

Notions de base

Chapitre 35

Ensembles, applications, relations

L'activité mathématique se développe suivant trois axes principaux :

- la construction d'objets mathématiques, qui peuvent être des nombres, des fonctions, des figures géométriques... Ces objets servent de modèles pour étudier des phénomènes physiques, chimiques, biologiques...
- la recherche de propriétés reliant ces objets : ce sont des conjectures qui peuvent être élaborées par exemple à partir de cas particuliers ou par utilisation de moyens informatiques,
- la démonstration des propriétés énoncées précédemment. Une fois démontrées, ces propriétés prennent le nom de théorème.

Dans ce livre, pour distinguer les différents théorèmes que nous allons démontrer, nous leur donnons les noms de :

- **proposition** pour la plupart des résultats,
- **théorème** pour les résultats les plus fondamentaux,
- **corollaire** pour les conséquences (le plus souvent immédiates) des résultats précédents,
- **lemme** pour certains résultats préliminaires, utiles pour la suite, mais dont l'intérêt intrinsèque est assez limité.

Les démonstrations obéissent à des règles précises dont nous allons donner un aperçu dans ce chapitre.

1. Assertions

1.1 Assertions

La notion d'*assertion* est une notion première. Intuitivement, une assertion est un assemblage de mots dont la construction obéit à une certaine syntaxe et à laquelle on peut donner une valeur de vérité : V (Vraie) ou F (Fausse).

Exemples

1. « 2 est un entier impair » est une assertion (fausse) ;
2. « $(1000 + 1)^2 = 1000^2 + 2000 + 1$ » est une assertion (vraie) ;
3. « $1 = 2 + \dots$ » n'est pas une assertion.

On dit que deux assertions sont logiquement équivalentes, si elles ont la même valeur de vérité.

1.2 Connecteurs

À partir d'un certain nombre d'assertions, on peut en fabriquer de nouvelles en utilisant des *connecteurs*.

Connecteurs élémentaires

Si P et Q sont deux assertions, on définit les assertions :

- ($\text{NON } P$) qui est vraie lorsque P est fausse, et fausse sinon,
- (P ET Q) qui est vraie lorsque les deux assertions P et Q sont vraies, et fausse sinon,
- (P OU Q) qui est vraie lorsqu'au moins une des deux assertions est vraie, et fausse sinon.

Les valeurs de vérité de ces nouvelles assertions satisfont donc aux tables suivantes (appelées *tables de vérité*) :

P	$\text{NON } P$
V	F
F	V

P	Q	P ET Q	P OU Q
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

Remarques

- On voit que les tableaux précédents donnent un sens précis au connecteur $\bullet\cup$, alors que dans le langage courant ce mot peut être utilisé avec des sens différents. Par exemple :

- ou exclusif : « fromage ou dessert » ;
 - ou mathématique : « qu'il pleuve ou qu'il fasse du vent, je ne jouerai pas au tennis » ;
 - ou “conditionnel” : « mange ta soupe ou tu auras une fessée ».
- Les assertions (P ET Q) et NON(NON P OU NON Q) sont équivalentes, et il en est de même de (P OU Q) et NON(NON P ET NON Q). Cela permettrait de n'introduire que deux connecteurs élémentaires et de définir le troisième en fonction des deux autres, mais à cause de la symétrie entre les connecteurs ET et OU, il est plus judicieux de ne pas privilégier l'un par rapport à l'autre.

Implication, équivalence

Si P et Q sont deux assertions, on définit les assertions $P \Rightarrow Q$ et $P \Leftrightarrow Q$ par :

$$\begin{aligned} P \Rightarrow Q &: (\text{NON } P) \text{ OU } Q, \\ P \Leftrightarrow Q &: (P \Rightarrow Q) \text{ ET } (Q \Rightarrow P). \end{aligned}$$

Leurs valeurs de vérité vérifient le tableau suivant :

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

Remarques

- Par définition, l'assertion $P \Rightarrow Q$ est vraie dès que P est fausse ; elle peut donc être vraie même lorsque Q est fausse.
Par exemple, l'assertion « $(2 = 3) \Rightarrow (1 = 4)$ » est vraie.
- Si P est vraie et si $P \Rightarrow Q$ est vraie, alors Q est vraie.
- L'équivalence $P \Leftrightarrow Q$ est vraie si, et seulement si, P et Q sont logiquement équivalentes.

Les propriétés intuitives des connecteurs peuvent se vérifier facilement grâce aux tables de vérité.

Exemples

1. Quelles que soient les valeurs de vérité de P , \bullet et R , on a équivalence entre les deux assertions de chacune des lignes ci-après :

$\text{NON}(\text{NON } P)$	P
$P \text{ ET } Q$	$Q \text{ ET } P$
$(P \text{ OU } Q) \text{ OU } R$	$P \text{ OU } (Q \text{ OU } R)$
$(P \text{ OU } Q) \text{ ET } R$	$(P \text{ ET } R) \text{ OU } (Q \text{ ET } R)$

2. Il en est de même si l'on échange les rôles de ET et OU.
3. Les assertions $P \Leftrightarrow P$, $((P \text{ ET } Q) \Rightarrow P)$ et $(P \Rightarrow (P \text{ OU } Q))$ sont vraies quelles que soient les valeurs de vérité de leurs variables. De telles assertions sont appelées *tautologies*.

1.3 Méthodes de démonstration

Dans une théorie mathématique :

- un *axiome* est une assertion que l'on pose vraie *a priori*. Par exemple les axiomes d'Euclide en géométrie plane ;
- un *théorème* est une assertion que l'on peut déduire d'axiomes ou d'autres théorèmes. Le théorème de Pythagore en est un exemple en géométrie plane.

Les règles de déduction sont fondées sur les propriétés élémentaires des connecteurs ainsi que sur les règles suivantes.

Modus ponens : si l'on a $P \text{ ET } (P \Rightarrow Q)$ alors on a Q . Cette règle est fondée sur la tautologie $(P \text{ ET } (P \Rightarrow Q)) \Rightarrow Q$ que l'on vérifie facilement à l'aide des tables de vérité.

Ainsi, pour démontrer que Q est un théorème, il suffit de vérifier que P et $P \Rightarrow Q$ sont des théorèmes ou des axiomes.

Transitivité de l'implication : si l'on a $(P \Rightarrow Q) \text{ ET } (Q \Rightarrow R)$, alors on a $P \Rightarrow R$.

Ainsi, pour démontrer $P \Rightarrow R$, il suffit de montrer que R est conséquence de Q , lui-même conséquence de P .

Contraposée : on a $P \Rightarrow Q$ si, et seulement si, on a $\text{NON } Q \Rightarrow \text{NON } P$.

Ainsi, pour démontrer l'implication $P \Rightarrow Q$, il suffit de montrer sa contraposée $\text{NON } Q \Rightarrow \text{NON } P$.

Disjonction des cas : si l'on a $(P \text{ OU } Q) \text{ ET } (P \Rightarrow R) \text{ ET } (Q \Rightarrow R)$, alors on a R .

Ainsi, pour démontrer le résultat R , il suffit de montrer que l'on a P ou Q , et que dans chacun des cas on peut en déduire R .

Raisonnement par l'absurde : si l'on a $(\text{NON } P \Rightarrow Q) \text{ ET } (\text{NON } P \Rightarrow \text{NON } Q)$ alors on a P .

Ainsi, pour démontrer P , on montre que sa négation $\text{NON } P$ entraîne une assertion et son contraire, c'est-à-dire une contradiction.

2. Ensembles, prédictats

2.1 Généralités

Les notions d'*ensemble* et d'*élément* sont des notions premières ; un ensemble correspond intuitivement à une collection. On dispose de deux types d'assertions :

- $a \in E$ qui se lit : a appartient à E ou a est élément de E , et dont la négation s'écrit $a \notin E$.
- $E \subset F$ qui se lit : E inclus dans F et qui signifie que tout élément de E est aussi élément de F . Sa négation s'écrit $E \not\subset F$.

Deux ensembles E et F sont égaux ($E = F$) si ils ont les mêmes éléments, c'est-à-dire si l'on a simultanément $E \subset F$ et $F \subset E$. Pour démontrer une égalité d'ensembles, on prouvera donc en général une double inclusion.

On admet les résultats suivants.

- Il existe un ensemble, appelé *ensemble vide* et noté \emptyset , qui ne contient aucun élément. Il est inclus dans tout ensemble.
- Si E est un ensemble, il existe un ensemble, appelé *ensemble des parties* de E et noté $\mathcal{P}(E)$, dont les éléments sont tous les ensembles inclus dans E . Il vérifie donc, pour tout ensemble F :

$$F \in \mathcal{P}(E) \iff F \subset E.$$

Exemple Si $E = \{a, b, c\}$ est l'ensemble dont les éléments sont a , b et c , l'ensemble de ses parties est :

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, E\}.$$

2.2 Prédicats

Exemples

1. « x est pair » n'est pas une assertion, puisqu'on ne peut pas lui donner de valeur de vérité tant qu'on ne connaît pas x . C'est ce que l'on appelle un prédictat sur \mathbb{N} : il dépend d'une variable x , et lorsqu'on remplace x par une valeur entière, on obtient une assertion.
2. De même, « $x^2 + 1 > 0$ » est un prédictat sur \mathbb{R} , mais pas sur \mathbb{C} tant que l'on n'a pas défini de relation $>$ sur les complexes.
3. « $x + y^2 = 0$ » est un prédictat à deux variables réelles.
4. Lorsque l'on substitue à x , dans le prédictat précédent, le réel 1, on obtient le prédictat à une variable « $1 + y^2 = 0$ ».

Un *prédictat* est ainsi un énoncé $A(x, y, \dots)$ dépendant de variables x, y, \dots tel que, lorsqu'on substitue à ces variables des éléments de certains ensembles, on obtienne une assertion.

2.3 Quantificateurs

À partir d'un prédictat $A(x)$ à une variable x dans un ensemble E , on peut construire trois assertions :

- $\forall x \in E : A(x)$ qui se lit « quel que soit l'élément x de E , $A(x)$ ».

Cette assertion est vraie lorsque $A(a)$ est vraie pour tout élément a de l'ensemble E .

Par exemple l'inclusion $E \subset F$ peut s'écrire $\forall x \in E, x \in F$.

Le symbole \forall est appelé *quantificateur universel*.

- $\exists x \in E : A(x)$ qui se lit « il existe un élément x de E tel que $A(x)$ ».

Cette assertion est vraie lorsque $A(a)$ est vraie pour au moins un élément a de l'ensemble E .

Le symbole \exists est appelé *quantificateur existentiel*.

► **Attention** Malgré les apparences, les assertions $\forall x \in E, A(x)$ et $\exists x \in E : A(x)$ * ne sont pas des prédictats dépendant de la variable x . On dit que le x figurant dans ces assertions (et qui est quantifié) est une variable muette. Le nom x peut être remplacé par n'importe quel autre nom.

Exemples

1. $\exists x \in \mathbb{R} : x^2 + 1 = 0$ est une assertion fausse.

2. $\exists x \in \mathbb{C} : x^2 + 1 = 0$ est une assertion vraie.

3. À partir du prédictat à deux variables réelles $x + y^2 = 0$, on peut former :

- $\forall x \in \mathbb{R}, x + y^2 = 0$ est un prédictat $P(y)$. Ce prédictat n'est vérifié pour aucune valeur de y .
- $\exists x \in \mathbb{R} : x + y^2 = 0$ est un prédictat $Q(y)$. Ce prédictat est vérifié pour toute valeur de y .
- $\exists y \in \mathbb{R} : x + y^2 = 0$. C'est un prédictat $R(x)$ vérifié lorsque la variable x prend une valeur négative.

* Dans cet ouvrage, nous adoptons des notations différentes pour les deux quantificateurs. Le quantificateur universel est suivi d'une virgule, alors que le quantificateur existentiel utilise le deux-points qui se lit « tel que ».

4. Plus généralement, en quantifiant une variable d'un prédicat à n variables, on obtient un prédicat à $n - 1$ variables.
5. Si E est l'ensemble vide et P un prédicat à une variable :
 - la proposition $\forall x \in E, P(x)$ est vraie,
 - la proposition $\exists x \in E : P(x)$ est fausse.

2.4 Négation de quantificateurs

Les règles suivantes ne font que codifier le sens intuitif des quantificateurs :

$$\text{NON}(\forall x \in E, A(x)) \iff \exists x \in E : \text{NON } A(x)$$

$$\text{NON}(\exists x \in E : A(x)) \iff \forall x \in E, \text{NON } A(x)$$

Exemples

1. La négation de $(\forall x \in E, A(x) \Rightarrow B(x))$ est :

$$\exists x \in E : (A(x) \text{ ET } \text{NON } B(x)).$$

En effet, le prédicat $(A(x) \Rightarrow B(x))$ est logiquement équivalent à :

$$(\text{NON } A(x) \text{ OU } B(x)).$$

2. L'assertion $(\forall x \in E, A(x) \Leftrightarrow B(x))$ est équivalente à :

$$\forall x \in E, (A(x) \Rightarrow B(x)) \text{ ET } (B(x) \Rightarrow A(x)).$$

Sa négation est donc :

$$\exists x \in E : (A(x) \text{ ET } \text{NON } B(x)) \text{ OU } (B(x) \text{ ET } \text{NON } A(x)).$$

Remarque Il arrive souvent que certains quantificateurs universels soient sous-entendus, lorsque la variable correspondante apparaît dans les deux membres d'une implication ou d'une équivalence. Par exemple, l'assertion « la suite u est croissante à partir d'un certain rang » peut s'écrire :

$$\exists N \in \mathbb{N} : u_n \geq N \Rightarrow u_{n+1} \geq u_n$$

au lieu de :

$$\exists N \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq N \Rightarrow u_{n+1} \geq u_n.$$

Toutefois, pour écrire sans risque d'erreur la négation, il est alors impératif de rétablir les quantificateurs manquants. Dans l'exemple ci-dessus, cela donne :

$$\forall N \in \mathbb{N}, \exists n \in \mathbb{N} : (n \geq N \text{ ET } u_{n+1} < u_n).$$

2.5 Sous-ensembles définis par un prédictat

Si P est un prédictat à une variable et si E est un ensemble, on peut définir la partie de E constituée des éléments de E vérifiant P . On la note :

$$F = \{x \in E \mid P(x)\}^{**}.$$

Cette partie est donc caractérisée par l'équivalence suivante :

$$\forall x \in E, x \in F \iff P(x).$$

Exemple L'ensemble des entiers naturels pairs peut être défini par :

$$\{n \in \mathbb{N} \mid \exists k \in \mathbb{N} : n = 2k\}.$$

Remarques

- Toute partie F de E peut ainsi être associée à un prédictat : il suffit de prendre par exemple le prédictat $x \in F$.
- Si A et B sont deux parties de E , définies respectivement par les prédictats $P(x)$ et $Q(x)$, l'inclusion $A \subset B$ est équivalente à l'assertion $\forall x \in E, P(x) \Rightarrow Q(x)$.

2.6 Opérations sur les parties

Soient A et B deux parties d'un ensemble E . On appelle :

- *intersection* de A et B , la partie de E définie par :

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

- *réunion* de A et B , la partie de E définie par :

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

- *différence* de A et de B , la partie de E définie par :

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

- *complémentaire* de A dans E , la différence :

$$\complement_E A = E \setminus A.$$

** La barre verticale se lit « tels que ».

Remarques

- Soient $P(x)$ et $Q(x)$ deux prédictats. On définit les ensembles :

$$A = \{x \in E \mid P(x)\} \quad \text{et} \quad B = \{x \in E \mid Q(x)\}.$$

Les prédictats $(P(x) \text{ ET } Q(x))$, $(P(x) \text{ OU } Q(x))$ et $(\text{NON } P(x))$ sont alors associés respectivement aux ensembles $A \cap B$, $A \cup B$ et $\complement_E A$.

- Les propriétés élémentaires de l'intersection, de la réunion et de la différence, se déduisent donc des propriétés correspondantes des connecteurs. Par exemple, les relations :

$$A \cup A = A$$

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

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

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

proviennent des tautologies :

$$(P \text{ OU } P) \Leftrightarrow P$$

$$(P \text{ OU } (Q \text{ OU } R)) \Leftrightarrow ((P \text{ OU } Q) \text{ OU } R)$$

$$(P \text{ ET } Q) \Leftrightarrow (Q \text{ ET } P)$$

$$(P \text{ OU } (Q \text{ ET } R)) \Leftrightarrow ((P \text{ OU } Q) \text{ ET } (P \text{ OU } R)).$$

On a encore :

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

$$A \subset B \implies \complement_E B \subset \complement_E A$$

ainsi que les résultats obtenus en échangeant, dans les assertions ci-dessus, les rôles de \cap et \cup .

2.7 Couples, produit cartésien

- À partir de deux éléments a et b , on peut construire le couple (a, b) , avec la propriété fondamentale suivante :

$$(a, b) = (a', b') \iff (a = a' \text{ ET } b = b').$$

Étant donnés deux ensembles A et B , l'ensemble des couples de la forme (a, b) , avec $a \in A$ et $b \in B$ est appelé *produit cartésien* de A par B et se note $A \times B$.

On a donc :

$$A \times B = \{(a, b) \mid a \in A \text{ ET } b \in B\}.$$

Lorsque $A = B$, le produit cartésien $A \times B$ se note aussi A^2 .

- De même, on peut définir la notion de *triplet* (a, b, c) vérifiant la propriété :

$$(a, b, c) = (a', b', c') \iff (a = a' \text{ ET } b = b' \text{ ET } c = c')$$

ainsi que le produit :

$$A \times B \times C = \{(a, b, c) \mid a \in A \text{ ET } b \in B \text{ ET } c \in C\}.$$

Le produit $A \times A \times A$ se note aussi A^3 .

- Plus généralement, pour $n \in \mathbb{N}^*$, on peut définir la notion de *n-uplet* ou de *n-liste* (a_1, a_2, \dots, a_n) ainsi que l'ensemble :

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Lorsque $A_1 = A_2 = \dots = A_n = A$, le produit $A_1 \times A_2 \times \dots \times A_n$ est noté A^n .

En particulier lorsque $n = 1$, on identifie la 1-liste (a) avec son unique élément a . On a ainsi $A^1 = A$.

Par convention, il existe une unique 0-liste, appelée liste vide. On note alors A^0 l'ensemble qui contient comme unique élément la liste vide.

3. Applications

Dans toute cette section, E et F désignent des ensembles quelconques.

3.1 Définitions

Définition 1

- On appelle *graphe* de E vers F toute partie du produit cartésien $E \times F$.
- Une *application* (ou *fonction*) est un triplet $u = (E, F, \Gamma)$ où Γ est un graphe de E vers F tel que, pour tout $x \in E$, il existe un unique $y \in F$ tel que $(x, y) \in \Gamma$.

On dit aussi que u est une application de E dans F ou de E vers F .

Avec les notations précédentes :

- E est appelé *l'ensemble de départ* ou *ensemble de définition* de u ,
- F est *l'ensemble d'arrivée* de u ,
- pour $x \in E$, l'unique $y \in F$ tel que $(x, y) \in \Gamma$ s'appelle *image* de x par u et se note $u(x)$,
- pour $y \in F$, tout $x \in E$ tel que $y = u(x)$ est appelé un *antécédent* de y ,
- le *graphe* Γ de u , est égal à $\{(x, u(x)) \mid x \in E\}$,

- l'ensemble :

$\{y \in F \mid \exists x \in E : y = u(x)\}$ noté $\{u(x) \mid x \in E\}$

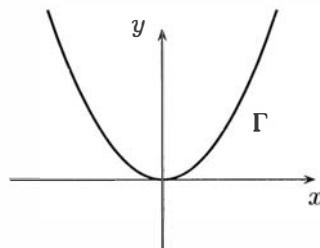
est l'*ensemble image* de u ; c'est une partie de F ,

- l'application u se note :

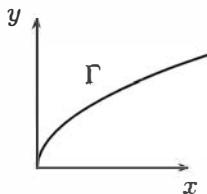
$$E \xrightarrow{u} F \quad \text{ou} \quad u : E \longrightarrow F \quad \text{ou} \quad u : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & u(x). \end{array}$$

Exemples

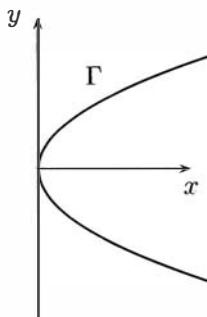
1. Si $\Gamma = \{(t, t^2) \mid t \in \mathbb{R}\}$, alors $(\mathbb{R}, \mathbb{R}, \Gamma)$ est une application de \mathbb{R} vers \mathbb{R} notée $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ t & \longmapsto & t^2 \end{array}$



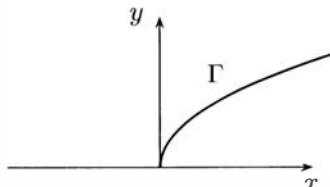
2. Si $\Gamma = \{(t^2, t) \mid t \in \mathbb{R}_+\}$, alors $(\mathbb{R}_+, \mathbb{R}_+, \Gamma)$ est une application de \mathbb{R}_+ vers \mathbb{R}_+ , représentée par $\begin{array}{ccc} \mathbb{R}_+ & \longrightarrow & \mathbb{R}_+ \\ t & \longmapsto & \sqrt{t} \end{array}$.



3. Si $\Gamma = \{(t^2, t) \mid t \in \mathbb{R}\}$, alors $(\mathbb{R}_+, \mathbb{R}, \Gamma)$ n'est pas une application car, pour $x \in \mathbb{R}_+^*$, il existe deux éléments $y \in \mathbb{R}$ tels que $(x, y) \in \Gamma$.



4. Si $\Gamma = \{(t^2, t) \mid t \in \mathbb{R}_+\}$, alors $(\mathbb{R}, \mathbb{R}_+, \Gamma)$ n'est pas une application car, pour un $x < 0$, il n'existe pas de y tel que $(x, y) \in \Gamma$.



5. L'application $f : E \rightarrow E$ est appelée identité de E et se note Id_E .
- $$\begin{array}{rcl} E & \longrightarrow & E \\ x & \longmapsto & x \end{array}$$
6. Une application constante est une application du type $E \rightarrow F$, où a est un élément fixé de F . Par abus, on la note souvent a .
7. Si E est vide, il existe une unique application de E dans F : celle dont le graphe est vide.
8. Si F est vide et E non vide, il n'existe pas d'application de E dans F .

Égalité de deux applications Comme conséquence de la définition, on déduit que l'égalité de deux applications u et v signifie :

- (1) l'égalité des ensembles de départ,
- (2) l'égalité des ensembles d'arrivée,
- (3) l'égalité $u(x) = v(x)$ pour tout x appartenant à l'ensemble de départ commun.

Ne pas oublier de vérifier les conditions (1) et (2).

Remarque Le plus souvent en pratique, on dispose d'une expression $u(x)$ et il faut commencer par déterminer des ensembles E et F tels que la relation $y = u(x)$ définisse une application de E dans F .

Lorsque l'on connaît ces ensembles, on dit alors : « soit l'application définie de E dans F par $x \mapsto u(x)$ ». On la note encore $(x \in E) \mapsto (u(x) \in F)$.

Exemples

1. La relation $y = \frac{1}{x^2 - 1}$ définit une application de $]-\infty, -1[\cup]-1, 1[\cup]1, +\infty[$ dans \mathbb{R} .
2. La relation $y = \sin x$ définit une application de \mathbb{R} dans \mathbb{R} , mais elle peut aussi définir une application de \mathbb{R} dans $[-1, 1]$. Ces deux applications ne sont pas égales car elles n'ont pas le même ensemble d'arrivée.

■ **Notation** L'ensemble des applications (ou fonctions) d'un ensemble E dans un ensemble F se note $\mathcal{F}(E, F)$ ou encore F^E .

Définition 2

Soit u une application de E vers F .

- Si A est une partie de E , la *restriction* de u à A , notée $u|_A$, est l'application de A dans F définie par :

$$\forall x \in A, u|_A(x) = u(x).$$

- On appelle *prolongement* de u toute application v définie sur un ensemble A contenant E et vérifiant :

$$\forall x \in E, v(x) = u(x).$$

Remarques

- En fait $u|_A$ est le triplet (A, F, Γ_1) avec $\Gamma_1 = \{(x, u(x)) \mid x \in A\}$.
- u est une restriction de v si, et seulement si, v est un prolongement de u .
- Dans le cas $E = F$, lorsque A est stable par u , c'est-à-dire lorsque l'on a $\forall x \in A, u(x) \in A$, l'application $(x \in A) \mapsto (u(x) \in A)$ est appelée application induite sur A par u . On la note parfois abusivement $u|_A$, alors que la restriction de u à A est en réalité une application de A dans E .

3.2 Injectivité, surjectivité, bijectivité**Définition 3**

On dit qu'une application u de E dans F est une *injection* ou est *injective* si elle vérifie l'une des trois propriétés équivalentes suivantes :

- Tout élément de F a au plus un antécédent par u .
- Pour tout $y \in F$, l'équation $u(x) = y$ possède au plus une solution.
- $\forall (x_1, x_2) \in E^2, u(x_1) = u(x_2) \implies x_1 = x_2$.

Définition 4

On dit qu'une application u de E dans F est une *surjection* ou est *surjective* si elle vérifie l'une des trois propriétés équivalentes suivantes :

- Tout élément de F a au moins un antécédent par u .
- Pour tout $y \in F$, l'équation $u(x) = y$ possède au moins une solution.
- $\forall y \in F, \exists x \in E : y = u(x)$.

Définition 5

On dit qu'une application u de E dans F est une *bijection* ou est *bijective* si elle est injective et surjective, c'est-à-dire si elle vérifie l'une des deux propriétés équivalentes suivantes :

- (i) tout élément de F a un et un seul antécédent par u ,
- (ii) pour tout $y \in F$, l'équation $u(x) = y$ possède une unique solution.

Définition 6

Une application bijective de E sur E est encore appelée *permutation* de E . L'ensemble des permutations de E est habituellement noté $\mathcal{S}(E)$.

Exemples

1. L'application $t \mapsto t^2$ de \mathbb{R} dans \mathbb{R}_+ :
 - est surjective car tout élément de \mathbb{R}_+ possède au moins un antécédent,
 - n'est pas injective car -1 et 1 ont même image.
2. L'application $t \mapsto t^2$ de \mathbb{R}_+ dans \mathbb{R}_+ est bijective car tout élément de \mathbb{R}_+ possède un unique antécédent qui est sa racine carrée.
3. L'identité de E est une permutation de E .

3.3 Composition d'applications

Soient E , F , G et H quatre ensembles.

Définition 7

Si $u \in \mathcal{F}(E, F)$ et $v \in \mathcal{F}(F, G)$, l'application $x \mapsto v(u(x))$ définie sur E et à valeurs dans G est appelée *composée* des applications v et u ; on la note $v \circ u$.

Remarque En fait $v \circ u$ est le triplet (E, G, Γ) avec $\Gamma = \{(x, v(u(x))) \mid x \in E\}$.

Proposition 1

Étant données trois applications $E \xrightarrow{u} F \xrightarrow{v} G \xrightarrow{w} H$, on a :

$$w \circ (v \circ u) = (w \circ v) \circ u.$$

Démonstration Les applications $w \circ (v \circ u)$ et $(w \circ v) \circ u$ ont évidemment même ensemble de départ E , même ensemble d'arrivée H , et pour tout $x \in E$, on a :

$$(w \circ (v \circ u))(x) = w((v \circ u)(x)) = w(v(u(x)))$$

et :

$$((w \circ v) \circ u)(x) = (w \circ v)(u(x)) = w(v(u(x)))$$

ce qui prouve le résultat. \square

Proposition 2

Soient $u \in \mathcal{F}(E, F)$ et $v \in \mathcal{F}(F, G)$.

1. Si u et v sont injectives, alors $v \circ u$ est injective.
2. Si u et v sont surjectives, alors $v \circ u$ est surjective.
3. Si u et v sont bijectives, alors $v \circ u$ est bijective.

Démonstration

1. Supposons u et v injectives.

Soient x et x' deux éléments de E tels que $v(u(x)) = v(u(x'))$.

Grâce à l'injectivité de v on a $u(x) = u(x')$; l'injectivité de u donne alors $x = x'$.

L'application $v \circ u$ est donc injective.

2. Supposons u et v surjectives.

Soit z un élément de G .

Grâce à la surjectivité de v on peut trouver $y \in F$ tel que $z = v(y)$.

Comme u est surjective, on peut trouver $x \in E$ tel que $y = u(x)$, et on a alors :

$$z = v(u(x)) = (v \circ u)(x).$$

L'application $v \circ u$ est donc surjective.

3. Conséquence immédiate des précédents. \square

3.4 Application réciproque

Définition 8

Si u est une application bijective de E dans F , alors l'application de F dans E qui associe à tout élément de F son unique antécédent dans E s'appelle *application réciproque* de u et se note u^{-1} .

On a donc :

$$\forall (x, y) \in E \times F, y = u(x) \iff x = u^{-1}(y).$$

Exemples

1. L'application $\mathbb{R}_+ \rightarrow \mathbb{R}_+$ est bijective et sa réciproque est notée $\sqrt{}$.

$$\begin{array}{ccc} t & \longmapsto & t^2 \end{array}$$

2. L'application $[-\frac{\pi}{2}, \frac{\pi}{2}] \rightarrow [-1, 1]$ est bijective. Sa réciproque est notée \arcsin .

$$\begin{array}{ccc} x & \longmapsto & \sin x \end{array}$$

Proposition 3

Si u est une application bijective de E dans F , on a :

$$u^{-1} \circ u = \text{Id}_E \quad \text{et} \quad u \circ u^{-1} = \text{Id}_F.$$

Démonstration

- $u^{-1} \circ u$ et Id_E sont deux applications de E dans E , et pour tout $x \in E$, on a $u^{-1}(u(x)) = x$ puisque $u(x)$ possède, par u , un unique antécédent qui est évidemment x .
 Donc $u^{-1} \circ u = \text{Id}_E$.
- $u \circ u^{-1}$ et Id_F sont deux applications de F dans F , et pour tout $y \in F$, on a :

$$u(u^{-1}(y)) = y$$

car $u^{-1}(y)$ est par définition l'antécédent de y par u .

Donc $u \circ u^{-1} = \text{Id}_F$. □

► **Attention** Si u est une application bijective de E dans F , l'égalité :

$$u \circ u^{-1} = u^{-1} \circ u$$

n'a de sens que si les ensembles E et F sont égaux.

Proposition 4

Si $u \in \mathcal{F}(E, F)$ et $v \in \mathcal{F}(F, E)$ sont deux applications vérifiant $u \circ v = \text{Id}_F$ et $v \circ u = \text{Id}_E$, alors elles sont toutes deux bijectives et réciproques l'une de l'autre.

Démonstration

- L'existence d'une application $v \in \mathcal{F}(F, E)$ telle que $v \circ u = \text{Id}_E$ entraîne que u est injective. En effet, si x et x' sont deux éléments de E tels que $u(x) = u(x')$, alors $v(u(x)) = v(u(x'))$ et donc $x = x'$ puisque $v \circ u = \text{Id}_E$.
- L'existence d'une application $v \in \mathcal{F}(F, E)$ telle que $u \circ v = \text{Id}_F$ entraîne la surjectivité de u . En effet, si y est un élément de F et que l'on pose $x = v(y)$, on a $u(x) = y$ puisque $u \circ v = \text{Id}_F$.
- L'application u est donc bijective et on peut écrire :

$$v = \text{Id}_E \circ v = u^{-1} \circ u \circ v = u^{-1} \circ \text{Id}_F = u^{-1}.$$

- Par symétrie, v est bijective et $v^{-1} = u$. □

Remarque On notera qu'en adaptant légèrement cette démonstration, on peut prouver que :

- si $v \circ u$ est injective, alors u est injective,
- si $v \circ u$ est surjective, alors v est surjective.

Corollaire 5

Si u est une bijection de E dans F , alors u^{-1} est une bijection de F dans E et $(u^{-1})^{-1} = u$.

■ **Méthode** Pour démontrer qu'une application $u \in \mathcal{F}(E, F)$ est bijective et trouver sa réciproque, on peut :

- soit exhiber une application $v \in \mathcal{F}(F, E)$ telle que $u \circ v = \text{Id}_F$ et $v \circ u = \text{Id}_E$,
- soit résoudre l'équation $y = u(x)$ pour montrer qu'elle admet, quel que soit $y \in F$, une unique solution $x = v(y)$.

Exemple La relation $y = x + \sqrt{x^2 + 1}$ définit une application u de \mathbb{R} dans \mathbb{R}_+^* puisque pour $x \in \mathbb{R}$, on a $\sqrt{x^2 + 1} > \sqrt{x^2} \geq |x|$ et évidemment $x + |x| \geq 0$. Montrons qu'elle est bijective et trouvons sa réciproque. Pour $x \in \mathbb{R}$ et $y \in \mathbb{R}_+^*$, on a :

$$\begin{aligned} x + \sqrt{x^2 + 1} = y &\iff \sqrt{x^2 + 1} = y - x \\ &\iff x^2 + 1 = (y - x)^2 \quad \text{et} \quad x \leq y \\ &\iff 2xy = y^2 - 1 \quad \text{et} \quad x \leq y \\ &\iff x = \frac{y^2 - 1}{2y} \quad \text{et} \quad x \leq y \\ &\iff x = \frac{y^2 - 1}{2y} \end{aligned}$$

la dernière équivalence venant du fait que si $y > 0$, on a :

$$\frac{y^2 - 1}{2y} = y - \frac{y^2 + 1}{2y} \leq y.$$

Donc f est bijective et sa réciproque est :

$$\begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ y & \longmapsto & \frac{y^2 - 1}{2y}. \end{array}$$

Définition 9

Une *involution* de E , ou *application involutive* de E , est une application u de E dans lui même vérifiant $u \circ u = \text{Id}_E$.

Proposition 6

Une application involutive de E est bijective, et elle est sa propre réciproque ; c'est donc une permutation de E .

Exemple L'application $\varphi : \begin{array}{ccc} \mathcal{P}(E) & \longrightarrow & \mathcal{P}(E) \\ A & \longmapsto & \mathbf{C}_E A \end{array}$ est une permutation de $\mathcal{P}(E)$

puisque elle est involutive.

Proposition 7

Soient E , F et G trois ensembles. Si $E \xrightarrow{u} F \xrightarrow{v} G$ sont deux applications bijectives alors $v \circ u$ est bijective et :

$$(v \circ u)^{-1} = u^{-1} \circ v^{-1}.$$

Démonstration Il suffit d'utiliser la proposition 4 de la page 1034 en vérifiant :

$$(u^{-1} \circ v^{-1}) \circ (v \circ u) = u^{-1} \circ (v^{-1} \circ v) \circ u = u^{-1} \circ u = \text{Id}_E$$

$$(v \circ u) \circ (u^{-1} \circ v^{-1}) = v \circ (u \circ u^{-1}) \circ v^{-1} = v \circ v^{-1} = \text{Id}_G.$$

□

3.5 Images directes, images réciproques**Définition 10**

Soient u une application de E dans F ainsi que A une partie de E et B une partie de F . On appelle :

- *image (directe)* de A par u , l'ensemble :

$$u(A) = \{y \mid \exists x \in A : y = u(x)\} = \{u(x) \mid x \in A\},$$

- *image réciproque* de B par u , l'ensemble :

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

Remarques

1. L'utilisation de la notation $u^{-1}(B)$ ne suppose pas que u est bijective.
2. Lorsque u est bijective, $u^{-1}(B)$ représente aussi bien l'image directe de B par l'application u^{-1} , que l'image réciproque de B par u car on a alors :

$$\{x \in E \mid u(x) \in B\} = \{u^{-1}(y) \mid y \in B\}$$

comme on peut le vérifier par double inclusion.

Exemples

1. Si f est l'application $\mathbb{R} \longrightarrow \mathbb{R}$, on a :

$$x \longmapsto x^2$$

- $f([-2, 2]) = [0, 4]$; • $f([-1, 2]) = [0, 4]$;
- $f^{-1}([0, 4]) = [-2, 2]$; • $f^{-1}([-2, 4]) = [-2, 2]$;
- $f^{-1}([-2, -1]) = \emptyset$.

2. Si $u \in \mathcal{F}(E, F)$, alors on a :

- $u^{-1}(\emptyset) = \emptyset$ et $u(\emptyset) = \emptyset$,
- $u^{-1}(F) = E$ mais l'inclusion $u(E) \subset F$ n'est une égalité que si u est surjective.

3. Une application u de E dans F est :

- injective si, et seulement si, pour tout $y \in F$, l'ensemble $u^{-1}(\{y\})$ a au plus un élément,
- surjective si, et seulement si, pour tout $y \in F$, l'ensemble $u^{-1}(\{y\})$ a au moins un élément,
- bijective si, et seulement si, pour tout $y \in F$, l'ensemble $u^{-1}(\{y\})$ a exactement un élément.

■ Méthode

Soit $u \in \mathcal{F}(E, F)$.

- ▶ Pour trouver l'image réciproque d'une partie B de F par u , il suffit de résoudre $u(x) \in B$.
- ▶ Pour trouver l'image directe d'une partie A de E par u , il suffit de trouver les éléments $y \in F$ pour lesquels l'équation ($y = u(x)$ et $x \in A$) a au moins une solution.

Exemple Soit $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$(x,y) \mapsto (x+y, xy).$$

- Soit $(s,p) \in \mathbb{R}^2$. Pour que (s,p) appartienne à l'image de f , il faut et il suffit que le système :

$$\begin{cases} x + y = s \\ xy = p \end{cases}$$

admette des solutions dans \mathbb{R}^2 , c'est-à-dire que l'équation du second degré $X^2 - sX + p = 0$ admette des solutions réelles.

L'image de f est donc :

$$\{(s,p) \in \mathbb{R}^2 \mid s^2 - 4p \geq 0\}.$$

- L'image réciproque par f de l'ensemble $\{(s,p) \in \mathbb{R}^2 \mid s^2 - 4p = 1\}$ est l'ensemble des couples (x,y) tels que $(x+y)^2 - 4xy = 1$.
Cette équation est équivalente à $(y-x)^2 = 1$, ce qui prouve que l'ensemble cherché est la réunion des deux droites d'équations $y = x+1$ et $y = x-1$.

Exemples

1. Étant donnés $u \in \mathcal{F}(E,F)$ ainsi que B et B' deux parties de F , on a les relations suivantes :

- $B \subset B' \implies u^{-1}(B) \subset u^{-1}(B')$,
- $u^{-1}(B \cup B') = u^{-1}(B) \cup u^{-1}(B')$,
- $u^{-1}(B \cap B') = u^{-1}(B) \cap u^{-1}(B')$,
- $u^{-1}(\complement_F B) = \complement_E u^{-1}(B)$.

Démonstration

- Si $B \subset B'$, on a :

$$x \in u^{-1}(B) \implies u(x) \in B \implies u(x) \in B' \implies x \in u^{-1}(B').$$

- On a :

$$\begin{aligned} x \in u^{-1}(B \cup B') &\iff u(x) \in B \cup B' \\ &\iff u(x) \in B \text{ ou } u(x) \in B' \\ &\iff x \in u^{-1}(B) \text{ ou } x \in u^{-1}(B') \\ &\iff x \in u^{-1}(B) \cup u^{-1}(B'). \end{aligned}$$

- Même démonstration en remplaçant \cup par \cap et « ou » par « et ».

(d) L'équivalence :

$$x \in u^{-1}(B) \iff u(x) \in B$$

peut s'écrire :

$$x \notin u^{-1}(B) \iff u(x) \notin B$$

ce qui donne :

$$x \in C_E(u^{-1}(B)) \iff u(x) \in C_F B \iff x \in u^{-1}(C_F B). \quad \square$$

2. Les résultats correspondants pour l'image directe ne sont pas toujours vérifiés.

Soient $u \in \mathcal{F}(E, F)$ ainsi que $A \subset E$ et $A' \subset E$.

- On a évidemment $A \subset A' \implies u(A) \subset u(A')$.
- On a bien $u(A \cup A') = u(A) \cup u(A')$:
 - comme $A \subset A \cup A'$, on a $u(A) \subset u(A \cup A')$. Par symétrie on a donc aussi $u(A') \subset u(A \cup A')$, ce qui donne $u(A) \cup u(A') \subset u(A \cup A')$.
 - si $y \in u(A \cup A')$, on peut trouver $x \in A \cup A'$ tel que $y = u(x)$. Comme x appartient à A ou à A' , l'élément y appartient à $u(A)$ ou à $u(A')$ et donc à leur réunion.
- De même que ci-dessus, les inclusions $A \cap A' \subset A$ et $A \cap A' \subset A'$ entraînent $u(A \cap A') \subset u(A) \cap u(A')$, mais l'inclusion inverse est fausse en général comme le prouvent par exemple les égalités suivantes :

$$\sin([0, 2\pi]) \cap \sin([- \pi, \pi]) = [-1, 1]$$

$$\sin([0, 2\pi] \cap [-\pi, \pi]) = [0, 1].$$

3.6 Familles

Définition 11

Étant donnés deux ensembles I et E , on appelle *famille* d'éléments de E indexée par I toute application de I dans E .

Remarques

- L'utilisation du terme famille sous-entend que l'on utilise une notation indiquée $(x_i)_{i \in I}$ à la place d'une notation fonctionnelle $i \mapsto x(i)$.
On peut d'ailleurs aussi écrire $(x(i))_{i \in I}$.
- Suivant que l'on utilise l'écriture indicée ou l'écriture fonctionnelle, une application I dans E est plutôt considérée comme :
 - une collection d'objets étiquetés par les éléments de I ,
 - un processus permettant de calculer les images des éléments de I .

Exemples

1. Si p est un entier naturel non nul et $I = \llbracket 1, p \rrbracket$, une famille $(x_i)_{i \in \llbracket 1, p \rrbracket}$ est identifiée avec la p -liste (x_1, x_2, \dots, x_p) .
2. Si $I = \mathbb{N}$, une famille $(x_i)_{i \in \mathbb{N}}$ de E est appelée suite d'éléments de E .
3. Par extension, on appelle suite d'éléments de E , une famille indexée par une partie de \mathbb{N} du type $\{n \in \mathbb{N} \mid n \geq n_0\}$; on la note aussi $(x_n)_{n \geq n_0}$.
4. Étant donnés deux ensembles I et E , une famille de parties de E indexée par I est une famille $(A_i)_{i \in I}$ d'éléments de $\mathcal{P}(E)$.

On peut généraliser à la famille $(A_i)_{i \in I}$ les notions d'intersection et de réunion par :

$$\bigcap_{i \in I} A_i = \{x \in E \mid \forall i \in I, x \in A_i\}$$

$$\bigcup_{i \in I} A_i = \{x \in E \mid \exists i \in I : x \in A_i\}$$

Avec ces définitions, on a les propriétés suivantes :

$$\bigcap_{i \in I \cup J} A_i = \left(\bigcap_{i \in I} A_i \right) \cap \left(\bigcap_{i \in J} A_i \right)$$

$$\bigcup_{i \in I \cup J} A_i = \left(\bigcup_{i \in I} A_i \right) \cup \left(\bigcup_{i \in J} A_i \right)$$

$$\complement_E \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} \complement_E A_i$$

$$\complement_E \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} \complement_E A_i$$

4. Relations d'ordre

4.1 Relations binaires

Soit E un ensemble quelconque.

Définition 12

Si G est un graphe de E , le prédictat \mathcal{R} défini par :

$$\mathcal{R}(x, y) \iff (x, y) \in G$$

est appelé *relation binaire* sur E .

La plupart du temps on donne une relation binaire par le prédictat \mathcal{R} sans parler de G et on écrit $x \mathcal{R} y$ au lieu de $\mathcal{R}(x, y)$.

Exemples

1. La relation définie sur \mathbb{R} par $x \mathcal{R} y \iff x \leq y$ a pour graphe le demi-plan situé au dessus de la première bissectrice.
2. La relation définie sur \mathbb{R} par $x \mathcal{R} y \iff x^2 = y^2$ a pour graphe la réunion des droites d'équations $y = x$ et $y = -x$.

4.2 Ensembles ordonnés

Définition 13

Une relation binaire \mathcal{R} sur un ensemble E est une relation d'ordre sur E si elle est :

réflexive : $\forall x \in E, x \mathcal{R} x$

antisymétrique : $\forall (x,y) \in E^2, (x \mathcal{R} y \text{ et } y \mathcal{R} x) \implies x = y$

transitive : $\forall (x,y,z) \in E^3, (x \mathcal{R} y \text{ et } y \mathcal{R} z) \implies x \mathcal{R} z$

On appelle *ensemble ordonné* un couple (E, \mathcal{R}) où \mathcal{R} est une relation d'ordre sur E .

Exemples

1. Les relations d'ordre usuelles sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} ou \mathbb{R} notées \leq ou \geq .
2. La relation d'ordre strict $<$ utilisée habituellement sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} ou \mathbb{R} n'est pas une relation d'ordre : elle est antisymétrique et transitive, mais elle n'est pas réflexive.
3. La relation d'inclusion sur $\mathcal{P}(E)$.
4. La relation de divisibilité définie dans \mathbb{N} par :

$$x | y \iff \exists k \in \mathbb{N} : y = kx.$$

5. La relation de divisibilité définie dans \mathbb{Z} par :

$$x | y \iff \exists k \in \mathbb{Z} : y = kx$$

n'est pas une relation d'ordre car elle n'est pas antisymétrique.

6. L'*ordre lexicographique* défini sur \mathbb{R}^2 par :
- $$(a,c) \leq (b,d) \iff (a < b \text{ ou } (a = b \text{ et } c \leq d)).$$
7. Sur \mathbb{C} , on peut définir des relations d'ordre (ordre lexicographique par exemple) mais, en général, on ne les utilise pas car elles ne sont pas compatibles avec la structure de corps de \mathbb{C} , c'est-à-dire qu'aucune ne vérifie, pour tous z_1, z_2, z les deux propriétés suivantes :

$$z_1 \leq z_2 \implies z_1 + z \leq z_2 + z \quad \text{et} \quad (z_1 \leq z_2 \text{ et } 0 \leq z) \implies z_1 z \leq z_2 z.$$

8. L'*ordre alphabétique* sur l'ensemble des mots de la langue française ; c'est en fait une généralisation de l'*ordre lexicographique* défini ci-dessus sur \mathbb{R}^2 .

Remarques

- On note souvent une relation d'ordre par le symbole \leqslant , qui se lit « inférieur ou égal », ce qui ne signifie pas forcément que l'on travaille sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} ou \mathbb{R} munis de leur relation d'ordre usuelle. Si $x \leqslant y$ est vérifié, on dit aussi que « x est plus petit que y » ou que « y est plus grand que x ».
- Lorsque la relation d'ordre est notée \leqslant , on écrit $x < y$ pour signifier $x \leqslant y$ et $x \neq y$, et on dit que « x est strictement plus petit que y » ou que « y est strictement plus grand que x ».
- On pourra écrire $a \leqslant b \leqslant c$ à la place de $a \leqslant b$ et $b \leqslant c$. Par transitivité, cela implique évidemment aussi : $a \leqslant c$.

4.3 Propriétés

Définition 14

On dit que la relation d'ordre \leqslant définit un *ordre total* sur E si :

$$\forall (x, y) \in E^2, (x \leqslant y \text{ ou } y \leqslant x).$$

Dans le cas contraire on dit que c'est un *ordre partiel*.

Exemples d'ordre total

- Les relations d'ordre usuelles sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} ou \mathbb{R} .
- L'ordre lexicographique sur \mathbb{R}^2 .
- L'ordre alphabétique dans un dictionnaire.

Exemples d'ordre partiel

- La relation de divisibilité dans \mathbb{N} .
- La relation d'inclusion sur $\mathcal{P}(E)$ lorsque E contient au moins deux éléments.
- Sur \mathbb{R}^2 la relation définie par $(a, c) \leqslant (b, d) \iff (a \leqslant b \text{ et } c \leqslant d)$.

► **Attention** Bien prendre garde que certaines réactions que l'on peut avoir ne s'appliquent qu'à un ordre total. Par exemple, une réflexion trop hâtive peut laisser croire que la négation de $x \leqslant y$ est $y < x$, c'est-à-dire $y \leqslant x$ et $x \neq y$. Il n'en est rien comme le prouve $X \subset Y$ dont la négation n'est pas $Y \subsetneq X$.

Définition 15

Soient (E, \leqslant) un ensemble ordonné, A une partie de E et a un élément de A .

- On dit que a est le *plus grand élément* de A si $\forall x \in A, x \leqslant a$.

Quand il existe, le plus grand élément de A se note $\max(A)$ ou $\max A$.

- On dit que a est le *plus petit élément* de A si $\forall x \in A, a \leqslant x$.

Quand il existe, le plus petit élément de A se note $\min(A)$ ou $\min A$.

Démonstration L'utilisation de l'article défini « le » dans la définition précédente exige une démonstration d'unicité.

Supposons que a et b soient deux plus grands éléments de A ; on a :

- $a \leq b$ car b est plus grand élément,
- $b \leq a$ car a est plus grand élément,

et donc, par antisymétrie, $a = b$.

Il en est de même pour le plus petit élément. □

Exemples

1. Dans \mathbb{N} , \mathbb{Z} , \mathbb{Q} ou \mathbb{R} munis de leur ordre usuel, il n'y a pas de plus grand élément.
2. L'intervalle $[0, 1]$ muni de l'ordre usuel possède :
 - un plus grand élément 1,
 - un plus petit élément 0.
3. L'intervalle $]0, 1]$ muni de l'ordre usuel :
 - possède un plus grand élément 1,
 - ne possède pas de plus petit élément.
4. $\mathcal{P}(E)$ possède, pour l'inclusion, un plus grand élément E et un plus petit élément \emptyset .
5. Si E possède au moins deux éléments, l'ensemble $\mathcal{P}(E) \setminus \{E\}$ ne possède pas de plus grand élément pour l'inclusion.
6. Dans \mathbb{N} muni de la divisibilité, le plus petit élément est 1, et le plus grand élément est 0.
7. Soit f une application d'un ensemble X dans un ensemble ordonné E . Si $\{f(x) \mid x \in X\}$ admet un plus grand élément, ce dernier est appelé *maximum* de f sur X et se note $\max_X f$.

Cet exemple permet d'expliquer la notation \max pour désigner le plus grand élément.

De même, on note $\min_X f$ le *minimum* de f sur X , c'est-à-dire le plus petit élément de $\{f(x) \mid x \in X\}$, lorsqu'il existe.

Définition 16

Si A est une partie d'un ensemble ordonné (E, \leq) , un élément $a \in E$ est :

- un *majorant* de A si $\forall x \in A, x \leq a$,
- un *minorant* de A si $\forall x \in A, a \leq x$.

Exemples

1. Dans (\mathbb{R}, \leq) , l'intervalle $[0, 1]$ a pour majorant tout élément de $[1, +\infty[$.
2. Dans (\mathbb{R}, \leq) , l'intervalle $[0, 1[$ a pour majorant tout élément de $[1, +\infty[$.
3. Dans $(\mathcal{P}(E), \subset)$, la partie $\{X, Y\}$ est majorée par tout ensemble contenant $X \cup Y$.
4. Dans $(\mathbb{N}, |)$, les majorants de $\{8, 18, 12\}$ sont les multiples de 72.

Définition 17

Soient E et F deux ensembles ordonnés. Une application f de E dans F est :

- *croissante* si $\forall (x, y) \in E^2, x \leq y \implies f(x) \leq f(y)$,
- *décroissante* si $\forall (x, y) \in E^2, x \leq y \implies f(x) \geq f(y)$,
- *strictement croissante* si $\forall (x, y) \in E^2, x < y \implies f(x) < f(y)$,
- *strictement décroissante* si $\forall (x, y) \in E^2, x < y \implies f(x) > f(y)$,
- *(strictement) monotone* si elle est (strictement) croissante ou (strictement) décroissante.

Remarque Une application monotone est strictement monotone si, et seulement si, elle est injective.

Chapitre 36

Entiers naturels, ensembles finis, dénombrément

1. Principe de récurrence

1.1 L'ensemble \mathbb{N}

L'ensemble \mathbb{N} des *entiers naturels* est un ensemble non vide totalement ordonné qui possède les propriétés fondamentales suivantes :

- Toute partie non vide de \mathbb{N} possède un plus petit élément.
- Toute partie non vide majorée de \mathbb{N} possède un plus grand élément.

Remarques

- Si n est un entier naturel, l'ensemble des entiers strictement plus grands que n est un ensemble non vide ; son plus petit élément, appelé *successeur* de n , est $n + 1$. Si x est un entier naturel, on a donc l'équivalence :

$$x > n \iff x \geq n + 1.$$

- Si n est un entier naturel non nul, l'ensemble des entiers strictement plus petits que n est non vide (il contient 0) et majoré par n ; son plus grand élément, appelé *prédécesseur* de n , est $n - 1$. Si x est un entier naturel, on a donc l'équivalence :

$$x < n \iff x \leq n - 1.$$

- Soit A une partie non vide de \mathbb{Z} majorée par $M \in \mathbb{Z}$. En prenant $n_0 \in A$, l'ensemble $A' = \mathbb{N} \cap \{n - n_0 \mid n \in A\}$ est une partie non vide de \mathbb{N} majorée par $M - n_0 \in \mathbb{N}$. Elle possède donc un plus grand élément a' , et il est clair que $a' + n_0$ est alors le plus grand élément de A .
Toute partie non vide majorée de \mathbb{Z} possède donc un plus grand élément.
- De même, si A est une partie non vide de \mathbb{Z} minorée par $m \in \mathbb{Z}$, on démontre que A possède un plus petit élément en considérant $\{n - m \mid n \in A\}$.

1.2 Raisonnement par récurrence

Théorème 1

Soit P une propriété définie sur \mathbb{N} . Si :

- (1) $P(0)$ est vraie,
- (2) $\forall n \in \mathbb{N}, (P(n) \implies P(n+1))$.

Alors, pour tout entier naturel n , $P(n)$ est vraie.

Démonstration Raisonnons par l'absurde en supposant que la propriété P n'est pas vérifiée sur \mathbb{N} .

L'ensemble A des entiers n pour lesquels $P(n)$ est faux est alors une partie non vide de \mathbb{N} qui admet donc un plus petit élément α . D'après (1), l'entier 0 n'appartient pas à A . Par suite, α est non nul et, comme c'est le plus petit élément de A , l'entier $\alpha - 1$ n'appartient pas à A .

On en déduit que $P(\alpha - 1)$ est vraie, ce qui implique, d'après la propriété (2), que $P(\alpha)$ est vraie, et contredit l'appartenance de α à A .

La propriété $P(n)$ est donc vraie pour tout entier naturel n . □

Exemple On démontre par récurrence les identités classiques :

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

$$\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=0}^n k^3 = \frac{n^2(n+1)^2}{4}.$$

En appliquant le théorème 1 à la propriété $P(n_0 + n)$, on déduit :

Corollaire 2 (Récurrence à partir d'un entier $n_0 \in \mathbb{Z}$)

Soit P une propriété définie sur $\llbracket n_0, +\infty \rrbracket$. On suppose que :

- (1) $P(n_0)$ est vraie,
- (2) $\forall n \geq n_0, (P(n) \implies P(n+1))$.

Alors, pour tout entier $n \geq n_0$, la propriété $P(n)$ est vraie.

Corollaire 3

Soit P une propriété définie sur $\llbracket n_0, +\infty \rrbracket$. On suppose que :

- (1) $P(n_0)$ et $P(n_0 + 1)$ sont vraies,
- (2) $\forall n \geq n_0, ((P(n) \text{ et } P(n+1)) \implies P(n+2))$.

Alors, pour tout entier naturel $n \geq n_0$, la propriété $P(n)$ est vraie.

Démonstration Il suffit d'appliquer le corollaire 2 à la propriété $(P(n) \text{ et } P(n+1))$. \square

► **Attention** Dans le cas d'utilisation de cette forme de récurrence, il ne faut surtout pas oublier de vérifier la double initialisation $P(n_0)$ et $P(n_0 + 1)$.

Exemple Soit $(u_n)_{n \in \mathbb{N}}$ la suite définie par :

$$\begin{cases} u_0 = 2 \\ u_1 = 3 \\ \forall n \in \mathbb{N}, u_{n+2} = 3u_{n+1} - 2u_n. \end{cases}$$

On peut déterminer les premières valeurs prises par la suite :

n	0	1	2	3	4	5	6
u_n	2	3	5	9	17	33	65

Ce tableau nous suggère $\forall n \in \mathbb{N}, u_n = 2^n + 1$. Démontrons donc par récurrence la propriété $P(n) : u_n = 2^n + 1$.

- $P(0)$ et $P(1)$ sont vraies d'après les deux premières colonnes du tableau ci-dessus.
- Soit n un entier ; supposons $P(n)$ et $P(n+1)$. Alors d'après la définition de la suite :

$$u_{n+2} = 3 \times (2^{n+1} + 1) - 2 \times (2^n + 1) = 2^{n+2} + 1$$

ce qui montre $P(n+2)$.

Corollaire 4

Soit P une propriété définie sur $[n_0, +\infty[$. On suppose que :

(1) $P(n_0)$ est vraie,

(2) $\forall n \geq n_0, ((P(n_0) \text{ et } P(n_0+1) \dots \text{ et } P(n)) \implies P(n+1))$.

Alors, pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Démonstration Appliquons le corollaire 2 de la page précédente à la propriété Q définie sur $[n_0, +\infty[$ par :

$$Q(n) : \forall k \in [n_0, n], P(k).$$

- $Q(n_0)$ est vraie d'après (1).
- Soit n un entier supérieur ou égal à n_0 ; supposons $Q(n)$. De la propriété (2), on déduit que $P(n+1)$ est vraie, ce qui montre que la propriété $(Q(n) \text{ et } P(n+1))$, c'est-à-dire $Q(n+1)$, est vraie.

D'après le corollaire 2 de la page précédente, on en déduit que $Q(n)$ est vraie pour tout $n \geq n_0$, d'où en particulier :

$$\forall n \geq n_0, P(n).$$

□

Exemple Démontrons par récurrence que tout entier supérieur ou égal à 2 admet un diviseur premier.

Soit $P(n)$: « L'entier n admet un diviseur premier ».

- $P(2)$ est vraie, puisque 2 est un diviseur premier de lui-même.
- Soit n un entier supérieur ou égal à 2 ; supposons la propriété vraie jusqu'au rang n , c'est-à-dire supposons $P(2), P(3), \dots, P(n)$. Il y a deux cas possibles pour l'entier $n+1$:
 - soit $n+1$ est premier, et alors l'entier $n+1$ est lui-même un diviseur premier de $n+1$.
 - soit $n+1$ n'est pas premier et alors $n+1$ admet un diviseur k strictement compris entre 1 et $n+1$; comme $2 \leq k \leq n$, on sait que $P(k)$ est vraie et donc que l'entier k a un diviseur premier d ; par transitivité, l'entier $n+1$ admet d comme diviseur premier.

Dans chacun des cas, l'entier $n+1$ a un diviseur premier, ce qui signifie que $P(n+1)$ est vraie.

1.3 Suites définies par récurrence

Si E est un ensemble, une suite d'éléments de E est une famille d'éléments de E indexée par \mathbb{N} , et plus généralement par une partie de \mathbb{N} .

Étant donnés une application f de E dans lui-même, ainsi qu'un élément a de E , le principe de récurrence entraîne qu'il existe une unique suite u , définie sur \mathbb{N} , telle que :

$$u_0 = a \quad \text{et} \quad \forall n \in \mathbb{N}, u_{n+1} = f(u_n).$$

Plus généralement, une suite $(u_n)_{n \in \mathbb{N}}$ est entièrement définie par :

- la donnée de u_0 et d'une relation de récurrence du type $u_{n+1} = f(n, u_n)$, où f est une application de $\mathbb{N} \times E$ dans E .
- la donnée de u_0 et u_1 ainsi que d'une relation du type $u_{n+2} = f(u_n, u_{n+1})$, où f est une application de $E \times E$ dans E .
- la donnée de u_0 et u_1 ainsi que d'une relation du type $u_{n+2} = f(n, u_n, u_{n+1})$, où f est une application de $\mathbb{N} \times E \times E$ dans E .
- la donnée de u_0, u_1, \dots , et u_p ainsi que d'une relation du type $u_{n+p} = f(n, u_n, u_{n+1}, \dots, u_{n+p-1})$, où p est un entier naturel et f est une application de $\mathbb{N} \times E^p$ dans E .
- la donnée de u_0 ainsi que d'une relation du type $u_{n+1} = f_n(n, u_0, u_1, \dots, u_n)$, où pour tout entier naturel n , f_n est une application de $\mathbb{N} \times E^{n+1}$ dans E .

2. Ensembles finis

2.1 Définitions

Lemme

Si n et m sont deux entiers naturels tels que $\llbracket 1, n \rrbracket$ et $\llbracket 1, m \rrbracket$ soient en bijection, alors $n = m$.

Démonstration Montrons par récurrence la propriété H_n : « Pour tout entier naturel m , si $\llbracket 1, n \rrbracket$ et $\llbracket 1, m \rrbracket$ sont en bijection, alors $n = m$. »

- H_0 est vraie, car l'ensemble vide n'est en bijection qu'avec lui-même.
- Supposons H_n pour $n \in \mathbb{N}$. Soit $m \in \mathbb{N}$ et $h : \llbracket 1, n+1 \rrbracket \rightarrow \llbracket 1, m \rrbracket$ une bijection.

Premier cas : si $h(n+1) \neq m$. Posons $a = h(n+1)$ et considérons $\tilde{h} = \varphi \circ h$ où φ est l'application de $\llbracket 1, m \rrbracket$ dans lui-même échangeant a et m et laissant fixes les autres éléments. L'application \tilde{h} est une bijection de $\llbracket 1, n+1 \rrbracket$ sur $\llbracket 1, m \rrbracket$, puisque φ est involutive et h bijective. De plus, elle vérifie $\tilde{h}(n+1) = m$. Quitte à remplacer h par \tilde{h} , on peut donc supposer être dans le cas suivant.

Deuxième cas : si $h(n+1) = m$. Alors h induit une bijection de $\llbracket 1, n \rrbracket$ sur $\llbracket 1, m-1 \rrbracket$ et donc, d'après H_n , on a $n = m-1$, c'est-à-dire $n+1 = m$.

D'où H_{n+1} . □

Définition 1

Un ensemble E est un *ensemble fini* s'il existe un entier naturel n tel que E soit en bijection avec $\llbracket 1, n \rrbracket$. Il y a alors unicité d'un tel entier n , que l'on appelle **cardinal de E** et que l'on note $\text{card}(E)$ ou $\text{card } E$.

Un ensemble qui n'est pas fini est appelé *ensemble infini*.

Démonstration Soit φ une bijection de E sur $\llbracket 1, n \rrbracket$ et ψ une bijection de E sur $\llbracket 1, m \rrbracket$. Alors l'application $\psi \circ \varphi^{-1}$ est une bijection de $\llbracket 1, n \rrbracket$ sur $\llbracket 1, m \rrbracket$, ce qui prouve $n = m$ d'après le lemme précédent. □

Exemples

1. L'ensemble vide est un ensemble fini de cardinal 0.
2. Si n est un entier naturel, l'intervalle $\llbracket 1, n \rrbracket$ est fini et a pour cardinal n .
3. Si n et p sont deux entiers naturels, l'application $k \mapsto k+p$ est une bijection de $\llbracket 1, n \rrbracket$ dans $\llbracket p+1, p+n \rrbracket$. L'intervalle $\llbracket p+1, p+n \rrbracket$ est donc un ensemble fini à n éléments.
4. Si p et q sont deux entiers relatifs tels que $p \leq q$, l'ensemble $\llbracket p, q \rrbracket$ est fini de cardinal $q-p+1$.
En particulier, pour $n \in \mathbb{N}$, l'ensemble $\llbracket 0, n \rrbracket$ est fini de cardinal $n+1$.
5. La composée de deux bijections étant une bijection, tout ensemble en bijection avec un ensemble fini de cardinal n est lui-même fini et de cardinal n .
6. Un ensemble en bijection avec un ensemble infini est lui-même infini.

Remarques Soit $n \in \mathbb{N}^*$.

- Une bijection de $\llbracket 1, n \rrbracket$ dans E permet de numérotter les éléments de E et d'écrire l'ensemble en extension :

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

- Mais l'écriture $E = \{x_1, x_2, \dots, x_n\}$ n'implique pas $\text{card } E = n$. Il faut en plus que les x_k soient distincts deux à deux, pour que l'application $i \mapsto x_i$ soit une bijection de $\llbracket 1, n \rrbracket$ dans E .

2.2 Propriétés des cardinaux

Sous-ensemble d'un ensemble fini

Lemme

Étant donnés un ensemble fini E de cardinal $n \neq 0$ et un élément a de E , l'ensemble $E' = E \setminus \{a\}$ est fini de cardinal $n - 1$.

Démonstration Soit h une bijection de E sur $\llbracket 1, n \rrbracket$.

- Si $h(a) = n$, l'application h induit une bijection de E' sur $\llbracket 1, n - 1 \rrbracket$, ce qui prouve que E' est fini de cardinal $n - 1$.
- Si $h(a) = p < n$, on se ramène au cas précédent en posant $\tilde{h} = \varphi \circ h$, où φ est l'involution de $\llbracket 1, n \rrbracket$ échangeant p et n et laissant les autres fixes.

□

Théorème 5

Si E est un ensemble fini et F une partie de E , alors :

- F est un ensemble fini et $\text{card } F \leq \text{card } E$,
- $\text{card } F = \text{card } E \iff F = E$.

Démonstration Démontrons ce résultat par récurrence sur le cardinal de E .

- Si $\text{card } E = 0$, alors E est vide et les résultats sont évidents.
- Supposons le résultat pour tout ensemble fini de cardinal n . Soit E de cardinal $n + 1$ et F une partie de E .
 - Si $F = E$, alors F est fini et $\text{card } F = \text{card } E$.
 - Sinon, il existe un élément e de E qui n'est pas dans F . On a alors $F \subset E' = E \setminus \{e\}$ avec $\text{card } E' = n$ d'après le lemme précédent. L'hypothèse de récurrence nous dit donc que F est fini et que :

$$\text{card } F \leq \text{card } E' = n < n + 1 = \text{card } E.$$

On a donc démontré :

$$\text{card } F \leq \text{card } E \quad \text{et} \quad \text{card } F = \text{card } E \iff F = E.$$

□

Remarques

1. Le résultat précédent prouve qu'il est impossible qu'un ensemble fini E soit en bijection avec l'une de ses parties strictes.
2. L'exemple de la bijection $n \mapsto 2n$ de \mathbb{N} sur l'ensemble des pairs montre que :
 - \mathbb{N} est infini
 - il se peut qu'un ensemble (infini) soit en bijection avec une de ses parties strictes.

Parties de \mathbb{N}

Proposition 6

Soit E un ensemble. Les propositions suivantes sont équivalentes :

- (i) E est infini,
- (ii) il existe une injection de \mathbb{N} dans E , c'est-à-dire une suite d'éléments de E distincts deux à deux,
- (iii) il existe une partie de E en bijection avec \mathbb{N} .

Démonstration

(i) \implies (ii). Construisons une suite d'éléments de E distincts deux à deux.

- ▶ Puisque E n'est pas lini, il est non vide. On peut donc trouver un élément $x_0 \in E$.
- ▶ Supposons construits x_0, x_1, \dots et x_{n-1} des éléments de E distincts deux à deux. Alors, puisque E n'est pas lini, l'inclusion $\{x_0, x_1, \dots, x_{n-1}\} \subset E$ est stricte, ce qui permet de trouver un élément $x_n \in E$ distinct des précédents.

(ii) \implies (iii). Si f est une injection de \mathbb{N} dans E , elle induit une bijection de \mathbb{N} sur $f(\mathbb{N})$.

(iii) \implies (i). Une partie de E en bijection avec \mathbb{N} est inlinie, ce qui prouve que E ne peut pas être lini. \square

Remarque Si E est un ensemble infini, on peut trouver une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de E distincts deux à deux. L'application $f : x_n \mapsto x_{n+1}$ est alors une injection de $F = \{x_n \mid n \in \mathbb{N}\}$ dans lui-même. En prolongeant f sur E par $\forall x \in E \setminus F, f(x) = x$, on obtient une injection de E dans E , non bijective puisque x_0 n'a pas d'antécédent.

Tout ensemble infini est donc en bijection avec une de ses parties strictes.

Proposition 7 (Caractérisation des parties finies de \mathbb{N})

Une partie de \mathbb{N} est finie si, et seulement si, elle est majorée.

Démonstration

- ▶ Soit P une partie majorée de \mathbb{N} . Il existe donc un entier n_0 majorant P , et P étant une partie de l'ensemble lini $[\![0, n_0]\!]$, est elle-même finie.
- ▶ Démontrons par récurrence sur n que toute partie à n éléments de \mathbb{N} est majorée.
 - Seul l'ensemble vide a un cardinal nul, et il est majoré par 0 (par exemple) puisque l'on a $\forall x \in \emptyset, x \leqslant 0$.
 - Supposons la propriété vraie au rang $n - 1$. Soit A une partie à n éléments ; la partie A s'écrit $A = A' \cup \{a\}$, avec $\text{card } A' = n - 1$.

D'après l'hypothèse de récurrence, la partie A' à $n - 1$ éléments est majorée par un entier M , et par suite la partie A est majorée par $\max(a, M)$.

D'où le résultat au rang n . □

Lemme

1. Soit $n \in \mathbb{N}$. Si f est une application strictement croissante de $\llbracket 0, n \rrbracket$ dans \mathbb{N} , alors $\forall p \in \llbracket 0, n \rrbracket$, $f(p) \geq p$.
2. Si f est une application strictement croissante de \mathbb{N} dans \mathbb{N} , alors $\forall n \in \mathbb{N}$, $f(n) \geq n$.

Démonstration

1. Raisonnons par récurrence sur n .

- Si $n = 0$, le résultat est évident.
- Supposons le résultat vrai pour $n \in \mathbb{N}$. Si f est une application strictement croissante de $\llbracket 0, n + 1 \rrbracket$ dans \mathbb{N} , alors sa restriction à $\llbracket 0, n \rrbracket$ est strictement croissante et l'hypothèse de récurrence donne $\forall p \leq n$, $f(p) \geq p$. Alors $f(n + 1) > f(n) \geq n$, ce qui prouve $f(n + 1) \geq n + 1$. Le résultat est donc vrai pour $n + 1$.

2. Pour tout $n \in \mathbb{N}$, il suffit d'appliquer le résultat précédent à $f|_{\llbracket 0, n \rrbracket}$. □

Proposition 8

Si P est une partie finie non vide de \mathbb{N} de cardinal n , il existe une bijection (strictement) croissante, et une seule, de l'intervalle $\llbracket 1, n \rrbracket$ sur P .

Démonstration

Existence. Raisonnons par récurrence sur le cardinal de P .

- Si P a un seul élément x , l'application $1 \mapsto x$ est évidemment une bijection croissante de $\llbracket 1, 1 \rrbracket$ dans P .
- Supposons le résultat vrai pour toute partie de \mathbb{N} de cardinal $n - 1$. Soit P une partie de \mathbb{N} à n éléments. Alors, d'après la proposition précédente, P est majorée. C'est alors une partie non vide majorée de \mathbb{N} , qui possède donc un plus grand élément a .

Comme $P \setminus \{a\}$ possède $n - 1$ éléments, on peut trouver une bijection croissante f de $\llbracket 1, n - 1 \rrbracket$ sur $P \setminus \{a\}$. En prolongeant f par $f(n) = a$, on obtient une bijection croissante de $\llbracket 1, n \rrbracket$ sur P .

D'où le résultat pour toute partie de \mathbb{N} à n éléments.

Unicité. Si f est une bijection croissante de $\llbracket 1, n \rrbracket$ sur P , alors sa réciproque est une bijection croissante. En effet, si x et y sont deux éléments de P tels que $x < y$, on ne peut pas avoir $f^{-1}(x) \geq f^{-1}(y)$ d'après la croissance de f et donc, puisque \mathbb{N} est totalement ordonné, on a $f^{-1}(x) < f^{-1}(y)$.

Si maintenant f et g sont deux bijections croissantes de $\llbracket 1, n \rrbracket$ sur P , la composée $h = f^{-1} \circ g$ ainsi que sa réciproque sont des bijections croissantes de $\llbracket 1, n \rrbracket$ sur lui-même. On a donc d'après le lemme précédent :

$$\forall p \in \llbracket 1, n \rrbracket, h(p) \geqslant p \quad \text{et} \quad \forall p \in \llbracket 1, n \rrbracket, h^{-1}(p) \geqslant p.$$

Donc $\forall p \in \llbracket 1, n \rrbracket, h(p) = p$, ce qui prouve $f = g$. \square

Proposition 9

Si P est une partie infinie de \mathbb{N} , il existe une bijection (strictement) croissante, et une seule, de \mathbb{N} sur P .

Démonstration

Existence. Comme P est infinie, elle est non vide ; on peut donc définir $a_0 = \min P$.

Définissons par récurrence une application f de \mathbb{N} dans P .

- On pose $f(0) = a_0$.
- Supposons construits $f(0) < f(1) < \dots < f(n-1)$. Comme P est infini, il n'est pas majoré par $f(n-1)$, et donc l'ensemble des éléments de P strictement supérieurs à $f(n-1)$ est une partie non vide de \mathbb{N} . On peut donc prendre pour $f(n)$ son plus petit élément, qui vérifie donc $f(n) > f(n-1)$.

Par construction, la fonction f est strictement croissante, donc injective.

Montrons par l'absurde qu'elle est surjective. Si elle ne l'est pas, l'ensemble $P \setminus f(\mathbb{N})$ est une partie non vide de \mathbb{N} et admet donc un plus petit élément a , différent de a_0 puisque $a_0 = f(0)$. L'ensemble des éléments de P strictement inférieurs à a est une partie non vide et majorée de \mathbb{N} . Elle admet donc un plus grand élément b , qui est alors l'image d'un certain entier n puisque a est le plus petit élément de P n'ayant pas d'antécédent. Par construction, $f(n+1)$ est le plus petit élément de P strictement plus grand que b , c'est-à-dire a . D'où la contradiction.

Donc f est une bijection croissante de \mathbb{N} sur P .

Unicité. De même que pour la proposition précédente, si f et g sont deux telles bijections, la composée $f^{-1} \circ g$ est une bijection strictement croissante de \mathbb{N} sur \mathbb{N} ainsi que sa réciproque. D'après le lemme, on a alors $f^{-1} \circ g = \text{Id}_{\mathbb{N}}$, c'est-à-dire $f = g$. \square

Remarques

- Les deux propositions précédentes peuvent encore s'énoncer :
 - toute partie finie non vide de \mathbb{N} s'écrit de façon unique sous la forme $\{x_1, x_2, \dots, x_n\}$ avec $x_1 < x_2 < \dots < x_n$,
 - toute partie infinie de \mathbb{N} s'écrit de façon unique sous la forme $\{x_n \mid n \in \mathbb{N}\}$ où $(x_n)_{n \in \mathbb{N}}$ est une suite strictement croissante.

- Ces deux derniers résultats montrent que toute famille indexée par une partie de \mathbb{N} peut, quitte à renommer ses éléments (sans changer leur ordre), être indexée par \mathbb{N} ou par $\llbracket 1, n \rrbracket$ avec $n \in \mathbb{N}$.

L'étude d'une telle famille indexée par une partie infinie de \mathbb{N} se ramène donc à l'étude d'une suite.

Réunion d'ensembles finis

Proposition 10

Si A et B sont deux ensembles finis disjoints, alors $A \cup B$ est fini et :

$$\text{card}(A \cup B) = \text{card } A + \text{card } B.$$

Démonstration Soient m et n les cardinaux respectifs des ensembles A et B .

Étant données une bijection f de A dans $\llbracket 1, m \rrbracket$ et une bijection g de B dans $\llbracket m+1, m+n \rrbracket$ (cf. exemple 3. de la page 1050), on définit l'application h de $A \cup B$ dans $\llbracket 1, m+n \rrbracket$ par :

$$\forall x \in A, h(x) = f(x)$$

$$\forall x \in B, h(x) = g(x).$$

Cette application h est bien définie car A et B sont disjoints ; c'est une bijection dont la réciproque est donnée par :

$$\forall k \in \llbracket 1, m \rrbracket, h'(k) = f^{-1}(k)$$

$$\forall k \in \llbracket m+1, m+n \rrbracket, h'(k) = g^{-1}(k).$$

Donc $A \cup B$ est un ensemble fini de cardinal $m+n$. □

Exemple Soit E un ensemble fini de cardinal n . Si $a \notin E$, l'ensemble $E \cup \{a\}$ est fini de cardinal $n+1$.

Corollaire 11

Si A est une partie d'un ensemble fini E , alors :

$$\text{card}(\complement_E A) = \text{card } E - \text{card } A.$$

Démonstration Les ensembles A et $\complement_E A$ sont finis d'après le théorème 5 de la page 1051.

De plus, ils sont disjoints et $E = A \cup (\complement_E A)$. On a donc :

$$\text{card } E = \text{card } A + \text{card}(\complement_E A)$$

ce qui prouve le résultat. □

Par une récurrence immédiate, on généralise la proposition 10 de la page précédente :

Proposition 12

Si $(A_k)_{1 \leq k \leq p}$ est une famille de p ensembles finis deux à deux disjoints, alors $\bigcup_{k=1}^p A_k$ est un ensemble fini et :

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

Proposition 13

Si A et B sont deux ensembles finis, alors $A \cup B$ est fini et :

$$\text{card}(A \cup B) = \text{card } A + \text{card } B - \text{card}(A \cap B).$$

Démonstration On a les égalités :

$$A \cup B = (A \setminus B) \cup B \quad \text{et} \quad (A \setminus B) \cap B = \emptyset$$

ce qui prouve que $A \cup B$ est fini et que l'on a :

$$\text{card}(A \cup B) = \text{card}(A \setminus B) + \text{card } B. \quad (a)$$

De même, on a :

$$\text{card}(A \setminus B) + \text{card}(A \cap B) = \text{card } A \quad (b)$$

puisque :

$$(A \setminus B) \cup (A \cap B) = A \quad \text{et} \quad (A \setminus B) \cap (A \cap B) = \emptyset.$$

En ajoutant membre à membre les égalités (a) et (b) puis en simplifiant par $\text{card}(A \setminus B)$, on obtient :

$$\text{card}(A \cup B) + \text{card}(A \cap B) = \text{card } B + \text{card } A. \quad \square$$

Exemple Soient A , B et C trois ensembles finis. On a la relation :

$$\begin{aligned} \text{card}(A \cup B \cup C) &= \text{card } A + \text{card } B + \text{card } C \\ &\quad - \text{card}(A \cap B) - \text{card}(A \cap C) - \text{card}(B \cap C) \\ &\quad + \text{card}(A \cap B \cap C). \end{aligned}$$

En effet, d'après la proposition précédente, on a :

$$\begin{aligned} \text{card}(A \cup (B \cup C)) &= \text{card } A + \text{card}(B \cup C) - \text{card}(A \cap (B \cup C)) \\ \text{card}(B \cup C) &= \text{card } B + \text{card } C - \text{card}(B \cap C). \end{aligned}$$

Comme $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, on obtient :

$$\text{card}(A \cap (B \cup C)) = \text{card}(A \cap B) + \text{card}(A \cap C) - \text{card}(A \cap B \cap C)$$

ce qui prouve la relation annoncée.

Produit d'ensembles finis

Proposition 14

Si A et B sont deux ensembles finis, alors $A \times B$ est fini et :

$$\text{card}(A \times B) = \text{card } A \text{ card } B.$$

Démonstration Le résultat est évident si A est vide ; supposons donc $A \neq \emptyset$. Si p est le cardinal de l'ensemble A , on peut écrire A en extension :

$$A = \{a_1, a_2, \dots, a_p\}.$$

L'ensemble $A \times B$ s'écrit alors :

$$A \times B = \bigcup_{k=1}^p \{a_k\} \times B.$$

Chaque ensemble $\{a_k\} \times B$ est en bijection avec B par l'application $b \mapsto (a_k, b)$, et donc $A \times B$ est la réunion de p ensembles finis de même cardinal que B et disjoints deux à deux. Par suite, $A \times B$ est fini et :

$$\text{card}(A \times B) = p \text{ card } B = \text{card } A \text{ card } B.$$

□

Corollaire 15

Soient $p \in \mathbb{N}^*$ et A un ensemble fini. L'ensemble A^p est fini et :

$$\text{card}(A^p) = (\text{card } A)^p.$$

Démonstration Récurrence sur l'entier p en utilisant le résultat précédent.

□

Applications d'un ensemble fini dans un ensemble fini

Proposition 16

Soient E et F deux ensembles finis et f une application de E dans F . On a :

- (1) $\text{card } f(E) \leq \text{card } E$,
- (2) L'application f est injective si, et seulement si, $\text{card } f(E) = \text{card } E$.

Démonstration

- (1) Pour tout élément y de $f(E)$ choisissons un élément x de E tel que $y = f(x)$. Soit A la partie de E constituée par les éléments x ainsi sélectionnés.

L'application :

$$\begin{array}{ccc} A & \longrightarrow & f(E) \\ x & \longmapsto & f(x) \end{array}$$

est bijective puisque tout élément de $f(E)$ admet dans A un antécédent et un seul. Par suite les ensembles A et $f(E)$ ont même cardinal.

Comme l'ensemble A est une partie de E , son cardinal est inférieur au cardinal de E , ce qui implique :

$$\text{card}(f(E)) = \text{card } A \leq \text{card } E.$$

- (2) ▶ Si f est injective, elle induit une bijection de E dans $f(E)$ et on a donc $\text{card } E = \text{card}(f(E))$.
- ▶ Supposons $\text{card}(f(E)) = \text{card } E$. En reprenant les notations de (1), on obtient alors les égalités :

$$\text{card } A = \text{card}(f(E)) = \text{card } E.$$

La partie A de E a même cardinal que E , donc $A = E$. Tout élément de $f(E)$ admet donc un unique antécédent dans E par f , ce qui prouve que f est injective. □

Remarques

- Soient E et F deux ensembles finis et f une application de E dans F . Le théorème 5 de la page 1051 donne immédiatement les résultats suivants, symétriques de ceux énoncés dans la proposition précédente :
 - ▶ $\text{card}(f(E)) \leq \text{card } F$ car $f(E)$ est une partie de F ;
 - ▶ si f est surjective, alors $\text{card } F \leq \text{card } E$;
 - ▶ l'application f est surjective si, et seulement si, $\text{card}(f(E)) = \text{card } F$, puisque cette égalité de cardinaux est équivalente à $f(E) = F$.
- L'ensemble $E = \{x_1, x_2, \dots, x_n\}$ est un ensemble fini de cardinal au plus n , puisque l'application $f : i \mapsto x_i$ est une surjection de $\llbracket 1, n \rrbracket$ sur E . Si, de plus $\text{card } E = n$, alors f est injective d'après la proposition précédente, et donc les x_i sont distincts deux à deux.

Théorème 17

Soient E et F deux ensembles finis de même cardinal et f une application de E dans F . Les propriétés suivantes sont équivalentes :

- (i) l'application f est injective,
- (ii) l'application f est surjective,
- (iii) l'application f est bijective.

Démonstration D'après les résultats précédents, on a les équivalences :

$$f \text{ injective} \iff \text{card}(f(E)) = \text{card } E$$

$$f \text{ surjective} \iff \text{card}(f(E)) = \text{card } F$$

Comme $\text{card } E = \text{card } F$, les propriétés (i) et (ii) sont équivalentes. D'où l'équivalence des propriétés (i), (ii) et (iii). □

3. Dénombrement

Dans toute cette section, p et n désignent des entiers naturels. Pour l'instant et sauf mention du contraire, ils sont supposés non nuls.

3.1 Applications d'un ensemble fini dans un ensemble fini

Nombre de p -listes d'un ensemble fini

Proposition 18

Si E est un ensemble fini de cardinal n , le nombre de p -listes d'éléments de E est n^p .

Démonstration En effet, $\text{card}(E^p) = (\text{card } E)^p = n^p$. □

Nombre d'applications d'un ensemble fini dans un ensemble fini

Soient E et F des ensembles de cardinaux respectifs p et n . L'ensemble des applications de E dans F est noté F^E ou $\mathcal{F}(E, F)$.

Proposition 19

Si $E = \{\alpha_1, \alpha_2, \dots, \alpha_p\}$, l'application Φ :

$$\begin{array}{rcl} F^E & \longrightarrow & F^p \\ u & \longmapsto & (u(\alpha_1), u(\alpha_2), \dots, u(\alpha_p)) \end{array}$$

est une bijection.

Démonstration Si (b_1, b_2, \dots, b_p) est un élément quelconque de F^p , il existe une unique application u de E dans F telle que :

$$\forall k \in [1, p], u(\alpha_k) = b_k,$$

ce qui exprime que l'élément $(b_1, b_2, \dots, b_p) \in F^p$ admet un unique antécédent par Φ .

L'application Φ est donc une bijection. □

Corollaire 20

Si $\text{card } E = p$ et $\text{card } F = n$, alors $\text{card } \mathcal{F}(E, F) = n^p$.

Remarques

- La notation F^E est donc bien adaptée pour désigner l'ensemble des applications de E dans F , puisque le résultat précédent s'écrit :

$$\text{card}(F^E) = (\text{card } F)^{\text{card } E} \quad (*)$$

- Si E est vide ($p = 0$ et n quelconque), il y a une seule application de E dans F : celle dont le graphe est vide. La relation (*) reste vraie car on a alors $n^0 = 1$ (même si $n = 0$).
- Si F est vide et E non vide ($p > 0$ et $n = 0$), il n'y a aucune application de E dans F , car par une application, l'image d'une partie non vide est non vide. La relation (*) reste encore vraie car on a alors $0^p = 0$.

Nombre d'injections

Proposition 21

Étant donnés deux entiers n et p strictement positifs et un ensemble F de cardinal n , le nombre de p listes d'éléments de F distincts deux à deux est :

$$\underbrace{n(n-1)\dots(n-p+1)}_{p \text{ termes}}.$$

Il est en particulier nul si $p > n$.

Démonstration Notons A_n^p ce nombre et démontrons, par récurrence sur p , la propriété H_p définie par :

$$\forall n \in \mathbb{N}^*, A_n^p = n(n-1)\dots(n-p+1).$$

- H_1 est vraie car si F possède n éléments, il y a évidemment n listes de longueur 1 dans F , et elles sont évidemment constituées d'éléments distincts deux à deux.
- Supposons H_p pour $p \geq 1$ et prouvons H_{p+1} . Soient n un entier naturel fixé quelconque et F un ensemble de cardinal n .
 - Si $n = 1$, il n'y a aucune $(p+1)$ -liste de F , puisque $p+1 \geq 2$, et on a alors $A_1^{p+1} = 0 = n(n-1)\dots(n-p)$.

- Sinon, une $(p+1)$ -liste $(a_0, a_1, \dots, a_p) \in F^{p+1}$ est déterminée par son premier terme a_0 et la p -liste (a_1, a_2, \dots, a_p) .

Ces éléments sont distincts deux à deux si, et seulement si, (a_1, a_2, \dots, a_p) est une p -liste d'éléments distincts de $F \setminus \{a_0\}$. Il y a n façons de choisir a_0 et, d'après l'hypothèse de récurrence H_p , pour chaque choix de a_0 , il y a :

$$A_{n-1}^p = (n-1)\dots(n-p+1)(n-p)$$

manières de choisir (a_1, a_2, \dots, a_p) .

On a donc :

$$A_n^{p+1} = n((n-1)\dots(n-p+1)(n-p)).$$

Ainsi H_{p+1} est vraie, ce qui termine la démonstration par récurrence. □

Remarque Soient E et F deux ensembles non vides de cardinaux respectifs p et n . L'application Φ de la proposition 19 de la page 1059 induit une bijection de l'ensemble des injections de E dans F sur l'ensemble des p -listes d'éléments de F distincts deux à deux.

Le nombre d'applications injectives de E dans F est donc aussi $n(n - 1) \dots (n - p + 1)$.

Nombre de permutations

On rappelle qu'une permutation d'un ensemble E est une bijection de E dans lui-même.

Proposition 22

Si $\text{card } E = n$, alors le nombre de permutations de E vaut :

$$n \times (n - 1) \times \dots \times 2 \times 1.$$

On le note $n!$ (lire « factorielle n »).

Démonstration Comme E est un ensemble fini, une application de E dans E est bijective si, et seulement si, elle est injective ; le nombre de permutations de E est donc le nombre d'applications injectives de E dans E , d'où le résultat. \square

Remarques

- Plus généralement, $n!$ est le nombre de bijections d'un ensemble de cardinal n dans un autre ensemble de cardinal n .
- Il n'y a pas de bijection de E dans F si $\text{card } E \neq \text{card } F$.

Convention On convient que $0! = 1$ d'où :

$$\forall n \in \mathbb{N}, (n + 1)! = (n + 1)n!.$$

3.2 Nombre de parties à p éléments

Parties d'un ensemble fini

Définitions – Notations Soit E un ensemble fini de cardinal n .

- On désigne par $\mathcal{P}_p(E)$ l'ensemble des parties à p éléments de E .
- Le nombre de parties de E à p éléments ne dépend que de n et de p ; on le note $\binom{n}{p}$.
- On trouve aussi la notation C_n^p à la place de $\binom{n}{p}$.

Proposition 23

Le nombre de parties de E à p éléments est :

$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p!}$$

le numérateur étant par convention égal à 1 si $p = 0$.

Démonstration

- Pour $p = 0$, le résultat est vrai par convention.
- Pour $p > n$, l'égalité est encore vérifiée puisque les deux membres sont nuls.
- Pour $1 \leq p \leq n$, comptons le nombre de p -listes d'éléments de E distincts deux à deux : il y en a $n(n-1)\dots(n-p+1)$.

D'autre part, se donner une telle liste revient à se donner une partie de E à p éléments (soit $\binom{n}{p}$ possibilités) puis d'ordonner ces éléments, c'est-à-dire de choisir une permutation de cette partie ($p!$ possibilités).

On a ainsi $n(n-1)\dots(n-p+1) = p! \binom{n}{p}$. □

Corollaire 24

Étant donnés deux entiers naturels n et p , on a :

- si $p \leq n$ alors $\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{n(n-1)\dots(n-p+1)}{p!}$,
- si $p > n$ alors $\binom{n}{p} = 0$.

Remarque Le cas $p = 0$ vient de la convention $0! = 1$.

Formules fondamentales**Proposition 25**

Étant donnés deux entiers naturels n et p , on a :

- $\binom{n}{p} = \binom{n}{n-p}$ si $p \leq n$,
- $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ si $n \geq 1$ et $p \geq 1$. **(Relation de Pascal)**

Démonstration On peut vérifier ces relations par le calcul en utilisant l'expression explicite des $\binom{n}{p}$, mais nous allons les démontrer par des méthodes de dénombrement en considérant un ensemble E à n éléments.

- L'involution de $\mathcal{P}(E)$, qui à toute partie de E associe son complémentaire, induit une bijection de $\mathcal{P}_p(E)$ sur $\mathcal{P}_{n-p}(E)$; ce qui entraîne la première relation.
- Soit a un élément de E fixé. Les $\binom{n}{p}$ parties de E à p éléments se partagent en deux catégories disjointes :
 - celles qui contiennent a : ce sont les parties de la forme $\{a\} \cup X$, où X est une partie à $p-1$ éléments de $E \setminus \{a\}$; leur nombre est donc $\binom{n-1}{p-1}$.
 - celles qui ne contiennent pas a : ce sont les parties à p éléments de $E \setminus \{a\}$; leur nombre est donc $\binom{n-1}{p}$.

D'où la relation de Pascal. □

Triangle de Pascal

La relation $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ permet de construire le triangle de Pascal, dont les premières lignes sont :

$$\begin{array}{ccccccc}
 & & 1 & & & & \\
 & 1 & & 1 & & & \\
 & 1 & & 2 & & 1 & \\
 & 1 & & 3 & & 3 & & 1 \\
 & 1 & & 4 & & 6 & & 4 & & 1 \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & \vdots & & & & \boxed{\binom{n-1}{p-1}} & & \boxed{\binom{n-1}{p}} & & & & \\
 & & & & & & & & & & & \ddots
 \end{array}$$

La formule :

$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p(p-1)\dots 1} \quad (*)$$

est en général la plus rapide pour calculer $\binom{n}{p}$ (ne pas oublier de changer p en $n-p$ si p est strictement supérieur à $n/2$).

Pour limiter la taille des nombres entiers à manipuler, on peut aussi utiliser la proposition suivante qui permet de calculer $\binom{n}{p}$ par récurrence sur p .

Proposition 26

Étant donnés deux entiers naturels n et p tels que $n \geq p \geq 1$, on a :

$$\binom{n}{p} = \frac{n}{p} \binom{n-1}{p-1} \quad \text{et} \quad \binom{n}{p} = \frac{n-p+1}{p} \binom{n}{p-1}.$$

Démonstration Il suffit, dans la formule (*), de factoriser p au dénominateur et n ou $n-p+1$ au numérateur. \square

D'où l'algorithme :

DONNÉES: deux entiers n et p tels que $0 \leq p \leq n$.

VARIABLES: k (l'indice de boucle), C (le résultat).

- $C \leftarrow 1$
- Pour k allant de 1 jusqu'à p :
 - $C \leftarrow (n-k+1) * C$
 - $C \leftarrow C/k$ (* division exacte *)

RÉSULTAT: C .

Proposition 27

Si E est un ensemble fini à n éléments, l'ensemble $\mathcal{P}(E)$ des parties de E est fini et a pour cardinal 2^n .

On a ainsi :

$$\sum_{p=0}^n \binom{n}{p} = 2^n.$$

Démonstration Ce résultat peut se prouver par récurrence en utilisant le même type de raisonnement que pour la démonstration de la relation de Pascal.

Il peut aussi être vu comme une conséquence de la formule du binôme de Newton (voir page 1081) puisque :

$$(1+1)^n = \sum_{p=0}^n \binom{n}{p} 1^p 1^{n-p}.$$

\square

Chapitre 37

Structures algébriques usuelles

Le but de ce chapitre est de définir le vocabulaire élémentaire sur les structures algébriques usuelles (groupes, anneaux, corps, espaces vectoriels). Ces structures sont une formalisation des propriétés classiques des ensembles \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} et \mathbb{R}^n munis de leurs opérations usuelles $+$ et \times , propriétés que nous supposerons connues.

1. Lois de composition interne

1.1 Généralités

Définition

Définition 1

Soit E un ensemble. On appelle *loi de composition interne* sur E , une application de $E \times E$ dans E :

$$\begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x * y \end{array}$$

Exemples

1. L'addition, la multiplication sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .

La soustraction sur \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} .

La division sur \mathbb{Q}^* , \mathbb{R}^* , \mathbb{R}_+^* et \mathbb{C}^* .

2. Si E est un ensemble, on a sur $\mathcal{P}(E)$ les lois de composition interne suivantes :

- l'intersection notée \cap ,
- la réunion notée \cup .

3. La composition des applications notée \circ est une loi de composition interne sur :

- A^A , l'ensemble des applications de A dans A ,
- $S(A)$, l'ensemble des permutations de A , c'est-à-dire des bijections de A dans A .

Propriétés des lois de composition interne

Soit $*$ une loi de composition interne sur un ensemble E .

Définition 2

On dit que $*$ est :

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

Exemples

1. Sur \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} , l'addition et la multiplication sont associatives et commutatives.
2. Sur $\mathcal{P}(E)$, les lois \cap et \cup sont associatives et commutatives.
3. Sur \mathbb{R} , la soustraction n'est ni commutative, ni associative.
4. Sur E^E , la composition des applications est associative, mais non commutative si E a au moins deux éléments.
5. Le produit vectoriel dans l'espace euclidien n'est ni commutatif ni associatif.

Remarque La notation additive $+$ est utilisée exclusivement pour une loi commutative.

Définition 3

Soient \oplus et \otimes deux lois de composition interne sur E . On dit que \otimes est *distributive* par rapport à \oplus si pour tous x , y et z de E , on a :

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \quad \text{et} \quad (x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z).$$

Exemples

1. Sur \mathbb{R} , la multiplication est distributive par rapport à l'addition.
2. Sur $\mathcal{P}(E)$, la réunion et l'intersection sont chacune distributive par rapport à l'autre.

Dans toute la suite de ce chapitre, nous ne considérons que des lois de composition interne associatives.

Propriétés des éléments

Soit $*$ une loi de composition interne sur un ensemble E .

Définition 4

On dit que $a \in E$ est *régulier* ou *simplifiable* pour $*$ si pour tout $(x, y) \in E^2$, on a :

$$a * x = a * y \implies x = y \quad \text{et} \quad x * a = y * a \implies x = y.$$

Exemples

1. Dans \mathbb{N} :

- tous les éléments sont réguliers pour l'addition,
- tous les éléments non nuls sont réguliers pour la multiplication.

2. Dans $\mathcal{P}(E)$, seul E est régulier pour l'intersection.

Définition 5

On dit que $e \in E$ est *élément neutre* pour $*$ si :

$$\forall x \in E, x * e = e * x = x.$$

Un tel élément, quand il existe, est unique.

Démonstration de l'unicité. Si e et e' sont deux éléments neutres, alors $e = e * e' = e'$. \square

Exemples

1. Sur \mathbb{R} :

- 0 est élément neutre pour l'addition,
- 1 est élément neutre pour la multiplication.

2. Id_E est élément neutre pour la composition sur E^E .

3. E est élément neutre pour l'intersection sur $\mathcal{P}(E)$.

4. \mathbb{N}^* n'a pas d'élément neutre pour l'addition.

Remarque L'élément neutre est toujours régulier.

Définition 6

Étant donné un ensemble E muni d'une loi associative $*$ et possédant un élément neutre e , un élément x de E est *symétrisable* ou *inversible* si :

$$\exists y \in E : x * y = y * x = e.$$

Il y a alors unicité d'un tel élément y que l'on appelle le *symétrique* de x .

Démonstration de l'unicité. Soient y et z de E tels que $x * y = z * x = e$. Alors, par associativité de la loi :

$$z = z * e = z * (x * y) = (z * x) * y = e * y = y.$$

□

Remarque Le symétrique d'un élément x se note :

- x^{-1} pour une loi notée multiplicativement et s'appelle *inverse* de x .
- $-x$ pour une loi notée additivement et s'appelle *opposé* de x .

Exemples

1. Pour l'addition dans \mathbb{Z} , \mathbb{Q} ou \mathbb{R} , tout élément admet un opposé.
2. Pour la multiplication de \mathbb{R} , tout élément non nul admet un inverse.
3. L'élément neutre de $(E, *)$ est inversible pour $*$ et il est son propre symétrique.
4. Dans (E^E, \bullet) , les éléments inversibles sont les bijections, qui admettent pour symétrique leur bijection réciproque.
5. Dans $\mathcal{P}(E)$, seul l'élément neutre E admet un symétrique pour \cap .

Proposition 1

Si a et b sont deux éléments inversibles de $(E, *)$, alors $a * b$ est inversible et :

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

Démonstration Il suffit de vérifier :

$$(a * b) * (b^{-1} * a^{-1}) = e \quad \text{et} \quad (b^{-1} * a^{-1}) * (a * b) = e,$$

ce qui découle de l'associativité de $*$.

□

Exemples

1. Si f et g sont deux bijections d'un ensemble E dans lui-même, alors $f \circ g$ est aussi bijective et sa réciproque est $g^{-1} \circ f^{-1}$.
2. Si A et B sont deux matrices inversibles, le produit AB est inversible et $(AB)^{-1} = B^{-1}A^{-1}$.

Proposition 2

Soit E un ensemble muni d'une loi associative $*$ et possédant un élément neutre e . Tout élément inversible de E est régulier.

Démonstration Soit x inversible et y son symétrique. On a :

$$y * (x * a) = (y * x) * a = e * a = a$$

et de même $y * (x * b) = b$.

On en déduit donc que si $x * a = x * b$, alors $a = b$.

On démontre de même l'implication $a * x = b * x \implies a = b$. \square

► **Attention** Un élément régulier n'est pas forcément inversible car, par exemple, dans $(\mathbb{N}, +)$, tout élément est régulier, alors que seul 0 est inversible.

1.2 Itérés d'un élément

Soit E un ensemble muni d'une loi associative $*$ et possédant un élément neutre e . Pour $x \in E$ et $n \in \mathbb{N}^*$, l'élément :

$$x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$$

appelé itéré $n^{\text{ème}}$ de x est défini par récurrence :

$$x^0 = e \quad \text{et} \quad x^{n+1} = x * (x^n) \quad \text{si } n \geq 0.$$

Si $x \in E$ est inversible, alors, pour tout entier naturel n , l'élément x^n est inversible et son inverse est $(x^{-1})^n$ que l'on note x^{-n} .

Proposition 3

Étant donné $x \in E$, on a pour tout $(p, q) \in \mathbb{N}^2$:

$$x^{p+q} = x^p * x^q \quad \text{et} \quad (x^p)^q = x^{pq}.$$

Ces relations sont vraies pour $(p, q) \in \mathbb{Z}^2$ si x est inversible.

Démonstration Ces propriétés se démontrent aisément par récurrence si p et q sont des entiers naturels.

Par passage à l'inverse, on en déduit les résultats pour p et q entiers relatifs quelconques si x est inversible. \square

1.3 Produit de n éléments

Soit E un ensemble muni d'une loi associative $*$ et possédant un élément neutre e .

Étant donnée une suite $(x_p)_{p \in [1..n]}$ d'éléments de E , le produit :

$$x_1 * x_2 * \cdots * x_n = \prod_{1 \leq p \leq n} x_p$$

est défini par récurrence :

$$\prod_{1 \leq p \leq n} x_p = \begin{cases} e & \text{si } n = 0 \\ \left(\prod_{1 \leq p \leq n-1} x_p \right) * x_n & \text{si } n \geq 1. \end{cases}$$

Ce produit est aussi noté $\prod_{p=1}^n x_p$.

Lorsque tous les x_i sont inversibles, le produit $x_1 * x_2 * \dots * x_n$ est inversible, d'inverse $x_n^{-1} * \dots * x_2^{-1} * x_1^{-1}$.

Cas des lois commutatives

Lorsque la loi $*$ est commutative, on peut effectuer le produit $x_1 * x_2 * \dots * x_n$ dans n'importe quel ordre ; on peut alors le noter $\prod_{p \in [1, n]} x_p$.

Plus généralement, si I est un ensemble fini, et $(x_i)_{i \in I}$ une famille indexée par I d'éléments de E , on note $\prod_{i \in I} x_i$ le produit (dans n'importe quel ordre) des éléments de la famille. Par définition, ce produit est égal à e si I est vide.

Avec ces définitions, si J et K sont deux ensembles finis disjoints, on a :

$$\left(\prod_{i \in J} x_i \right) * \left(\prod_{i \in K} x_i \right) = \prod_{i \in J \cup K} x_i.$$

1.4 Notation additive

Lorsque la loi est commutative et qu'elle est notée additivement :

- l'élément neutre est noté 0 ,
- l'itéré $n^{\text{ème}}$ d'un élément x s'écrit $n.x$ ou $n x$ au lieu de x^n pour $n \in \mathbb{N}$ (ou $n \in \mathbb{Z}$ si x est inversible).

Les résultats de la proposition 3 de la page précédente s'écrivent alors, pour $(p, q) \in \mathbb{N}^2$ (ou $(p, q) \in \mathbb{Z}^2$ si x admet un opposé) :

$$(p + q).x = p.x + q.x \quad \text{et} \quad p.(q.x) = (pq).x.$$

La somme de n éléments x_1, x_2, \dots, x_n est notée :

$$\sum_{1 \leq p \leq n} x_p, \quad \sum_{p \in [1, n]} x_p \quad \text{ou} \quad \sum_{p=1}^n x_p$$

et vérifie donc :

$$\sum_{1 \leq p \leq n} x_p = \begin{cases} 0 & \text{si } n = 0 \\ \left(\sum_{1 \leq p \leq n-1} x_p \right) + x_n & \text{si } n \geq 1. \end{cases}$$

Plus généralement, si I est un ensemble fini, et $(x_i)_{i \in I}$ une famille d'éléments de E indexée par I , on note $\sum_{i \in I} x_i$ la somme (dans n'importe quel ordre) des éléments de la famille. Par définition, cette somme est nulle si I est vide.

1.5 Construction de lois

Partie stable — loi induite

Définition 7

Soient E muni d'une loi de composition interne $*$ et F une partie de E .

On dit que F est *stable* par $*$ si :

$$\forall (x,y) \in F^2, x * y \in F.$$

La loi de composition interne alors définie sur F par :

$$\begin{array}{ccc} F^2 & \longrightarrow & F \\ (x,y) & \longmapsto & x * y \end{array}$$

est appelée *loi induite* par $*$ sur F .

Exemples

1. Dans \mathbb{C} , l'ensemble \mathcal{U} des nombres complexes de module 1 est stable par \times .
2. \mathbb{N} est stable par l'addition et la multiplication de \mathbb{Z} .

Loi produit

Définition 8

Soient $(E, *)$ et $(F, *)$ deux ensembles munis de lois de composition interne. On définit la *loi produit* sur $E \times F$ en posant :

$$(x, y) * (x', y') = (x * x', y * y').$$

Exemples

1. On définit ainsi une addition sur \mathbb{R}^2 en posant :

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

2. Soit \mathcal{U} l'ensemble des nombres complexes de module 1 muni de la multiplication des nombres complexes, et \mathbb{R}_+^* muni de la multiplication. La loi produit sur $\mathbb{R}_+^* \times \mathcal{U}$ est définie par :

$$(r, u) \cdot (r', u') = (rr', uu').$$

3. Si \mathbb{R}_+^* est muni de la multiplication et \mathbb{R} de l'addition, la loi produit sur $\mathbb{R}_+^* \times \mathbb{R}$ est définie par :

$$(r, \theta) * (r', \theta') = (rr', \theta + \theta').$$

On peut généraliser ce procédé de construction à un produit quelconque d'ensembles munis de lois de composition interne, ce qui permet, par exemple, de définir une addition sur \mathbb{R}^n :

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

Lois sur E^X

Exemple Si f et g sont des fonctions définies sur un même ensemble X et à valeurs dans \mathbb{R} , on définit leur somme $f + g$ et leur produit $f \cdot g$ par :

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (f \cdot g)(x) = f(x)g(x).$$

- L'élément neutre pour l'addition est l'application nulle.
- Tout élément f admet pour opposé l'application $(-f)$: $x \mapsto -f(x)$.
- L'élément neutre pour la multiplication est l'application constante égale à 1.
- Une fonction f est inversible pour la multiplication si, et seulement si, elle ne s'annule pas ; son inverse est alors :

$$\frac{1}{f} : x \mapsto \frac{1}{f(x)}.$$

Plus généralement :

Définition 9

Soient E un ensemble muni d'une loi de composition interne $*$ et X un ensemble. On définit sur E^X la loi de composition interne, notée encore $*$, par :

$$\forall x \in X, (f * g)(x) = f(x) * g(x).$$

Les propriétés (associativité, commutativité,...) de la loi ainsi définie sur E^X sont les mêmes que celles de la loi correspondante sur E . Par exemple si E a un élément neutre e pour $*$, alors E^X possède un élément neutre pour $*$ qui est :

$$\begin{array}{ccc} X & \longrightarrow & E \\ x & \longmapsto & e. \end{array}$$

1.6 Morphismes

Définition 10

Soient E et E' deux ensembles, $*$ une loi de composition interne sur E , et $*'$ une loi de composition interne sur E' .

On dit qu'une application f de E dans E' est un *morphisme* de $(E, *)$ dans $(E', *')$ si :

$$\forall (x, y) \in E^2, f(x * y) = f(x) *' f(y).$$

- Un morphisme bijectif est appelé *isomorphisme*.
- Un morphisme de $(E, *)$ dans lui-même est appelé *endomorphisme* de E .
- Un endomorphisme bijectif est appelé *automorphisme*.

Exemples

1. La fonction logarithme est un isomorphisme de (\mathbb{R}_+^*, \times) sur $(\mathbb{R}, +)$.
Sa réciproque, l'exponentielle, est un isomorphisme de $(\mathbb{R}, +)$ sur (\mathbb{R}_+^*, \times) .
2. Si $*$ est une loi de composition interne sur E , l'identité est un automorphisme de $(E, *)$.
3. Soit $x \in \mathbb{Z}$.
 - L'application $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & nx \end{array}$ est un endomorphisme de $(\mathbb{Z}, +)$.
 - L'application $\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & x^n \end{array}$ est un morphisme de $(\mathbb{N}, +)$ dans (\mathbb{Z}, \times) .
4. La règle $x^p * x^q = x^{p+q}$ de calcul sur les itérés peut s'énoncer en disant que l'application :

$$\begin{array}{ccc} \mathbb{N} & \longrightarrow & E \\ n & \longmapsto & x^n \end{array}$$

est un morphisme de $(\mathbb{N}, +)$ dans $(E, *)$.

Proposition 4

La composée de deux morphismes est un morphisme.

Démonstration Soient $(E, *) \xrightarrow{f} (F, *) \xrightarrow{g} (G, *)$ deux morphismes. (Nous utilisons pour simplifier la même notation pour les lois de E , F et G .)

Pour $(x, y) \in E^2$, on a :

$$\begin{aligned}(g \circ f)(x * y) &= g(f(x * y)) \\&= g(f(x) * f(y)) \\&= g(f(x)) * g(f(y)) \\&= (g \circ f)(x) * (g \circ f)(y).\end{aligned}$$

□

Proposition 5

La réciproque d'un isomorphisme est un isomorphisme.

Démonstration Soient f un isomorphisme de $(E, *)$ dans $(F, *)$ et $(x, y) \in F^2$. On a :

$$f(f^{-1}(x) * f^{-1}(y)) = f(f^{-1}(x)) * f(f^{-1}(y)) = x * y = f(f^{-1}(x * y))$$

et, puisque f est injective, on en déduit $f^{-1}(x) * f^{-1}(y) = f^{-1}(x * y)$. □

2. Groupes

2.1 Définitions, exemples

Définition 11

Étant donné un ensemble G , on dit que $(G, *)$ est un *groupe* si :

- $*$ est une loi de composition interne associative sur G ,
- $(G, *)$ possède un élément neutre,
- tout élément de G possède un symétrique dans G .

Si de plus $*$ est commutative, on dit que G est un groupe *commutatif* (ou *abélien*).

Remarques

- Par abus de langage et lorsqu'il n'y a aucune ambiguïté, on dit souvent « soit G un groupe... » sans préciser la loi.
- Dans un groupe, tout élément est régulier, puisqu'inversible.

Exemples

1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, (\mathbb{R}^*, \times) , (\mathbb{R}_+^*, \times) , $(\mathbb{C}, +)$, (\mathbb{C}^*, \times) sont des groupes commutatifs.
2. $(\mathbb{N}, +)$ et (\mathbb{R}, \times) ne sont pas des groupes puisqu'ils ont des éléments non inversibles.

3. L'ensemble $(\mathcal{S}(E), \circ)$ des permutations de E est un groupe qui n'est pas commutatif si E a au moins trois éléments.
4. (E^E, \circ) n'est pas un groupe si E a au moins 2 éléments, puisqu'une application constante n'est pas inversible.
5. Si G est un groupe et A un ensemble non vide, alors G^A est un groupe pour la loi déduite de celle de G . Il est abélien si, et seulement si, G est abélien.
L'inverse de $f \in G^A$ est l'application $x \mapsto (f(x))^{-1}$.
6. Si G et H sont des groupes, alors $G \times H$ muni de la loi produit est un groupe.
Le neutre de $G \times H$ est (e, e') où e est le neutre de G et e' celui de H .
Le symétrique de $(x, y) \in G \times H$ est (x^{-1}, y^{-1}) .

2.2 Sous-groupes

Définition 12

Soit G un groupe. Une partie H de G est un *sous-groupe* de G si elle est stable par produit et passage au symétrique, et si elle contient l'élément neutre de G .

Exemples

1. \mathbb{Z} est un sous-groupe de $(\mathbb{R}, +)$.
2. \mathbb{R}_+^* est un sous-groupe de (\mathbb{R}^*, \times) mais pas de $(\mathbb{R}, +)$.
3. Dans le groupe (\mathbb{C}^*, \times) , l'ensemble \mathcal{U} des éléments de module 1 et l'ensemble \mathcal{U}_n des racines n ^{èmes} de l'unité, sont des sous-groupes de \mathbb{C}^* .
4. G et $\{e\}$ sont des sous-groupes du groupe G . On les appelle *sous-groupe triviaux* de G .

Proposition 6

Muni de la loi induite, un sous-groupe est un groupe.

Démonstration Soit H un sous-groupe d'un groupe G .

- La restriction de la loi de G à H (qui est stable par hypothèse) est évidemment associative.
- L'élément neutre de G est aussi neutre de H .
- Si $x \in H$, son inverse x^{-1} dans G appartient à H et est alors évidemment son inverse dans H .

□

2.3 Morphismes de groupes

Définition 13

Soient G et G' deux groupes. On appelle *morphismes de groupes* de G dans G' , une application de G dans G' qui est un morphisme pour leurs lois respectives.

On utilise la terminologie (isomorphisme, endomorphisme, automorphisme) de la définition 10 de la page 1073.

Exemples

1. La fonction logarithme est un isomorphisme de groupes de (\mathbb{R}_+^*, \times) dans $(\mathbb{R}, +)$.
2. L'application qui envoie tous les éléments d'un groupe G sur l'élément neutre d'un groupe G' est un morphisme de groupes.
3. L'application :

$$\begin{aligned} GL_n(\mathbb{R}) &\longrightarrow \mathbb{R}^* \\ A &\longmapsto \det A \end{aligned}$$

est un morphisme de groupes de $(GL_n(\mathbb{R}), \times)$ dans (\mathbb{R}^*, \times) .

4. Si \mathcal{U} est l'ensemble des nombres complexes de module 1, l'application $(\mu, u) \mapsto \mu u$ est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times) \times (\mathcal{U}, \times)$ dans (\mathbb{C}^*, \times) .

Proposition 7

Soit f un morphisme de groupes de G (d'élément neutre e) dans G' (d'élément neutre e'). On a :

- $f(e) = e'$,
- $\forall x \in G, (f(x))^{-1} = f(x^{-1})$,
- $\forall x \in G, \forall n \in \mathbb{Z}, (f(x))^n = f(x^n)$.

Démonstration

- En notant $*$ les lois de G et de G' , on a :

$$e' * f(e) = f(e) = f(e * e) = f(e) * f(e).$$

En simplifiant par $f(e)$ qui est régulier dans le groupe G' , on en déduit donc $f(e) = e'$.

- D'autre part :

$$f(x) * f(x^{-1}) = f(x * x^{-1}) = f(e) = e'$$

et de même :

$$f(x^{-1}) * f(x) = e',$$

ce qui prouve que le symétrique de $f(x)$ est $f(x^{-1})$.

- Une récurrence permet de prouver la dernière formule pour $n \in \mathbb{N}$. Pour $n \in \mathbb{Z}^+$, on écrit alors :

$$f(x)^n = (f(x)^{-n})^{-1} = (f(x^{-n}))^{-1} = f((x^{-n})^{-1}) = f(x^n).$$

□

Exemples

1. Dans le cas particulier de la fonction logarithme, on obtient :

$$\ln 1 = 0 \quad \text{et} \quad \forall x > 0, \ln(1/x) = -\ln x.$$

2. Si A est une matrice inversible, alors $\det(A^{-1}) = \frac{1}{\det A}$.

2.4 Noyau, image

Soient G et G' deux groupes d'éléments neutres respectifs e et e' , ainsi que f un morphisme de groupes de G dans G' .

Proposition 8

- Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de G' .
- Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de G .

Démonstration

- Soit H un sous-groupe de G et $H'_0 = f(H)$.

Comme H contient l'élément neutre e de G , H'_0 contient $e' = f(e)$ qui est l'élément neutre de G' .

Soit $(y, y') \in H'_0$. Prenons $(x, x') \in H^2$ tel que $y = f(x)$ et $y' = f(x')$. Alors :

- $y * y' = f(x) * f(x') = f(x * x') \in H'_0$ puisque $x * x' \in H$.
- $y^{-1} = f(x)^{-1} = f(x^{-1}) \in H'_0$ puisque $x^{-1} \in H$.

Donc H'_0 est un sous-groupe de G' .

- Soit H' un sous-groupe de G' et $H_0 = f^{-1}(H')$.

Comme $f(e) = e' \in H'$, on a $e \in H_0$.

Soit $(x, x') \in H_0^2$. Alors $f(x) \in H'$ et $f(x') \in H'$, et puisque H' est un sous-groupe :

- $f(x * x') = f(x) * f(x') \in H'$
- $f(x^{-1}) = f(x)^{-1} \in H'$

et par suite $x * x'$ et x^{-1} appartiennent à H_0 .

Donc H_0 est un sous-groupe de G .

□

Corollaire 9

- $f(G)$, l'image de f , est un sous-groupe de G' . On le note $\text{Im}(f)$ ou $\text{Im } f$.
- L'ensemble $f^{-1}(\{e'\})$, appelé *noyau* de f , est un sous-groupe de G . On le note $\text{Ker}(f)$ ou $\text{Ker } f$.

Exemples

1. Si $n \in \mathbb{N}^*$, l'application $\begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & x^n \end{array}$ est un endomorphisme surjectif du groupe (\mathbb{C}^*, \times) . Son noyau est \mathcal{U}_n , l'ensemble des racines $n^{\text{èmes}}$ de l'unité, ce qui permet de prouver que ce dernier est un sous-groupe de \mathbb{C}^* .
2. Le morphisme $\begin{array}{ccc} G & \longrightarrow & G' \\ x & \longmapsto & e' \end{array}$ a pour noyau G et pour image $\{e'\}$.
3. L'application $\theta \mapsto e^{i\theta}$ est un morphisme surjectif du groupe $(\mathbb{R}, +)$ sur le groupe (\mathcal{U}, \times) . Son noyau est $2\pi\mathbb{Z}$.
4. L'application $z \mapsto e^z$ est un morphisme surjectif du groupe $(\mathbb{C}, +)$ sur le groupe (\mathbb{C}^*, \times) . Son noyau est $2i\pi\mathbb{Z}$.
5. L'application $(\rho, \theta) \mapsto \rho e^{i\theta}$ est un morphisme surjectif du groupe $(\mathbb{R}_+^*, \times) \times (\mathbb{R}, +)$ sur le groupe (\mathbb{C}^*, \times) .

Théorème 10

L'application f est injective si, et seulement si, $\text{Ker } f = \{e\}$, c'est-à-dire :

$$\forall x \in G, f(x) = e' \implies x = e. \quad (*)$$

Démonstration

- La propriété $(*)$ signifie $\text{Ker } f \subset \{e\}$, ce qui est bien équivalent à $\text{Ker } f = \{e\}$ puisque, $\text{Ker } f$ étant un sous-groupe de G , il contient l'élément neutre.
- Supposons f injective. Si $x \in \text{Ker } f$ alors $f(x) = e' = f(e)$ donc $x = e$ puisque f est injective.
- Supposons $\text{Ker } f = \{e\}$. Soit $(x, y) \in G^2$ tel que $f(x) = f(y)$. Alors :

$$f(x * y^{-1}) = f(x) * f(y)^{-1} = e',$$

c'est-à-dire $x * y^{-1} \in \text{Ker } f$. Donc $x * y^{-1} = e$, ce qui donne $x = y$.
Donc f est injective. □

3. Anneaux

3.1 Définitions

Définition 14

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

- $(A, +)$ est un groupe commutatif,
- \times est associative,
- A possède un élément neutre pour \times ,
- \times est distributive par rapport à $+$.

On dit que l'anneau est commutatif si \times est commutative.

■ **Notation** Dans un anneau A :

- on note 0 (ou 0_A) l'élément neutre pour $+$.
- on note 1 (ou 1_A) l'élément neutre pour \times .
- on note couramment $x.y$ ou même $x \cdot y$ à la place de $x \times y$.
- on utilise simultanément les deux notations :
 - $n.a$ ou na avec $n \in \mathbb{Z}$ pour l'itéré additif.
 - a^n avec $n \in \mathbb{N}$ (ou $n \in \mathbb{Z}$ si a est inversible) pour l'itéré multiplicatif.
- on a $\forall x \in A$, $x^0 = 1$. En particulier, $0^0 = 1$.

Exemples

1. \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des anneaux commutatifs pour l'addition et la multiplication usuelles.
2. $(\mathbb{R}^\mathbb{R}, +, \times)$ est un anneau commutatif.
3. En revanche, $(\mathbb{R}^\mathbb{R}, +, \circ)$ n'est pas un anneau puisque \circ n'est pas distributive par rapport à $+$:
 - par définition de $f + g$, on a bien l'égalité $(f + g) \circ h = f \circ h + g \circ h$,
 - mais la relation $f \circ (g + h) = f \circ g + f \circ h$ n'est pas vraie en général (prendre par exemple $f = 1$).
4. Si $(G, +)$ est un groupe commutatif, l'ensemble des endomorphismes de groupe de G muni de l'addition et de la composition est un anneau, non commutatif en général.

5. Si A est un anneau et E un ensemble, alors A^E est un anneau pour les lois déduites de celles de A .
6. Si A et B sont des anneaux, alors $A \times B$ muni des lois produit est un anneau.
7. $(\{0\}, +, \times)$ est un anneau.

3.2 Règles de calcul

Proposition 11

Dans un anneau A , on a les propriétés suivantes :

- $\forall a \in A, 0 \times a = a \times 0 = 0,$ *(0 est absorbant)*
- $\forall (a, b) \in A^2, (-a) \times b = a \times (-b) = -(a \times b).$ *(règle des signes)*

Démonstration

► Pour $a \in A$, on a :

$$a \times 0 + a \times 0 = a \times (0 + 0) = a \times 0 = a \times 0 + 0.$$

Puisque $(A, +)$ est un groupe, on peut simplifier par $a \times 0$, ce qui donne $a \times 0 = 0$.

Raisonnement analogue pour montrer $0 \times a = 0$.

► Soit $(a, b) \in A^2$. Montrons que $a \times (-b)$ et $a \times b$ sont opposés :

$$a \times (-b) + a \times b = a \times (b - b) = a \times 0 = 0.$$

Donc $a \times (-b) = -(a \times b)$. On prouve de même $(-a) \times b = -(a \times b)$. □

Remarque Si dans un anneau A on a $0_A = 1_A$, alors :

$$\forall x \in A, x = 1_A x = 0_A x = 0_A$$

et donc $A = \{0_A\}$.

Dans toute la suite, nous ne considérerons que des anneaux A contenant au moins deux éléments, et donc vérifiant $0_A \neq 1_A$.

Proposition 12 (Distributivité généralisée)

Si $(a_i)_{i \in I}$ et $(b_j)_{j \in J}$ sont deux familles d'éléments d'un anneau A , indexées par des ensembles finis I et J , on a :

$$\left(\sum_{i \in I} a_i \right) \cdot \left(\sum_{j \in J} b_j \right) = \left(\sum_{(i,j) \in I \times J} a_i b_j \right).$$

Démonstration On démontre par récurrence la propriété H_n :

si I a n éléments, on a pour tout J fini :

$$\left(\sum_{i \in I} a_i \right) \cdot \left(\sum_{j \in J} b_j \right) = \left(\sum_{(i,j) \in I \times J} a_i b_j \right).$$

- H_0 est vérifié puisque si I est vide, alors $I \times J$ aussi et les deux membres de l'égalité sont nuls.
- H_1 se démontre par récurrence sur le nombre d'éléments de J en utilisant la distributivité.
- Supposons H_{n-1} pour $n \geq 1$, et prenons un ensemble I à n éléments. En écrivant I comme réunion disjointe d'un singleton $\{i_0\}$ et d'un ensemble I' à $n - 1$ éléments, on a :

$$\begin{aligned} \left(\sum_{i \in I} a_i \right) \cdot \left(\sum_{j \in J} b_j \right) &= \left(a_{i_0} + \sum_{i \in I'} a_i \right) \cdot \left(\sum_{j \in J} b_j \right) \\ &= a_{i_0} \cdot \left(\sum_{j \in J} b_j \right) + \left(\sum_{i \in I'} a_i \right) \cdot \left(\sum_{j \in J} b_j \right) \\ &= \sum_{j \in J} a_{i_0} \cdot b_j + \left(\sum_{(i,j) \in I' \times J} a_i b_j \right) \quad \text{d'après } H_1 \text{ et } H_{n-1} \\ &= \left(\sum_{(i,j) \in I \times J} a_i b_j \right). \end{aligned}$$

□

Proposition 13

Soient a et b deux éléments d'un anneau A tels que $a b = b a$ (on dit que a et b commutent).

(a) **Formule du binôme de Newton :**

$$\forall n \in \mathbb{N}, \quad (a + b)^n = \sum_{p=0}^n \binom{n}{p} a^p b^{n-p}.$$

(b) Pour $n \in \mathbb{N}$:

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

(c) Pour $p \in \mathbb{N}$:

$$a^{2p+1} + b^{2p+1} = (a + b)(a^{2p} - a^{2p-1}b + \cdots - ab^{2p-1} + b^{2p}).$$

En particulier, ces relations sont vraies quels que soient les éléments a et b d'un anneau commutatif.

Démonstration

(a) Par récurrence sur n : pour $n = 0$, on obtient $(a + b)^0 = 1 = \binom{0}{0} a^0 b^0$.

Supposons $(a + b)^n = \sum_{p=0}^n \binom{n}{p} a^p b^{n-p}$. Alors :

$$\begin{aligned}(a + b)^{n+1} &= (a + b) \sum_{p=0}^n \binom{n}{p} a^p b^{n-p} \\&= \sum_{p=0}^n \binom{n}{p} a^{p+1} b^{n-p} + \sum_{p=0}^n \binom{n}{p} a^p b^{n-p+1} \\&= \sum_{q=1}^{n+1} \binom{n}{q-1} a^q b^{n-q+1} + \sum_{p=0}^n \binom{n}{p} a^p b^{n-p+1} \quad \text{en posant } q = p + 1 \\&= \binom{n}{0} b^{n+1} + \sum_{p=1}^n \left(\binom{n}{p-1} + \binom{n}{p} \right) a^p b^{n-p+1} + \binom{n}{n} a^{n+1} \\&= \sum_{p=0}^{n+1} \binom{n+1}{p} a^p b^{n-p+1}\end{aligned}$$

puisque $\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}$ et $\binom{n}{0} = \binom{n}{n} = \binom{n+1}{0} = \binom{n+1}{n+1}$.

(b) Il suffit de développer le produit :

$$\begin{aligned}(a - b) \sum_{p=0}^{n-1} a^p b^{n-1-p} &= \sum_{p=0}^{n-1} a^{p+1} b^{n-1-p} - \sum_{p=0}^{n-1} a^p b^{n-p} \\&= \sum_{p=1}^n a^p b^{n-p} - \sum_{p=0}^{n-1} a^p b^{n-p} \\&= a^n - b^n.\end{aligned}$$

(c) La dernière formule s'obtient à partir de la précédente en remplaçant n par $2p+1$ et b par $-b$. □

Remarque Grâce à la formule du binôme de Newton, on peut vérifier que si E est un ensemble fini de cardinal n , alors $\mathcal{P}(E)$ a pour cardinal 2^n .

En effet, l'ensemble $\mathcal{P}(E)$ est la réunion disjointe des $\mathcal{P}_p(E)$ pour $p \in \llbracket 0, n \rrbracket$, où $\mathcal{P}_p(E)$, ensemble des parties à p éléments de E , a pour cardinal $\binom{n}{p}$.

Donc :

$$\text{card } \mathcal{P}(E) = \sum_{p=0}^n \binom{n}{p} = (1+1)^n = 2^n.$$

3.3 Anneaux intègres

Définition 15

Soit A un anneau commutatif. On dit que $a \in A$ est un *diviseur de 0* si $a \neq 0$ et s'il existe un élément x de A non nul tel que $ax = 0$.

Proposition 14

Un élément non nul d'un anneau commutatif est régulier pour la multiplication si, et seulement si, ce n'est pas un diviseur de 0.

Démonstration

- Supposons a régulier. Si $ax = 0$, alors $ax = a0$ et par suite $x = 0$.
Donc a n'est pas diviseur de 0.
- Supposons a non diviseur de 0.
Si $ax = ay$, alors $a(x - y) = 0$ donc $x - y = 0$ c'est-à-dire $x = y$.
Donc a est régulier.

□

Définition 16

Un anneau *intègre* est un anneau commutatif, différent de $\{0\}$, et sans diviseur de 0.

Remarque Dans un anneau intègre, on retrouve la propriété, utilisée couramment dans \mathbb{R} ou \mathbb{C} , disant qu'un produit ne peut être nul que si l'un des facteurs est nul.

Exemples

1. \mathbb{Z} , \mathbb{Q} , \mathbb{R} et \mathbb{C} sont intègres.
2. \mathbb{R}^2 muni de l'addition et la multiplication produit n'est pas un anneau intègre, puisque $(0,1) \times (1,0) = (0,0)$.
3. Si X est un ensemble ayant au moins 2 éléments, alors $(\mathbb{R}^X, +, \times)$ n'est pas intègre car on peut trouver f et g , deux applications non nulles de X dans \mathbb{R} , telles qu'en tout point de X l'une ou l'autre soit nulle.

3.4 Sous-anneaux

Définition 17

On appelle *sous-anneau* d'un anneau $(A, +, \times)$, un sous-groupe de $(A, +)$ qui est stable par \times et qui contient 1_A .

Remarques

- Un sous-anneau de A est donc une partie de A contenant 1_A , stable pour les deux lois de A et passage à l'opposé. En effet, une telle partie contient $0_A = 1_A + (-1_A)$ et par suite est un sous-groupe de $(A, +)$.
- Muni des lois induites, un sous-anneau est évidemment un anneau.

Exemples

1. \mathbb{Z} est un sous-anneau de \mathbb{R} .
2. Le singleton $\{0\}$ est inclus dans \mathbb{R} et il est stable pour les deux lois d'anneau de \mathbb{R} , mais ce n'est pas un sous-anneau de \mathbb{R} , puisqu'il ne contient pas 1.

3.5 Morphismes d'anneaux

Définition 18

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. On dit que $f : A \rightarrow B$ est un *morphisme d'anneaux* si :

1. $\forall (x, y) \in A^2, f(x + y) = f(x) + f(y),$
2. $\forall (x, y) \in A^2, f(x \times y) = f(x) \times f(y),$
3. $f(1_A) = 1_B.$

Les morphismes d'anneaux de $(A, +, \times)$ dans $(B, +, \times)$ sont en particulier des morphismes de groupes de $(A, +)$ dans $(B, +)$. Ils en ont donc toutes les propriétés et on utilise la même terminologie : endomorphisme, isomorphisme, automorphisme.

Exemples

1. L'identité est l'unique endomorphisme de \mathbb{Z} , puisque si f est un tel endomorphisme, on a $f(1) = 1$ ce qui entraîne par récurrence :

$$\forall n \in \mathbb{N}, f(n) = n,$$

puis :

$$\forall n \in \mathbb{Z}^-, f(n) = -f(-n) = -(-n) = n.$$

2. L'application f :

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 0 \end{array}$$

est un morphisme pour les deux lois de \mathbb{R} , mais n'est pas un morphisme d'anneaux puisqu'on n'a pas l'égalité $f(1) = 1$.

3. Si B est un sous-anneau de A , l'application :

$$\begin{array}{ccc} B & \longrightarrow & A \\ x & \longmapsto & x \end{array}$$

est un morphisme d'anneaux.

Proposition 15

L'image d'un sous-anneau de A par un morphisme d'anneaux de A dans B est un sous-anneau de B .

Démonstration Évident d'après les définitions. \square

Remarque Si f est un morphisme d'anneaux de A dans B , c'est aussi un morphisme de groupes, ce qui permet de parler de son noyau $\text{Ker } f = f^{-1}(\{0_B\})$. Mais ce dernier n'est pas un sous-anneau de A , puisqu'il ne contient pas 1_A (on a supposé $A \neq \{0_A\}$).

On conserve évidemment l'équivalence :

$$f \text{ injectif} \iff \text{Ker } f = \{0\}.$$

3.6 Éléments inversibles, unités

Définition 19

Soit A un anneau, on appelle *unité* de A tout élément de A inversible pour la multiplication.

Proposition 16

L'ensemble des unités de A forme un groupe pour \times , et se note A^* .

Démonstration Soit G l'ensemble des unités de A .

- G est stable par \times car si $(u, v) \in G^2$, alors uv est inversible, d'inverse $v^{-1}u^{-1}$.
- \times est associative sur A donc aussi sur G .
- 1_A est une unité ; c'est le neutre de G .
- Si $u \in G$, alors $u^{-1} \in G$ car u^{-1} est inversible d'inverse u .

Donc G est un groupe. \square

Exemples

1. Le groupe des unités de \mathbb{Z} est $\{-1, 1\}$. Mais l'usage veut que \mathbb{Z}^* représente $\mathbb{Z} \setminus \{0\}$ et non le groupe des unités de \mathbb{Z} .
2. Le groupe des unités de \mathbb{R} est $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
3. Le groupe des unités de $\mathbb{R}^{\mathbb{R}}$ est l'ensemble des applications qui ne s'annulent pas sur \mathbb{R} :
 - il est nécessaire que f ne s'annule pas pour pouvoir trouver g telle que $f.g = 1$,
 - c'est suffisant, puisqu'alors $1/f$ convient.

4. Corps

4.1 Définitions

Définition 20

On dit que $(\mathbf{K}, +, \times)$ est un *corps* si $(\mathbf{K}, +, \times)$ est un anneau commutatif non réduit à $\{0\}$ et dont tous les éléments non nuls sont inversibles, c'est-à-dire dont le groupe des unités est $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$.

Remarques

- Dans toute la suite de ce cours, nous ne considérerons que des corps commutatifs, c'est-à-dire dont la seconde loi est commutative. Par abus, nous dirons corps à la place de corps commutatif.
- Un corps est un anneau intègre puisqu'il est commutatif, non réduit à $\{0\}$ et que tous ses éléments non nuls sont inversibles donc réguliers.

Exemples

1. \mathbb{Q} , \mathbb{R} et \mathbb{C} munis des lois usuelles sont des corps.
2. \mathbb{Z} n'est pas un corps, puisque seuls 1 et -1 sont inversibles.
3. $\mathcal{F}(X, \mathbb{R})$ n'est pas un corps si l'ensemble X contient au moins 2 éléments, puisqu'alors il n'est pas intègre.
4. On peut munir l'ensemble $\mathbf{K} = \{0, 1\}$ des lois $+$ et \times définies par les tables suivantes :

$+$	0	1
0	0	1
1	1	0

\times	0	1
0	0	0
1	0	1

(Ce sont les lois usuelles, hormis la relation $1 + 1 = 0$.)

On peut vérifier facilement que $(\mathbb{K}, +, \times)$ est un corps. Dans ce corps, chaque élément est son propre symétrique pour l'addition. En particulier on a $1 = -1$ et $2 \cdot 1 = 1 + 1 = 0$ (il s'agit de l'itéré pour l'addition).

■ **Notation** Si a et b sont deux éléments d'un corps \mathbb{K} (commutatif), b étant non nul, on note $\frac{a}{b}$ l'élément $a \times b^{-1} = b^{-1} \times a$ de \mathbb{K} .

Pour $(a, b, a', b', x) \in \mathbb{K}^5$, $b \neq 0$, $b' \neq 0$ et $x \neq 0$, on a alors les règles de calcul suivantes :

- $\frac{a}{b} = \frac{a'}{b'} \iff a'b' = a'b$.
- $\frac{ax}{bx} = \frac{a}{b}$.
- $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$.
- $\frac{a}{b} \times \frac{a'}{b'} = \frac{aa'}{bb'}$.
- Si $a \neq 0$, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Proposition 17

Soient \mathbb{K} un corps, $a \in \mathbb{K} \setminus \{1\}$ et $n \in \mathbb{N}$. On a

$$1 + a + \cdots + a^n = \frac{1 - a^{n+1}}{1 - a}.$$

Démonstration Conséquence de la proposition 13 de la page 1081. □

Définition 21

Soit \mathbb{K} un corps. On appelle *sous-corps* de \mathbb{K} un sous-anneau de \mathbb{K} qui est un corps.

Exemples

1. \mathbb{Q} , \mathbb{R} et \mathbb{C} sont trois sous-corps de \mathbb{C} .
2. Si \mathbb{K} est un sous-corps de \mathbb{C} , il contient 1 et par conséquent tous les entiers naturels, puis tous les entiers relatifs. Comme il est stable par produit et passage à l'inverse, il contient donc tous les rationnels. Ainsi $\mathbb{Q} \subset \mathbb{K}$ et donc \mathbb{Q} est le plus petit sous-corps de \mathbb{C} .

4.2 Corps des fractions

MPSI

On admet le résultat suivant :

Proposition 18

Soit A un anneau intègre. Il existe un corps \mathbf{K} , unique à un isomorphisme près, tel que A soit un sous-anneau de \mathbf{K} et que tout élément de \mathbf{K} soit de la forme $\frac{a}{b}$, avec $(a, b) \in A^2$ et $b \neq 0$.

Ce corps est appelé *corps des fractions* de l'anneau intègre A .

Remarques

- Ce corps est unique à un isomorphisme près, ce qui signifie que si \mathbf{K} et \mathbf{K}' sont deux corps vérifiant les propriétés précédentes, alors il existe un isomorphisme de \mathbf{K} sur \mathbf{K}' .
- L'expression $\frac{a}{b}$ représente $a \times b^{-1} = b^{-1} \times a$, où b^{-1} désigne l'inverse dans \mathbf{K} de l'élément b appartenant à A donc à \mathbf{K} .

Exemples

1. Le corps des fractions de \mathbb{Z} est appelé corps des rationnels et noté \mathbb{Q} .
2. Le corps des fractions de $\mathbf{K}[X]$, anneau des polynômes à coefficients dans le corps \mathbf{K} , est appelé corps des fractions rationnelles à coefficients dans \mathbf{K} et noté $\mathbf{K}(X)$.

MPSI

5. Espaces vectoriels

Voir page 777.

EXERCICES

1. Soit $(x, y) \in \mathbb{R}^2$. Écrire les négations des propositions suivantes :
 - a) $1 \leq x < y$.
 - b) $xy = 0$ (avec des propositions portant séparément sur x et/ou sur y).
 - c) $x^2 = 1 \Rightarrow x = 1$

2. Écrire les implications ou équivalences correctes :
 - $[\forall x \in E, p(x) \text{ et } q(x)] \dots [\forall x \in E, p(x)] \text{ et } [\forall x \in E, q(x)]$
 - $[\exists x \in E : p(x) \text{ et } q(x)] \dots [\exists x \in E : p(x)] \text{ et } [\exists x \in E : q(x)]$
 - $[\forall x \in E, p(x) \text{ ou } q(x)] \dots [\forall x \in E, p(x)] \text{ ou } [\forall x \in E, q(x)]$
 - $[\exists x \in E : p(x) \text{ ou } q(x)] \dots [\exists x \in E : p(x)] \text{ ou } [\exists x \in E : q(x)]$

3. Les propositions suivantes sont-elles vraies ou fausses ?
 - a) Pour qu'un réel soit strictement supérieur à 3, il suffit qu'il soit strictement supérieur à 4.
 - b) Pour qu'un réel soit strictement supérieur à 3, il faut qu'il soit différent de 2.
 - c) Une condition suffisante pour qu'un réel soit supérieur ou égal à 2, est qu'il soit supérieur ou égal à 3.
 - d) Pour qu'un réel soit strictement supérieur à 2, il suffit que son carré soit strictement supérieur à 4.
 - e) Un condition nécessaire et suffisante pour qu'un entier naturel soit strictement supérieur à 1 est qu'il soit supérieur ou égal à 2.

4. Les propositions suivantes sont-elles vraies ou fausses ?
 - a) $\exists x \in \mathbb{Z} : \exists y \in \mathbb{N} : x \leq -y^2$
 - b) $\exists x \in \mathbb{Z} : \forall y \in \mathbb{N} : x \leq -y^2$
 - c) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{N} : x \leq -y^2$
 - d) $\forall x \in \mathbb{Z}, \forall y \in \mathbb{N}, x \leq -y^2$

5. Écrire les négations des propositions suivantes :
 - a) $\forall x \in E, \forall x' \in E, x \neq x' \Rightarrow f(x) \neq f(x')$
 - b) $\forall \varepsilon > 0, \exists \eta > 0 : \forall x \in]a, b[, |x - x_0| < \eta \Rightarrow |f(x) - f(x_0)| < \varepsilon$
 - c) $\forall a \in \mathbb{Z}, \forall b \in \mathbb{N}^*, \exists q \in \mathbb{Z}, \exists r \in \mathbb{Z} : a = bq + r \text{ et } 0 \leq r < b$

6. L'application f de \mathbb{R}^2 dans \mathbb{R}^2 définie par :

$$f(x,y) = (x, xy - y^3)$$

est-elle injective, surjective ?

7. Soient E, F, G trois ensembles, f une application de E dans F et g une application de E dans G . On considère h de E dans $F \times G$ définie par $h(x) = (f(x), g(x))$. Montrer que si f ou g est injective alors h est injective. On suppose f et g surjectives, h est-elle surjective ?

8. Soient E, F, G trois ensembles, f une application de E dans F et g une application de F dans G . Montrer que :

- a) si $g \circ f$ est injective alors f est injective.
- b) si $g \circ f$ est surjective alors g est surjective
- c) si $g \circ f$ est injective et f surjective, alors g est injective.
- d) si $g \circ f$ est surjective et g injective, alors f est surjective.

9. Montrer que pour tout entier n :

$$2^n > n.$$

10. Soit $n \in \mathbb{N}^*$. Donner une forme plus simple de l'expression :

$$1.1! + 2.2! + \cdots + n.n!.$$

11. Trouver toutes les applications f de \mathbb{N} dans \mathbb{N} telles que :

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

12. Trouver toutes les applications g de \mathbb{N} dans \mathbb{N} telles que :

$$\forall (m,n) \in \mathbb{N}^2, g(m+n) = g(n)g(m).$$

13. Trouver toutes les injections f de \mathbb{N} dans \mathbb{N} telles que :

$$\forall n \in \mathbb{N}, f(n) \leq n.$$

14. Soit $(A_k)_{1 \leq k \leq n}$ une suite finie d'ensembles finis.

Montrer par récurrence sur n que :

$$\begin{aligned} \text{Card} \left(\bigcup_{i=1}^n A_i \right) &= \sum_{i=1}^n \text{Card}(A_i) - \sum_{1 \leq i < j \leq n} \text{Card}(A_i \cap A_j) + \\ &\quad + \sum_{1 \leq i < j < k \leq n} \text{Card}(A_i \cap A_j \cap A_k) + \cdots + (-1)^{n-1} \text{Card} \left(\bigcap_{i=1}^n A_i \right). \end{aligned}$$

15. Soient n et p deux entiers non nuls tels que $n \geq p$.

Quel est le nombre d'applications strictement croissantes de $\{1, \dots, p\}$ dans $\{1, \dots, n\}$?

16. Déterminer le nombre de solutions dans \mathbb{N}^3 de l'équation :

$$x + y + z = n$$

où n est un entier naturel donné.

17. Déterminer le nombre de solutions dans \mathbb{N}^3 du système :

$$\begin{cases} x + y + z = n \\ x \leq y + z \\ y \leq z + x \\ z \leq x + y \end{cases}$$

où n est un entier donné.

18. Soit E un ensemble fini à n éléments.

Trouver le cardinal des ensembles suivants :

a) $F = \{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) \mid A \cup B = E, A \cap B = \emptyset\}$

b) Si A est une partie fixée de E à p éléments.

$$G_A = \{B \in \mathcal{P}(E) \mid A \cup B = E\}$$

c) $H = \{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) \mid A \cup B = E\}$.

19. Soient $p \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que $p < n$.

Montrer que :

$$\binom{n}{p+1} = \binom{p}{p} + \binom{p+1}{p} + \cdots + \binom{n-1}{p}.$$

20. Soient $p \in \mathbb{N}^*$, $q \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ tels que $n \leq p$ et $n \leq q$.

Montrer que :

$$\begin{aligned} \binom{p+q}{n} &= \binom{p}{0} \binom{q}{n} + \binom{p}{1} \binom{q}{n-1} + \cdots \\ &\quad + \binom{p}{j} \binom{q}{n-j} + \cdots + \binom{p}{n} \binom{q}{0}. \end{aligned}$$

En déduire une expression simple de :

$$\binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2.$$

- 21.** Soient $p \in \mathbb{N}$, $n \in \mathbb{N}$ avec $1 \leq p \leq n$.

Établir les relations suivantes :

$$2^p \binom{n}{p} = \binom{n}{0} \binom{n}{p} + \binom{n}{1} \binom{n-1}{p-1} + \cdots + \binom{n}{p} \binom{n-p}{0}$$

$$0 = \binom{n}{0} \binom{n}{p} - \binom{n}{1} \binom{n-1}{p-1} + \cdots + (-1)^p \binom{n}{p} \binom{n-p}{0}.$$

- 22.** En calculant de deux manières le module de $(1+i)^n$, montrer que :

$$\left(1 - \binom{n}{2} + \binom{n}{4} - \cdots\right)^2 + \left(\binom{n}{1} - \binom{n}{3} + \cdots\right)^2 = 2^n$$

- 23.** Soit E un ensemble fini de cardinal n et A une partie de E qui contient p éléments ($p \leq n$).

- a) Quel est le nombre de parties à k éléments de E contenant un et un seul élément de A ?
- b) Quel est le nombre de parties à k éléments de E contenant au moins un élément de A ?

- 24.** Soient $(n,p) \in \mathbb{N}^{*2}$ et $S_{p,n}$ le nombre de surjections d'un ensemble à p éléments dans un ensemble à n éléments.

- a) On suppose $p < n$. Que vaut $S_{p,n}$?
- b) Calculer $S_{n+1,n}$ et $S_{p,2}$.
- c) Montrer que :

$$\forall (n,p) \in (\mathbb{N}^{*})^2, \quad n^p = \sum_{i=1}^n \binom{n}{i} S_{p,i}.$$

- 25.** Soient n et p deux entiers non nuls.

a_1, a_2, \dots, a_p sont p entiers tels que :

$$\sum_{i=1}^p a_i = n.$$

Calculer le nombre d'applications de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, p\}$ telles que pour tout i entre 1 et p , i ait exactement a_i antécédents.

- 26.** On donne n points dans le plan, trois quelconques de ces points n'étant pas alignés. On joint ensuite ces points par des droites de toutes les manières possibles et l'on suppose que ces droites ne sont jamais parallèles et que trois droites ne peuvent être concourantes qu'aux points initiaux.

Calculer le nombre de points d'intersection ainsi obtenus (non compris les n points initiaux).

- 27.** a) Calculer la somme des cardinaux de toutes les parties d'un ensemble E fini à n éléments.

- b) Soit F une partie de E de cardinal k .

Trouver le nombre de couples (X, Y) de $\mathcal{P}(E)^2$ vérifiant $X \cap Y = F$.

En déduire $\sum_{(X,Y) \in (\mathcal{P}(E))^2} \text{Card}(X \cap Y)$.

- 28.** Soit E un ensemble à np éléments ($n \in \mathbb{N}^*$, $p \in \mathbb{N}^*$).

On note $P_{n,p}$ le nombre de partitions de E en n parties à p éléments.

Montrer que :

$$P_{n,p} = \frac{1}{n} \binom{np}{p} P_{n-1,p}.$$

En déduire $P_{n,p}$.

Chapitre 24

Arithmétique dans \mathbb{Z}

PCSI Seules sont au programme de PCSI :

- la divisibilité et la division euclidienne,
- la définition des nombres premiers page 696,
- la décomposition en facteurs premiers (théorème 25 de la page 698) que l'on admettra.

PCSI

1. Divisibilité dans \mathbb{Z}

1.1 Diviseurs, multiples

Définition 1

Étant donnés deux entiers relatifs a et b , on dit que a est un *diviseur* de b , ou que b est un *multiple* de a , s'il existe $k \in \mathbb{Z}$ tel que $b = k a$.

■ Notations

- Si d est un diviseur de a on note $d | a$.
- L'ensemble des diviseurs de a est noté $\mathcal{D}(a)$.
- L'ensemble des multiples de a est noté $\mathcal{M}(a)$ ou $a\mathbb{Z}$.

Exemples

- 1 et -1 divisent tous les entiers, mais ne sont divisibles que par 1 et -1 .
- 0 est un multiple de tous les entiers, mais n'est diviseur que de lui-même.
- $\mathcal{D}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Remarque

- La relation “divise” est réflexive et transitive, mais n'est pas une relation d'ordre dans \mathbb{Z} , car elle n'est pas antisymétrique.
- En revanche, d'après la proposition suivante, sa restriction à \mathbb{N} est une relation d'ordre. Pour cet ordre, le plus petit élément de \mathbb{N} est 1, et le plus grand 0.
- La divisibilité sur \mathbb{N}^* est liée à l'ordre naturel de \mathbb{N}^* par la relation:

$$a | b \implies a \leq b.$$

En effet, si $a | b$ alors $b = k a$ avec $k \in \mathbb{Z}$ et, puisque a et b sont strictement positifs, on a $k \in \mathbb{N}^*$ et par suite $b \geq a$.

Ce résultat est faux dans \mathbb{N} puisque, par exemple, $1 | 0$.

Proposition 1

On a $(a | b \text{ et } b | a) \iff |a| = |b|$.

Démonstration

- Supposons $a | b$ et $b | a$. Il existe alors des entiers relatifs k et k' tels que $b = k a$ et $a = k' b$, ce qui donne $a = k' k a$.
 - Si $a = 0$, alors $b = k 0 = 0$ et $|a| = |b| = 0$.
 - Si $a \neq 0$, alors $k' k = 1$. Comme k et k' sont des entiers relatifs, on a $|k| = |k'| = 1$, ce qui montre $|a| = |b|$.
- Si $|a| = |b|$, alors $a = b$ ou $a = -b$. Donc $a | b$ et $b | a$. □

La proposition suivante est une conséquence évidente de la définition.

Proposition 2

Soient a et b deux entiers relatifs.

- Si $(u, v) \in \mathbb{Z}^2$, alors :

$$(d | a \text{ et } d | b) \implies d | au + bv.$$

- Si x est un entier non nul, alors :

$$a | b \iff ax | bx.$$

1.2 Division euclidienne sur \mathbb{Z}

Théorème 3

Soient a un entier relatif et b un entier naturel non nul. Il existe un unique couple d'entiers relatifs (q, r) tel que :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b. \quad (*)$$

- q est appelé *quotient de la division euclidienne de a par b* ,
- r est appelé *reste de la division euclidienne de a par b* .

Démonstration

Unicité. Soient (q, r) et (q', r') deux couples vérifiant (*). Montrons que $q = q'$ et $r = r'$.

Puisque $0 \leq r < b$ et $0 \leq r' < b$, on a $b|q - q'| = |r' - r| < b$, ce qui entraîne $|q - q'| = 0$ puis $r' - r = 0$.

Existence.

- Si $a \in \mathbb{N}$: l'ensemble $A = \{n \in \mathbb{N} \mid nb \leq a\}$ est une partie de \mathbb{N} non vide puisque $0 \in A$.

De plus A est majorée par a puisque si $n \in A$, alors $n \leq nb \leq a$ (b est non nul donc supérieur ou égal à 1).

Donc A admet un plus grand élément q qui vérifie alors :

- $qb \leq a$ puisque $q \in A$,
- $(q+1)b > a$ puisque $q+1 \notin A$.

En posant $r = a - bq$, on a alors $a = bq + r$ et $0 \leq r < (q+1)b - bq = b$.

- Cas général : comme $b \geq 1$, on a $|a|b \geq |a|$, et donc $a + |a|b \in \mathbb{N}$. En appelant q' et r le reste et quotient de la division euclidienne de $a + |a|b$ par b , on obtient :

$$a = bq' + r - |a|b = bq + r$$

avec $q = q' - |a|$.

□

Remarques

- Si q est le quotient et r le reste de la division euclidienne de a par $b \neq 0$, on a :

$$q = E\left(\frac{a}{b}\right) \quad \text{et} \quad r \equiv a \pmod{b}$$

où E désigne la fonction partie entière, puisque l'on a l'équivalence :

$$\forall q \in \mathbb{Z}, \left(q \leq \frac{a}{b} < q+1 \iff bq \leq a < bq+b \right).$$

- Si q est le quotient de la division euclidienne de l'entier naturel a par b , l'ensemble $A = \{n \in \mathbb{N} \mid nb \leq a\}$ est l'intervalle $[0, q]$.

- Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, notons q et r les quotient et reste de la division euclidienne de a par b .
 - Si $r = 0$, alors $a = bq$ et donc $b | a$.
 - Réciproquement, si $b | a$, alors on a $a = kb + 0$ avec $k \in \mathbb{Z}$ et $0 \leq r < b$. L'unicité de la division euclidienne nous donne donc $k = q$ et $r = 0$.
- On a donc l'équivalence $b | a \iff r = 0$.

Exemple En MAPLE, la division euclidienne des entiers naturels se fait à l'aide des fonctions `iquo` et `irem`, la première donnant le quotient et la deuxième le reste.

```
> q:=iquo(123456,456);
                                         q := 270
> r:=irem(123456,456);
                                         r := 336
> q*456+r;
                                         123456
```

2. Plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM)

MPSI

2.1 Définitions

Soient a et b deux entiers relatifs.

- Si $(a,b) \neq (0,0)$, l'ensemble des diviseurs communs à a et b est une partie de \mathbb{Z} , non vide puisqu'elle contient 1, et majorée par $\max(|a|,|b|)$ ¹. Elle possède donc un plus grand élément, supérieur ou égal à 1.
- Si $a, b \neq 0$, l'ensemble des multiples strictement positifs communs à a et b est une partie de \mathbb{N} , non vide car elle contient $|ab|$. Elle possède donc un plus petit élément.

Définition 2

- Le PGCD de a et b , noté $a \wedge b$, est :
 - le plus grand des diviseurs communs à a et b lorsque $(a,b) \neq (0,0)$,
 - 0 lorsque $a = b = 0$.
- Le PPCM de a et b , noté $a \vee b$, est :
 - le plus petit des multiples strictement positifs communs à a et b lorsque $ab \neq 0$,
 - 0 lorsque $a = 0$ ou $b = 0$.

¹ Elle est même majorée par $\min(|a|,|b|)$ si a et b sont non nuls

Remarques

- Étant donnés deux entiers relatifs a et b , on a :

$$a \wedge b = |a| \wedge |b| \quad \text{et} \quad a \vee b = |a| \vee |b|.$$

C'est pourquoi l'on supposera souvent par la suite que a et b sont des entiers naturels.

- Par définition, on a, pour tout $a \in \mathbb{Z}$:

$$a \wedge 0 = |a| \quad \text{et} \quad a \vee 0 = 0.$$

- Si $a = b = 0$, les diviseurs communs à a et b sont tous les entiers, et il n'en existe donc pas de plus grand pour la relation d'ordre \leqslant (voir cependant la remarque de la page 688).
- Si $ab = 0$, seul 0 est un multiple commun à a et b et il n'existe donc pas de multiple strictement positif commun à a et b .

Exemple En MAPLE, ce sont les fonctions `igcd` et `ilcm` qui calculent le PGCD et le PPCM :

```
> igcd(342, 564);
> ilcm(342, 364);
```

$$\frac{6}{32148}$$

2.2 Algorithme d'Euclide

Proposition 4

Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$. Si $a = bq + r$, alors :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r) \cap \mathcal{D}(b)$$

et par conséquent $a \wedge b = b \wedge r$.

Démonstration

- Si $d \in \mathcal{D}(a) \cap \mathcal{D}(b)$, alors $d \mid (bq)$ et $d \mid a$, donc $d \mid (a - bq) = r$, par suite $d \in \mathcal{D}(r) \cap \mathcal{D}(b)$.
- Par symétrie, puisque $r = a - bq$, on a aussi $\mathcal{D}(r) \cap \mathcal{D}(b) \subset \mathcal{D}(a) \cap \mathcal{D}(b)$.

D'où l'égalité :

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r) \cap \mathcal{D}(b)$$

et donc les plus grands éléments de $\mathcal{D}(a) \cap \mathcal{D}(b)$ et de $\mathcal{D}(r) \cap \mathcal{D}(b)$ sont égaux, ce qui donne le résultat. \square

Le résultat précédent est en particulier vrai lorsque q et r sont respectivement les quotient et reste de la division euclidienne de a par b et donc pour calculer le PGCD de a et b , il suffit de calculer celui de b et de r .

Comme $r < b$, on se ramène à un couple d'entiers plus petits. Il suffit alors de recommencer, ce qui constitue l'*algorithme d'Euclide* que nous décrivons ci-dessous.

Description

Étant donnés deux entiers naturels a et b , définissons :

- $r_0 = a$
- $r_1 = b$.
- Pour $n \geq 1$, si $r_n \neq 0$, r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n .

La suite r ne peut pas être définie sur \mathbb{N} , car elle est strictement décroissante à partir du rang 1 et à valeurs dans \mathbb{N} . Il existe donc un rang N pour lequel on a $r_N \neq 0$ et $r_{N+1} = 0$.

D'après la proposition précédente, on a alors :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_N \wedge r_{N+1}$$

et comme $r_{N+1} = 0$, on a $r_N \wedge r_{N+1} = r_N$.

Le PGCD de a et de b est donc le dernier reste non nul obtenu dans la suite des divisions successives.

Remarque Historiquement, l'algorithme d'Euclide reposait sur l'égalité $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a - b) \cap \mathcal{D}(b)$. Il était ainsi plus long, puisque si q et r sont les quotient et reste de la division euclidienne de a par b , il fallait q étapes pour se ramener au couple (b, r) .

En revanche, il était plus simple puisqu'il ne nécessitait que des soustractions et pas de division.

Algorithme

DONNÉES : les entiers naturels a et b .

VARIABLES : x , y et r .

- $x \leftarrow a$
- $y \leftarrow b$
- tant que $y \neq 0$
 - $r \leftarrow$ reste de la division de x par y
 - $x \leftarrow y$
 - $y \leftarrow r$

RÉSULTAT : x .

Remarques

- Lorsque $b = 0$, on n'effectue aucune division et le résultat obtenu est bien $a = a \wedge 0$.
- Lorsque $a < b$, la première division donne a pour reste et l'algorithme commence donc par échanger x et y . Par la suite, on a toujours $x > y$.

2.3 Coefficients de Bézout

Soient a et b deux entiers relatifs.

Proposition 5

Il existe des entiers relatifs u et v tels que :

$$\bullet u + bv = a \wedge b.$$

Un tel couple (u, v) est appelé un couple de *coefficients de Bézout* de a et b .

Démonstration Quitte à remplacer a par $|a|$ et b par $|b|$, il suffit de traiter le cas où a et b sont des entiers naturels.

Démontrons par récurrence sur $b \in \mathbb{N}$ la propriété H_b : "Pour tout entier naturel a , il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$."

- H_0 est vraie car $a \times 1 + 0 \times 0 = a = a \wedge 0$.
- Supposons la propriété vraie jusqu'au rang $b - 1$, avec $b \in \mathbb{N}^*$. Soit $a \in \mathbb{N}$; notons d le PGCD de a et b . On effectue la division euclidienne de a par b :

$$a = bq + r \quad \text{avec} \quad 0 \leq r < b.$$

D'après la proposition 4 de la page 685, on a donc $d = b \wedge r$ et la propriété H_r montre qu'il existe $(u', v') \in \mathbb{Z}^2$ tel que :

$$bu' + rv' = d.$$

On a donc :

$$bu' + (a - bq)v' = d$$

ce qui donne :

$$au + bv = d$$

avec $u = u'$ et $v = v' - qv'$. D'où H_b . □

Proposition 6

Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.

Démonstration En reprenant les notations de l'algorithme d'Euclide de la page précédente, on a $\mathcal{D}(r_0) \cap \mathcal{D}(r_1) = \mathcal{D}(r_N) \cap \mathcal{D}(r_{N+1}) = \mathcal{D}(r_N)$ et donc $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$, ce qu'il fallait démontrer. □

Remarque Le PGCD de a et b est donc le plus grand, au sens de la divisibilité, des diviseurs positifs communs à a et à b .

Ce résultat est valable même si $a = b = 0$, car dans ce cas, l'ensemble des diviseurs positifs communs est égal à \mathbb{N} et 0 est bien le plus grand élément de \mathbb{N} pour la divisibilité. En revanche, pour l'ordre naturel de \mathbb{N} , il n'existe pas dans ce cas de plus grand diviseur commun à a et b .

2.4 Entiers premiers entre eux

Définition 3

Les entiers a et b sont *premiers entre eux* si $a \wedge b = 1$, c'est-à-dire si les seuls diviseurs communs à a et b sont 1 et -1 .

Proposition 7 (Identité de Bézout)

Les entiers a et b sont premiers entre eux si, et seulement si, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Démonstration

- Si a et b sont premiers entre eux, alors $a \wedge b = 1$ et, d'après la proposition 5 de la page précédente, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b = 1$.
- S'il existe deux entiers relatifs u et v tels que $au + bv = 1$, alors tout diviseur commun à a et b divise $au + bv$ donc est égal à 1 ou à -1 . On en déduit que a et b sont premiers entre eux. \square

Proposition 8

Si $d = a \wedge b$, alors il existe deux entiers a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Démonstration

- Si $a = b = 0$, on a $d = 0$ et il suffit de prendre $a' = b' = 1$.
- Sinon, comme d divise a et b , il est clair qu'il existe a' et b' tels que $a = da'$ et $b = db'$. Comme d est le PGCD de a et b , il existe u et v entiers tels que $d = au + bv$, ce qui donne $1 = a'u + b'v$. Ainsi, a' et b' sont premiers entre eux. \square

Corollaire 9

Tout nombre rationnel s'écrit sous forme irréductible, c'est-à-dire sous la forme $\frac{a}{b}$ où a et b sont des entiers premiers entre eux, b étant non nul.

Pour obtenir cette forme irréductible d'un rationnel quelconque, il suffit de diviser son numérateur et son dénominateur par leur PGCD.

2.5 Théorème de Gauss

Théorème 10

Étant donnés trois entiers relatifs a, b et c , on a :

$$(a \wedge b = 1 \text{ et } a \mid bc) \iff a \mid c.$$

Démonstration Supposons $a \wedge b = 1$ et $a \mid bc$. D'après l'identité de Bézout, il existe deux entiers relatifs u et v tels que $au + bv = 1$, ce qui implique $acu + bcv = c$.

Comme $a \mid bc$, on a $a \mid bcv$ et donc :

$$a \mid acu + bcv = c.$$

□

Remarque Ce théorème est également appelé parfois lemme de Gauss.

Exemple Étant donné un rationnel possédant deux formes irréductibles $\frac{a_1}{b_1}$ et $\frac{a_2}{b_2}$, on a $a_1 b_2 = a_2 b_1$. Ainsi b_1 divise $a_1 b_2$, et comme il est premier avec a_1 , on en déduit qu'il divise b_2 . Par symétrie, on a aussi $b_2 \mid b_1$.

Alors $b_2 = \varepsilon b_1$ avec $\varepsilon = \pm 1$ et par suite $a_2 = \varepsilon a_1$.

Un rationnel r s'écrit donc de manière unique sous la forme $\frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $a \wedge b = 1$. C'est ce que l'on appelle l'*écriture canonique* de r .

Proposition 11

Étant donnés trois entiers relatifs a, b et c , on a :

$$(a \wedge b = 1 \text{ et } a \wedge c = 1) \iff a \wedge (bc) = 1.$$

Démonstration

- Supposons $a \wedge b = 1$ et $a \wedge c = 1$. On peut montrer à l'aide du théorème de Gauss que a et bc sont premiers entre eux, mais on peut aussi utiliser l'identité de Bézout : si $a \wedge b = 1$ et $a \wedge c = 1$, il existe $(u, v, u', v') \in \mathbb{Z}^4$ tel que :

$$au + bv = 1 \text{ et } au' + cv' = 1.$$

En multipliant membre à membre ces deux égalités on obtient alors immédiatement une relation du type $aU + bcV = 1$, ce qui prouve que a et bc sont premiers entre eux.

- La réciproque est évidente, puisque $u \wedge b$ et $u \wedge c$ sont des diviseurs communs à a et bc . □

Cette proposition se généralise facilement par récurrence à un produit fini quelconque :

Proposition 12

Un produit est premier avec un entier a si, et seulement si, chacun de ses facteurs est premier avec a .

Corollaire 13

Si a et b sont deux entiers relatifs premiers entre eux, alors on a :

$$\forall (m, n) \in \mathbb{N}^2, a^m \wedge b^n = 1.$$

2.6 PPCM**Proposition 14**

Si a et b sont deux entiers premiers entre eux, alors les multiples communs à a et b sont les multiples de ab .

En particulier, on a $a \vee b = |ab|$.

Démonstration Il est évident que les multiples de ab sont des multiples communs à a et b . Réciproquement, supposons $a \mid x$ et $b \mid x$; il existe donc un entier c tel que $x = bc$. Comme $a \mid x$ et $a \wedge b = 1$, le théorème de Gauss montre que a divise c . Il existe donc un entier y tel que $c = ay$, ce qui donne $x = aby$ et prouve le résultat. \square

On peut facilement généraliser ce résultat à un produit fini quelconque d'entiers premiers entre eux :

Corollaire 15

Si des entiers premiers entre eux deux à deux divisent un entier a , alors leur produit divise a .

Corollaire 16

Soient a et b deux entiers. Notons d leur PGCD et prenons a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

- Les multiples communs à a et b sont les multiples de $da'b'$.
- En particulier, on a $a \vee b = d|a'b'|$ et :

$$(a \vee b)(a \wedge b) = |ab|.$$

Démonstration Il est évident que $da'b' = a'b' = a'b$ est un multiple de a et b .

Réciproquement, soit x un multiple commun à a et b . Alors x est un multiple de d et l'on peut écrire $x = dx'$, avec $x' \in \mathbb{Z}$.

On a donc $a' \mid x'$ et $b' \mid x'$ (même si $d = 0$, puisqu'alors $a' = b' = 1$) et comme a' et b' sont premiers entre eux, $a'b' \mid x'$. Ainsi $da'b' \mid dx' = x$.

Le deuxième point est immédiat. \square

Corollaire 17

Les multiples communs à a et b sont les multiples de $a \vee b$.

Remarque Le PPCM de a et b est donc, au sens de la divisibilité, le plus petit des multiples positifs communs à a et à b . Le plus grand multiple commun est, quant à lui, égal à 0 (toujours pour la relation de divisibilité).

Exemple Soient a et b deux entiers relatifs.

Si $a = xa'$ et $b = xb'$ avec $(x, a', b') \in \mathbb{Z}^3$, alors :

$$a \wedge b = |x|(a' \wedge b') \quad \text{et} \quad a \vee b = |x|(a' \vee b').$$

Démonstration Les résultats étant évidents pour $x = 0$, on peut supposer $x \neq 0$.

► Soient $d = a \wedge b$ et $d' = a' \wedge b'$.

- Comme $d' \mid a'$ et $d' \mid b'$, on a $xd' \mid xa' = a$ et $xd' \mid xb' = b$. Donc $xd' \mid d$.
- On peut alors écrire $d = xd'z = xy$ avec $y = d'z$ qui est donc divisible par d' . Par suite, on a :

$$xy = d \mid a = xa'$$

et de même $xy \mid xb'$ ce qui prouve, puisque $x \neq 0$, que y divise a' et b' et donc leur PGCD d' . On a ainsi $d = xy \mid xd'$.

En conclusion $d = |x|d'$.

► Soient $m = a \vee b$ et $m' = a' \vee b'$.

- Comme $a' \mid m'$ et $b' \mid m'$, on a $a = xa' \mid xm'$ et $b = xb' \mid xm'$. Donc xm' est un multiple commun à a et b , et par suite $m \mid xm'$.
- Puisque m est un multiple de $a = xa'$, on peut écrire $m = xy$. On a alors $xa' \mid xy$ et $xb' \mid xy$ ce qui donne, puisque $x \neq 0$, $a' \mid y$ et $b' \mid y$. Donc $m' \mid y$ ce qui prouve $xm' \mid xy = m$.

En conclusion $m = |x|m'$. □

2.7 Résolution dans \mathbb{Z} de l'équation $ax + by = c$

Soient a , b et c trois entiers relatifs, a et b étant non nuls. Considérons l'équation :

$$ax + by = c \tag{E}$$

dont on cherche les solutions (x, y) dans \mathbb{Z}^2 .

Solution générale

- Si c n'est pas multiple de $a \wedge b$, l'équation (E) n'a pas de solution, car pour tout $(x, y) \in \mathbb{Z}^2$, l'entier $ax + by$ est un multiple de $a \wedge b$.

- Si c est un multiple de $a \wedge b$, il s'écrit $c = \lambda(a \wedge b)$.
- D'après la proposition 5 de la page 687 il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$, et le couple $(\lambda u, \lambda v)$ est alors une solution de l'équation (E) . L'équation (E) possède donc des solutions ; dans la suite on note (x_0, y_0) une solution particulière.
- Posons $d = a \wedge b$ et prenons a' et b' , tels que $a = da'$ et $b = db'$. On a $a' \wedge b' = 1$.
Un couple $(x, y) \in \mathbb{Z}^2$ est solution de (E) si, et seulement si, on a :

$$ax + by = ax_0 + by_0$$

c'est-à-dire :

$$a(x - x_0) = b(y_0 - y)$$

soit encore :

$$a'(x - x_0) = b'(y_0 - y) \quad (*)$$

- * Si (x, y) est solution de $(*)$, alors $a' \mid b'(y_0 - y)$ et, comme a' et b' sont premiers entre eux, le théorème de Gauss implique $a' \mid (y_0 - y)$. Il existe donc $k \in \mathbb{Z}$ tel que $y_0 - y = a' k$ ce qui, en reportant dans $(*)$ et en simplifiant par $a' \neq 0$, donne $x - x_0 = b' k$.
- * Réciproquement si $k \in \mathbb{Z}$, le couple $(x_0 + b' k, y_0 - a' k)$ est solution de (E) .

L'ensemble des solutions de l'équation (E) est donc :

$$\{(x_0 + b' k, y_0 - a' k) \mid k \in \mathbb{Z}\}.$$

Algorithme de recherche d'une solution particulière

Pour résoudre (E) , il suffit donc de trouver une solution particulière de l'équation $ax + by = d$, avec $d = a \wedge b$, c'est-à-dire un couple de coefficients de Bézout.

Première méthode. Prenons la famille $(r_n)_{n \in \llbracket 0, N+1 \rrbracket}$ des restes successifs de l'algorithme d'Euclide décrit page 686. On a $r_0 = a$, $r_1 = b$ et :

$$\forall k \in \llbracket 1, N \rrbracket, r_{k-1} = q_k r_k + r_{k+1}$$

avec $r_{N+1} = 0$. On sait alors que l'on a $\forall k \in \llbracket 1, N+1 \rrbracket, d = r_{k-1} \wedge r_k$, et en particulier $d = r_N$.

La relation $r_{N-2} - q_{N-1} r_{N-1} = r_N = d$ nous donne immédiatement un couple de coefficients de Bézout pour r_{N-2} et r_{N-1} .

D'autre part, si l'on a $r_k u + r_{k+1} v = d$, on obtient :

$$d = r_k u + (r_{k-1} - q_k r_k) v = r_{k-1} v + r_k (u - q_k v).$$

On peut ainsi, de proche en proche, en remontant l'algorithme d'Euclide, trouver un couple de coefficients de Bézout pour a et b .

Exemple

$$\begin{array}{l} 19 = 2 \times 7 + 5 \\ 7 = 1 \times 5 + 2 \\ 5 = 2 \times 2 + 1 \end{array} \quad \boxed{\begin{array}{l} 1 = 3 \times 19 - 8 \times 7 \\ 1 = -2 \times 7 + 3 \times 5 \\ 1 = 1 \times 5 - 2 \times 2 \end{array}}$$

(Dans les équations de droite, on remplace l'entier entouré par la valeur tirée de l'équation de gauche correspondante.)

Malheureusement la méthode précédente, qui correspond à une programmation récursive, exige de garder en mémoire toutes les divisions euclidiennes successives, ce qui rend coûteuse une programmation itérative. On peut cependant modifier l'algorithme d'Euclide pour qu'il donne, en plus du PGCD, un couple de coefficients de Bézout.

Seconde méthode. Le principe consiste à garder, à chaque étape, un couple (u_k, v_k) tel que $a u_k + b v_k = r_k$.

- Pour $k = 0$, on pose $u_0 = 1$ et $v_0 = 0$.
- Pour $k = 1$, on pose $u_1 = 0$ et $v_1 = 1$.
- Si pour $1 \leq k \leq N - 1$, il existe $u_{k-1}, v_{k-1}, u_k, v_k$ tels que :

$$r_{k-1} = a u_{k-1} + b v_{k-1} \quad \text{et} \quad r_k = a u_k + b v_k$$

alors on a :

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_k r_k \\ &= a u_{k-1} + b v_{k-1} - q_k(a u_k + b v_k) \\ &= a(u_{k-1} - q_k u_k) + b(v_{k-1} - q_k v_k). \end{aligned}$$

En posant $u_{k+1} = u_{k-1} - q_k u_k$ et $v_{k+1} = v_{k-1} - q_k v_k$, on a bien :

$$r_{k+1} = a u_{k+1} + b v_{k+1}.$$

- Pour $k = N$, on a alors :

$$d = r_N = a u_N + b v_N.$$

Une solution particulière de l'équation $a x + b y = d$ est donc (u_N, v_N) .

Algorithme

DONNÉES : les entiers naturels a et b .

VARIABLES : x, y, u_0, v_0, u_1, v_1 , et q .

- $(x, y) \leftarrow (a, b)$
- $(u_0, v_0) \leftarrow (1, 0)$
- $(u_1, v_1) \leftarrow (0, 1)$
- tant que $y \neq 0$
 - $q \leftarrow$ quotient de la division de x par y
 - $(x, y) \leftarrow (y, x - qy)$
 - $(u_0, u_1) \leftarrow (u_1, u_0 - qu_1)$
 - $(v_0, v_1) \leftarrow (v_1, v_0 - qv_1)$

RÉSULTAT : (x, u_0, v_0) .

Interprétation matricielle

Si l'on pose $M_k = \begin{pmatrix} r_{k-1} & r_k \\ u_{k-1} & u_k \\ v_{k-1} & v_k \end{pmatrix}$, les relations :

$$\begin{cases} r_{k+1} = r_{k-1} - q_k r_k \\ u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$$

se traduisent matriciellement par $M_{k+1} = M_k Q_k$, où $Q_k = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}$.

En posant $\Omega = Q_1 Q_2 \dots Q_N$, on a alors $M_{N+1} = M_1 \Omega$ avec :

$$M_{N+1} = \begin{pmatrix} d & 0 \\ u_N & u_{N+1} \\ v_N & v_{N+1} \end{pmatrix} \quad \text{et} \quad M_1 = \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

et par suite :

$$\Omega = \begin{pmatrix} u_N & u_{N+1} \\ v_N & v_{N+1} \end{pmatrix}.$$

- Les coefficients de Bézout (u_N, v_N) forment donc la première colonne de Ω .
- De plus, la deuxième colonne est constituée de (u_{N+1}, v_{N+1}) qui vérifient donc $a u_{N+1} + b v_{N+1} = 0$.

- Comme Ω est le produit de matrices de déterminant -1 , elle a un déterminant égal à ± 1 , ce qui prouve $u_N v_{N+1} - v_N u_{N+1} = \pm 1$ et donc que u_{N+1} et v_{N+1} sont premiers entre eux.

Une forme irréductible de la fraction $\frac{a}{b}$ est donc $-\frac{v_{N+1}}{u_{N+1}}$.



2.8 Plus grand commun diviseur de plusieurs entiers

On peut généraliser les propriétés du PGCD de deux entiers à une famille $(a_k)_{1 \leq k \leq p}$ d'entiers relatifs ($p \geq 2$).

Les démonstrations par récurrence de ces propriétés sont laissées au lecteur.

Définition

Définition 4

On appelle plus grand commun diviseur de la famille $(a_k)_{1 \leq k \leq p}$, l'entier noté $a_1 \wedge a_2 \wedge \dots \wedge a_p$ défini par :

- $a_1 \wedge a_2 \wedge \dots \wedge a_p = 0$, si $a_1 = a_2 = \dots = a_p = 0$.
- sinon, $a_1 \wedge a_2 \wedge \dots \wedge a_p$ est le plus grand, au sens de la relation \leq , des diviseurs communs à tous les entiers a_k et il est alors supérieur ou égal à 1.

Proposition 18

Il existe une famille $(u_k)_{1 \leq k \leq p}$ d'entiers relatifs tels que :

$$\sum_{k=1}^p u_k a_k = a_1 \wedge a_2 \wedge \dots \wedge a_p$$

Proposition 19

Les diviseurs communs à a_1, a_2, \dots, a_p sont les diviseurs de $a_1 \wedge a_2 \wedge \dots \wedge a_p$.

Entiers premiers entre eux

Définition 5

Les entiers a_1, a_2, \dots, a_p sont premiers entre eux dans leur ensemble, si $a_1 \wedge a_2 \wedge \dots \wedge a_p = 1$, c'est-à-dire si $\bigcap_{k=1}^p \mathcal{D}(a_k) = \{-1, 1\}$.

Proposition 20 (Identité de Bézout)

Les entiers a_1, a_2, \dots, a_p sont premiers entre eux dans leur ensemble si, et seulement si, il existe une famille $(u_k)_{1 \leq k \leq p}$ d'entiers relatifs telle que :

$$\sum_{k=1}^p u_k a_k = 1.$$

Remarques

- Des entiers premiers entre eux deux à deux sont évidemment premiers entre eux dans leur ensemble.
- La réciproque est fausse ; si $a_1 \wedge a_2 \wedge \dots \wedge a_p = 1$ il se peut même que $\forall (i, j), a_i \wedge a_j \neq 1$, comme le prouve l'exemple des entiers 6, 10 et 15.

MPSI

3. Nombres premiers

Dans cette section, nous nous limitons à l'ensemble \mathbb{N} des entiers naturels.

3.1 Définition

Définition 6

On appelle nombre premier tout entier naturel différent de 1 n'admettant pour diviseurs que 1 et lui-même.

Exemples 2, 3, 5, 7, 11, ..., 65 537, ..., 311 159, ... sont premiers.

■ **Notation** L'ensemble des nombres premiers est noté \mathcal{P} .

3.2 Propriétés

Proposition 21

Si $p \in \mathcal{P}$, alors p est premier avec tous les entiers qu'il ne divise pas. En particulier, si p est un nombre premier, on a :

$$\forall k \in [1, p - 1], k \wedge p = 1.$$

Démonstration Étant donné un entier naturel k non multiple de p , si d est un diviseur commun à k et à p , alors l'entier d est un diviseur de p différent de p donc est égal à 1 puisque p est premier. Par suite, k est premier avec p . □

Exemples

- Deux nombres premiers distincts sont premiers entre eux.
- Étant donné un nombre premier p , pour tout entier $k \in [1, p - 1]$, le coefficient binomial $\binom{p}{k}$ est divisible par p .

En effet, si $k \in [1, p - 1]$, la relation $\binom{p}{k} = \frac{p}{k} \binom{p-1}{k-1}$ s'écrit aussi $k \binom{p}{k} = p \binom{p-1}{k-1}$ et prouve donc que p divise $k \binom{p}{k}$.
 Comme p et k sont premiers entre eux, le théorème de Gauss entraîne $p \mid \binom{p}{k}$.

Corollaire 22

Un nombre premier divise un produit si, et seulement si, il divise l'un de ses facteurs.

Démonstration S'il ne divise aucun des facteurs, il est premier avec chacun d'entre eux et donc avec leur produit, ce qui prouve qu'il ne divise pas ce produit.

La réciproque est évidente. \square

Proposition 23

Tout entier naturel strictement supérieur à 1 admet un diviseur premier.

Démonstration Soit $n > 1$. L'ensemble des diviseurs de n strictement supérieurs à 1 est non vide puisqu'il contient n ; son plus petit élément p est un entier supérieur ou égal à 2. Or, tout diviseur de p est un diviseur de n , donc p n'a pas de diviseur strictement compris entre 1 et p , c'est-à-dire que p est premier. \square

Corollaire 24

Il y a une infinité de nombres premiers.

Démonstration Si n est un entier naturel, l'entier $N = 1 + n!$ admet un diviseur premier p (éventuellement lui-même). Si $p \leq n$, alors p divise N et $n!$ et donc leur différence 1, ce qui est impossible. Donc $p > n$.

On a montré que pour tout entier n , il existe un nombre premier p strictement supérieur à n , ce qui prouve que l'ensemble des nombres premiers est non majoré, donc infini. \square

3.3 Décomposition en produit de facteurs premiers

Théorème 25

Soit n un entier naturel supérieur ou égal à 2.

- Il admet une décomposition en facteurs premiers $n = q_1 q_2 \dots q_k$ où q_1, q_2, \dots, q_k sont des nombres premiers, décomposition que l'on peut encore écrire :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où p_1, p_2, \dots, p_r sont des nombres premiers distincts deux à deux, et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls.

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

Remarques

- Si $\{p_1, p_2, \dots, p_r\}$ est un ensemble de nombres premiers contenant tous les facteurs premiers de n , on peut encore écrire :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

en prenant $\alpha_i = 0$ si p_i n'est pas un diviseur de n .

- Avec cette convention, 1 peut aussi s'écrire sous cette forme en prenant tous les α_i nuls.
- Étant donnés deux entiers naturels a et b non nuls, on peut écrire :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

en utilisant les mêmes nombres premiers. Il suffit pour cela de prendre tous les facteurs premiers du produit ab .

MPSI

Démonstration du théorème 25.

Existence. Démontrons par récurrence la propriété H_n : "Tout entier naturel compris entre 2 et n admet une décomposition en facteurs premiers".

- H_2 est vérifiée puisque 2 est premier.
- Supposons H_{n-1} pour $n \geq 3$ et montrons que n admet une décomposition en facteurs premiers, ce qui prouvera H_n .
 - Si n est premier, alors c'est un produit d'un seul nombre premier.
 - Sinon, n admet un diviseur premier p . En posant $n = pq$, on a $1 < q < n$ et donc q est un produit de nombres premiers $q = q_1 q_2 \dots q_k$. Alors $n = p q_1 q_2 \dots q_k$ est aussi un produit de nombres premiers.

Unicité. Soit $n = q_1 q_2 \dots q_k$ une décomposition en facteurs premiers de n . Chaque nombre premier q_i divise n et réciproquement, si un nombre premier p divise n , alors il divise l'un des q_i donc lui est égal puisqu'il s'agit de deux nombres premiers (positifs). Les facteurs premiers intervenant dans une telle décomposition sont donc tous les diviseurs premiers de n .

Soient alors deux décompositions de n , que l'on peut donc écrire :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

où les p_i sont premiers et deux à deux distincts.

Si, pour un entier i , on a $\alpha_i \neq \beta_i$, par exemple $\alpha_i < \beta_i$, alors on a :

$$\prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i - \alpha_i} \prod_{j \neq i} p_j^{\beta_j}$$

et donc p_i divise $\prod_{j \neq i} p_j^{\alpha_j}$, ce qui est impossible puisque si $j \neq i$, les entiers p_i et p_j sont premiers entre eux.

Par suite $\forall i, \alpha_i = \beta_i$, ce qui montre l'unicité de la décomposition. □ MPSI

Exemples

1. $7007 = 7 \times 7 \times 11 \times 13$.

2. En MAPLE :

```
> ifactor(123456789);
```

$$(3)^2(3803)(3607)$$

MPSI

Proposition 26

Soient a et b deux entiers naturels non nuls. Si :

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

où p_1, p_2, \dots, p_k sont des nombres premiers distincts, alors on a :

1. $a \mid b \iff \forall i \in [1, k], \alpha_i \leq \beta_i$.

2. $a \wedge b = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}$ et $a \vee b = \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)}$.

Démonstration

1. Si $a \mid b$, alors pour tout $i \in [1, k]$, $p_i^{\alpha_i} \mid a$ et donc $p_i^{\alpha_i} \mid b$, ce qui montre $\alpha_i \leq \beta_i$. La réciproque est évidente.

2. Les diviseurs d communs à a et à b sont :

$$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} \quad \text{avec} \quad \forall i, \delta_i \leq \alpha_i \quad \text{et} \quad \delta_i \leq \beta_i.$$

Le plus grand des diviseurs communs à a et à b est donc obtenu lorsque :

$$\forall i, \delta_i = \min(\alpha_i, \beta_i),$$

ce qui montre la première égalité.

- Les multiples m communs à a et à b s'écrivent :

$$m = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k} \quad \text{avec} \quad \forall i, \mu_i \geq \alpha_i \text{ et } \mu_i \geq \beta_i.$$

Le plus petit des multiples communs à a et à b est donc obtenu lorsque :

$$\forall i, \mu_i = \max(\alpha_i, \beta_i),$$

ce qui montre la deuxième égalité. □

Exemples

1. Étant donné un entier naturel n non nul dont la décomposition en facteurs premiers est :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

les diviseurs d de n s'écrivent :

$$d = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k} \quad \text{avec} \quad \forall i, \delta_i \leq \alpha_i.$$

Un diviseur d est donc déterminé par le k -uplet $(\delta_1, \delta_2, \dots, \delta_k)$ élément de $E = [0, \alpha_1] \times \cdots \times [0, \alpha_k]$ et par suite le nombre de diviseurs positifs de n est

le cardinal de E , c'est-à-dire $\prod_{i=1}^k (1 + \alpha_i)$.

2. Étant donnés deux entiers naturels non nuls a et b , on retrouve la formule :

$$(a \wedge b)(a \vee b) = ab$$

puisque pour tout couple d'entiers (α, β) , on a :

$$\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta.$$

EXERCICES

1. Trouver le nombre d'entiers relatifs qui, dans la division euclidienne par 23, ont un quotient égal au reste.
2. Trouver la puissance de 2 dans la décomposition en produit de facteurs premiers du nombre $1000!$.
3. Montrer que l'équation $x^3 + x^2 + 2x + 1 = 0$ n'a pas de racines dans \mathbb{Q} .
4. Soit $n \in \mathbb{Z}$, quel est le PPCM de n et de $2n + 1$?
5. Montrer qu'il existe des intervalles de \mathbb{N} de longueur aussi grande que l'on veut qui ne contiennent aucun nombre premier.
6. Soit p un nombre premier.
 - a) Soit k un entier tel que $0 < k < p$.
Montrer que $\binom{p}{k}$ est divisible par p .
 - b) Soient a et b dans \mathbb{Z} , montrer que:

$$p \mid (a+b)^p - a^p - b^p.$$
 - c) En déduire que:

$$\forall m \in \mathbb{N}^*, \quad p \mid m^p - m.$$
 - d) Montrer que si m et p sont premiers entre eux alors:

$$p \mid m^{p-1} - 1.$$
7. Soient $n \in \mathbb{N}^*$ et $(a,b) \in \mathbb{Z}^2$.
 - a) Montrer que si a a pour reste r_1 dans la division euclidienne par n et b a pour reste r_2 dans la division euclidienne par n , alors $a + b$ a pour reste le reste de la division euclidienne de $r_1 + r_2$ par n et ab a pour reste le reste de la division euclidienne de r_1r_2 par n .
 - b) Quels sont les restes de la division euclidienne de 10^k par 9 ?
Expliquer le principe de la *preuve par 9*.
 - c) Expliquer le principe de la *preuve par 11*.

- 8.** On remarque que $1001 = 7 \times 11 \times 13$.

En déduire un critère de divisibilité par 13.

Si n s'écrit dans le système décimal $\overline{a_p a_{p-1} \dots a_1 a_0}$, on pourra considérer les nombres $\overline{a_2 a_1 a_0}$, $\overline{a_5 a_4 a_3}$, $\overline{a_8 a_7 a_6} \dots$

Donner également un critère de divisibilité par 7.

- 9.** Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Montrer que :

$$E\left(\frac{a}{b}\right) + E\left(\frac{a+1}{b}\right) + \dots + E\left(\frac{a+b-1}{b}\right) = a.$$

On déterminera les entiers $x \in \mathbb{Z}$ tels que $E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right)$ ainsi que ceux tels que $E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right) + 1$.

- 10.** Soit $n \in \mathbb{N}^*$ et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers.

a) Calculer le nombre de diviseurs positifs de n .

b) Calculer la somme $S(n)$ des diviseurs positifs de n .

c) Montrer que si m et n sont premiers entre eux alors $S(mn) = S(m)S(n)$.

- 11.** Trouver n de la forme $3^p 5^q$ sachant que le produit de ses diviseurs est 45^{42} .

- 12.** Soit $n \geq 2$ et $a \in \mathbb{Z}$ un entier premier avec n .

Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de a^k par n .

Montrer que la suite r_k est périodique.

Quel est le reste de la division euclidienne de 3^{2003} par 5 ?

Montrer que 13 divise $3^{126} + 5^{126}$.

- 13.** Soit n un entier avec $n \geq 2$.

Montrer que si $2^n - 1$ est premier, alors n est premier.

- 14.** Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier.

Montrer que m est de la forme $m = 2^n$ où $n \in \mathbb{N}$.

15. Soit $n \in \mathbb{N}^*$, on note $F_n = 2^{2^n} + 1$.

Montrer que si $n \neq m$ alors F_n et F_m sont premiers entre eux.

16. Soit p un nombre entier tel que $2^p - 1$ soit premier. On sait alors (voir exercice 13) que p est premier.

a) Montrer que le nombre $n = 2^{p-1}(2^p - 1)$ est parfait, c'est-à-dire que $2n = S(n)$ où $S(n)$ représente la somme de ses diviseurs.

b) Montrer que tout nombre parfait pair est de la forme $2^{p-1}(2^p - 1)$ où p est premier.



17. a) Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$.

b) Montrer qu'il existe une infinité de nombres premiers de la forme $6k + 5$.

18. Soit $n \in \mathbb{N}$ et p_n le $n^{\text{ème}}$ nombre premier.

a) Montrer que :

$$p_{n+1} \leq p_1 p_2 \dots p_n + 1.$$

b) En déduire que $p_n \leq 2^{2^n}$.

c) Soit $x \in \mathbb{R}_+$, on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x .

Montrer que pour x assez grand :

$$\ln(\ln x) \leq \pi(x) \leq x.$$

On utilisera le fait que pour $n \geq 3$, $e^{e^{n-1}} \geq 2^{2^n}$.

19. Montrer qu'il existe une application d de \mathbb{N}^* dans \mathbb{Z} et une seule telle que pour tout nombre premier p , $d(p) = 1$ et :

$$\forall (u, v) \in (\mathbb{N}^*)^2, \quad d(uv) = ud(v) + vd(u).$$

Résoudre l'équation $d(n) = n$.

20. a) Soient a et b deux entiers naturels tels que $0 < a < b$.

Montrer que :

$$(a+b) \wedge (a \vee b) = a \wedge b.$$

b) Trouver a et b tels que :

$$\begin{cases} a + b = 144 \\ a \vee b = 420. \end{cases}$$

21. Résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation :

$$x^y = y^x.$$

Chapitre 25

Polynômes

Dans tout ce chapitre, \mathbb{K} désigne le corps \mathbb{R} des réels ou le corps \mathbb{C} des complexes.

On rappelle que les éléments de \mathbb{K} sont appelés scalaires.

1. Ensemble des polynômes à coefficients dans \mathbb{K}

1.1 Polynômes

Construction

Définition 1

On appelle *polynôme à une indéterminée à coefficients dans \mathbb{K}* toute suite d'éléments de \mathbb{K} nulle à partir d'un certain rang.

■ Notations

- Si $A = (a_k)_{k \in \mathbb{N}}$ est un polynôme à coefficients dans \mathbb{K} , alors :

$$\exists n \in \mathbb{N} : \forall k > n, a_k = 0.$$

On note $A = (a_0, a_1, \dots, a_n, 0, 0, \dots)$, et les nombres a_0, a_1, \dots, a_n sont appelés coefficients du polynôme A .

- On désigne par 0 le polynôme nul, c'est-à-dire le polynôme $(0, 0, \dots)$

Si $A = (a_0, a_1, \dots, a_p, 0, 0, \dots)$ et $B = (b_0, b_1, \dots, b_q, 0, 0, \dots)$ sont deux polynômes, il est évident que pour $(\lambda, \mu) \in \mathbb{K}^2$, la suite $\lambda A + \mu B$ est nulle au moins à partir du rang $\max(p, q) + 1$. On en déduit immédiatement :

Proposition 1

L'ensemble des polynômes à coefficients dans \mathbb{K} est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$.

Produit de polynômes

Étant donnés $A = (a_k)_{k \in \mathbb{N}}$ et $B = (b_k)_{k \in \mathbb{N}}$ deux polynômes, on définit la suite $C = (c_n)_{n \in \mathbb{N}}$ en posant :

$$\forall k \in \mathbb{N}, c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Lemme

Si :

$$\forall k > p_0, a_k = 0 \quad \text{et} \quad \forall k > q_0, b_k = 0,$$

alors la suite C définie ci-dessus vérifie :

$$\forall k > p_0 + q_0, c_k = 0 \quad \text{et} \quad c_{p_0+q_0} = a_{p_0} b_{q_0}.$$

C'est donc un polynôme.

Démonstration En effet supposons $k \geq p_0 + q_0$.

Si (i, j) est un couple tel que $i + j = k$, on a $i \geq p_0$ ou $j \geq q_0$ (sinon $i + j < p_0 + q_0$).

Donc tous les termes de la somme $\sum_{i+j=k} a_i b_j$ sont nuls, sauf éventuellement celui correspondant

à $i = p_0$ et $j = q_0$.

- Si $k > p_0 + q_0$, alors il n'y a aucun terme non nul dans la somme et donc $c_k = 0$.
- Si $k = p_0 + q_0$, alors le seul terme qui reste est $a_{p_0} b_{q_0}$, qui est donc égal à $c_{p_0+q_0}$. □

Le polynôme C défini par :

$$\forall k \in \mathbb{N}, c_k = \sum_{i+j=k} a_i b_j.$$

est appelé *produit* de A par B et noté $A \times B$ ou AB .

On définit ainsi une loi de composition interne, appelée *multiplication*, sur l'ensemble des polynômes.

Anneau des polynômes

Proposition 2

Muni de l'addition et de la multiplication, l'ensemble des polynômes à coefficients dans \mathbb{K} est un anneau commutatif.

Démonstration

- C'est un sous-espace vectoriel, donc un sous-groupe additif, de $\mathbb{K}^{\mathbb{N}}$.
- La multiplication des polynômes :
 - est interne,
 - est commutative, car la formule donnant le coefficient générique du produit de deux polynômes est symétrique,
 - est associative, car si A , B et C sont trois polynômes, alors on a, en posant $D = A(BC)$:

$$d_n = \sum_{i+l=n} a_i \left(\sum_{j+k=l} b_j c_k \right) = \sum_{i+j+k=n} a_i b_j c_k,$$

et l'expression obtenue étant symétrique en A , B et C , on en déduit :

$$A(BC) = C(AB)$$

ce qui, en utilisant la commutativité, prouve :

$$A(BC) = C(AB) = (AB)C$$

- possède comme élément neutre le polynôme $(1, 0, 0, \dots)$,
- est distributive par rapport à l'addition (évident sur la formule donnant le coefficient générique du produit),

□

► **Attention** L'anneau des polynômes n'est pas un sous-anneau de $\mathbb{K}^{\mathbb{N}}$, car la multiplication des polynômes n'est pas la multiplication terme à terme des suites.

■ Notation définitive

En posant $X = (0, 1, 0, 0, \dots)$, on vérifie par récurrence sur $k \in \mathbb{N}$, quel l'on a :

$$X^k = (\underset{0}{\uparrow}, \underset{1}{\uparrow}, 0, \dots, 0, \underset{k}{\uparrow}, 0, \dots).$$

On peut alors écrire :

$$A = (a_0, a_1, \dots, a_r, 0, 0, \dots) = \sum_{k=0}^n a_k X^k.$$

Avec cette notation, on peut réécrire les propriétés vues précédemment.

- Le polynôme $A = \sum_{k=0}^n a_k X^k$ est nul si, et seulement si, tous les a_k sont nuls.
- Si $A = \sum_{k=0}^n a_k X^k$ et $B = \sum_{k=0}^m b_k X^k$, alors :

$$A + B = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$$

où, par convention, les a_k (respectivement les b_k) ne figurant pas dans l'écriture de A (respectivement de B) sont nuls.

- Si $A = \sum_{k=0}^n a_k X^k$ et $B = \sum_{k=0}^m b_k X^k$, alors :

$$AB = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) X^k = \sum_{i=0}^n \left(\sum_{j=0}^m a_i b_j X^{i+j} \right).$$

■ **Notation** On désigne par $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .

Remarque Dans certains cas, on peut être amené à écrire :

$$A = \sum_{k=0}^n a_k X^k = \sum_{k=0}^{\infty} a_k X^k.$$

Malgré son apparence, cette dernière somme est une somme finie car il n'y a qu'un nombre fini de coefficients a_k non nuls. Une telle écriture peut parfois s'avérer utile, notamment pour exprimer une somme de polynômes. Si l'on a :

$$A = \sum_{k=0}^{\infty} a_k X^k \quad \text{et} \quad B = \sum_{k=0}^{\infty} b_k X^k,$$

alors :

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

Définition 2

On appelle :

- *monôme*, tout polynôme du type λX^k ,
- *polynôme constant*, tout polynôme du type $(\lambda, 0, 0, \dots) = \lambda X^0$,

avec $\lambda \in \mathbb{K}$.

On identifie l'élément λ de \mathbb{K} avec le polynôme constant $(\lambda, 0, 0, \dots) = \lambda X^0$ ce qui permet d'écrire :

$$A = \sum_{k=0}^n a_k X^k = a_0 X^0 + a_1 X + \cdots + a_n X^n = a_0 + a_1 X + \cdots + a_n X^n.$$

1.2 Degré d'un polynôme

Lorsqu'un polynôme A n'est pas nul, l'ensemble $\{k \in \mathbb{N} \mid a_k \neq 0\}$ est une partie non vide de \mathbb{N} , majorée puisque la suite $(a_k)_{k \in \mathbb{N}}$ est nulle à partir d'un certain rang, et admettant donc un plus grand élément.

Définition 3

Soit $A = \sum_{k=0}^{\infty} a_k X^k$ un polynôme à coefficients dans \mathbb{K} , on définit le *degré* de A , noté $\deg(A)$ ou $\deg A$ par :

$$\deg(A) = \begin{cases} \max\{k \in \mathbb{N} \mid a_k \neq 0\} & \text{si } A \neq 0 \\ -\infty & \text{si } A = 0. \end{cases}$$

Remarques

- Un polynôme $A = \sum_{k=0}^n a_k X^k$ est de degré inférieur ou égal à n . Il est de degré n si, et seulement si, $a_n \neq 0$. Dans ce cas le coefficient a_n s'appelle le *coefficent dominant* du polynôme.
- Un polynôme (non nul) dont le coefficient dominant est égal à 1 est appelé *polynôme unitaire* ou *normalisé*.

Proposition 3

Étant donnés deux polynômes A et B de $\mathbb{K}[X]$, on a :

1. $\deg(A + B) \leq \max(\deg A, \deg B)$, avec égalité lorsque $\deg A \neq \deg B$,
2. $\deg(A B) = \deg A + \deg B$.

Démonstration

1. Si $A = B = 0$, alors $A + B = 0$ et le résultat est évident.

Sinon, posons $n = \max(\deg A, \deg B) \in \mathbb{N}$; on peut alors écrire :

$$A = \sum_{k=0}^n a_k X^k \quad \text{et} \quad B = \sum_{k=0}^n b_k X^k,$$

ce qui donne $A + B = \sum_{k=0}^n (a_k + b_k) X^k$ et prouve $\deg(A + B) \leq n$.

De plus, le terme de degré n est $a_n + b_n$. Si $\deg A \neq \deg B$, par exemple $\deg A < \deg B$, alors $a_n = 0$ et $b_n \neq 0$, et par suite $a_n + b_n \neq 0$, ce qui prouve que $A + B$ est de degré n .

2. Si $A = 0$ ou $B = 0$, alors $A B = 0$ et :

$$\deg(A B) = \deg(0) = -\infty = \deg A + \deg B$$

car avec l'extension des opérations arithmétiques sur $\overline{\mathbb{R}}$, on a pour tout $n \in \mathbb{N} \cup \{-\infty\}$:

$$n + (-\infty) = -\infty + n = -\infty.$$

Sinon, soit $p_0 = \deg A$ et $q_0 = \deg B$. Le lemme de la page 706 prouve que :

- les coefficients de $A B$ d'indice strictement supérieur à $p_0 + q_0$ sont nuls, ce qui donne $\deg(A B) \leq p_0 + q_0$,
- le coefficient de $A B$ d'indice $p_0 + q_0$ vaut $a_{p_0} b_{q_0}$ qui est donc non nul, puisque c'est le produit de deux éléments non nuls d'un corps. Donc $\deg(A B) = p_0 + q_0$. □

Remarques

- Si $\lambda \in \mathbb{K}$ et $A \in \mathbb{K}[X]$, alors :

$$\deg(\lambda A) = \begin{cases} \deg A & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0. \end{cases}$$

- Si $(\lambda, \mu) \in \mathbb{K}^2$ et $(A, B) \in \mathbb{K}[X]^2$, alors :

$$\deg(\lambda A + \mu B) \leq \max(\deg A, \deg B).$$

Corollaire 4

L'ensemble $\mathbb{K}_n[X]$ des polynômes de degré inférieur ou égal à n est un sous-espace vectoriel de $\mathbb{K}[X]$.

Démonstration Il contient le polynôme nul, et il est stable par combinaisons linéaires, puisqu'une combinaison linéaire de polynômes de degrés inférieurs ou égaux à n est de degré inférieur ou égal à n . \square

► **Attention** Si $n \geq 1$, le sous-espace vectoriel $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$ puisque $X^n \times X^n \notin \mathbb{K}_n[X]$.

Proposition 5

Dans l'anneau $(\mathbb{K}[X], +, \times)$, on a la propriété :

$$\forall (A, B) \in \mathbb{K}[X]^2, A B = 0 \implies (A = 0 \text{ ou } B = 0).$$

Démonstration En effet, la formule $\deg(A B) = \deg A + \deg B$ entraîne :

$$(A \neq 0 \text{ et } B \neq 0) \implies A B \neq 0. \quad \square$$

► **Remarque** On dit alors que l'anneau $(\mathbb{K}[X], +, \times)$ est *intègre* (voir page 1083).

Proposition 6

Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0.

Démonstration

- Si A est un polynôme de degré 0, c'est-à-dire une constante non nulle λ , le polynôme constant λ^{-1} est l'inverse de A .
- Réciproquement, si A est un polynôme inversible, c'est-à-dire tel qu'il existe $B \in \mathbb{K}[X]$ vérifiant $A B = 1$, alors A et B sont non nuls et l'on a :

$$0 = \deg(1) = \deg(A B) = \deg A + \deg B.$$

Comme $\deg A$ et $\deg B$ sont des entiers naturels, on en déduit $\deg A = 0$. \square

1.3 Substitution

Fonction polynomiale

Définition 4

Soit $A = \sum_{k=0}^{\infty} a_k X^k$ un élément de $\mathbb{K}[X]$.

- Pour $\alpha \in \mathbb{K}$, on définit :

$$A(\alpha) = \sum_{k=0}^{\infty} a_k \alpha^k = \sum_{k=0}^n a_k \alpha^k \text{ pour tout } n \geq \deg A.$$

- La fonction définie sur \mathbb{K} par $x \mapsto A(x)$ est appelée *fonction polynomiale* associée au polynôme A .

Remarque Pour obtenir $A(\alpha)$, on dit que l'on substitue α à X , ou que l'on remplace X par α .

Proposition 7

Étant donnés deux éléments A et B de $\mathbb{K}[X]$ ainsi que trois scalaires α , λ et μ , on a :

1. $(\lambda A + \mu B)(\alpha) = \lambda A(\alpha) + \mu B(\alpha)$,
2. $(A B)(\alpha) = A(\alpha) B(\alpha)$.

Démonstration La linéarité de $A \mapsto A(\alpha)$ est évidente.

Pour le produit, si $A = \sum_{k=0}^n a_k X^k$ et $B = \sum_{l=0}^m b_l X^l$, alors :

$$AB = \sum_{k=0}^n \sum_{l=0}^m a_k b_l X^{k+l}$$

et, d'après la linéarité de l'application $P \mapsto P(\alpha)$:

$$\begin{aligned} (AB)(\alpha) &= \sum_{k=0}^n \sum_{l=0}^m a_k b_l \alpha^{k+l} \\ &= \left(\sum_{k=0}^n a_k \alpha^k \right) \left(\sum_{l=0}^m b_l \alpha^l \right) \\ &= A(\alpha) B(\alpha). \end{aligned}$$

Il faut remarquer que la définition du produit sur $\mathbb{K}[X]$ a justement été choisie pour avoir ce résultat. \square

Algorithme de Horner

En informatique, pour calculer la valeur en α du polynôme $A = \sum_{i=0}^n a_i X^i$, on utilise habituellement l'*algorithme de Horner* consistant à calculer :

$$A(\alpha) = a_0 + (a_1 + (a_2 + \cdots + (a_{n-2} + (a_{n-1} + a_n \alpha) \alpha) \alpha \cdots) \alpha) \alpha$$

qui nécessite bien moins d'opérations (n multiplications) que l'algorithme naïf calculant toutes les puissances de α (qui nécessite $n(n+1)/2$ multiplications).

Cet algorithme s'écrit :

DONNÉES : La liste (a_0, a_1, \dots, a_n) des coefficients du polynôme.
Le scalaire α .

VARIABLES : Le compteur de boucle k , le scalaire *Résultat*.

- $Résultat \leftarrow 0$
 - Pour k allant de n jusqu'à 0 par pas de -1 :

$$Résultat \leftarrow a_k + Résultat * \alpha$$

RÉSULTAT : *Résultat.*

Exemple avec MAPLE

```

> A:=X^4+3*X^3+2*X^2+X+1;
           $A := X^4 + 3X^3 + 2X^2 + X + 1$ 

> A1:=subs(X=alpha,A);
           $A1 := \alpha^4 + 3\alpha^3 + 2\alpha^2 + \alpha + 1$ 

> convert(A1,horner,alpha);
           $1 + (1 + (2 + (3 + \alpha)\alpha)\alpha)\alpha$ 

```

Exponentiation rapide

L'algorithme de Horner permet de limiter le nombre de multiplications à n pour calculer la valeur d'une fonction polynomiale de degré n . Cependant, pour un monôme, on peut faire encore mieux.

En effet, pour calculer α^n , on peut naïvement effectuer $n - 1$ multiplications :

$$\alpha^n = \underbrace{\alpha \times \alpha \times \cdots \times \alpha}_{n \text{ fois}}.$$

montre que l'on peut faire beaucoup mieux (ici 10 multiplications au lieu de 1023).

L'algorithme d'exponentiation rapide part de la remarque :

- si $n = 0$, alors $\alpha^n = 1$,
 - si $n = 2p$, alors $\alpha^n = (\alpha^p)^2$,
 - si $n = 2p + 1$, alors $\alpha^n = (\alpha^p)^2 \times \alpha$.

Le calcul de α^n peut donc se faire à l'aide de la fonction (réursive) MAPLE suivante :

```
> puiss:=(alpha,n)->
  if n=0 then
    RETURN(1)
  elif (n mod 2) = 1 then
    RETURN(puiss(alpha,iquo(n,2))^2*alpha)
  else
    RETURN(puiss(alpha,iquo(n,2))^2)
  fi:
puiss(2,560);

377396242482154135224155458098826889091692122\
041644042837620630024562416239214885208\
612672517765876754146837503076384489977\
058462992479263256143425143269604364939\
5326976
```

Remarques

- Notons M_n le nombre de multiplications (ou d'élévation au carré) effectuées dans cet algorithme lors du calcul de α^n , et montrons par récurrence sur k la propriété $H_k : 2^{k-1} \leq n < 2^k \Rightarrow k \leq M_n \leq 2k$.
 - H_1 est évident puisque $M_1 = 2$.
 - Supposons H_k , pour $k \geq 1$. Soit $2^k \leq n < 2^{k+1}$.
 - ★ Si $n = 2p$, on a $2^{k-1} \leq p < 2^k$ et donc $k \leq M_p \leq 2k$.
On a de plus $M_n = 1 + M_p$, ce qui donne bien $k + 1 \leq M_n \leq 2(k + 1)$.
 - ★ Si $n = 2p + 1$, on a $2^{k-1} \leq p + \frac{1}{2} < 2^k$ et comme p est un entier, $2^{k-1} \leq p < 2^k$. Donc $k \leq M_p \leq 2k$.
On a de plus $M_n = 2 + M_p$, qui donne bien $k + 1 \leq M_n \leq 2(k + 1)$.
- D'où H_{k+1} .
- Le nombre de multiplications effectuées est donc équivalent à $\lg n$, où \lg représente le logarithme en base 2.
- Plus précisément, on peut montrer que si l'écriture de n en base 2 comporte k chiffres dont ℓ égaux à 1, alors $M_n = k + \ell$.

Composition des polynômes

Définition 5

Étant donnés $A = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$, on définit :

$$A \circ P = A(P) = \sum_{k=0}^{\infty} a_k P^k = \sum_{k=0}^n a_k P^k \quad \text{pour tout } n \geq \deg A.$$

Remarques

1. Dans le cas particulier où $P = X$, le polynôme $A(P) = A(X)$ est donc égal à A , c'est pourquoi on utilise aussi bien A que $A(X)$ pour désigner ce polynôme.
2. Si A et P sont non nuls, on a $\deg(A \circ P) = \deg(A) \deg(P)$.
3. On a des résultats analogues à ceux de la proposition 7 de la page 712 :

$$(\lambda A + \mu B)(P) = \lambda A(P) + \mu B(P)$$

$$(AB)(P) = A(P)B(P)$$

et ils se démontrent de façon similaire.

4. Comme pour le calcul d'une valeur numérique, il est préférable d'utiliser le schéma de Horner pour développer le polynôme $A \circ P$. Pour s'en convaincre il suffit de comparer, sous MAPLE (à l'aide de la fonction `time`), les temps d'exécution des lignes suivantes :

```
> A:=expand((1+X)^100):
> expand(subs(X=1+u^2,A)):
> A1:=convert(A,horner,X):
> expand(subs(X=1+u^2,A1)):
```

On trouve sur cet exemple que la conversion au schéma de Horner (dont le temps d'exécution est négligeable) apporte une amélioration approximativement d'un facteur 10 dans le temps de calcul.

Exemples

1. Un polynôme A est *pair* si $A(-X) = A(X)$.

Si $A = \sum_{n=0}^{+\infty} a_n X^n$, on a $A(-X) = \sum_{n=0}^{+\infty} (-1)^{-n} a_n X^n$.

Donc A est pair si, et seulement si, $\forall n \in \mathbb{N}$, $a_{2n+1} = 0$ c'est-à-dire si, et seulement si, A est combinaison linéaire de puissances paires de X .

- De même un polynôme A est *impair*, c'est-à-dire vérifie $A(-X) = -A(X)$, si, et seulement si, il est combinaison linéaire de puissances impaires de X .

2. Divisibilité dans $\mathbb{K}[X]$

2.1 Multiples, diviseurs

Définition 6

Soient A et B deux polynômes de $\mathbb{K}[X]$. On dit que A *divise* B ou que B est *multiple* de A si $\exists C \in \mathbb{K}[X] : AC = B$.

On note alors $A | B$.

Exemples

- Le polynôme $(X - 1)(X - 2)$ divise $(X - 1)^2(X - 2)(X^2 + X + 1)$.
- Le polynôme 0 est divisible par tous les polynômes mais il ne divise que lui-même.
- Si $A | B$ avec B non nul, alors $\deg B \geq \deg A$, car on a $B = AC$ avec $C \neq 0$, et donc $\deg B = \deg A + \deg C \geq \deg A$.
- La relation $A | B$ est réflexive et transitive, mais elle n'est pas antisymétrique lorsque $\mathbb{K} \neq \{0, 1\}$ car si $\lambda \in \mathbb{K} \setminus \{0, 1\}$, on a par exemple $X | \lambda X$ et $\lambda X | X$. Ce n'est donc pas une relation d'ordre.

Proposition 8

Étant donnés deux polynômes A et B il est équivalent de dire:

- (i) A divise B et B divise A .
- (ii) Il existe un scalaire $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

Dans ce cas, A et B sont dits *associés*.

Démonstration

(i) \implies (ii). Avec l'hypothèse (i), on peut trouver C_1 et C_2 tels que :

$$B = A C_1 \quad \text{et} \quad A = B C_2$$

et donc $A = A C_1 C_2$.

- Si $A = 0$, alors la relation $B = A C_1$ prouve que $B = 0$, et donc toute valeur $\lambda \in \mathbb{K}^*$ convient.
- Si $A \neq 0$, on peut simplifier par A , car $\mathbb{K}[X]$ est intègre, ce qui donne $C_1 C_2 = 1$. D'après la proposition 6 de la page 711, on en déduit que C_2 est un polynôme de degré 0, c'est-à-dire une constante non nulle.

(ii) \implies (i). Évident. □

Remarque La relation de divisibilité restreinte à l'ensemble des polynômes unitaires est une relation d'ordre. En effet, d'après la proposition précédente, deux polynômes unitaires associés sont égaux, ce qui prouve l'antisymétrie.

2.2 Division euclidienne sur $\mathbb{K}[X]$

Théorème 9

Étant donnés deux polynômes A et B de $\mathbb{K}[X]$ avec $B \neq 0$, il existe un unique couple (Q, R) de polynômes de $\mathbb{K}[X]$ vérifiant :

$$A = B Q + R \quad \text{avec} \quad \deg R < \deg B.$$

Q est appelé le *quotient* et R le *reste* de la division euclidienne de A par B .

Démonstration

Unicité. Supposons qu'il existe deux couples (Q_1, R_1) et (Q_2, R_2) vérifiant :

$$A = B Q_1 + R_1 \quad \text{avec} \quad \deg R_1 < \deg B,$$

$$A = B Q_2 + R_2 \quad \text{avec} \quad \deg R_2 < \deg B.$$

On a alors :

$$(Q_1 - Q_2) B = R_2 - R_1.$$

Si $Q_1 \neq Q_2$, alors :

$$\deg(R_2 - R_1) = \deg((Q_1 - Q_2) B) = \deg(Q_1 - Q_2) + \deg B \geq \deg B$$

et :

$$\deg(R_2 - R_1) \leq \max(\deg R_1, \deg R_2) < \deg B$$

ce qui est contradictoire. Donc $Q_1 = Q_2$ et par suite $R_1 = R_2$.

Existence. $B = \sum_{k=0}^m b_k X^k$ étant fixé, avec $b_m \neq 0$, démontrons par récurrence sur n

la propriété H_n : pour tout polynôme A de degré strictement inférieur à n , il existe un couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = B Q + R$ avec $\deg R < m$.

► H_m est vraie car si $\deg A < m$, il suffit de prendre $R = A$ et $Q = 0$.

► Supposons H_n pour $n \geq m$, et démontrons H_{n+1} .

Si $A \in \mathbb{K}[X]$ est de degré strictement plus petit que $n + 1$, alors $A = \sum_{k=0}^n a_k X^k$ est le polynôme :

$$A_1 = A - a_n b_m^{-1} X^{n-m} B \quad (a)$$

appartient à $\mathbb{K}_{n-1}[X]$. On peut donc lui appliquer l'hypothèse de récurrence et trouver un couple (Q_1, R) tel que :

$$A_1 = B Q_1 + R \quad \text{avec} \quad \deg R < m. \quad (b)$$

En posant :

$$Q = Q_1 + a_n b_m^{-1} X^{n-m}$$

et en utilisant (a) et (b), on a :

$$A = B Q + R \quad \text{avec} \quad \deg R < m.$$

□

Exemples

1. Le reste de la division euclidienne de A par $X - \alpha$ est un polynôme de degré strictement inférieur à 1, degré de $X - \alpha$, et donc une constante λ . En désignant par Q le quotient, on a alors $A = (X - \alpha) Q(X) + \lambda$.

Si l'on remplace X par α dans cette dernière relation, les résultats de la proposition 7 de la page 712 donnent $\lambda = A(\alpha)$.

2. Le polynôme B divise A si, et seulement si, le reste de la division de A par B est 0. En effet :

- si le reste est nul, on a $A = B Q$,
- si B divise A , il existe un polynôme Q tel que $A = B Q$ et l'unicité de la division euclidienne prouve que Q et 0 sont respectivement les quotient et reste de la division de A par B .

3. En MAPLE, ce sont les fonctions `quo` et `rem` qui permettent de déterminer le quotient et le reste d'une division euclidienne.

> $A := X^5 + 4X^4 + 2X^3 + X^2 - X - 1;$

$$A := X^5 + 4X^4 + 2X^3 + X^2 - X - 1$$

> $B := X^3 - 2X + 3;$

$$B := X^3 - 2X + 3$$

> quo(A,B,X); rem(A,B,X);

$$X^2 + 4X + 4$$

$$6X^2 - 5X - 13$$

Remarque Soit $(A, B) \in \mathbb{R}[X]^2$, avec $B \neq 0$. Effectuons la division euclidienne de A par B dans $\mathbb{R}[X]$:

$$A = BQ + R \quad \text{avec} \quad (Q, R) \in \mathbb{R}[X] \quad \text{et} \quad \deg R < \deg B. \quad (*)$$

Les polynômes Q et R sont aussi dans $\mathbb{C}[X]$ et la relation $(*)$ ainsi que l'unicité de la division euclidienne montrent que ce sont aussi les quotient et reste de la division euclidienne dans $\mathbb{C}[X]$ de A par B .

En particulier, B divise A dans $\mathbb{R}[X]$ si, et seulement si, il divise A dans $\mathbb{C}[X]$.

Algorithme de la division euclidienne

La démonstration d'existence de la proposition précédente fournit une méthode pour déterminer le quotient et le reste d'une division euclidienne. On a l'habitude de poser les calculs comme suit :

$$\begin{array}{lll} A = & X^5 + 4X^4 + 2X^3 + X^2 - X - 1 & \left| \begin{array}{c} X^3 - 2X + 3 \\ X^2 + 4X + 4 \end{array} \right. = B \\ A_1 = A - X^2 B = & 4X^4 + 4X^3 - 2X^2 - X - 1 & = Q \\ A_2 = A_1 - 4X B = & 4X^3 + 6X^2 - 13X - 1 & \\ A_3 = A_2 - 4B = R = & 6X^2 - 5X - 13 & \end{array}$$

La programmation de la division euclidienne utilise l'algorithme suivant.

DONNÉES : Le polynôme A de degré n .

Le polynôme B de degré m et de coefficient dominant $b_m \neq 0$.

VARIABLES : Le compteur de boucle k .

Les polynômes Q et R .

- $Q \leftarrow 0 ; R \leftarrow A$
- Pour k allant de $n - m$ jusqu'à 0 par pas de -1 :
 - (*On a $\deg R \leq k + m$ *)
 - $q_k \leftarrow r_{k+m}/b_m$
 - $R \leftarrow R - q_k X^k B$ (* r_{k+m} est donc nul *)

RÉSULTAT : (Q, R) .

Remarque Si $n < m$, la boucle n'est pas exécutée et alors le résultat est $(0, A)$.

3. Racines d'un polynôme

3.1 Racines

Soit A un polynôme à coefficients dans \mathbb{K} .

Définition 7

Un élément α de \mathbb{K} est *racine* du polynôme A si $A(\alpha) = 0$.

Proposition 10

Un élément α de \mathbb{K} est racine de A si, et seulement si, $(X - \alpha)$ divise A .

Démonstration Le polynôme $(X - \alpha)$ divise A si, et seulement si, $A(\alpha)$, reste de la division euclidienne de A par $(X - \alpha)$, est nul (cf. exemples 1. et 2. de la page 718). \square

Proposition 11

Si $\alpha_1, \alpha_2, \dots, \alpha_p$ sont p racines distinctes de A , alors A est divisible par $\prod_{i=1}^p (X - \alpha_i)$.

Démonstration Démontrons par récurrence sur p qu'un polynôme qui admet p racines distinctes $\alpha_1, \alpha_2, \dots, \alpha_p$ est divisible par $\prod_{i=1}^p (X - \alpha_i)$.

- C'est vrai pour $p = 1$ d'après la proposition précédente.
- Supposons le résultat vrai pour p et démontrons-le pour $p + 1$. Soient $\alpha_0, \alpha_1, \dots, \alpha_p$, $p + 1$ racines distinctes d'un polynôme A .

D'après l'hypothèse de récurrence, il existe un polynôme $B_1 \in \mathbb{K}[X]$ tel que :

$$A = B_1 \prod_{i=1}^p (X - \alpha_i).$$

Comme α_0 est racine de A , on a :

$$B_1(\alpha_0) \prod_{i=1}^p (\alpha_0 - \alpha_i) = 0,$$

ce qui prouve $B_1(\alpha_0) = 0$ puisque $\prod_{i=1}^p (\alpha_0 - \alpha_i) \neq 0$. Il existe donc un polynôme B_2 tel que :

$$B_1 = (X - \alpha_0) B_2$$

c'est-à-dire :

$$A = B_2 \prod_{i=1}^p (X - \alpha_i).$$

□

Corollaire 12

Un polynôme non nul de degré n admet au plus n racines distinctes.

Démonstration Si A est un polynôme non nul admettant p racines distinctes $\alpha_1, \alpha_2, \dots, \alpha_p$, la proposition 11 de la page ci-contre montre qu'il est divisible par $\prod_{i=1}^p (X - \alpha_i)$. On a donc $p \leq \deg A$.

□

Remarque On utilise souvent le corollaire précédent pour démontrer qu'un polynôme est nul :

- soit en exhibant $n + 1$ racines lorsque l'on sait que $\deg A \leq n$,
- soit, plus radicalement, en exhibant une infinité de racines de A .

Exemples

1. Étant donné $n \in \mathbb{N}$, on sait (cf. page 33) qu'il existe un polynôme A tel que :

$$\forall x \in \mathbb{R}, A(\cos x) = \cos(nx).$$

Montrons son unicité. S'il existe deux tels polynômes A et B , on a alors :

$$\forall x \in \mathbb{R}, A(\cos x) = B(\cos x)$$

et comme la fonction cosinus a pour image $[-1, 1]$:

$$\forall u \in [-1, 1], (A - B)(u) = 0.$$

Le polynôme $A - B$ possède donc une infinité de racines, et par suite $A = B$.

2. La fonction exponentielle complexe n'est pas polynomiale. En effet, s'il existait un polynôme $A \in \mathbb{C}[X]$ tel que $\forall z \in \mathbb{C}, A(z) = e^z$, alors le polynôme $A - 1$ posséderait pour racines tous les complexes de la forme $2ik\pi$ ($k \in \mathbb{Z}$), et donc serait nul. On aurait alors $A = 1$, ce qui est impossible puisque, par exemple, $e^{i\pi} = -1$.

Corollaire 13

Si A est de degré n et admet n racines distinctes $\alpha_1, \alpha_2, \dots, \alpha_n$, alors :

$$A = \lambda \prod_{i=1}^n (X - \alpha_i)$$

où λ est le coefficient dominant de A .

Démonstration D'après la proposition 11 de la page 720, il existe un polynôme Q tel que :

$$A = Q \prod_{i=1}^n (X - \alpha_i)$$

Comme les polynômes A et $\prod_{i=1}^n (X - \alpha_i)$ sont de même degré n , le polynôme Q est de degré 0

donc $Q = \lambda \in \mathbb{K}^*$, et le coefficient dominant de A est alors λ . □

Exemple Pour $n \in \mathbb{N}^*$, le polynôme unitaire $X^n - 1$ possède n racines qui sont les n racines n èmes de l'unité. On a donc :

$$X^n - 1 = \prod_{k=1}^n \left(X - \exp\left(\frac{2ik\pi}{n}\right) \right).$$

3.2 Identification entre polynôme et fonction polynomiale

■ **Notation** Si A est un élément de $\mathbb{K}[X]$, on note \tilde{A} sa fonction polynomiale associée :

$$\begin{aligned} \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\longmapsto A(x). \end{aligned}$$

Proposition 14

L'application $A \mapsto \tilde{A}$ est un morphisme injectif d'espaces vectoriels de $\mathbb{K}[X]$ dans $\mathcal{F}(\mathbb{K}, \mathbb{K})$, dont l'image s'appelle ensemble des fonctions polynomiales.

Démonstration C'est évidemment une application linéaire, donc pour démontrer son injectivité, il suffit de prouver que son noyau est réduit à $\{0\}$.

Soit $A \in \mathbb{K}[X]$ tel que $\tilde{A} = \mathbf{0}$. On a alors :

$$\forall x \in \mathbb{K}, \quad A(x) = \tilde{A}(x) = \mathbf{0}$$

et le polynôme A possède comme racines tous les éléments de \mathbb{K} , donc une infinité. Par suite $A = 0$. □

Méthode Pour démontrer que deux polynômes sont égaux, il suffit de montrer que leurs fonctions polynomiale coïncident sur \mathbb{K} , voire même sur une partie infinie de \mathbb{K} .

Remarques

- La démonstration précédente utilise le fait que le corps \mathbb{K} , égal à \mathbb{R} ou à \mathbb{C} , est infini.
- On sait, d'après la proposition 7 de la page 712, que l'application $A \mapsto \bar{A}$ est un morphisme d'anneaux. L'ensemble des fonctions polynomiales est donc un anneau isomorphe à $\mathbb{K}[X]$. Il en a donc toutes les propriétés algébriques, et en particulier il est intègre.
- Par conséquent, un produit de deux fonctions polynomiales est nul si, et seulement si, l'une des deux fonctions est nulle, ce résultat étant évidemment faux pour des fonctions quelconques.
- Si l'on définit l'anneau des polynômes à coefficients dans un corps (commutatif) quelconque de la même façon que sur \mathbb{R} ou \mathbb{C} , tous les résultats précédents subsistent excepté la proposition 14 de la page précédente qui ne reste vraie que dans le cas d'un corps infini.
- Lorsque le corps est fini, si l'on note a_1, a_2, \dots, a_n ses éléments, le polynôme $\prod_{i=1}^n (X - a_i)$ est non nul puisque de degré n , alors que sa fonction polynomiale associée est nulle.

3.3 Racines multiples

Soit A un polynôme non nul.

Définition 8

Étant donnés un scalaire α et un entier naturel p non nul, on dit que α est :

- racine d'ordre au moins p de A , si $(X - \alpha)^p \mid A$.
- racine d'ordre p de A , si α est racine d'ordre au moins p mais pas $p + 1$.
L'entier p est alors appelé ordre de multiplicité de la racine α .
- racine multiple de A , si α est racine d'ordre au moins 2 de A .

Remarques

- Une racine de A est racine d'ordre au moins 1 de A .

- Si α est une racine d'un polynôme non nul A de degré n , le polynôme $(X - \alpha)^{n+1}$ ne divise pas A , ce qui prouve l'existence d'un plus grand entier p tel que $(X - \alpha)^p$ divise A . Comme cet entier est évidemment unique, on peut donc bien définir l'ordre de multiplicité de la racine α ; c'est un entier inférieur ou égal à n .
- Par extension, on dit que α est racine d'ordre 0 de A si α n'est pas racine de A .
- Les racines d'ordre 1, 2, 3, ... sont respectivement appelées *racines simples, doubles, triples, ...*

Proposition 15

Soient α une racine d'ordre au moins p d'un polynôme non nul A , et $B \in \mathbb{K}[X]$ tel que $A = (X - \alpha)^p B$.

Alors α est racine d'ordre p du polynôme A si, et seulement si, $B(\alpha) \neq 0$.

Démonstration Il suffit de démontrer que α est racine de A d'ordre au moins $p + 1$ si, et seulement si, $B(\alpha) = 0$.

- Si $B(\alpha) = 0$, on peut trouver un polynôme B_1 tel que $B(X) = (X - \alpha)B_1(X)$, et donc :

$$A(X) = (X - \alpha)^{p+1} B_1(X)$$

ce qui signifie que α est une racine de A d'ordre au moins $p + 1$.

- Réciproquement si α est racine de A , d'ordre au moins $p + 1$, alors $(X - \alpha)^{p+1}$ divise A et on peut trouver un polynôme $B_1 \in \mathbb{K}[X]$ tel que :

$$(X - \alpha)^{p+1} B_1(X) = A(X) = (X - \alpha)^p B(X).$$

L'anneau $\mathbb{K}[X]$ étant intègre et $(X - \alpha)^p$ n'étant pas le polynôme nul, on en déduit $(X - \alpha)B_1(X) = B(X)$ et donc $B(\alpha) = 0$. □

Exemple Une racine simple (racine d'ordre 1) du polynôme A est donc caractérisée par :

$$\exists B \in \mathbb{K}[X] : A(X) = (X - \alpha)B(X) \quad \text{avec} \quad B(\alpha) \neq 0.$$

Proposition 16

Soit A un polynôme non nul de $\mathbb{K}[X]$. Si $\alpha_1, \alpha_2, \dots, \alpha_p$ sont p racines distinctes de A d'ordre respectivement au moins égal à r_1, r_2, \dots, r_p , alors A est divisible par $\prod_{i=1}^p (X - \alpha_i)^{r_i}$.

Démonstration

- Si $p = 1$, la propriété est vraie par définition de l'ordre d'une racine.
- Supposons la propriété vraie au rang p et considérons $\alpha_0, \alpha_1, \dots, \alpha_p$, $p+1$ racines distinctes de A d'ordre respectivement au moins égal à r_0, r_1, \dots, r_p .

D'après l'hypothèse de récurrence, il existe un polynôme $B_1 \in \mathbb{K}[X]$ tel que :

$$A = B_1 \prod_{i=1}^p (X - \alpha_i)^{r_i}.$$

Soit r l'unique entier (éventuellement nul) tel que :

$$B_1 = (X - \alpha_0)^r B \quad \text{avec} \quad B(\alpha_0) \neq 0.$$

En posant $B_2 = B \prod_{i=1}^p (X - \alpha_i)^{r_i}$, on a :

$$A = (X - \alpha_0)^r B_2 \quad \text{avec} \quad B_2(\alpha_0) \neq 0.$$

Donc α_0 est racine de A d'ordre r , ce qui prouve $r \geq r_0$. Par suite, le polynôme $\prod_{i=0}^p (X - \alpha_i)^{r_i}$ divise $(X - \alpha_0)^r \prod_{i=1}^p (X - \alpha_i)^{r_i}$ et donc aussi A .

On a ainsi montré la propriété au rang $p + 1$. □

Lorsque l'on dénombre les racines d'un polynôme, on peut :

- soit compter le nombre de racines distinctes,
- soit compter chaque racine avec (c'est-à-dire autant de fois que) son ordre de multiplicité ; dans ce cas, une racine d'ordre r compte comme r racines.

Exemple Le polynôme $(X - 1)(X + 1)^2(X - 2)^3$ possède :

- 3 racines distinctes : $-1, 1, 2$
- 6 racines comptées avec leur ordre de multiplicité : $-1, -1, 1, 2, 2, 2$.

De même que pour les racines distinctes, on a les deux résultats suivants, qui se démontrent de manière analogue :

Corollaire 17

Un polynôme non nul de degré n possède au plus n racines comptées avec leur ordre de multiplicité.

Corollaire 18

Soit A un polynôme non nul de $\mathbb{K}[X]$. Si $\alpha_1, \alpha_2, \dots, \alpha_p$ sont p racines distinctes de A , d'ordre respectivement égal à r_1, r_2, \dots, r_p et

si $\deg A = \sum_{k=1}^p r_k$, alors :

$$A = \lambda \prod_{i=1}^p (X - \alpha_i)^{r_i}$$

où λ est le coefficient dominant de A .

3.4 Polynômes scindés, fonctions symétriques élémentaires**Définition 9**

Un polynôme A non nul est *scindé* sur \mathbb{K} s'il peut s'écrire sous la forme :

$$A = \lambda \prod_{i=1}^n (X - \alpha_i)$$

où $\lambda, \alpha_1, \alpha_2, \dots, \alpha_n$ sont des scalaires.

Exemples

1. Un polynôme de degré n qui admet n racines distinctes dans \mathbb{K} est scindé sur \mathbb{K} .
2. Un polynôme de degré n qui admet n racines dans \mathbb{K} comptées avec leur ordre de multiplicité est scindé sur \mathbb{K} .
3. Réciproquement, si $A = \lambda \prod_{i=1}^n (X - \alpha_i)$ est scindé sur \mathbb{K} , alors les racines de A dans \mathbb{K} sont les α_i , et il y en a n comptées avec leur ordre de multiplicité.

Soit $A = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ un polynôme scindé sur \mathbb{K} avec $a_n \neq 0$. On peut écrire :

$$A = a_n (X - x_1)(X - x_2) \dots (X - x_n)$$

$$= a_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^p \sigma_p X^{n-p} + \dots + (-1)^n \sigma_n)$$

avec :

$$\sigma_p = \sum_{i_1 < i_2 < \dots < i_p} x_{i_1} x_{i_2} \dots x_{i_p}$$

et en particulier :

$$\begin{aligned}\sigma_1 &= \sum_{i=1}^n x_i = x_1 + x_2 + \cdots + x_n \\ \sigma_2 &= \sum_{i < j} x_i x_j = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ \sigma_n &= \prod_{i=1}^n x_i = x_1 x_2 \dots x_n.\end{aligned}$$

Définition 10

Les quantités σ_i sont appelées *fonctions symétriques élémentaires* des racines du polynôme A .

Exemples

1. Pour $n = 2$, si :

$$A = a_2 X^2 + a_1 X + a_0 = a_2(X - x_1)(X - x_2).$$

il y a deux fonctions symétriques élémentaires :

$$\begin{aligned}\sigma_1 &= x_1 + x_2 = -\frac{a_1}{a_2} \\ \sigma_2 &= x_1 x_2 = \frac{a_0}{a_2}\end{aligned}$$

2. Pour $n = 3$, si :

$$A = a_3 X^3 + a_2 X^2 + a_1 X + a_0 = a_3(X - x_1)(X - x_2)(X - x_3),$$

il y a trois fonctions symétriques élémentaires :

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3 = -\frac{a_2}{a_3} \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{a_1}{a_3} \\ \sigma_3 &= x_1 x_2 x_3 = -\frac{a_0}{a_3}\end{aligned}$$

Plus généralement, les égalités :

$$\begin{aligned}A &= a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \\ &= a_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^p \sigma_p X^{n-p} + \cdots + (-1)^n \sigma_n)\end{aligned}$$

permettent d'exprimer les fonctions symétriques élémentaires des racines du polynôme A en fonction des coefficients de A .

$$\boxed{\sigma_1 = -\frac{a_{n-1}}{a_n} \quad \sigma_2 = \frac{a_{n-2}}{a_n} \quad \cdots \quad \sigma_r = (-1)^r \frac{a_{n-r}}{a_n} \quad \cdots \quad \sigma_n = (-1)^n \frac{a_0}{a_n}}$$

Il faut savoir que toute expression polynomiale symétrique en les racines d'un polynôme peut s'exprimer de façon polynomiale à l'aide des fonctions symétriques élémentaires et donc des coefficients du polynôme.

Exemples

1. Si x_1, x_2, x_3 sont les trois racines complexes d'une équation $x^3 + px + q = 0$, on a :

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_1 x_3 + x_2 x_3) \\ &= \sigma_1^2 - 2\sigma_2 = -2p. \end{aligned}$$

2. Si x_1, x_2, x_3 sont les trois racines complexes d'une équation $x^3 + px + q = 0$, avec $q \neq 0$, le calcul de :

$$\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$$

est plus simple si l'on commence par écrire :

$$\begin{aligned} (x_1 - x_2)^2 &= (x_1 + x_2)^2 - 4x_1 x_2 \\ &= x_3^2 + 4 \frac{q}{x_3} \\ &= \frac{x_3^3 + 4q}{x_3} \\ &= \frac{-px_3 + 3q}{x_3}. \end{aligned}$$

Par suite :

$$\begin{aligned} \Delta &= \left(\frac{-px_1 + 3q}{x_1} \right) \left(\frac{-px_2 + 3q}{x_2} \right) \left(\frac{-px_3 + 3q}{x_3} \right) \\ &= \frac{-p^3 x_1^3 + 3q p^2 x_1^2 - 9q^2 p x_1 + 27q^3}{\sigma_3} \\ &= -(4p^3 + 27q^2). \end{aligned}$$

On en déduit qu'une condition nécessaire et suffisante pour que le polynôme $X^3 + pX + q$ admette une racine multiple est $4p^3 + 27q^2 = 0$.

On peut noter que cette condition, établie pour $q \neq 0$, reste clairement vraie lorsque $q = 0$.

3. Déterminer x, y et z vérifiant :

$$\begin{cases} x + y + z = 2 \\ x^2 + y^2 + z^2 = 14 \\ x^3 + y^3 + z^3 = 20 \end{cases}$$

- Soit (x, y, z) un triplet solution du système. En désignant par $t^3 + at^2 + bt + c$ le polynôme unitaire ayant pour racines x, y et z , on a :

$$\begin{cases} 2 = x + y + z = -a \\ 14 = x^2 + y^2 + z^2 = a^2 - 2b \\ 20 = x^3 + y^3 + z^3 = -14a - 2b - 3c \end{cases}$$

puisque $x^3 + y^3 + z^3 = -a(x^2 + y^2 + z^2) - b(x + y + z) - 3c$.

La résolution en (a, b, c) du système donne :

$$a = -2, b = -5, c = +6.$$

Conseil $t^3 - 2t^2 - 5t + 6 = (t - 1)(t + 2)(t - 3)$, le triplet cherché est, à l'ordre près, égal à $(-2, 1, 3)$.

- Réciproquement, il est immédiat de vérifier que $(-2, 1, 3)$, et donc tout triplet obtenu par permutation de $(-2, 1, 3)$, est solution du système.

4. Dérivation des polynômes

MPSI 4.1 Polynôme dérivé

Définition 11

Pour $A = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$, on définit A' , le *polynôme dérivé* de A , par :

$$A' = \sum_{k=1}^{\infty} k a_k X^{k-1} = \sum_{k=1}^n k a_k X^{k-1} \quad \text{pour tout } n \geq \deg A.$$

Remarque Lorsque $\mathbb{K} = \mathbb{R}$, on a de façon évidente $(\tilde{A})' = \widetilde{A'}$ et l'identification entre polynôme et fonction polynomiale permet de transférer à cette dérivation formelle les résultats que l'on a démontrés sur les fonctions de $\mathcal{D}(\mathbb{R})$. Toutefois il est nécessaire de justifier les résultats correspondants lorsque $\mathbb{K} = \mathbb{C}$. C'est l'objet de ce qui suit.

Proposition 19

Soit $A \in \mathbb{K}[X]$.

- (1) Si $\deg A > 0$, alors $\deg(A') = \deg(A) - 1$.
- (2) Le polynôme A est constant si, et seulement si, $A' = 0$.

Démonstration

(1) Supposons $A = \sum_{k=0}^n a_k X^k$ avec $\deg A = n > 0$.

Comme $A' = \sum_{k=1}^n k a_k X^{k-1}$ avec $na_n \neq 0$, on en déduit $\deg A = n - 1$.

(2) Si $A = a_0$ alors $A' = 0$.

Si $\deg A > 0$, alors d'après (1) on a $\deg(A') \geq 0$ et donc $A' \neq 0$. \square

Proposition 20 (Linéarité de la dérivation)

Étant donnés deux éléments A et B de $\mathbb{K}[X]$ ainsi que deux scalaires λ et μ , on a :

$$(\lambda A + \mu B)' = \lambda A' + \mu B'.$$

Démonstration Évident d'après la définition. \square

Proposition 21

Étant donnés deux éléments A et B de $\mathbb{K}[X]$, on a :

$$(AB)' = A'B + AB'.$$

Démonstration Si $A = \sum_{j=0}^{\infty} a_j X^j$ et $B = \sum_{k=0}^{\infty} b_k X^k$, on a :

$$AB = \sum_{j,k} a_j b_k X^{j+k}.$$

La linéarité de la dérivation des polynômes nous donne :

$$(AB)' = \sum_{j,k} a_j b_k (X^{j+k})'.$$

D'autre part les relations $A' = \sum_{j=0}^{\infty} a_j (X^j)'$ et $B' = \sum_{k=0}^{\infty} b_k (X^k)'$ permettent d'écrire :

$$\begin{aligned} A'B + AB' &= \sum_{j,k} a_j b_k (X^j)' X^k + \sum_{j,k} a_j b_k X^j (X^k)' \\ &= \sum_{j,k} a_j b_k ((X^j)' X^k + X^j (X^k)'). \end{aligned}$$

Il suffit donc de vérifier, pour tout couple $(j, k) \in \mathbb{N}^2$, la relation :

$$(X^{j+k})' = (X^j)' X^k + X^j (X^k)'.$$

C'est évident si $j = 0$ ou $k = 0$; si $j \neq 0$ et $k \neq 0$, on a :

$$(X^{j+k})' = (j+k) X^{j+k-1} = j X^{j-1} X^k + X^j k X^{k-1} = (X^j)' X^k + X^j (X^k)'. \quad \square$$

4.2 Dérivées successives, formule de Taylor

Définition 12

Pour $r \in \mathbb{N}$, on définit, par récurrence, le polynôme dérivé d'ordre r :

$$A^{(0)} = A \quad \text{et} \quad \forall r \geq 0, \quad A^{(r+1)} = (A^{(r)})'.$$

Remarque Pour $r \in \mathbb{N}$, l'application $A \mapsto A^{(r)}$ est linéaire puisque c'est l'itérée $r^{\text{ème}}$ de la dérivation.

Exemple Pour $n \in \mathbb{N}$ et $p \in \llbracket 0, n \rrbracket$, on a :

$$(X^n)^{(p)} = n(n-1)\dots(n-p+1) X^{n-p} = p! \binom{n}{p} X^{n-p}.$$

Proposition 22 (Formule de Leibniz)

Si A et B sont deux polynômes on a :

$$(AB)^{(r)} = \sum_{k=0}^r \binom{r}{k} A^{(k)} B^{(r-k)}.$$

Démonstration Cette formule se démontre par récurrence de la même façon que pour les fonctions dérivables, en utilisant le résultat :

$$\left(A^{(k)} B^{(r-k)} \right)' = A^{(k+1)} B^{(r-k)} + A^{(k)} B^{(r-k+1)}.$$

□

Proposition 23 (Formule de Taylor)

Étant donnés $A \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$, on a :

$$A(X) = \sum_{p=0}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^p,$$

ce qui peut encore s'écrire :

$$A(\alpha + X) = \sum_{p=0}^{\infty} \frac{A^{(p)}(\alpha)}{p!} X^p.$$

Remarque Malgré les apparences, la somme $\sum_{p=0}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^p$ est finie car, pour un polynôme A fixé, tous les polynômes dérivés $A^{(p)}$ sont nuls dès que $p > \deg A$.

Démonstration L'application $\varphi : A \mapsto \sum_{p=0}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^p$ est manifestement linéaire.

Pour démontrer $\forall A \in \mathbb{K}[X], \varphi(A) = A$, il suffit de le montrer pour les polynômes X^n , puisque tout élément de $\mathbb{K}[X]$ est combinaison linéaire de ces derniers.

Or, pour $n \in \mathbb{N}$, on a :

$$\begin{aligned}\varphi(X^n) &= \sum_{p=0}^{\infty} \frac{(X^n)^{(p)}(\alpha)}{p!} (X - \alpha)^p \\ &= \sum_{p=0}^n \frac{(X^n)^{(p)}(\alpha)}{p!} (X - \alpha)^p \\ &= \sum_{p=0}^n \binom{n}{p} \alpha^{n-p} (X - \alpha)^p = X^n.\end{aligned}$$

□

4.3 Caractérisation de l'ordre d'une racine

Proposition 24

Soient $r \in \mathbb{N}^*$ et $A \in \mathbb{K}[X]$. Si $\alpha \in \mathbb{K}$ est racine d'ordre r de A , alors α est racine d'ordre $r - 1$ du polynôme dérivé A' .

Démonstration Soit α une racine d'ordre r de $A \in \mathbb{K}[X]$. On peut écrire :

$$A(X) = (X - \alpha)^r B(X) \quad \text{avec} \quad B(\alpha) \neq 0.$$

Alors :

$$\begin{aligned}A'(X) &= (X - \alpha)^{r-1} (r B(X) + (X - \alpha) B'(X)) \\ &= (X - \alpha)^{r-1} B_1(X)\end{aligned}$$

avec $B_1(\alpha) = r B(\alpha) \neq 0$, ce qui prouve le résultat.

□

Remarque Le résultat est valable même si $r = 1$, puisqu'on a convenu qu'un scalaire qui n'est pas racine de A est racine d'ordre 0 de A .

Proposition 25

Pour $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}^*$, il est équivalent de dire :

- (i) α est racine d'ordre r de A ,
- (ii) $A(\alpha) = A'(\alpha) = \dots = A^{(r-1)}(\alpha) = 0$ et $A^{(r)}(\alpha) \neq 0$.

Démonstration

(i) \implies (ii). Soit α une racine d'ordre r de A . D'après la proposition précédente, pour $k \in \llbracket 0, r \rrbracket$, le scalaire α est racine d'ordre $r - k$ de $A^{(k)}$.

Donc α est racine des polynômes $A, A', \dots, A^{(r-1)}$ et α est racine d'ordre 0 de $A^{(r)}$, c'est-à-dire n'est pas racine de $A^{(r)}$.

(ii) \implies (i). En utilisant la formule de Taylor, on peut écrire :

$$\begin{aligned} A(X) &= \sum_{p=0}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^p \\ &= \sum_{p=r}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^p \\ &= (X - \alpha)^r \sum_{p=r}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^{p-r} \\ &= (X - \alpha)^r B(X) \end{aligned}$$

avec $B(X) = \sum_{p=r}^{\infty} \frac{A^{(p)}(\alpha)}{p!} (X - \alpha)^{p-r}$ et donc $B(\alpha) = \frac{A^{(r)}(\alpha)}{r!} \neq 0$, ce qui prouve que α est racine d'ordre r de A . □

Corollaire 26

Soit A un polynôme. Un scalaire α est racine multiple de A si, et seulement si, $A(\alpha) = A'(\alpha) = 0$.

MPSI

5. Étude de $\mathbb{C}[X]$ et $\mathbb{R}[X]$ **5.1 Factorisation dans $\mathbb{C}[X]$** **Théorème 27 (Théorème de d'Alembert)**

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans \mathbb{C} .

Démonstration Voir en annexe page 747. □

Corollaire 28

Tout polynôme non nul de $\mathbb{C}[X]$ est scindé sur \mathbb{C} .

Démonstration Désignons par $\alpha_1, \alpha_2, \dots, \alpha_p$ les racines (complexes) distinctes de A et par r_1, r_2, \dots, r_p leurs ordres respectifs. D'après la proposition 16 de la page 724, il existe un polynôme Q tel que :

$$A = \prod_{k=1}^p (X - \alpha_k)^{r_k} Q.$$

Si Q est de degré non nul, il admet au moins une racine complexe qui est alors une racine α_j de A , et donc $(X - \alpha_j)^{r_j+1}$ divise A , ce qui contredit la définition de r_j .

Par suite Q est une constante λ et on a :

$$A = \lambda \prod_{k=1}^p (X - \alpha_k)^{r_k}$$

où λ est évidemment le coefficient dominant de A . □

Remarques

1. Ce résultat est évidemment faux dans $\mathbb{R}[X]$, puisque par exemple $X^2 + 1$ n'est pas scindé sur \mathbb{R} . Cependant, tout polynôme à coefficients réels est aussi un polynôme à coefficients complexes et par suite est scindé sur \mathbb{C} .
2. La démonstration précédente montre que tout polynôme A dont les racines (complexes) distinctes sont $\alpha_1, \alpha_2, \dots, \alpha_p$ d'ordres respectifs r_1, r_2, \dots, r_p s'écrit :

$$A = \lambda \prod_{k=1}^p (X - \alpha_k)^{r_k}.$$

3. Une telle factorisation est unique à une permutation près des facteurs, puisque l'ensemble des racines de A est alors $\{\alpha_1, \alpha_2, \dots, \alpha_p\}$, chaque entier r_k étant l'ordre de la racine α_k , et que λ est égal au coefficient dominant du polynôme A .

5.2 Conjugaison

Si $A = \sum_{k=0}^{+\infty} a_k X^k$ est un polynôme à coefficients complexes, on appelle conjugué de A , le polynôme $\overline{A} = \sum_{k=0}^{+\infty} \bar{a}_k X^k$. Par exemple $\overline{X} = X$.

Les propriétés de la conjugaison dans \mathbb{C} nous donnent immédiatement, pour $(A, B) \in \mathbb{C}[X]^2$:

- $\overline{A + B} = \overline{A} + \overline{B}$ et $\overline{AB} = \overline{A}\overline{B}$,

- $\forall \alpha \in \mathbb{C}, \overline{A(\alpha)} = \overline{A}(\overline{\alpha}),$
- $A \in \mathbb{R}[X] \iff \overline{A} = A.$

Lemme

Étant donnés $A \in \mathbb{C}[X]$ et $r \in \mathbb{N}$, un complexe α est racine de A d'ordre r si, et seulement si, $\overline{\alpha}$ est racine de \overline{A} d'ordre r .

Démonstration Le complexe α est racine d'ordre r de A si, et seulement si, l'on a :

$$A(\alpha) = A'(\alpha) = \cdots = A^{(r-1)}(\alpha) = 0 \quad \text{et} \quad A^{(r)}(\alpha) \neq 0$$

c'est-à-dire en conjuguant :

$$\overline{A(\alpha)} = \overline{A'(\alpha)} = \cdots = \overline{A^{(r-1)}(\alpha)} = 0 \quad \text{et} \quad \overline{A^{(r)}(\alpha)} \neq 0.$$

Le résultat s'ensuit, puisque :

$$\forall k \in \mathbb{N}, \overline{A^{(k)}} = \overline{A^{(k)}}.$$

□

Proposition 29

Soit $A \in \mathbb{R}[X]$. Si un complexe α est racine de A , alors $\overline{\alpha}$ est racine de A au même ordre de multiplicité.

5.3 Factorisation dans $\mathbb{R}[X]$ **Proposition 30**

Tout polynôme non nul $A \in \mathbb{R}[X]$, peut s'écrire sous la forme :

$$A = \lambda \prod_{k=1}^p (X - \alpha_k)^{r_k} \prod_{k=1}^q (X^2 + \beta_k X + \gamma_k)^{s_k}$$

où p et q sont deux entiers naturels, λ et les α_k, β_k et γ_k des réels vérifiant $\forall k \in \llbracket 1, q \rrbracket, \beta_k^2 - 4\gamma_k < 0$, et les r_k et s_k des entiers naturels non nuls.

Démonstration Puisque A est à coefficients réels, on sait que si ω est une racine complexe non réelle de A d'ordre s , alors $\overline{\omega}$ est aussi racine d'ordre s . Comme A est scindé sur \mathbb{C} , il s'écrit donc :

$$A = \lambda \prod_{k=1}^p (X - \alpha_k)^{r_k} \prod_{k=1}^q (X - \omega_k)^{s_k} \prod_{k=1}^q (X - \overline{\omega}_k)^{s_k}$$

où λ est le coefficient dominant de A , donc réel, les ω_k et $\overline{\omega}_k$ sont les racines non réelles et les α_k les racines réelles de A .

Le résultat s'ensuit, puisque :

$$(X - \omega_k)(X - \bar{\omega}_k) = (X^2 + \beta_k X + \gamma_k) \in \mathbb{R}[X]$$

avec $\beta_k = -\omega_k - \bar{\omega}_k = -2 \operatorname{Re}(\omega_k) \in \mathbb{R}$ et $\gamma_k = \omega_k \bar{\omega}_k = |\omega_k|^2 \in \mathbb{R}$.

Ce polynôme n'ayant pas de racine réelle, son discriminant $\Delta = \beta_k^2 - 4\gamma_k$ est strictement négatif. \square

Exemples

- Pour décomposer $X^4 + 1$, on peut écrire :

$$\begin{aligned} X^4 + 1 &= (X^2 + 1)^2 - 2X^2 \\ &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1). \end{aligned}$$

Comme $X^4 + 1$ n'a pas de racines réelles, ces deux polynômes du second degré n'ont pas de racines réelles, et donc leur discriminant est strictement négatif.

- Décomposition de $X^8 - 1$:

$$\begin{aligned} X^8 - 1 &= (X^4 - 1)(X^4 + 1) \\ &= (X^2 - 1)(X^2 + 1)(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \\ &= (X - 1)(X + 1)(X^2 + 1)(X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1). \end{aligned}$$

- Pour décomposer $X^5 + 1$, on commence par le décomposer dans $\mathbb{C}[X]$:

$$X^5 + 1 = \left(X - e^{\frac{i\pi}{5}}\right) \left(X - e^{\frac{3i\pi}{5}}\right) (X + 1) \left(X - e^{\frac{7i\pi}{5}}\right) \left(X - e^{\frac{9i\pi}{5}}\right)$$

puis l'on regroupe les termes conjugués :

$$\begin{aligned} X^5 + 1 &= (X + 1) \left((X - e^{\frac{i\pi}{5}})(X - e^{\frac{9i\pi}{5}})\right) \left((X - e^{\frac{3i\pi}{5}})(X - e^{\frac{7i\pi}{5}})\right) \\ &= (X + 1) \left(X^2 - 2X \cos\left(\frac{\pi}{5}\right) + 1\right) \left(X^2 - 2X \cos\left(\frac{3\pi}{5}\right) + 1\right). \end{aligned}$$

MPSI 6. Plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM)

6.1 Plus grand commun diviseur, algorithme d'Euclide

Proposition 31

Soit $(A, B) \in \mathbb{K}[X]^2$ tel que $B \neq 0$. Si Q et R sont les quotient et reste de la division euclidienne de A par B , alors les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R .

Démonstration Conséquence des égalités $A = BQ + R$ et $R = A - BQ$. \square

Proposition 32

Soit $(A, B) \in \mathbb{K}[X]^2$. Il existe un unique polynôme D nul ou unitaire dont les diviseurs sont les diviseurs communs à A et B c'est-à-dire tel que l'on ait :

$$\forall P \in \mathbb{K}[X], (P | A \text{ et } P | B) \iff P | D.$$

De plus, il existe deux polynômes U et V tels que $AU + BV = D$.

- Le polynôme D est appelé PGCD de A et B et noté $A \wedge B$.
- Le couple (U, V) est un couple de coefficients de Bézout de A et B .

Démonstration

Unicité. Si D_1 et D_2 répondent au problème, alors D_1 divise A et B et donc il divise D_2 . Par symétrie on a aussi $D_2 | D_1$, ce qui prouve que D_1 et D_2 sont associés.

Si l'un est nul, l'autre aussi et sinon puisqu'ils sont unilaires, ils sont égaux.

Existence. Démontrons par récurrence sur n que si $\deg B < n$, alors pour tout A il existe un polynôme D dont les diviseurs sont les diviseurs communs à A et B , ainsi que U et V tels que $AU + BV = D$.

- Si $n = 0$, alors $B = 0$, et il suffit de prendre $D = A$, $U = 1$ et $V = 0$.
- Supposons le résultat vrai pour $n \in \mathbb{N}$. Soient B de degré strictement plus petit que $n+1$ et A quelconque.

Si $\deg B < n$, l'hypothèse de récurrence donne immédiatement le résultat. Sinon, B est non nul ; soient respectivement Q et R les quotient et reste de la division euclidienne de A par B . Comme $\deg R < \deg B$, on a $\deg R < n$ et l'hypothèse de récurrence nous donne l'existence d'un polynôme D dont les diviseurs sont les diviseurs communs à B et R , ainsi que U_1 et V_1 tels que $BU_1 + RV_1 = D$.

D'après la proposition 31 de la page précédente, les diviseurs communs à A et B sont les mêmes que ceux communs à B et R , et donc sont les diviseurs de D . D'autre part, la relation $BU_1 + RV_1 = D$ donne $BU_1 + (A - BQ)V_1 = D$. Le triplet $(D, V_1, U_1 - QV_1)$ est donc solution.

En divisant D , U et V par le coefficient dominant de D , si $D \neq 0$, on obtient bien un polynôme répondant au problème. \square

Remarques

- Le PGCD de A et B est le plus grand des diviseurs de A et B au sens de la divisibilité.
- Le PGCD de A et B est nul si, et seulement si, $A = B = 0$.
- Il n'y a pas unicité des polynômes U et V , puisque si (U_0, V_0) est un couple de coefficients de Bézout de A et B , alors il en est de même du couple $(U_0 + QB, V_0 - QA)$ pour tout polynôme Q (voir la proposition 43 de la page 742 pour un résultat d'unicité).

- Si A et B sont dans $\mathbb{R}[X]$, on déduit de la remarque de la page 719 que le PGCD de A et B est le même en travaillant dans $\mathbb{R}[X]$ que celui obtenu dans $\mathbb{C}[X]$.
- Comme pour le cas des entiers, le calcul du PGCD est basé sur l'algorithme d'Euclide. En remontant l'algorithme on peut alors trouver un couple de coefficients de Bézout. Mais on peut aussi utiliser l'algorithme suivant (même démonstration que dans le cas des entiers) :

DONNÉES : les polynômes A et B .

VARIABLES : U_0, V_0, U_1, V_1, Q et λ .

- $(U_0, V_0) \leftarrow (1, 0)$
- $(U_1, V_1) \leftarrow (0, 1)$
- tant que $B \neq 0$
 - $Q \leftarrow$ quotient de la division de A par B
 - $(A, B) \leftarrow (B, A - Q B)$
 - $(U_0, U_1) \leftarrow (U_1, U_0 - Q U_1)$
 - $(V_0, V_1) \leftarrow (V_1, V_0 - Q V_1)$
- si $A \neq 0$:
 - $\lambda \leftarrow$ coefficient dominant de A
 - $A \leftarrow A/\lambda, U_0 \leftarrow U_0/\lambda, V_0 \leftarrow V_0/\lambda$

RÉSULTAT : (A, U_0, V_0) .

Exemple En MAPLE, c'est la fonction gcd qui calcule le PGCD de deux polynômes :

$$\begin{aligned} > \text{gcd}(1+x+x^2+x^3, 1+x^2+x^3+x^4+x^5+x^6); \\ & X^2 + 1 \end{aligned}$$

6.2 Plus petit commun multiple

Proposition 33

Soit $(A, B) \in \mathbb{K}[X]^2$. Il existe un unique polynôme M nul ou unitaire dont les multiples sont les multiples communs à A et B c'est-à-dire tel que l'on ait :

$$\forall P \in \mathbb{K}[X], (A \mid P \text{ et } B \mid P) \iff M \mid P.$$

Ce polynôme est appelé **PPCM** de A et B et il est noté $A \vee B$.

Démonstration

Unicité. De même que pour le PGCD, si M_1 et M_2 sont deux tels polynômes, alors ils sont associés, donc égaux.

Existence. Si $A = 0$ ou $B = 0$, il suffit de prendre $M = 0$. Supposons donc $A \neq 0$ et $B \neq 0$.

Il existe alors des multiples non nuls communs à A et B (par exemple AB). Prenons M un multiple commun non nul de degré minimal, polynôme que l'on peut supposer unitaire.

- Comme M est un multiple de A et B , ses multiples sont aussi multiples de A et B .
- Réciproquement, soit P un multiple commun à A et B . En effectuant la division euclidienne de P par M , on obtient $P = M Q + R$, avec $\deg R < \deg M$. Alors, $R = P - M Q$ est un multiple de A et de B . Comme il est de degré strictement plus petit que celui de M , et que M a été choisi de degré minimal, on en déduit $R = 0$. Donc $P = M Q$ est un multiple de M . \square

Remarque Le PPCM de A et B est donc le plus petit, au sens de la divisibilité, des multiples communs à A et à B .

6.3 Polynômes premiers entre eux

Définition 13

Deux polynômes A et B sont premiers entre eux si $A \wedge B = 1$, c'est-à-dire si les seuls diviseurs communs à A et B sont les polynômes de degré 0.

Exemples

1. Soient a et b deux éléments distincts de \mathbb{K} . Si p et q sont deux entiers naturels, les polynômes $A = (X - a)^p$ et $B = (X - b)^q$ sont premiers entre eux puisque les diviseurs unitaires de A sont les polynômes $(X - a)^k$, avec $k \leq p$, et que parmi eux, seul 1 divise B .
2. Pour $(a_1, a_2, \dots, a_p) \in \mathbb{K}^p$, le polynôme $(X - a_1)(X - a_2) \dots (X - a_p)$ est premier avec tout polynôme n'admettant aucun a_i pour racine. En effet, les diviseurs unitaires de A sont les polynômes de la forme $\prod_{i \in I} (X - a_i)$, avec $I \subset [1, p]$ et aucun d'eux, hormis 1, ne divise B puisque A et B n'ont pas de racines communes.
3. Si $A = 0$, alors A et B sont premiers entre eux si, et seulement si, le polynôme B est constant non nul.

Proposition 34 (Identité de Bézout)

Les polynômes A et B sont premiers entre eux si, et seulement si, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.

Démonstration

- Si A et B sont premiers entre eux, alors $A \wedge B = 1$ et, d'après la proposition 32 de la page 737, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = A \wedge B = 1$.

- S'il existe deux polynômes U et V tels que $AU + BV = 1$, alors tout diviseur commun à A et B divise $AU + BV$ donc est de degré 0. On en déduit que A et B sont premiers entre eux. \square

6.4 Propriétés du PGCD et du PPCM

Soient A et B deux polynômes.

Proposition 35

Si $A = PA_1$ et $B = PB_1$ avec $(P, A_1, B_1) \in \mathbb{K}[X]^3$ et P unitaire, alors :

$$A \wedge B = (A_1 \wedge B_1)P \quad \text{et} \quad A \vee B = (A_1 \vee B_1)P.$$

Démonstration

- Soient $D = A \wedge B$ et $D_1 = A_1 \wedge B_1$.
 - Comme $D_1 \mid A_1$ et $D_1 \mid B_1$, on a $PD_1 \mid PA_1 = A$ et $PD_1 \mid PB_1 = B$. Donc $PD_1 \mid D$.
 - On peut alors écrire $D = PD_1 R = PQ$ avec $D_1 \mid Q$. Par suite, on a :

$$PQ = D \mid A = PA_1$$

et de même $PQ \mid PB_1$ ce qui prouve, puisque $P \neq 0$, que Q divise A_1 et B_1 et donc leur PGCD D_1 . On a ainsi $D = PQ \mid PD_1$.

En conclusion D et PD_1 sont associés, et comme ils sont unitaires (ou nuls), on en déduit qu'ils sont égaux.

- Soient $M = A \vee B$ et $M_1 = A_1 \vee B_1$.
 - Comme $A_1 \mid M_1$ et $B_1 \mid M_1$, on a $A = PA_1 \mid PM_1$ et $B = PB_1 \mid PM_1$. Donc PM_1 est un multiple commun à A et B , et par suite $M \mid PM_1$.
 - Puisque M est un multiple de $A = PA_1$, on peut écrire $M = PQ$. On a alors $PA_1 \mid PQ$ et $PB_1 \mid PQ$ ce qui donne, puisque $P \neq 0$, $A_1 \mid Q$ et $B_1 \mid Q$. Donc $M_1 \mid Q$ ce qui prouve $PM_1 \mid PQ = M$.

En conclusion $M = PM_1$, puisque ce sont deux polynômes unitaires (ou nuls) associés. \square

Proposition 36

Soit $(A, B) \in \mathbb{K}[X]^2$. Il existe deux polynômes A_1 et B_1 premiers entre eux tels que : $A = DA_1$ et $B = DB_1$ avec $D = A \wedge B$.

Démonstration

- Si $A = B = 0$, on a $D = 0$ et il suffit de prendre $A_1 = B_1 = 1$.
- Sinon, comme D divise A et B , on peut trouver A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. La proposition précédente nous donne alors :

$$D = A \wedge B = (A_1 \wedge B_1)D$$

ce qui prouve que A_1 et B_1 sont premiers entre eux puisque $D \neq 0$. \square

6.5 Théorème de Gauss

Théorème 37

Étant donnés trois polynômes A , B et C , on a :

$$(A \wedge B = 1 \text{ et } A \mid BC) \implies A \mid C.$$

Démonstration Supposons $A \wedge B = 1$ et $A \mid BC$. D'après l'identité de Bézout, il existe deux polynômes U et V tels que $AU + BV = 1$, ce qui implique $ACU + BCV = C$.

On a alors $A \mid ACU + BCV = C$. □

Corollaire 38

Si A et B sont deux polynômes premiers entre eux, alors $A \vee B$ et AB sont associés.

Démonstration Il est évident que les multiples de AB sont des multiples communs à A et B .

Réciproquement, supposons $A \mid P$ et $B \mid P$; il existe donc un polynôme Q tel que $P = BQ$. Comme A divise P et qu'il est premier avec B , on en déduit d'après le théorème de Gauss que A divise Q . Il existe donc un polynôme R tel que $Q = AR$, ce qui donne $P = ABR$.

Les multiples communs à A et à B sont donc les multiples de AB , ce qui prouve le résultat. □

Corollaire 39

Si $(A, B) \in \mathbb{K}[X]^2$, les polynômes AB et $(A \wedge B)(A \vee B)$ sont associés.

Démonstration Le résultat étant évident si $AB = 0$, on peut supposer A et B non nuls, et unitaires quitte à les diviser par leurs coefficients dominants.

Soit $D = A \wedge B$. Prenons A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$ et $A_1 \wedge B_1 = 1$. Comme A_1 et B_1 sont unitaires et premiers entre eux, on a $A_1 \vee B_1 = A_1 B_1$.

Alors :

$$A \vee B = D(A_1 \vee B_1) = DA_1 B_1$$

et par suite $D(A \vee B) = AB$. □

Proposition 40

Étant donnés trois polynômes A , B et C , on a :

$$(A \wedge B = 1 \text{ et } A \wedge C = 1) \iff A \wedge (BC) = 1.$$

Démonstration

- Supposons $A \wedge B = A \wedge C = 1$. Il existe donc des polynômes U_1, V_1, U_2 et V_2 tels que :

$$AU_1 + BV_1 = 1$$

$$AU_2 + CV_2 = 1$$

En multipliant ces deux égalités, on obtient une relation du type $AU + (BC)V = 1$, ce qui prouve que A et BC sont premiers entre eux.

- La réciproque est évidente, puisque $A \wedge B$ et $A \wedge C$ sont des diviseurs communs à A et BC .

□

Les propositions 38 et 40 se généralisent facilement par récurrence à des produits quelconques :

Proposition 41

Si des polynômes premiers entre eux deux à deux divisent un polynôme A , alors leur produit divise A .

Proposition 42

Un produit est premier avec A si, et seulement si, chacun de ses facteurs est premier avec A .

Exemples

On peut ainsi retrouver plus rapidement des résultats déjà connus.

- Si a et b sont deux scalaires distincts, les polynômes $X - a$ et $X - b$ sont premiers entre eux, comme le prouve l'identité de Bézout $\frac{X - a}{b - a} + \frac{X - b}{a - b} = 1$. On en déduit, pour $(p, q) \in \mathbb{N}^2$, que $(X - a)^p$ et $(X - b)^q$ sont premiers entre eux.
- Soit A un polynôme admettant pour racines distinctes $\alpha_1, \alpha_2, \dots, \alpha_p$ d'ordres respectifs r_1, r_2, \dots, r_p . Par définition, les polynômes $(X - \alpha_i)^{r_i}$ divisent A , et comme ils sont premiers entre eux deux à deux, leur produit divise A .

Proposition 43

Étant donnés deux polynômes non constants A et B premiers entre eux, il existe un unique couple de polynômes (U_0, V_0) tel que :

$$AU_0 + BV_0 = 1 \quad \text{avec} \quad \deg U_0 < \deg B \quad \text{et} \quad \deg V_0 < \deg A.$$

Démonstration

Unicité. Si (U_1, V_1) et (U_2, V_2) sont deux tels couples, on a :

$$(U_1 - U_2) A = (V_2 - V_1) B.$$

Le polynôme A divise donc $(V_2 - V_1) B$, et comme $A \wedge B = 1$, le théorème de Gauss entraîne $A \mid (V_2 - V_1)$.

Le polynôme $V_2 - V_1$ est alors un multiple de A de degré strictement inférieur à $\deg A$, ce qui prouve qu'il est nul.

Donc $V_1 = V_2$, et par suite $U_1 = U_2$ puisque $A \neq 0$.

Existence. Soit (U, V) un couple de coefficients de Bézout pour A et B . Notons Q le quotient de la division euclidienne de U par B . L'égalité $AU + BV = 1$ nous donne $A(U - QB) + B(V + QA) = 1$, ce qui donne $AU_0 + BV_0 = 1$ avec $U_0 = U - QB$ et $V_0 = V + QA$.

Comme U_0 est le reste de la division euclidienne de U pas B , on a $\deg U_0 < \deg B$.

Puisque B n'est pas constant, le polynôme U_0 ne peut pas être nul (sinon on aurait $BV_0 = 1$) et donc $\deg(AU_0) > 0$. Alors :

$$\deg(BV_0) = \deg(1 - AU_0) = \deg(AU_0)$$

ce qui donne $\deg V_0 = \deg A + \deg U_0 - \deg B < \deg A$.

□ MPSI

7. Polynômes irréductibles

7.1 Définition

Définition 14

On appelle *polynôme irréductible* de $\mathbb{K}[X]$ tout polynôme P vérifiant :

- $\deg P \geq 1$,
- les seuls diviseurs de P sont les éléments de \mathbb{K}^* et les associés de P ,

c'est-à-dire tel que P soit non constant et que pour tout $(A, B) \in \mathbb{K}[X]^2$, on ait :

$$P = AB \implies (\deg A = 0 \quad \text{ou} \quad \deg B = 0).$$

Exemples

1. Tout polynôme de degré 1 est irréductible, puisque le produit de deux polynômes non constants est au moins de degré 2.
2. Un polynôme irréductible dans $\mathbb{K}[X]$ possédant une racine $\alpha \in \mathbb{K}$ est de degré 1. En effet, il est divisible par le polynôme non constant $X - \alpha$ qui lui est donc associé.
3. Un polynôme qui n'admet pas de racine dans \mathbb{K} n'est pas nécessairement irréductible dans $\mathbb{K}[X]$, comme le prouve l'exemple de $(X^2 + 1)^2$ dans $\mathbb{R}[X]$.

4. En revanche un polynôme de degré 2 ou 3 qui n'a pas de racine dans \mathbb{K} est irréductible dans $\mathbb{K}[X]$, puisqu'une décomposition non triviale d'un tel polynôme utilise nécessairement un polynôme de degré 1 qui a donc une racine.
5. Un polynôme de $\mathbb{R}[X]$ de degré 2 est donc irréductible dans $\mathbb{R}[X]$ si, et seulement si, son discriminant est strictement négatif.

Proposition 44

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration On sait que tout polynôme de degré 1 est irréductible. D'autre part, le théorème de d'Alembert nous dit qu'un polynôme non constant est scindé sur \mathbb{C} , c'est-à-dire produit de polynômes de degré 1. Un polynôme de degré au moins 2 n'est donc pas irréductible. \square

Proposition 45

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1,
- les polynômes de degré 2 dont le discriminant est strictement négatif.

Démonstration

- Les polynômes de degré 1 sont irréductibles.
- D'après l'exemple 5. ci-dessus, un polynôme de degré 2 est irréductible si, et seulement si, son discriminant est strictement négatif.
- Comme tout polynôme non constant est produit de polynômes de degré 1 ou 2 (proposition 30 de la page 735), on en déduit qu'un polynôme de degré au moins 3 n'est pas irréductible. \square

MPSI 7.2 Propriétés

Proposition 46

Un polynôme P irréductible est premier avec tous les polynômes qu'il ne divise pas.

Démonstration Les diviseurs communs à P et à un polynôme A sont des diviseurs de P , donc sont, soit constants, soit associés à P . Donc, si P ne divise pas A , les seuls diviseurs communs à P et A sont les constantes. \square

Exemple Deux polynômes irréductibles non associés sont premiers entre eux.

En particulier, deux polynômes irréductibles unitaires distincts sont premiers entre eux.

Corollaire 47

Un polynôme irréductible divise un produit si, et seulement si, il divise l'un des facteurs.

Démonstration S'il ne divise aucun des facteurs, il est premier avec chacun d'entre eux et donc avec leur produit, ce qui prouve qu'il ne divise pas ce produit.

La réciproque est évidente. □ MPSI

7.3 Décomposition d'un polynôme en produit de facteurs irréductibles

Proposition 48

Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$. De plus cette décomposition est unique à l'ordre près des facteurs.

PCSI Admis en PCSI

MPSI Démonstration

Existence. On démontre par récurrence, pour $n \geq 1$ la propriété H_n :

Tout polynôme non constant de $\mathbb{K}[X]$ de degré inférieur ou égal à n peut s'écrire sous forme d'un produit de polynômes irréductibles.

- H_1 est vraie de façon évidente car tout polynôme de degré 1, étant irréductible, est un produit d'un seul polynôme irréductible.
- Supposons H_n . Soit A un polynôme de degré $n+1$.
 - Si A est irréductible, alors c'est un produit d'un seul polynôme irréductible.
 - Sinon, on peut trouver deux polynômes non constants B et C tels que $A = BC$. Les polynômes B et C ont donc des degrés strictement inférieurs à celui de A et l'on peut leur appliquer l'hypothèse de récurrence, ce qui permet d'obtenir une décomposition de A en un produit de polynômes irréductibles.

En mettant en facleur les coefficients dominants de chaque polynôme irréductible, on obtient la décomposition annoncée.

Unicité. Soit $A = \lambda Q_1 Q_2 \dots Q_k$ une telle décomposition d'un polynôme A . Alors, le scalaire λ est le coefficient dominant de A . De plus, chaque polynôme irréductible unitaire Q_i divise A et réciproquement. si un polynôme irréductible unitaire P divise A , alors il divise l'un des Q_i donc lui est égal puisqu'il s'agit de deux irréductibles unitaires. Les facteurs intervenant dans une telle décomposition sont donc tous les diviseurs irréductibles unitaires de A .

Soient alors deux décompositions de A , que l'on peut donc écrire :

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r} = \lambda P_1^{\beta_1} P_2^{\beta_2} \dots P_r^{\beta_r}$$

où les P_i sont irréductibles unitaires et deux à deux distincts.

Si, pour un entier i , on a $\alpha_i \neq \beta_i$, par exemple $\alpha_i < \beta_i$, alors on a :

$$\prod_{j \neq i} P_j^{\alpha_j} = P_i^{\beta_i - \alpha_i} \prod_{j \neq i} P_j^{\beta_j}$$

et donc P_i divise $\prod_{j \neq i} P_j^{\alpha_j}$, ce qui est impossible puisque P_i est premier avec P_j si $j \neq i$.

Par suite $\forall i, \alpha_i = \beta_i$, ce qui montre l'unicité de la décomposition. □ MPSI

Remarques

- En fait, nous avons vu à la section 5. page 733 que :
 - tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur \mathbb{C} ,
 - tout polynôme non constant de $\mathbb{R}[X]$ est produit de polynômes de degré 1 et de polynômes de degré 2 à discriminant strictement négatif.

Dans les deux cas, on a démontré que tout polynôme non constant est produit de polynômes irréductibles.

La proposition précédente montre l'unicité de cette décomposition.

- Si l'on travaillait sur un autre corps que \mathbb{R} ou \mathbb{C} , les polynômes irréductibles seraient bien sûr différents, mais la même démonstration prouverait l'existence et l'unicité de la décomposition en produit de facteurs irréductibles.

Exemples

1. Décomposition en facteurs irréductibles sur $\mathbb{R}[X]$ de $X^6 - 1$:

$$X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1).$$

2. La fonction `factor` de MAPLE décompose un polynôme de $\mathbb{Q}[X]$ en un produit de polynômes irréductibles dans $\mathbb{Q}[X]$ mais pas nécessairement dans $\mathbb{R}[X]$.

```
> factor(x^2-2);
          
$$X^2 - 2$$

> factor(x^2-3*x+2);
          
$$(X - 1)(X - 2)$$

```

MPSI Proposition 49

Soient A et B deux polynômes non nuls. Si :

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \quad \text{et} \quad B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$$

où P_1, P_2, \dots, P_k sont des polynômes irréductibles unitaires distincts deux à deux, alors on a :

1. $A \mid B \iff \forall i \in \llbracket 1, k \rrbracket, \alpha_i \leq \beta_i$.

2. $A \wedge B = \prod_{i=1}^k P_i^{\min(\alpha_i, \beta_i)}$ et $A \vee B = \prod_{i=1}^k P_i^{\max(\alpha_i, \beta_i)}$.

Démonstration

1.
 - Si $A \mid B$, alors pour $i \in \llbracket 1, k \rrbracket$, $P_i^{\alpha_i} \mid A$ et donc $P_i^{\alpha_i} \mid B$, ce qui montre $\alpha_i \leq \beta_i$.
 - Si $\forall i \in \llbracket 1, k \rrbracket, \alpha_i \leq \beta_i$, alors $P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \mid P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$, c'est-à-dire $A \mid B$.

- 2.** ➤ Les diviseurs unitaires D communs à A et à B sont :

$$D = P_1^{\delta_1} P_2^{\delta_2} \dots P_k^{\delta_k} \quad \text{avec} \quad \forall i, \delta_i \leq \alpha_i \quad \text{et} \quad \delta_i \leq \beta_i.$$

Le plus grand des diviseurs communs à A et à B est obtenu lorsque :

$$\forall i, \delta_i = \min(\alpha_i, \beta_i),$$

ce qui montre la première égalité.

- Les multiples unitaires M communs à A et à B s'écrivent :

$$M = P_1^{\mu_1} P_2^{\mu_2} \dots P_k^{\mu_k} \quad \text{avec} \quad \forall i, \mu_i \geq \alpha_i \quad \text{et} \quad \mu_i \geq \beta_i.$$

Le plus petit des multiples communs à A et à B est donc obtenu lorsque :

$$\forall i, \mu_i = \max(\alpha_i, \beta_i),$$

ce qui montre la deuxième égalité. □

Exemple Étant donnés deux polynômes unitaires A et B , on retrouve la formule :

$$(A \wedge B)(A \vee B) = AB$$

puisque pour tout couple d'entiers (α, β) , on a :

$$\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta.$$

MPSI

Démonstration du théorème de d'Alembert

Soit A un polynôme à coefficients complexes de degré $p > 0$. Pour montrer que A possède une racine complexe, considérons $\alpha = \inf_{z \in \mathbb{C}} |A(z)|$, qui existe puisque $\{|A(z)| \mid z \in \mathbb{C}\}$ est une partie non vide de \mathbb{R}_+ , et montrons que cette borne inférieure est atteinte, puis qu'elle est nulle.

- Si $A = \sum_{k=0}^p a_k X^k$ avec $a_p \neq 0$, pour $|z| = r$, on a :

$$|A(z)| \geq |a_p z^p| - \left| \sum_{k=0}^{p-1} a_k z^k \right| \geq |a_p| r^p - \sum_{k=0}^{p-1} |a_k| r^k.$$

Ce minorant définit une fonction réelle polynomiale de r , qui tend vers $+\infty$ quand r tend vers $+\infty$ puisqu'elle est équivalente à $|a_p|r^p$. Elle est donc plus grande que $\alpha + 1$ au voisinage de $+\infty$, ce qui prouve qu'il existe un disque D centré en 0 en dehors duquel on a $|A(z)| \geq \alpha + 1$.

Puisque $\alpha = \inf_{z \in \mathbb{C}} |A(z)|$, on peut trouver une suite de complexes $(u_n)_{n \in \mathbb{N}}$ telle que

$\lim_{n \rightarrow +\infty} |A(u_n)| = \alpha$. Cette suite est donc, à partir d'un certain rang, dans le disque D , et par suite elle est bornée. On peut donc en extraire une sous-suite $(u_{\varphi(n)})_{n \in \mathbb{N}}$ convergeant vers un complexe z_0 .

Comme :

$$A(u_{\varphi(n)}) = \sum_{k=0}^p a_k u_{\varphi(n)}^k,$$

on en déduit $\lim_{n \rightarrow +\infty} A(u_{\varphi(n)}) = A(z_0)$, ce qui donne :

$$\alpha = \lim_{n \rightarrow +\infty} |A(u_{\varphi(n)})| = |A(z_0)|.$$

- Montrons par l'absurde que $A(z_0) = 0$ en supposant $\alpha > 0$. Quitte à considérer le polynôme $\frac{A(z_0) + X}{A(z_0)}$, on peut supposer $\alpha = 1$ et $z_0 = 0$.

Le polynôme non constant A s'écrit donc :

$$A = 1 - a_q X^q + \sum_{k=q+1}^p a_k X^k \quad \text{avec } a_q \neq 0 \quad \text{et } 1 \leq q \leq p.$$

Posons $a_q = \rho e^{-i\theta}$ avec $\rho \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$. Pour $z = r e^{i\theta/q}$, avec $r > 0$, on a :

$$A(z) = 1 - \rho r^q + \sum_{k=q+1}^p a_k r^k e^{ik\theta/q}$$

et donc :

$$|A(z)| \leq |1 - \rho r^q| + \sum_{k=q+1}^p |a_k| r^k.$$

Si l'on suppose $r \leq \sqrt[q]{1/\rho}$, on a $|1 - \rho r^q| = 1 - \rho r^q$ et donc :

$$|A(z)| - 1 \leq -\rho r^q + \sum_{k=q+1}^p |a_k| r^k.$$

Ce majorant définissant une fonction polynomiale de r , équivalente en 0 à $-\rho r^q$, il est strictement négatif au voisinage de 0.

Par conséquent, il existe $z \in \mathbb{C}$ tel que $|A(z)| < 1 = \alpha$, ce qui est contradictoire.

□ MPSI

EXERCICES

- 1.** Soit P un polynôme de $\mathbb{K}[X]$.

Déterminer le degré du polynôme :

$$P(X+1) - P(X)$$

en fonction du degré de P .

- 2.** Soit $n \in \mathbb{N}$, factoriser le polynôme :

$$P = 1 + \frac{X}{1} + \frac{X(X+1)}{2!} + \cdots + \frac{X(X+1)\dots(X+n-1)}{n!}.$$

- 3.** Montrer qu'il n'existe pas de polynôme $P \in \mathbb{C}[X]$ tel que :

$$\forall z \in \mathbb{C}, \quad P(z) = \bar{z}.$$

- 4.** Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$.

Déterminer le reste de la division du polynôme $(\cos\theta + X \sin\theta)^n$ par $X^2 + 1$.

- 5.** Calculer la valeur du polynôme :

$$P = 2X^5 - 4X^4 - 2X^3 + 3X^2 - 5X - 4$$

en $1 + \sqrt{2}$ (on utilisera la division euclidienne de P par un polynôme à coefficients rationnels qui s'annule pour $1 + \sqrt{2}$).

- 6.** Déterminer tous les polynômes de $\mathbb{C}[X]$ dont la fonction polynomiale associée est T -périodique ($T \in \mathbb{C}^*$).

- 7.** Soit $n \in \mathbb{N}$, montrer que le polynôme :

$$(X-1)^{n+2} + X^{2n+1} \in \mathbb{C}[X]$$

est divisible par $X^2 - X + 1$.

- 8.** Trouver les racines dans \mathbb{C} du polynôme $X^4 + 12X - 5$ sachant qu'il possède deux racines dont la somme est 2.

- 9.** On considère le polynôme :

$$X^4 + pX^2 + qX + r$$

($r \neq 0$) dont les racines dans \mathbb{C} sont notées x_1, x_2, x_3, x_4 .
Calculer en fonction de p, q , et r :

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \frac{1}{x_4}$$

puis :

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} + \frac{1}{x_4^2}.$$

- 10.** Déterminer tous les polynômes P tels que :

$$P(2) = 6, \quad P'(2) = 1 \quad \text{et} \quad P''(2) = 4$$

et :

$$\forall n \geq 3, \quad P^{(n)}(2) = 0.$$

- 11.** Trouver une condition nécessaire et suffisante sur n pour que le polynôme $X^{2n} + X^n + 1$ soit divisible par $1 + X + X^2$.

- 12.** Soit n un entier naturel supérieur ou égal à 1.

Trouver une condition nécessaire et suffisante sur a et b pour que $P = aX^{n+1} + bX^n + 1$ soit divisible par $(X - 1)^2$.

- 13.** Soit $n \in \mathbb{N}^*$. Trouver le reste de la division euclidienne du polynôme :

$$X^n + nX^{n-1} + X^2 + 1$$

par $(X + 1)^2$.

- 14.** Calculer le PGCD des deux polynômes : $X^5 - 4X^4 + 6X^3 - 6X^2 + 5X - 2$ et $X^4 + X^3 + 2X^2 + X + 1$.

- 15.** Décomposer les polynômes suivants :

a) $X^4 + X^2 + 1$

b) $X^8 + X^4 + 1$

c) $X^6 + 1$

en produits de polynômes irréductibles sur $\mathbb{R}[X]$.

16. Soient P un polynôme de $\mathbb{C}[X]$ et a un nombre complexe.

Donner une condition nécessaire et suffisante sur P et a pour que a soit racine de multiplicité 3 du polynôme :

$$Q(X) = (X - a)(P'(X) + P'(a)) - 2(P(X) - P(a)).$$

17. Soit $n \in \mathbb{N}^*$, montrer que les racines distinctes de 1 du polynôme :

$$P(X) = nX^n - X^{n-1} - X^{n-2} - \cdots - X - 1$$

sont de module strictement inférieur à 1 et que toutes les racines de P sont simples.

On pourra considérer le polynôme $Q(X) = (X - 1)P(X)$.

18. Soit P un polynôme de $\mathbb{K}[X]$

Montrer que $P(P(X)) - X$ est divisible par $P(X) - X$.

19. Soient P , A et B trois polynômes de $\mathbb{K}[X]$ avec $\deg P \geq 1$ tels que $A(P(X))$ divise $B(P(X))$.

Montrer que A divise B .

20. Soient n et p deux entiers naturels non nuls tels que $n \geq p$.

Faire la division euclidienne de $X^n - 1$ par $X^p - 1$ (on donnera l'expression du quotient et du reste).

Donner une condition nécessaire et suffisante pour que $X^n - 1$ soit divisible par $X^p - 1$.

21. Soient n et p deux entiers naturels non nuls et $P = \sum_{k=0}^n a_k X^k$ un polynôme de $\mathbb{C}[X]$.

Montrer que le reste de la division euclidienne de P par $X^p - 1$ est :

$$R = \sum_{k=0}^n a_k X^{r_k}$$

où r_k désigne le reste de la division de k par p .

22. Soient n et p deux entiers naturels non nuls.

Calculer le PGCD de $X^n - 1$ et de $X^p - 1$.

- 23.** On considère le polynôme $P = X^3 + pX^2 + qX + r$ dans $\mathbb{C}[X]$. Trouver une condition nécessaire et suffisante sur p , q et r pour qu'une des racines de P soit la somme des deux autres.
- 24.** Soient p , q et r trois nombres complexes et a , b , c les trois racines de l'équation $x^3 + px^2 + qx + r = 0$. Calculer en fonction de p , q et r l'expression :
- $$S = a^3b + a^3c + b^3c + b^3a + c^3a + c^3b.$$
- 25.** Trouver une condition nécessaire et suffisante pour que les racines dans \mathbb{C} de l'équation :
- $$x^3 + ax^2 + bx + c = 0$$
- soient en progression arithmétique.
- 26.** Soient x_1 , x_2 et x_3 les trois racines complexes du polynôme $X^3 + pX + q$.
- Trouver le polynôme normalisé du troisième degré dont les racines sont $x_1 + x_2$, $x_2 + x_3$ et $x_1 + x_3$.
 - Trouver le polynôme normalisé du troisième degré dont les racines sont x_1x_2 , x_2x_3 et x_1x_3 .
- 27.** Soient a et b deux nombres complexes avec $b \neq 0$. Trouver les polynômes de degré 5 tel que $P(X) + a$ soit divisible par $(X + b)^3$ et $P(X) - a$ par $(X - b)^3$.
- 28.** Soit P un polynôme de $\mathbb{R}[X]$ scindé dans \mathbb{R} et $\lambda \in \mathbb{R}^*$. Montrer que le polynôme $P^2 + \lambda^2$ n'a que des racines simples.
- 29.** Soit P un polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à 2. Montrer que les images dans le plan complexe des zéros de P' peuvent s'écrire comme des barycentres à coefficients positifs des images dans le plan complexe des zéros de P .
- $\left(\text{On considérera la fraction } \frac{P'}{P} \right).$
- 30.** Soit P un polynôme de $\mathbb{R}[X]$. Montrer que les deux propriétés suivantes sont équivalentes :
- $\forall x \in \mathbb{R}, P(x) \geq 0$
 - $\exists A \in \mathbb{R}[X], \exists B \in \mathbb{R}[X], A^2 + B^2 = P$.

31. Déterminer les polynômes non nuls de $\mathbb{C}[X]$ qui vérifient :

$$P(X^2) + P(X)P(X+1) = 0.$$

32. Montrer que les polynômes P et Q sont premiers entre eux si et seulement si $P+Q$ et PQ le sont.

33. Soient A et B deux polynômes.

Trouver tous les polynômes C tels que chacun des trois polynômes A , B et C divise le produit des deux autres.

34. a) Soit P un polynôme de $\mathbb{C}[X]$ de degré n .

Montrer que si P a k racines distinctes dans \mathbb{C} , alors $P \wedge P'$ est de degré $n - k$.

b) Le résultat précédent est-il vrai dans $\mathbb{R}[X]$?

c) Trouver tous les polynômes P de $\mathbb{C}[X]$ de degré n tel que P' divise P , $P(1) = 0$ et $P(0) = 1$.

35. Soit $n \geqslant 1$.

a) Montrer qu'il existe un unique couple de polynômes de degrés strictement inférieurs à n tel que :

$$(1-X)^n P(X) + X^n Q(X) = 1.$$

b) Montrer que :

$$P(X) = Q(1-X) \text{ et } Q(X) = P(1-X).$$

c) Montrer qu'il existe une constante k telle que :

$$(1-X)P'(X) - nP(X) = kX^{n-1}$$

d) En déduire les coefficients de P .

36. Soient $(a_0, a_1, \dots, a_n) \in \mathbb{Z}^{n+1}$

On considère l'équation :

$$P(x) = a_0 + a_1x + \cdots + a_nx^n = 0$$

a) Montrer que si $r = \frac{p}{q}$ (avec $p \wedge q = 1$) est racine de l'équation alors $q \mid a_n$ et

$$p \mid a_0.$$

Que peut-on conclure si $a_n = 1$?

b) Montrer alors que :

$$\forall m \in \mathbb{Z}, p - mq \mid P(m)$$

c) Donner une décomposition en produit de facteurs irréductibles sur $\mathbb{Q}[X]$ des polynômes suivants :

- $X^3 - X - 1$
- $3X^3 - 2X^2 - 2X - 5$
- $6X^4 + 19X^3 - 7X^2 - 26X + 12 = 0$

d) On suppose qu'il existe deux entiers relatifs distincts m_1 et m_2 tels que :

$$|P(m_1)| = 1 \text{ et } |P(m_2)| = 1.$$

Montrer que si $|m_1 - m_2| > 2$, alors P n'a pas de racine rationnelle.

Montrer que si $|m_1 - m_2| \leq 2$ et si P a une racine rationnelle alors cette racine est nécessairement $\frac{m_1 + m_2}{2}$.

Chapitre 26

Fractions rationnelles

Dans tout ce chapitre, \mathbf{K} désigne le corps \mathbb{R} des réels ou le corps \mathbb{C} des complexes.

PCSI Ce chapitre est hors programme en PCSI.

PCSI

MPSI 1. Corps des fractions rationnelles

1.1 Définition, règles de calcul

L'anneau $\mathbf{K}[X]$ est intègre ; on admet que l'on peut définir son corps des fractions $\mathbf{K}(X)$ appelé *corps des fractions rationnelles* à coefficients dans \mathbf{K} . C'est un corps admettant $\mathbf{K}[X]$ comme sous-anneau et dont tout élément F s'écrit sous la forme :

$$F = \frac{P}{Q} \quad \text{avec} \quad (P, Q) \in \mathbf{K}[X]^2 \quad \text{et} \quad Q \neq 0.$$

Un tel couple (P, Q) s'appelle un *représentant* de la fraction rationnelle F .

On a les règles de calcul suivantes (dans lesquelles Q , Q_1 et R sont des polynômes non nuls) :

- $\frac{P}{Q} + \frac{P_1}{Q_1} = \frac{PQ_1 + P_1Q}{QQ_1}$
- $\frac{PP_1}{QQ_1} = \frac{P_1P}{Q_1Q}$
- $\frac{P}{Q} = \frac{P_1}{Q_1} \iff PQ_1 = P_1Q$

- $\frac{P}{Q} = \frac{P}{Q}$
- Si $P \neq 0$, $\left(\frac{P}{Q}\right)^{-1} = \frac{Q}{P}$.

Conjuguée d'une fraction rationnelle à coefficients complexes

Si (P, Q) et (P_1, Q_1) sont deux représentants d'une fraction rationnelle F à coefficients dans \mathbb{C} , alors $\frac{\overline{P}}{\overline{Q}} = \frac{\overline{P_1}}{\overline{Q_1}}$ puisque l'on a :

$$PQ_1 = P_1 Q \implies \overline{PQ_1} = \overline{P_1 Q}.$$

Cette fraction rationnelle est appelée *conjuguée* de F et notée \overline{F} .

Les propriétés sur les polynômes nous donnent immédiatement, pour $(F, G) \in \mathbb{C}(X)^2$:

$$\overline{F+G} = \overline{F} + \overline{G} \quad \text{et} \quad \overline{FG} = \overline{F}\overline{G}.$$

1.2 Représentant irréductible d'une fraction rationnelle

Définition 1

- On appelle *représentant irréductible* d'une fraction rationnelle F tout représentant (P, Q) de F où P et Q sont premiers entre eux.
- On appelle *représentant irréductible unitaire* d'une fraction rationnelle F tout représentant irréductible (P, Q) de F tel que Q soit un polynôme unitaire.

Proposition 1

- Si $\frac{P}{Q}$ est une forme irréductible d'une fraction rationnelle $F = \frac{P_1}{Q_1}$, alors :

$$\exists R \in \mathbb{K}[X] : (P_1 = RP \quad \text{et} \quad Q_1 = RQ).$$

- Si $\frac{P}{Q}$ et $\frac{P_1}{Q_1}$ sont deux formes irréductibles d'une fraction F , alors :

$$\exists \lambda \in \mathbb{K}^* : (P_1 = \lambda P \quad \text{et} \quad Q_1 = \lambda Q).$$

- Toute fraction rationnelle admet un représentant irréductible unitaire et un seul.

Démonstration

- On a $PQ_1 = QP_1$ et donc Q divise PQ_1 . Comme P et Q sont premiers entre eux, on en déduit d'après le théorème de Gauss que Q divise Q_1 .

On peut donc trouver un polynôme $R \in \mathbf{K}[X]$ tel que $Q_1 = RQ$, et l'on a :

$$P_1 = \frac{PQ_1}{Q} = RP.$$

- Soient (P, Q) et (P_1, Q_1) deux représentants irréductibles de F . Alors, d'après le point précédent, Q divise Q_1 et Q_1 divise Q . Les polynômes Q et Q_1 sont donc associés et par conséquent, le polynôme R est une constante non nulle.

- L'unicité est évidente d'après ce qui précéde.

Pour l'existence, il suffit de prendre un représentant quelconque (P, Q) , de diviser P et Q par leur PGCD et de diviser le numérateur et le dénominateur par le coefficient dominant de ce dernier (qui est non nul). \square

Remarque Un polynôme P admet $P/1$ pour représentant irréductible unitaire. En particulier, $0/1$ est la forme irréductible unitaire de la fraction rationnelle nulle.

Exemple Soit $F \in \mathbb{C}(X)$ telle que $\overline{F} = F$. Si (P, Q) est un représentant irréductible unitaire de F , alors :

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

D'après la proposition précédente, il existe donc un polynôme R tel que $\overline{Q} = RQ$. Comme Q et \overline{Q} sont deux polynômes unitaires de même degré, on en déduit $R = 1$ et par suite $Q = \overline{Q} \in \mathbb{R}[X]$ et $P = \overline{P} \in \mathbb{R}[X]$. Par suite, $F \in \mathbb{R}(X)$.

La réciproque étant évidente, on a donc, pour $F \in \mathbb{C}(X)$, l'équivalence :

$$F \in \mathbb{R}(X) \iff \overline{F} = F.$$

1.3 Degré d'une fraction rationnelle

Définition 2

Si F est une fraction rationnelle, la quantité $\deg P - \deg Q \in \mathbb{Z} \cup \{-\infty\}$ ne dépend pas du représentant (P, Q) choisi pour la fraction F . On l'appelle *degré de F* et on le note $\deg(F)$ ou $\deg F$.

En particulier, on a $\deg 0 = -\infty$.

Démonstration On peut bien définir ainsi le degré de F car :

- la quantité $\deg P - \deg Q$ est toujours définie puisque Q étant non nul, on a $\deg Q \neq -\infty$,

- la quantité $\deg P - \deg Q$ ne dépend pas du représentant (P, Q) choisi pour la fraction rationnelle F , car si (P_1, Q_1) est un autre représentant, on a $PQ_1 = QP_1$ et donc :

$$\deg P + \deg Q_1 = \deg(PQ_1) = \deg(P_1Q) = \deg P_1 + \deg Q$$

c'est-à-dire, puisque $\deg Q$ et $\deg Q_1$ sont des entiers naturels :

$$\deg P - \deg Q = \deg P_1 - \deg Q_1.$$

□

Remarque Un polynôme P est égal à la fraction $\frac{P}{1}$ dont le degré est $\deg P$. Donc la définition du degré sur $\mathbb{K}(X)$ prolonge celle du degré défini sur $\mathbb{K}[X]$.

Proposition 2

Étant données deux fractions rationnelles F_1 et F_2 de $\mathbb{K}(X)$, on a :

1. $\deg(F_1 + F_2) \leq \max(\deg F_1, \deg F_2)$
2. $\deg(F_1F_2) = \deg F_1 + \deg F_2$

Démonstration Posons $F_1 = \frac{P_1}{Q_1}$ et $F_2 = \frac{P_2}{Q_2}$.

1. On a alors $F_1 + F_2 = \frac{P_1Q_2 + P_2Q_1}{Q_1Q_2}$, ce qui donne :

$$\deg(F_1 + F_2) = \deg(P_1Q_2 + P_2Q_1) - \deg(Q_1Q_2).$$

Supposons, par exemple, $\deg F_1 \geq \deg F_2$. Alors :

$$\deg P_1 - \deg Q_1 \geq \deg P_2 - \deg Q_2,$$

et puisque $\deg Q_1$ et $\deg Q_2$ sont des entiers :

$$\deg(P_1Q_2) = \deg P_1 + \deg Q_2 \geq \deg P_2 + \deg Q_1 = \deg(P_2Q_1).$$

Les résultats sur le degré d'une somme de polynômes impliquent :

$$\deg(F_1 + F_2) \leq \deg(P_1Q_2) - \deg(Q_1Q_2) = \deg P_1 - \deg Q_1$$

ce qui donne :

$$\deg(F_1 + F_2) \leq \deg F_1 = \max(\deg F_1, \deg F_2).$$

2. On a de même $F_1F_2 = \frac{P_1P_2}{Q_1Q_2}$, ce qui donne :

$$\deg(F_1F_2) = \deg(P_1P_2) - \deg(Q_1Q_2)$$

$$= \deg P_1 + \deg P_2 - \deg Q_1 - \deg Q_2$$

$$= \deg F_1 + \deg F_2.$$

□

Exemple La somme de deux fractions rationnelles de degrés strictement négatifs est une fraction rationnelle de degré strictement négatif.

1.4 Racines, pôles

Définition 3

Soit F une fraction rationnelle de forme irréductible $\frac{P}{Q}$.

- On appelle *racine* de F toute racine de P .
- On appelle *pôle* de F toute racine de Q .
- Si a est une racine (respectivement un pôle) de $F \neq 0$, l'*ordre de multiplicité* de a est l'ordre de multiplicité de a en tant que racine du polynôme P (respectivement Q).

Démonstration Vérifions que ces notions ne dépendent pas du représentant irréductible choisi.

La proposition 1 de la page 756 nous dit que les formes irréductibles de F sont $\frac{\lambda P}{\lambda Q}$, avec $\lambda \in \mathbb{K}^*$. Donc les racines (respectivement les pôles) de F sont les racines de P (respectivement de Q) dans toute forme irréductible $\frac{P}{Q}$. \square

Remarque Un élément a de \mathbb{K} ne peut pas être à la fois racine et pôle d'une fraction rationnelle F . Sinon, en prenant une forme irréductible $F = \frac{P}{Q}$, on aurait $P(a) = Q(a) = 0$, et donc les polynômes P et Q seraient divisibles par $X - a$, ce qui contredirait le caractère irréductible de $\frac{P}{Q}$.

► **Attention** Les racines (respectivement les pôles) d'une fraction rationnelle F ne peuvent être obtenues qu'à partir d'une forme irréductible de F .

Par exemple, $F = \frac{X^3 - 1}{X^2 - 1}$ n'admet 1 ni comme racine ni comme pôle, car $F = \frac{X^2 + X + 1}{X + 1}$.

Définition 4

Soit F une fraction rationnelle, de forme irréductible $\frac{P}{Q}$, dont on désigne par A l'ensemble des pôles.

- Pour $\alpha \in \mathbb{K} \setminus A$, on définit $F(\alpha) = \frac{P(\alpha)}{Q(\alpha)}$.
- La fonction définie sur $\mathbb{K} \setminus A$ par $x \mapsto F(x)$ est appelée *fonction rationnelle* associée à la fraction rationnelle F .

Exemple La fonction rationnelle f associée à la fraction rationnelle $F = \frac{X^2 - 4X + 3}{X^2 - 1}$ est définie sur $\mathbb{R} \setminus \{-1\}$ par $f(x) = \frac{x-3}{x+1}$.

Remarques

- Si $F \in \mathbb{K}(X)$ s'écrit sous une forme $F = \frac{P_1}{Q_1}$ non nécessairement irréductible, et si $Q_1(\alpha) \neq 0$, alors α n'est pas pôle de F et on a :

$$F(\alpha) = \frac{P_1(\alpha)}{Q_1(\alpha)}.$$

- Étant donnés deux fractions rationnelles F et G , deux scalaires λ et μ , et $\alpha \in \mathbb{K}$ qui n'est pas pôle ni de F ni de G , alors α n'est pas pôle ni de $\lambda F + \mu G$ ni de FG , et on a :

$$\begin{aligned} (\lambda F + \mu G)(\alpha) &= \lambda F(\alpha) + \mu G(\alpha) \\ (FG)(\alpha) &= F(\alpha) G(\alpha). \end{aligned}$$

1.5 Composition

Si $F = \frac{P}{Q}$ est une fraction rationnelle et R un polynôme non constant, alors le polynôme $Q \circ R$ est non nul, puisqu'il est de degré $\deg Q \deg R$.

De plus, si (P_1, Q_1) est un autre représentant de la fraction F , l'égalité $PQ_1 = P_1Q$ entraîne $(P \circ R)(Q_1 \circ R) = (P_1 \circ R)(Q \circ R)$. Le quotient $\frac{P \circ R}{Q \circ R}$ ne dépend donc pas du représentant (P, Q) choisi pour la fraction rationnelle F . C'est une fraction rationnelle dont le degré vaut $\deg F \deg R$, que l'on appelle *composée* de F par R et que l'on note $F(R)$.

Exemples

- Si $F \in \mathbb{K}(X)$, on a $F(X) = F$.
- Si $\alpha \in \mathbb{K}$ et $F \in \mathbb{K}(X)$, la fraction rationnelle $F(X - \alpha)$ est de même degré que F . L'ensemble de ses racines (respectivement de ses pôles) est $\alpha + A$, où A est l'ensemble des racines (respectivement des pôles) de F .
- Une fraction rationnelle F est dite *paire* si $F(X) = F(-X)$.

Si P et Q sont deux polynômes pairs, alors $\frac{P}{Q}$ est évidemment paire.

Réiproquement, si $F = \frac{P}{Q}$ est paire, alors on peut trouver un représentant (P_1, Q_1) de F avec P_1 et Q_1 pairs.

En effet, quitte à considérer $X P$ et $X Q$, on peut supposer que Q n'est pas impair. On a alors :

$$F(X) = \frac{P(X)}{Q(X)} = \frac{P(-X)}{Q(-X)} = \frac{P(X) + P(-X)}{Q(X) + Q(-X)}$$

avec $P(X) + P(-X)$ et $Q(X) + Q(-X)$ deux polynômes pairs, le deuxième étant non nul.

4. De même, une fraction rationnelle F est *impaire*, c'est-à-dire vérifie $F(X) = -F(-X)$, si, et seulement si, elle est de la forme $\frac{P}{Q}$ avec P un polynôme impair et Q un polynôme pair.

2. Décomposition en éléments simples

2.1 Partie entière

Proposition 3

Toute fraction rationnelle F s'écrit de façon unique comme la somme d'un polynôme, appelé *partie entière* de F , et d'une fraction rationnelle de degré strictement négatif.

Démonstration

Unicité. Supposons :

$$F = E_1 + F_1 = E_2 + F_2$$

avec $(E_1, E_2) \in \mathbb{K}[X]^2$, $(F_1, F_2) \in \mathbb{K}(X)^2$, $\deg F_1 < 0$ et $\deg F_2 < 0$.

Alors $E_1 - E_2$ est un polynôme, et comme il est égal à $F_2 - F_1$, son degré est strictement négatif. Donc $E_1 - E_2 = 0$ c'est-à-dire $E_1 = E_2$ et par suite $F_1 = F_2$.

Existence. Soit $F = \frac{P}{Q}$ une fraction rationnelle, avec $Q \neq 0$. Si l'on appelle E le quotient et R

le reste de la division euclidienne de P par Q , on obtient :

$$F = E + \frac{R}{Q} \quad \text{avec} \quad \deg R < \deg Q,$$

ce qui constitue l'écriture cherchée. □

■ **Méthode** D'après la démonstration précédente, la partie entière d'une fraction rationnelle $\frac{P}{Q}$ est le quotient de la division euclidienne du numérateur P par le dénominateur Q .

Exemples

- Si $\deg F < 0$, alors sa partie entière est nulle.

2. Si F est de degré 0, alors sa partie entière est le polynôme constant quotient du coefficient dominant du numérateur par celui du dénominateur.
3. La partie entière de la fraction $\frac{X^5}{(X^2 + X + 1)^2}$ est $X - 2$.
4. Si F est une fraction rationnelle paire, alors sa partie entière est paire.

En effet, si :

$$F(X) = E(X) + F_0(X) \quad \text{avec} \quad E \in \mathbb{K}[X] \quad \text{et} \quad \deg F_0 < 0$$

alors on a :

$$F(X) = F(-X) = E(-X) + F_0(-X)$$

avec $E(-X) \in \mathbb{K}[X]$ et $\deg F_0(-X) < 0$.

L'unicité de la partie entière nous donne alors $E(X) = E(-X)$.

5. De même, la partie entière d'une fraction rationnelle impaire est impaire.

6. La fraction rationnelle $F = \frac{X^5 + X^3 + X}{(X^2 + 1)^2} = \frac{X^5 + \dots}{X^4 + \dots}$ a une partie entière de la forme $X + \alpha$. Comme F est impaire, on a $\alpha = 0$ et la partie entière de F est donc X .

2.2 Partie polaire

Proposition 4

Si F est une fraction rationnelle admettant a pour pôle d'ordre n , il existe un unique n -uplet de scalaires $(\lambda_p)_{p \in \llbracket 1, n \rrbracket}$ et une unique fraction F_0 n'admettant pas a pour pôle tels que :

$$F = \sum_{p=1}^n \frac{\lambda_p}{(X - a)^p} + F_0.$$

La quantité :

$$\sum_{p=1}^n \frac{\lambda_p}{(X - a)^p}$$

s'appelle la *partie polaire* de F relative au pôle a .

Démonstration

Unicité. Supposons l'existence de deux n -uplets distincts $(\lambda_p)_{p \in \llbracket 1, n \rrbracket}$ et $(\mu_p)_{p \in \llbracket 1, n \rrbracket}$ et de deux fractions rationnelles F_1 et F_2 n'admettant pas a pour pôle vérifiant :

$$F = \sum_{k=1}^n \frac{\lambda_k}{(X - a)^k} + F_1 = \sum_{k=1}^n \frac{\mu_k}{(X - a)^k} + F_2$$

et prenons $p = \max\{k \in \llbracket 1, n \rrbracket \mid \lambda_k \neq \mu_k\}$.

Comme $\forall k \in [p+1, n]$, $\lambda_k = \mu_k$, on a :

$$\sum_{k=1}^p \frac{\lambda_k}{(X-a)^k} + F_1 = \sum_{k=1}^p \frac{\mu_k}{(X-a)^k} + F_2$$

ce qui, en multipliant par $(X-a)^p$, donne :

$$\lambda_p + \sum_{k=1}^{p-1} \lambda_k (X-a)^{p-k} + (X-a)^p F_1 = \mu_p + \sum_{k=1}^{p-1} \mu_k (X-a)^{p-k} + (X-a)^p F_2.$$

En substituant a à X dans cette égalité de fractions rationnelles n'admettant pas a pour pôle, on obtient $\lambda_p = \mu_p$ ce qui est en contradiction avec la définition de p .

D'où l'unicité de la famille $(\lambda_p)_{p \in [1, n]}$ et par suite de la fraction $F_0 = F - \sum_{k=1}^n \frac{\lambda_k}{(X-a)^k}$.

Existence. Soit $F = \frac{P}{(X-a)^n Q_1}$ avec Q_1 un polynôme unitaire tel que $Q_1(a) \neq 0$.

Les polynômes Q_1 et $(X-a)^n$ sont premiers entre eux, puisque le seul facteur irréductible de $(X-a)^n$ est $(X-a)$, et que ce dernier ne divise pas Q_1 .

D'après l'identité de Bézout, on peut donc trouver des polynômes U et V tels que $Q_1 U + (X-a)^n V = 1$. On a alors :

$$F = \frac{PU}{(X-a)^n} + \frac{PV}{Q_1}.$$

La formule de Taylor permet d'écrire :

$$(PU)(X) = \sum_{p=0}^{+\infty} \alpha_p (X-a)^p,$$

ce qui entraîne :

$$\frac{PU}{(X-a)^n} = \sum_{p=0}^{n-1} \frac{\alpha_p}{(X-a)^{n-p}} + R$$

où R est un polynôme.

Alors :

$$F = \sum_{p=0}^{n-1} \frac{\alpha_p}{(X-a)^{n-p}} + R + \frac{PV}{Q_1}$$

et la fraction rationnelle $R + \frac{PV}{Q_1}$ n'admet pas a pour pôle. □

Remarques

- On peut remarquer l'analogie avec un développement limité : on cherche à écrire la fraction comme combinaison linéaire de puissances de $X-a$.
- Si l'on désigne par a_1, a_2, \dots, a_p les autres pôles de F et par r_1, r_2, \dots, r_p leurs ordres de multiplicité respectifs, alors F_0 admet comme pôles a_1, a_2, \dots, a_p d'ordres de multiplicité respectifs r_1, r_2, \dots, r_p .

En effet, soit $\frac{P}{Q}$ une forme irréductible de F et R la partie polaire associée à a . La fraction $F - R$ n'admet pas a pour pôle et s'écrit sous la forme (non forcément irréductible) :

$$F - R = \frac{P_p}{Q} \quad \text{avec} \quad P_p \in \mathbb{K}[X].$$

Si l'on désigne par $\frac{A}{B}$ la forme irréductible de $F - R$, le polynôme B divise Q donc admet au plus pour racines a_1, a_2, \dots, a_p d'ordres respectifs $\alpha_1, \alpha_2, \dots, \alpha_p$ avec $0 \leq \alpha_i \leq r_i$ pour tout $i \in [1, p]$. L'égalité $F = R + \frac{A}{B}$ prouve alors, en réduisant au même dénominateur $(X - a)^n B$, que F admet a_i pour pôle d'ordre au plus α_i . Donc $\alpha_i = r_i$.

■ Méthode

Soit F une fraction rationnelle admettant a pour pôle.

- Si a est pôle d'ordre 1 de F , on peut écrire $F = \frac{P}{(X - a) Q_1}$ où Q_1 est un polynôme n'admettant pas a pour racine.
On cherche le scalaire λ_1 tel que :

$$F = \frac{\lambda_1}{X - a} + F_0$$

où F_0 est une fraction rationnelle qui n'admet pas a pour pôle.

En multipliant cette égalité par $X - a$, on obtient :

$$\frac{P}{Q_1} = \lambda_1 + (X - a) F_0$$

ce qui, en substituant a à X , donne $\frac{P(a)}{Q_1(a)} = \lambda_1$.

La partie polaire relative au pôle a est donc :

$$\frac{\lambda}{(X - a)} \quad \text{avec} \quad \lambda = \frac{P(a)}{Q_1(a)} = \frac{P(a)}{Q'(a)}$$

la dernière égalité venant de la relation $Q' = (X - a) Q_1' + Q_1$.

- Si a est pôle d'ordre 2 de F , on peut écrire $F = \frac{P}{(X - a)^2 Q_2}$ où Q_2 est un polynôme n'admettant pas a pour racine.

On cherche les scalaires λ_1 et λ_2 tels que :

$$F = \frac{\lambda_2}{(X - a)^2} + \frac{\lambda_1}{X - a} + F_0$$

où F_0 est une fraction rationnelle qui n'admet pas a pour pôle.

En multipliant cette égalité par $(X - a)^2$, on obtient :

$$\frac{P}{Q_2} = \lambda_2 + \lambda_1(X - a) + (X - a)^2 F_0$$

ce qui, en substituant a à X , donne $\frac{P(a)}{Q_2(a)} = \lambda_2$.

La partie polaire relative au pôle a est donc :

$$\boxed{\frac{\lambda_1}{X - a} + \frac{\lambda_2}{(X - a)^2} \text{ avec } \lambda_2 = \frac{P(a)}{Q_2(a)}}.$$

Pour trouver λ_1 , on peut alors retrancher $\frac{\lambda_2}{(X - a)^2}$ pour obtenir une fraction dont a n'est pas pôle, ou est pôle simple ce qui ramène au cas précédent.

- Dans le cas général, si a est pôle d'ordre n , alors $F = \frac{P}{(X - a)^n Q_n}$ avec $Q_n(a) \neq 0$, et la partie polaire relative au pôle a est :

$$\boxed{\sum_{p=1}^n \frac{\lambda_p}{(X - a)^p} \text{ avec } \lambda_n = \frac{P(a)}{Q_n(a)}}$$

comme on le voit en multipliant l'égalité :

$$F = \sum_{p=1}^n \frac{\lambda_p}{(X - a)^p} + F_0$$

par $(X - a)^n$ et en substituant a à X .

Comme de plus $Q = (X - a)^n Q_n$, alors on a $Q_n(a) = \frac{Q^{(n)}(a)}{n!}$ (par exemple en utilisant la formule de Leibniz ou la formule de Taylor).

Exemples

- Soit $F = \frac{X^5 + 1}{X(X - 1)^2}$.

- La partie polaire associée au pôle 0 est $\frac{\lambda}{X}$ avec $\lambda = 1$.

- La partie polaire associée au pôle 1 est $\frac{\lambda}{X-1} + \frac{\mu}{(X-1)^2}$ avec $\mu = 2$. Comme :

$$F - \frac{2}{(X-1)^2} = \frac{X^4 + X^3 + X^2 + X - 1}{(X-1)X}$$

on en déduit $\lambda = 3$.

- Soit $F = \frac{1}{X^5 - 1}$. Si ω est un pôle de F , c'est-à-dire une racine cinquième de l'unité, alors la partie polaire associée à ω est $\frac{\lambda}{X-\omega}$ avec :

$$\lambda = \frac{1}{5\omega^4} = \frac{\omega}{5\omega^5} = \frac{\omega}{5}.$$

2.3 Décomposition en éléments simples dans $\mathbb{C}(X)$

Dans cette partie, on suppose $\mathbf{K} = \mathbb{C}$. Le dénominateur d'une fraction rationnelle est donc scindé.

Théorème 5

Etant donnée une fraction rationnelle $F \in \mathbb{C}(X)$ dont les pôles sont a_1, a_2, \dots, a_n distincts deux à deux et d'ordres de multiplicité respectifs r_1, r_2, \dots, r_n , il existe un unique polynôme $E \in \mathbb{C}[X]$ et une unique famille de scalaires $(\lambda_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r_i}}$ tels que :

$$F = E + \sum_{i=1}^n \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X-a_i)^j} \right).$$

Autrement dit, toute fraction rationnelle de $\mathbb{C}(X)$ est la somme de sa partie entière et des parties polaires associées à chacun de ses pôles.

Cette décomposition s'appelle la *décomposition en éléments simples* dans $\mathbb{C}(X)$ de la fraction F .

Démonstration

Unicité. Si $F = E + \sum_{i=1}^n \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X-a_i)^j} \right)$, alors E est la partie entière de F puisque $F - E$

est une somme de fractions de degrés strictement négatifs

Pour $1 \leq k \leq n$, on a :

$$F = \sum_{j=1}^{r_k} \frac{\lambda_{k,j}}{(X-a_k)^j} + F_k$$

où la fraction $F_k = E + \sum_{i \neq k} \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X - a_i)^j} \right)$ n'admet pas a_k pour pôle.

Donc $\sum_{j=1}^{r_k} \frac{\lambda_{k,j}}{(X - a_k)^j}$ est la partie polaire de F associée au pôle a_k , ce qui prouve l'unicité de $\lambda_{k,1}, \lambda_{k,2}, \dots, \lambda_{k,r_k}$.

Existence. On a vu qu'en retranchant à une fraction rationnelle F la partie polaire associée à un de ses pôles, on obtient une fraction rationnelle dont les pôles sont les autres pôles de F , avec le même ordre de multiplicité que dans F .

Donc, en retranchant à une fraction rationnelle F les parties polaires associées à chacun de ses pôles, on obtient une fraction de forme irréductible $\frac{P}{Q}$ qui n'admet plus de pôle. Donc le polynôme Q n'a pas de racine, ce qui prouve qu'il est constant puisqu'il est scindé sur \mathbb{C} .

On a ainsi montré que F était la somme d'un polynôme et des parties polaires associées à chacun de ses pôles. \square

Exemples

- La partie entière de la fraction rationnelle $F = \frac{X^5 + 1}{X(X - 1)^2}$ est $X^2 + 2X + 3$.

L'exemple 1. de la page 765 nous donne donc :

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

- L'exemple 2. de la page ci-contre nous donne les parties polaires associées aux cinq pôles simples de la fraction rationnelle $F = \frac{1}{X^5 - 1}$.

Ces pôles sont $1, \omega_1 = e^{2i\pi/5}, \omega_2 = e^{4i\pi/5}, \overline{\omega_1}$ et $\overline{\omega_2}$. Comme la partie entière est nulle, on a :

$$F = \frac{1}{5(X - 1)} + \frac{\omega_1}{5(X - \omega_1)} + \frac{\overline{\omega_1}}{5(X - \overline{\omega_1})} + \frac{\omega_2}{5(X - \omega_2)} + \frac{\overline{\omega_2}}{5(X - \overline{\omega_2})}.$$

- Soit P un polynôme dont les racines sont a_1, a_2, \dots, a_n d'ordres de multiplicité respectifs r_1, r_2, \dots, r_n , c'est-à-dire un polynôme de la forme :

$$P = \lambda \prod_{i=1}^n (X - a_i)^{r_i} \quad \text{avec} \quad \lambda \in \mathbb{C}^*.$$

La décomposition de $\frac{P'}{P}$ en éléments simples s'obtient directement en écrivant (dérivée d'un produit) :

$$P' = \lambda \sum_{i=1}^n \left(r_i (X - a_i)^{r_i - 1} \prod_{j \neq i} (X - a_j)^{r_j} \right),$$

ce qui donne :

$$\frac{P'}{P} = \sum_{i=1}^n \frac{r_i}{X - a_i}.$$

Avec MAPLE, c'est la fonction `convert(..., parfrac)` qui retourne la décomposition en éléments simples d'une fraction rationnelle de $\mathbb{Q}(X)$ dont le dénominateur est scindé sur \mathbb{Q} . Lorsque son dénominateur n'est pas scindé sur \mathbb{Q} , il est de la responsabilité de l'utilisateur d'en obtenir une factorisation en produit de polynômes du premier degré.

Exemples

```
> F:=(X^6+X+1) / (X^5-4*X^3-2*X^2+3*X+2);
```

$$F := \frac{X^6 + X + 1}{X^5 - 4X^3 - 2X^2 + 3X + 2}$$

```
> convert(F,parfrac,X);
```

$$\begin{aligned} X - \frac{3}{8} \frac{1}{X - 1} + \frac{67}{27} \frac{1}{X - 2} + \frac{1}{6} \frac{1}{(X + 1)^3} - \frac{25}{36} \frac{1}{(X + 1)^2} \\ + \frac{409}{216} \frac{1}{X + 1} \end{aligned}$$

```
> alias(j=RootOf(X^2+X+1));
> P:=factor(x^3-1,{j});
```

$$P := (X - j)(X + 1 + j)(X - 1)$$

```
> F:=convert(1/P^2,parfrac,X);
> # Résultat non simplifié et sans intérêt.
> map(factor,F);
> # Applique factor à chaque terme de la somme.
```

$$\begin{aligned} & -\frac{2}{9} \frac{j}{X - j} - \frac{1}{9} \frac{j + 1}{(X - j)^2} + \frac{2}{9} \frac{j + 1}{X + 1 + j} + \frac{1}{9} \frac{j}{(X + 1 + j)^2} \\ & - \frac{2}{9} \frac{1}{X - 1} + \frac{1}{9} \frac{1}{(X - 1)^2} \end{aligned}$$

2.4 Méthodes pratiques

Soit $F = \frac{P}{Q}$ une fraction rationnelle à coefficients complexes dont les pôles sont $\alpha_1, \alpha_2, \dots, \alpha_n$ d'ordres de multiplicité respectifs r_1, r_2, \dots, r_n . Sa décomposition en éléments simples est de la forme :

$$F = E + \sum_{i=1}^n \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X - \alpha_i)^j} \right).$$

- La détermination de la partie entière E se fait à l'aide de la division euclidienne de P par Q , division limitée puisque seul le quotient nous intéresse.
- Les coefficients λ_{i,r_i} se calculent immédiatement à l'aide des formules :

$$\lambda_{i,r_i} = \frac{P(\alpha_i)}{Q_i(\alpha_i)} = \frac{r_i! P(\alpha_i)}{Q^{(r_i)}(\alpha_i)}$$

avec $Q = (X - \alpha_i)^{r_i} Q_i$.

- Si tous les pôles sont simples, on a ainsi la décomposition en éléments simples de F . Sinon, on peut retrancher à F chaque fraction $\frac{\lambda_{i,r_i}}{(X - \alpha_i)^{r_i}}$ et recommencer avec la fraction ainsi obtenue. Mais il est souvent beaucoup plus rapide de déterminer les derniers coefficients en utilisant certaines des méthodes qui suivent.

Si la fraction est à coefficients réels...

Si F est une fraction rationnelle à coefficients réels et si α est un pôle non réel de F d'ordre r , alors $\bar{\alpha}$ est aussi un pôle d'ordre r et les coefficients des parties polaires associées à α et $\bar{\alpha}$ sont conjugués deux à deux.

En effet :

- Puisque le dénominateur Q de F est réel, si α est une racine non réelle de Q , alors $\bar{\alpha}$ est aussi racine de Q au même ordre de multiplicité.
- Si $F = \sum_{i=1}^r \frac{\lambda_i}{(X - \alpha)^i} + F_1$ où α n'est pas pôle de la fraction rationnelle F_1 , alors :

$$F = \overline{F} = \sum_{i=1}^r \frac{\overline{\lambda_i}}{(X - \bar{\alpha})^i} + \overline{F_1}$$

et la fraction rationnelle $\overline{F_1}$ n'admet pas $\bar{\alpha}$ pour pôle. Donc, la partie polaire associée au pôle $\bar{\alpha}$ est :

$$\sum_{i=1}^r \frac{\overline{\lambda_i}}{(X - \bar{\alpha})^i}$$

(unicité de la partie polaire).

Si la fraction est paire ou impaire...

Si la fraction rationnelle F est paire ou impaire et que a est un pôle de F d'ordre n , alors $-a$ est aussi pôle de F d'ordre n et la comparaison des décompositions en éléments simples de $F(X)$ et $F(-X) = \pm F(X)$ donne des relations entre les coefficients.

Exemple La fraction $F = \frac{4}{(X^2 - 1)^2}$ se décompose en éléments simples :

$$F = \frac{a}{X-1} + \frac{b}{X+1} + \frac{c}{(X-1)^2} + \frac{d}{(X+1)^2}.$$

On a :

$$F(X) = F(-X) = \frac{a}{-X-1} + \frac{b}{-X+1} + \frac{c}{(-X-1)^2} + \frac{d}{(-X+1)^2}.$$

L'unicité de la décomposition en éléments simples nous donne alors $a = -b$ et $c = d$.

- On a immédiatement $c = \frac{4}{(1+1)^2} = 1$, donc $c = d = 1$.
- Pour déterminer a et b , il suffit de substituer 0 à X , ce qui donne :

$$4 = -a + b + c + d = 2 - 2a,$$

donc $a = -1$ et $b = 1$. On a donc :

$$F = \frac{4}{(X^2 - 1)^2} = -\frac{1}{X-1} + \frac{1}{X+1} + \frac{1}{(X-1)^2} + \frac{1}{(X+1)^2}.$$

Si la fraction est de degré strictement négatif...

Soit F une fraction rationnelle de degré strictement négatif. Si f est la restriction à \mathbb{R} de sa fonction rationnelle associée, alors la fonction $x \mapsto x f(x)$ a une limite finie en l'infini : on peut ainsi trouver des relations entre les coefficients des termes en $\frac{1}{X - a_i}$ de la décomposition en éléments simples de F .

Exemple Soit la fraction rationnelle $F = \frac{4X^3}{(X^2 - 1)^2}$.

L'imparité de F nous dit que sa décomposition en éléments simples est du type :

$$F = \frac{a}{X-1} + \frac{a}{X+1} + \frac{b}{(X-1)^2} - \frac{b}{(X+1)^2}.$$

Alors $b = 1$ et puisque $\lim_{x \rightarrow \infty} x f(x) = 4$, on a $2a = 4$. Donc :

$$F = \frac{2}{X-1} + \frac{2}{X+1} + \frac{1}{(X-1)^2} - \frac{1}{(X+1)^2}.$$

S'il ne reste qu'un ou deux coefficients à calculer...

Lorsqu'il ne reste plus qu'un ou deux coefficients à déterminer, on peut substituer à X une ou deux valeurs simples.

Exemple Soit :

$$F = \frac{X^4 + 1}{(X+1)^2(X^2+1)} = 1 + \frac{a}{(X+1)^2} + \frac{b}{X+1} + \frac{c}{X-i} + \frac{\bar{c}}{X+i}.$$

On trouve d'abord :

$$c = \frac{i^4 + 1}{(i+i)(i+1)^2} = \frac{2}{(2i)^2} = -\frac{1}{2} \quad \text{et} \quad a = \frac{1+1}{1+1} = 1.$$

En substituant 0 à X , on obtient de plus :

$$1 = 1 + a + b - \frac{c}{i} + \frac{\bar{c}}{\bar{i}} = 2 + b$$

et donc $b = -1$. D'où :

$$F = \frac{X^4 + 1}{(X+1)^2(X^2+1)} = 1 + \frac{1}{(X+1)^2} - \frac{1}{X+1} - \frac{1}{2(X-i)} - \frac{1}{2(X+i)}.$$

EXERCICES

1. Montrer que si F_1 et F_2 sont deux fractions rationnelles, la partie entière de $F_1 + F_2$ est la somme des parties entières.

2. Décomposer en éléments simples sur $\mathbb{C}[X]$ les fractions suivantes :
 - a) $F = \frac{10X^3}{(X^2 + 1)(X^2 - 4)}$
 - b) $F = \frac{X^4 + 1}{X^4 + X^2 + 1}$
 - c) $F = \frac{X^3 - 1}{(X - 1)(X - 2)(X - 3)}$
 - d) $F = \frac{X^2}{(X^2 + X + 1)^2}$
 - e) $F = \frac{(X^2 + 4)^2}{(X^2 + 1)(X^2 - 2)^2}$

3. Simplifier les sommes suivantes :
 - a) $\sum_{k=1}^n \frac{1}{k(k+1)}$
 - b) $\sum_{k=1}^n \frac{1}{k(k+1)(k+2)}.$

4. Soit $n \in \mathbb{N}^*$. Décomposer en éléments simples sur $\mathbb{C}[X]$, les fractions :
 - a) $\frac{1}{X^n - 1}$
 - b) $\frac{X^{n-1}}{X^n - 1}$
 - c) $\frac{1}{(X - 1)(X^n - 1)}$

5. Soit F une fraction de $\mathbb{C}[X]$, $F = \frac{P}{Q}$ avec :

$$Q = (X - x_1)^{\lambda_1} \cdots (X - x_n)^{\lambda_n}$$

la fraction n'étant pas nécessairement sous forme irréductible.

Montrer que l'on peut écrire :

$$F = E + \sum_{i=1}^n \mathcal{P}_i$$

où :

$$\mathcal{P}_i = \sum_{j=1}^{\lambda_i} \frac{a_{i,j}}{(X - x_i)^j}.$$

Application : donner la décomposition en éléments simples de la fraction :

$$\frac{X^3 + aX^2 + bX + c}{(X - 1)^2(X + 1)}.$$

6. Soient a , b et c trois nombres complexes et F la fraction :

$$F(X) = \frac{aX^2 + bX + c}{(X - 1)^2(X - 2)^2}$$

Trouver une condition nécessaire et suffisante sur a , b et c pour que F admette une primitive rationnelle.

7. Calculer les dérivées d'ordre n des fonctions définies par :

a) $f(x) = \frac{1}{(x - a)(x - b)},$

b) $f(x) = \arctan x,$

c) $f(x) = \frac{1}{x^2 - 2x \cos a + 1},$

d) $f(x) = \frac{1}{x^2 - 2x \operatorname{ch} a + 1}.$

8. Réduire sous la forme $\frac{P(X)}{Q(X)}$ la fraction :

$$\sum_{i=1}^n \frac{\omega_i^2}{X - \omega_i}$$

où les ω_i sont les racines $n^{\text{èmes}}$ de l'unité ($n \geq 2$).

9. Montrer l'existence et l'unicité d'un polynôme P tel que :

$$\forall x \in \mathbb{R}, P(\cos x) = \cos(nx).$$

Quelles sont les racines de P ?

Décomposer $\frac{1}{P}$ en éléments simples.

10. Soient x_1, x_2, \dots, x_n n éléments distincts deux à deux.

On pose :

$$P(X) = (X - x_1)(X - x_2) \dots (X - x_n)$$

et :

$$F(X) = \frac{1}{P(X)^2}.$$

Décomposer F en éléments simples.

On exprimera les coefficients en fonction de $P'(x_i)$ et $P''(x_i)$.

11. Soit $n \in \mathbb{N}$.

Décomposer en éléments simples la fraction suivante :

$$F(X) = \frac{1}{X} + \frac{1!}{X(X+1)} + \dots + \frac{n!}{X(X+1)\dots(X+n)}.$$

12. Soit $n \in \mathbb{N}^*$.

a) Quel est le développement limité en 0 à l'ordre $n-1$ de $\frac{1}{(1-x)^n}$?

b) Décomposer en éléments simples sur $\mathbb{R}[X]$ la fraction :

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

c) Décomposer en éléments simples sur $\mathbb{R}[X]$ la fraction :

$$\frac{1}{(X-a)^n(X-b)^n}.$$

d) Trouver un couple (U, V) de polynômes de $\mathbb{R}[X]$ tels que :

$$(1-X)^n U(X) + X^n V(X) = 1.$$

13. Soient $a \in \mathbb{C}$ et F une fraction de $\mathbb{C}[X]$ de la forme :

$$F = \frac{P(X)}{(X-a)^n Q(X)}$$

avec $Q(a) \neq 0$.

Exprimer la partie polaire relative au pôle a à l'aide des dérivées $k^{\text{èmes}}$ de $G(X) = F(X)(X-a)^n$ en a .

14. On considère la fraction :

$$F(X) = \frac{1}{(X^3 - 1)^3}.$$

Calculer la partie polaire relative au pôle 1.

Puis, en remarquant que $F(jX) = F(j^2 X) = F(X)$, déterminer la décomposition en éléments simples de F .

15. Soit P un polynôme de $\mathbb{C}[X]$.

Montrer que si les racines de P sont réelles et simples alors le polynôme $Q = P'^2 - PP''$ n'a pas de racines réelles.

On considérera la fraction $-\left[\frac{P'(X)}{P(X)}\right]'$.

16. Soit P un polynôme de $\mathbb{R}[X]$ de degré n et à n racines simples réelles :

$$a_1 < a_2 < \dots < a_{n-1} < a_n.$$

On sait que P' a $n - 1$ racines réelles b_1, b_2, \dots, b_n vérifiant :

$$\forall i \in [1, n-1], \quad a_i < b_i < a_{i+1}$$

(voir exercice 8 du chapitre 12).

On pose $\delta_i = a_{i+1} - a_i$, montrer que :

$$a_i + \frac{\delta_i}{n} < b_i < a_{i+1} - \frac{\delta_i}{n}.$$

On décomposera la fraction $\frac{P'}{P}$ en éléments simples.

17. Soient a_i et α_i ($1 \leq i \leq n$), $2n$ scalaires.

Résoudre le système linéaire suivant :

$$\left\{ \begin{array}{l} \frac{x_1}{a_1 + \alpha_1} + \frac{x_2}{a_2 + \alpha_1} + \dots + \frac{x_n}{a_n + \alpha_1} = 1 \\ \frac{x_1}{a_1 + \alpha_2} + \frac{x_2}{a_2 + \alpha_2} + \dots + \frac{x_n}{a_n + \alpha_2} = 1 \\ \vdots \\ \frac{x_1}{a_1 + \alpha_n} + \frac{x_2}{a_2 + \alpha_n} + \dots + \frac{x_n}{a_n + \alpha_n} = 1 \end{array} \right.$$

18. Soient a, b et c trois nombres complexes.

Donner une expression simple de :

$$\begin{aligned} A = & \frac{a^2}{(a-b)(a-c)(b+c-a)} \\ & + \frac{b^2}{(b-a)(b-c)(c+a-b)} \\ & + \frac{c^2}{(c-a)(c-b)(a+b-c)} \end{aligned}$$

19. Soient x_1, x_2, \dots, x_n, n nombres complexes distincts et y_1, y_2, \dots, y_n, n nombres complexes.

On veut déterminer tous les polynômes P de $\mathbb{C}[X]$ vérifiant :

$$\forall i \in \{1, \dots, n\}, P(x_i) = y_i.$$

En considérant la fraction :

$$\frac{P}{(X - x_1)(X - x_2) \dots (X - x_n)}$$

montrer que les polynômes cherchés sont de la forme :

$$P = (X - x_1)(X - x_2) \dots (X - x_n)Q(X) + \sum_{i=1}^n \frac{y_i}{Q_i(x_i)} Q_i(X)$$

où Q est un polynôme quelconque de $\mathbb{C}[X]$ et :

$$Q_i = (X - x_1)(X - x_2) \dots (X - x_{i-1})(X - x_{i+1}) \dots (X - x_n).$$