Groupes, anneaux, corps, arithmétique

Sommaire

I Lois de composition

I.1 Généralités

Définition

Une *loi de composition* sur un ensemble E est une application de $E \times E$ vers E.

Notations

- Plutôt que *loi de composition*, on dit aussi *opération*, ou plus simplement *loi*.
- Plutôt que de noter par exemple $f(u,v)$ (notation *préfixée*) l'image du couple (u,v), on la note $u * v$, $u \mathsf{T} v$, $u + v$, etc. (notation *infixée*) et on parle alors des lois $*$, T, $+$, etc.
- On note souvent $(E,*)$ pour désigner un ensemble E muni d'une loi de composition $*$.

Exemples

- Les lois $\cup$ (union), $\cap$ (intersection) et Δ (différence symétrique) sur $\mathcal{P}(E)$.
- La loi $\circ$ (loi de composition) sur $\mathcal{F}(E)$, ensemble des applications de E dans E.
- Les lois $+$ et $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$.
  La loi $\times$est notée par *juxtaposition* : ab plutôt que $a \times b$.
- Sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ (ou sur tout ensemble totalement ordonné) les lois min et max (minimum et maximum). Elles sont notées de façon préfixée : $\min(x,y)$, $\max(x,y)$.
- Deux autres lois notées de façon préfixée sont les lois pgcd et ppcm sur $\mathbb{N}$ ou $\mathbb{Z}$.
- La "soustraction" (opération $-$) est une loi de composition sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$, mais ce n'est pas une loi de composition sur $\mathbb{N}$ (elle n'est pas *partout définie*).
- Si E est muni de la loi $*$ et si X est un ensemble, on définit une loi, encore notée $*$, sur l'ensemble $\mathcal{F}(X,E)$ des applications de E vers X, en posant :

$$\forall\,(f,g) \in \mathcal{F}(E,X)^2, \forall\, x \in X, (f*g)(x) = f(x) * g(x)$$

  On définit ainsi $+$ et $\times$ sur l'ensemble des applications de X vers $\mathbb{R}$ (ou $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$).
  Quand $X = \mathbb{N}$, on définit ainsi la loi $*$ sur l'ensemble des suites de E.

I.2 Partie stable pour une loi

Définition

Soit E un ensemble muni de la loi $*$, et F une partie de E.
On dit que F est *stable* pour la loi $*$ si : $\forall\,(x,y) \in F \times F, x * y \in F$.
La restriction à $F \times F$ de la loi $*$ définit alors une loi de composition sur F, appelée *loi induite*, en général encore notée $*$.

Exemples

- $\mathbb{R}^-$ et $\mathbb{R}^+$ sont deux parties stables de $\mathbb{R}$, pour la loi $+$.
- Pour la loi $\times$, $\mathbb{R}^+$ est encore une partie stable, mais ce n'est pas le cas de $\mathbb{R}^-$.
- Toujours pour la loi $\times$, $[-1, 1]$ est une partie stable de $\mathbb{R}$.

I.3 Homomorphismes

Définition

Soient E et F deux ensembles, munis respectivement des lois $*$ et T.
Soit f une application de E dans F.
On dit que f est un *homomorphisme* (ou un *morphisme*) de $(E, *)$ dans (F, T) si :
$\forall (x, y) \in E^2, f(x * y) = f(x) \mathsf{T} f(y)$.

Cas particuliers

- Un morphisme de $(E, *)$ dans $(E, *)$ est appelé un *endomorphisme* de $(E, *)$.
- Un morphisme bijectif de $(E, *)$ dans (F, T) est appelé un *isomorphisme*.
- Si un tel isomorphisme existe, on dit que $(E, *)$ et (F, T) sont *isomorphes*.
  D'un point de vue mathématique, deux ensembles isomorphes ont exactement les mêmes propriétés, relativement à leurs lois respectives, et peuvent être considérés comme deux représentations différentes d'une même situation.
- Un isomorphisme de $(E, *)$ sur lui-même est appelé un *automorphisme* de $(E, *)$.

Proposition *(Isomorphisme réciproque)*

Soit f un isomorphisme de $(E, *)$ sur (F, T).
Alors f^{-1} est un isomorphisme de (F, T) sur $(E, *)$.

Exemples

- Le "passage au complémentaire" est un isomorphisme de $(\mathcal{P}(E), \cup)$ sur $(\mathcal{P}(E), \cap)$.
  Il est son propre isomorphisme réciproque.
- L'application $x \to \exp(x)$ est un isomorphisme de $(\mathbb{R}, +)$ sur $(\mathbb{R}^{+*}, \times)$.
  L'application $x \to \ln(x)$ est l'isomorphisme réciproque, de $(\mathbb{R}^{+*}, \times)$ sur $(\mathbb{R}, +)$.

I.4 Commutativité et associativité

Définition

Soit $*$ une loi sur un ensemble E.
On dit que la loi $*$ est *commutative* si : $\forall (x, y) \in E^2, x * y = y * x$.
On dit que la loi $*$ est *associative* si : $\forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$.

Exemples

- Les lois $+$ et $\times$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$, sont commutatives et associatives.
- Il en est de même avec les lois min et max sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
- Même chose avec les lois $\cup$, $\cap$, Δ sur $\mathcal{P}(E)$.
- La loi $-$ (sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et $\mathbb{C}$) n'est ni commutative, ni associative.
- La loi $\circ$ (composition des applications) est associative sur $\mathcal{F}(E)$. Elle n'est pas commutative dès que E possède au moins deux éléments (considérer les applications constantes).
- Si X est un ensemble et si E est muni de $*$ commutative (resp. associative), alors la loi $*$ définie sur $\mathcal{F}(X, E)$ par $\forall\, x \in X, (f * g)(x) = f(x) * g(x)$ est commutative (resp. associative).

Remarques

- Même si la loi $*$ sur E n'est pas commutative, il peut se trouver des éléments x et y de E qui vérifient $x * y = y * x$. On dit alors que x et y *commutent*.
  Par exemple, dans un plan affine euclidien $\mathcal{P}$, les rotations de même centre commutent deux à deux (pour la loi $\circ$).
- Quand une loi $*$ est associative, une expression comme $a * b * \ldots * x * y * z$ est définie sans ambiguité : les parenthèses qui indiquent dans quel ordre on combine les éléments deux à deux sont en effet inutiles.
  Si de plus la loi $*$ est commutative, alors on peut changer l'ordre des termes et en particulier regrouper ceux d'entre eux qui sont identiques.
  On notera ainsi $x * y * x * y * z * y * x * y = x^3 * y^4 * z$, à condition de poser, pour tout n de $\mathbb{N}$, $a^n = a * a * \ldots * a$ (a apparaissant n fois).
- L'associativité permet de noter :
  $\begin{cases} \min(x, y, z, \ldots) \text{ ou } \max(x, y, z, \ldots) \text{ pour tous réels } x,\ y,\ z, \text{ etc.} \\ \text{ppcm}(a, b, c, \ldots) \text{ ou } \text{pgcd}(a, b, c, \ldots) \text{ pour tous entiers } a,\ b,\ c, \text{ etc.} \end{cases}$

I.5 Distributivité

Définition

Soit E un ensemble muni de deux lois $*$ et T.

On dit que la loi $*$ est *distributive* par rapport à la loi T si, pour tous x, y, z de E :

$$\begin{cases} x * (y \mathsf{T} z) = (x * y) \mathsf{T} (x * z) & \text{(distributivité } \textit{à gauche}\text{)} \\ (x \mathsf{T} y) * z = (x * z) \mathsf{T} (y * z) & \text{(distributivité } \textit{à droite}\text{)} \end{cases}$$

Exemples et remarques

- Si la loi $*$ est commutative, l'une de ces deux propriétés implique l'autre.
- Dans $\mathcal{P}(E)$, les lois $\cup$ et $\cap$ sont distributives l'une par rapport à l'autre.
- Dans $\mathcal{P}(E)$, la loi $\cap$ est distributive par rapport à la loi Δ.
  En revanche la loi Δ n'est pas distributive par rapport à la loi $\cap$.
- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la loi $\times$ est distributive par rapport à la loi $+$.

– Si X est un ensemble et si E est muni de deux lois $*$ et T ($*$ étant distributive par rapport à T), on définit des lois homonymes sur $\mathcal{F}(X,E)$:
$\forall\, x \in X, (f*g)(x) = f(x)*g(x)$, et $(f\mathsf{T}g)(x) = f(x)\mathsf{T}g(x)$.
Alors, dans $\mathcal{F}(E,X)$, $*$ est encore distributive par rapport à T.
– La distributivité de $*$ par rapport à T (supposée ici associative) permet d'écrire :
$(a\mathsf{T}b)*(c\mathsf{T}d) = (a*c)\mathsf{T}(a*d)\mathsf{T}(b*c)\mathsf{T}(b*d)$.

I.6 Elément neutre

Définition

Soit E un ensemble muni d'une loi de composition $*$. Soit e un élément de E.
On dit que e est *élément neutre*, pour la loi $*$, si : $\forall\, a \in E, a*e = e*a = a$.

Remarque

Si la loi $*$ est commutative, l'égalité $a*e = e*a$ est automatiquement réalisée.

Proposition *(Unicité de l'élément neutre)*

L'élément neutre de E pour la loi $*$, s'il existe, est unique.

Remarques

– Il est beaucoup plus juste de dire que c'est E qui *possède* un élément neutre e pour la loi $*$, plutôt que de dire que c'est la loi $*$ qui possède l'élément neutre e.
– La notation $+$ peut être employée en dehors des ensembles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$: elle doit cependant être réservée aux lois commutatives. Dans ce cas, l'élément neutre, s'il existe, sera noté 0. De même, pour une loi noté multiplicativement (ou par juxtaposition), on pourra noter 1 l'élément neutre éventuel (s'il n'y a pas de risque d'ambiguité).

Exemples et remarques

– Dans $\mathcal{P}(E)$: $\emptyset$ est neutre pour la loi $\cup$ (et pour la loi Δ), et E est neutre pour la loi $\cap$.
– Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$: 0 est neutre pour la loi $+$ et 1 est neutre pour la loi $\times$.
– Dans $\mathcal{F}(E)$: l'application Identité id_E est neutre pour la loi $\circ$ (composition).
– Dans $\mathbb{N}$: 0 est neutre pour la loi max, et il n'y a pas de neutre pour la loi min.
– Dans $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$: les lois min et max n'ont pas d'élément neutre.
– Soit X un ensemble quelconque, et E un ensemble muni d'une loi $*$ avec un neutre e.
On munit $\mathcal{F}(X,E)$ de la loi $*$, définie par :
$\forall\,(f,g) \in \mathcal{F}(X,E)^2, \forall\, x \in X, (f*g)(x) = f(x)*g(x)$.
Alors l'application constante, qui à tout x de E associe e, est neutre pour cette loi.
Ainsi, sur l'ensemble $\mathcal{F}(\mathbb{N},\mathbb{K})$ des suites (à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), la suite constante 0 est neutre pour l'addition, et la suite constante 1 est neutre pour le produit.

I.7 Structure de monoïde

Définition

Soit E un ensemble muni d'une loi $*$. On dit que E possède une structure de *monoïde* pour la loi $*$, ou encore que $(E,*)$ est un monoïde, si : $\begin{cases} \text{La loi } * \text{ est associative.} \\ \text{Il existe un élément neutre } e. \end{cases}$

Exemples et remarques

- De par la définition, un monoïde est toujours non vide.
- $(\mathbb{N},+)$ et $(\mathbb{N},\times)$ sont des monoïdes (idem en remplaçant $\mathbb{N}$ par $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$).
- $(\mathcal{P}(E),\cup)$, $(\mathcal{P}(E),\cap)$ et $(\mathcal{P}(E),\Delta)$ sont des monoïdes.
- $(\mathcal{F}(E),\circ)$ est un monoïde.
- Si $(E,*)$ est un monoïde, et si X est un ensemble, $(\mathcal{F}(X,E),*)$ est un monoïde.
  En particulier, l'ensemble $(\mathcal{F}(\mathbb{N},E),*)$ des suites à valeurs dans le monoïde E, muni de la loi homonyme $*$, est lui-même un monoïde.
- Si $(E,*)$ est un monoïde, et si F est une partie stable de E contenant le neutre e, alors $(F,*)$ (avec la loi induite) est encore un monoïde.

I.8 Symétrique d'un élément

Définition

Soit $(E,*)$ un monoïde d'élément neutre e. Soit x un élément de E.

On dit que x est *symétrisable* (ou *inversible*) pour la loi $*$, s'il existe un élément x' de E tel que $x*x'=x'*x=e$.

Si un tel élément x' existe, il est unique. On l'appelle le *symétrique* (ou l'*inverse*) de x.

Notation additive

Dans le cas d'une loi $+$ (nécessairement commutative, d'élément neutre 0), le symétrique d'un élément x est appelé son *opposé*, et est noté $-x$.

Pour tous éléments x et y (x possédant un opposé), on note $y-x$ plutôt que $y+(-x)$.

Notation multiplicative

Dans le cas d'une loi multiplicative $\times$ (éventuellement notée par juxtaposition), le symétrique d'un élément x est en général appelé son *inverse*, et est noté x^{-1}.

Si ce produit est commutatif et si on note 1 son neutre, on peut écrire $\dfrac{1}{x}$ plutôt que x^{-1}.

Le produit yx^{-1} peut alors être noté $\dfrac{y}{x}$ (notamment dans les ensembles de nombres).

Propriétés et remarques

- Soit $(E, *)$ un monoïde, de neutre e. Alors e est inversible et est son propre inverse.
- Si x et y sont inversibles, leur composé $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$ (attention à l'ordre des facteurs si la loi $*$ n'est pas commutative).
- Si F est une partie stable du monoïde $(E, *)$ contenant le neutre e (un "sous-monoïde" de $(E, *)$) et si x appartient à F, alors l'inversibilité de x doit être examinée relativement à l'appartenance de x :
  Si x est inversible dans F, il est inversible dans E (avec le même inverse).
  La réciproque est fausse : pour le produit, 2 est inversible dans $\mathbb{R}$ mais pas dans $\mathbb{Z}$.

Exemples

- Dans $(\mathbb{N}, +)$ seul 0 est symétrisable.
  Mais tous les éléments de $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ le sont.
- Les éléments inversibles de $(\mathbb{R}, \times)$ sont les éléments non nuls.
  C'est la même chose avec $(\mathbb{Q}, \times)$ et $(\mathbb{C}, \times)$.
  Le seul élément inversible de $(\mathbb{N}, \times)$ est 1. Ceux de $(\mathbb{Z}, \times)$ sont -1 et 1.
- On se place dans l'ensemble $\mathcal{F}(\mathbb{N}, \mathbb{R})$ des suites à valeurs dans $\mathbb{R}$.
  Toutes les suites (u_n) sont symétrisables pour l'addition : l'opposé de la suite de terme général u_n est la suite de terme général $-u_n$.
  Seules les suites ne s'annulant jamais sont symétrisables pour le produit : l'inverse de la suite de terme général u_n est alors la suite de terme général $\dfrac{1}{u_n}$.
- Dans $(\mathcal{F}(E), \circ)$, une application est inversible si et seulement si elle est bijective.
  Son inverse est alors sa bijection réciproque. La notation f^{-1} est donc justifiée.

I.9 Eléments simplifiables

Définition

Soit E un ensemble muni d'une loi $*$. Soit x un élément de E.
On dit qu'un élément x de E est *simplifiable* (ou encore *régulier*) si :

$$\forall (y, z) \in E^2 : \begin{cases} x * y = x * z \Rightarrow y = z & (1) \\ y * x = z * x \Rightarrow y = z & (2) \end{cases}$$

Remarques

- x est simplifiable $\Leftrightarrow$ les applications $t \to x * t$ et $t \to t * x$ sont injectives de E dans E.
- On pourrait traduire (1) en disant : x est simplifiable *à gauche*.
  De même, (2) signifie : x est simplifiable *à droite*.
- Quand la loi $*$ est commutative, les propriétés (1) et (2) sont équivalentes.

Propriétés et exemples

- Si la loi $*$ est associative, et si a et b sont simplifiables, alors $a*b$ est simplifiable.
- Si $(E,*)$ est un monoïde et si x est inversible, alors x est simplifiable.
  Il suffit par exemple de composer par x^{-1} à gauche pour simplifier x dans l'égalité $x*y=x*z$.
- La réciproque de cette propriété est fausse. En effet, dans $(\mathbb{Z},\times)$ par exemple, tous les éléments non nuls sont simplifiables, mais seuls -1 et 1 sont inversibles.
- Dans $(\mathcal{P}(E),\cup)$, seul $\emptyset$ est inversible, donc simplifiable.
  De même, seul E est inversible, donc simplifiable dans $(\mathcal{P}(E),\cap)$.

I.10 Propriétés transportées par un morphisme surjectif

Soit f un morphisme de $(E,*)$ sur (F,T).

- L'ensemble image $f(E)$ est stable pour T.
  Dans la suite de cette sous-section, on suppose que f est surjectif de E sur F.
- Si e est neutre dans $(E,*)$ alors $f(e)$ est neutre dans (F,T).
  Si x' est le symétrique de x dans $(E,*)$ alors $f(x')$ est celui de $f(x)$ dans (F,T).
- Si la loi $*$ est commutative alors la loi T est commutative.
  Si la loi $*$ est associative alors la loi T est associative.
  Un morphisme surjectif "transporte" donc les propriétés principales des lois de composition.
- Soit x un élément simplifiable de E.
  L'élément $f(x)$ peut ne pas être simplifiable dans F.
  En revanche, si on suppose que f est bijective, alors $f(x)$ est simplifiable.

II Groupes, sous-groupes

II.1 Structure de groupe

Définition

Soit G un ensemble muni d'une loi de composition $*$.

On dit que $(G,*)$ est un *groupe* si :

- $(G,*)$ est un monoïde, c'est-à-dire :
  La loi $*$ est associative, et il y a un neutre e. (en particulier $G \neq \emptyset$.)
- Tout élément de G possède un symétrique.

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

Exemples et remarques

- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs.
- Idem avec $(\{-1,1\},\times)$, $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}^{+*},\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}^{+*},\times)$ et $(\mathbb{C}^*,\times)$.
- Si E est un ensemble et si on note $\mathcal{B}(E)$ l'ensemble des bijections de E dans lui-même (on dit aussi les *permutations* de E), alors $\mathcal{B}(E)$ est un groupe pour la loi de composition des applications (non commutatif dès que E possède au moins trois éléments).
- Dans un groupe, tout élément est simplifiable (car inversible).
- Si a et b sont deux éléments du groupe $(G,*)$, les équations $a*x=b$ et $x*a=b$ admettent une solution unique, respectivement $x=a^{-1}*b$ et $x=b*a^{-1}$.
  On peut exprimer cette propriété en disant que les applications $x \to a*x$ et $x \to x*a$ sont des bijections de G dans lui-même.

Proposition *Groupe produit*

Soit $(G,*)$ un groupe, de neutre e.

On définit une loi $*$ sur $G\times G$ en posant : $(a,b)*(c,d)=(a*c,b*d)$.

Muni de cette loi, $G\times G$ est un groupe :

- Le neutre est (e,e).
- L'inverse de (a,b) est (a^{-1},b^{-1}).

Généralisation

On peut facilement généraliser à G^n, pour tout n de $\mathbb{N}^*$.

Par exemple $(\mathbb{R}^n,+)$ est un groupe.

Ordre d'un groupe fini

Soit $(G,*)$ un groupe fini. Le cardinal de l'ensemble G est appelé l'*ordre* du groupe.

Par exemple, si E de cardinal p, le groupe des permutations de E est d'ordre $p!$

Table d'un groupe fini

La *table* d'un groupe fini $G = \{a_1, a_2, \dots, a_n\}$ d'ordre n est le tableau (de dimension $n \times n$) des composés $a_i * a_j$, pour tous les couples (i, j) de $[\![1, n]\!]^2$.

Dans ce tableau, le résultat $a_i * a_j$ vient se placer à l'intersection de la ligne d'indice i et de la colonne d'indice j. Dans la table de G, chaque ligne et chaque colonne contient une fois et une seule chaque élément du groupe.

II.2 Sous-groupes

Définition

Soit $(G, *)$ un groupe et soit H une partie de G.

On dit que H est un *sous-groupe* de $(G, *)$ si :

- H est stable pour la loi $*$: $\forall (x, y) \in H^2, x * y \in H$.
- Muni de la loi induite, $(H, *)$ possède lui-même une structure de groupe.

Remarque

On vérifie facilement que si H est un sous-groupe de $(G, *)$:

- Les groupes $(H, *)$ et $(G, *)$ partagent le même élément neutre.
- Le symétrique d'un élément x de H est le même, que l'on considère x comme un élément du groupe $(H, *)$ ou un élément du groupe $(G, *)$.

Proposition *(Première caractérisation des sous-groupes)*

Soit $(G, *)$ un groupe et soit H une partie de G.

H est un sous-groupe de $(G, *) \Leftrightarrow$:

- H est non vide
- H est stable pour la loi $*$: $\forall (x, y) \in H^2, x * y \in H$.
- H est stable pour le "passage à l'inverse" : $\forall x \in H, x^{-1} \in H$.

Proposition *(Seconde caractérisation des sous-groupes)*

Soit $(G, *)$ un groupe et soit H une partie de G.

$$H \text{ est un sous-groupe de } (G, *) \Leftrightarrow : \begin{cases} H \text{ est non vide} \\ \forall (x, y) \in H^2, x * y^{-1} \in H. \end{cases}$$

Cas de la notation additive

Pour un groupe$(G, +)$ (nécessairement commutatif), ces caractérisations s'écrivent :

$$H \text{ sous-groupe de } (G, +) \Leftrightarrow \begin{cases} H \neq \emptyset \\ \forall x \in H, -x \in H \\ \forall (x, y) \in H^2, x + y \in H \end{cases} \Leftrightarrow \begin{cases} H \neq \emptyset \\ \forall (x, y) \in H^2, x - y \in H \end{cases}$$

Exemples

- Soit $(G, *)$ est un groupe de neutre e.
  Alors $\{e\}$ et G en sont deux sous-groupes (dits *triviaux*).
- Dans $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, chacun est un sous-groupe du suivant.
- Même chose avec $(\{-1, 1\}, \times)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$.
- De même, $(\mathbb{R}^{+*}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
- L'ensemble $\mathcal{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$.

Proposition *(Intersection de sous-groupes)*

Une intersection quelconque de sous-groupes de G est encore un sous-groupe de G.

Remarque

C'est faux pour la réunion !
Plus précisément, si H et K sont deux sous-groupes de G, $H \cup K$ est un sous-groupe de G $\Leftrightarrow H \subset K$ (auquel cas $H \cup K = K$) ou $K \subset H$ (auquel cas $H \cup K = H$).

Définition

Soit n un élément de $\mathbb{N}$. On note $n\mathbb{Z} = \{kn, k \in \mathbb{Z}\}$.

Remarques

- En particulier $0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$.
- $\forall\, (n, p) \in \mathbb{N}^2, n\mathbb{Z} \subset p\mathbb{Z} \Leftrightarrow p \mid n$, et $n\mathbb{Z} = p\mathbb{Z} \Leftrightarrow n = p$.
- On pourrait définir les $n\mathbb{Z}$, $n \in \mathbb{Z}$, mais c'est sans intérêt : $\forall\, n \in \mathbb{Z}, n\mathbb{Z} = (-n)\mathbb{Z}$.

Proposition *(Sous-groupes de $\mathbb{Z}$)*

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

Théorème *(Théorème de Lagrange)*

Soit $(G, *)$ un groupe fini, et H un sous-groupe de G.
Alors l'ordre de H divise l'ordre de G.

Cas particulier

Si G est d'ordre premier, ses seuls sous-groupes sont $\{e\}$ et G.

II.3 Morphismes de groupes

Proposition *(Image d'un groupe par un morphisme)*

Soit $(G, *)$ un groupe, et H un ensemble muni d'une loi de composition T.
Soit f un morphisme de $(G, *)$ dans (H, T). Alors $(f(G), \mathsf{T})$ est un groupe.

On peut donc dire que l'image d'un groupe par un homomorphisme est un groupe.

Si le groupe $(G,*)$ est commutatif, alors le groupe $(f(G),\mathsf{T})$ est commutatif.

Définition *(Morphismes de groupes)*

Soient $(G,*)$ et (H,T) deux groupes ; on note e_H le neutre de H.
Soit f un morphisme de $(G,*)$ dans (H,T). On dit que f est un *morphisme de groupes*.
Si f est bijective, f est appelée un *isomorphisme de groupes*.
On dit alors que $(G,*)$ et (H,T) sont deux *groupes isomorphes*.

Proposition

Soit f un morphisme de groupes de $(G,*)$ dans (H,T).
- Soit G' un sous-groupe de $(G,*)$. Alors $f(G')$ est un sous-groupe de (H,T).
- Soit H' un sous-groupe de (H,T). Alors $\overset{-1}{f}(H')$ est un sous-groupe de $(G,*)$.

Cas particuliers : image et noyau

- $f(G)$ est un sous-groupe de (H,T), appelé *image* de f, et noté $\mathrm{im}\,(f)$.
- $\overset{-1}{f}(\{e_H\}) = \{x \in G, f(x) = e_H\}$ est un sous-groupe de $(G,*)$.
  Ce sous-groupe est appelé *noyau* de f, et noté $\ker(f)$.

Proposition *(Caractérisation de l'injectivité d'un morphisme de groupes)*

Soient $(G,*)$ et (H,T) deux groupes. Soit e_G le neutre de G.
Soit f un morphisme de $(G,*)$ dans (H,T).
f est injective $\Leftrightarrow \ker(f) = \{e_G\}$.

Remarque

On retiendra plus généralement que : $\forall\,(x,y) \in G^2, f(x) = f(y) \Leftrightarrow x * y^{-1} \in \ker(f)$,
et en notation additive : $f(x) = f(y) \Leftrightarrow x - y \in \ker(f)$.

II.4 Sous-groupe engendré par un élément

Définition *(Puissances entières d'un élément)*

Soit $(G,*)$ un groupe, d'élément neutre e, et a un élément de G.
On définit les puissances entières a^n $(n \in \mathbb{Z})$ de a de la manière suivante :
- $a^0 = e$.
- $\forall\, n \in \mathbb{N}, a^{n+1} = a * a^n$.
- $\forall\, n \in \mathbb{N}, a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

Remarques et propriétés

– $\forall\,(n,m)\in\mathbb{Z}^2, a^n * a^m = a^{n+m}$, et $(a^n)^m = a^{nm}$.

– Si a et b commutent, $(a*b)^n = a^n * b^n$.

– En notation additive, la notation a^n devient na, $n\in\mathbb{Z}$.

Proposition *(Sous-groupe engendré par une partie)*

Soit $(G,*)$ un groupe, et X une partie non vide quelconque de G.
Il existe un plus petit (au sens de l'inclusion) sous-groupe de $(G,*)$ qui contient X :
C'est l'intersection de tous les sous-groupes de $(G,*)$ qui contiennent X.
On l'appelle le sous-groupe de $(G,*)$ *engendré* par X.
On dit aussi que les éléments de X en constituent un *système générateur*.

Proposition

Le sous-groupe de $(G,*)$ engendré par une partie X de G est l'ensemble des produits finis $a*b*\ldots*z$, où $a,b,\ldots,z$ sont des éléments de X ou des inverses d'éléments de X.

Proposition *(Sous-groupe engendré par un élément)*

Soit $(G,*)$ un groupe, et a un élément de G.
Le sous-groupe engendré par a est noté (a) et vérifie : $(a)=\{a^m, m\in\mathbb{Z}\}$.
En notation additive, $(a)=\{ma, m\in\mathbb{Z}\}$.

Proposition *(Ordre d'un élément dans un groupe)*

Soit $(G,*)$ un groupe, de neutre e. Soit a un élément de G.
L'application f définie par $f(m)=a^m$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,*)$.
L'image de f n'est autre que le sous-groupe (a) de $(G,*)$, engendré par a.
Il existe un unique entier naturel n tel que $\ker(f)=n\mathbb{Z}$.
L'entier n est appelé l'*ordre* de a.

Premier cas

a est d'ordre 0, c'est-à-dire $\ker(f)=\{0\}$.
L'application f est donc injective : $\forall\,(m,p)\in\mathbb{Z}^2, m\neq p\Rightarrow a^m\neq a^p$.
f est un isomorphisme du groupe $(\mathbb{Z},+)$ sur le groupe $((a),*)$.
Le groupe (a) est donc infini et isomorphe à $\mathbb{Z}$.

Deuxième cas

a est d'ordre n strictement positif. Par définition, on a :
$\forall\, m\in\mathbb{Z}, a^m=e\Leftrightarrow n\mid m\Leftrightarrow\exists\, k\in\mathbb{Z}, m=kn$.
$\forall\,(m,p)\in\mathbb{Z}^2, a^m=a^p\Leftrightarrow n\mid m-p\Leftrightarrow\exists\, k\in\mathbb{Z}, m-p=kn$.
Pour tout entier relatif m, $a^m=a^r$, où r est le reste dans la division de m par n.
Le sous-groupe engendré par a est fini, d'ordre n : $(a)=\{a^k, 0\leq k\leq n-1\}$.

II.5 Groupes monogènes, groupes cycliques

Définition

On dit qu'un groupe G est *monogène* s'il est engendré par l'un de ses éléments a, donc si $G = (a) = \{a^m, m \in \mathbb{Z}\}$ (ou $\{ma, m \in \mathbb{Z}\}$ en notation additive).

Un tel groupe est commutatif.

Premier cas

G est infini (l'élément a est d'ordre 0).
Le groupe $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$ par l'application $m \to a^m$.

Deuxième cas

G est fini d'ordre n (l'élément a est d'ordre $n > 0$).
On dit dans ce cas que G est un *groupe cyclique* : $G = \{e, a, a^2, \ldots, a^{n-1}\}$.
Soit $k \in [\![1, n-1]\!]$: $b = a^k$ est un générateur de $G \Leftrightarrow k$ et n sont premiers entre eux.

Proposition

Tout groupe fini d'ordre premier est cyclique.

Un exemple de groupe cyclique

- Soit n un entier naturel non nul. On note $\mathcal{U}_n = \{z \in \mathbb{C}, z^n = 1\}$.
  Les éléments de $\mathcal{U}_n$ sont appelés *racines n-ièmes de l'unité*.
- $(\mathcal{U}_n, \times)$ est un sous-groupe de $(\mathbb{C}, \times)$.
- $\mathcal{U}_n = \{\exp \dfrac{2ik\pi}{n}, k \in \mathbb{Z}\} = \{\omega^k, k \in \mathbb{Z}\} = (\omega)$, où $\omega = \exp \dfrac{2i\pi}{n}$.
- ω étant d'ordre n, $\mathcal{U}_n$ est un groupe cyclique d'ordre n : $\mathcal{U}_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.
- Les générateurs de $\mathcal{U}_n$ sont les $\omega^k = \exp \dfrac{2ik\pi}{n}$, avec $1 \leq k \leq n-1$, et k premier avec n.
- En particulier, si n est premier, tous les éléments de $\mathcal{U}_n$ (sauf $\omega^0 = 1$) engendrent $\mathcal{U}_n$.

Remarques et exemples

- Cet exemple montre que pour tout n de $\mathbb{N}^*$, il existe au moins un groupe d'ordre n ...
  D'autre part, tout groupe cyclique d'ordre n est isomorphe au groupe $(\mathcal{U}_n, \times)$.
  On peut donc dire que $(\mathcal{U}_n, \times)$ est le modèle du groupe cyclique d'ordre n.
- Il existe des groupes finis qui ne sont pas cycliques. Par exemple, pour tout n de $\mathbb{N}^*$, le groupe des permutations d'un ensemble à n éléments est fini d'ordre $n!$ mais il n'est pas cyclique si $n > 2$ (tout simplement parce qu'il n'est pas commutatif).
- $\mathcal{U}_1 = \{1\}$; $\mathcal{U}_2 = \{1, -1\}$ (seul générateur : -1).
  $\mathcal{U}_3 = \{1, j, j^2\}$, avec $j = \exp \dfrac{2i\pi}{3}$: les générateurs sont j et j^2.
  $\mathcal{U}_4 = \{1, i, -1, -i\}$: les générateurs sont i et $-i$.

III Le groupe symétrique

III.1 Le groupe symétrique

Définition

Pour tout entier $n \geq 1$, on note $E_n = \{1, \dots, n\}$.

On appelle *groupe symétrique* d'indice n le groupe noté $\mathcal{S}_n$ de toutes les *permutations* de E_n, c'est-à-dire de toutes les bijections de E_n sur lui-même.

$\mathcal{S}_n$ est effectivement un groupe pour la loi de composition des applications, non commutatif dès que $n \geq 3$, et il est d'ordre $n!$

Notation

Un élément σ de $\mathcal{S}_n$ est représenté par $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

En particulier l'application identité, neutre du groupe $\mathcal{S}_n$, se note $\mathrm{Id} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

Par exemple, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 6 & 2 \end{pmatrix}$ représente l'élément σ de $\mathcal{S}_6$ défini par :

$$\sigma(1) = 3, \quad \sigma(2) = 5, \quad \sigma(3) = 1, \quad \sigma(4) = 4, \quad \sigma(5) = 6, \quad \sigma(6) = 2$$

Exemples

Si $n = 1$, le groupe $\mathcal{S}_1$ se réduit à l'application identité de E_1 dans lui-même.

Si $n = 2$, $\mathcal{S}_2 = \{\mathrm{Id}, \sigma\}$, où σ est définie par : $\sigma(1) = 2$ et $\sigma(2) = 1$.

Si $n = 3$, $\mathcal{S}_3$ est formé de six éléments, qui sont :

$$\sigma_0 = \mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_4^2$$

On vérifie par exemple que $\sigma_1 \circ \sigma_3 = \sigma_5$ et $\sigma_3 \circ \sigma_1 = \sigma_4$. Donc $\mathcal{S}_3$ n'est pas commutatif.

III.2 Cycles et transpositions

Définition *(Cycles)*

Soit σ un élément de $\mathcal{S}_n$, avec $n \geq 2$. Soit p un entier de $\{2, \dots, n\}$.

On dit que σ est un *cycle* de longueur p s'il existe p éléments $a_1, a_2, \dots, a_p$ distincts de $E_n = \{1, \dots, n\}$ tels que : $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\dots$, $\sigma(a_{p-1}) = a_p$, $\sigma(a_p) = a_1$, et si pour tout élément b de $E_n \setminus \{a_1, \dots, a_p\}$ on a $\sigma(b) = b$.

On dit alors que l'ensemble $\{a_1, \dots, a_p\}$ est le *support* du cycle σ (c'est l'ensemble des éléments qui ne sont pas invariants par σ).

En général, on représente un tel cycle en écrivant $\sigma = (\, a_1 \quad a_2 \quad \dots \quad a_p \,)$.

Dans $\mathcal{S}_n$, un cycle de longueur n est appelé une *permutation circulaire*.

Exemples

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 3 & 1 & 2 & 4 & 7 \end{pmatrix}$ est le cycle $(1 \quad 5 \quad 2 \quad 6 \quad 4)$.

Cette dernière notation ne dit pas que la permutation σ_1 est un élément de $\mathcal{S}_7$, mais qu'elle pourrait en fait être un élément de $\mathcal{S}_n$ pour tout $n \geq 6$ (en principe le contexte est clair, mais de toutes façons c'est sans grande importance).

Le support de σ_1 est $\{1, 2, 4, 5, 6\}$. Les éléments 3 et 7 sont fixes par σ_1.

On remarque qu'on peut aussi écrire $\sigma_1 = (5 \quad 2 \quad 6 \quad 4 \quad 1)$, ou $\sigma_1 = (2 \quad 6 \quad 4 \quad 1 \quad 5)\ldots$

En revanche $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 3 & 8 & 7 & 4 & 2 & 1 \end{pmatrix}$ n'est pas un cycle.

Cependant on a visiblement $\sigma = s \circ t = t \circ s$, où $s = (1 \quad 6 \quad 4 \quad 8)$ et $t = (2 \quad 5 \quad 7)$.

$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 1 & 4 & 2 & 3 \end{pmatrix}$ est la permutation circulaire $(1 \quad 7 \quad 3 \quad 6 \quad 2 \quad 5 \quad 4)$.

Propriétés

- Si $\sigma = (a_1 \quad a_2 \quad \ldots \quad a_p)$ alors σ^{-1} est le cycle $(a_p \quad a_{p-1} \quad \ldots \quad a_1)$.
- Les puissances d'un cycle ne sont pas toujours des cycles.
  Considérons par exemple le cycle $\sigma = (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6)$.
  On constate que $\sigma^2 = (1 \quad 3 \quad 5) \circ (2 \quad 4 \quad 6)$ et $\sigma^3 = (1 \quad 4) \circ (2 \quad 5) \circ (3 \quad 6)$.
  En revanche σ^5 est le cycle $(1 \quad 6 \quad 5 \quad 4 \quad 3 \quad 2)$.
  Pour être précis, et si σ est un cycle de longueur p, on montre que σ^k est un cycle si et seulement si k et p sont premiers entre eux.
- Soit σ un cycle de longueur $p \geq 2$. Alors $\sigma^p = \mathrm{Id}$ et $\forall\, k \in \{1, \ldots, p-1\},\ \sigma^k \neq \mathrm{Id}$.
  Cela permet de calculer les puissances quelconques du cycle σ. En effet, pour tout entier relatif m, si $m = qp + r$ est la division euclidienne de m par p, alors $\sigma^m = \sigma^r$.
- Deux cycles σ_1 et σ_2 dont les supports sont disjoints commutent : $\sigma_2 \circ \sigma_1 = \sigma_1 \circ \sigma_2$.

Définition *(Transpositions)*

Soit n un entier supérieur ou égal à 2. On dit qu'un élément σ de $\mathcal{S}_n$ est une *transposition* si σ est un cycle de longueur 2, c'est-à-dire s'il existe deux indices distincts i et j de E_n tels que $\sigma(i) = j$ et $\sigma(j) = i$, les autres élements de E_n étant invariants par σ.

Une telle transposition est notée $(i \quad j)$, ou $(j \quad i)$, ou $\tau_{i,j}$.

Remarques

- Une transposition est donc une permutation qui se contente d'échanger deux éléments.
  On ne confondra pas les mots "permutation" et "transposition".
- On a bien sûr : $\tau_{i,j} = \tau_{j,i}$, $\tau_{i,j}^2 = \mathrm{Id}$, $\tau_{i,j}^{-1} = \tau_{i,j}$.
- Soient $\tau_{a,b}$ et $\tau_{c,d}$ deux transpositions : $\tau_{a,b} \circ \tau_{c,d} = \tau_{c,d} \circ \tau_{a,b} \Leftrightarrow \begin{cases} \{a,b\} \cap \{c,d\} = \emptyset \\ \text{ou } \{a,b\} = \{c,d\} \end{cases}$
- Dans $\mathcal{S}_n$, il y a $\mathrm{C}_n^2 = \frac{n(n-1)}{2}$ transpositions.

III.3 Décompositions d'une permutation

Proposition *(Décomposition en produit de cycles)*

Toute permutation de $\mathcal{S}_n$ (avec $n \geq 2$) se décompose en un produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre près des facteurs.

Un exemple

Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 10 & 5 & 9 & 4 & 14 & 3 & 1 & 11 & 12 & 7 & 13 & 6 & 2 & 8 \end{pmatrix}$

On a $\sigma(1) = 10$, $\sigma(10) = 7$, et $\sigma(7) = 1$. Il apparaît donc le cycle $\sigma_1 = (1\ \ 10\ \ 7)$.

En considérant les images successives de 2, on trouve le cycle $\sigma_2 = (2\ \ 5\ \ 14\ \ 8\ \ 11\ \ 13)$.

En considérant les images successives de 3 (qui n'est pas apparu dans les cycles σ_1 et σ_2) on trouve le cycle $\sigma_3 = (3\ \ 9\ \ 12\ \ 6)$.

On constate enfin que $\sigma(4) = 4$ et que les autres éléments de $\{1, \dots, 14\}$ sont tous apparus une fois dans l'un des cycles $\sigma_1, \sigma_2, \sigma_3$.

On peut donc écrire $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$.

Les supports de ces cycles sont respectivement $\{1, 7, 10\}$, $\{2, 5, 8, 11, 13, 14\}$ et $\{3, 9, 6, 12\}$. Ils sont disjoints deux à deux : les cycles $\sigma_1, \sigma_2, \sigma_3$ commutent entre eux.

On pourrait donc aussi écrire : $\sigma = \sigma_3 \circ \sigma_2 \circ \sigma_1 = \sigma_1 \circ \sigma_3 \circ \sigma_2 = \sigma_2 \circ \sigma_3 \circ \sigma_1 = \cdots$

On en déduit également le calcul des puissances de σ : $\sigma^n = (\sigma_1 \circ \sigma_2 \circ \sigma_3)^n = \sigma_1^n \circ \sigma_2^n \circ \sigma_3^n$.

Compte tenu des longueurs des cycles $\sigma_1, \sigma_2, \sigma_3$, on a : $\sigma_1^3 = \mathrm{Id}$, $\sigma_2^6 = \mathrm{Id}$, $\sigma_3^4 = \mathrm{Id}$.

Le ppcm de $3, 6, 4$ est 12. On a donc $\sigma^{12} = (\sigma_1^3)^4 \circ (\sigma_2^6)^2 \circ (\sigma_3^4)^3 = \mathrm{Id}$.

On vérifie que pour tout entier k compris entre 1 et 12 on a $\sigma^k \neq \mathrm{Id}$.

Ainsi la permutation σ est un élément d'ordre 12 dans $\mathcal{S}_{14}$: dans ce groupe, σ engendre un groupe cyclique d'ordre 12 : $(\sigma) = \{\mathrm{Id}, \sigma, \sigma^2, \dots, \sigma^{11}\}$.

Si on veut calculer une puissance particulière de σ, par exemple σ^{2000}, on calcule les restes de 2000 dans les divisions euclidiennes par $3, 6, 4$.

On observe que $2000 \equiv 2 \bmod 3$, $2000 \equiv 2 \bmod 6$ et $2000 \equiv 0 \bmod 4$.

On en déduit $\sigma^{2000} = \sigma_1^2 \circ \sigma_2^2 \circ \sigma_3^0$.

Or $\sigma_1^2 = (1\ \ 7\ \ 10)$ et $\sigma_2^2 = (2\ \ 14\ \ 11) \circ (5\ \ 8\ \ 13)$.

On trouve donc : $\sigma^{2000} = (1\ \ 7\ \ 10) \circ (2\ \ 14\ \ 11) \circ (5\ \ 8\ \ 13)$.

Finalement : $\sigma^{2000} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 14 & 3 & 4 & 8 & 6 & 10 & 13 & 9 & 1 & 2 & 12 & 5 & 11 \end{pmatrix}$

Alors que σ n'a qu'un point fixe, on constate que σ^{2000} en a cinq.

Enfin le calcul de σ^{-1} peut s'effectuer en écrivant :

$\sigma^{-1} = \sigma_1^{-1} \circ \sigma_2^{-1} \circ \sigma_3^{-1} = (1\ \ 7\ \ 10) \circ (2\ \ 13\ \ 11\ \ 8\ \ 14\ \ 5) \circ (3\ \ 6\ \ 12\ \ 9)$

On pouvait aussi trouver σ^{-1} directement (en lisant dans σ à partir de la ligne du bas) :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 13 & 6 & 4 & 2 & 12 & 10 & 14 & 3 & 1 & 8 & 9 & 11 & 5 \end{pmatrix}$$

Proposition *(Décomposition d'une permutation en produit de transpositions)*

Tout cycle de $\mathcal{S}_n$ peut s'écrire comme un produit de transpositions.

Il en découle que toute permutation de $\mathcal{S}_n$ peut s'écrire comme un produit de transpositions.

Remarques et exemples

– Pour décomposer une permutation σ en un produit de transpositions, il est plus commode en général d'écrire σ comme un produit de cycles à supports disjoints pour ensuite décomposer chaque σ_k en un produit de transpositions. Par exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 8 & 6 & 2 & 5 & 1 \end{pmatrix} = (1\ \ 4\ \ 8)(2\ \ 7\ \ 5\ \ 6) = (1\ \ 4)(4\ \ 8)(2\ \ 7)(7\ \ 5)(5\ \ 6)$$

– Il n'y a pas unicité de la décomposition d'une permutation en un produit de transpositions. Par exemple : $\sigma = (1\ \ 2\ \ 3) = (1\ \ 2)(2\ \ 3) = (1\ \ 2)(1\ \ 3)(1\ \ 2)(1\ \ 3) = (2\ \ 3)(1\ \ 3)$

III.4 Signature d'une permutation

Définition *(Inversions d'une permutation)*

Soit σ un élément de $\mathcal{S}_n$, avec $n \geq 2$. Soient $i < j$ deux éléments distincts de E_n.

On dit que la paire $\{i, j\}$ est une inversion de σ si $\sigma(i) > \sigma(j)$.

On note $\text{Inv}(\sigma)$ le nombre d'inversions de la permutation σ.

Exemples

– Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 8 & 6 & 2 & 5 & 1 \end{pmatrix}$. On a $\text{Inv}(\sigma) = 19$. En effet les inversions de σ sont :

$\{1,3\}$ $\{1,6\}$ $\{1,8\}$ $\{2,3\}$ $\{2,5\}$ $\{2,6\}$ $\{2,7\}$ $\{2,8\}$ $\{3,6\}$ $\{3,8\}$
$\{4,5\}$ $\{4,6\}$ $\{4,7\}$ $\{4,8\}$ $\{5,6\}$ $\{5,7\}$ $\{5,8\}$ $\{6,8\}$ $\{7,8\}$

– *Inversions d'une transposition*

Soient $i < j$ deux éléments distincts de E_n, et τ la transposition qui échange i et j.

Les inversions de τ sont $\{i, i+1\}, \{i, i+2\}, \ldots, \{i, j\}, \{i+1, j\}, \{i+2, j\}, \ldots, \{j-1, j\}$.

On constate donc que $\text{Inv}(\tau) = 2(j-i)+1$.

Conclusion : une transposition présente toujours un nombre impair d'inversions.

Définition *(Signature d'une permutation)*

Soit σ un élément de $\mathcal{S}_n$, avec $n \geq 2$. Soit $\text{Inv}(\sigma)$ le nombre de ses inversions.

La quantité $\varepsilon(\sigma) = (-1)^{\text{Inv}(\sigma)}$ est appelée *signature* de σ.

On dit que σ est une *permutation paire* si $\varepsilon(\sigma) = 1$ donc si σ a un nombre pair d'inversions.

Dans le cas contraire, c'est-à-dire si $\varepsilon(\sigma) = -1$, ou encore si σ a un nombre impair d'inversions, on dit que σ est une *permutation impaire*.

Remarques

– L'application identité est une permutation paire. Elle ne présente en effet aucune inversion.

– On sait qu'une transposition présente toujours un nombre impair d'inversions.
Toute transposition est donc une permutation impaire.

Proposition *(Une expression de la signature)*

Soit σ un élément de $\mathcal{S}_n$. Alors $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i}$.

Proposition *(Signature de la composée de deux permutations)*

Soient σ et σ' deux éléments de $\mathcal{S}_n$. Alors $\varepsilon(\sigma' \circ \sigma) = \varepsilon(\sigma')\,\varepsilon(\sigma)$.

Remarques et propriétés

– La proposition précédente peut s'interpréter en disant que la signature est un morphisme du groupe $(\mathcal{S}_n, \circ)$ sur le groupe $(\{-1, 1\}, \times)$.
Ce morphisme est surjectif puisqu'il existe des permutations paires (par exemple l'identité) et des permutations impaires (par exemple les transpositions).

– Une permutation σ et son inverse σ^{-1} ont la même signature.
La composée de deux permutations de même parité est une permutation paire.
La composée de deux permutations de parités opposées est une permutation impaire.
Si σ est une permutation paire, alors pour tout p de $\mathbb{Z}$ la permutation σ^p est paire.
Si σ est une permutation impaire, alors la permutation σ^p a la parité de l'entier relatif p.

– La signature d'un cycle de longueur p est $(-1)^{p-1}$. Autrement dit :
◇ Un cycle de longueur paire est une permutation impaire.
◇ Un cycle de longueur impaire est une permutation paire.

– Pour calculer la signature de $\sigma \in \mathcal{S}_n$, le plus simple est souvent de décomposer σ en cycles à supports disjoints $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_p$ et d'écrire $\varepsilon(\sigma) = \varepsilon(\sigma_1)\,\varepsilon(\sigma_2)\cdots\varepsilon(\sigma_p)$
Par exemple : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 3 & 8 & 6 & 2 & 5 & 1 \end{pmatrix} = \sigma_1 \circ \sigma_2$ avec $\begin{cases} \sigma_1 = (1\ \ 4\ \ 8) \\ \sigma_2 = (2\ \ 7\ \ 5\ \ 6) \end{cases}$
On a $\begin{cases} \varepsilon(\sigma_1) = (-1)^2 = 1 \\ \varepsilon(\sigma_2) = (-1)^3 = -1 \end{cases}$. On en déduit $\varepsilon(\sigma) = -1$: σ est une permutation impaire.

– La décomposition d'une permutation σ en un produit de transpositions n'est pas unique. Cependant la parité du nombre de transpositions apparaissant dans les décompositions de σ est toujours la même : c'est la parité de σ.
Par exemple : $\sigma = (1\ \ 2\ \ 3) = (1\ \ 2)(2\ \ 3) = (1\ \ 2)(1\ \ 3)(1\ \ 2)(1\ \ 3) = (2\ \ 3)(1\ \ 3)$
Le cycle $(1\ \ 2\ \ 3)$ est pair : il est toujours le produit d'un nombre pair de transpositions.

Définition *(Groupe alterné)*

Soit $n \geq 2$. On appelle *groupe alterné* d'indice n et on note $\mathcal{A}_n$ le sous-groupe de $\mathcal{S}_n$ formé des permutations paires.

Remarques

Le groupe alterné $\mathcal{A}_n$ est le noyau du morphisme "signature".

Il y a autant de permutations paires que de permutations impaires. Ainsi $\text{Card}(\mathcal{A}_n) = \frac{1}{2}\,n!$.

IV Anneaux, sous-anneaux, corps

IV.1 Structure d'anneau

Définition

Soit A un ensemble muni de deux lois de composition, notées $+$ et $\times$.
On dit que $(A,+,\times)$ est un *anneau* si :
- $(A,+)$ est un groupe commutatif (son neutre est en général noté 0).
- La loi $\times$ est associative et distributive par rapport à l'addition.
- Il existe un élément neutre pour le produit $\times$ (en général noté 1).

Si de plus la loi $\times$ est commutative, on dit que $(A,+,\times)$ est un *anneau commutatif*.

Exemples

- $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.
- Si E est un ensemble, $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif.
- Soient $(A,+,\times)$ un anneau et X un ensemble non vide.
  Soit $\mathcal{F}(X,A)$ l'ensemble des applications de X vers A.
  $\mathcal{F}(X,A)$, muni des lois $+$ et $\times$ déduites de celles de A, est un anneau.
  $\begin{cases}\text{Le neutre pour l'addition est l'application constante égale à 0.}\\ \text{Celui du produit est l'application constante égale à 1.}\end{cases}$
  En particulier $\mathcal{F}(\mathbb{R},\mathbb{R})$ et $\mathcal{F}(\mathbb{N},\mathbb{R})$ (suites réelles) sont des anneaux.
- Soit A l'ensemble des applications de $\mathbb{C}$ dans $\mathbb{C}$, de la forme $z\to \alpha z+\beta\bar{z}$.
  $(A,+,\circ)$ est un anneau non commutatif (le produit est la loi de composition).

Anneau nul

Soit $(A,+,\times)$ un anneau de neutres 0 (pour la loi $+$) et 1 (pour la loi $\times$).
Il est possible que les deux éléments 0 et 1 de A soient identiques.
Mais dans ce cas A se réduit à $\{0\}$ (anneau nul, sans grand intérêt).

Anneau produit

Soit $(A,+,\times)$ un anneau.
On définit des lois $+$ et $\times$ sur $A\times A$ en posant : $\begin{cases}(a,b)+(c,d)=(a+c,b+d).\\ (a,b)(c,d)=(ac,bd).\end{cases}$
On vérifie que $(A\times A,+,\times)$ est un anneau : $\begin{cases}\text{Le neutre additif est } (0,0).\\ \text{Le neutre multiplicatif est } (1,1).\end{cases}$
On peut généraliser à A^n, pour tout n de $\mathbb{N}^*$. Par exemple $(\mathbb{R}^n,+,\times)$ est un anneau.

IV.2 Calculs dans un anneau

Règles de calcul

Soit $(A,+,\times)$ un anneau (on note 0 le neutre pour $+$, et 1 le neutre pour $\times$).
Rappelons qu'on note $a-b$ plutôt que $a+(-b)$.
Pour tout (a,b,c) de A^3, et tout entier relatif m, on a :

$$\begin{cases} a0=0a=0, & (-a)b=a(-b)=-(ab) \\ (-a)(-b)=ab, & a(b-c)=ab-ac \\ (a-b)c=ac-bc, & a(mb)=(ma)b=m(ab) \end{cases}$$

Sommes et produits. Développements

Soit $(A,+,\times)$ un anneau.
Pour toute famille finie $a_m, a_{m+1}, \dots, a_n$ d'éléments de A, on pose :

$$a_m+\cdots+a_n=\sum_{k=m}^{n} a_k \quad \text{et} \quad a_m\times\cdots\times a_n=\prod_{k=m}^{n} a_k$$

Si $m>n$, on pose encore $\displaystyle\sum_{k=m}^{n} a_k=0$ et $\displaystyle\prod_{k=m}^{n} a_k=1$.
On vérifie les égalités, pour tout b de A :

$$b\left[\sum_{k=m}^{n} a_k\right]=\sum_{k=m}^{n}(ba_k) \quad \text{et} \quad \left[\sum_{k=m}^{n} a_k\right]b=\sum_{k=m}^{n}(a_kb)$$

Plus généralement (notations analogues) :

$$\left[\sum_{j=m}^{n} a_j\right]\left[\sum_{k=p}^{q} b_k\right]=\sum_{j=m}^{n}\left[a_j\sum_{k=p}^{q} b_k\right]=\sum_{j=m}^{n}\sum_{k=p}^{q} a_jb_k$$

Si a et b commutent, alors, pour tout n de $\mathbb{N}$:

$$a^{n+1}-b^{n+1}=(a-b)\left[\sum_{k=0}^{n} a^{n-k}b^k\right]$$

En particulier :

$$\forall\, q\in A, \forall\, n\in\mathbb{N}^*, 1-q^n=(1-q)\sum_{k=0}^{n-1} q^k=(1-q)(1+q+q^2+\cdots+q^{n-1})$$

On en déduit que si $q^n=0$, $1-q$ est inversible et

$$(1-q)^{-1}=1+q+\cdots+q^{n-1}$$

Si a et b commutent, on a la formule du binôme :

$$\forall\, n\in\mathbb{N}, (a+b)^n=\sum_{k=0}^{n} \mathrm{C}_n^k\, a^k\, b^{n-k}$$

IV.3 Eléments remarquables dans un anneau

Proposition *(Groupe des éléments inversibles)*

Soit A un anneau non nul.
On note A^* l'ensemble des éléments de A inversibles pour le produit.
A^* est un groupe pour la loi $\times$.

Remarques

- On note que $A^* \subset A - \{0\}$.
  Il peut y avoir inclusion stricte. Par exemple, $\mathbb{Z}^* = \{-1, 1\}$.
- Dans l'anneau $(\mathcal{F}(\mathbb{R}), +, \times)$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, les fonctions qui sont inversibles pour le produit sont celles qui ne s'annulent jamais.
  L'inverse d'une telle fonction f est $\dfrac{1}{f}$.
  On ne confondra pas avec la bijection inverse pour la composition des applications.

Définition *(Diviseurs de zéro)*

Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A.
On dit que a est un *diviseur de zéro* s'il existe b dans A, non nul, tel que $ab = 0$ ou $ba = 0$.

Exemples et remarques

- Dans $(A^2, +, \times)$ les couples $(a, 0)$ et $(0, a)$, où $a \neq 0$, sont des diviseurs de zéro.
- a est un diviseur de zéro $\Leftrightarrow$ a est non simplifiable pour le produit.
- Si a est inversible, il est simplifiable, et n'est donc pas un diviseur de zéro.
  En prenant la contraposée : si a est un diviseur de zéro, il n'est pas inversible.
- Ces deux notions ne sont cependant pas équivalentes.
  Par exemple 2 n'est pas inversible dans l'anneau $(\mathbb{Z}, +, \times)$, et pourtant ce n'est pas un diviseur de zéro (il est simplifiable).

Définition *(Anneau intègre)*

On dit qu'un anneau $(A, +, \times)$ est *intègre* s'il est commutatif et sans diviseur de zéro.
Un anneau intègre est donc un anneau commutatif A dans lequel $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Exemples

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres.
- Si $(A, +, \times)$ est non nul, les anneaux $(A^n, +, \times)$ $(n \geq 2)$ ne sont pas intègres.
- Soit E un ensemble contenant au moins deux éléments.
  L'anneau commutatif $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre : $\forall X \subset E, X \cap \overline{X} = \emptyset$.

Définition *(Eléments nilpotents)*

Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A.
On dit que a est *nilpotent* s'il existe un entier naturel n tel que $a^n = 0$.
Avec ces notations, $\forall\, p \geq n, a^p = 0$.
Le plus petit entier n tel que $a^n = 0$ est appelé *indice de nilpotence* de a.

Propriétés et exemples

- Si a est nilpotent, alors a est un diviseur de 0. Il n'est donc pas inversible.
- Si a et b commutent et sont nilpotents, $a + b$ est nul ou nilpotent.
- Soit $(A, +, \circ)$ l'anneau des applications $z \to \alpha z + \beta \bar{z}$, avec $(\alpha, \beta) \in \mathbb{C}^2$.
  L'application $f : z \to iz + \bar{z}$ est nilpotente, car $f \circ f = 0$ (application nulle).

IV.4 Sous-anneaux

Définition

Soit $(A, +, \times)$ un anneau (on note 1 le neutre pour le produit). Soit B une partie de A.
On dit que B est un *sous-anneau* de $(A, +, \times)$ si :

- $1 \in B$
- $\forall\, (a, b) \in B^2, a + b \in B$ (stabilité pour la loi $+$)
- $\forall\, (a, b) \in B^2, ab \in B$ (stabilité pour la loi $\times$)
- Muni des lois induites, $(B, +, \times)$ possède lui-même muni d'une structure d'anneau.

Proposition *(Caractérisation d'un sous-anneau)*

B est un sous-anneau de $(A, +, \times)$ si et seulement si :
• $1 \in B$ • $\forall\, (a, b) \in B^2,\ a - b \in B$ • $\forall\, (a, b) \in B^2,\ ab \in B$

Exemples

- Dans $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, chacun est un sous-anneau du suivant.
- Le seul sous-anneau de $(\mathbb{Z}, +, \times)$ est $(\mathbb{Z}, +, \times)$ lui-même.
- Soit D l'ensemble $\{m10^{-n}, m \in \mathbb{Z}, n \in \mathbb{N}\}$ de tous les nombres décimaux.
  D est un sous-anneau de $(\mathbb{Q}, +, \times)$.
- L'ensemble $\{r + s\sqrt{2}, (r, s) \in \mathbb{Q}^2\}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Définition *(Morphismes d'anneaux)*

Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux.
On note 1_A et 1_B les neutres multiplicatifs. On note 0_A et 0_B les neutres additifs.
On dit qu'une application f de A vers B est un *morphisme d'anneaux* si :

- $f(1_A) = 1_B$
- $\forall\, (a, b) \in A^2, f(a + b) = f(a) + f(b)$
- $\forall\, (a, b) \in A^2, f(ab) = f(a)f(b)$

Remarques
- En particulier, f est un morphisme de groupes, de $(A,+)$ vers $(B,+)$.
- On note encore $\ker(f)=\{a\in A, f(a)=0_B\}$. $\forall (a,b)\in A^2, f(a)=f(b)\Leftrightarrow b-a\in\ker(f)$.
- Le morphisme f est injectif $\Leftrightarrow \ker(f)=\{0_A\}$.

IV.5 Structure de corps

Définition

Soit K un ensemble muni de deux lois $+$ et $\times$.
On dit que $(K,+,\times)$ est un *corps* si :
- $(K,+,\times)$ est un anneau commutatif non réduit à $\{0\}$.
- $K^*=K-\{0\}$, c'est-à-dire tout élément non nul de K est inversible pour le produit.

Exemples et remarques
- $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps, mais pas $(\mathbb{Z},+,\times)$.
- Dans un corps, tous les éléments non nuls sont simplifiables.
  Il n'y a donc pas de diviseur de 0, et à fortiori pas d'élément nilpotent.
- Un corps est un cas particulier d'anneau intègre ($xy=0$ implique $x=0$ ou $y=0$).
- Si $(K,+,\times)$ est un corps, $(K^2,+,\times)$ n'est pas un corps (idem avec K^n, si $n\geq 2$).

Définition *(Sous-corps)*

Soit $(K,+,\times)$ un corps.
On dit qu'une partie L de K est un *sous-corps* de $(K,+,\times)$ si :
- L est un sous anneau de $(K,+,\times)$
- $\forall x\in L$, avec $x\neq 0$, $x^{-1}\in L$.
- Muni des lois induites, $(L,+,\times)$ possède alors lui-même une structure de corps.

Proposition *(Caractérisation des sous-corps)*

L est un *sous-corps* de $(K,+,\times)\Leftrightarrow$:
- $1\in L$
- $\forall (x,y)\in L^2, x-y\in L$
- $\forall (x,y)\in L^2$, avec $y\neq 0$, $xy^{-1}\in L$.

Remarques et exemples
- Si L est un sous-corps de $(K,+,\times)$, on dit que K est une *extension* de $(L,+,\times)$.
- Dans $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, chacun est un sous-corps du suivant.
- Le seul sous-corps de $(\mathbb{Q},+,\times)$ est lui-même.
- L'ensemble $\{r+s\sqrt{2},(r,s)\in\mathbb{Q}^2\}$ est un sous-corps de $(\mathbb{R},+,\times)$.

Définition *(Morphisme de corps)*

Soient $(K,+,\times)$ et $(L,+,\times)$ deux corps.

On dit qu'une application f de K dans L est un *morphisme de corps* si f est un morphisme de l'anneau $(K,+,\times)$ dans l'anneau $(L,+,\times)$, c'est-à-dire si :

- $f(1_K)=1_L$
- $\forall (x,y)\in K^2, f(x+y)=f(x)+f(y)$
- $\forall (x,y)\in K^2, f(xy)=f(x)f(y)$

Si de plus f est bijective, on dit que f est un *isomorphisme de corps*.

Proposition *(Corps des fractions d'un anneau intègre)*

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

Il existe un corps $(K,+,\times)$, unique à un isomorphisme près, tel que $(A,+,\times)$ est un sous-anneau de K, et tel que $K=\{ab^{-1},(a,b)\in A^2, b\neq 0\}$.

On dit que K est le *corps des fractions* de l'anneau intègre A.

Remarques et exemples

- Dire que K est unique à un isomorphisme près, c'est dire que si K et K' répondent à la question, alors il existe un isomorphisme f de corps de $(K,+,\times)$ sur $(K',+,\times)$.
- $(\mathbb{Q},+,\times)$ est le corps des fractions de l'anneau intègre $(\mathbb{Z},+,\times)$.
- C'est la proposition précédente qui permet de construire le corps $(K(X),+,\times)$ des fractions rationnelles à coefficients dans K, à partir de l'anneau intègre $(K[X],+,\times)$ des polynômes à coefficients dans K.

V Arithmétique élémentaire

V.1 Bases de numération dans N

Proposition *(Numération en base b)*

Soit b un entier supérieur ou égal à 2.
Tout entier $n \geq 1$ s'écrit de manière unique $n = c_p b^p + c_{p-1} b^{p-1} + \cdots + c_1 b + c_0 = \sum_{k=0}^{p} c_k b^k$,
avec : $p \in \mathbb{N}, \forall\, k \in \{0, \ldots, p\}, c_k \in [\![\, 0, \ldots, b-1 \,]\!]$ et $c_p \neq 0$.
On pose alors $n = \overline{c_p c_{p-1} \ldots c_1 c_0}$ et on parle de l'écriture de n *en base* b.
On dit que $c_p, c_{p-1}, \ldots, c_1, c_0$ sont les *chiffres* de la représentation de n en base b.

Exemples

- On utilise le plus souvent les bases $b = 2$ (numérotation *binaire*, les chiffres sont 0 et 1), $b = 8$ (numérotation *octale*, les chiffres sont $0, 1, \ldots, 7$), $b = 10$ (numérotation *décimale*, les chiffres sont $0, 1, \ldots, 9$), ou $b = 16$ (numérotation *hexadécimale*, les chiffres sont $0, 1, \ldots, 9$ puis A, B, C, D, E, F qui remplacent respectivement $10, 11, 12, 13, 14, 15$).
- L'entier $n = 2001$ (en numération décimale) s'écrit $n = \overline{11111010001}$ en numération binaire, $n = \overline{3721}$ en numération octale, et $n = \overline{7D1}$ en numération hexadécimale.

Interprétation et calcul des chiffres en base b

- Si $n = \overline{c_p c_{p-1} \ldots c_1 c_0}$, alors c_0 est le reste dans la division euclidienne de n par la base b, et $q = \overline{c_p c_{p-1} \ldots c_1}$ est le quotient dans cette division.
  Les chiffres $c_0, c_1, \ldots, c_p$ sont donc les restes obtenus successivement dans des divisions répétées par b (jusqu'à obtenir un quotient nul, c_p étant le reste dans cette dernière division).
  L'écriture de b en base b est $\overline{10}$. Celle de b^m est $\overline{10 \ldots 0}$ (le chiffre 1 suivi par m chiffres 0).
- Si $n = \overline{c_p c_{p-1} \ldots c_1 c_0}$ et si $1 \leq m \leq p$, les entiers $\overline{c_p c_{p-1} \ldots c_m}$ et $\overline{c_{m-1} \ldots c_1 c_0}$ représentent respectivement le quotient et le reste dans la division de n par b^m.

Comparaison de deux nombres écrits en base b

- Soient $n = \overline{c_p c_{p-1} \ldots c_1 c_0}$ et $m = \overline{d_q d_{q-1} \ldots d_1 d_0}$, avec la convention $c_p \neq 0$ et $d_q \neq 0$.
  Si $p \neq q$, alors n et m sont dans le même ordre que p et q.
  Si $p = q$, alors n et m sont dans le même ordre que les $(p+1)$-uplets $(c_p, c_{p-1}, \ldots, c_1, c_0)$ et $(d_p, d_{p-1}, \ldots, d_1, d_0)$ classés suivant l'ordre lexicographique (c'est-à-dire départagés par la première inégalité entre chiffres de même rang, dans une lecture de gauche à droite.)
- Les entiers qui s'écrivent $n = \overline{c_{p-1} \ldots c_1 c_0}$ (c'est-à-dire avec p chiffres) sont ceux compris entre $b^{p-1} = \overline{10 \ldots 0}$ (le chiffre 1 suivi de $p-1$ fois le chiffre 0) et $b^p - 1 = \overline{\alpha\alpha \ldots \alpha}$ (p fois le chiffre noté ici α et correspondant à la valeur $b-1$.)

Somme de deux nombres écrits en base b

– Soient x et y deux entiers naturels non nuls.

Quitte à rajouter en tête des chiffres égaux à 0, on peut supposer que les écritures en base b des entiers x et y ont la même longueur.

Si $x=\overline{x_p\dots x_1x_0}=\sum_{k=0}^{p}x_kb^k$ et $y=\overline{y_p\dots y_1y_0}=\sum_{k=0}^{p}y_kb^k$, on a $z=x+y=\sum_{k=0}^{p}(x_k+y_k)b^k$.

Dans cette écriture, les entiers x_k+y_k sont compris entre 0 et $2b-2$. Ils peuvent être supérieurs à $b-1$ et ne représentent donc pas en général les chiffres z_k de $z=x+y$.

Pour obtenir cette représentation, il faut utiliser et reporter une retenue de 1 à chaque fois que la somme intermédiaire obtenue est supérieure ou égale à b.

La procédure Maple suivante additionne deux entiers représentés par les listes X et Y de leurs chiffres (aucun test n'est effectué sur la validité des arguments). On place dans x la plus longue des deux listes (l'autre est complétée par des 0) et on forme la somme dans la liste x :

```
somme:=proc(X,Y) global base; local x,y,n,r,k:
  if nops(X)>=nops(Y) then x:=X: y:=Y else x:=Y: y:=X fi;
  n:=nops(x): y:=[0$n-nops(y),op(y)]; r:=0;
  for k from n to 1 by -1 do
    x[k]:=x[k]+y[k]+r;
    if x[k]>=base then x[k]:=x[k]-base: r:=1 else r:=0 fi;
  od;
  if r=1 then [1,op(x)] else x fi;
end:
```

Produit de deux nombres écrits en base b

– Le produit de $n=\overline{c_pc_{p-1}\dots c_1c_0}$ par la base b s'écrit $\overline{c_pc_{p-1}\dots c_1c_00}$. Plus généralement le produit par b^m s'obtient en ajoutant m fois le chiffre 0 à la droite de la représentation de n.

– Soient x et y deux entiers naturels non nuls, écrits en base b :

Si $x=\overline{x_p\dots x_1x_0}=\sum_{j=0}^{p}x_jb^j$ et $y=\overline{y_q\dots y_1y_0}=\sum_{k=0}^{q}y_kb^k$ (avec $x_p\neq0$ et $y_q\neq0$).

Alors le produit $z=xy$ peut s'écrire $z=\sum_{j=0}^{p}x_jb^jy=\sum_{j=0}^{p}\left(\sum_{k=0}^{q}x_jy_kb^{k+j}\right)$.

Notons $t_j=\sum_{k=0}^{q}x_jy_kb^{k+j}$ le produit de y par x_jb^j.

En base b, on peut écrire $t_j=\overline{(x_jy_q)\dots(x_jy_1)(x_jy_0)0\dots0}$ (il y a j chiffres 0 à la fin).

En fait, il n'en est pas exactement ainsi car les produits x_jy_k peuvent atteindre et dépasser la valeur de b : le calcul des chiffres de t_j s'effectue donc en utilisant une retenue r.

Contrairement à l'opération d'addition, où r ne pouvait prendre que les valeurs 0 et 1, la retenue peut ici prendre toutes les valeurs comprises entre 0 et $b-1$, c'est-à-dire être un chiffre quelconque dans la base de numération b.

En effet : le produit de deux entiers a,b de $[\![0,b-1]\!]$, s'il est affecté d'une retenue r de $[\![0,b-1]\!]$, conduit à un résultat inférieur ou égal à $(b-1)^2+r$ donc inférieur ou égal à $b(b-1)$. Modulo b, ce résultat produit donc à son tour une retenue inférieure ou égale à $b-1$.

L'algorithme de multiplication consiste donc à former et à additionner successivement les produits partiels t_j. Voici une procédure Maple effectuant le produit de deux entiers repésentés par les listes x et y de leurs chiffres (aucun test n'est effectué sur la validité des arguments).

```
> produit:=proc(x,y)
    global base;
    local nx,ny,j,k,r,z,xj;
    nx:=nops(x); ny:=nops(y); z:=[0$nx+ny];
    for j from nx to 1 by -1 do
      xj:=x[j]: r:=0;
      for k from ny to 1 by -1 do
        z[j+k]:=irem(z[j+k]+xj*y[k]+r,base,'r');
      od;
      z[j]:=r;
    od;
    if r=0 then subsop(1=NULL,z) else z fi;
  end:
```

Voici un exemple d'utilisation de la procédure *produit* (en base 10, ce qui permet de vérifier facilement que le résultat est correct) :

```
> base:=10: produit([9,9,7,3,8,2],[9,3,1,5]), 997382*9315;
```

$$[9,2,9,0,6,1,3,3,3,0], \quad 9290613330$$

Exponentiation rapide

– Soit E un monoïde, dont la loi est notée par juxtaposition.
Soit a un élément de E et n un entier naturel non nul.
Pour calculer a^n il est inefficace d'effectuer le produit de n exemplaires de a, car on peut obtenir le même résultat avec beaucoup moins d'opérations en utilisant la représentation de l'exposant n en base 2.

– Posons en effet $n = \overline{b_p \dots b_1 b_0} = \sum_{k=0}^{p} b_k 2^k$ (pour tout k, $b_k = 0$ ou $b_k = 1$.)
Notons S l'ensemble des k de $\{0, \dots, p\}$ tels que $b_k = 1$. Alors $n = \sum_{k \in S} 2^k$ puis $a^n = \prod_{k \in S} a^{2^k}$.
Il suffit donc de calculer les $u_k = a^{2^k}$. Or $u_0 = a$ et pour tout k on a $u_{k+1} = u_k^2$. On calcule donc les u_k (pour $k \in S$) par des élévations au carré successives, et on les multiplie.
On calcule les chiffres binaires b_k de n par divisions successives par 2 (le premier dividende est n, le suivant est le quotient entier de n par 2, etc.) Le chiffre b_k est le reste dans la $(k+1)$-ième division : k est dans S si le dividende de la $(k+1)$-ième division est impair.

– Par exemple $1234 = \overline{10011010010}$. Pour calculer a^{1234}, il suffit donc de calculer
  ◇ $u_1 = a^2$ (une élévation au carré)
  ◇ $u_4 = a^{2^4} = ((u_1^2)^2)^2$ (trois élévations au carré)
  ◇ $u_6 = a^{2^6} = (u_4^2)^2$ (deux élévations au carré)
  ◇ $u_7 = a^{2^7} = u_6^2$ (une élévation au carré)

◇ $u_{10} = a^{2^{10}} = ((u_7^2)^2)^2$ (trois élévations au carré)

On a alors $a^{1234} = u_{10}u_7u_6u_4u_1$ (quatre produits).

Ainsi 14 produits suffisent à calculer a^{1234}.

– La procédure Maple suivante calcule la puissance n-ième d'un élément a. Pour garder toute sa généralité au calcul, on appelle une fonction nommée *produit* pour effectuer les multiplications intermédiaires. On utilise également une variable globale nommée *neutre* pour représenter l'élément neutre du monoïde.

```
> puissance:=proc(a,N::nonnegint)
    global neutre;local n,u,p;
    n:=N; u:=a; p:=neutre;
    while n<>0 do
      if type(n,odd) then p:=produit(u,p) fi;
      u:=produit(u,u); n:=iquo(n,2);
    end; eval(p);
  end:
```

Voici un exemple d'exponentiation d'un entier écrit dans une base de numération (ici la base 10 pour vérifier le résultat). On utilise la fonction *produit* définie précédemment.

```
> neutre:=[1]: base:=10:
> puissance([4,2,8,3],5),4283^5;
```

$$[1,4,4,1,2,5,3,4,9,0,1,1,0,5,8,1,6,4,3], \quad 1441253490110581643$$

Programmation récursive de l'exponentiation rapide

On peut aussi utiliser une programmation récursive, en notant que a^n peut être défini par $a^n = \left(a^{n/2}\right)^2$ si n est pair et $a^n = a\left(a^{(n-1)/2}\right)^2$ si n est impair.

Voici une procédure Maple utilisant cette méthode, avec le même exemple d'utilisation :

```
> rec_puissance:=proc(a,n::nonnegint)
    local t;
    if n=0 then neutre
    else t:=rec_puissance(a,iquo(n,2)); t:=produit(t,t);
      if type(n,odd) then produit(a,t) else eval(t) fi;
    fi;
  end:
> neutre:=[1]: base:=10:
> rec_puissance([4,2,8,3],5),4283^5;
```

$$[1,4,4,1,2,5,3,4,9,0,1,1,0,5,8,1,6,4,3], \quad 1441253490110581643$$

Application au calcul matriciel

On peut utiliser les procédures précédentes pour calculer les puissances d'une matrices carrée. Voici d'abord comment modifier la définition de la procédure *produit* et de l'élément neutre :

```
> produit:=(A,B)->evalm(A&*B): neutre:=&*():
```

On calcule ici la puissance quinzième d'une matrice carrée d'ordre 2 (évidemment il y a une fonction intégrée à Maple pour vérifier le résultat) :

```
> A:=matrix([[4,-1],[2,-3]]):
> puissance(A,15),rec_puissance(A,15),evalm(A&^15);
```

$$\begin{bmatrix} 351343134 & -52871731 \\ 105743462 & -18758983 \end{bmatrix}, \begin{bmatrix} 351343134 & -52871731 \\ 105743462 & -18758983 \end{bmatrix}, \begin{bmatrix} 351343134 & -52871731 \\ 105743462 & -18758983 \end{bmatrix}$$

Si $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ alors $A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$, où F_n est terme d'indice n de la suite de Fibonacci, définie par $F_1 = F_2 = 1$ et $F_n = F_{n-1} + F_{n-2}$.

```
> A:=matrix([[1,1],[1,0]]): puissance(A,125);
```

$$\begin{bmatrix} 961518554630184224687745 68 & 594251147575126432128751 25 \\ 594251147575126432128751 25 & 367267407055057792558994 43 \end{bmatrix}$$

On vérifie le résultat avec la fonction intégrée *fibonacci* du package *combinat* :

```
> with(combinat): fibonacci(124); fibonacci(125); fibonacci(126);
```

$$36726740705505779255899443$$
$$59425114757512643212875125$$
$$96151855463018422468774568$$

V.2 Divisibilité dans Z

Définition

Soient a et b deux entiers relatifs. On dit que b est un *diviseur* de a, ou encore que a est un *multiple* de b, et on note $b \mid a$, s'il existe un entier relatif q tel que $a = qb$.

Définition

Pour tout n de $\mathbb{Z}$, on note $n\mathbb{Z} = \{qn, q \in \mathbb{Z}\}$ l'ensemble des multiples de n.
On note $\mathcal{D}(n)$ l'ensemble des diviseurs de n.
Pour tous a, b dans $\mathbb{Z}$, on a donc : $a \mid b \Leftrightarrow b \in a\mathbb{Z} \Leftrightarrow a \in \mathcal{D}(b)$.

Remarques et propriétés

– On a bien sûr $n\mathbb{Z} = (-n)\mathbb{Z}$ et $\mathcal{D}(n) = \mathcal{D}(-n)$ ce qui permettrait de se limiter à $n \geq 0$.
Par exemple $2\mathbb{Z}$ est l'ensemble des entiers relatifs pairs.
On rappelle que les $n\mathbb{Z}$ sont les sous-groupes de $(\mathbb{Z}, +)$.

– 0 est multiple de tout entier b (car $0 = 0b$) mais ne divise que lui-même (car $a = q0 \Rightarrow a = 0$.)
Les entiers 1 et -1 divisent tous les entiers relatifs ($a = a1 = (-a)(-1)$) mais ils ne sont multiples que d'eux mêmes ($qb \in \{-1, 1\} \Rightarrow b \in \{-1, 1\}$).
Ainsi $0\mathbb{Z} = \{0\}$, $1\mathbb{Z} = \mathbb{Z}$, $\mathcal{D}(0) = \mathbb{Z}$ et $\mathcal{D}(1) = \{-1, 1\}$.

– En posant $a \mid b$, on définit une relation binaire sur $\mathbb{Z}$ qui est réflexive et transitive. Contrairement à sa restriction à $\mathbb{N}$, elle n'est pas antisymétrique (donc ce n'est pas une relation d'ordre). En effet : $\forall (a,b) \in \mathbb{Z}^2$, $\begin{cases} a \mid b \\ b \mid a \end{cases} \Leftrightarrow |a| = |b|$.

– Pour tous entiers relatifs a, b, on a : $a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b \mid a \Leftrightarrow \mathcal{D}(b) \subset \mathcal{D}(a)$.
On en déduit $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow |a| = |b| \Leftrightarrow \mathcal{D}(a) = \mathcal{D}(b)$.

Définition *(division euclidienne dans $\mathbb{Z}$)*

Soit (a,b) dans $\mathbb{Z} \times \mathbb{N}^*$.
Il existe un unique couple (q,r) de $\mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r \leq b-1$
Le passage du couple (a,b) au couple (q,r) s'appelle *division euclidienne* de a par b.
Dans cette division, a est le *dividende*, b le *diviseur*, q le *quotient*, et r le *reste*.

Remarques

– Soient a, b deux entiers relatifs, avec $b > 0$. Dire que b divise a (ou encore que a appartient à $b\mathbb{Z}$) c'est dire que le reste dans la division de a par b est nul.

– Le quotient entier dans la division de a par b est la partie entière du rationnel $\frac{a}{b}$.

– Soit n dans $\mathbb{N}^*$. La relation $x \equiv y \Leftrightarrow y - x \in n\mathbb{Z}$ (c'est-à-dire$\Leftrightarrow n \mid y - x$) est une relation d'équivalence sur $\mathbb{Z}$ (appelée relation de *congruence modulo* n).
On a $x \equiv y \Leftrightarrow x$ et y ont le même reste dans la division par n. Tout entier x est en relation avec un unique r de $\{0, \dots, n-1\}$, l'entier r étant le reste dans la division de x par n.
On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ l'ensemble des classes d'équivalence.

V.3 Pgcd de deux entiers relatifs

Proposition

Soit $(G,+)$ un groupe abélien. Soient H et K deux sous-groupes de G.
On note $H + K = \{h + k, h \in H, k \in K\}$.
Alors $H + K$ est un sous-groupe de G qui contient H et K.
Plus précisément $H + K$ est le plus petit sous-groupe de G qui contient H et K : c'est donc le sous-groupe de G engendré par $H \cup K$.

Remarque

Ce résultat peut être généralisé à une famille finie $H_1, \dots, H_n$ de sous-groupes de $(G,+)$: $H_1 + \cdots + H_n = \{h_1 + \cdots + h_n, h_k \in H_k\}$ est le sous-groupe de G engendré par $\bigcup_{k=1}^{n} H_k$.

Définition *(pgcd de deux entiers)*

Soient a et b deux entiers relatifs.
Il existe un unique entier naturel n tel que $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$.
On dit que n est le pgcd de a et de b. On note $n = \text{pgcd}(a,b)$, ou $n = a \wedge b$.

Remarque

Par construction, il existe des entiers u et v tels que $a \wedge b = au + bv$.
Réciproquement tout entier qui s'écrit $au + bv$ est un multiple de $a \wedge b$.

Proposition *(caractérisation du pgcd)*

Soient a et b deux entiers relatifs, et soit $n = a \wedge b$.
D'une part n divise a et b. D'autre part tout diviseur de a et b divise n.
Ces propriétés caractérisent entièrement l'entier $n = a \wedge b$.
Autrement dit, $a \wedge b$ est l'unique entier naturel n tel que $\mathcal{D}(n) = \mathcal{D}(a) \cap \mathcal{D}(b)$.

Remarques et propriétés

- Si $a = b = 0$ alors $n = 0 \wedge 0 = 0$ (les diviseurs communs à a et b sont tous les entiers relatifs.)
- Si a et b ne sont pas tous deux nuls, alors $n = a \wedge b$ est strictement positif.
  L'entier n est alors le plus grand élément de $\mathcal{D}(n)$ c'est-à-dire le plus grand des diviseurs communs des entiers a et b.
  Cette propriété justifie l'appellation "pgcd".
- Pour tous entiers relatifs a et b, on a : $a \wedge b = b \wedge a = |a| \wedge b = a \wedge |b| = |a| \wedge |b|$.
  Pour tout a de $\mathbb{Z}$: $a \wedge 0 = |a|$, et $a \wedge 1 = 1$.
  On a l'égalité $a \wedge b = |a|$ si et seulement si a divise b.
- Pour tous entiers relatifs a, b, k, on a : $a \wedge b = (a - kb) \wedge b$.
- Pour tous entiers relatifs a, b, k, on a : $(ka) \wedge (kb) = |k|\,(a \wedge b)$.
  De même, si k est un diviseur commun à a et b, on a : $\frac{a}{k} \wedge \frac{b}{k} = \frac{a \wedge b}{|k|}$.

Proposition *(Algorithme d'Euclide)*

Soient a et b deux entiers relatifs. On veut calculer $a \wedge b$.
On suppose $b \neq 0$ (sinon $a \wedge b = |a|$) et même $b > 0$ (quitte à remplacer b par $-b$).
Soit $a = bq_1 + r_1$ la division euclidienne de a par b : on sait que $0 \leq r_1 < b$.
On a $\text{pgcd}(a, b) = \text{pgcd}(b, r_1)$. Si $r_1 = 0$ alors $\text{pgcd}(a, b) = b$.
Sinon, soit $b = r_1 q_2 + r_2$ la division euclidienne de b par r_1. On a $0 \leq r_2 < r_1$.
Si $r_2 = 0$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = r_1$.
Sinon on divise r_1 par r_2, et le procédé se poursuit.
On forme ainsi une suite $b > r_1 > r_2 > r_3 > \cdots \geq 0$ strictement décroissante d'entiers.
On peut passer de r_k à r_{k+1} tant que $r_k \neq 0$.
Cette suite de premier terme b est nécessairement finie.
Il existe donc un entier naturel n tel que $r_n > 0$ et $r_{n+1} = 0$.
On a alors $\text{pgcd}(a, b) = r_n$.
Ainsi $\text{pgcd}(a, b)$ est le dernier reste non nul dans cette succession de divisions.

Utilisation de Maple

La procédure suivante calcule le pgcd de deux entiers naturels a et b.

```
> euclide:=proc(A::nonnegint,B::nonnegint)
    local a,b,r;
    a:=A; b:=B;
    while b>0 do
      r:=irem(a,b); a:=b; b:=r;
    od;
    a;
  end:
```

Voici un exemple d'utilisation, et la confirmation du résultat avec la fonction intégrée *igcd* :

```
> euclide(267914296,317811), igcd(267914296,317811);
```

$$377, \quad 377$$

Voici le détail des calculs, qui ne demandent que trois divisions :

$$267914296 = 842 * 317811 + 317434, \quad 317811 = 1 * 317434 + 377 \quad 317434 = 842 * 377$$

On peut également utiliser une méthode récursive très simple :

```
> euclide_rec:=proc(a::nonnegint,b::nonnegint)
    if b=0 then a
       else euclide_rec(b,irem(a,b))
    fi
  end:
> euclide_rec(267914296,317811);
```

$$377$$

V.4 Entiers premiers entre eux

Définition

Soient a et b deux entiers relatifs.
On dit que a et b sont *premiers entre eux* (ou encore *étrangers*) si $a \wedge b = 1$.
Cela équivaut à dire que les seuls diviseurs communs à a et b sont 1 et -1.
Il revient au même d'écrire $\mathcal{D}(a) \cap \mathcal{D}(b) = \{-1, 1\}$.

Proposition *(identité de Bezout)*

Soient a et b deux entiers relatifs.
a et b sont premiers entre eux$\Leftrightarrow$il existe deux entiers relatifs u, v tels que $au + bv = 1$.

Théorème *(Théorème de Gauss)*

Soient a, b, c trois entiers relatifs.
Si a divise bc et si a est premier avec b, alors a divise c.

Remarques et propriétés

- Deux entiers relatifs a et b non nuls sont premiers entre eux si et seulement si le dernier reste non nul dans l'algorithme d'Euclide des divisions successives est égal à 1.
- Soient a et b deux entiers relatifs (non tous deux nuls), et d leur pgcd.
  Les deux entiers a' et b' tels que $a = da'$ et $b = db'$ sont premiers entre eux.
  Le rationnel $r = \dfrac{a}{b}$ admet donc la forme simplifiée (on dit aussi *irréductible*) $r = \dfrac{a'}{b'}$.
  La forme irréductible de $r \in \mathbb{Q}^*$ est unique si on impose au dénominateur d'être > 0.
- Soient u, v deux entiers relatifs premiers entre eux.
  Pour tout entier $\delta > 0$, le pgcd des entiers $a = \delta u$ et $b = \delta v$ est égal à δ.
- Soient a, b, c trois entiers relatifs.
  Si a est premier avec b et avec c, alors il est premier avec bc.
  Autrement dit $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow a \wedge (bc) = 1$.
  Plus généralement si pour tous indices j et k les entiers a_j et b_k sont premiers entre eux, alors les produits $a_1 a_2 \dots a_m$ et $b_1 b_2 \cdots b_n$ sont premiers entre eux.
  En particulier : $a \wedge b = 1 \Rightarrow a^m \wedge b^n = 1$.
- Réciproquement si un entier a est premier avec le produit bc, il est premier avec b et avec c.
  Plus généralement si les produits $a_1 a_2 \dots a_m$ et $b_1 b_2 \cdots b_n$ sont premiers entre eux, alors chacun des a_j est premier avec chacun des b_k.
- Soient a, b, c trois entiers relatifs.
  On suppose que a et b divisent c et que $a \wedge b = 1$. Alors le produit ab divise c.
  Plus généralement si les entiers $a_1, a_2, \dots, a_n$ sont premiers entre eux deux à deux, et si chacun des a_k divise l'entier c, alors le produit $a_1 a_2 \dots a_n$ divise c.

V.5 Résolution dans Z de l'équation ax+by=c

Proposition *(résolution de $ax + by = 1$)*

Soient a et b deux entiers relatifs non nuls et premiers entre eux.
Alors il existe une infinité de couples (x, y) de $\mathbb{Z}^2$ tels que $ax + by = 1$.
Si (x_0, y_0) est l'un d'eux, les autres sont donnés par $\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases}$ avec $k \in \mathbb{Z}$.

Proposition *(résolution de $ax + by = a \wedge b$)*

Soient a et b deux entiers relatifs non nuls.
Soient a' et b' les entiers (premiers entre eux) tels que $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$.
Il existe une infinité de couples (x, y) de $\mathbb{Z}^2$ tels que $ax + by = a \wedge b$.
Chacun d'eux est appelé un *couple de coefficients de Bezout* de (a, b).
Si (x_0, y_0) est l'un d'eux, les autres sont donnés par $\begin{cases} x = x_0 + kb' \\ y = y_0 - ka' \end{cases}$ avec $k \in \mathbb{Z}$.

Recherche d'un couple de coefficients de Bezout

– On applique l'algorithme d'Euclide au couple $(|a|,|b|)$.
On forme ainsi des divisions successives $r_{k-1}=q_kr_k+r_{k+1}$ avec au départ $r_0=|a|$ et $r_1=|b|$.
La dernière de ces divisions s'écrit $r_{n-1}=q_nr_n$ (donc $r_{n+1}=0$).
Le pgcd de a et b est égal à r_n (dernier reste non nul).
L'avant dernière division $r_{n-2}=q_{n-1}r_{n-1}+r_n$ donne alors $a\wedge b=r_{n-2}-q_{n-1}r_{n-1}$.
La division précédente $r_{n-3}=q_{n-2}r_{n-2}+r_{n-1}$ permet alors d'exprimer r_{n-1} et donc $a\wedge b$ en fonction de r_{n-2} et de r_{n-3}. En "remontant" les calculs, on obtient ainsi une expression de $a\wedge b$ sous la forme $ax+by$, ce qui fournit une solution particulière au problème.

– Voici comment calculer une solution de $ax+by=a\wedge b$, avec $a=14938$ et $b=9471$.
On effectue d'abord les calculs de la première colonne, qui donnent $a\wedge b=77$.
On effectue ensuite ceux de la deuxième colonne, qui donnent $26a-41b=77$.

$$\begin{aligned}
14938 &= 1\cdot 9471+5467 \\
9471 &= 1\cdot 5467+4004 \\
5467 &= 1\cdot 4004+1463 \\
4004 &= 2\cdot 1463+1078 \\
1463 &= 1\cdot 1078+385 \\
1078 &= 2\cdot 385+308 \\
385 &= 1\cdot 308+77 \\
308 &= 4\cdot 77
\end{aligned}
\qquad
\begin{aligned}
77 &= 385-308 \\
77 &= 385-(1078-2\cdot 385)=3\cdot 385-1078 \\
77 &= 3(1463-1078)-1078=-4\cdot 1078+3\cdot 1463 \\
77 &= -4\cdot(4004-2\cdot 1463)+3\cdot 1463=11\cdot 1463-4\cdot 4004 \\
77 &= 11\cdot(5467-4004)-4\cdot 4004=-15\cdot 4004+11\cdot 5467 \\
77 &= -15\cdot(9471-5467)+11\cdot 5467=26\cdot 5467-15\cdot 9471 \\
77 &= 26\cdot(14938-9471)-15\cdot 9471=26\cdot 14938-41\cdot 9471
\end{aligned}$$

– *Méthode récursive*
Soit $a=bq+r$ la division euclidienne de a par b.
Soit (x',y') un couple vérifiant $bx'+ry'=b\wedge r$.
Alors $a\wedge b=b\wedge r=bx'+(a-bq)y'=ay'+b(x'-qy')$.
Autrement dit, le couple $(x=y',y=x'-qy')$ vérifie $ax+by=a\wedge b$.
Voici donc une procédure Maple utilisant cette idée, en notant que si $b=0$ une solution (x,y) de l'équation $ax+by=a\wedge b=a$ est $(1,0)$:

```
> coeffbezout_rec:=proc(a::nonnegint,b::nonnegint)
    local q,t:
    if b=0 then 1,0 else
      t:=coeffbezout_rec(b,irem(a,b,'q')); t[2],t[1]-q*t[2];
    fi;
  end:
```

On reprend ici l'exemple $a=14938, b=9471$.
On vérifie le résultat avec la fonction intégrée *igcdex* :

```
> A:=14938: B:=9471: coeffbezout_rec(A,B); igcdex(A,B,'x','y'): x,y;
```

$$26,-41$$

$$26,-41$$

– *Méthode itérative*

Notons E_d l'équation $ax+by=d$, où d est un entier relatif quelconque.

Soient α et β deux éléments de $\mathbb{Z}$, avec $\beta \neq 0$.

Soient (x_1, y_1) une solution de E_α et (x_2, y_2) une solution de E_β.

Soit $\alpha = q\beta + r$ la division euclidienne de α par β.

Les égalités $\begin{cases} ax_1+by_1=\alpha \\ ax_2+by_2=\beta \end{cases}$ impliquent $a(x_1-qx_2)+b(y_1-qy_2)=\alpha-q\beta=r$.

Autrement dit le couple $(x_3=x_1-qx_2, y_3=y_1-qy_2)$ est solution de E_r.

On remarque que $(1,0)$ est une solution de E_a et que $(0,1)$ est une solution de E_b.

Si on applique l'idée précédente et l'algorithme d'Euclide au couple (a,b), on va former, pour chacun des restes successifs r_k de cette méthode, une solution (x_k, y_k) de l'équation E_{r_k}.

Si r_n est le dernier reste non nul (donc $r_n = a \wedge b$) alors on obtient une solution (x_n, y_n) de l'équation E_{r_n}, c'est-à-dire de l'équation $ax+by=a\wedge b$.

Voici une proédure Maple utilisant cette méthode, et un exemple d'utilisation :

```
> coeffbezout:=proc(A::nonnegint,B::nonnegint)
    local a,b,xy1,xy2,q,r,t;
    a:=A; b:=B; xy1:=[1,0]; xy2:=[0,1];
    while b<>0 do q:=iquo(a,b,'r'); a:=b; b:=r;
      t:=xy1; xy1:=xy2; xy2:=t-q*xy2;
    od;
    op(xy1);
  end:
> A:=14938: B:=9471: coeffbezout(A,B);
```

$$26, -41$$

Résolution de l'équation $ax+by=c$ dans le cas général

On veut résoudre dans $\mathbb{Z}^2$ l'équation (E) $ax+by=c$, où a, b, c sont dans $\mathbb{Z}$, avec $(a,b) \neq (0,0)$.

– Si l'entier c n'est pas un multiple de $a \wedge b$, alors l'équation (E) n'a pas de solutions dans $\mathbb{Z}^2$.

– Supposons au contraire que l'entier c s'écrive $\lambda(a\wedge b)$, avec $\lambda \in \mathbb{Z}$.

Soit (x_0, y_0) un couple de coefficients de bezout de (a,b).

On a $ax_0+bx_0 = a\wedge b$ donc $a(\lambda x_0)+b(\lambda y_0)=c$.

Ainsi le couple $(\lambda x_0, \lambda y_0)$ est une solution particulière de (E).

L'équation (E) s'écrit alors $ax+by=a(\lambda x_0)+b(\lambda y_0)$, c'est-à-dire $a(x-\lambda x_0)=b(\lambda y_0 - y)$.

– En notant a' et b' les entiers (premiers entre eux) définis par $a=a'(a\wedge b)$ et $b=b'(a\wedge b)$, cette dernière équation équivaut à : $a'(x-\lambda x_0)=b'(\lambda y_0 - y)$.

On peut alors appliquer le théorème de Gauss.

Les solutions de (E) sont donc les couples (x,y) définis par $\begin{cases} x=\lambda x_0 + kb' \\ y=\lambda y_0 - ka' \end{cases}$ avec $k \in \mathbb{Z}$.

V.6 Ppcm de deux entiers relatifs

Définition *(ppcm de deux entiers)*

Soient a, b dans $\mathbb{Z}$. Il existe un unique n dans $\mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$.
On dit que n est le pgcd de a et b. On note $n = \text{ppcm}(a, b)$, ou $n = a \vee b$.

Remarques et propriétés

- *Caractérisation du ppcm*
  Soient a et b deux entiers relatifs, et soit $n = a \vee b$.
  D'une part n est multiple de a et b. D'autre part tout multiple de a et b est multiple de n.
  Ces propriétés caractérisent entièrement l'entier naturel $n = a \vee b$.
- Si $a = 0$ ou $b = 0$ alors $a \vee b = 0$ (le seul multiple commun à a et b est 0).
- Si $a \neq 0$ et $b \neq 0$, alors $n = a \vee b > 0$.
  L'entier n est alors le plus petit entier strictement positif de $n\mathbb{Z}$, c'est-à-dire le plus petit multiple commun *strictement positif* de a et b (ce qui justifie l'appellation "ppcm").
  La condition "strictement positif" est importante car dans $\mathbb{N}$ le plus petit multiple commun de deux entiers quelconques a et b est toujours 0...
- Pour tous entiers relatifs a et b, on a : $a \vee b = b \vee a = |a| \vee b = a \vee |b| = |a| \vee |b|$.
  On a l'égalité $a \wedge b = |a|$ si et seulement si a est un multiple de b.
- Pour tous entiers relatifs a, b, k, on a : $(ka) \vee (kb) = |k|\,(a \vee b)$.
  De même, si k est un diviseur commun à a et b, on a : $\frac{a}{k} \vee \frac{b}{k} = \frac{a \vee b}{|k|}$.
- Si a et b sont premiers entre eux, alors $a \vee b = |ab|$, et la réciproque est vraie.
- Pour tous entiers relatifs a et b, on a l'égalité : $(a \wedge b)(a \vee b) = |ab|$.

V.7 Extension au cas de plusieurs entiers relatifs

Proposition

Les lois $(a, b) \mapsto a \wedge b$ et $(a, b) \mapsto a \vee b$ sont commutatives et associatives dans $\mathbb{Z}$.
Soient $a_1, a_2, \ldots, a_n$ dans $\mathbb{Z}$, avec $n \geq 2$. Les notations $\begin{cases} a_1 \wedge a_2 \wedge \cdots \wedge a_n \\ a_1 \vee a_2 \vee \cdots \vee a_n \end{cases}$ ont donc un sens, indépendamment de l'ordre des facteurs a_k et de celui dans lequel on effectue les calculs.

Définition

Soit $a_1, a_2, \ldots, a_n$ une famille de n entiers relatifs, avec $n \geq 2$.
On note $\text{pgcd}(a_1, a_2, \ldots, a_n) = a_1 \wedge a_2 \wedge \cdots \wedge a_n$ et $\text{ppcm}(a_1, a_2, \ldots, a_n) = a_1 \vee a_2 \vee \cdots \vee a_n$.

Caractérisation du pgcd et du ppcm

- $d = \text{pgcd}(a_1, a_2, \dots, a_n)$ est l'unique entier naturel tel que $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$.
  En particulier, il existe des entiers relatifs u_k tels que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = d$.
  d est également l'unique entier naturel tel que $\mathcal{D}(a_1) \cap \mathcal{D}(a_2) \cap \cdots \cap \mathcal{D}(a_n) = \mathcal{D}(d)$.
  Ainsi un entier x divise $a_1, a_2, \dots, a_n$ si et seulement s'il divise leur pgcd.
- $m = \text{ppcm}(a_1, a_2, \dots, a_n)$ est l'unique entier naturel tel que $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z} = m\mathbb{Z}$.
  Ainsi un entier x est multiple de $a_1, a_2, \dots, a_n$ si et seulement s'il est multiple de leur ppcm.

Définition *(entiers premiers entre eux dans leur ensemble)*

On dit que les n entiers relatifs $a_1, a_2, \dots, a_n$ (avec $n \geq 2$) sont *premiers entre eux dans leur ensemble* si leur pgcd est égal à 1.

Cela équivaut à dire que les seuls diviseurs communs à $a_1, a_2, \dots, a_n$ sont 1 et -1.

Cela équivaut également à l'existence de n entiers relatifs $u_1, u_2, \dots, u_n$ tels qu'on ait l'égalité $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$ (identité de Bezout).

Remarques et propriétés

- Si deux au moins des entiers $a_1, \dots, a_n$ sont premiers entre eux, et à fortiori si $a_1, \dots, a_n$ sont premiers entre eux *deux à deux*, alors ils le sont *dans leur ensemble*.
  Dès que $n \geq 3$, la réciproque est fausse comme le montre l'exemple de $6, 10, 15$: le pgcd de ces trois entiers est égal à 1, mais $6 \wedge 10 = 2$, $6 \wedge 15 = 3$, $10 \wedge 15 = 5$.
- Soient $\lambda, a_1, \dots, a_n$ des entiers relatifs. Soit μ un diviseur de $a_1, \dots, a_n$. On a les égalités :

$$\begin{cases} \text{pgcd}(\lambda a_1, \dots, \lambda a_n) = |\lambda| \,\text{pgcd}(a_1, \dots, a_n) \\ \text{ppcm}(\lambda a_1, \dots, \lambda a_n) = |\lambda| \,\text{ppcm}(a_1, \dots, a_n) \end{cases} \qquad \begin{cases} \text{pgcd}(\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}) = \frac{1}{|\mu|} \,\text{pgcd}(a_1, \dots, a_n) \\ \text{ppcm}(\frac{a_1}{\mu}, \dots, \frac{a_n}{\mu}) = \frac{1}{|\mu|} \,\text{ppcm}(a_1, \dots, a_n) \end{cases}$$

- Soit $\mu > 0$ un diviseur de $a_1, \dots, a_n$.
  $\mu = \text{pgcd}(a_1, \dots, a_n) \Leftrightarrow$les entiers $\frac{a_k}{\mu}$ sont premiers entre eux dans leur ensemble.
- Si $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble, alors $\text{ppcm}(a_1, \dots, a_n) = |a_1 \dots a_n|$.
- Attention : l'égalité $(a \wedge b)(a \vee b) = |ab|$ ne se généralise pas à plus de deux entiers.

V.8 Nombres premiers

Définition

Soit p un entier naturel.

On dit que p est premier si $p \geq 2$ et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

On note $\mathcal{P}$ l'ensemble des nombres premiers.

Remarques et propriétés

- On remarque que 1 n'est pas considéré comme un nombre premier.
- On peut aussi adopter la définition suivante : un entier naturel p est dit premier s'il possède exactement deux diviseurs distincts dans $\mathbb{N}$ (ce qui exclut les entiers 0 et 1.)
- Les dix "premiers" nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.
  A l'exception de 2, tous les nombres premiers sont impairs.
- Dans la phrase "a est premier avec b", il n'y en général pas de nombre premier...
- Soit p un nombre premier, et a un entier relatif.
  Si p ne divise pas a, alors p est premier avec a.
  En particulier, p est premier avec tous les entiers de $\{1, \dots, p-1\}$.
  Une autre conséquence est que deux nombres premiers distincts sont premiers entre eux.
- Soit p un nombre premier, et soit $a_1, a_2, \dots, a_n$ une famille d'entiers relatifs.
  Alors p divise le produit $a_1 a_2 \dots a_n$ si et seulement si p divise l'un au moins des a_k.

Proposition

Tout entier naturel $n \geq 2$ est divisible par au moins un nombre premier.

Proposition

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

Théorème *(décomposition en produit de facteurs premiers)*

Tout entier $n \geq 2$ s'écrit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, où :
- m est un entier strictement positif.
- $p_1, p_2, \dots, p_m$ sont des nombres premiers distincts deux à deux.
- $\alpha_1, \alpha_2, \dots, \alpha_m$ sont des entiers strictement positifs.

Une telle écriture de n est unique à l'ordre près des facteurs.
On l'appelle *décomposition de n en produits de facteurs premiers.*

Remarques et propriétés

- Dans l'écriture précédente de n, les p_k sont les diviseurs premiers de n.
- Supposons qu'en fait $\{p_1, p_2, \dots, p_m\}$ *contienne* l'ensemble des diviseurs premiers de n.
  Alors on peut encore écrire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, où les α_k sont seulement supposés ≥ 0.
  Pour un ensemble $\{p_1, p_2, \dots, p_m\}$ donné, il y a encore unicité de l'écriture.
  L'entier 1 peut s'écrire sous cette forme, avec des α_k tous égaux à 0.
- Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ dans $\mathbb{N}^*$ (ici les p_k sont premiers disctincts, et les α_k sont ≥ 0).
  Soit m un entier strictement positif.
  On a $m \mid n \Leftrightarrow m$ s'écrit $p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$, avec $0 \leq \beta_k \leq \alpha_k$ pour tout k.
  En particulier, l'entier n possède $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1)$ diviseurs distincts dans $\mathbb{N}$.

– Soient x et y deux entiers naturels.
Soit $\{p_1, p_2, \dots, p_m\}$ l'ensemble des nombres premiers distincts qui divisent x ou y.
On peut donc écrire $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ et $y = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$, où les α_k, β_k sont ≥ 0.
Dans ces conditions $\begin{cases} x \wedge y = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_m^{\gamma_m} \\ x \vee y = p_1^{\delta_1} p_2^{\delta_2} \dots p_m^{\delta_m} \end{cases}$ avec $\begin{cases} \gamma_k = \min(\alpha_k, \beta_k) \\ \delta_k = \max(\alpha_k, \beta_k) \end{cases}$ pour tout k.
Ce résultat peut se généraliser au calcul des pgcd et ppcm de n entiers $x_1, x_2, \dots, x_n$.

– Le résultat précédent permet de retrouver l'égalité $(x \wedge y)(x \vee y) = xy$.
On a en effet $\gamma_k + \delta_k = \alpha_k + \beta_k$ pour tout indice k.

– On peut étendre aux entiers n de $\mathbb{Z}$ (sauf $-1, 0, 1$) le principe de la décomposition en produits de facteurs premiers : il suffit d'écrire $n = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, avec $\varepsilon = \pm 1$.