et pour éviter une confusion on précise généralement **anneau unitaire**, un anneau ayant un neutre multiplicatif.
- Quand il n y a pas d'ambiguïté on utilisera 0 à la place de 0_A, 1 à la place de 1_A et ab à la place de $a \times b$.

Exemples d'anneaux commutatifs

1. L'ensemble à un seul élément $A = \{0\}$ est un anneau commutatif fini, appelé **anneau nul**, ou **anneau trivial**. Dans cette anneau on a $0 = 1$. Notons que si A n'est pas l'anneau nul, alors $1 \neq 0$. L'anneau nul est donc le seul anneau dans lequel on a : $1 = 0$.
2. $(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs infinis.
3. L'ensemble $(\mathbb{Z}/n\mathbb{Z},+,\times)$ des classes de congruence modulo un nombre entier strictement positif donné n est un anneau commutatif fini.

4. L'ensemble des suites réelles, muni de l'addition et du produit des suites, est un anneau commutatif infini.
5. Si $I \subseteq \mathbb{R}$ alors l'ensemble $A(I,\mathbb{R})$ des applications de I vers $\mathbb{R}$ est un anneau commutatif avec les opérations $(f+g)(x) = f(x)+g(x)$ et $(fg)(x) = f(x)g(x)$.
6. Si $I \subseteq \mathbb{R}$ alors l'ensemble $C(I,\mathbb{R})$ des fonctions continues de I vers $\mathbb{R}$ constituent, pour l'addition et la multiplication usuelle, un anneau commutatif.
7. $A[X]$ l'ensemble des polynômes à coefficients dans un anneau commutatif A est aussi un anneau commutatif.
8. $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} : a,b \in \mathbb{Z}\}$.
9. $\mathbb{Z}[i] = \{a+bi | a,b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.
10. $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$.
11. $A[X]$ l'ensemble des polynômes à coefficients dans l'anneau intègre A.
12. Prenons $A = \mathbb{R}\times\mathbb{R}$. Pour $(a,b) \in A$ et $(c,d) \in A$, posons :
$$(a,b)+(c,d) = (a+c, b+d), \qquad (a,b)(c,d) = (ac, bd).$$
Alors A est un anneau commutatif, l'élément unité étant $(1,1)$ et l'élément nul étant $(0,0)$.
13. Soit $S = \{a,b\}$ avec les opérations définies par les tableaux suivants :

$+$	a	b
a	a	b
b	b	a

$\times$	a	b
a	a	a
b	a	b

Exemples d'un anneaux non commutatifs.

14. $M_n(\mathbb{Z})$ l'ensemble des matrices carrées à coefficient dans $\mathbb{Z}$, avec les opérations d'addition et de multiplication de matrices usuelles, est un anneau unitaire non commutatif.
15. Soit $T = \{a,b,c,d\}$ avec les opérations définies par les tableaux suivants :

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\times$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

Noter par exemple que $bc = a$ mais $cb = c$.

Contre-exemples

16. L'ensemble $\mathbb{N}$ des entiers naturels n'est pas un anneau, car ce n'est pas un groupe quand on le munit de l'addition : l'existence des opposés fait défaut. C'est un **semi-anneau**.
17. L'ensemble $2\mathbb{Z}$ des entiers (relatifs) pairs n'est pas un anneau, car sa multiplication n'a pas d'élément neutre. C'est un **pseudo-anneau**.

18. Pour tout groupe non trivial $(G,+)$, le groupe des applications de G dans G devient, lorsqu'on le munit de la composition $\circ$, un **presque-anneau** , mais pas un anneau même si G est commutatif, car la distributivité à gauche n'est pas vérifiée : on n'a pas $f\circ(g+h)=(f\circ g)+(f\circ h)$.

Règles de calculs dans un anneau

Dans un anneau, il est généralement impossible de simplifier dans une multiplication sans précautions. On sait par exemple que si des matrices carrées A,B et C vérifient l'identité $AB=AC$, on ne peut en déduire que $B=C$ et ce même si A n'est pas la matrice nulle.

Nous nous proposons de donner des règles de calcul qui nous permettent de développer les produits de sommes d'éléments d'un anneau A en tenant compte de l'ordre des termes. Si A est commutatif, on peut procéder à des simplifications.
Soit A un anneau. Toutes les règles de calcul valables dans un groupe abélien s'appliquent évidemment au groupe additif de A qui est l'ensemble A considéré comme groupe abélien. Par exemple, l'opposé d'un élément $a\in A$ se note $-a$ et on note $a+(-b)=a-b$.

Proposition 4.
Soient A un anneau et a,b des éléments non nuls de A. Alors ; pour tout $m,n\in\mathbb{N}$ on a :

1. $a0=0a=0$*, on dit que que* 0 *est absorbant pour la multiplication ;*
2. $a(-b)=(-a)b=-(ab)$*;*
3. $(-a)(-b)=ab$*;*
4. $(a)(-1)=(a)(-1)=-a$*;*
5. $(-a)(-1)=(-1)(-a)=-(-a)=a$.
6. $a^m\cdot a^n=a^{m+n}$.
7. $(m+n)a=ma+na$.

Démonstration. On fera les démonstrations quand a est à gauche. La même chose peut être faite quand a est à droite.

1. $a0=a(0+0)=a0+a0\Rightarrow a0=0$.
2. $ab+a(-b)=a(b-b)=a0\Rightarrow a(-b)=-ab$;
3. $(-a)(-b)=-(a(-b))=-(-ab)=ab$;
4. On remplace b par 1 dans (2) ;
5. On remplace b par 1 dans (3) .
6. On définit par récurrence pour $n\in\mathbb{N}$; $a^0=1, a^n=aa^{n-1}$
7. On définit par récurrence pour $n\in\mathbb{N}$; $0a=0, na=a+(n-1)a$.

□

Proposition 5.
Soit A un anneau et soient a et b deux éléments permutables de A. Pour tout entier $n > 1$, on a :

1. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, *la formule dite du binôme.*
2. $(a^n - b^n) = (a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} = (a-b)(b^{n-1} + ab^{n-2} + a^2 b^{n-3} + \cdots + a^{n-1})$.
3. $(1-a^n) = (1-a)\sum_{k=0}^{n-1} a^k = (1-a)(1+a+a^2+\cdots+a^{n-1})$.

Démonstration. Les preuves sont classique et se font par récurrence sur n.

3.4. Anneaux intègres

Dans cette section nous allons donner deux cas particuliers importants d'anneaux, les anneaux intègres et les corps. Ces anneaux jouent un rôle principale dans la résolution des équations.

Supposons que nous voulons résoudre l'équation $P(x) = x^2 - 3x + 2 = 0$ dans $\mathbb{R}$. On factorise le coté gauche comme suit :

$$x^2 - 3x + 2 = (x-1)(x-2) = 0 \quad \text{on obtient le solutions} \quad x = 1, 2.$$

Dans ce processus on a utiliser une propriété des réels très importante :

« Un produit de facteurs est nul si et seulement si l'un des facteurs est nul »

Cette propriété est valide das $\mathbb{R}$ par exemple, mais ne l'est pas toujours vraie dans d'autre structures algébriques. Penons par exemple la même équation dans l'anneau $\mathbb{Z}/6\mathbb{Z}$, soit

$$P(x) = x^2 - 3x + 2 \equiv 0(\mod 6).$$

On a $P(1) = P(2) = 0 \equiv 0(\mod 6)$ donc $x = 1, 2$ sont des solutions. Mais on a aussi $P(4) = 6 \equiv 0(\mod 6)$ et $P(5) = 12 \equiv 0(\mod 6)$, donc $x = 4, 5$ sont aussi des solutions. Donc la propriété précédente n'est vraie dans le cas de $\mathbb{Z}/6\mathbb{Z}$.

Éléments particuliers d'un anneau

Soit A un anneau et soit $a \in A$. Alors nous savons que $a \cdot 0 = 0 \cdot a = 0$. On voit ainsi que dans un anneau, le produit de deux facteurs est nul lorsque l'un des facteurs est nul. La réciproque est inexacte comme le montre l'exemple suivant.

Prenons $A = \mathbb{R} \times \mathbb{R}$. Pour $(a, b) \in A$ et $(c, d) \in A$, posons :

$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b)(c, d) = (ac, bd).$$

Alors A est un anneau commutatif, l'élément unité étant $(1, 1)$ et l'élément nul étant $(0, 0)$. On a $(1, 0)(0, 1) = (0, 0) = 0$ et pourtant $(1, 0) \neq 0$ et $(0, 1) \neq 0$.

Nous donnons dans cette section des éléments particuliers dans un anneau qui jouent un rôle significatif dans les structures algébriques liées aux anneaux.

Définition 8.
Soit a un élément **non nul** d'un anneau commutatif A. On dit que :

1. a est un **diviseur** b s'il existe $c \in A$ tel que $b = ca$. On note $a|b$.
2. a est un **diviseur de** 0 s'il existe $b \in A$ non nul et $ab = ba = 0$;
3. a est **simplifiable** (ou régulier) si pour tout élément non nul $x \in A$, on a $ax \neq 0$ et $xa \neq 0$;
4. a est **inversible** ou **unité** s'il existe $b \in A$ tel que $ab = ba = 1$;
5. a est **nilpotent** s'il existe un entier $n \geqslant 1$ tel que $a^n = 0$.

Dans $(\mathbb{Z},+,\cdot)$ on a $x\cdot y=0$ implique $x=0$ ou bien $y=0$. Cela n'est pas nécessairement vrai en algèbre générale. Par exemple dans l'anneau commutatif $\mathbb{Z}/6\mathbb{Z}$ on a $2\cdot 3\equiv 0(\mod 6)$. On dit alors que 2 et 3 sont des diviseurs de 0 dans $\mathbb{Z}/6\mathbb{Z}$.

Dans $M_2(\mathbb{Z})$, l'ensemble des matrices carrées à coefficients dans $\mathbb{Z}$, on a :

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

Donc les matrices $\begin{pmatrix}1&1\\0&0\end{pmatrix}$ et $\begin{pmatrix}1&0\\-1&0\end{pmatrix}$ sont des diviseurs de 0 dans $M_2(\mathbb{Z})$.

Puisque dans $\mathbb{Z}/6\mathbb{Z}$ on a $2\cdot 3\equiv 0(\mod 6)$, alors 2 et 3 ne sont pas simplifiables.
En fait tout diviseur de zéro n'est pas simplifiable.

Exemples

1. Les anneaux $\mathbb{Z},\mathbb{Q},\mathbb{R}$ et $\mathbb{C}$ nont pas de diviseurs de 0.
2. Dans l'anneau $\mathbb{Z}/12\mathbb{Z}$ les éléments $1,2,3,4,6,12$ sont tous des diviseurs de 0.
3. Les diviseurs de zéro dans $(\mathbb{Z}/n\mathbb{Z})$ sont les éléments p,q tels que $pq\equiv 0(\mod n)$.
4. Si p est premier alors $(\mathbb{Z}/p\mathbb{Z})$ n'a pas de diviseur de zéro.
5. Tout élément nilpotent est un diviseur de zéro.
6. Les inversibles de $(\mathbb{Z},+,\times)$ sont ± 1, donc $\mathbb{Z}^\times=\pm 1$.
7. $\mathbb{Q}^\times=\mathbb{Q}-\{0\}$, $\mathbb{R}^\times=\mathbb{R}-\{0\}$ et $\mathbb{C}^\times=\mathbb{C}-\{0\}$.
8. Les inversibles de $(K[X],+,\times)$ sont les constantes non nulles.
9. Les inversibles de $C(X,\mathbb{R})$ sont les fonctions qui ne s'annulent pas.
10. Les inversibles de $(\mathbb{Z}[X],+,\times)$ sont ± 1.
11. Les inversibles de $(\mathbb{Z}/n\mathbb{Z},+,\times)$ sont les éléments p,q tels que $pq\equiv 1(\mod n)$.
12. L'élément 2 est nilpotent dans $\mathbb{Z}/2\mathbb{Z}$ car $2^2\equiv 0(\mod 2)$.
13. L'élément 3 est nilpotent dans $\mathbb{Z}/9\mathbb{Z}$ car on a $3^2\equiv 0(\mod 9)$.
14. L'élément $M=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ est nilpotent dans $M_2(\mathbb{Z})$ car on a $M^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

Propriétés des anneaux

Soit $(A,+,\cdot)$ un anneau, alors on a les résultats suivants.

- S'il existe, l'inverse de a est unique et on le note a^{-1}.
- L'inverse de 1 est lui même, i.e. $(1)^{-1}=1$.
- L'élément 0 n'est pas inversible sauf si l'anneau est trivial ; car si 0 avait un inverse b, on aurait $0\cdot b=1\Rightarrow 0=1$.
- Un élément inversible n'est jamais un diviseur de 0.

- A^* l'ensemble des inversibles de A , est stable pour la multiplication car on a , $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$.
- $(A^\times,\cdot)$ est un groupe. (Pourquoi ?)
- Les éléments simplifiables sont ceux qui ne divisent pas zéro.
- Aucun élément nilpotent ne peut être une unité (excepté dans l'anneau trivial 0 qui possède seulement un élément $0 = 1$).
- Tous les éléments nilpotents non nuls sont des diviseurs de zéro.
- Si x est nilpotent, alors on a $(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1-x^n = 1$ donc $(1-x)$ est inversible.
- Les éléments nilpotents d'un anneau commutatif forment un idéal.

Anneaux intègres

On a vue que dans l'un anneau non commutatif $M_n(\mathbb{Z})$, $A\cdot B = 0$ n'entraîne pas $A = 0$ ou $B = 0$. On dit alors que $M_n(\mathbb{Z})$ n'est pas un anneau intègre.

Définition 9.
L'anneau (commutatif non trivial) A est dit **intègre** si, $ab = 0$ implique $a = 0$ ou $b = 0$.

Une définition équivalente est que A est intègre si tout élément non nul de A est simplifiable.

Remarque.
Dans un anneau intègre le produit d'éléments non nuls est non nul.
Si $a, b \in A$ avec $a \neq 0, b \neq 0$, alors le produit $ab \neq 0$.

Exemples d'anneaux intègres

1. $(\mathbb{Z},+,\times)$ est anneau intègre.
2. $(\mathbb{Q},+,\times),(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux intègres.
3. $\mathbb{Z}[i] = \{a+bi | a,b\in\mathbb{Z}\}$ l'ensemble des entiers de Gauss.
4. $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$.
5. $A[X]$ l'ensemble des polynômes à coefficients dans l'anneau intègre A.
6. $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} : a,b\in\mathbb{Z}\}$.
7. $\mathbb{Z}/p\mathbb{Z}$ avec p premier.
8. Tout sous-anneau d'un anneau intègre est intègre.

Exemples d'anneaux non intègres

9. $\mathbb{Z}/n\mathbb{Z}$ avec n réductible (non premier) n'est pas intègre.
   On vue que dans $\mathbb{Z}/6\mathbb{Z}$, $2\cdot 3 = 0$.

10. $M_n(\mathbb{Z})$ l'ensemble des matrices carrées à coefficients dans $\mathbb{Z}$ n'est pas intègre.
    On a $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ mais $M^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.
11. $C(\mathbb{R},\mathbb{R})$ l'anneau des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ n'est pas intègre, car $f(x) = x+|x|$ et $g(x) = x-|x|$ sont non nuls et continues mais leur produit $f(x)\cdot g(x) = 0$.

Remarque
L'équation $2x = 3$ n'a pas de solution dans $\mathbb{Z}$ mais possède une solutions unique $x = 3/2$ dans $\mathbb{Q}$. Cependant l'équation $x^2 = 1$ n'a pas de solution dans $\mathbb{R}$ mais possède deux solutions $x = \pm i$ dans $\mathbb{C}$. Donc, l'existence de solution(s) dépend de l'équation et de la structure algébrique où on travail.

Théorème 2 (Simplification)**.**
Soit A un anneau intègre et $a, b, c \in A$. Si $a \neq 0$ et $ab = ac$, alors $b = c$.

Démonstration.

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0.$$

Puisque $a \neq 0$ et A est intègre alors $b - c = 0 \Rightarrow b = c$. □

Corollaire 1.
Soient A un anneau intègre, $a \in A, a \neq 0$, et $ax = 0$ alors $x = 0$.

Démonstration.

$$ax = b \Rightarrow a^{-1}ax = a^{-1}b \Rightarrow x = a^{-1}b.$$

Si $a^{-1}b \notin A$ alors l'équation n'a pas de solution, sinon sa solution est $x = a^{-1}b$.
Dans notre cas $b = 0$ donc $x = 0$. □

Corollaire 2.
Soit A un anneau intègre. Alors tout polynôme de degré $n \geqslant 0$ admet au plus n zéros dans A.

3.5. Corps

Définition 10.
(1) Un **corps** $(K,+,\cdot)$ est un anneau commutatif non trivial dans lequel tout élément non nul est inversible.

(2) Si $(K,+,\cdot)$ est un corps, un sous-corps de K est un sous-anneau K_1 de K tel que pour tout élément non nul x de K_1 , on a $x^{-1} \in K_1$; $(K_1,+,\cdot)$ est alors un corps.

Remarques.

1. Un élément inversible n'est jamais un diviseur de 0.
2. Tout corps est un anneau intègre (la réciproque est évidemment fausse).
3. K est corps si et seulement si les inversibles de K, $K^\times = K - \{0\}$.
4. Tout sous-anneau d'un corps est intègre.

Proposition 6.
Tout corps est un anneau intègre .

Démonstration. Supposons que $a \neq 0$ et $ab = 0$. Puisque $a \neq 0$, a^{-1} existe et

$$a^{-1}ab = a^{-1}0 \Rightarrow 1b = 0 \Rightarrow b = 0.$$

Donc est un anneau intègre . □

Proposition 7.
Tout anneau intègre fini K est un corps fini.

Démonstration. On doit montrer que tout $a \in K$ et $a \neq 0$ est inversible.
Si $a = 1$ alors $a^{-1} = 1$ et donc a est inversible.
Supposons donc que $a \neq 1$ et considérons la suite d'éléments de K : $a, a^2, a^3, a^4, \ldots$.
Puisque K est fini, il existe $i, j \in \mathbb{N}$ avec $i > j$ et $a^i = a^j$.
Par simplification , $a^{i-j} = 1$. Puisque $a \neq 1, i - j > 0 \Rightarrow a^{i-i-1} = a^{-1}$.
Donc a est inversible et par conséquence K est un corps. □

Proposition 8.
$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Démonstration. En effet, p est premier équivaut à ce que 0 ne soit pas produit de deux entiers non nuls modulo p, par le lemme d'Euclide. Il faut donc que p soit premier pour que $\mathbb{Z}/p\mathbb{Z}$ soit un corps.
De plus, ceci assure que si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est intègre et partant, comme il est fini, un corps. L'identité de Bézout assure directement l'existence d'un inverse, et un calcul efficace de celui-ci par l'algorithme d'Euclide étendu. □

Exemples de corps et sous-corps.

1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
2. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, où p est un nombre premier, est un corps commutatif.
3. $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$ est sous corps de de $\mathbb{R}$.
4. $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}, i^2 = -1\}$ est un sous corps de de $\mathbb{C}$.
5. $\mathbb{Z}$ n'est pas un corps car 2 n'est pas inversible.
6. $\mathbb{Z}/n\mathbb{Z}$, où n n'est pas un nombre premier, n'est pas un corps.
7. $A = \mathbb{R}^2$, et pour $(a, b) \in A$ et $(c, d) \in A$, posons :
$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b)(c, d) = (ac, bd).$$
Alors A est un corps, l'élément unité étant $(1, 1)$ et l'élément nul étant $(0, 0)$.

Corps finis

En mathématiques et plus précisément en algèbre, un corps fini est un corps commutatif qui est par ailleurs fini. À isomorphisme près, un corps fini est entièrement déterminé par son cardinal, qui est toujours une puissance d'un nombre premier, ce nombre premier étant sa caractéristique.

Les corps finis sont utilisés en théorie algébrique des nombres, où ils apparaissent comme une structure essentielle à la géométrie arithmétique. Cette branche a permis, entre autres, de démontrer le dernier théorème de Fermat.

Les corps finis ont trouvé de nouvelles applications avec le développement de l'informatique. En théorie des codes, ils permettent par exemple de déterminer des codes correcteurs efficaces. Ils interviennent également en cryptographie, dans la conception des chiffrements à clé secrète comme le standard AES, ainsi que dans celle des chiffrement à clé publique, à travers, entre autres, le problème du logarithme discret.

Remarque sur la terminologie : une convention courante en français est de considérer qu'un corps n'est pas nécessairement commutatif. Dans le cas des corps finis, la convention est en fait de peu d'importance car, d'après le théorème de Wedderburn, tout corps fini est commutatif, et, dans cet article les corps seront supposés d'emblée commutatifs.

Les corps finis sont (ou ont été) appelés également corps de Galois, ou plus rarement champs de Galois. Ils ont été en effet étudiés par Évariste Galois dans un article publié en 1830 qui est à l'origine de la théorie. En fait, Carl Friedrich Gauss avait déjà découvert les résultats de Galois à la fin du xviiie siècle mais n'en fit pas état ; ses travaux ne furent connus qu'après sa mort et n'eurent pas l'influence de ceux de Galois.

Le corps fini de cardinal q (nécessairement puissance d'un nombre premier) est noté F_q (de l'anglais field qui signifie corps commutatif) ou $GF(q)$ (Galois field).

Le plus petit corps

Le plus petit corps fini est noté F_2. Il est composé de deux éléments distincts, 0 qui est

l'élément neutre pour l'addition, et 1 qui est élément neutre pour la multiplication. Ceci détermine les tables de ces deux opérations en dehors de 1+1 qui ne peut alors être que 0, car 1 doit avoir un opposé. On vérifie alors qu'elles définissent bien un corps commutatif.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Le corps F_2 peut s'interpréter diversement. C'est l'anneau $\mathbb{Z}/2\mathbb{Z}$, les entiers pris modulo 2, c'est-à-dire que 0 représente les entiers pairs, 1 les entiers impairs (c'est le reste de leur division par 2), et les opérations se déduisent de celles sur $\mathbb{Z}$.

C'est aussi l'ensemble des valeurs de vérité classiques, 0 pour le faux, et 1 pour le vrai. L'addition est le « ou exclusif » (xor), la multiplication le « et ».

Une généralisation naturelle de $F_2 = \mathbb{Z}/2\mathbb{Z}$ est, pour p premier, le corps $\mathbb{Z}/p\mathbb{Z}$ à p éléments, noté aussi F_p, qu'on a montrer est un corps fini de cardinal p.

Il est vrai que pour tout nombre premier p, $\mathbb{Z}/p\mathbb{Z}$ est à isomorphisme près le seul corps de cardinal p, et qu'il ne contient pas d'autre sous-corps que lui-même. Un tel corps est appelé corps premier, et les $\mathbb{Z}/p\mathbb{Z}$, p premier, sont les seuls corps premiers finis.

Chapitre 4

Anneau de polynômes

Motivation

Les polynômes sont des objets très simples mais aux propriétés extrêmement riches. Vous savez déjà résoudre les équations de degré 2 : $aX^2+bX+c=0$. Savez-vous que la résolution des équations de degré 3, $aX^3+bX^2+cX+d=0$, a fait l'objet de luttes acharnées dans l'Italie du XVI^{e} siècle ? Un concours était organisé avec un prix pour chacune de trente équations de degré 3 à résoudre. Un jeune italien, Tartaglia, trouve la formule générale des solutions et résout les trente équations en une seule nuit ! Cette méthode que Tartaglia voulait garder secrète sera quand même publiée quelques années plus tard comme la « méthode de Cardan ». Dans ce chapitre, après quelques définitions des concepts de base, nous allons étudier l'arithmétique des polynômes. Il y a une grande analogie entre l'arithmétique des polynômes et celles des entiers. On continue avec un théorème fondamental de l'algèbre : « Tout polynôme de degré n admet n racines complexes. » On termine avec les fractions rationnelles : une fraction rationnelle est le quotient de deux polynômes.

Dans ce chapitre $\mathbb{K}$ désignera l'un des corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

4.1. Définitions

Définitions

Définition 1.
Un **polynôme** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$P(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_2X^2+a_1X+a_0,$$

avec $n\in\mathbb{N}$ et $a_0,a_1,\ldots,a_n\in\mathbb{K}$.
L'ensemble des polynômes est noté $\mathbb{K}[X]$.

- Les a_i sont appelés les **coefficients** du polynôme.
- Si tous les coefficients a_i sont nuls, P est appelé le **polynôme nul**, il est noté 0.
- On appelle le **degré** de P le plus grand entier i tel que $a_i\neq 0$; on le note $\deg P$. Pour le degré du polynôme nul on pose par convention $\deg(0)=-\infty$.

- Un polynôme de la forme $P = a_0$ avec $a_0 \in \mathbb{K}$ est appelé un **polynôme constant**. Si $a_0 \neq 0$, son degré est 0.

Exemple 1.

- $X^3 - 5X + \frac{3}{4}$ est un polynôme de degré 3.
- $X^n + 1$ est un polynôme de degré n.
- 2 est un polynôme constant, de degré 0.

Opérations sur les polynômes

- **Égalité.** Soient $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ et $Q = b_n X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0$ deux polynômes à coefficients dans $\mathbb{K}$.
$$P = Q \iff \forall i \quad a_i = b_i$$
et on dit que P et Q sont égaux.
- **Addition.** Soient $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ et $Q = b_n X^n + b_{n-1}X^{n-1} + \cdots + b_1 X + b_0$.
On définit :
$$P + Q = (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \cdots + (a_1 + b_1)X + (a_0 + b_0)$$
- **Multiplication.** Soient $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ et $Q = b_m X^m + b_{m-1}X^{m-1} + \cdots + b_1 X + b_0$. On définit
$$P \times Q = c_r X^r + c_{r-1}X^{r-1} + \cdots + c_1 X + c_0$$
$$\text{avec } r = n + m \text{ et } c_k = \sum_{i+j=k} a_i b_j \text{ pour } k \in \{0, \ldots, r\}.$$
- **Multiplication par un scalaire.** Si $\lambda \in \mathbb{K}$ alors $\lambda \cdot P$ est le polynôme dont le i-ème coefficient est λa_i.

Exemple 2.

- Soient $P = aX^3 + bX^2 + cX + d$ et $Q = \alpha X^2 + \beta X + \gamma$. Alors $P + Q = aX^3 + (b + \alpha)X^2 + (c + \beta)X + (d + \gamma)$, $P \times Q = (a\alpha)X^5 + (a\beta + b\alpha)X^4 + (a\gamma + b\beta + c\alpha)X^3 + (b\gamma + c\beta + d\alpha)X^2 + (c\gamma + d\beta)X + d\gamma$. Enfin $P = Q$ si et seulement si $a = 0$, $b = \alpha$, $c = \beta$ et $d = \gamma$.
- La multiplication par un scalaire $\lambda \cdot P$ équivaut à multiplier le polynôme constant λ par le polynôme P.

L'addition et la multiplication se comportent sans problème :

Proposition 1.
Pour $P, Q, R \in \mathbb{K}[X]$ alors

- $0 + P = P, \quad P + Q = Q + P, \quad (P + Q) + R = P + (Q + R)$;
- $1 \cdot P = P, \quad P \times Q = Q \times P, \quad (P \times Q) \times R = P \times (Q \times R)$;
- $P \times (Q + R) = P \times Q + P \times R$.

Pour le degré il faut faire attention :

Proposition 2.
Soient P et Q deux polynômes à coefficients dans $\mathbb{K}$.

$$\boxed{\deg(P\times Q)=\deg P+\deg Q}$$

$$\boxed{\deg(P+Q)\leqslant \max(\deg P,\deg Q)}$$

On note $\mathbb{R}_n[X]=\{P\in\mathbb{R}[X]\mid \deg P\leqslant n\}$. Si $P,Q\in\mathbb{R}_n[X]$ alors $P+Q\in\mathbb{R}_n[X]$.

Vocabulaire

Complétons les définitions sur les polynômes.

Définition 2.

- Les polynômes comportant un seul terme non nul (du type a_kX^k) sont appelés **monômes**.
- Soit $P=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0$, un polynôme avec $a_n\neq 0$. On appelle **terme dominant** le monôme a_nX^n. Le coefficient a_n est appelé le **coefficient dominant** de P.
- Si le coefficient dominant est 1, on dit que P est un **polynôme unitaire**.

Exemple 3.
$P(X)=(X-1)(X^n+X^{n-1}+\cdots+X+1)$. On développe cette expression : $P(X)=\big(X^{n+1}+X^n+\cdots+X^2+X\big)-\big(X^n+X^{n-1}+\cdots+X+1\big)=X^{n+1}-1$. $P(X)$ est donc un polynôme de degré $n+1$, il est unitaire et est somme de deux monômes : X^{n+1} et -1.

Remarque.
Tout polynôme est donc une somme finie de monômes.

Mini-exercices.

1. Soit $P(X)=3X^3-2$, $Q(X)=X^2+X-1$, $R(X)=aX+b$. Calculer $P+Q$, $P\times Q$, $(P+Q)\times R$ et $P\times Q\times R$. Trouver a et b afin que le degré de $P-QR$ soit le plus petit possible.
2. Calculer $(X+1)^5-(X-1)^5$.
3. Déterminer le degré de $(X^2+X+1)^n-aX^{2n}-bX^{2n-1}$ en fonction de a,b.
4. Montrer que si $\deg P\neq\deg Q$ alors $\deg(P+Q)=\max(\deg P,\deg Q)$. Donner un contre-exemple dans le cas où $\deg P=\deg Q$.
5. Montrer que si $P(X)=X^n+a_{n-1}X^{n-1}+\cdots$ alors le coefficient devant X^{n-1} de $P(X-\frac{a_{n-1}}{n})$ est nul.

4.2. Arithmétique des polynômes

Il existe de grandes similitudes entre l'arithmétique dans $\mathbb{Z}$ et l'arithmétique dans $\mathbb{K}[X]$. Cela nous permet d'aller assez vite et d'omettre certaines preuves.

Division euclidienne

Définition 3.
Soient $A, B \in \mathbb{K}[X]$, on dit que B **divise** A s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B|A$.

On dit aussi que A est multiple de B ou que A est divisible par B.
Outre les propriétés évidentes comme $A|A$, $1|A$ et $A|0$ nous avons :

Proposition 3.
Soient $A, B, C \in \mathbb{K}[X]$.

1. *Si $A|B$ et $B|A$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.*
2. *Si $A|B$ et $B|C$ alors $A|C$.*
3. *Si $C|A$ et $C|B$ alors $C|(AU + BV)$, pour tout $U, V \in \mathbb{K}[X]$.*

Théorème 1 (Division euclidienne des polynômes)**.**
Soient $A, B \in \mathbb{K}[X]$, avec $B \neq 0$, alors il existe un unique polynôme Q et il existe un unique polynôme R tels que :

$$\boxed{A = BQ + R \quad \text{et} \quad \deg R < \deg B.}$$

Q est appelé le **quotient** et R le **reste** et cette écriture est la **division euclidienne** de A par B.
Notez que la condition $\deg R < \deg B$ signifie $R = 0$ ou bien $0 \leqslant \deg R < \deg B$.
Enfin $R = 0$ si et seulement si $B|A$.

Démonstration.
Unicité. Si $A = BQ + R$ et $A = BQ' + R'$, alors $B(Q - Q') = R' - R$. Or $\deg(R' - R) < \deg B$. Donc $Q' - Q = 0$. Ainsi $Q = Q'$, d'où aussi $R = R'$.
Existence. On montre l'existence par récurrence sur le degré de A.

- Si $\deg A = 0$ et $\deg B > 0$, alors A est une constante, on pose $Q = 0$ et $R = A$. Si $\deg A = 0$ et $\deg B = 0$, on pose $Q = A/B$ et $R = 0$.
- On suppose l'existence vraie lorsque $\deg A \leqslant n-1$. Soit $A = a_n X^n + \cdots + a_0$ un polynôme de degré n ($a_n \neq 0$). Soit $B = b_m X^m + \cdots + b_0$ avec $b_m \neq 0$. Si $n < m$ on pose $Q = 0$ et $R = A$.

  Si $n \geqslant m$ on écrit $A = B \cdot \frac{a_n}{b_m} X^{n-m} + A_1$ avec $\deg A_1 \leqslant n - 1$. On applique l'hypothèse de récurrence à A_1 : il existe $Q_1, R_1 \in \mathbb{K}[X]$ tels que $A_1 = BQ_1 + R_1$ et $\deg R_1 < \deg B$. Il

vient :

$$A = B\left(\frac{a_n}{b_m}X^{n-m} + Q_1\right) + R_1.$$

Donc $Q = \frac{a_n}{b_m}X^{n-m} + Q_1$ et $R = R_1$ conviennent.

□

Exemple 4.

On pose une division de polynômes comme on pose une division euclidienne de deux entiers. Par exemple si $A = 2X^4 - X^3 - 2X^2 + 3X - 1$ et $B = X^2 - X + 1$. Alors on trouve $Q = 2X^2 + X - 3$ et $R = -X + 2$. On n'oublie pas de vérifier qu'effectivement $A = BQ + R$.

$$\begin{array}{rl|l}
 & 2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\
- & \underline{2X^4 - 2X^3 + 2X^2} & \\
 & X^3 - 4X^2 + 3X - 1 & 2X^2 + X - 3 \\
- & \underline{X^3 - X^2 + X} & \\
 & -3X^2 + 2X - 1 & \\
- & \underline{-3X^2 + 3X - 3} & \\
 & -X + 2 &
\end{array}$$

Exemple 5.

Pour $X^4 - 3X^3 + X + 1$ divisé par $X^2 + 2$ on trouve un quotient égal à $X^2 - 3X - 2$ et un reste égale à $7X + 5$.

$$\begin{array}{rl|l}
 & X^4 - 3X^3 + X + 1 & X^2 + 2 \\
- & \underline{X^4 + 2X^2} & \\
 & -3X^3 - 2X^2 + X + 1 & X^2 - 3X - 2 \\
- & \underline{-3X^3 - 6X} & \\
 & -2X^2 + 7X + 1 & \\
- & \underline{-2X^2 - 4} & \\
 & 7X + 5 &
\end{array}$$

pgcd

Proposition 4.

Soient $A, B \in \mathbb{K}[X]$, avec $A \neq 0$ ou $B \neq 0$. Il existe un unique polynôme unitaire de plus grand degré qui divise à la fois A et B.

Cet unique polynôme est appelé le **pgcd** (plus grand commun diviseur) de A et B que l'on note $\text{pgcd}(A, B)$.

Remarque.

- $\text{pgcd}(A,B)$ est un polynôme unitaire.
- Si $A|B$ et $A \neq 0$, $\text{pgcd}(A,B) = \frac{1}{\lambda}A$, où λ est le coefficient dominant de A.
- Pour tout $\lambda \in K^*$, $\text{pgcd}(\lambda A, B) = \text{pgcd}(A,B)$.
- Comme pour les entiers : si $A = BQ + R$ alors $\text{pgcd}(A,B) = \text{pgcd}(B,R)$. C'est ce qui justifie l'algorithme d'Euclide.

Algorithme d'Euclide.
Soient A et B des polynômes, $B \neq 0$.
On calcule les divisions euclidiennes successives,

$$\begin{array}{ll} A = BQ_1 + R_1 & \deg R_1 < \deg B \\ B = R_1Q_2 + R_2 & \deg R_2 < \deg R_1 \\ R_1 = R_2Q_3 + R_3 & \deg R_3 < \deg R_2 \\ \vdots & \\ R_{k-2} = R_{k-1}Q_k + R_k & \deg R_k < \deg R_{k-1} \\ R_{k-1} = R_kQ_{k+1} & \end{array}$$

Le degré du reste diminue à chaque division. On arrête l'algorithme lorsque le reste est nul.
Le pgcd est le dernier reste non nul R_k (rendu unitaire).

Exemple 6.
Calculons le pgcd de $A = X^4 - 1$ et $B = X^3 - 1$. On applique l'algorithme d'Euclide :

$$\begin{aligned} X^4 - 1 &= (X^3 - 1) \times X + X - 1 \\ X^3 - 1 &= (X - 1) \times (X^2 + X + 1) + 0 \end{aligned}$$

Le pgcd est le dernier reste non nul, donc $\text{pgcd}(X^4 - 1, X^3 - 1) = X - 1$.

Exemple 7.
Calculons le pgcd de $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ et $B = X^4 + 2X^3 + X^2 - 4$.

$$\begin{aligned} X^5 + X^4 + 2X^3 + X^2 + X + 2 &= (X^4 + 2X^3 + X^2 - 4) \times (X - 1) + 3X^3 + 2X^2 + 5X - 2 \\ X^4 + 2X^3 + X^2 - 4 &= (3X^3 + 2X^2 + 5X - 2) \times \tfrac{1}{9}(3X + 4) - \tfrac{14}{9}(X^2 + X + 2) \\ 3X^3 + 2X^2 + 5X - 2 &= (X^2 + X + 2) \times (3X - 1) + 0 \end{aligned}$$

Ainsi $\text{pgcd}(A,B) = X^2 + X + 2$.

Définition 4.
Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont **premiers entre eux** si $\text{pgcd}(A,B) = 1$.

Pour A, B quelconques on peut se ramener à des polynômes premiers entre eux : si $\text{pgcd}(A,B) = D$ alors A et B s'écrivent : $A = DA'$, $B = DB'$ avec $\text{pgcd}(A', B') = 1$.

Théorème de Bézout

Théorème 2 (Théorème de Bézout)**.**
Soient $A, B \in \mathbb{K}[X]$ des polynômes avec $A \neq 0$ ou $B \neq 0$. On note $D = \text{pgcd}(A, B)$. Il existe deux polynômes $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.

Ce théorème découle de l'algorithme d'Euclide et plus spécialement de sa remontée comme on le voit sur l'exemple suivant.

Exemple 8.
Nous avons calculé $\text{pgcd}(X^4-1, X^3-1) = X-1$. Nous remontons l'algorithme d'Euclide, ici il n'y avait qu'une ligne : $X^4 - 1 = (X^3-1) \times X + X - 1$, pour en déduire $X - 1 = (X^4-1) \times 1 + (X^3-1) \times (-X)$. Donc $U = 1$ et $V = -X$ conviennent.

Exemple 9.
Pour $A = X^5 + X^4 + 2X^3 + X^2 + X + 2$ et $B = X^4 + 2X^3 + X^2 - 4$ nous avions trouvé $D = \text{pgcd}(A, B) = X^2 + X + 2$. En partant de l'avant dernière ligne de l'algorithme d'Euclide on a d'abord : $B = (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X+4) - \frac{14}{9}D$ donc

$$-\frac{14}{9}D = B - (3X^3 + 2X^2 + 5X - 2) \times \frac{1}{9}(3X+4).$$

La ligne au-dessus dans l'algorithme d'Euclide était : $A = B \times (X-1) + 3X^3 + 2X^2 + 5X - 2$. On substitue le reste pour obtenir :

$$-\frac{14}{9}D = B - \big(A - B \times (X-1)\big) \times \frac{1}{9}(3X+4).$$

On en déduit

$$-\frac{14}{9}D = -A \times \frac{1}{9}(3X+4) + B\Big(1 + (X-1) \times \frac{1}{9}(3X+4)\Big)$$

Donc en posant $U = \frac{1}{14}(3X+4)$ et $V = -\frac{1}{14}\big(9 + (X-1)(3X+4)\big) = -\frac{1}{14}(3X^2 + X + 5)$ on a $AU + BV = D$.

Le corollaire suivant s'appelle aussi le théorème de Bézout.

Corollaire 1.
Soient A et B deux polynômes. A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.

Corollaire 2.
Soient $A, B, C \in \mathbb{K}[X]$ avec $A \neq 0$ ou $B \neq 0$. Si $C|A$ et $C|B$ alors $C|\,\text{pgcd}(A, B)$.

Corollaire 3 (Lemme de Gauss)**.**
Soient $A, B, C \in \mathbb{K}[X]$. Si $A|BC$ et $\text{pgcd}(A, B) = 1$ alors $A|C$.

ppcm

Proposition 5.
Soient $A, B \in \mathbb{K}[X]$ des polynômes non nuls, alors il existe un unique polynôme unitaire M de plus petit degré tel que $A|M$ et $B|M$.

Cet unique polynôme est appelé le **ppcm** (plus petit commun multiple) de A et B qu'on note $\text{ppcm}(A,B)$.

Exemple 10.
$\text{ppcm}\left(X(X-2)^2(X^2+1)^4, (X+1)(X-2)^3(X^2+1)^3\right) = X(X+1)(X-2)^3(X^2+1)^4$.

De plus le ppcm est aussi le plus petit au sens de la divisibilité :

Proposition 6.
Soient $A, B \in \mathbb{K}[X]$ des polynômes non nuls et $M = \text{ppcm}(A,B)$. Si $C \in \mathbb{K}[X]$ est un polynôme tel que $A|C$ et $B|C$, alors $M|C$.

Mini-exercices.

1. Trouver les diviseurs de X^4+2X^2+1 dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
2. Montrer que $X-1|X^n-1$ (pour $n \geqslant 1$).
3. Calculer les divisions euclidiennes de A par B avec $A = X^4-1$, $B = X^3-1$. Puis $A = 4X^3+2X^2-X-5$ et $B = X^2+X$; $A = 2X^4-9X^3+18X^2-21X+2$ et $B = X^2-3X+1$; $A = X^5-2X^4+6X^3$ et $B = 2X^3+1$.
4. Déterminer le pgcd de $A = X^5+X^3+X^2+1$ et $B = 2X^3+3X^2+2X+3$. Trouver les coefficients de Bézout U, V. Mêmes questions avec $A = X^5-1$ et $B = X^4+X+1$.
5. Montrer que si $AU+BV = 1$ avec $\deg U < \deg B$ et $\deg V < \deg A$ alors les polynômes U, V sont uniques.

4.3. Racine d'un polynôme, factorisation

Racines d'un polynôme

Définition 5.
Soit $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$. Pour un élément $x \in \mathbb{K}$, on note $P(x) = a_n x^n + \cdots + a_1 x + a_0$. On associe ainsi au polynôme P une **fonction polynôme** (que l'on note encore P)

$$P : \mathbb{K} \to \mathbb{K}, \quad x \mapsto P(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Définition 6.
Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une **racine** (ou un **zéro**) de P si $P(\alpha) = 0$.

Proposition 7.

$$P(\alpha) = 0 \iff X - \alpha \text{ divise } P$$

Démonstration. Lorsque l'on écrit la division euclidienne de P par $X - \alpha$ on obtient $P = Q \cdot (X - \alpha) + R$ où R est une constante car $\deg R < \deg(X - \alpha) = 1$. Donc $P(\alpha) = 0 \iff R(\alpha) = 0 \iff R = 0 \iff X - \alpha | P$. □

Définition 7.
Soit $k \in \mathbb{N}^*$. On dit que α est une **racine de multiplicité k** de P si $(X - \alpha)^k$ divise P alors que $(X - \alpha)^{k+1}$ ne divise pas P. Lorsque $k = 1$ on parle d'une **racine simple**, lorsque $k = 2$ d'une **racine double**, etc.

On dit aussi que α est une **racine d'ordre k**.

Proposition 8.
Il y a équivalence entre :

(i) α *est une racine de multiplicité* k *de* P.

(ii) *Il existe* $Q \in \mathbb{K}[X]$ *tel que* $P = (X - \alpha)^k Q$, *avec* $Q(\alpha) \neq 0$.

(iii) $P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ *et* $P^{(k)}(\alpha) \neq 0$.

La preuve est laissée en exercice.

Remarque.
Par analogie avec la dérivée d'une fonction, si $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ alors le polynôme $P'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$ est le **polynôme dérivé** de P.

Théorème de d'Alembert-Gauss

Passons à un résultat essentiel de ce chapitre :

Théorème 3 (Théorème de d'Alembert-Gauss)**.**
Tout polynôme à coefficients complexes de degré $n \geqslant 1$ a au moins une racine dans $\mathbb{C}$. Il admet exactement n racines si on compte chaque racine avec multiplicité.

Nous admettons ce théorème.

Exemple 11.
Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2 à coefficients réels : $a, b, c \in \mathbb{R}$ et $a \neq 0$.

- Si $\Delta = b^2 - 4ac > 0$ alors P admet 2 racines réelles distinctes $\frac{-b+\sqrt{\Delta}}{2a}$ et $\frac{-b-\sqrt{\Delta}}{2a}$.
- Si $\Delta < 0$ alors P admet 2 racines complexes distinctes $\frac{-b+\mathrm{i}\sqrt{|\Delta|}}{2a}$ et $\frac{-b-\mathrm{i}\sqrt{|\Delta|}}{2a}$.
- Si $\Delta = 0$ alors P admet une racine réelle double $\frac{-b}{2a}$.

En tenant compte des multiplicités on a donc toujours exactement 2 racines.

Exemple 12.
$P(X) = X^n - 1$ admet n racines distinctes.
Sachant que P est de degré n alors par le théorème de d'Alembert-Gauss on sait qu'il admet n racines comptées avec multiplicité. Il s'agit donc maintenant de montrer que ce sont des racines simples. Supposons –par l'absurde– que $\alpha \in \mathbb{C}$ soit une racine de multiplicité $\geqslant 2$. Alors $P(\alpha) = 0$ et $P'(\alpha) = 0$. Donc $\alpha^n - 1 = 0$ et $n\alpha^{n-1} = 0$. De la seconde égalité on déduit $\alpha = 0$, contradictoire avec la première égalité. Donc toutes les racines sont simples. Ainsi les n racines sont distinctes. (Remarque : sur cet exemple particulier on aurait aussi pu calculer les racines qui sont ici les racines n-ième de l'unité.)

Pour les autres corps que les nombres complexes nous avons le résultat plus faible suivant :

Théorème 4.
Soit $P \in \mathbb{K}[X]$ de degré $n \geqslant 1$. Alors P admet au plus n racines dans $\mathbb{K}$.

Exemple 13.
$P(X) = 3X^3 - 2X^2 + 6X - 4$. Considéré comme un polynôme à coefficients dans $\mathbb{Q}$ ou $\mathbb{R}$, P n'a qu'une seule racine (qui est simple) $\alpha = \frac{2}{3}$ et il se décompose en $P(X) = 3(X - \frac{2}{3})(X^2 + 2)$. Si on considère maintenant P comme un polynôme à coefficients dans $\mathbb{C}$ alors $P(X) = 3(X - \frac{2}{3})(X - \mathrm{i}\sqrt{2})(X + \mathrm{i}\sqrt{2})$ et admet 3 racines simples.

Polynômes irréductibles

Définition 8.
Soit $P \in \mathbb{K}[X]$ un polynôme de degré $\geqslant 1$, on dit que P est **irréductible** si pour tout $Q \in \mathbb{K}[X]$ divisant P, alors, soit $Q \in \mathbb{K}^*$, soit il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Remarque.

- Un polynôme irréductible P est donc un polynôme non constant dont les seuls diviseurs de P sont les constantes ou P lui-même (à une constante multiplicative près).
- La notion de polynôme irréductible pour l'arithmétique de $\mathbb{K}[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.
- Dans le cas contraire, on dit que P est **réductible** ; il existe alors des polynômes A, B de $\mathbb{K}[X]$ tels que $P = AB$, avec $\deg A \geqslant 1$ et $\deg B \geqslant 1$.

Exemple 14.

- Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.
- $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ est réductible.
- $X^2 + 1 = (X - \mathrm{i})(X + \mathrm{i})$ est réductible dans $\mathbb{C}[X]$ mais est irréductible dans $\mathbb{R}[X]$.
- $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ est réductible dans $\mathbb{R}[X]$ mais est irréductible dans $\mathbb{Q}[X]$.

Nous avons l'équivalent du lemme d'Euclide de $\mathbb{Z}$ pour les polynômes :

Proposition 9 (Lemme d'Euclide)**.**
Soit $P \in \mathbb{K}[X]$ un polynôme irréductible et soient $A, B \in \mathbb{K}[X]$. Si $P \mid AB$ alors $P \mid A$ ou $P \mid B$.

Démonstration. Si P ne divise pas A alors $\operatorname{pgcd}(P, A) = 1$ car P est irréductible. Donc, par le lemme de Gauss, P divise B. □

Théorème de factorisation

Théorème 5.
Tout polynôme non constant $A \in \mathbb{K}[X]$ s'écrit comme un produit de polynômes irréductibles unitaires :

$$A = \lambda P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$$

où $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $k_i \in \mathbb{N}^*$ et les P_i sont des polynômes irréductibles distincts.
De plus cette décomposition est unique à l'ordre près des facteurs.

Il s'agit bien sûr de l'analogue de la décomposition d'un nombre en facteurs premiers.

Factorisation dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème 6.
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Donc pour $P \in \mathbb{C}[X]$ de degré $n \geqslant 1$ la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2} \cdots (X-\alpha_r)^{k_r}$, où $\alpha_1, \ldots, \alpha_r$ sont les racines distinctes de P et $k_1, \ldots, k_r$ sont leurs multiplicités.

Démonstration. Ce théorème résulte du théorème de d'Alembert-Gauss. □

Théorème 7.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 ayant un discriminant $\Delta < 0$.
Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. Alors la factorisation s'écrit $P = \lambda(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_r)^{k_r}Q_1^{\ell_1}\cdots Q_s^{\ell_s}$, où les α_i sont exactement les racines réelles distinctes de multiplicité k_i et les Q_i sont des polynômes irréductibles de degré 2 : $Q_i = X^2+\beta_i X+\gamma_i$ avec $\Delta = \beta_i^2 - 4\gamma_i < 0$.

Exemple 15.
$P(X) = 2X^4(X-1)^3(X^2+1)^2(X^2+X+1)$ est déjà décomposé en facteurs irréductibles dans $\mathbb{R}[X]$ alors que sa décomposition dans $\mathbb{C}[X]$ est $P(X) = 2X^4(X-1)^3(X-\mathrm{i})^2(X+\mathrm{i})^2(X-j)(X-j^2)$ où $j = e^{\frac{2\mathrm{i}\pi}{3}} = \frac{-1+\mathrm{i}\sqrt{3}}{2}$.

Exemple 16.
Soit $P(X) = X^4+1$.

- Sur $\mathbb{C}$. On peut d'abord décomposer $P(X) = (X^2+\mathrm{i})(X^2-\mathrm{i})$. Les racines de P sont donc les racines carrées complexes de i et $-\mathrm{i}$. Ainsi P se factorise dans $\mathbb{C}[X]$:
$$P(X) = \big(X - \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\big)\big(X + \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\big)\big(X - \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\big)\big(X + \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\big).$$
- Sur $\mathbb{R}$. Pour un polynôme à coefficient réels, si α est une racine alors $\bar{\alpha}$ aussi. Dans la décomposition ci-dessus on regroupe les facteurs ayant des racines conjuguées, cela doit conduire à un polynôme réel :
$$\begin{aligned} P(X) &= \Big[\big(X - \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\big)\big(X - \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\big)\Big]\Big[\big(X + \tfrac{\sqrt{2}}{2}(1+\mathrm{i})\big)\big(X + \tfrac{\sqrt{2}}{2}(1-\mathrm{i})\big)\Big] \\ &= \big[X^2+\sqrt{2}X+1\big]\big[X^2-\sqrt{2}X+1\big], \end{aligned}$$
qui est la factorisation dans $\mathbb{R}[X]$.

Mini-exercices.

1. Trouver un polynôme $P(X) \in \mathbb{Z}[X]$ de degré minimal tel que : $\frac{1}{2}$ soit une racine simple, $\sqrt{2}$ soit une racine double et i soit une racine triple.
2. Montrer cette partie de la proposition 8 : « $P(\alpha) = 0$ et $P'(\alpha) = 0 \iff \alpha$ est une racine de multiplicité $\geqslant 2$ ».
3. Montrer que pour $P \in \mathbb{C}[X]$: « P admet une racine de multiplicité $\geqslant 2 \iff P$ et P' ne sont pas premiers entre eux ».
4. Factoriser $P(X) = (2X^2+X-2)^2(X^4-1)^3$ et $Q(X) = 3(X^2-1)^2(X^2-X+\frac{1}{4})$ dans $\mathbb{C}[X]$. En déduire leur pgcd et leur ppcm. Mêmes questions dans $\mathbb{R}[X]$.
5. Si $\operatorname{pgcd}(A,B) = 1$ montrer que $\operatorname{pgcd}(A+B, A\times B) = 1$.
6. Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}\setminus\mathbb{R}$ tel que $P(\alpha) = 0$. Vérifier que $P(\bar{\alpha}) = 0$. Montrer que $(X-\alpha)(X-\bar{\alpha})$ est un polynôme irréductible de $\mathbb{R}[X]$ et qu'il divise P dans $\mathbb{R}[X]$.

4.4. Fractions rationnelles

Définition 9.
Une **fraction rationnelle** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$F = \frac{P}{Q}$$

où $P, Q \in \mathbb{K}[X]$ sont deux polynômes et $Q \neq 0$.

Toute fraction rationnelle se décompose comme une somme de fractions rationnelles élémentaires que l'on appelle des « éléments simples ». Mais les éléments simples sont différents sur $\mathbb{C}$ ou sur $\mathbb{R}$.

Décomposition en éléments simples sur $\mathbb{C}$

Théorème 8 (Décomposition en éléments simples sur $\mathbb{C}$)**.**
Soit P/Q une fraction rationnelle avec $P, Q \in \mathbb{C}[X]$, $\operatorname{pgcd}(P,Q) = 1$ et $Q = (X-\alpha_1)^{k_1} \cdots (X-\alpha_r)^{k_r}$. Alors il existe une et une seule écriture :

$$\begin{aligned}\frac{P}{Q} = E &+ \frac{a_{1,1}}{(X-\alpha_1)^{k_1}} + \frac{a_{1,2}}{(X-\alpha_1)^{k_1-1}} + \cdots + \frac{a_{1,k_1}}{(X-\alpha_1)} \\ &+ \frac{a_{2,1}}{(X-\alpha_2)^{k_2}} + \cdots + \frac{a_{2,k_2}}{(X-\alpha_2)} \\ &+ \cdots\end{aligned}$$

Le polynôme E s'appelle la **partie polynomiale** (ou **partie entière**). Les termes $\frac{a}{(X-\alpha)^i}$ sont les **éléments simples** sur $\mathbb{C}$.

Exemple 17.

- Vérifier que $\frac{1}{X^2+1} = \frac{a}{X+\mathrm{i}} + \frac{b}{X-\mathrm{i}}$ avec $a = \frac{1}{2}\mathrm{i}$, $b = -\frac{1}{2}\mathrm{i}$.
- Vérifier que $\frac{X^4-8X^2+9X-7}{(X-2)^2(X+3)} = X + 1 + \frac{-1}{(X-2)^2} + \frac{2}{X-2} + \frac{-1}{X+3}$.

Comment se calcule cette décomposition ? En général on commence par déterminer la partie polynomiale. Tout d'abord si $\deg Q > \deg P$ alors $E(X) = 0$. Si $\deg P \leqslant \deg Q$ alors effectuons la division euclidienne de P par Q : $P = QE + R$ donc $\frac{P}{Q} = E + \frac{R}{Q}$ où $\deg R < \deg Q$. La partie polynomiale est donc le quotient de cette division. Et on s'est ramené au cas d'une fraction $\frac{R}{Q}$ avec $\deg R < \deg Q$. Voyons en détails comment continuer sur un exemple.

Exemple 18.
Décomposons la fraction $\dfrac{P}{Q} = \dfrac{X^5 - 2X^3 + 4X^2 - 8X + 11}{X^3 - 3X + 2}$.

- **Première étape : partie polynomiale.** On calcule la division euclidienne de P par Q : $P(X) = (X^2+1)Q(X) + 2X^2 - 5X + 9$. Donc la partie polynomiale est $E(X) = X^2 + 1$ et la fraction s'écrit $\frac{P(X)}{Q(X)} = X^2 + 1 + \frac{2X^2-5X+9}{Q(X)}$. Notons que pour la fraction $\frac{2X^2-5X+9}{Q(X)}$ le degré du numérateur est strictement plus petit que le degré du dénominateur.

- **Deuxième étape : factorisation du dénominateur.** Q a pour racine évidente $+1$ (racine double) et -2 (racine simple) et se factorise donc ainsi $Q(X) = (X-1)^2(X+2)$.
- **Troisième étape : décomposition théorique en éléments simples.** Le théorème de décomposition en éléments simples nous dit qu'il existe une unique décomposition : $\frac{P(X)}{Q(X)} = E(X) + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$. Nous savons déjà que $E(X) = X^2+1$, il reste à trouver les nombres a, b, c.
- **Quatrième étape : détermination des coefficients.** Voici une première façon de déterminer a, b, c. On récrit la fraction $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ au même dénominateur et on l'identifie avec $\frac{2X^2-5X+9}{Q(X)}$:
$$\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2} = \frac{(b+c)X^2 + (a+b-2c)X + 2a - 2b + c}{(X-1)^2(X+2)}$$
qui doit être égale à
$$\frac{2X^2-5X+9}{(X-1)^2(X+2)}.$$
On en déduit $b+c=2$, $a+b-2c=-5$ et $2a-2b+c=9$. Cela conduit à l'unique solution $a=2$, $b=-1$, $c=3$. Donc
$$\frac{P}{Q} = \frac{X^5-2X^3+4X^2-8X+11}{X^3-3X+2} = X^2+1+\frac{2}{(X-1)^2} + \frac{-1}{X-1} + \frac{3}{X+2}.$$
Cette méthode est souvent la plus longue.
- **Quatrième étape (bis) : détermination des coefficients.** Voici une autre méthode plus efficace.
Notons $\frac{P'(X)}{Q(X)} = \frac{2X^2-5X+9}{(X-1)^2(X+2)}$ dont la décomposition théorique est : $\frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$
Pour déterminer a on multiplie la fraction $\frac{P'}{Q}$ par $(X-1)^2$ et on évalue en $x=1$.
Tout d'abord en partant de la décomposition théorique on a :
$$F_1(X) = (X-1)^2\frac{P'(X)}{Q(X)} = a + b(X-1) + c\frac{(X-1)^2}{X+2} \quad \text{donc} \quad F_1(1) = a$$
D'autre part
$$F_1(X) = (X-1)^2\frac{P'(X)}{Q(X)} = (X-1)^2\frac{2X^2-5X+9}{(X-1)^2(X+2)} = \frac{2X^2-5X+9}{X+2}$$
donc $F_1(1) = 2$. On en déduit $a=2$.
On fait le même processus pour déterminer c : on multiplie par $(X+2)$ et on évalue en -2. On calcule $F_2(X) = (X+2)\frac{P'(X)}{Q(X)} = \frac{2X^2-5X+9}{(X-1)^2} = a\frac{X+2}{(X-1)^2} + b\frac{X+2}{X-1} + c$ de deux façons et lorsque l'on évalue $x=-2$ on obtient d'une part $F_2(-2) = c$ et d'autre part $F_2(-2) = 3$. Ainsi $c=3$.
Comme les coefficients sont uniques tous les moyens sont bons pour les déterminer. Par exemple lorsque l'on évalue la décomposition théorique $\frac{P'(X)}{Q(X)} = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+2}$ en $x=0$, on obtient :
$$\frac{P'(0)}{Q(0)} = a - b + \frac{c}{2}$$
Donc $\frac{9}{2} = a - b + \frac{c}{2}$. Donc $b = a + \frac{c}{2} - \frac{9}{2} = -1$.

Décomposition en éléments simples sur $\mathbb{R}$

Théorème 9 (Décomposition en éléments simples sur $\mathbb{R}$)**.**
Soit P/Q une fraction rationnelle avec $P,Q \in \mathbb{R}[X]$, $\operatorname{pgcd}(P,Q) = 1$. Alors P/Q s'écrit de manière unique comme somme :

- *d'une partie polynomiale $E(X)$,*
- *d'éléments simples du type $\frac{a}{(X-\alpha)^i}$,*
- *d'éléments simples du type $\frac{aX+b}{(X^2+\alpha X+\beta)^i}$.*

Où les $X-\alpha$ et $X^2+\alpha X+\beta$ sont les facteurs irréductibles de $Q(X)$ et les exposants i sont inférieurs ou égaux à la puissance correspondante dans cette factorisation.

Exemple 19.
Décomposition en éléments simples de $\frac{P(X)}{Q(X)} = \frac{3X^4+5X^3+8X^2+5X+3}{(X^2+X+1)^2(X-1)}$. Comme $\deg P < \deg Q$ alors $E(X) = 0$. Le dénominateur est déjà factorisé sur $\mathbb{R}$ car X^2+X+1 est irréductible. La décomposition théorique est donc :

$$\frac{P(X)}{Q(X)} = \frac{aX+b}{(X^2+X+1)^2} + \frac{cX+d}{X^2+X+1} + \frac{e}{X-1}.$$

Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir :

$$\frac{P(X)}{Q(X)} = \frac{2X+1}{(X^2+X+1)^2} + \frac{-1}{X^2+X+1} + \frac{3}{X-1}.$$

Mini-exercices

Mini-exercices.

1. Soit $Q(X) = (X-2)^2(X^2-1)^3(X^2+1)^4$. Pour $P \in \mathbb{R}[X]$ quelle est la forme théorique de la décomposition en éléments simples sur $\mathbb{C}$ de $\frac{P}{Q}$? Et sur $\mathbb{R}$?
2. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$ et $\mathbb{C}$: $\frac{1}{X^2-1}$; $\frac{X^2+1}{(X-1)^2}$; $\frac{X}{X^3-1}$.
3. Décomposer les fractions suivantes en éléments simples sur $\mathbb{R}$: $\frac{X^2+X+1}{(X-1)(X+2)^2}$; $\frac{2X^2-X}{(X^2+2)^2}$; $\frac{X^6}{(X^2+1)^2}$.
4. Soit $F(X) = \frac{2X^2+7X-20}{X+2}$. Déterminer l'équation de l'asymptote oblique en $\pm\infty$. Étudier la position du graphe de F par rapport à cette droite.

Annexe : Nombres complexes

Chapitre 5

Préambule

L'équation $x+5=2$ a ses coefficients dans $\mathbb{N}$ mais pourtant sa solution $x=-3$ n'est pas un entier naturel. Il faut ici considérer l'ensemble plus grand $\mathbb{Z}$ des entiers relatifs.

$$\mathbb{N} \xhookrightarrow{x+5=2} \mathbb{Z} \xhookrightarrow{2x=-3} \mathbb{Q} \xhookrightarrow{x^2=\frac{1}{2}} \mathbb{R} \xhookrightarrow{x^2=-\sqrt{2}} \mathbb{C}$$

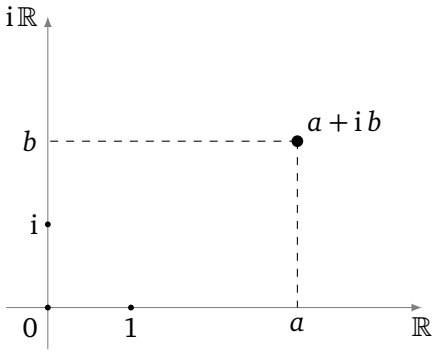
De même l'équation $2x=-3$ a ses coefficients dans $\mathbb{Z}$ mais sa solution $x=-\frac{3}{2}$ est dans l'ensemble plus grand des rationnels $\mathbb{Q}$. Continuons ainsi, l'équation $x^2=\frac{1}{2}$ à coefficients dans $\mathbb{Q}$, a ses solutions $x_1=+1/\sqrt{2}$ et $x_2=-1/\sqrt{2}$ dans l'ensemble des réels $\mathbb{R}$. Ensuite l'équation $x^2=-\sqrt{2}$ à ses coefficients dans $\mathbb{R}$ et ses solutions $x_1=+\mathrm{i}\sqrt{\sqrt{2}}$ et $x_2=-\mathrm{i}\sqrt{\sqrt{2}}$ dans l'ensemble des nombres complexes $\mathbb{C}$. Ce processus est-il sans fin ? Non ! Les nombres complexes sont en quelque sorte le bout de la chaîne car nous avons le théorème de d'Alembert-Gauss suivant : « *Pour n'importe quelle équation polynomiale* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$ *où les coefficients* a_i *sont des complexes (ou bien des réels), alors les solutions* $x_1, \ldots, x_n$ *sont dans l'ensemble des nombres complexes* ».

Outre la résolution d'équations, les nombres complexes s'appliquent à la trigonométrie, à la géométrie (comme nous le verrons dans ce chapitre) mais aussi à l'électronique, à la mécanique quantique, etc.

Les nombres complexes

Définition

Définition 1.
Un **nombre complexe** est un couple $(a,b) \in \mathbb{R}^2$ que l'on notera $a+\mathrm{i}\,b$

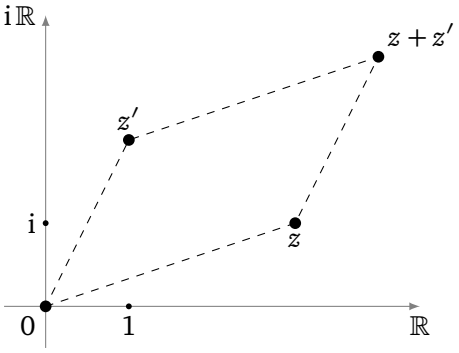


Cela revient à identifier 1 avec le vecteur $(1,0)$ de $\mathbb{R}^2$, et i avec le vecteur $(0,1)$. On note $\mathbb{C}$ l'ensemble des nombres complexes. Si $b=0$, alors $z=a$ est situé sur l'axe des abscisses, que l'on identifie à $\mathbb{R}$. Dans ce cas on dira que z est **réel**, et $\mathbb{R}$ apparaît comme un sous-ensemble de $\mathbb{C}$, appelé **axe réel**. Si $b\neq 0$, z est dit **imaginaire** et si $b\neq 0$ et $a=0$, z est dit **imaginaire pur**.

Opérations

Si $z=a+\mathrm{i}\,b$ et $z'=a'+\mathrm{i}\,b'$ sont deux nombres complexes, alors on définit les opérations suivantes :

- ***addition*** : $(a+\mathrm{i}\,b)+(a'+\mathrm{i}\,b')=(a+a')+\mathrm{i}(b+b')$

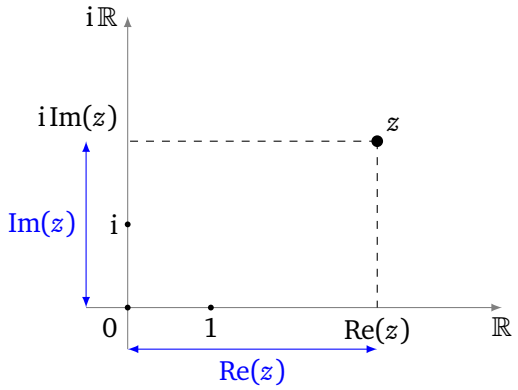


- ***multiplication*** : $(a+\mathrm{i}\,b)\times(a'+\mathrm{i}\,b')=(aa'-bb')+\mathrm{i}(ab'+ba')$. On développe en suivant les règles de la multiplication usuelle avec la convention suivante :

$$\boxed{\mathrm{i}^2=-1}$$

Partie réelle et imaginaire

Soit $z=a+\mathrm{i}\,b$ un nombre complexe, sa **partie réelle** est le réel a et on la note $\mathrm{Re}(z)$; sa **partie imaginaire** est le réel b et on la note $\mathrm{Im}(z)$.



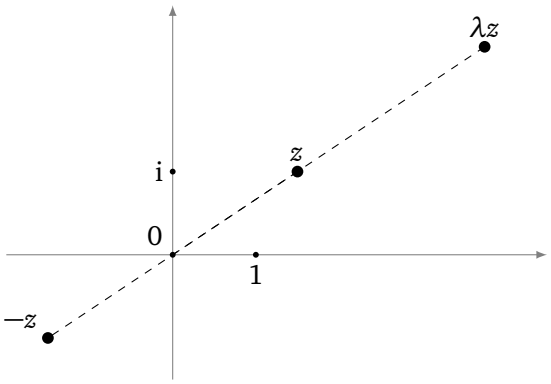
Par identification de $\mathbb{C}$ à $\mathbb{R}^2$, l'écriture $z = \mathrm{Re}(z) + \mathrm{i}\,\mathrm{Im}(z)$ est unique :

$$z = z' \iff \begin{cases} \mathrm{Re}(z) = \mathrm{Re}(z') \\ \text{et} \\ \mathrm{Im}(z) = \mathrm{Im}(z') \end{cases}$$

En particulier un nombre complexe est réel si et seulement si sa partie imaginaire est nulle. Un nombre complexe est nul si et et seulement si sa partie réelle et sa partie imaginaire sont nuls.

Calculs

Quelques définitions et calculs sur les nombres complexes.



- L'**opposé** de $z = a + \mathrm{i}\,b$ est $-z = (-a) + \mathrm{i}(-b) = -a - \mathrm{i}\,b$.
- La **multiplication par un scalaire** $\lambda \in \mathbb{R}$: $\lambda \cdot z = (\lambda a) + \mathrm{i}(\lambda b)$.
- L'**inverse** : si $z \neq 0$, il existe un unique $z' \in \mathbb{C}$ tel que $zz' = 1$ (où $1 = 1 + \mathrm{i} \times 0$).
  Pour la preuve et le calcul on écrit $z = a + \mathrm{i}\,b$ puis on cherche $z' = a' + \mathrm{i}\,b'$ tel que $zz' = 1$. Autrement dit $(a + \mathrm{i}\,b)(a' + \mathrm{i}\,b') = 1$. En développant et identifiant les parties réelles et imaginaires on obtient les équations
  $$\begin{cases} aa' - bb' = 1 & (L_1) \\ ab' + ba' = 0 & (L_2) \end{cases}$$
  En écrivant $aL_1 + bL_2$ (on multiplie la ligne (L_1) par a, la ligne (L_2) par b et on additionne) et $-bL_1 + aL_2$ on en déduit
  $$\begin{cases} a'\left(a^2 + b^2\right) = a \\ b'\left(a^2 + b^2\right) = -b \end{cases} \quad \text{donc} \quad \begin{cases} a' = \frac{a}{a^2+b^2} \\ b' = -\frac{b}{a^2+b^2} \end{cases}$$

L'inverse de z, noté $\frac{1}{z}$, est donc

$$z' = \frac{1}{z} = \frac{a}{a^2+b^2} + \mathrm{i}\,\frac{-b}{a^2+b^2} = \frac{a-\mathrm{i}\,b}{a^2+b^2}.$$

- La **division** : $\frac{z}{z'}$ est le nombre complexe $z \times \frac{1}{z'}$.
- Propriété d'intégrité : si $zz' = 0$ alors $z = 0$ ou $z' = 0$.
- Puissances : $z^2 = z \times z$, $z^n = z \times \cdots \times z$ (n fois, $n \in \mathbb{N}$). Par convention $z^0 = 1$ et $z^{-n} = \left(\frac{1}{z}\right)^n = \frac{1}{z^n}$.

Proposition 1.
Pour tout $z \in \mathbb{C}$ différent de 1

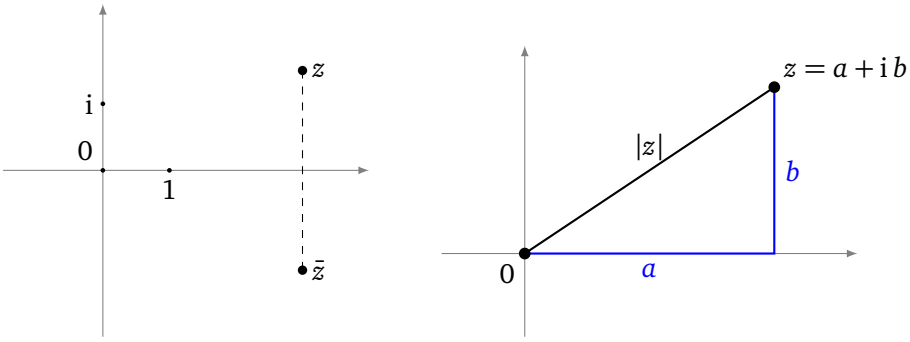
$$\boxed{1 + z + z^2 + \cdots + z^n = \frac{1-z^{n+1}}{1-z}.}$$

La preuve est simple : notons $S = 1+z+z^2+\cdots+z^n$, alors en développant $S\cdot(1-z)$ presque tous les termes se télescopent et l'on trouve $S\cdot(1-z) = 1-z^{n+1}$.

Remarque.
Il n'y pas d'ordre naturel sur $\mathbb{C}$, il ne faut donc jamais écrire $z \geqslant 0$ ou $z \leqslant z'$.

Conjugué, module

Le **conjugué** de $z = a + \mathrm{i}\,b$ est $\bar{z} = a - \mathrm{i}\,b$, autrement dit $\mathrm{Re}(\bar{z}) = \mathrm{Re}(z)$ et $\mathrm{Im}(\bar{z}) = -\mathrm{Im}(z)$.
Le point $\bar{z}$ est le symétrique du point z par rapport à l'axe réel.
Le **module** de $z = a + \mathrm{i}\,b$ est le réel positif $|z| = \sqrt{a^2+b^2}$. Comme $z \times \bar{z} = (a+\mathrm{i}\,b)(a-\mathrm{i}\,b) = a^2+b^2$ alors le module vaut aussi $|z| = \sqrt{z\bar{z}}$.

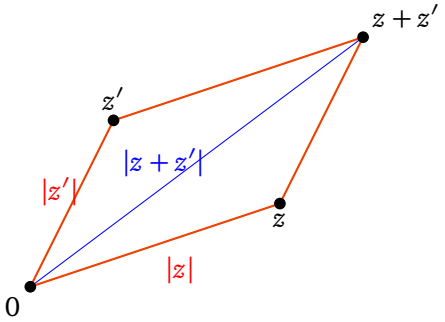


Quelques formules :

- $\overline{z+z'} = \bar{z} + \overline{z'}$, $\quad \bar{\bar{z}} = z$, $\quad \overline{zz'} = \bar{z}\,\overline{z'}$
- $z = \bar{z} \iff z \in \mathbb{R}$
- $|z|^2 = z \times \bar{z}$, $\quad |\bar{z}| = |z|$, $\quad |zz'| = |z||z'|$
- $|z| = 0 \iff z = 0$

Proposition 2 (L'inégalité triangulaire)**.**

$$\boxed{|z+z'| \leqslant |z| + |z'|}$$



Avant de faire la preuve voici deux remarques utiles. Soit $z = a + \mathrm{i}\, b \in \mathbb{C}$ avec $a, b \in \mathbb{R}$:

- $|\mathrm{Re}(z)| \leqslant |z|$ (et aussi $|\mathrm{Im}(z)| \leqslant |z|$). Cela vient du fait que $|a| \leqslant \sqrt{a^2+b^2}$. Noter que pour un réel $|a|$ est à la fois le module et la valeur absolue.
- $\boxed{z + \bar{z} = 2\,\mathrm{Re}(z)}$ et $z - \bar{z} = 2\,\mathrm{i}\,\mathrm{Im}(z)$. Preuve : $z+\bar{z} = (a+\mathrm{i}\,b)+(a-\mathrm{i}\,b) = 2a = 2\,\mathrm{Re}(z)$.

Démonstration. Pour la preuve on calcule $|z+z'|^2$:

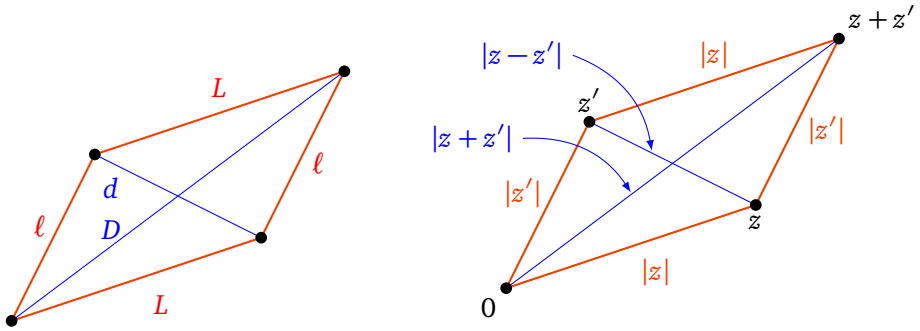
$$\begin{aligned} |z+z'|^2 &= \left(z+z'\right)\overline{(z+z')} = z\bar{z} + z'\overline{z'} + z\overline{z'} + z'\bar{z} = |z|^2 + |z'|^2 + 2\,\mathrm{Re}(z'\bar{z}) \\ &\leqslant |z|^2 + |z'|^2 + 2|z'\bar{z}| \leqslant |z|^2 + |z'|^2 + 2|zz'| \leqslant (|z| + |z'|)^2 \end{aligned}$$

□

Exemple 1.
Dans un parallélogramme, la somme des carrés des diagonales égale la somme des carrés des côtés.

Si les longueurs des côtés sont notées L et ℓ et les longueurs des diagonales sont D et d alors il s'agit de montrer l'égalité

$$D^2 + d^2 = 2\ell^2 + 2L^2.$$



Démonstration. Cela devient simple si l'on considère que notre parallélogramme a pour sommets 0, z, z' et le dernier sommet est donc $z+z'$. La longueur du grand côté est ici $|z|$,

celle du petit côté est $|z'|$. La longueur de la grande diagonale est $|z+z'|$. Enfin il faut se convaincre que la longueur de la petite diagonale est $|z-z'|$.

$$\begin{aligned} D^2+d^2 = \left|z+z'\right|^2+\left|z-z'\right|^2 &= \left(z+z'\right)\overline{(z+z')}+\left(z-z'\right)\overline{(z-z')} \\ &= z\bar{z}+z\overline{z'}+z'\bar{z}+z'\overline{z'}+z\bar{z}-z\overline{z'}-z'\bar{z}+z'\overline{z'} \\ &= 2z\bar{z}+2z'\overline{z'} = 2\left|z\right|^2+2\left|z'\right|^2 \\ &= 2\ell^2+2L^2 \end{aligned}$$

□

Mini-exercices.

1. Calculer $1-2\,\mathrm{i}+\frac{\mathrm{i}}{1-2\,\mathrm{i}}$.
2. Écrire sous la forme $a+\mathrm{i}\,b$ les nombres complexes $(1+\mathrm{i})^2$, $(1+\mathrm{i})^3$, $(1+\mathrm{i})^4$, $(1+\mathrm{i})^8$.
3. En déduire $1+(1+\mathrm{i})+(1+\mathrm{i})^2+\cdots+(1+\mathrm{i})^7$.
4. Soit $z\in\mathbb{C}$ tel que $|1+\mathrm{i}\,z| = |1-\mathrm{i}\,z|$, montrer que $z\in\mathbb{R}$.
5. Montrer que si $|\mathrm{Re}\,z| \leqslant |\mathrm{Re}\,z'|$ et $|\mathrm{Im}\,z| \leqslant |\mathrm{Im}\,z'|$ alors $|z| \leqslant |z'|$, mais que la réciproque est fausse.
6. Montrer que $1/\bar{z} = z/|z|^2$ (pour $z\neq 0$).

Racines carrées, équation du second degré

Racines carrées d'un nombre complexe

Pour $z \in \mathbb{C}$, une **racine carrée** est un nombre complexe ω tel que $\omega^2 = z$.
Par exemple si $x \in \mathbb{R}_+$, on connaît deux racines carrées : $\sqrt{x}, -\sqrt{x}$. Autre exemple : les racines carrées de -1 sont i et $-\mathrm{i}$.

Proposition 3.
Soit z un nombre complexe, alors z admet deux racines carrées, ω et $-\omega$.

Attention ! Contrairement au cas réel, il n'y a pas de façon privilégiée de choisir une racine plutôt que l'autre, donc pas de fonction racine. On ne dira donc jamais « soit ω la racine de z ».
Si $z \neq 0$ ces deux racines carrées sont distinctes. Si $z = 0$ alors $\omega = 0$ est une racine double.
Pour $z = a + \mathrm{i}\,b$ nous allons calculer ω et $-\omega$ en fonction de a et b.

Démonstration. Nous écrivons $\omega = x + \mathrm{i}\,y$, nous cherchons x, y tels que $\omega^2 = z$.

$$\begin{aligned} \omega^2 = z &\iff (x+\mathrm{i}\,y)^2 = a + \mathrm{i}\,b \\ &\iff \begin{cases} x^2 - y^2 = a & \text{en identifiant parties} \\ 2xy = b & \text{et parties imaginaires.} \end{cases} \end{aligned}$$

Petite astuce ici : nous rajoutons l'équation $|\omega|^2 = |z|$ (qui se déduit bien sûr de $\omega^2 = z$) qui s'écrit aussi $x^2 + y^2 = \sqrt{a^2+b^2}$. Nous obtenons des systèmes équivalents aux précédents :

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases} \iff \begin{cases} 2x^2 = \sqrt{a^2+b^2} + a \\ 2y^2 = \sqrt{a^2+b^2} - a \\ 2xy = b \end{cases} \iff \begin{cases} x = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a} \\ y = \pm\frac{1}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a} \\ 2xy = b \end{cases}$$

Discutons suivant le signe du réel b. Si $b \geqslant 0$, x et y sont de même signe ou nuls (car $2xy = b \geqslant 0$) donc

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} + \mathrm{i}\sqrt{\sqrt{a^2+b^2}-a}\right),$$

et si $b \leqslant 0$

$$\omega = \pm\frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} - \mathrm{i}\sqrt{\sqrt{a^2+b^2}-a}\right).$$

En particulier si $b = 0$ le résultat dépend du signe de a, si $a \geqslant 0$, $\sqrt{a^2} = a$ et par conséquent $\omega = \pm\sqrt{a}$, tandis que si $a < 0$, $\sqrt{a^2} = -a$ et donc $\omega = \pm\mathrm{i}\sqrt{-a} = \pm\mathrm{i}\sqrt{|a|}$. □

Il n'est pas nécessaire d'apprendre ces formules mais il est indispensable de savoir refaire les calculs.

Exemple 2.
Les racines carrées de i sont $+\frac{\sqrt{2}}{2}(1+\mathrm{i})$ et $-\frac{\sqrt{2}}{2}(1+\mathrm{i})$.

En effet :

$$\begin{aligned}\omega^2 = \mathrm{i} &\iff (x+\mathrm{i}\,y)^2 = \mathrm{i}\\ &\iff \begin{cases} x^2-y^2=0\\ 2xy=1\end{cases}\end{aligned}$$

Rajoutons la conditions $|\omega|^2 = |\mathrm{i}|$ pour obtenir le système équivalent au précédent :

$$\begin{cases} x^2-y^2=0\\ 2xy=1\\ x^2+y^2=1\end{cases} \iff \begin{cases} 2x^2=1\\ 2y^2=1\\ 2xy=1\end{cases} \iff \begin{cases} x=\pm\frac{1}{\sqrt{2}}\\ y=\pm\frac{1}{\sqrt{2}}\\ 2xy=1\end{cases}$$

Les réels x et y sont donc de même signe, nous trouvons bien deux solutions :

$$x+\mathrm{i}\,y = \frac{1}{\sqrt{2}}+\mathrm{i}\frac{1}{\sqrt{2}} \quad \text{ou} \quad x+\mathrm{i}\,y = -\frac{1}{\sqrt{2}}-\mathrm{i}\frac{1}{\sqrt{2}}$$

Équation du second degré

Proposition 4.
L'équation du second degré $az^2+bz+c=0$, où $a,b,c\in\mathbb{C}$ et $a\neq 0$, possède deux solutions $z_1,z_2\in\mathbb{C}$ éventuellement confondues.
Soit $\Delta = b^2-4ac$ le discriminant et $\delta\in\mathbb{C}$ une racine carrée de Δ. Alors les solutions sont

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

Et si $\Delta = 0$ alors la solution $z = z_1 = z_2 = -b/2a$ est unique (elle est dite double). Si on s'autorisait à écrire $\delta = \sqrt{\Delta}$, on obtiendrait la même formule que celle que vous connaissez lorsque a,b,c sont réels.

Exemple 3.

- $z^2+z+1=0$, $\Delta=-3$, $\delta=\mathrm{i}\sqrt{3}$, les solutions sont $z=\dfrac{-1\pm\mathrm{i}\sqrt{3}}{2}$.
- $z^2+z+\frac{1-\mathrm{i}}{4}=0$, $\Delta=\mathrm{i}$, $\delta=\frac{\sqrt{2}}{2}(1+\mathrm{i})$, les solutions sont $z=\dfrac{-1\pm\frac{\sqrt{2}}{2}(1+\mathrm{i})}{2} = -\frac{1}{2}\pm\frac{\sqrt{2}}{4}(1+\mathrm{i})$.

On retrouve aussi le résultat bien connu pour le cas des équations à coefficients réels :

Corollaire 1.
Si les coefficients a,b,c sont réels alors $\Delta\in\mathbb{R}$ et les solutions sont de trois types :

- *si $\Delta=0$, la racine double est réelle et vaut $-\dfrac{b}{2a}$,*
- *si $\Delta>0$, on a deux solutions réelles $\dfrac{-b\pm\sqrt{\Delta}}{2a}$,*
- *si $\Delta<0$, on a deux solutions complexes, mais non réelles, $\dfrac{-b\pm\mathrm{i}\sqrt{-\Delta}}{2a}$.*

Démonstration. On écrit la factorisation

$$\begin{aligned} az^2+bz+c &= a\left(z^2+\frac{b}{a}z+\frac{c}{a}\right)=a\left(\left(z+\frac{b}{2a}\right)^2-\frac{b^2}{4a^2}+\frac{c}{a}\right)\\ &= a\left(\left(z+\frac{b}{2a}\right)^2-\frac{\Delta}{4a^2}\right)=a\left(\left(z+\frac{b}{2a}\right)^2-\frac{\delta^2}{4a^2}\right)\\ &= a\left(\left(z+\frac{b}{2a}\right)-\frac{\delta}{2a}\right)\left(\left(z+\frac{b}{2a}\right)+\frac{\delta}{2a}\right)\\ &= a\left(z-\frac{-b+\delta}{2a}\right)\left(z-\frac{-b-\delta}{2a}\right)=a(z-z_1)(z-z_2) \end{aligned}$$

Donc le binôme s'annule si et seulement si $z=z_1$ ou $z=z_2$. □

Théorème fondamental de l'algèbre

Théorème 1 (d'Alembert–Gauss)**.**
Soit $P(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$ un polynôme à coefficients complexes et de degré n. Alors l'équation $P(z)=0$ admet exactement n solutions complexes comptées avec leur multiplicité.
En d'autres termes il existe des nombres complexes $z_1,\ldots,z_n$ (dont certains sont éventuellement confondus) tels que

$$P(z)=a_n(z-z_1)(z-z_2)\cdots(z-z_n).$$

Nous admettons ce théorème.

Mini-exercices.

1. Calculer les racines carrées de $-\mathrm{i}$, $3-4\mathrm{i}$.
2. Résoudre les équations : $z^2+z-1=0$, $2z^2+(-10-10\mathrm{i})z+24-10\mathrm{i}=0$.
3. Résoudre l'équation $z^2+(\mathrm{i}-\sqrt{2})z-\mathrm{i}\sqrt{2}$, puis l'équation $Z^4+(\mathrm{i}-\sqrt{2})Z^2-\mathrm{i}\sqrt{2}$.
4. Montrer que si $P(z)=z^2+bz+c$ possède pour racines $z_1,z_2\in\mathbb{C}$ alors $z_1+z_2=-b$ et $z_1\cdot z_2=c$.
5. Trouver les paires de nombres dont la somme vaut i et le produit 1.
6. Soit $P(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0$ avec $a_i\in\mathbb{R}$ pour tout i. Montrer que si z est racine de P alors $\bar{z}$ aussi.

Index