Computaional Reology - REDUCTION

1 Chapiter 2 : Conservation Laws and the Stress Tensor

1.1 The Stress Tensor

Théorème 2.1.
Transformation from a stress vector $\boldsymbol{s}_n(\boldsymbol{x},t)$ at a surface to a stress tensor $\boldsymbol{\sigma}(\boldsymbol{x},t)$. Proved its existence provided that the stress tensor is symmetric (for uniqueness ? See appendix)

$$\boldsymbol{s}_n(\boldsymbol{x},t) = \boldsymbol{n}\cdot\boldsymbol{\sigma}(\boldsymbol{x},t)$$

2.4 Newtonian Fluid
Write the components σ_{ij} of $\boldsymbol{\sigma}$ in

$$\sigma_{ij} = -p\delta_{ij} + T_{ij}$$
$$T_{ij} = A_{ijkl}\frac{\partial u_k}{\partial x_l}$$

An isotropic material is said to have invariance under rotation of axes, meaning that $\boldsymbol{T}$ should be isotropic tensor function of the components of $\nabla\boldsymbol{u}$. And Newtonian means linear. From eq(2.23) to eq(2.28), we prove for the Newtonian fluid $3\lambda + 2\eta = 0$ and for incompressible Newtonian fluid, $T_{ij} = \eta\dot{\gamma}_{ij}$ where $\dot{\boldsymbol{\gamma}} = (\nabla\boldsymbol{u} + (\nabla\boldsymbol{u})^T)$

2.4.1 Generalized Newtonian Fluid
Towards the non-Newtonian, first step is to simulate the shear-thining by making variant viscosity as eq(2.41) where the I_i is the invariants of the second order symmetric tensor $\dot{\boldsymbol{\gamma}}$

$$\sigma_{ij} = -p\delta_{ij} + \eta(I_1, I_2, I_3)\dot{\gamma}_{ij}$$

As two of the invariants vanishes (one for incompressibility, another vanishes in a 1D simple shear flow), visosity is dependant only on eq(2.43) $\dot{\gamma}_{ij}\dot{\gamma}_{ji}$. Well, it is then usual to write η as function of shear-rate $\dot{\gamma}$ where

$$\dot{\gamma} = \sqrt{\frac{1}{2}\boldsymbol{\gamma}:\boldsymbol{\gamma}} = \sqrt{\frac{1}{2}\dot{\gamma}_{ij}\dot{\gamma}_{ji}}$$

The $A:B$ between the two second order tensor is an operation taking lines of A and colons B taking scalar product and sum :

$$\boldsymbol{A}:\boldsymbol{B} = A_{ij}B_{ji}$$

2.5.2-2.5.3 Order Fluids
In eq(2.55) kth-order Rivlin-Ericksen tensor $\boldsymbol{A_k}$ is obtained by k-time time-derivative then making $t' = t$ where t' is used to define $\boldsymbol{C}$.

Under Rivlin and Ericksen's assumption, extra-stress tenosr (or deviatoric stress) $\boldsymbol{T} = \boldsymbol{\sigma} + p\boldsymbol{I}$ is a polynomial function of the first N Rivlin-Ericksen tensors i.e. gradients of the velocity, acceleration and higer time derivatives. For 1st, 2nd and 3rd respectively (Note A_i has dimension of t^{-i} where t is the time) :

$$\boldsymbol{T_1} = a_1\boldsymbol{A_1}$$
$$\boldsymbol{T_2} = a_1\boldsymbol{A_1} + a_2\boldsymbol{A_2} + a_{11}\boldsymbol{A_1}^2$$
$$\boldsymbol{T_3} = ...$$

Well, a first order fluid is Newtonian (linear and non-variant viscosity). For both first and second order fluid, the viscosity is invariant (see eq(2.66)).

First and second normal stress coefficients have an analytic expression : eq(2.67) and eq(2.68)

2.5.4 CEF Equation
It can be seen that $A_3 = 0$ for a simple shear flow from eq(2.64). From the recurrence relation, we have $A_k = 0, \forall k \geqslant 3$. Criminale, Ericksen and Filbey in 1958 made simplifications and derived the CEF Equation eq(2.80).

$$\boldsymbol{T} = \eta(\dot{\gamma})\boldsymbol{A_1} - \frac{1}{2}\Phi_1(\dot{\gamma})\boldsymbol{A_2} + (\Phi_1(\dot{\gamma}) + \Phi_2(\dot{\gamma}))\boldsymbol{A_1}^2$$

2.6 More compilcated constitutive models
2.6.1 Differential constitutive models
Oldroyd-type
FENE, Phan-Thien-Tanne

1.2 2.3

– Si a, b sont des entiers, alors $a + b$ est un entier
– Si a, b, c sont des entiers, alors $a + (b + c) = (a + b) + c$
– L'entier 0 a la propriété : $\forall a \in \mathbb{Z}, a + 0 = 0 + a = a$
– Pour tout entier a, il existe un entier b avec $a + b = b + a = 0$

Bien sûr, ces propriétés sont très simples. Nous allons voir qu'elles se retrouvent dans beaucoup de situations, pour d'autres ensembles que $\mathbb{Z}$ et pour d'autres opérations que la somme.

> **Définition.** *Un groupe est un ensemble G et une opération binaire interne $*$ sur G qui vérifie les trois propriétés suivantes :*
> *1. Associativité : $\forall x, y, z \in G, x * (y * z) = (x * y) * z$*
> *2. Element neutre : $\exists e \in G, \forall x \in G, x * e = e * x = x$*
> *3. Inverse : $\forall x \in G, \exists y \in G, x * y = y * x = e$.*

Commentaires.
1. Une opération binaire interne est une opération qui associe à deux éléments x, y de G un élément $x * y$ de G ; elle est dite binaire parce qu'elle a besoin de deux éléments pour exister ; elle est dite interne parce que si x, y sont dans G, $x * y$ est aussi dans G
2. La première propriété, l'associativité, montre que si on fait au moins deux opérations, les parenthèses ne sont pas nécessaires. On pourra écrire, sans qu'il y ait ambiguïté, des expressions comme $x * y * z$ ou $a * b * c * d$.
3. L'élément neutre (qui est toujours unique, comme nous allons le voir) dans notre exemple de $\mathbb{Z}$ avec l'addition est bien sûr le nombre entier 0.
4. Si x est donné, nous allons voir que l'inverse de x est unique. On le note en général x^{-1}, de sorte que $x * x^{-1} = x^{-1} * x = e$. Dans notre exemple de $\mathbb{Z}$, l'inverse du nombre entier a est le nombre entier $-a$.

Notation.
Dorénavant nous allons noter xy au lieu de $x * y$. Il faut garder à l'esprit que xy n'est pas nécessairement une multiplication entre deux nombres, mais une notation pour une situation plus générale. D'ailleurs, pour l'exemple de la somme dans $\mathbb{Z}$, xy désigne la somme de x et y.

1.3 Exemples

1. $(\mathbb{Z}, +)$ est un groupe. L'élément neutre est 0, et l'inverse de a est le nombre $-a$.

2. De même, $(\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes.

3. $(\mathbb{N}, +)$ n'est pas un groupe, car il n'existe pas d'élément $n \in \mathbb{N}$ avec $1 + n = 0$.

4. $([-1, 1], +)$ n'est pas un groupe, car $1 + 1 \notin [-1, 1]$.

5. $(\mathbb{R}_+^*, \cdot)$ est un groupe d'élément neutre 1, et l'inverse de x est le nombre $\dfrac{1}{x}$.

6. $(\mathbb{R}^*, \cdot)$ est un groupe.

7. $(\mathbb{R}, \cdot)$ n'est pas un groupe, car il n'existe pas d'élément $x \in \mathbb{R}$ avec $0 \cdot x = 1$.

8. On note U l'ensemble des nombres complexes de module 1. La multiplication des nombres complexes est une opération interne sur U, car si z, z' sont de module 1, alors zz' est aussi de module 1. Ensuite l'associativité est évidente, l'élément neutre est le nombre complexe 1, et tout $z \in U$ possède un inverse dans U, à savoir $\dfrac{1}{z}$.
Donc $(U, \cdot)$ est un groupe.

1.4 Groupes commutatifs. Groupes non commutatifs

Dans les exemples ci-dessous, les groupes ont tous la propriété $xy = yx$. Cette propriété ne fait pas partie de la définition d'un groupe, mais elle est souvent vraie.

Définition. *Un groupe* **commutatif** *est un groupe G dans lequel on a $\forall x, y \in G, xy = yx$.*

Un groupe commutatif peut aussi être appelé groupe **abélien**, en hommage au mathématicien *Abel*.
Un groupe qui n'est pas commutatif est appéle groupe **non commutatif** ou **non abélien**.

Exemple : Un groupe non commutatif.
On prend un entier $n \geqslant 3$, et on considère l'ensemble S_n de toutes les **bijections** de $E = \{1, \ldots, n\}$ vers $E = \{1, \ldots, n\}$. L'ensemble S_n est de cardinal $n!$. Si f, g sont deux bijections de E vers E, la composée $f \circ g$ est aussi une bijection de E vers E. Donc l'opération $\circ$ est une opération binaire interne sur S_n. Montrons que $(S_n, \circ)$ est un groupe. L'associativité est évidente, car l'opération $\circ$ est toujours associative. L'élément neutre pour $\circ$ est la bijection identité, qui envoie tout élément $x \in E$ sur x. L'inverse de la bijection f est sa bijection réciproque. On a montré que $(S_n, \circ)$ est un groupe. Mais ce n'est pas un groupe commutatif. En effet, considérons la bijection $f : E \to E$ qui est définie par

$$f(1) = 2, f(2) = 3, f(3) = 1, \qquad f(n) = n \text{ pour } n \geqslant 4$$

Considérons également la bijection $g : E \to E$ définie par

$$g(1) = 2, g(2) = 1, \qquad g(n) = n \text{ pour } n \geqslant 3$$

On voit que $(f \circ g)(1) = f(2) = 3$ et $(g \circ f)(1) = g(2) = 1$. Donc $f \circ g \neq g \circ f$, ce qui montre que $(S_n, \circ)$ n'est pas un groupe commutatif (pour $n \geqslant 3$). Le groupe $(S_n, \circ)$ est appelé **le groupe symétrique sur n éléments**. C'est un groupe non commutatif pour $n \geqslant 3$. Lorsque $n = 1$ ou $n = 2$, c'est un groupe commutatif.

1.5 Sous-groupes et morphismes

Définition.
Soit $(G, \cdot)$ un groupe. Un **sous-groupe de** *G est un sous-ensemble H de G qui possède les propriétés suivantes :*
1. $e \in H$ (e est le neutre du groupe G)
2. $\forall x, y \in H, xy \in H$ (propriété de stabilité de H par l'opération de groupe)
3. $\forall x \in H, x^{-1} \in H$ (propriété de stabilité de H par passage à l'inverse)

Exemples.
$(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.
$(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
$(\mathbb{R}, +)$ est un sous-groupe de $(\mathbb{C}, +)$.
$(\{+1, -1\}, \cdot)$ est un sous-groupe de $(U, \cdot)$ (U est l'ensemble des nombres complexes de module 1).
$(U, \cdot)$ est un sous-groupe de $(\mathbb{C} - \{0\}, \cdot)$.

Le résultat suivant est très simple à démontrer. C'est pourquoi nous en laissons la preuve au lecteur.

Théorème 2.2. *Si H est un sous-groupe de G, alors H, muni de l'opération de G, est un groupe.*

Définition. *Soient $(G, \cdot), (H, *)$ deux groupes.* **Un morphisme de groupes** *est une application $f : G \to H$ qui vérifie*

$$\forall x, y \in G, f(x \cdot y) = f(x) * f(y)$$

Important : Pour former $x \cdot y$, on utilise l'opération de G, et pour former $f(x) * f(y)$, celle de H.

Exemples.
1. L'application $\exp : \mathbb{R} \to \mathbb{R}_+^* : x \mapsto e^x$ est un morphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \cdot)$, car $e^{x+y} = e^x \cdot e^y$.
2. L'application $\mathbb{R}_+^* \to \mathbb{R} : x \mapsto \ln x$ est un morphisme de groupes de $(\mathbb{R}_+^*, \cdot)$ vers $(\mathbb{R}, +)$.

Définition.
Un isomorphisme de groupes *est un morphisme de groupes qui est bijectif.*
Un endomorphisme de groupe *est un morphisme d'un groupe vers le même groupe.*
Un automorphisme de groupe *est un endomorphisme de groupe qui est bijectif.*
Deux groupes G, H sont appelés **isomorphes** *s'il existe un isomorphisme de groupes de G vers H.*

Exemples.
1. L'application $\exp : \mathbb{R} \to \mathbb{R}_+^* : x \mapsto e^x$ est un isomorphisme de groupes de $(\mathbb{R}, +)$ vers $(\mathbb{R}_+^*, \cdot)$. Donc les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \cdot)$ sont isomorphes.
2. Si a est un entier, l'application $\mathbb{Z} \to \mathbb{Z} : n \mapsto an$ est un endomorphisme du groupe $(\mathbb{Z}, +)$.
C'est un automorphisme si et seulement si $a = \pm 1$.

Théorème 2.3. *Soit G un groupe, et x, y, z trois éléments quelconques de G.*
1. Si $xz = yz$, alors $x = y$.
2. Si $zx = zy$, alors $x = y$.

Preuve. 1. On suppose $xz = yz$. Mais alors $(xz)z^{-1} = (yz)z^{-1}$. Donc $x(zz^{-1}) = y(zz^{-1})$, ce qui donne $x = y$. Pour la partie 2. on procède de manière analogue. □.

Théorème 2.4. *Soit $f : G \to H$ un morphisme de groupes. Alors*
1. $f(e_G) = e_H$
2. $\forall x \in G, f(x^{-1}) = f(x)^{-1}$

Preuve.
1. On a $e_H f(e_G) = f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$, la dernière égalité étant vraie parce f est un morphisme. En vertu du théorème qui précède, on peut dire $e_H = f(e_G)$.
2. On part de $xx^{-1} = x^{-1}x = e_G$. Donc $f(xx^{-1}) = f(x^{-1}x) = f(e_G) = e_H$. Comme f est un morphisme, $f(x)f(x^{-1}) = f(x^{-1})f(x) = e_H$. On peut en déduire que $f(x^{-1})$ est l'inverse de $f(x)$.
□

1.6 Noyau et image d'un morphisme de groupes

Définition. *Soit $f : G \to H$ un morphisme de groupes.*
Le noyau de *f, noté* $\ker f$*, est l'ensemble des éléménts de G qui sont envoyés sur e_H.*
L'image de *f, notée Im f est l'ensemble des images des éléments de G par f.*

$$\ker f = \{x \in G | f(x) = e_H\} \subset G \qquad Im\ f = \{f(x) | x \in G\} \subset H$$

Dire que $y \in$ Im f est équivalent à : $y \in H$ et $\exists x \in G, f(x) = y$.

Théorème 2.5. *Soit $f : G \to H$ un morphisme de groupes.*
Alors $\ker f$ *est un sous-groupe de G et Im f est un sous-groupe de H.*

Preuve. Montrons d'abord que $\ker f$ est un sous-groupe de G.
L'élément neutre de G appartient au noyau, car $f(e_G) = e_H$.
Si x, y sont dans le noyau, alors $f(xy) = f(x)f(y) = e_H e_H = e_H$, donc xy est aussi dans le noyau.
Si x est dans le noyau, alors $f(x^{-1}) = f(x)^{-1} = e_H^{-1} = e_H$.
Nous avons bien montré que $\ker f$ est un sous-groupe de G.
Montrons maintenant que Im f est un sous-groupe de H.
L'élément neutre de H appartient dans l'image, car $e_H = f(e_G)$.
Si x, y sont dans l'image, alors on peut écrire $x = f(a), y = f(b)$, avec $a, b \in G$. Donc $xy = f(a)f(b) = f(ab)$, et comme $ab \in G$, on voit que xy est dans l'image.
Si x est dans l'image, alors $f(a) = x$ pour un certain a et alors $x^{-1} = f(a^{-1})$, ce qui achève la preuve. □

Si on a un morphisme de groupes entre deux groupes G et H, on construit donc facilement de nouveaux groupes en considérant le noyau et l'image de ce morphisme. On obtient un sous-groupe de G (le noyau) et un sous-groupe de H (l'image). En voici une application :

Théorème 2.6. *Pour tout $n \geqslant 1$, l'ensemble des racines n-èmes de l'unité, muni de la multiplication des nombres complexes, est un groupe commutatif.*

Rappel. Une racine n-ème de l'unité est un nombre complexe tel que $z^n = 1$.

Preuve. On sait que $(\mathbb{C}^* = \mathbb{C} - \{0\}, \cdot)$ est un groupe commutatif, d'élément neutre 1. L'application $f : \mathbb{C} \to \mathbb{C} : z \mapsto z^n$ est un endomorphisme du groupe $(\mathbb{C}^*, \cdot)$, car on a clairement $(zz')^n = z^n z'^n$. Donc le noyau de cet endomorphisme est un sous-groupe de $(\mathbb{C}^*, \cdot)$. Mais le noyau est exactement

l'ensemble des nombres complexes non nuls z tels que $z^n = 1$. C'est exactement l'ensemble des racines n-èmes de l'unité. C'est donc un sous-groupe de $(\mathbb{C}^*, \cdot)$. Donc, si on munit cet ensemble de la multiplication des nombres complexes, on obtient un groupe, qui est également commutatif, car il est sous-groupe d'un groupe commutatif. □

On note U_n le groupe des racines n-èmes de l'unité. Il possède exactement n éléments. Ce sont les nombres complexes z de la forme $z = e^{\frac{2\pi ik}{n}}$, avec $k \in \mathbb{Z}$. Bien entendu, si on remplace k par $k + n$, on obtient le même nombre complexe z, car $e^{2\pi i} = 1$.

2 Anneaux

2.1 Définition d'un anneau

Nous avons déjà vu que l'ensemble $\mathbb{Z}$, avec l'opération de somme, est un groupe commutatif. Mais sur les entiers, il y a une autre opération binaire interne, la multiplication. Elle a notamment les propriétés suivantes

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativité)
$a \cdot 1 = 1 \cdot a = a$ (neutre pour la multiplication)
$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ et
$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributivité de la multiplication par rapport à l'addition)

Nous rencontrerons souvent ce type de propriété avec deux lois binaires internes. Nous allons donner une définition très générale, qui correspond à des ensembles appelés **anneaux**.

Définition. *Soit A un ensemble muni de deux lois binaires internes, notées $+$ et $\cdot$*
On dit que $(A, +, \cdot)$ est **un anneau** *si les propriétés suivantes sont satisfaites :*
1. $(A, +)$ est un groupe commutatif
2. L'opération $\cdot$ est associative
3. Il existe un élément $m \in A$ tel que $\forall x \in A, x \cdot m = m \cdot x = x$
4. $\forall x, y, z \in A, x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ et $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Définition. *On dit qu'un anneau est* **commutatif** *si la loi $\cdot$ est commutative.*

Remarques.
1. Dans la notation mathématique, on décide que la deuxième opération (souvent appelée la multiplication) est **prioritaire** sur la première opération (souvent appelée l'addition). C'est pourquoi on peut écrire $x \cdot y + x \cdot z$ au lieu de $(x \cdot y) + (x \cdot z)$.
2. Comme pour les groupes, on montre que l'élément m tel que $m \cdot x = x \cdot m = x$ est unique. On l'appelle **le neutre pour la multiplication** $\cdot$

2.2 Exemples

$(\mathbb{Z}, +, \cdot)$ est un anneau commutatif. Il en est de même de $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$.

Il existe des exemples un peu plus étranges. Ainsi, si E est un ensemble, et $\mathcal{P}(E)$ l'ensemble des sous-ensembles de E, alors $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. L'opération Δ est la différence symétrique, et $\cap$ l'intersection. On pourra vérifier les détails. En particulier, on verra que l'élément neutre pour Δ est $\varnothing$, que l'inverse de $A \subset E$ pour Δ est A, et que l'élément neutre pour $\cap$ est E. Cet anneau est un anneau commutatif. Plus tard, nous verrons des exemples d'anneaux non commutatifs.

2.3 Premières propriétés

Théorème 2.7. *Soit $(A, +, \cdot)$ un anneau. On note 0 l'élément neutre de l'opération $+$, et on note $-x$ l'inverse de x pour cette même opération $+$.*
1. $\forall x \in A, \quad 0 \cdot x = x \cdot 0 = 0$
2. $\forall x, y \in A, \quad x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$

Preuve. 1. Par distributivité $x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Cela peut aussi s'écrire $x \cdot 0 + 0 = x \cdot 0 + x \cdot 0$. En ajoutant l'inverse (par rapport à la loi $+$) de $x \cdot 0$ on trouve $0 = x \cdot 0$. On prouve de la même manière que $0 = 0 \cdot x$.

2. On utilise $(-x)\cdot y + x\cdot y = (-x+x)\cdot y = 0$. □

Théorème 2.8. *Soit $(A,+,\cdot)$ un anneau, et $a_1,\dots,a_m$, $b_1,\dots,b_n$ des éléments de A.*
Si I est un ensemble fini, et $(x_i)_{i\in I}$ une famille d'éléments de A indexée par I, on note $\sum_{i\in I} x_i$ la somme (pour l'opération $+$ de A) de tous les éléments x_i. Comme $+$ est une opération commutative, l'ordre des termes n'a pas d'importance.
Alors on a la formule

$$\left(\sum_{i=1}^{m} a_i\right)\cdot\left(\sum_{j=1}^{n} b_j\right) = \sum_{(i,j)\in[[1,m]]\times[[1,n]]} a_i\cdot b_j$$

Puisque l'ordre dans la somme n'a pas d'importance, on peut aussi écrire

$$\left(\sum_{i=1}^{m} a_i\right)\cdot\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} a_i\cdot b_j\right)$$

et

$$\left(\sum_{i=1}^{m} a_i\right)\cdot\left(\sum_{j=1}^{n} b_j\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_i\cdot b_j\right)$$

Preuve. Utiliser la distributivité de l'anneau. □

2.4 Inversibles d'un anneau

Définition. *Soit $(A,+,\cdot)$ un anneau. On note 1 l'élément neutre pour $\cdot$.* **Un élément inversible de** *A est un élément $x\in A$ tel qu'il existe $y\in A$ avec $x\cdot y = y\cdot x = 1$.*

Exemples.
1. Dans l'anneau $\mathbb{Z}$, il y a exactement deux éléments inversibles, à savoir 1 et -1.
2. Dans l'anneau $(\mathcal{P}(E),\Delta,\cap)$, il y a un seul élément inversible, à savoir E.
3. Dans l'anneau $\mathbb{Q}$, tous les éléments différents de 0 sont inversibles.

Théorème 2.9. *Soit $(A,+,\cdot)$ un anneau.*
1. Le produit de deux éléments inversibles de A est un élément inversible de A.
2. L'opération $\cdot$ est une opération de groupe sur l'ensemble des éléments inversibles de A.

Preuve. 1. Soient x,x' deux éléments inversibles de A, alors il existe des éléments y,y' de A avec $xy = yx = x'y' = y'x' = 1$. Mais alors $(xx')(y'y) = 1$ et $(y'y)(xx') = 1$, donc xx' est bien inversible.
2. L'opération $\cdot$ est donc binaire interne sur l'ensemble des éléments inversibles. Il est ensuite très facile qu'il s'agit d'une opération de groupe sur cet ensemble. □

Définition. *Si A est un anneau, on appelle* **groupe des inversibles de** *A l'ensemble des éléments inversibles de A, muni de la deuxième opération de A. On note ce groupe A^o.*

Exemples.
1. $\mathbb{Z}^o = (\{+1,-1\},\cdot)$. Ce groupe est isomorphe à $(U_2,\cdot)$.
2. $\mathbb{Q}^o = (\mathbb{Q}^*,\cdot)$. De même $\mathbb{R}^o = (\mathbb{R}^*,\cdot)$.

2.5 Le binôme de Newton

Rappelons que le symbole C_n^k désigne le nombre $\dfrac{n!}{k!(n-k)!}$, où k,n sont deux entiers avec $0\leqslant k\leqslant n$.

Théorème 2.10. *Soient x,y deux éléments d'un anneau commutatif A et n un entier naturel. Alors*

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k} = y^n + nxy^{n-1} + \frac{n(n-1)}{2}x^2y^{n-2} + \cdots + nx^{n-1}y + x^n$$

Remarque. Le terme $C_n^k x^k y^{n-k}$ signifie qu'on additionne C_n^k fois l'élément $x^k y^{n-k}$ de l'anneau A (les entiers de $\mathbb{Z}$ ne font pas forcément partie de l'anneau A).

Preuve. Par récurrence sur n. Si $n = 0$, $(x+y)^n = (x+y)^0 = 1$ et $\displaystyle\sum_{k=0}^{0} C_n^k x^k y^{n-k} = C_0^0 x^0 y^0 = 1$, donc la propriété est vraie pour $n = 0$.
Supposons maintenant que la formule est vraie pour un entier donné n, et prouvons qu'alors elle est aussi vraie pour $n+1$. On peut donc dire que

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

Si on multiplie l'équation par $x+y$ on trouve

$$(x+y)^{n+1} = (x+y)\sum_{k=0}^{n} C_n^k x^k y^{n-k} = x(\sum_{k=0}^{n} C_n^k x^k y^{n-k}) + y(\sum_{k=0}^{n} C_n^k x^k y^{n-k})$$

On poursuit le calcul par les règles de distributivité

$$(x+y)^{n+1} = \sum_{k=0}^{n} x C_n^k x^k y^{n-k} + \sum_{k=0}^{n} y C_n^k x^k y^{n-k}$$

Comme on suppose que A est commutatif on a le droit d'écrire

$$(x+y)^{n+1} = \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^k y^{n+1-k}$$

Changeons de variable dans le premier terme

$$(x+y)^{n+1} = \sum_{k=1}^{n+1} C_n^{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} C_n^k x^k y^{n+1-k} = y^{n+1} + \sum_{k=1}^{n} (C_n^{k-1} + C_n^k) x^k y^{n+1-k} + x^{n+1}$$

Or on sait que $C_n^{k-1} + C_n^k = C_{n+1}^k$. D'où

$$(x+y)^{n+1} = y^{n+1} + \sum_{k=1}^{n} C_{n+1}^k x^k y^{n+1-k} + x^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}$$

Ceci démontre la propriété pour l'exposant $n+1$. La preuve par récurrence s'achève ici. □

Généralisation.
Dans la preuve, on a seulement utilisé que $xy = yx$. Donc on n'a pas besoin d'exiger que A soit commutatif, mais seulement que $xy = yx$ pour les deux éléments qui figurent dans la formule du binôme de Newton.

Corollaire 2.11. *Pour tout $n \geqslant 0$, on a $\displaystyle\sum_{k=0}^{n} C_n^k = 2^n$. Pour tout $n \geqslant 1$, on a $\displaystyle\sum_{k=0}^{n} (-1)^k C_n^k = 0$.*

Preuve. Pour la première relation, on applique le binôme de Newton avec $x = y = 1$. Pour la seconde, on prend $x = -1, y = 1$. □

2.6 Factorisation de $x^n - y^n$

Théorème 2.12. *Soient x, y deux éléments $(A, +, \cdot)$ un anneau commutatif (ou plus généralement deux éléments d'un anneau quelconque avec $x \cdot y = y \cdot x$). Alors pour tout entier $n \geqslant 1$, on a*

$$x^n - y^n = (x-y) \cdot \sum_{k=0}^{n-1} x^k y^{n-1-k}$$

Preuve.
Il suffit de développer le membre de droite par distributivité, appliquer $xy = yx$ et simplifier. □

Remarques.
1. La célèbre égalité $(x+y)(x-y) = x^2 - y^2$ est simplement le cas $n = 2$ du théorème ci-dessus.
2. Si $y = 1$, on trouve $x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$.

3 Corps

3.1 Définition et exemples

Définition.
Un corps *est un anneau* $(A, +, \cdot)$ *non réduit à* $\{0_A\}$ *dans lequel tout* $x \in A - \{0_A\}$ *est inversible.*
Un corps est donc un anneau A *pour lequel* $(A - \{0\}, \cdot)$ *est un groupe.*
On dit qu'un corps est **commutatif** *si la loi* $\cdot$ *est commutative.*

Exemples. Les anneaux $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sont tous les trois des corps commutatifs.
L'anneau $(\mathbb{Z}, +, \cdot)$ n'est pas un corps, car $2 \neq 0$ et 2 n'est pas inversible dans $\mathbb{Z}$, c'est-à-dire il n'existe pas d'entier n avec $2 \cdot n = n \cdot 2 = 1$.

Commentaire. Nous avons vu trois objets algébriques, d'abord les groupes, puis les anneaux et enfin les corps. Dans un groupe $(G, +)$ on peut «ajouter» et «soustraire» (faire $x + y$ et $x + (-y)$). Dans un anneau, on peut «ajouter», «soustraire» (comme dans un groupe) mais aussi «multiplier» (faire $x \cdot y$). Enfin, dans un corps, on peut «ajouter», «soustraire», «multiplier» et «diviser (par autre chose que 0)». La division de x par $y \neq 0$ dans un corps, c'est par définition $x \cdot y^{-1}$ (ou $y^{-1} \cdot x$), avec y^{-1} qui désigne l'inverse de y. Cet inverse existe précisément parce qu'on est dans un corps.

3.2 Sommes de progressions géométriques

Rappelons qu'une progression géométrique est une suite de nombres non nuls $a_0, a_1, \ldots$ telle que le rapport $\frac{a_{n+1}}{a_n}$ soit constant. Ce rapport est appelé **la raison de la progression géoémtrique**. Le résultat ci-dessous nous donne une formule pour des sommes d'un nombre fini de termes dans une progression géométrique. Nous allons l'énoncer dans un cadre très général, à savoir celui d'un corps quelconque.

Théorème 2.13. *Soit* K *un corps,* n *un entier* $\geqslant 1$ *et* $q \in K$ *avec* $q \neq 1_K$*. Alors*

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

Ici $(q-1)^{-1}$ *désigne l'inverse multiplicatif de* $q - 1$*, qui existe car* K *est un corps et* $q - 1 \neq 0$*.*

Remarque. Dans les corps usuels commutatifs, c'est-à-dire $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, on écrira évidemment $\frac{q^n - 1}{q - 1}$ au lieu de $(q^n - 1) \cdot (q - 1)^{-1}$.

Preuve. Comme K est un anneau, et que $q \cdot 1 = 1 \cdot q$, on peut appliquer le résultat de factorisation de $q^n - 1^n$. On aura

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

et aussi

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

Si on multiplie la première équation à gauche par $(q-1)^{-1}$, et la seconde équation à droite par $(q-1)^{-1}$, on obtient les résultats voulus. □

Application. Calculer $2^a + 2^{a+1} + \cdots + 2^b$, où a, b sont deux entiers de $\mathbb{Z}$ avec $a \leqslant b$.

On reconnaît une progression géométrique de raison 2. On peut écrire

$$2^a + 2^{a+1} + \cdots + 2^b = 2^a(2^0 + 2^1 + \cdots + 2^{b-a}) = 2^a \frac{2^{b-a+1} - 1}{2 - 1} = 2^{b+1} - 2^a$$

4 Vocabulaire du chapitre

Un groupe	abélien	l'image
un anneau	le groupe symétrique	prioritaire
un corps	un sous-groupe	inversible
un entier	un morphisme	le groupe des inversibles
une opération interne	un isomorphisme	le binôme de Newton
neutre	un automorphisme	une factorisation
inverse	un endomorphisme	une progression géométrique
le module	isomorphes	la raison
commutatif	le noyau	

5 Exercices

1. Soient a, b deux éléments quelconques d'un corps K. Résoudre dans K l'équation $ax + b = 0$ d'inconnue x. Résoudre dans K l'équation $xa + b = 0$.

2. Soit $n \geqslant 2$ et $\omega \in \mathbb{C} - \{1\}$ tel que $\omega^n = 1$. Combien y a-t-il de valeurs pour ω ? Calculer $1 + \omega + \omega^2 + \cdots + \omega^{n-1}$.

3. Soit G un groupe. On note
$$Z(G) = \{x \in G | \forall y \in G, xy = yx\}.$$
Montrer que $Z(G)$ est un sous-groupe de G. Que peut-on dire de G si on a l'égalité $Z(G) = G$?

4. Soit $(G, \times)$ un groupe fini. Montrer que pour tout $g \in G$, il existe un entier $n > 0$ tel que
$$g^n = \underbrace{g \times g \times \cdots \times g}_{n} = e.$$

5. Dans un anneau commutatif, calculer $(a + b + c)(-a + b + c)(a - b + c)(a + b - c)$.

6. Dans un anneau commutatif, factoriser $xy(y - x) + yz(z - y) + zx(x - z)$.

7. Dans un corps, montrer qu'on a l'implication
$$a_1 a_2 \cdots a_n = 0 \Rightarrow a_1 = 0 \text{ ou } a_2 = 0 \text{ ou } \cdots \text{ ou } a_n = 0.$$

8. Soit K un corps commutatif. On suppose que $a, b \in K$ et $x, y \in K - \{0\}$. Donner une écriture factorisée pour
$$a \cdot x^{-1} + b \cdot y^{-1}.$$

9. Soit K un corps commutatif et $x \in K - \{0_K, 1_K\}$ (x différent des deux neutres de K). Simplifier
$$\frac{1}{1 - \dfrac{1}{1 - \dfrac{1}{1 - x}}}.$$

10. Dans un corps non commutatif K, on prend a, b avec b non nul. Quel est le sens de l'écriture $\dfrac{a}{b}$?

11. Dans un anneau commutatif, calculer
$$(a - b)(a^2 + ab + b^2)(a^6 + a^3 b^3 + b^6)(a^{18} + a^9 b^9 + b^{18}).$$

12. Pourquoi le nombre de bijections de $[[1, n]]$ vers lui-même est-il égal à $n!$?

13. Montrer : S'il existe un isomorphisme de groupes $\varphi : G_1 \to G_2$, alors il existe aussi un isomorphisme de groupes $\psi : G_2 \to G_1$.