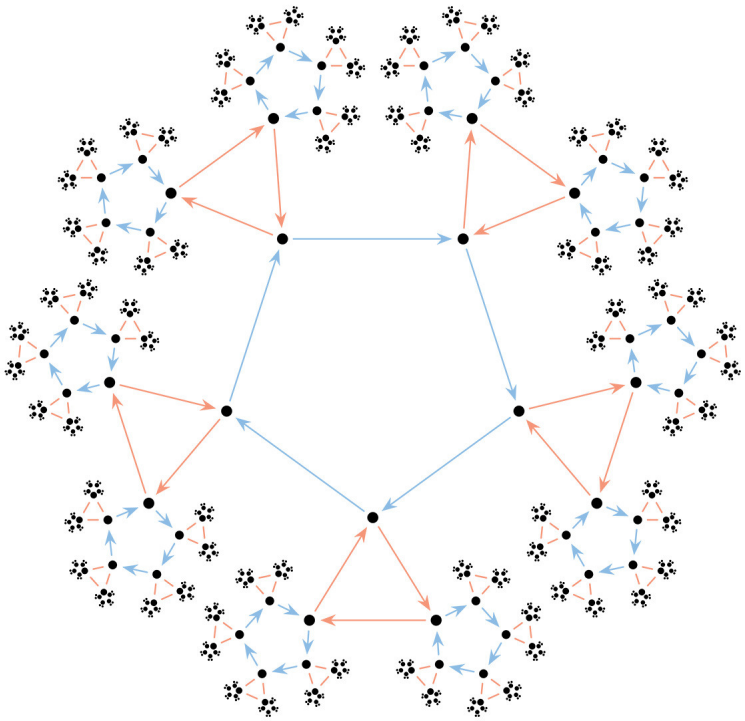
Algèbre I - Printemps 2019

David Cimasoni



$\mathrm{Cay}(G,S)$ où $G := < a, b \mid a^5,\ b^3 >$ et $S := \{a,\ b\}$

Contents

0 Introduction

L'algèbre classique c'est l'étude de la résolution d'équations:

$$x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 = 0$$

où x est l'inconnue: Une équation polynomiale de degré n.

$n = 1$: équation linéaire $x + a_0 = 0 \iff x = -a_0$

L'étude de la résolution d'un système d'équations linéaires est "l'algèbre linéaire", vu au 1er semestre

$n = 2$: équation quadratique

$$x^2 + a_1 x + a_0 = 0 \iff x = -\frac{a_1}{2} \pm \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}$$

Connue dès le IX ème siècle dans le traité "al-jabr" du savant perse al-Kwarizmi.

$n = 3$: équation cubique

$$x^3 + a_2 x^2 + a_1 x + a_0 = 0$$
$$x + \frac{a_2}{3} =: u \to u^3 + au = b$$
$$\implies u = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

del Ferro 1515, Cardeno 1545

$n = 4$ équation quartique, il existe aussi une solution comme en degrés $n \leq 3$

Conclusion

Pour $n \leq 4$, on peut écrire les solutions de l'équation polynomiale de degré n à partir des coefficients, via des additions, soustractions, multiplications, divisions, et racines: Cette équation est dite "résoluble par radicaux"

Question

Et en degré $n \geq 5$?

Réponse

- ⋆ Ruffini (1820), Abel (1826):
  L'équation générale de degré $n \geq 5$ n'est pas résoluble par radicaux.
- ⋆ Galois (1832):
  Caractérisation des équations résolubles par radicaux.

Ces résultats ont nécessité l'introduction d'outils d'un type nouveau: des "structures algébriques abstraites", dont l'étude est le sujet de ce cours.

Plan (grossier) du cours

Chapitre I	Groupes
Chapitre II	Anneaux et corps
Chapitre III	Algèbre linéaire

Vous verrez ces thèmes dans le cours d'Algèbre II ("Théorème de Galois")
Mais l'algèbre formel a une multitude d'autres application, par exemple, en:

- Topologie algébrique (voir cours "Géométrie et topologie", 3ème)
  - Pourquoi la sphère et le tore ne sont pas déformables l'un dans l'autre ?
  - Dans un polyèdre, (#sommets) - (#arrêtes) + (#faces) = 2
    (on verra une preuve au chapitre III)
- Géométrie élémentaire (Géométrie I + Algèbre II)
  - À la règle et au compas, il est impossible de trisecter un angle quelconque, dupliquer un cube, construire un cercle d'aire égale à l'aire d'un carré donné (quadrature du cercle)
  - le n-gone régulier est constructible à la règle et au compas $\iff$ la décomposition en premiers de n est de la forme:

    $$n = 2^n p_1 \dots p_r, \quad \text{avec} \quad p_i \neq p_j \quad \text{pour} \quad i \neq j, \quad \text{et les } p_i \text{ des premiers de la forme} \quad p = 2^{2^2} + 1$$

    Ce sont des "premiers de Fermat"

    par exemple:

    $$2^{2^0} + 1 = 3, \quad 2^{2^1} + 1 = 5, \quad 2^{2^2} + 1 = 17, \quad 2^{2^3} + 1 = 257, \quad 2^{2^4} + 1 = 63'537 \quad \text{, premiers}$$

- Théorie des nombres
  - Si p est premier et a est un entier non-divisible par p alors $a^{p-1} - 1$ est un multiple de p (petit théorème de Fermat, voir Chapitre I)
  - Il n'existe pas d'entiers non-nuls x, y, z tels que $x^n + y^n = z^n$ pour $n > 2$. (dernier théorème de Fermat, montré en 1994)

De manière générale, l'algèbre moderne s'enseigne dans un ordre anti-chronologique

Historiquement

$$\begin{array}{c}\text{problèmes}\\ \text{concrèts}\end{array} \quad \rightsquigarrow \quad \begin{array}{c}\text{tentatives de}\\ \text{résolution ,}\\ \text{essais et erreurs}\end{array} \quad \rightsquigarrow \quad \text{théorie formelle}$$

Pédagogiquement

$$\begin{array}{c}\text{théorie}\\ \text{formelle}\end{array} \quad \rightsquigarrow \quad \begin{array}{c}\text{applications à la résolution}\\ \text{des problèmes, comme}\\ \text{corollaires de la théorie}\end{array}$$

Conséquence

La théorie est assez aride et abstraite.

Un des buts

Entrainer la déduction logique, le raisonnement formel, la rédaction de preuves rigoureuses.

1 Groupes

La structure de groupe est simple (une loi, 3 axiomes), mais les concepts les plus importants sont déjà présents (sous-structures, homéomorphismes, quotients, produits, ...)

1.1 Groupes: axiomes et exemples

Définition

Soit G un ensemble muni d'une loi de composition, i.e. d'une application : $\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g*h \end{array}$

G est appelé un groupe s'il satisfait les axiomes suivants:

(G1) $g*(h*k) = (g*h)*k, \quad \forall g,h,k \in G$ (l'associativité)

(G2) $\exists e \in G \quad$ t.q. $e*g = g*e = g, \quad \forall g \in G$ (élément neutre)

(G3) $\forall g \in G$, $\exists g' \in G$ t.q. $g*g' = g'*g = e$ (inverse)

Si de plus, G satisfait:

$$g*h = h*g \quad \forall g,h \in G$$

alors le groupe G est dit abélien (ou commutatif). La cardinalité de G, notée $|G|$, est appelée l'ordre de G.

Remarques et notations

1. Formellement, un groupe est donc la donnée d'une paire $(G,*)$, avec G un ensemble et $*$ une loi de composition. Mais on le note habituellement G.
   De même, on notera habituellement $g*h =: gh$
   Dans le cas abélien, on notera souvent $g*h =: g+h$

2. $(G1)$ signifie que "l'on n'a pas à se soucier des parenthèses", par ex:

$$((g_1g_2)g_3)g_4 \overset{(G1)}{=} (g_1(g_2g_3))g_4 \overset{(G1)}{=} g_1((g_2g_3)g_4) \overset{(G1)}{=} g_1(g_2(g_3g_4))$$

   qu'on notera simplement $g_1g_2g_3g_4$.

3. L'élément neutre est unique.
   Preuve:
   en effet:
   Soient $e_1, e_2 \in G$ deux éléments neutres. Alors:

$$e_2 \underset{e_1 \text{ neutre}}{=} e_1 * e_2 \underset{e_2 \text{ neutre}}{=} e_1$$

   □

   On le note habituellement $e, e_G, 1, 1_G$, ou $0, 0_G$ dans le cas abélien.

4. L'égalité $g'g = e$ fait de g' un inverse-à-gauche de g et $gg'' = e$ fait de g'' un inverse-à-droite de g. Si les deux existent, alors ils coincident:
   Preuve:

$$g' \overset{(G2)}{=} g'e = g'(gg'') \overset{(G1)}{=} (g'g)g'' = eg'' \overset{(G2)}{=} g''$$

   □

Dans un groupe, (G3) stipule l'existence pour tout $g \in G$ d'un inverse (= inverse-à-gauche et inverse-à-droite). Il est donc unique!
On le note habituellement g^{-1}, ou $-g$ dans le cas abélien. On note aussi $g + (-h) =: g - h$.
On obtient donc $gg^{-1} = g^{-1}g = 1$, et $g - g = 0$ dans le cas abélien

5. Etant donné $g \in G$ et $n \in \mathbb{Z}$, la n-ème puissance de g est l'élément $g^n \in G$ défini par:

$$g^n := \begin{cases} \overbrace{g * g * \ldots * g}^{n} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ \underbrace{g^{-1} * \ldots * g^{-1}}_{|n|} & \text{si } n < 0 \end{cases}$$

On montre facilement les règles de calcul:

(i)

$$\begin{aligned} \forall x, g, h \in G, xg = xh &\implies g = h \\ \text{et} \quad gx = hx &\implies g = h \end{aligned}$$

(ii)

$$\forall g, h, \in G,\ (g^{-1})^{-1} = g \quad \text{et} \quad (gh)^{-1} = h^{-1}g^{-1}$$

(iii)

$$\forall g \in G,\ \forall n, m \in \mathbb{Z},\ g^n g^m = g^{n+m} \quad \text{et} \quad (g^n)^m = g^{nm}$$

6. Attention : Pour vérifier que $(G, *)$ est un groupe, il faut montrer $(G1), (G2), (G3)$, mais aussi vérifier que la loi est "interne"/"stable", i.e. $g, h \in G \implies g * h \in G$.
Par exemple: $G = \{-1, 0, 1\}$, muni de l'addition n'est pas stable. En effet $1 + 1 = 2 \notin G$

Exemples

1. $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ muni de l'addition "+"
est un groupe abélien d'ordre infini.
De même, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes abéliens d'ordre infini.
$\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ muni de la multiplication est un groupe abélien d'ordre infini, de même que $\mathbb{R}^*$, $\mathbb{C}^*$
Par contre, $\mathbb{N} := \{0, 1, 2, \ldots\}$ satisfait $(G1), (G2)$ (pour $+$), mais pas $(G3)$: ce n'est pas un groupe. (On parle de monoïde)

2. Si E est un $\mathbb{K}$-espace vectoriel ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$), alors $(E, +)$ est un groupe abélien:
Ce sont les axiomes $(A1) - (A4)$ d'un espace vectoriel.

3. Pour tout $n \geq 1$, l'ensemble $\mathrm{GL}(n, \mathbb{K}) := \{M \in M_n(\mathbb{K}) | \det M \neq 0\}$ est un groupe pour la multiplication matricielle, le groupe général linéaire de degré n sur $\mathbb{K}$
Démonstration:

Si $M_1, M_2 \in \mathrm{GL}(n, \mathbb{K})$, alors $\det(M_1 \cdot M_2) = \det M_1 \cdot \det M_2 \neq 0$
On a donc bien que $M_1 M_2 \in \mathrm{GL}(n, \mathbb{K})$.

(a)

$$M_1(M_2M_3) = (M_1M_2)M_3 \quad \forall M_1, M_2, M_3 \in M_n(\mathbb{K}) \ : \text{ vu en algèbre linéaire}$$

(b)

$$e = I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \ : \ I_n M = M I_n = M \quad \forall M \in M_n(\mathbb{K})$$

(c)

$$M \in \mathrm{GL}(n,\mathbb{K}) \implies \det M \neq 0 \implies \exists M^{-1} \text{ t.q. } MM^{-1} = M^{-1}M = I_n$$

De plus

$$1 = \det(I_n) = \det(M^{-1}M) = \ldots \implies \det(M^{-1}) \neq 0 \iff M^{-1} \in \mathrm{GL}(n,\mathbb{K})$$

Par exemple, pour $n = 1$, on obtient à nouveau $\mathrm{GL}(n,\mathbb{K}) = \mathbb{K}^*$ avec la multiplication.
Mais $\mathrm{GL}(n,\mathbb{K})$ n'est pas abélien pour $n > 1$

□

4. Dans le même genre: $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $n \geq 1$
   $\mathrm{SL}(n,\mathbb{K}) := \{M \in \mathrm{Mn}(\mathbb{K}) \mid \det M = 1\}$ est un groupe pour la multiplication matricielle : le groupe spécial linéaire de degré n sur $\mathbb{K}$.
   Par exemple, si $n = 1$, $\mathrm{SL}(1,\mathbb{K}) = \{(1)\}$: une des incarnations du groupe trivial

5. L'ensemble $S^1 := \{z \in \mathbb{C} \mid \|z\| = 1\}$ est un groupe abélien pour la multiplication complexe

6. Pour $n \geq 1$, l'ensemble des racines n-ème de l'unité

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\}$$

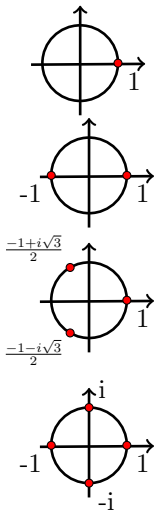
est un groupe abélien d'ordre n pour la multiplication complexe

$n = 1$ $\quad \mu_1(\mathbb{C}) = \{1\}$

$n = 2$ $\quad \mu_2(\mathbb{C}) = \{1, -1\}$

$n = 3$ $\quad \mu_3(\mathbb{C}) = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$

$n = 4$ $\quad \mu_4(\mathbb{C}) = \{1, i, -1, -i\}$



7. Soit X un ensemble non-vide quelconque, Posons:

$$S(X) := \{f : X \to X \mid f \text{ bijective}\}$$

C'est un groupe pour la composition des applications: le groupe symétrique sur X.

Démonstration:

$f, g : X \to X$ bijectives $\implies f \circ g$ est bijective : ✓
$f, g, h : X \to X$, $f \circ (g \circ h) = (f \circ g) \circ h$: ✓
$id_X : X \to X$ t.q. $id_X \circ f = f \circ id_X = f \quad \forall f : X \to X$: ✓
$f : X \to X$ bijective $\implies \exists g : X \to X$ t.q. $f \circ g = g \circ f = id_X$: ✓

□

Si $X = \{1, 2, \ldots, n\}$, alors $S(X)$ est noté S_n:
C'est le groupe des permutations de n objets.
Un élément $\sigma \in S_n$ est souvent noté $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Exemples

$n = 1 \quad S_1 = \{id\}$, le groupe trivial
$n = 2 \quad S_2 = \left\{ id, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$
$n = 3 \implies S_3$ n'est pas abélien

8. Si $(G_1, *)$ et $(G_2, \cdot)$ sont deux groupes, alors le produit castésien $G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}$ est un groupe pour $(g_1, g_2) \cdot (h_1, h_2) := (g_1 * h_1, g_2 \cdot h_2)$
C'est le produit direct de G_1 et G_2
Pluis généralement, pour $G_1, G_2, \ldots, G_n$ des groupes, le produit $G_1 \times G_2 \times \ldots \times G_n$ est un groupe pour la loi:

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) := (g_1 h_1, \ldots, g_n h_n)$$

Exemples

- $(\mathbb{R}^n, +)$ est le groupe donné par le produit direct de n copies de $(\mathbb{R}, +)$.
- $G := \{-1, 1\} \times \{-1, 1\}$ est appelé le groupe de Klein

$G_1 \times G_2$ est abélien $\iff$ G_1 et G_2 sont abéliens.

9. (moins formel, voir Géométrie I pour les détails)
Soit $P \subset \mathbb{R}^n$. Alors, l'ensemble:

$$\mathrm{Sym}(P) := \{\ f : \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ est une isométrie, } f(P) = P\}$$

est un groupe pour la composition des applications.
C'est le groupe des symétries de P dans $\mathbb{R}^n$.

Exemple

pour $n = 2$, les isométries du plan $\mathbb{R}^2$ sont des compositions de translations et de réflexions par des droites.

- $P =$  $\subset \mathbb{R}^2$, $\mathrm{Sym}(P) = \{id\}$, groupe trivial
- $P =$ une droite, $\mathrm{Sym}(P)$ contient en particulier toutes les translations parallèles à P

1.2 Sous-groupes

Définition

Soit G un groupe. Un sous-ensemble H de G est appelé sous-groupe de G, noté $H < G$, si H est un groupe pour la restriction de la loi de composition sur G.

Concrètement, il faut vérifier:

(1) $\forall h_1, h_2 \in H, \quad h_1 h_2 \in H$

(2) $e_G \in H$

(3) $\forall h \in H, \quad h^{-1} \in H$

Mais en fait, ces 3 conditions sont équivalentes à une seule:

Proposition I.1

Soit G un groupe, et $H \subset G$ un sous-ensemble non-vide.
Alors, H est un sous-groupe de $G \iff \forall h_1 h_2 \in H$, on a $h_1 h_2^{-1} \in H$

Preuve:
$[\implies]$:
Soit donc $h_1, h_2 \in H$. On a $h_2 \in H \overset{(3)}{\implies} h_2^{-1} \in H$
On a donc $h_1 \in H$, $h_2^{-1} \in H \overset{(1)}{\implies} h_1 h_2^{-1} \in H$.

$[\impliedby]$:
On a $H \neq \varnothing \implies \exists h \in H \implies hh^{-1} \in H \iff e \in H$ ((2) OK.)
Pour verifier (3), fixons $h \in H$, et appliquons l'hypothèse à $h_1 = e \in H$, $h_2 = h$. On a donc $e \cdot h^{-1} = h^{-1} \in H$, ce qui montre (3).
Pour verifier (1), fixons $h_1, h_2 \in H$; on sait que $h_2^{-1} \in H$. Par notre hypothèse, on a donc $h_1 (h_2^{-1})^{-1} = h_1 h_2 \in H$, ce qui montre (1), et conclut la preuve.

□

Exemples de sous-groupes

1. Tout groupe G admet $H = \{e\}$ et $H = G$ comme sous-groupe. Un sous-groupe de G qui n'est pas de cette forme est dit sous-groupe propre.
2. On a la chaine de sous-groupes (propres) suivante:
$$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$$
3. De même, on a:
$$(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$$
4. Si F est un sous-espace vectoriel d'un espace vectoriel E, alors $(F, +) < (E, +)$.
5. $\mathrm{SL}(n, k) < \mathrm{GL}(n, k)$
6. Pour tout n, $(\mu_n(\mathbb{C}), \cdot) < (S^1, \cdot)$
7. Pour $X \neq \varnothing$ un ensemble, et $A \subset X$ un sous-ensemble
$$\{f \in S(X) \mid f(A) = A\} \quad \text{et} \quad \{f \in S(X) \mid f(a) = a \, \forall a \in A\}$$
Sont des sous-groupes de $S(X)$.

8. Pour tout $n \in \mathbb{Z}$, le sous-ensemble $n\mathbb{Z} := \{n \cdot m \mid m \in \mathbb{Z}\}$ des multiples de n est un sous-groupe de $\mathbb{Z}$ (ex.1, S.2)

   Fait: ce sont les seuls

9. Soit G un groupe quelconque. Alors, $Z(G) := \{h \in G \mid gh = hg \; \forall g \in G\}$ est un sous-groupe de G, appelé le centre de G.

   Démonstration:
   Vérifions (1), (2), (3).

   (2) $\forall g \in G$, on a $ge = eg \, (= g) \implies e \in Z(G)$.

   (1) Soient $h_1, h_2 \in Z(G)$; on veut vérifier $h_1 h_2 \in Z(G)$: $\forall g \in G$, on a $g(h_1 h_2) = (gh_1)h_2 \overset{h_1 \in Z(G)}{=} (h_1 g)h_2 = h_1(gh_2) \overset{h_2 \in Z(G)}{=} h_1(h_2 g) = (h_1 h_2)g$.

   (3) Soit $h \in Z(G)$; on veut verifier que $h^{-1} \in Z(G)$.
   $\forall g \in G$, on a $gh = hg \implies h^{-1}(gh)h^{-1} = h^{-1}(hg)h^{-1}$
   $\implies h^{-1} \in Z(G)$

   □

10. Soit G un groupe quelconque, et $g \in G$ fixé, Alors $Z_G(g) := \{h \in G \mid gh = hg\}$ est un sous-groupe de G, le centralisateur de d dans G
    Par exemple, $Z_G(e) = G$. Notons que:
    $$Z(G) = \bigcap_{g \in G} Z_G(g)$$
    par définition.

Remarque

Pour G un groupe fixé, voici une méthode pour construire des sous-groupes.
Fixons $E \neq \varnothing$ un sous-ensemble de G, et posons

$$H = \langle E \rangle := \{g_1 g_2 \cdots g_n \in G \mid n \geq 1, \, \forall i \in \{1, \ldots, n\}, \, g_i \in E \text{ ou } g_i^{-1} \in E\} \cup \{e_G\}$$

C'est un sous-groupe de G, appelé le sous-groupe engendré par E. On dit que E est un système de générateurs de H.

Finalement, s'il existe $g \in G$ t.q. $G = \langle g \rangle$, alors on dit que G est un groupe cyclique. Cela signifie que tous les éléments de G sont de la forme g^n, $n \in \mathbb{Z}$.

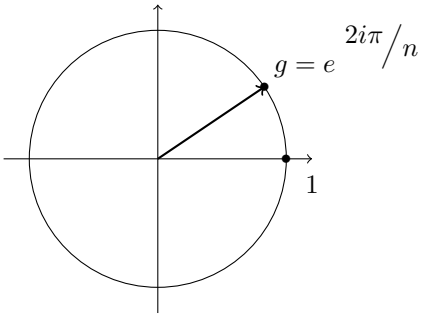
Exemples de groupes cycliques

1. $G = (\mathbb{Z}, +)$ est cyclique (d'ordre infini), engendré par $g = +1$. En effet, $\forall n \in \mathbb{Z}$, on peut écrire:

$$n = \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{n \text{ fois}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-1) + \cdots + (-1)}_{|n| \text{ fois}} & n < 0 \end{cases}$$

   (On peut aussi choisir $g = -1$)

2. $\forall n \geq 1, \quad G = \mu_n(\mathbb{C})$ est cyclique, engendré par $g = e^{2i\pi/n}$:



tout élément de $\mu_n(\mathbb{C})$ est de la forme $e^{2i\pi\frac{k}{n}} = g^k$

Terminologie: L'ordre de g

Soit $g \in G$. Alors $o(g) := |\langle g \rangle|$ est appelé l'ordre de $g \in G$
Ainsi:

- si $o(g) = \infty$, on a $g^n \neq e \quad \forall n \neq 0$
- si $o(g) = n < \infty$, cela signifie $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ et $g^n = e$
  Ainsi $o(g) = n$ est la plus petite puissance (positive) de g qui donne e.

Exemples

1. $o(g) = 1 \iff g = e$
2. Dans $G = (\mathbb{Z}, +)$, tout élément $m \neq 0$ a ordre $o(m) = \infty$
3. Dans $G = \mu_n(\mathbb{C})$, l'élément $g = \exp\left(\dfrac{2i\pi}{n}\right)$ a ordre $o(g) = n$
4. Dans $V = \{-1, 1\} \times \{-1, 1\}$, les 3 éléments $\neq (1, 1)$ ont ordre 2.

1.3 Homomorphismes de groupes

Définition

Une application $\varphi : G \to G'$ entre deux groupes est appelée un homomorphisme (de groupes) si:

$$\forall g_1, g_2 \in G, \quad \text{on a} \quad \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

Remarques

1. Il serait natuel de demander d'avoir aussi $\varphi(e_G) = e_{G'}$, et $\varphi(g^{-1}) = \varphi(g)^{-1} \quad \forall g \in G$ Ce sont en fait des conséquences de la définition.
   Preuve:

$$\varphi(e_G)\varphi(e_G) \overset{\varphi \text{ homo.}}{=} \varphi(e_G e_G) \overset{e_g \text{ neutre}}{=} \varphi(e_G) \overset{e_{G'} \text{ neutre}}{=} \varphi(e_G)e_{G'} \implies \varphi(e_G) = e_{G'}$$
$$\forall g \in G,\ \varphi(g)\varphi(g^{-1}) \overset{\varphi \text{ homo.}}{=} \varphi(gg^{-1}) = \varphi(e_G) \overset{\text{vu}}{=} e_{G'} \quad \text{de même} \quad \varphi(g^{-1})\varphi(g) = e_{G'}$$
$$\implies \varphi(g^{-1}) = \varphi(g)^{-1}$$

□

2. Si $\varphi : G \to G'$ et $\psi : G' \to G''$ sont des homomorphismes, alors $\psi \circ \varphi : G \to G''$ est aussi un homomorphisme
   Preuve:

$$\forall g_1, g_2 \in G,\ (\psi \circ \varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) \overset{\varphi \text{ homo.}}{=} \psi(\varphi(g_1)\varphi(g_2))$$
$$\underset{\psi \text{ homo.}}{=} \psi(\varphi(g_1))\psi(\varphi(g_1))\psi(\varphi(g_2)) = (\psi \circ \varphi)(g_1)(\psi \circ \varphi)(g_2)$$

□

Terminologie: Noyau et Image

Soit $\varphi : G \to G'$ un homomorphisme.
Son noyau est défini par $\text{Ker}(\varphi) := \{g \in G \mid \varphi(g) = e_G\} \subset G$
Son image est définie par $\text{Im}(\varphi) := \{\varphi(g) \mid g \in G\} \subset G'$

Proposition I.2

(i) $\text{Ker}(\varphi)$ est un sous-groupe de G, et $\text{Ker}(\varphi) = \{e_G\} \iff \varphi$ injectif.

(ii) $\text{Im}(\varphi)$ est un sous-groupe de G', et $\text{Im}(\varphi) = G' \iff \varphi$ surjectif.

Preuve:

(i) On a $\varphi(e_G) = e_{G'} \implies e_G \in \text{Ker}(\varphi)$, qui est donc non vide.
Pour vérifier que $\text{Ker}(\varphi) < G$, il suffit par Proposition I.1 de voir: $g_1, g_2 \in \text{Ker}(\varphi) \implies g_1 g_2^{-1} \in \text{Ker}(\varphi)$.
Soient donc $g_1, g_2 \in \text{Ker}(\varphi)$; calculons $\varphi(g_1 g_2) \overset{\text{homo.}}{=} \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_{G'}(e_{G'})^{-1}$
D'où : $g_1 g_2^{-1} \in \text{Ker}(\varphi)$

Montrons : $\text{Ker}(\varphi) = \{e_G\} \iff \varphi$ injectif

[$\Leftarrow$]: Supposons φ injectif, et montrons $\text{Ker}(\varphi) \subset \{e_G\}$ Soit donc $g \in \text{Ker}(\varphi)$;
on a : $\varphi(g) = e_{G'} = \varphi(e_G) \overset{\varphi \text{ inj.}}{\implies} g = e_G$

[⇒]: Supposons $\mathrm{Ker}(\varphi) = \{e_G\}$, et posons $g_1, g_2 \in G$ tels que $\varphi(g_1) = \varphi(g_2)$.
A voir: $g_1 = g_2$ (D'où φ injectif)
Calculons $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_1)^{-1} = e_G \implies g_1, g_2^{-1} \in \mathrm{Ker}(\varphi) = \{e_G\}$
On a donc $g_1 g_2^{-1} = e_G$, d'où $g_1 = g_2$

(ii) Exercice 5, Série 2.

□

Exemples d'homomorphismes

1. Pour tout groupe G, $id_G : G \to G$ est un homomorphisme ($\mathrm{Ker} = \{e\}$, $\mathrm{Im} = G$)
2. Pour tout sous-groupe $H < G$, l'inclusion $H \hookrightarrow G$ est un homomorphisme ($\mathrm{Ker} = \{e\}$, $\mathrm{Im} = H$)
3. Pour tous groupes G, G', on a l'homomorphisme : $\begin{array}{ccc} G & \longrightarrow & G' \\ g & \longmapsto & e_{G'} \end{array}$.
   C'est l'homomorphisme trivial. ($\mathrm{Ker} = G$, $\mathrm{Im} = \{e_{G'}\}$)
4. Soit G un groupe, et $g \in G$. Alors, l'application $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$ est un homomorphisme:
   $$\varphi(n+m) = g^{n+m} = g^n g^m = \varphi(n)\varphi(m)$$
   Par définition, $\mathrm{Im}(\varphi) = \langle g \rangle$, et $\mathrm{Ker}(\varphi) = \begin{cases} o(g)\mathbb{Z} & \text{si } o(g) < \infty \\ \{0\} & \text{si } o(g) = \infty \end{cases}$
5. Notons que $\mathbb{R}_+^* := (0, \infty)$ est un groupe pour la multiplication réelle.
   L'application : $\begin{array}{ccc} (\mathbb{C}^*, \cdot) & \longrightarrow & \mathbb{R}_+^* \\ z & \longmapsto & |z| \end{array}$ est un homomorphisme de noyau S^1, et d'image $\mathbb{R}_+^*$
6. $\det : \mathrm{GK}(n, \mathbb{K}) \to \mathbb{K}^*$ est un homomorphisme de noyau $\mathrm{SL}(n, \mathbb{K})$, et d'image $\mathbb{K}^*$
7. Une application linéaire $f : E \to E'$ est un homomorphisme de $(E, +)$ à $(E', +)$
8. L'application exponentielle $\varphi : \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}, \cdot) \\ x & \longmapsto & e^{ix} \end{array}$ est un homomorphisme (car: $e^{i(x+y)} = e^{ix}e^{iy}$) d'image S^1, et de noyau $2\pi\mathbb{Z} := \{2\pi k \mid k \in \mathbb{Z}\}$
9. Soit $m \in \mathbb{Z}$ ($m \neq 0$). Alors, la multiplication par m : $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & m \cdot n \end{array}$ est un homomorphisme (car $m(n_1 + n_2) = mn_1 + mn_2$), de noyau $\{0\}$ et d'image $m\mathbb{Z}$
10. L'application sgn : $\begin{array}{ccc} (\mathbb{R}^*, \cdot) & \longrightarrow & \{-1, 1\} \\ x & \longmapsto & \begin{cases} +1 & x > 0 \\ -1 & x < 0 \end{cases} \end{array}$
    est un homomorphisme, de noyau $\mathbb{R}_+^*$, et d'image $\{-1, 1\}$

Définition: Isomorphisme

Une homomorphisme $\varphi : G \to G'$ est appelé un isomorphisme s'il existe un homomorphisme $\psi : G' \to G$ tel que $\varphi \circ \psi = id_{G'}$ et $\psi \circ \varphi = id_G$
S'il existe un tel isomorphisme, on dit que G et G' sont isomorphes, noté $G \cong G'$

Remarques

1. Un homomorphisme $\varphi : G \to G'$ est un isomorphisme $\iff$ φ est un homomorphisme bijectif.
   Preuve:
   [$\Rightarrow$]: φ isomorphisme $\implies$ φ est un homomorphisme et $\exists \psi$ tel que $\varphi \circ \psi = id$ ($\implies$ φ surj.) et $\psi \circ \varphi = id$ ($\implies$ φ inj.), d'où φ bijectif
   [$\Leftarrow$]: Si φ est bijective, alors $\exists \psi : G' \to G$ telle que $\varphi \circ \psi = id$ et $\psi \circ \varphi = id$
   Reste à voir: ψ est un homomorphisme.
   En effet: soient $g'_1, g'_2 \in G'$: $\psi(g'_1 g'_2) = \psi(\varphi(\psi(g'_1)) \cdot \varphi(\psi(g'_2))) = \psi(\varphi(\psi(g'_1)\psi(g'_2)))$

   □

2. $$\left.\begin{array}{l} id_G : G \to G \quad \text{est un isomorphisme.} \\ \varphi : G \to G', \psi : G' \to G'' \quad \text{isos} \quad \implies \psi \circ \varphi : G \to G'' \quad \text{est un iso} \\ \varphi : G \to G' \quad \text{iso} \quad \implies \varphi^{-1} : G' \to G \quad \text{iso} \end{array}\right\} \begin{array}{l}\text{"est isomorphe"} \\ \text{est une relation d'équivalence}\end{array}$$

3. On a tendance à identifier 2 groupes isomorphes, de la même maniere qu'on identifie 2 ensembles en bijection en théorie des ensembles, et 2 espaces vectoriels isomorphes en algèbre linéaire.

4. Toutes les propriétés étudiées en théorie des groupes sont invarientes par isomorphisme, par exemple: si $G \cong G'$, alors $|G| = |G'|$, G abélien $\iff$ G' abélien, G a exactement 2 éléments d'ordre 3 $\iff$ G' a...

5. Pour montrer que G, G' sont isomorphes, il faut exhiber un isomorphisme $G \to G'$.
   Pour montrer que G, G' ne sont pas isomorphes, il faut trouver une propriété invariante que G possède mais que G' n'a pas.

Exemples d'isomorphismes

1. Tous les groupes d'ordre 1 sont isomorphes (c'est "le" groupe trivial)

2. Tous les groupes d'ordre 2 sont isomorphes (en particulier: $\mu_2(\mathbb{C}) \cong S_2$)
   Preuve:
   En effet, soit G un groupe d'ordre 2. Alors, on a $G = \{e, g\}$ avec $ee = e$, $eg = ge = g$, et $gg = e$ (inverse)
   (notation: $\begin{array}{c|cc} \cdot & e & g \\ \hline e & e & g \\ \hline g & g & e \end{array}$)
   Soient donc $G = \{e, g\}$, et $G' = \{e', g'\}$ 2 groupes. L'application $\varphi : \begin{array}{ccc} G & \longrightarrow & G' \\ e & \longmapsto & e' \\ g & & g' \end{array}$, est un isomorphisme.

   □

3. Tous les groupes d'ordre 3 sont isomorphes (Ex. 7, S.2)

4. Tous les groupes d'ordre 4 ne sont pas isomorphes:
   $\mu_4(\mathbb{C}) \ncong \{-1, 1\} \times \{-1, 1\} =: V$. En effet $i \in \mu_4(\mathbb{C})$ est d'ordre 4, alors que les éléments de V sont d'ordre 1 ou 2.

5. L'application $\varphi : \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & R_+^* \\ x & \longmapsto & e^x \end{array}$ est un isomorphisme (voir ex 9, S.2)

6. Si $f : X \to Y$ est une bijectoin, alors $\varphi : \begin{array}{ccc} S(X) & \longrightarrow & S(Y) \\ \sigma & \longmapsto & f \circ \sigma \circ f^{-1} \end{array}$ est un isomorphisme (Ex. 8, S.2)

Terminologie: Automorphisme

Un isomorphisme $\varphi : G \to G$ est appelé un automorphisme de G.

Remarque

L'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un groupe pour la composition des applications (par Remarque 2 ci-dessus)

Exemples d'automorphismes

1. Déterminons $\mathrm{Aut}(\mathbb{Z})$.
   Remarquons d'abord que tout homomorphisme $\varphi : \mathbb{Z} \to \mathbb{Z}$ est donné par la multiplication par $\varphi(1) \in \mathbb{Z}$
   En effet: pour $n > 0$, on a:

$$\varphi(n) = \varphi(\overbrace{1 + \cdots + 1}^{n}) \overset{\varphi\text{homo.}}{=} \overbrace{\varphi(1) + \cdots + \varphi(1)}^{n} = \varphi(1) \cdot n$$

   Pour $n = 0$: $\varphi(0) = 0 = \varphi(1) \cdot 0$
   Pour $n < 0$: $\varphi(n) = \varphi(\underbrace{(-1) + \cdots + (-1)}_{-n=|n|}) = (-n) \cdot \varphi(-1) = (-n)(-\varphi(1)) = \varphi(1)n$

   On a en fait: $(\mathrm{Homo}(\mathbb{Z}, \mathbb{Z}), \circ)$ est isomorphe à $(\mathbb{Z}, \cdot)$ comme monoïde via $\varphi \to \varphi(1) \in \mathbb{Z}$

   Ainsi, $\mathrm{Aut}(\mathbb{Z})$ est donné par les élements inversibles de $\mathrm{Homo}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$, c'est à dire, par $\{-1, 1\}$
   On a donc $\mathrm{Aut}(\mathbb{Z}) \cong \{-1, 1\}$

2. Pour G un groupe quelconque, et $g \in G$, l'application $\iota_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}$ est un automorphisme de G, appelé la <u>conjuaison par g</u>. ($\iota_g = id_G$ si G est abélien)

   <u>Démonstration:</u>

$$\forall x, y \in G,\ \iota_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right) = \iota_g(x)\iota_g(y)$$

   $\implies \iota_g$ est un homomorphisme

   De plus

$$\iota_{g'}(\iota_g(x)) = g^{-1}\left(gxg^{-1}\right)g = x \implies \iota_{g'} \circ \iota_g = id_G$$

   De même

$$\iota_g \circ \iota_{g'} = id_G \implies \iota_g \in \mathrm{Aut}(G)$$

   □

   De plus, l'application $\iota : \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \longmapsto & \iota_g \end{array}$ est un homomorphisme de noyau $Z(G)$. Son image, notée $\mathrm{Int}(G)$ est formée des <u>automorphismes intérieurs</u> de G.

   <u>Démonstration:</u>

   $\forall g, h \in G \quad \forall x \in G : \iota_g(\iota_h(x)) = g(h \times h^{-1})g^{-1} = (gh) \times (gh)^{-1} = \iota_{gh}(x) \implies \iota_g \circ \iota_h = \iota_{gh}$
   $g \in \mathrm{Ker}(\iota) \iff \iota_g = id_G \iff \iota_g(x) = x\ \forall x \in G \iff g \times g^{-1} = x\ \forall x \in G \iff gx = xg\ \forall x \in G \iff g \in Z(G)$

   □

1.4 Théorème de Lagrange, sous-groupe normaux et groupes quotients

Notations

Pour des sous-ensembels $X, Y \subset G$ et $g \in G$, on note.

$$gX := \{gx \mid x \in X\}, \quad Xg := \{xg \mid x \in X\}, \quad XY := \{xy \mid x \in X, y \in Y\}, \quad X^{-1} := \{x^{-1} \mid x \in G\}$$

Terminologie: Classe à gauche/droite

- Soit H un sous-groupe d'un groupe G.
  Un sous-ensemble de la forme gH (resp. Hg) est appelé une classe à gauche (resp. classe à droite) modulo H dans G.
- L'ensemble des classes à gauche (resp. droite) se note:

$$G/H := \{gH \mid g \in G\} \quad (\text{resp.} \quad H\backslash G := \{Hg \mid g \in G\})$$

- Le cardinal de G/H es appelé l'indice de H dans G, noté $[G : H]$

Remarque

L'application $G \to G, g \mapsto g^{-1}$ induit une bijection

$$f : G/H := \{gH \mid g \in G\} \to H\backslash G =: \{Hg \mid g \in G\}$$

Démonstration:
En effet : $f(gH) = (gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$ Cette application est bijective, d'inverse $Hg \mapsto g^{-1}H$

□

Ainsi $[G : H] \overset{\text{def.}}{:=} \left| G/H \right| = \left| H\backslash G \right|$.

Théorème de Lagrange

Si H est un sous-groupe d'un groupe fini G, alors $|G| = [G : H] \cdot |H|$

Preuve:
Soit G un groupe (quelconque), et $H < G$.
Pour $g_1, g_2 \in G$, notons $g_1 \sim g_2 :\iff g_2^{-1}g_1 \in H$
Verifions que c'est bien une relation d'équivalence sur G:

Réflexivité: $g \sim g \iff g^{-1}g \in H \iff e \in H$ ✓

Symétrie: $g_1 \sim g_2 \iff g_2^{-1}g_1 \in H \implies \left(g_2^{-1}g_1\right)^{-1} = g_1^{-1}g_2 \in H \overset{\text{déf.}}{\iff} g_2 \sim g_1$

Transitivité: $g_1 \sim g_2$ et $g_2 \sim g_3 \iff g_2^{-1}g_1 \in H$ et $g_3^{-1}g_2 \in H \implies \underbrace{\left(g_3^{-1}g_2\right)\left(g_2^{-1}g_1\right)}_{g_3^{-1}g_1} \in H \iff g_1 \sim g_3$

Les classes d'équivalences correspondantes sont:

$$[g]_H := \{g' \in G \mid g' \sim g\} = \{g' \in G \mid g^{-1}g' \in H\} = \{g' \in G \mid g' \in gH\} = gH, \quad \text{Les classes à gauche!}$$

Ainsi, les classes à gauche partitionnent G. Par définition, on a $[G : H]$ classes à gauche.

Finalement, $\forall g \in G$, on a une bijection : $\begin{array}{ccc} H & \longrightarrow & gH \\ h & \longmapsto & gh \end{array}$

$\ulcorner$

- surjectif par définition de gH
- injectif: $gh_1 = gh_2 \implies h_1 = h_2$: ✓

$\lrcorner$

Ainsi, G est partitionné en $[G : H]$ sous-ensembles, tous de cardinal $|H|$.

Donc, si G est fini, $|G| = [G : H] \cdot |H|$.

□

Corollaire I.3

Si $H < G$ fini, alors $|H|$ divise $|G|$ et $[G : H]$ divise $|G|$.

Corollaire I.4

Pour tout $g \in G$ avec G fini, $o(g)$ divise $|G|$.
Preuve:
Appliquer I.3 à $H = \langle g \rangle$

□

Corollaire I.5

Si G est un groupe d'ordre premier, alors G est un groupe cyclique, et tout $g \in G, g \neq e$ engendre G.

Preuve:
Soit donc G un groupe avec $|G|$ premier, et $g \in G, g \neq e$.

$$\left.\begin{array}{ll} g \neq e \iff & o(g) \geq 2 \\ \text{Par I.4,} & o(g) \mid |G| \end{array}\right\} \overset{|G| \text{ premier}}{\implies} \underset{=|\langle g \rangle|}{o(g)} \overset{\langle g \rangle \subset G}{\implies} \langle g \rangle = G$$

□

Corollaire I.6

Si G est fini, alors $g^{|G|} = e \qquad \forall g \in G$.

Preuve:
Pour tout $g \in G$, on a $o(g) \big| |G|$ par I.4, donc $\exists n \in \mathbb{Z}$ tel que $|G| = o(g) \cdot n$
On a donc $g^{|G|} = g^{o(g) \cdot n} = \left(g^{o(g)}\right)^n = e^n = e$

□

Remarque

On verra des conséquences de cet énoncé en théorie des nombres.

Exemples

1. Pour G fini quelconque, et $H = \{e\}$. Les classes à gauche sont $gH = \{g\}$, les élements de G.
   On a $[G : H] = |G|$, d'où $|G| = |G| \cdot 1$
2. Pour G fini quelconque, et $H = G$, les classes à gauche sont: $gH = gG = G$
   $\implies$ on a une unique classe à gauche, d'où $[G : G] = 1$; on a l'équation $|G| = 1 \cdot |G|$.
3. Pour $G = S_n$, posons $H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$. Calculons $[G : H]$ dans ce cas, en reprenant les notations de la preuve de Lagrange.
   Pour $\sigma_1, \sigma_2 \in S_n$, on a

   $$\sigma_1 \sim \sigma_2 \iff \sigma_2^{-1}\sigma_1 \in H \iff \sigma_2^{-1}(\sigma_1(n)) = n \iff \sigma_1(n) = \sigma_2(n) \in \{1, 2, \ldots, n\}$$

   Ainsi, le nombre de classes d'équivalence correspondantes (c'est à dire classes à gauche modulo H) est égal à $|\{1, 2, \ldots, n\}| = n$. On a donc $[G : H] = n$
   Par Lagrange, on obtient: $|S_n| = |G| = [G : H] \cdot |H| = n \cdots |S_{n-1}|$
   Par induction, on a: $|S_n| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$, comme il se doit.

Question

Quand la loi de composition dans G induit-elle une structure de groupe sur G/H ? (via $(g_1H) \cdot (g_2H) := g_1g_2H$, ou $[g_1]_H \cdot [g_2]_H := [g_1g_2]_H$)

Définition

Un sous-groupe $N < G$ est dit <u>normal</u> (ou <u>distingué</u>) dans G si: $\forall g \in G$, $gNg^{-1} = N$. Ceci est noté $N \triangleleft G$

Proposition I.7

Si $N \triangleleft G$, alors G/N est un groupe pour la loi : $\begin{array}{ccc} G/N \times G/N & \longrightarrow & G/N \\ (g_1N, g_2N) & \longmapsto & g_1g_2N \end{array}$.

De plus, la projection canonique $\pi : \begin{array}{ccc} G & \longrightarrow & G/N \\ g & \longmapsto & gN \end{array}$, est un homomorphisme surjectif, de noyau N.

<u>Preuve:</u>

- Vérifions que la loi de composition sur G/N est bien définie, ie. soient $g_1, h_1, g_2, h_2 \in G$ tels que $g_1N = h_1N$ et $g_2N = h_2N$.
  On veut voir: $g_1g_2N = h_1h_2N$

  $$\left.\begin{array}{l} g_1N = h_1N \iff h_1^{-1}g_1 \in N \overset{N \triangleleft G}{\implies} g_2^{-1}\left(h_1^{-1}g_1\right)g_2 \in N \\ g_2N = h_2N \iff h_2^{-1}g_2 \in N \end{array}\right\} h_2^{-1}\underbrace{g_2g_2^{-1}}_{=e}h_1^{-1}g_1g_2 \in N$$

  $$\iff (h_1h_2)^{-1}g_1g_2 \in N \iff h_1h_2N = g_1g_2N$$

- L'associativité découle de celle dans G
  Le neutre est $e_{G/N} = [e]_N = eN = N$
  L'inverse de gN est $g^{-1}N$
  $\Big\}$ G/N est un groupe.

- Par définition, $\pi(g_1g_2) = g_1g_2N = (g_1N)(g_2N) = \pi(g_1)\pi(g_2)$: c'est un homomorphisme, π est surjectif par définition de ${}^{G}\!/_{N}$.
  Et:

$$\mathrm{Ker}(\pi) = \{g \in G \mid \pi(g) = e_{G/N}\} = \{g \in G \,:\, gN = N\} = \{g \in G \mid g \sim_N e\} = \{g \in G \mid e^{-1}g \in N\} = N$$

□

Terminologie: Groupe quotient

${}^{G}\!/_{N}$ est appelé le groupe quotient (de G par N).

Remarques

1. $N \triangleleft G \overset{\text{déf}}{\iff} \forall g \in G,\ gNg^{-1} = N \iff \forall g \in G,\ gN = Ng \iff$ les classes à gauche et à droite coïncident.
2. $N \triangleleft G \iff \forall g \in G,\ \forall x \in N$, on a $gxg^{-1} \in N$

   Démonstration:
   $[\implies]$: ✓

   $[\impliedby]$: on a $\forall g \in G \quad gNg^{-1} \subset N$; appliquons à $g^{-1} \in G \,:\, g^{-1}Ng \subset N \iff N \subset gNg^{-1}$ On a donc bien $gNg^{-1} = N \quad \forall g \in G$, donc $N \triangleleft G$

□

Exemples de sous-groupes normaux

1. On a toujours $N = \{e\} \triangleleft G$ ($\forall g \in G$, on a $geg^{-1} = e \in N$)
2. On a toujours $N = G \triangleleft G$ ($\forall g, x \in G$, on a $gxg^{-1} \in G$)
3. Si G est abélien, alors tout sous-groupe est normal. ($\forall g \in G, \forall x \in N$, on a $gxg^{-1} = gg^{-1}x = x \in N$)
4. On a $Z(G) \triangleleft G$ (même preuve)
5. Si $\varphi : G \to G'$ est un homomorphisme, alors $\mathrm{Ker}(\varphi) \triangleleft G$.
   Démonstration:
   Soit donc $x \in \mathrm{Ker}(\varphi)$ et $g \in G$, à voir: $gxg^{-1} \in \mathrm{Ker}(\varphi)$

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$$

□

6. $\mathrm{SL}(n, \mathbb{K}) \triangleleft \mathrm{GL}(n, \mathbb{K})$ (car $\mathrm{SL}(n, \mathbb{K}) = \mathrm{Ker}(\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K}^*)$)
7. Pour tout groupe G, $\mathrm{Int}(G) \triangleleft \mathrm{AUT}(G)$
8. Tout sous-groupe d'indice 2 est normal.
   Démonstration:
   Soit $H < G$ avec $2 = [G : H] = \left| {}^{G}\!/_{H} \right| = \left| {}_{H}\backslash^{G} \right| \implies$ on a les partitions:

$$G = H \sqcup gH \quad (g \notin H), \quad \text{et} \quad G = H \sqcup Hg \quad (g \notin H)$$

   $$\left.\begin{array}{l} \text{On a donc que } gH = Hg \quad \forall g \notin H \\ \text{Pour } g \in H, \quad \text{on a} \quad gH = Hg = H \end{array}\right\} \implies \forall g \in G,\ gH = Hg \iff H \triangleleft G$$

□

9. Dans $G = S_3$, posons $H = \left\{ id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$. Alors $H \not\lhd G$.

   En effet, pour $x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in H$ et $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, on a:

$$gxg^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$$

Définition: Groupe simple

Un groupe est dit simple s'il n'a pas de sous-groupe normal propre (ie. $N \neq \{e\}, G$)

Exemple

Si G est d'ordre premier, alors G est simple (par Lagrange). (Nous verrons que ce sont les seuls groupes simples abéliens)

Proposition I.8

Soit G un groupe $N \lhd G$, et $\varphi : G \to G'$ un homomorphisme tel que $N \subset \mathrm{Ker}(\varphi)$
Alors, il existe un unique homomorphisme $\overline{\varphi} : {}^{G}\!/_{N} \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$.

Terminologie

- Un tel énoncé est une "propriété universelle".
- On dit que "φ passe au quotient"

Preuve:

- $\overline{\varphi}$ est unique: $\overline{\varphi}(gN) = \overline{\varphi}(\pi(g)) = (\overline{\varphi} \circ \pi)(g) = \varphi(g)$
  (En notations $[g]_N$, on a: $\overline{\varphi}([g]_N) = \varphi(g)$)

- $\overline{\varphi}$ est bien définie (ie: existe): soient $g_1, g_2 \in G$ tels que $g_1 N = g_2 N$

$$\iff g_2^{-1} g_1 \in N \overset{\text{hypo.}}{\subset} \mathrm{Ker}(\varphi) \implies e = \varphi(g_2^{-1} g_1) = \varphi(g_2)^{-1} \varphi(g_1) \iff \varphi(g_2) = \varphi(g_1)$$

  Ainsi, $\overline{\varphi}$ est bien défini.

- $\overline{\varphi}$ homomorphisme:

$$\overline{\varphi}((g_1 N)(g_2 N)) = \overline{\varphi}(g_1 g_2 N) \overset{\text{def } \overline{\varphi}}{=} \varphi(g_1 g_2) \overset{\varphi \text{ homo.}}{=} \varphi(g_1)\varphi(g_2) \overset{\text{def } \overline{\varphi}}{=} \overline{\varphi}(g_1 N)\overline{\varphi}(g_2 N)$$

□

Proposition I.9

Soit $\varphi : G \to G'$ un homomorphisme. Alors φ définit un isomorphisme $\overline{\varphi} : {}^{G}\!/_{\operatorname{Ker}\varphi} \to \operatorname{Im}(\varphi)$:

Preuve:
Soit donc $\varphi : G \to G'$ un homomorphisme. Comme $\operatorname{Ker}(\varphi) \triangleleft G$, on va appliquer I.8 à $N := \operatorname{Ker}(\varphi)$
Comme $N = \operatorname{Ker}(\varphi)$, on a bien $N \subset \operatorname{Ker}(\varphi)$, et on peut appliquer I.8, d'où: $\exists$ homo $\overline{\varphi} : {}^{G}\!/_{\operatorname{Ker}(\varphi)} \to G'$ tel que $\overline{\varphi} \circ \pi = \varphi$

- Notons que $\operatorname{Im}(\varphi) = \operatorname{Im}(\overline{\varphi} \circ \pi) \overset{\pi \text{ surj.}}{=} \operatorname{Im}(\overline{\varphi})$.
  D'où $\overline{\varphi} : {}^{G}\!/_{\operatorname{Ker}(\varphi)} \to \operatorname{Im}(\varphi)$ est un homomorphisme surjectif.
- Reste à voir: $\overline{\varphi}$ est injectif.
  Soit donc $gN \in \operatorname{Ker}(\overline{\varphi}) \iff e_{G'} = \overline{\varphi}(gN) = \overline{\varphi}(\pi(g)) = \varphi(g) \iff g \in \operatorname{Ker}(\varphi) = N \iff gN = N = e_{G/N}$
  On a donc $\operatorname{Ker}(\overline{\varphi}) = \{e_{G/N}\}$, d'où $\overline{\varphi}$ injective par I.1.

□

Intuitivement

- On rend φ surjective en restreignant l'image.
- On rend φ injective en "tuant" $\operatorname{Ker}\varphi = N$.

Exemples

1. L'homomorphisme trivial : $\begin{array}{ccc} G & \longrightarrow & G' \\ g & \longmapsto & e_{G'} \end{array}$ induit l'isomorphisme ${}^{G}\!/_{G} \cong \{e\}$
2. L'homomorphisme $id_G : G \to G$ induit l'isomorphisme ${}^{G}\!/_{\{e\}} \cong G$
3. L'homomorphisme det : $\operatorname{GL}(n,\mathbb{K}) \to \mathbb{K}^*$ induit l'isomorphisme ${}^{\operatorname{GL}(n,\mathbb{K})}\!/_{\operatorname{SL}(n,\mathbb{K})} \cong \mathbb{K}^*$
4. L'homomorphisme $\varphi : \begin{array}{ccc} (\mathbb{C},+) & \longrightarrow & (\mathbb{C}^*,\cdot) \\ z & \longmapsto & e^{2\pi i z} \end{array}$ a image $\mathbb{C}^*$ et noyau $\mathbb{Z}$, d'où l'isomorphisme: ${}^{\mathbb{C}}\!/_{\mathbb{Z}} \cong \mathbb{C}^*$
   La restriction de φ à $(\mathbb{R},+)$ a image $(S^1,\cdot)$ et noyau $\mathbb{Z}$, d'où: ${}^{\mathbb{R}}\!/_{\mathbb{Z}} \cong S^1$
5. L'homomorphisme $\iota : G \to \operatorname{Aut}(G)$ a image $\operatorname{Int}(G)$ et noyau $Z(G)$, d'où l'isomorphisme ${}^{G}\!/_{Z(G)} \cong \operatorname{Int}(G)$

1.5 Groupes cycliques

Considérons l'exemple de $G = (\mathbb{Z}, +)$.
Pour tout $n \in \mathbb{N}$, on a le sous-groupe $H = n\mathbb{Z} = \{\ldots, -2n, n, 0, n, 2n, \ldots\}$
La partition de $\mathbb{Z}$ en classes modulo H est $\mathbb{Z} = n\mathbb{Z} \sqcup (1 + n\mathbb{Z}) \sqcup (2 + n\mathbb{Z}) \sqcup \ldots \sqcup ((n-1) + n\mathbb{Z})$
$H \triangleleft \mathbb{Z}$ car $\mathbb{Z}$ est abélien.

$$\mathbb{Z}/H \;=\; \mathbb{Z}/n\mathbb{Z} \;= \{[0], [1], [2], \ldots, [n-1]\},\ n \text{ classes d'équivalences}$$

pour la relation: $[a] = [b] \iff a - b \in n\mathbb{Z} \overset{\text{not.}}{\iff} a \equiv b \pmod{n}$, a congrue à b modulo n.

$\mathbb{Z}/n\mathbb{Z}$ est appelé le roupe des entiers modulo n.
La loi: $[a] + [b] = [a + b]$, rete de la division par n.

Par exemple pour $n = 2$, on a $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$, avec la loi donnée par la table

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Pour $n = 3$, on $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$ et

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Notons que $\mathbb{Z}/n\mathbb{Z}$ est cyclique pour tout $n \in \mathbb{Z}$.

En effet :

- si $n = 0$, $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, infini cyclique engendré par 1
- si $n > 0$, $\mathbb{Z}/n\mathbb{Z}$ est engendré par $[1]$, car $[i] = \underbrace{[1] + \cdots + [1]}_{i \text{ fois}}$

On verra : tout G cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$! Pour cela on a besoin

Proposition I.10

Soit H un sous-groupe de $\mathbb{Z}$. Alors, il existe un unique $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ tel que $H = n\mathbb{Z}$.

Preuve:
Soit $H < \mathbb{Z}$. Si $H = \{0\}$, alors $H = o\mathbb{Z}$, trivial.
Supposons donc $H \neq \{0\}$. Dans ce cas, on a $H \cap \{1, 2, 3, \ldots\} \neq \varnothing$, car $h \in H \implies -h \in H$
Soit n le plus petit élément de $H \cap \{1, 2, \ldots\}$.

Affirmation : $H = n\mathbb{Z}$

En effet : $[\supset]$: $n \in H \overset{H \text{ groupe}}{\Longrightarrow} n\mathbb{Z} = \{\ldots, -n-n, -n, 0, n, n+n, \ldots\} \subset H$.

$[\subset]$: Soit $h \in H \subset \mathbb{Z}$. A voir : h est un multiple de n.
Par l'algorithme de division euclidienne: $\exists q \in \mathbb{Z}, r$ avec $0 \leq r < n$ tel que $h = qn + r$. $H < \mathbb{Z}, h \in H, n \in H \implies r = h - qn \in H$. Si $r > 0$, alors $r \in H \cap \{1, 2, \ldots\}$, impossible par minimalité de n (et $r < n$). Ainsi on a $r = 0$, d'où $h = qn \in n\mathbb{Z}$

Finalement, n est unique car $| \ {}^{\mathbb{Z}}\!/_{H} \ | = | \ {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ | = \begin{cases} n & \text{si } n > 0 \\ \infty & \text{si } n = 0 \end{cases}$ donc impossible d'avoir $H = n\mathbb{Z} = m\mathbb{Z}$ avec $n \neq m$

□

Théorème I.11: Classification des groupes cycliques

Soit G est un groupe cyclique.
Si G est infini, alors $G \cong \mathbb{Z}$. Sinon, $G \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ avec $n = |G|$.

Preuve:
Soit donc G un groupe cyclique. Par définition, il existe $g \in G$ tel que $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Cela signifie que l'homomorphisme $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & g^k \end{array}$ est surjectif.
Considérons $H = \operatorname{Ker} \varphi < \mathbb{Z}$. Par I.10, $\exists n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

- Si $n = 0$, on a $\operatorname{Ker} \varphi = 0\mathbb{Z} = \{0\} \iff \varphi$ injective $\implies \varphi$ iso $\implies G \cong \mathbb{Z}$.
- Si $n > 0$, on a $\operatorname{Ker} \varphi = n\mathbb{Z}$, d'où un isomorphisme $\overline{\varphi} : {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \to G$ par I.9, d'où $G \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Finalement $|G| = | \ {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ | = n$.

□

Exemple

$$\mu_n(\mathbb{C}) \cong {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ , \quad \text{via} \quad \exp\left(\frac{2i\pi k}{n}\right) \longleftrightarrow [k]$$

Voyons une application à la théorie des nombres (petit théorème de Fermat). Quelques rappels:

Terminologie

- Pour $a, b \in \mathbb{Z}$, on dit que $\underline{a \text{ divise } b}$, noté $a \mid b$, si $\exists q \in \mathbb{Z}$ tel que $aq = b$.
- Pour $u, v \in \mathbb{Z}$, le $\underline{\text{plus grand commun diviseur}}$ de u et v, noté $\text{pgcd}(u, v)$, est défini par:

$$\text{pgcd}(u, v) := \begin{cases} 0 & \text{si } u = v = 0 \\ \max\{n \in \mathbb{N} \mid n|u \text{ et } n|v\} & \text{sinon} \end{cases}$$

- Deux entiers $u, v \in \mathbb{Z}$ sont dits $\underline{\text{premiers entre eux}}$ si $\text{pgcd}(u, v) = 1$

Proposition I.12

Pour $u, v \in \mathbb{Z}$, $\{un + vm \mid n, m \in \mathbb{Z}\} = \text{pgcd}(u, v)\mathbb{Z}$.

Preuve:
Soient donc $u, v \in \mathbb{Z}$
Le sous-ensemble $H := \{un + vm \mid n, m \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

$\ulcorner$

$H \ni u \cdot 0 + v \cdot 0 = 0 \implies H \neq \varnothing$

$h_1 = un_1 + vm_1 \quad (n_1, m_1, n_2, m_2 \in \mathbb{Z}) \implies h_1 - h_2 = u(\overbrace{n_1 - n_2}^{\in\mathbb{Z}}) + v(\overbrace{m_1 - m_2}^{\in\mathbb{Z}}) \in H$

$h_2 = un_2 + vm_2$

$\lrcorner$

Par I.10, $\exists k \in \mathbb{N}$ tel que $H = k\mathbb{Z}$. A voir: $k = \text{pgcd}(u, v) =: j$.
Comme $u, v \in H = k\mathbb{Z}$, on a $k|u$ et $k|v \overset{\text{déf. de pgcd}}{\implies} 0 \leq k \leq j$.
D'autre part, $j|u$ et $j|v \implies u$ et v sont des multiples de j.
$\implies$ tout élément de H est un multiple de $j \overset{k \in H}{\implies} k$ est un multiple de j.
$\implies j \leq k \implies j = k$.

$\square$

Théorème de Bézout

Deux entiers $u, v \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe $m, n \in \mathbb{Z}$ tels que $um + vm = 1$

Preuve:
Par I.12, u, v premiers entre eux $\iff \{un + vm \mid n, m \in \mathbb{Z}\} = \mathbb{Z} \iff \{un + vm \mid n, m \in \mathbb{Z}\} \ni 1$

$\square$

Revenons à $\mathbb{Z}/n\mathbb{Z}$, avec $n > 0$.

Notation: $\left(\mathbb{Z}/n\mathbb{Z}\right)^* := \left\{[m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \text{pgcd}(m,n) = 1\right\}$
Sur $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, définissons $[m_1] \cdot [m_2] = [m_1 \cdot m_2]$

Affirmation : $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est un groupe pour la multiplication ci-dessus.

Preuve:
Notons d'abord que $\text{pgcd}(m_1, n) = \text{pgcd}(m_2, n) = 1 \implies \text{pgcd}(m_1 \cdot m_2, n) = 1$
De plus, si $[m_1] = [m_1']$, alors $m_1' = m_1 + k_1 n \implies m_1' m_2' = m_1 m_2 + (k_1 + k_2 + k_1 k_2 n)n$. De même pour $[m_2] = [m_2']$ ce qui implique $[m_1' m_2'] = [m_1 m_2]$

Ainsi, la loi est interne et bien définie. Elle est clairement associative le neutre est $[1] \in \mathbb{Z}/n\mathbb{Z}$

Reste à voir : inverse.
Soit $[m] \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$. Par Bézout, $\exists x, y \in \mathbb{Z}$ tels que $mx + ny = 1 \in \mathbb{Z}$

$$\implies [1] = [mx] + \underbrace{[ny]}_{=0} = [m][x] \implies \quad m \text{ a comme inverse } [x]$$

Finalement, $mx + ny = 1 \underset{\text{Bézout}}{\implies} x$ et n sont premiers entre eux $\iff [x] \in \left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

□

Notation

Pour $n \in \{1, 2, 3, \ldots\}$, notons $\varphi(n) := \#\{m \in \{1, 2, 3, \ldots, n\} \mid \text{pgcd}(m, n) = 1\}$, la fonction φ d'Euler.
Par exemple, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4, \ldots$.
Pour p premier, $\varphi(p) = p - 1$.

Corollaire I.12

Soient $n \geq 1$ un entier, et $a \in \mathbb{Z}$ tel que a et n sont premiers entre eux. Alors, $a^{\varphi(n)} - 1$ est un multiple de n.

Preuve:
Fixons donc $n \geq 1$, et $a \in \mathbb{Z}$. Par hypothèse, on a $[a] \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* =: G$. Le groupe G a ordre $|G| = \varphi(n)$.
Par Corollaire I.6, on a: $g^{|G|} = e_G$, ie:

$$[1] = [a]^{\varphi(n)} = [a^{\varphi(n)}] \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \subset \mathbb{Z}/n\mathbb{Z} \iff a^{\varphi(n)} - 1 \in n\mathbb{Z}$$

□

Petit théorème de Fermat

Soit p un premier et a un entier qui n'est pas un multiple de p. Alors, $a^{p-1} - 1$ est un multiple de p.

Preuve:
C'est le Corollaire I.12 dans le cas $n = p$.

□

Exemples

- $p = 2$: a impair $\implies$ $a - 1$ pair.
- $p = 3$: a pas multiple de 3 $\implies$ $a^2 - 1$ est multiple de 3.

$\ulcorner$

$$a = 3k + i,\ i \in \{1, 2\} \implies a^2 - 1 = \underbrace{9k^2 + 6ki}_{\text{mult. de 3}} + \underbrace{i^2 - 1}_{\in\{0,3\}} \quad \text{un multiple de 3}$$

$\lrcorner$

1.6 Commutateurs, abélianisé, groupes résolubles

Terminologie

Soit G un goupe, et $g, h \in G$.
Le commutateur de g et h est $[g,h] := ghg^{-1}h^{-1} \in G$.

Remarques

1. $[g,h] = e \iff ghg^{-1}h^{-1} = e \iff gh = hg \iff g$ et h commutent.
   En particulier, G est abélien $\iff [g,h] = e \quad \forall g, h \in G$

2. Si $\varphi : G \to G'$ est un homomorphisme, alors $\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$

3. $[g,h]^{-1} = \left(ghg^{-1}h^{-1}\right)^{-1} = hgh^{-1}g^{-1} = [h,g]$

4. $[e,g] = [g,e] = e \quad \forall g \in G$

5. Mais le produit de deux commutateur n'est en général pas un commutateur!
   On définit donc:

   Terminologie

   Soit G un groupe. Le groupe dérivé de G est le sous-groupe de G engendré par les commutateurs:

   $$[G,G] := \langle \{[g,h] \mid g, h \in G\} \rangle < G$$

6. Par la remarque 3, tout élément de $[G,G]$ est produit de commutateur.

7. Par la remarque 2, si $\varphi : G \to G'$ est un homomorphisme, $\varphi([G,G]) \subset [\varphi(G), \varphi(G)]$

Exemples

1. G abélien $\iff [G,G] = \{e\}$, par remarque 1.

2. Pour $G = S_3$, on a $[S_3, S_3]$ est le sous-groupe (d'ordre 3) de S_3 engendré par $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

3. Pour $n \geq 1$ on a $[\mathrm{GL}(n,\mathbb{K}), \mathrm{GL}(n,\mathbb{K})] = \mathrm{SL}(n,\mathbb{K})$.

   ⌜

   $[\subset]$: Clair, car $\det(M_1 M_2 M_1^{-1} M_2^{-1}) = \det M_1 \cdot \det M_2 \cdot (\det M_1)^{-1} \cdot (\det M_2)^{-1} = 1$.
   $[\supset]$: Trivial si $n = 1$, car $\mathrm{SL}(1,\mathbb{K}) = \{1\}$, mais pas facile pour $n > 1$! Voici l'idée.
   Si $n \geq 2$, alors on peut montrer (dur!) que $\mathrm{SL}(n,\mathbb{K})$ est engendré par les matrices:

   $$t_{ij}(\lambda) := \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \quad \text{avec} \quad t_{ij} = \lambda \quad \text{pour} \quad i \neq j \text{ et } \lambda \in \mathbb{K}$$

Ensuite, pour $n \geq 3$, on vérifie la relation: $t_{ij}(\lambda) = t_{ik}(\lambda)t_{kj}(1)t_{ik}(\lambda)^{-1}t_{kj}(1)^{-1}$, pour $i \neq j, j \neq k, i \neq k$.
Cela implique: $\mathrm{SL}(n,\mathbb{K}) \subset [\mathrm{SL}(n,\mathbb{K}), \mathrm{SL}(n\mathbb{K})] \subset [\mathrm{GL}(n,\mathbb{K}) m \,\mathrm{GL}(n,\mathbb{K})]$
(Pour $n = 2$, une autre relation est utilisée, qui donne aussi $\mathrm{SL}(2,\mathbb{K}) \subset [\mathrm{SL}(2,\mathbb{K}), \mathrm{SL}(2,\mathbb{K})]$).

Notons que pour $n \geq 2$, on a $[\mathrm{SL}(n,\mathbb{K}), \mathrm{SL}(n,\mathbb{K})] = \mathrm{SL}(n,\mathbb{K})$

⌟

Théorème I.13

Soit G un groupe quelconque. Alors:

(i) $[G,G] \triangleleft G$

(ii) Le quotient $G/[G,G] =: G_{\mathrm{ab}}$ est abélien.

(iii) On a la propriété universelle suivante:

Pour tout homomorphisme $\varphi : G \to A$ avec A abélien, il existe un unique homomorphisme $\overline{\varphi} : G_{\mathrm{ab}} \to A$ tel que $\overline{\varphi} = \varphi$.

Remarques

1. G_{ab} est appelé l'abélianisé de G.

2. La propriété universelle signifie: le quotient $G \to G_{\mathrm{ab}}$ est la manière la plus économique de rendre un groupe abélien: on "tue" les commutateurs!

Preuve:

(i) Soit $g \in G$ quelconque, et ι_g la conjugaison par g. Comme ι_g est un homomorphisme, la remarque 7 donne:
$g[G,G]g^{-1} \overset{\text{def.}}{=} \iota_g([G,G]) \overset{\text{rem. } 7}{\subset} [\iota_g(G), \iota_g(G)] \subset [G,G]$ Donc $N = [G,G]$ est un sous-groupe normal.

(ii) Par remarque 1, $G_{\mathrm{ab}} = G/N$ est abélien $\iff$ tout commutateur dans G/N est trivial.
A voir donc: $\forall g, h \in G$, on a: $[gN, hN] = e_{G/N}$, avec $N = [G,G]$.
En notant $\pi : G \to G_{\mathrm{ab}} = G/N$ la projection, on a: $[gN, hN] = [\pi(g), \pi(h)] \overset{\text{rem. } 2}{=} \pi([g,h]) = e_{G/N}$ car $[g,h] \in [G,G] = N = \mathrm{Ker}(\pi)$

(iii) Soit donc $\varphi : G \to A$ un homomorphisme avec A groupe abélien.
Vérifions que $N = [G,G] \subset \mathrm{Ker}(\varphi)$, pour conclure à l'aide de Proposition I.8

En effet:

$$\varphi([G,G]) \overset{\text{rem. } 7}{\subset} [\varphi(G), \varphi(G)] \subset [A,A] = \{0_A\}, \quad \text{car } A \text{ est abélien.}$$

Ainsi, on a bien $N \subset \mathrm{Ker}(\varphi)$.

□

Exemples

1. G abélien $\iff [G,G] = \{e\} \iff G_{\text{ab}} = G$.

2. Comme $|[S_3, S_3]| = 3$, on a $(S_3)_{\text{ab}} \cong \mathbb{Z}/2\mathbb{Z}$
   On vera que $\forall n \geq 2$, $(S_n)_{\text{ab}} = \mathbb{Z}/[S_n, S_n] \cong \mathbb{Z}/2\mathbb{Z}$.

3. $\text{GL}(n,\mathbb{K})_{\text{ab}} \cong \text{GL}(n,\mathbb{K})/\text{SL}(n,\mathbb{K}) \underset{\text{vu}}{\cong} \mathbb{K}^*$

Terminologie

Pour un groupe G, notons $G = G^{(0)}, G^{(1)} := [G^{(0)}, G^{(0)}], \ldots, G^{(k+1)} = [G^{(k)}, G^{(k)}], \ldots$
On obtient une suite: $\cdots \triangleleft G^{(2)} \triangleleft G^{(1)} \triangleleft G^{(0)} = G$, appelée la suite dérivée de G.

Définition

G est dit résoluble s'il existe $k \geq 0$ tel que $G^{(k)} = \{e\}$

Exemples

1. G abélien $\iff G^{(1)} = \{e\} \implies G$ résoluble.

2. S_1, S_2 sont abéliens $\implies$ résolubles.
   S_3 pas abélien, mais $[S_3, S_3]$ abélien $\implies (S_3)^{(2)} = \{e\} \implies S_3$ résoluble.
   S_4 est aussi résoluble.
   On verra: S_n n'est pas résoluble pour $n \geq 5$.

3. $\text{GL}(n,\mathbb{K}) = \mathbb{K}^*$ abélien $\implies$ résoluble.
   $G = \text{GL}(n,\mathbb{K})$ pas résoluble pour $n \geq 2$, car $G^{(1)} = \text{SL}(n,\mathbb{K}), G^{(2)} = \text{SL}(n,\mathbb{K}), \ldots$
   $G^{(k)} = \text{SL}(n,\mathbb{K}) \quad \forall k \geq 1$

1.7 Groupes symétriques

Rappel

X ensemble ($\neq 0$), $S(X) := \{f : X \to X \mid f \text{ bij. }\}$ est un groupe (Le groupe symétrique sur X). Si X et Y sont en bijection, alors $S(X) \cong S(Y)$. Si X est fini, disons $n = |X|$, alors $S(X) =: S_n$, le groupe symétrique d'indice n, $\sigma \in S_n$ est appelé une permutation (de n objets).

Ces groupes sont d'une grande importance, en particulier à cause du théorème suivant.

Théorème de Cayley

Tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

Preuve:

Soit donc G un groupe quelconque. Posons $X = G$ et $\varphi : \begin{array}{ccc} X & \longrightarrow & S(G) \\ g & \longmapsto & \varphi(g) \end{array}$ définie par $\varphi(g) : \begin{array}{ccc} G & \longrightarrow & G \\ h & \longmapsto & gh \end{array}$

A voir:

$$\left.\begin{array}{ll} (1) & \varphi(g) \in S(G) \\ (2) & \varphi \text{ homomorphisme} \\ (3) & \varphi \text{ injective} \end{array}\right\} \implies \varphi \text{ définit un isomorphisme } G \to \mathrm{Im}(\varphi) < S(G), \text{ et on a terminé.}$$

(1) $(\varphi(g) \circ \varphi(g^{-1}))(h) = \varphi(g)(\varphi(g^{-1})(h)) = \varphi(g)(g^{-1}h) = g(g^{-1}h) = h = id_G(h) \qquad \forall h \in G$

$$\left.\begin{array}{l} \implies \varphi(g) \circ \varphi(g^{-1}) = id_G \\ \text{De même: } \varphi(g^{-1}) \circ \varphi(g) = id_G \end{array}\right\} \implies \varphi(g) \text{ est bij. (d'inverse } \varphi(g^{-1})) \implies \varphi(g) \in S(G).$$

(2) Soient $g_1, g_2 \in G$; à voir: $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2) \in S(G)$

$$\forall h \in G : \quad \varphi(g_1 g_2)(h) = (g_1 g_2) \cdot h = g_1(g_2 h) = \varphi(g_1)(g_2 h) = \varphi(g_1)(\varphi(g_2)(h)) = (\varphi(g_1) \circ \varphi(g_2))(h)$$

(3) $g \in \mathrm{Ker}\,\varphi \iff \varphi(g) = id_G \iff \varphi(g)(h) = h,\ \forall h \in G \iff gh = h,\ \forall h \in G$
$\implies g = e_G \implies \mathrm{Ker}\,\varphi = \{e_G\} \iff \varphi \text{ inj.}$

□

Remarque

Si G est fini, disons $|G| = n$, alors on obtient $G \cong \mathrm{Im}(\varphi) < S_n$. (Si G est infini, on n'a pas $G < S_n$.)

Dès à présent, on se restreint à X fini, et l'on étudie donc: $S_n = S(\{1, 2, \ldots, n\}), \qquad n \geq 1$

Notation et terminologie

- Soit $1 \leq r \leq n$. Une permutation $\sigma \in S_n$ est un r-cycle si $\exists \{x_1, \ldots, x_r\} \subset \{1, 2, \ldots, n\}$ tel que $\sigma(x_i) = x_{i+1}$ pour $i = 1, \ldots, r-1$, $\sigma(x_r) = x_1$ et $\sigma(y) = y\ \forall y \in \{1, 2, \ldots, n\} \setminus \{x_1, \ldots, x_r\}$.

On note $\sigma = (x_1\, x_2\, \ldots\, x_r)$ et l'ensemble $\{x_1, \ldots, x_r\}$ est le support du cycle σ.

- Un 2 cycle est appelé une transposition. (Le 1 cycle est l'identité)
- On notera $\sigma \circ \tau =: \sigma\tau \in S_n$, pour $\sigma, \tau \in S_n$.

Exemple

Dans S_3, la permutation notée $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ en algèbre linéaire est en fait la transposition $\sigma = (1\,2)$.
De même $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ est notée $\tau = (2\,3) = (3\,2)$
Calculons $\sigma\tau = (1\,2)(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = (1\,2\,3) \in S_3$. Et $\tau\sigma = (2\,3)(1\,2) = (3\,2\,1)$, et l'on voit que S_3 n'est pas abélien.

Dernier calcul: $\tau\sigma\tau^{-1} = (2\,3)(1\,2)(2\,3) = (1\,3)$.

Cela montre que $H = \langle\sigma\rangle = \{id, \sigma\}$ n'est pas normal dans S_3.

Proposition I.14

Soit $(x_1\, x_2\, \ldots\, x_r)$ un r-cycle dans S_n.

(i) $(x_1\, x_2\, \ldots\, x_r) = (x_2\, x_3\, \ldots\, x_r\, x_1) \in S_n$.

(ii) $(x_1\, x_2\, \ldots\, x_r) = (x_1\, x_2\, \ldots\, x_j)(x_j\, x_{j+1}\, \ldots\, x_r) \in S_n,\ \forall 1 \leq j \leq r$

(iii) L'ordre de $(x_1\, x_2\, \ldots\, x_r)$ dans S_n est r.

⌜

Par définition, pour $\sigma = (x_1\, x_2\, \ldots\, x_r)$, on a:

$$o(\sigma) \overset{\text{déf.}}{=} |\langle\sigma\rangle| \overset{\text{vu}}{=} \min\{k \mid \sigma^k = id\} \overset{\text{evident}}{=} r$$

⌟

(iv) Pour tout $\tau \in S_n$, on a $\tau(x_1\, x_2\, \ldots\, x_r)\tau^{-1} = (\tau(x_1)\, \tau(x_2)\, \ldots\, \tau(x_r))$

⌜

Supposons $r = 2$, $\sigma(x_1\, x_2) =: (i\, j)$. Calculons:

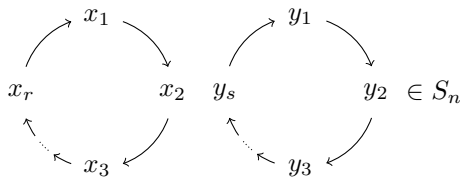
$$\tau(i\,j)\tau^{-1} : k \to \begin{cases} \tau(j) & k = \tau(i) \\ \tau(i) & k = \tau(j) \\ \tau(\tau^{-1}(k)) = k & \text{sinon} \end{cases}$$, c'est $(\tau(i)\,\tau(j))$. Donc ça marche pour $r = 2$.

Pour le cas général, on utilise (ii) (et une récurrence sur $r \geq 2$) pour obtenir:

$$\begin{aligned} \tau(x_1\, x_2\, \ldots\, x_r)\tau^{-1} &= \tau(x_1\, x_2)(x_2\, x_3)\cdots(x_{r-1}\, x_r)\tau^{-1} \\ &= \tau(x_1\, x_2)\tau^{-1}\tau(x_2\, x_3)\tau^{-1}\cdots\tau(x_{r-1}\, x_r)\tau^{-1} \\ &= (\tau(x_1)\tau(x_2))(\tau(x_2)\tau(x_3))\cdots(\tau(x_{r-1})\tau(x_r)) = (\tau(x_1)\tau(x_2)\cdots\tau(x_r)) \end{aligned}$$

(v) Deux cycles à support disjoint commutent.

Si $\sigma = (x_1\, x_2\, \ldots\, x_r)$ et $\tau = (y_1\, y_2\, \ldots\, y_s)$ avec $x_i \neq y_j$, $\forall i, j$. Alors $\sigma\tau = \tau\sigma$ est donné par:



Théorème I.15

Toute permutation est le produit de cycles à supports disjoints.

Preuve:
L'idée est claire: $1 \to \sigma(1) \to \sigma^2(1) \cdots \to \sigma^r(1) = 1 \rightsquigarrow$ un r-cycle.
Puis on continue avec $i \notin \{1, \sigma(1), \ldots, \sigma^{r-1}(1)\}$, etc...

Voici une preuve plus formelle:
Fixons $\sigma \in S_n$ une fois pour toute. Sur $\{1, 2, \ldots, n\}$, posons $i \sim j \overset{\text{def.}}{\iff} \exists m \in \mathbb{Z}$ tel que $i = \sigma^m(j)$.

C'est une relation d'équivalence:

– $i \sim i$ car $i = \sigma^0(i)$, $0 \in \mathbb{Z}$

– $i \sim j \iff i = \sigma^m(j) \iff j = \sigma^{-m}(i) \implies j \sim i \quad (m \in \mathbb{Z} \implies -m \in \mathbb{Z})$

– $i \sim j$ et $j \sim k \iff \exists m, l \in \mathbb{Z}$ tels que $i = \sigma^m(j)$ et $j = \sigma^l(k)$.
$\implies i = \sigma^m(\sigma^l(k)) = \sigma^{m+l}(k) \implies i \sim k \quad (m, l \in \mathbb{Z} \implies m + l \in \mathbb{Z})$

Ainsi, on obtient une partition $\{1,\dots,n\} = B_1 \sqcup B_2 \sqcup \cdots \sqcup B_k$ une classe d'équivalence.
On vérifie que $\forall s = 1,\dots,k$ et $\forall i \in B_s$, on a $B_s = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{r-1}(i)\}$, où $r := |B_s|$. (Donné sans détail ici car pas dur)

Si l'on pose $\sigma_s := (i\,\sigma(i)\,\sigma^2(i)\,\cdots\,\sigma^{r-1}(i))$ pour $s = 1,\dots,k$, on obtient $\sigma = \sigma_1\sigma_2\cdots\sigma_k$, avec support $(\sigma_s) = B_s$, et donc disjoints.

□

Exemple

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 2 & 3 \end{pmatrix} \in S_6$

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

Remarque

La décomposition d'une permutation en produit de cycles à supports disjoints est unique à:

(1) Permutation des cycles [I.14, (v)]
(2) Permutation cyclique dans chaque cycle [I.14, (i)]
(3) i-cycles

} près.

Par exemple: $\sigma = (1\,5\,2)(6\,3)(4) = (1\,5\,2)(6\,3) = (6\,3)(1\,5\,2) = (3\,6)(5\,2\,1)$

Corollaire I.16

Toute permutation est produit de transpositions. (ie. Les transpositions engendrent S_n)

Preuve:
Soit $\sigma \in S_n$. Par I.15, σ est produit de cycles. Par I.14 (ii), chaque cycle est produit de transpositions.

□

Définition

La signature d'une permutation $\sigma \in S_n$ est:

$$\varepsilon(\sigma) := \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \quad \in \mathbb{Q}^*$$

Exemples

1. $\sigma = id \implies \varepsilon(id) = \prod_{i<j} \frac{i-j}{i-j} = 1$

2. $\sigma = (1\,2) \in S_3 \implies \varepsilon(\sigma) = \frac{2-1}{1-2} \cdot \frac{1-3}{2-3} \cdot \frac{2-3}{1-3} = -1$

Proposition I.17

La signature a valeurs dans $\{-1,1\}$, et définit un homomorphisme $\varepsilon:\ S_n \to \{-1,1\}$.

Preuve:

Notons d'abord que $\varepsilon(\sigma) = \prod_{\substack{\{i,j\}\subset\{1,\dots,n\}\\ i\neq j}} \frac{\sigma(i)-\sigma(j)}{i-j}$.

Idée de la preuve:

(1) $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$
(2) Si σ est une transposition, alors $\varepsilon(\sigma) = -1$

$\Big\} \implies$ Par I.16, on a terminé!

(1) Pour $\sigma, \tau \in S_n$, calculons:

$$\begin{aligned}\varepsilon(\sigma\tau) &\overset{\text{def.}}{=} \prod_{\{i,j\}} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{i-j} = \prod_{\{i,j\}} \left(\frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} \cdot \frac{\tau(i)-\tau(j)}{i-j} \right) \\ &= \prod_{\{i,j\}} \frac{\sigma(\overbrace{\tau(i)}^{=:k}) - \sigma(\overbrace{\tau(j)}^{=:l})}{\tau(i)-\tau(j)} \cdot \prod_{\{i,j\}} \frac{\tau(i)-\tau(j)}{i-j} \\ &= \varepsilon(\sigma)\varepsilon(\tau)\end{aligned}$$

Cela démontre (1)

(2) (Pas la démo du prof mais la mienne)
Montrons donc que $\varepsilon(\sigma) = -1$ pour $\sigma = (u\,v)$ une transposition.

$$\begin{aligned}\varepsilon(\sigma) &\overset{\text{def.}}{=} \prod_{\{i,j\}} \frac{\sigma(i)-\sigma(j)}{i-j} = \prod_{\{i,j\}\neq\{u,v\}} \frac{\sigma(i)-\sigma(j)}{i-j} \cdot \prod_{\substack{i=u\\ j\neq v,u}} \frac{\sigma(i)-\sigma(j)}{i-j} \cdot \prod_{\substack{i=v\\ j\neq v,u}} \frac{\sigma(i)-\sigma(j)}{i-j} \cdot \prod_{\{i,j\}=\{u,v\}} \frac{\sigma(i)-\sigma(j)}{i-j} \\ &= \underbrace{\prod_{\{i,j\}\neq\{u,v\}} \frac{i-j}{i-j}}_{=1} \cdot \underbrace{\prod_{\substack{i=u\\ j\neq v,u}} \frac{v-j}{u-j} \cdot \prod_{\substack{i=v\\ j\neq v,u}} \frac{u-j}{v-j}}_{=1} \cdot \underbrace{\prod_{\{i,j\}=\{u,v\}} \frac{v-u}{u-v}}_{=-1} = -1\end{aligned}$$

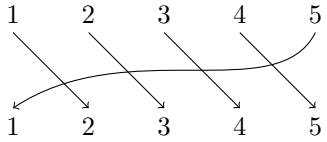
□

Remarques

1. Ainsi, $\sigma \in S_n$ a $\varepsilon(\sigma) = 1$ (resp. -1) $\iff$ σ s'écrit comme produit d'un nombre pair (resp. impair) de transpositions.
   Notons que ce produit n'est pas unique, par exemple: $(1\,3) = (2\,3)(1\,2)(2\,3)$.

   Mais la proposition I.17 montre que la parité du nombre de transpositions dans la décomposition d'une permutation donnée, est fixe !

2. Graphiquement, $\varepsilon(\sigma) = -1$, par exemple $\sigma = (1\,2\,3\,4\,5) \implies \varepsilon(\sigma) = (-1)^4$ par le diagrame:



Terminologie

Une permutation $\sigma \in S_n$ est dite paire (resp. impaire) si $\varepsilon(\sigma) = 1$ (resp. -1).

Définition

Le sous groupe $A_n := \mathrm{Ker}(\varepsilon) \triangleleft S_n$ des permutations paires est appelé le groupe alterné de degré n.

Remarque

Si $n > 1$, alors $\varepsilon : S_n \to \{-1, 1\}$ est surjective $\overset{I.9}{\Longrightarrow}$ $S_n \big/ A_n \cong \{-1, 1\}$

$2 = \left| S_n \big/ A_n \right| = [S_n : A_n] \overset{\text{Lagrange}}{=} \dfrac{|S_n|}{|A_n|} \implies |A_n| = \dfrac{n!}{2}$ pour $n > 1$

Exemples

- $(n = 1)$ $A_1 = S_1 = \{id\}$
- $(n = 2)$ $A_2 = \{id\} \triangleleft \{id, (1\,2)\} = S_2$
- $(n = 3)$ $A_3 = \{id, (1\,2\,3), (1\,3\,2)\} \triangleleft S_3$
- Un r-cycle a signature $(-1)^{r-1}$, en particulier, les 3-cycles sont dans A_n.

Proposition I.18

Le groupe A_n est engendré par les 3-cycles.

Preuve:
Comme tout élément de A_n est produit d'un nombre pair de transpositions, il suffit de vérifier que tout produit de 2 transpositions est produit de 3-cycles.

Soient donc $(x_1\,x_2)$ et $(x_3\,x_4)$ des transposition dans S_n.

Cas 1: $\{x_1, x_2\} = \{x_3, x_4\} \implies (x_1\,x_2)(x_3\,x_4) = (x_1\,x_2)(x_1\,x_2) = id$

Cas 2: $|\{x_1, x_2\} \cap \{x_3, x_4\}| = 1$, disons $x_1 = x_3$ et $x_2 \neq x_4$. Alors $(x_1\,x_2)(x_3\,x_4) = (x_1\,x_2)(x_1\,x_4) = (x_2\,x_1\,x_4)$.

Cas 3: $\{x_1, x_2\} \cap \{x_3, x_4\} = \varnothing \implies (x_1\,x_2)(x_3\,x_4) = (x_1\,x_2\,x_3)(x_2\,x_3\,x_4)$

□

*V*oici une série de résultats qui illustrent beaucoup de concepts vus au cours de ce chapitre.

La relation $\triangleleft$ n'est pas transitive.

Posons $N_2 := \{\sigma \in A_4 \mid \sigma^2 = id\}$ et $N_1 = \{id, \alpha\}$ pour $\alpha \in N_2 \setminus \{id\}$

$N_2 \triangleleft A_4$: Soit $\sigma \in N_2$, $\tau \in A_4$. Alors $\tau\sigma\tau^{-1} \in A_4$, et $\left(\tau\sigma\tau^{-1}\right)^2 = (\tau\sigma\tau^{-1})(\tau\sigma\tau^{-1}) = \tau\sigma^2\tau^{-1}$
$\underset{\sigma\in N_2}{=} \tau id\tau^{-1} = id \implies \tau\sigma\tau^{-1} \in N_2$

$N_1 \triangleleft N_2$: tous les éléments de N_2 sont d'ordre 2 $\implies$ N_2 abélien $\implies$ tout sous-groupe est normal.

$N_1 \not\triangleleft A_4$: Par exemple, si $\alpha = (1\,2)(3\,4)$ et $\tau = (1\,2\,3) \in A_4$, alors $\tau\alpha\tau^{-1} = (2\,3)(1\,4) \notin N_1$

$[S_n, S_n] = A_n \quad \forall n$ ($\implies (S_n)_{\text{ab}} = {S_n}\big/{[S_n, S_n]} = {S_n}\big/{A_n} \cong \{-1, 1\}$)

$\{\subset\}$: $\forall \sigma, \tau \in S_n, \quad \varepsilon([\sigma, \tau]) = [\varepsilon(\sigma), \varepsilon(\tau)] = 1$ car $\{-1, 1\}$ est abélien.
$\implies [\sigma, \tau] \in A_n \implies [S_n, S_n] \subset A_n$.

$\{\supset\}$: Tout 3-cycle est un commutateur: $(x_1\,x_2\,x_3) = [(x_2\,x_3)(x_1\,x_2)]$, et on conclut par I.18.

Pour $n \geq 5$, $[A_n, A_n] = A_n$ ($\implies (A_n)_{\text{ab}} = \{1\} \quad \forall n \geq 5$)

$\{\subset\}$: ✓

$\{\supset\}$: Soit $(i\,j\,k)$ un 3-cycle dans $A_n, n \geq 5 \implies \exists l, m \in \{1, \ldots, n\}$ tels que $|\{i, j, k, l, m\}| = 5$.
$[(i\,l\,k), (k\,j\,m)] = (i\,l\,k)(k\,j\,m)(i\,l\,k)^{-1}(k\,j\,m)^{-1} = (i\,j\,k) \implies (i\,j\,k) \in [A_n, A_n]$ et l'on conclut par I.18.

S_n est résoluble $\iff n \in \{1, 2, 3, 4\}$

– $S_1 = S_1^{(0)} = \{id\}$

– S_2 abélien $\implies S_2^{(1)} := [S_2, S_2] = \{id\} \implies S_2$ résoluble.

– $S_3^{(1)} = [S_3, S_3] = A_3$ abélien $\implies S_3^{(2)} = A_3^{(1)} = \{id\} \implies S_3$ résoluble.

– $S_4^{(1)} = [S_4, S_4] = A_4, S_4^{(2)} = [A_4, A_4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ abélien $\implies S_4^{(3)} = \{id\} \implies S_4$ résoluble

– Pour $n \geq 5$, $S_n^{(1)}[S_n, S_n] = A_n$, $S_n^{(k)} = [A_n, A_n]^{(k)} = A_n \implies S_n^{(k)} = A_n \neq \{id\}$, $\forall k \geq 1 \implies S_n$ n'est pas résoluble!

Pour tout $n > 2$, $Z(S_n) := \{\sigma \in S_n \mid \sigma\tau = \tau\sigma, \ \forall \tau \in S_n\}$ est trivial.

Preuve:
Soit $\sigma \in S_n (n \geq 3), \sigma \neq id$.
A voir: $\exists \tau \in S_n$ tel que $\tau\sigma\tau^{-1} \neq \sigma$ ($\implies \tau\sigma \neq \sigma\tau \implies \sigma \neq Z(S_n)$).
Par Proposition I.5, on peut écrire $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$ cycles à supports disjoints. Notons r la longueur maximale de ces cycles; on a $r \geq 2$, car sinon $\sigma = id$. Sans perte de généralité, supposons $\sigma_1 = (x_1, x_2, \ldots, x_r)$, avec $r \geq 2$.

Cas 1: $r \geq 3$
Dans ce cas, prenons $\tau := (x_1, x_2) \in S_n$. Calculons

$$\tau\sigma\tau^{-1} = \tau\sigma_1\sigma_2 \cdots \sigma_s\tau^{-1} = \tau\sigma_1\tau^{-1}\sigma_2 \cdots \sigma_s = (x_2, x_1, x_3, \ldots, x_r)\sigma_2 \cdots \sigma_3 \neq \sigma_1\sigma_2 \cdots \sigma_s = \sigma$$

Car $(x_2, x_1, \ldots, x_r) \neq (x_1, x_2, \ldots, x_r)$ puisque $r \geq 3$.

Cas 2: $r = 2$, ie: tous les cycles $\sigma_1, \sigma_2, \ldots, \sigma_s$ sont de longueur 1 ou 2.
Comme $\sigma_1 = (x_1, x_2)$ et $n \geq 3$, $\exists y \in \{1, \ldots, n\} \setminus \{x_1, x_2\}$. Posons $\tau := (x_1, y) \in S_n$.
Calculons $\tau\sigma\tau^{-1} = \tau\sigma_1 \cdots \sigma_s\tau^{-1} = \underbrace{(\tau\sigma_1\tau^{-1})}_{=(y,x_2)} \underbrace{\cdots (\tau\sigma_s\tau^{-1})}_{\tilde{\sigma}} = (y, x_2) \cdot \tilde{\sigma} \neq (x_1, x_2)\sigma_2 \cdots \sigma_s = \sigma$
On voit que $(x_2 \to y)$ et $(x_2 \to x_1)$, cela conclut la preuve.

□

Théorème I.19

Pour tout $n \geq 5$, A_n est simple.

Remarques:

1. Cela implique que $[A_n, A_n] = A_n$ pour $n \geq 5$ (déjà vu)

$$\text{Soit } N := [A_n, A_n] \lhd A_n;\ A_n \text{ simple} \Longrightarrow \left.\begin{array}{ll} N = \{id\} & \text{ou } N = A_n \\ \Updownarrow & \\ A_n \text{ abélien} & \text{, faux pour } n \geq 4. \end{array}\right\} \Longrightarrow N = A_n.$$

⌟

2. A_4 n'est <u>pas</u> simple ($[A_4, A_4]$ est un n-groupe normal propre de A_n, voir Série 5)

Lemme I.20

Pour $n \geq 5$, tous les 3-cycles sont conjugués dans A_n.

<u>Preuve:</u>
Soit donc (i, j, k) un 3-cycle quelconque dans A_n, $n \geq 5$. Soit $\sigma \in S_n$ tel que $\sigma(i) = 1, \sigma(j) = 2, \sigma(k) = 3$. On a:

$$\sigma(i, j, k)\sigma^{-1} = (1, 2, 3)$$

1. Si $\sigma \in A_n$, on a terminé.

2. Si $\sigma \notin A_n$, alors $\sigma' := (4, 5)\sigma \in A_n$ car $n \geq 5$. On a:

$$(\sigma')(i, j, k)(\sigma')^{-1} = (4, 5)\sigma(i, j, k)\sigma^{-1}(4, 5) = (4, 5)(1, 2, 3)(4, 5) = (1, 2, 3)$$

□

Preuve du théorème I.19. Soit $N \lhd A_n (n \geq 5),\ N \neq \{id\}$. A voir: $N = A_n$.

<u>Affirmation:</u> N contient un 3-cycle.

<u>Cela implique le théorème:</u>

Si N contient un 3-cycle, comme $N \lhd A_n$ et $n \geq 5$, N contient <u>tous</u> les 3-cycles par I.20. Par I.18 on aura $N \supset A_n$, d'où $N = A_n$.

⌜

Comme $N \neq \{id\}$, on a $x \in N, x \neq id$. Ecrivons $x = \sigma_1\sigma_2 \cdots \sigma_s \neq id$.

Cas 1: Un cycle a longueur > 3, disons $\sigma_1 = (i, j, k, l, \ldots)$. Posons $y := (i, j, k) \in A_n$.

$$x \in N \implies x^{-1} \in N \overset{N \lhd A_n}{\Longrightarrow} yx^{-1}y^{-1} \in N \overset{x \in N}{\Longrightarrow} xyx^{-1}y^{-1} \in N$$

Calculons $xyx^{-1}y^{-1} = \underbrace{\sigma_1 y \sigma_1^{-1}}_{(j,k,l)} y^{-1} = (j, k, l)(i, k, j) = (i, l, j) \in N$, donc OK.

Cas 2
Cas 3 On se ramène au Cas 1 déjà traité (sans détail ici).

⌟

□

1.8 Classification

Classifier les groupes abéliens finis n'est pas dur (cf. Alg. II):

Théorème

Soit G un groupe abélien fini. Alors, il existe une unique suite d'enntiers $m_1, m_2, \ldots, m_s \geq 2$ ($s \geq 0$), tel que $m_i \mid m_{i+1}$, $\forall i = 1, \ldots, s-1$, et $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$.

Remarque

On montre facilement que si $\text{pgcd}(m, n) = 1$, alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$.

Exemple

Classifions à isomorphisme près tous les groupes abélines d'ordre $36 = 2^2 \cdot 3^2$.

$$36 = 2 \cdot 18 = 3 \cdot 12 = 6 \cdot 6$$

Donc, G abélien d'ordre 36 est isomorphe à exactement un groupe parmi:

$$\mathbb{Z}/36\mathbb{Z} \ , \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \ , \ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \ , \ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

Le cas général (non-abélien) est infiniment plus dur. Mais les groupes finis simples peuvent être considéres comme les "briques" de base pour construire tous les groupes finis.
Et on connait tous les groupes finis simples.

Théorème

Tout groupe fini simple est isomorphe à exactement un groupe parmi:

- $\mathbb{Z}/p\mathbb{Z}$ avec p premier
- A_n pour $n \geq 5$
- Les "groupes classiques" (typiquement: des groupes de matrices sur un corps fini)
- 27 groupes "sporadiques" (le plus grand a $\approx 8 \cdot 10^{53}$ éléments)

2 Anneaux et corps

Dans le cours de "Logique et théorie des ensembles" nous avons étudié des notions d'arithmétique sur $\mathbb{Z}$.

- "a divise b" dans $\mathbb{Z}$ si $\exists c \in \mathbb{Z}$ tel que $b = ac$.
- Le pgcd de a et b: $d \geq 0$ tel que $d \mid a,\ d \mid b$, si $c \mid a,\ c \mid b$, alors $c \mid d$.
- $a, b \in \mathbb{Z}, b > 0, \exists q, r \in \mathbb{Z}$ tels que $a = qb + r$ avec $0 \leq r < b$ (division euclidienne).
- $p > 1$ est premier si $d \mid p \implies d = 1$ ou $d = p$ $(d > 0)$.
- Théorème fondamental de l'arithmétique:
  Tout $n > 1$ s'écrit de façon unique (à permutation des facteurs près) comme produit de premiers.

Le cadre formel où cette théorie se généralise est celui des anneaux (euclidiens). L'exemple fondamental est $\mathbb{Z}$, mais on a aussi $\mathbb{R}[x], \mathbb{Z}[i], \ldots$ C'est l'objet du Chapitre II.

2.1 Axiomes et exemples

Définition

Un anneau est un ensemble A muni de deux lois de composition $+$: $\begin{array}{ccc} A\times A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array}$ et $\cdot$: $\begin{array}{ccc} A\times A & \longrightarrow & A \\ (a,b) & \longmapsto & a\cdot b \end{array}$ tels que:

(A1) $(A,+)$ est un groupe abélien.

(A2) $a\cdot(b\cdot c)=(a\cdot b)\cdot c \quad \forall a,b,c\in A$

(A3) $\exists 1\in A$ tel que $1\cdot a=a\cdot 1=a \quad \forall a\in A$

(A4) $a\cdot(b+c)=a\cdot b+a\cdot c$ et $(b+c)\cdot a=b\cdot a+c\cdot a \quad \forall a,b,c\in A.$

Si de plus on a: $a\cdot b=b\cdot a \quad \forall a,b\in A$, alors A est un anneau commutatif.

Remarques et terminologie

1. La loi $+$ est appelée l'addition. Le neutre dans $(A,+)$ est noté $0=0_A$, et l'inverse de a dans $(A,+)$ est noté $-a$.

2. La loi $\cdot$ est appelée la multiplication. On notera souvant $a\cdot b=:ab$. (A2), (A3) signifient que $(A,\cdot)$ est un monoïde. En particulier, le neutre $1=1_A$ est unique (cf. Chapitre I).

3. L'axiome (A4) est un axiome de distributivité.
   Formellement, on aurait du l'écrire: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)(\neq a\cdot(b+a)\cdot c)$
   Mais on suit la convention habituelle...

4. On a les "règles de calcul" suivantes, $\forall a,b\in A$:

   (i) $a\cdot 0=0\cdot a=0$

   ⌜

   $$a\cdot 0\overset{(A1)}{=}a(0+0)\overset{(A4)}{=}a0+a0 \implies 0=a0+-(a0)=a0+a0-a0=a0$$

   De même pour $0\cdot a=0$.

   ⌟

   (ii) $a(-b)=(-a)b=-(ab)$

   ⌜

   $$ab+a(-b)\overset{(A4)}{=}a(b-b)=a0\overset{(i)}{=}0 \iff a(-b) \text{ est l'inverse additif de } ab \overset{\text{not.}}{\iff} a(-b)=-(ab)$$

   Idem pour $(-a)b=-(ab)$.

(iii) $(-a)(-b) = ab$

(iv) $(-1)a = -a$

(v) $(-1)(-1) = 1$

5. On a bien-sûr $a + b = a + c \implies b = c$, car $(A, +)$ est un groupe. En revanche, $a \cdot b = a \cdot c \not\Longrightarrow b = c$!! $(0 \cdot 1 = 0 \cdot 2 \in \mathbb{Z} \not\Longrightarrow 1 = 2)$

6. L'ensemble $A = \{0\}$ est un anneau (trivialement), appelé l'anneau nul, noté $A = 0$. Notons que $A = 0 \iff 0 = 1$.

   $[\Longrightarrow]$: Trivial
   $[\Longleftarrow]$: Si $0 = 1$, alors $\forall a \in A$, on a: $a = a \cdot 1 \overset{1=0}{=} a \cdot 0 \overset{(i)}{=} 0$, d'où $A = \{0\}$.

7. Pour $a \in A$ et $n \in \mathbb{Z}$, on note: $na := \begin{cases} \overbrace{a + \cdots + a}^{n} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{|n|} & n < 0 \end{cases}$ (Puissance, dans le cadre abélien)

   Par les ex. 2, 3, Série 1, on a, $\forall a, b \in A,\ \forall n, m \in \mathbb{Z}$:

$$(n + m)a = na + ma$$
$$(nm)a = n(ma)$$
$$n(a + b) = na + nb$$

   Mais on a de plus:

$$n(ab) = (na)b = a(nb)$$

   En effet, pour $n > 0$

$$n(ab) \overset{\text{def.}}{=} \overbrace{ab + \cdots + ab}^{n} \overset{(A4)}{=} \overbrace{(a + \cdots + a)}^{n} \cdot b \overset{\text{def.}}{=} (na)b$$
$$n(ab) = ab + \cdots + ab = a(b + \cdots + b) = a(nb)$$

Exemples d'anneaux

1. $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif. De même, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux commutatifs.

2. Si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, et $n \geq 1$, alors $A = M_n(\mathbb{K})$ est un anneau pour l'addition et la multiplication matricielles. (Cela découle de résultats vus en Algèbre linéaire)
   Pour $n = 1$, on a $M_1(\mathbb{K}) = \mathbb{K}$, commutatif. Mais $M_n(\mathbb{K})$ n'est pas commutatif dès que $n > 1$.

3. $A = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ différentiable}\}$ est un anneau commutatif.
   - f, g diff $\implies -f, f+g, f \cdot g$ diff.
   - $f(x) = 0 \quad \forall x$ et $g(x) = 1 \quad \forall x$ sont diff.

   De même pour $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continue }\}$

4. Soit G un groupe abélien. Alors l'ensemble des endomorphismes de G

$$\text{End}(G) := \{\varphi : G \to G \mid \varphi \text{ homomorphisme}\}$$

   est un anneau pour $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$ et $(\varphi \cdot \psi)(g) := \varphi(\psi(g)) \quad \forall g \in G$

5. Pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ est un anneau commutatif, pour

$$[a] + [b] := [a+b] \quad \text{et} \quad [a] \cdot [b] := [ab]$$

   où [ ] désigne la classe d'éqivalence modulo $n\mathbb{Z}$ ($a \sim b \iff a - b \in n\mathbb{Z}$)

   ⌜

   $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe abélien: découle de la théorie générale vue au Chapitre I.
   Vérifions que la multiplication est bien définie, ie: $[a] = [a'],\ [b] = [b'] \implies [ab] = [a'b']$

   En effet:

$$[a] = [a'] \iff a' - a \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} \text{ tel que } a' - a = kn$$
$$[b] = [b'] \iff b' - b \in n\mathbb{Z} \iff \exists \ell \in \mathbb{Z} \text{ tel que } b' - b = \ell n$$

$$\begin{aligned} a'b' - ab &= (a + kn)(b + \ell n) - ab \\ &= \cancel{ab} + a\ell n + knb + k\ell n^2 - \cancel{ab} = n(\underbrace{a\ell + b\overset{\in\mathbb{Z}}{k} + k\ell n}) \end{aligned}$$

   Et donc $[ab] = [a'b']$

   Le reste est automatiquement hérité de $\mathbb{Z}$, par exemple:

$$(A4) \qquad [a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b+c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c]$$

   Par exemple, on a la table de multiplication suivante dans $\mathbb{Z}/3\mathbb{Z}$:

$\cdot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

   ⌟

6. Si A_1, A_2 sont deux anneaux, alors $A_1 \times A_2$ est un anneau pour:
   $(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$
   $(a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot b_1, a_2 \cdot b_2)$ $\qquad \forall a_1, b_1 \in A_1,\ a_2, b_2 \in A_2$

Terminologie

Soit A un anneau.

- Un sous-ensemble $B \subset A$ est appelé un sous-anneau si $1_A \in B$, et $a, b \in B \implies -a, a+b, a \cdot b \in B$. En particulier, $(B, +)$ est un sous-groupe de $(A, +)$, et B est un anneau.

- $a \neq 0 \in A$ est un diviseur de zéro s'il existe $b \neq 0 \in A$ tel que $a \cdot b = 0$ ou $b \cdot a = 0$.

- Un anneau commutatif $A \neq 0$ est dit intègre s'il n'a pas de diviseur de zéro.
  (ie: $ab = 0 \implies a = 0$ ou $b = 0$)

  Dans A intègre, on a: $ab = ac, a \neq 0 \implies b = c$.

  $$ab = ac \iff 0 = ab - ac \overset{(A4)}{=} a \cdot (b - c) \overset{A \text{ intègre}}{\implies} a = 0 \text{ ou } b - c = 0 \overset{a \neq 0}{\implies} b - c = 0 \implies b = c$$

- On note $A^* := \{a \in A \mid \exists b \in A \text{ avec } ab = ba = 1\}$ l'ensemble des unités de A.

  Notons que $(A^*, \cdot)$ est un groupe. De plus si $A \neq 0$, alors $0 \notin A^*$ ($0 \cdot b = b \cdot 0 = 0 \overset{A \neq 0}{\neq} 1$)
  Ainsi, on a $A^* \subset A \setminus \{0\}$

Définition

Un anneau $K \neq 0$ commutatif est un corps si $K^* = K \setminus \{0\}$

Ainsi, un corps est un anneau commutatif non-nul tel que: $\forall a \neq 0 \in K$, $\exists b \in K$ tels que $ab = 1_K$

Remarque

Un corps K est un anneau intègre.

Si $ab = 0$ avec $a \neq 0$, $\exists a^{-1} \in K$ tel que $aa^{-1} = 1 \implies 0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$.
On a donc $b = 0$, et pas de diviseur de zéro dans K.

Retour aux exemples

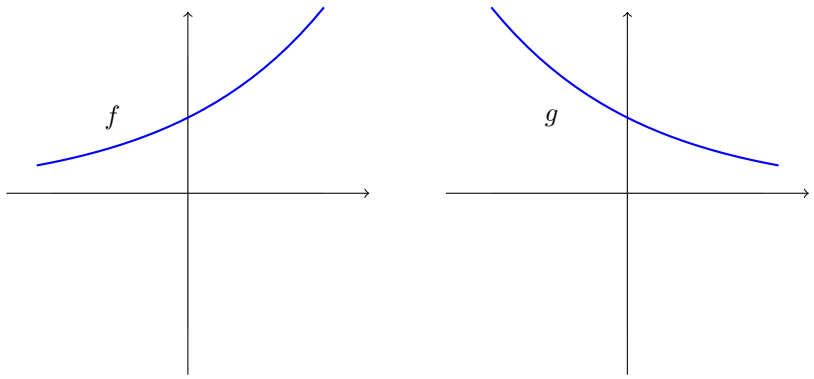
1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ est une suite de sous-anneaux, tous intègres.
   $\mathbb{Z}^* = \{-1, 1\}$: $\mathbb{Z}$ intègre, pas un corps.
   $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$: Ce sont des corps.

2. Soit $\mathbb{K} = \mathbb{R}, \mathbb{C}$, $n \geq 1$, et $A = M_n(\mathbb{K})$
   Si $n = 1$, $M_1(\mathbb{K}) = \mathbb{K}$ est un corps.
   Si $n \geq 2$, $M_n(\mathbb{K})$ possède des diviseurs de zéro: $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ($\implies$ pas intègre $\implies$ pas un corps).

   $$M_n(\mathbb{K})^* = \{M \in M_n(\mathbb{K}) \mid \exists N \in M_k(\mathbb{K}) \quad \text{avec} \quad MN = NM = I\} = \mathrm{GL}(n, \mathbb{K})$$

3. $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ dérivable}\}$ est un sous-anneau de $\{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continue}\}$.

Ces anneaux ne sont pas intègres:



$f \neq 0, g \neq 0$, mais $f \cdot g = 0$. $\{f \mid f \text{ continue}\}^* = \{f \mid f \text{ continue}, f(x) \neq 0 \forall x \in \mathbb{R}\}$ (idem pour dérivable)

4. $(G, +)$ un groupe abélien, $A = \text{End}(G)$.
En général, $\text{End}(G)$ a des diviseurs de zéro. (voir ex.6, S.6)
$A^* = \text{End}(G)^* = \text{Aut}(G)$.
Remarque: Au paragraphe I.3, on avait calculé $\text{Aut}(\mathbb{Z}) = \{-1, 1\}$. En fait, on avait commencé par montrer que $\text{End}(\mathbb{Z}) \cong \mathbb{Z}$, d'où la conclusion: $\text{Aut}(\mathbb{Z}) = \text{End}(\mathbb{Z})^* \cong \mathbb{Z}^* = \{-1, 1\}$

5. Considérons $n \geq 1$ et $A = \mathbb{Z}/n\mathbb{Z}$. Affirmation: $\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ n est premier.

Preuve:
$[\Longrightarrow]$: Par la contraposée, supposons n non-premier. Donc, il existe $1 < r, s < n$ tels que $r \cdot s = n$.
On a donc $a := [r] \neq 0 \in \mathbb{Z}/n\mathbb{Z}$, $b := [s] \neq 0 \in \mathbb{Z}/n\mathbb{Z}$, mais $ab = [r][s] = [rs] = [n] = [0] = 0 \in \mathbb{Z}/n\mathbb{Z}$
Ainsi, $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

$[\Longleftarrow]$: peut se démontrer diretement, mais découle aussi de l'affirmation suivante:
Affirmation: $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \left\{[m] \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(m, n) = 1\right\}$
Conséquence: Si n est premier, alors tout $m = 1, 2, \ldots, n-1$ est premier à n, et donc $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, et donc $\mathbb{Z}/n\mathbb{Z}$ est un corps ($\Longrightarrow$ intègre).

$\ulcorner$

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^* \overset{\text{déf.}}{=} \left\{[m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \exists [\ell] \in \mathbb{Z}/n\mathbb{Z} \text{ tq } [m][\ell] = [1] \in \mathbb{Z}/n\mathbb{Z}\right\}$$

$\exists [\ell] \in \mathbb{Z}/n\mathbb{Z}$ tq $[m][\ell] = [1] \in \mathbb{Z}/n\mathbb{Z} \iff \exists \ell, k \in \mathbb{Z}$ tq $m\ell + kn = 1 \iff \text{pgcd}(m, n) = 1$, par Bézout.

$\lrcorner$

□

En résumé: Sont équivalents

(a) $\mathbb{Z}/n\mathbb{Z}$ est intègre.

(b) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

(c) n est premier

Remarque: Vu en ex. S6: A fini, alors A intègre $\implies$ A un corps. Faux si A est infini, par exemple $A = \mathbb{Z}$ intègre, pas un corps.

Notation

Si $n = p$ premier, on notera $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ le corps des entiers modulo p.

6. Si A_1, A_2 sont 2 anneaux non-nuls, alors $A_1 \times A_2$ n'est pas intègre ($a = (1,0), b = (0,1)$), $a \cdot b = (0,0)0_{A_1 \times A_2}$, $a \neq 0, b \neq 0$ car $A_1 \neq 0, A_2 \neq 0$)
Finalement, $(A_1 \times A_2)^* = A_1^* \times A_2^*$

Une application

Le théorème de Wilson.
Pour $n \geq 2$, considérons $(n-1)!$ modulo n.

n	2	3	4	5	6	7	8	9	10	11	$\cdots$
$(n-1)!$	1	2	6	24	120	720	5040	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(n-1)! \pmod n$	1	2	2	4	0	6	0	0	0	10	$\cdots$

Théorème de Wilson

Un entier $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1 \pmod n$.

Preuve:
[$\Longleftarrow$]: Soit donc $n \geq 2$ avec $(n-1)! \equiv -1 \pmod n$, et soit $1 \leq d < n$ tel que $d \mid n$. A voir: $d = 1 (\implies n$ premier)

On a $(n-1)! \equiv -1 \pmod n \iff \left.\begin{array}{l} n \mid (n-1)! + 1 \\ d \mid n \end{array}\right\} \implies d \mid (n-1)! + 1.$

$d \leq n-1 \implies d \mid (n-1)!$
Ces deux points impliquent: $\implies d \mid ((n-1)! + 1) - (n-1)!$ ie: $d \mid 1$, et donc $d = 1$.
(En fait si $n > 4$ est non-premier, alors $(n-1)! \equiv 0 \pmod n$: ex3, S7)

[$\Longrightarrow$]: Supposons $n = p$ premier. Si $p = 2$, ça marche. On suppose donc $p > 2$.
On veut calculer $[(p-1)!] = [1 \cdot 2 \cdot 3 \cdots (p-1)] = [1][2][3] \cdots [p-1] \in \mathbb{Z}/p\mathbb{Z}$. C'est le produit de tous les éléments de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ (puisque $\left(\mathbb{Z}/p\mathbb{Z}\right)^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$). Dans ce produit, chaque a possède un inverse a^{-1} tel que $aa^{-1} = 1$. On obtient:

$$[(p-1)!] = \prod_{a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^*} a \overset{aa^{-1}=1}{=} \prod_{\substack{a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^* \\ tq\ a = a^{-1}}} a$$

Mais dans $\mathbb{Z}/p\mathbb{Z}$, on a: $a = a^{-1} \iff a^2 = 1 \iff a^2 - 1 = 0 \iff (a+1)(a-1) = 0 \underset{\mathbb{Z}/p\mathbb{Z} \text{ intègre}}{\iff} a+1 = 0$ ou $a - 1 = 0 \iff a = -1$ ou $a = +1$.

On a donc: $[(p-1)!] = (+1)(-1) = -1 \in \mathbb{Z}/p\mathbb{Z}$, donc: $(p-1)! \equiv -1 \pmod{p}$.

□

2.2 Homomorphismes d'anneaux

Définition

Une application $\varphi : A \to A'$ entre deux anneaux est un homomorphisme d'anneaux si:

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \qquad \forall a, b \in A \quad \text{et} \quad \varphi(1_A) = 1_{A'}$$

Remarques et terminologie

1. La première condition signifie que $\varphi : (A,+) \to (A',+)$ est un homomorphisme de groupes. En particulier, on aura $\varphi(0_A) = 0_{A'}$ et $\varphi(-a) = -\varphi(a) \quad \forall a \in A$.

2. Les deux premieres conditions n'impliquent pas la 3ème en général. Par exemple: $\varphi(a) = 0 \quad \forall a \in A \qquad (A' \neq 0)$ (Voir ausis ex4 et ex6, Série 7)

3. Si $\varphi : A \to A'$ est un homomorphisme, et si $a \in A^*$, alors $\varphi(a) \in (A')^*$

   $$\Big(a \in A^* \iff \exists b \in A \text{ tq } ab = ba = 1_A \implies 1_{A'} = \varphi(1_A) = \left.\begin{matrix} \varphi(ab) = \varphi(a)\varphi(b) \\ \varphi(ba) = \varphi(b)\varphi(a) \end{matrix}\right\} \implies \varphi(a) \in (A')^*,$$

   avec inverse $\varphi(b).\Big)$
   Ainsi, $\varphi|_{A^*}: A^* \to (A')^*$ est un homomorphisme de groupes par la multiplication.

4. $\varphi : A \to A', \psi : A' \to A''$ homomorphismes $\implies \psi \circ \varphi : A \to A''$ homomorphisme.

5. On défini le noyau et l'image de $\varphi : A \to A'$ par $\operatorname{Ker}(\varphi) = \{a \in | \ \varphi(a) = 0\}$, $\operatorname{Im}(\varphi) = \{\varphi(a) \mid a \in A\}$.
   Par Prop. I.2: $\operatorname{Ker}\varphi$ est un sous-groupe de $(A,+)$, φ inj $\iff \operatorname{Ker}\varphi = 0$. $\operatorname{Im}\varphi$ est un sous groupe de $(A'.+), \varphi$ surj $\iff \operatorname{Im}\varphi = A'$
   En fait: $\operatorname{Im}\varphi$ est un sous-anneau de A'.

   ⌜

   $$1_{A'} = \varphi(1_{A'}) \in \operatorname{Im}\varphi$$
   $$\varphi(a), \varphi(b) \in \operatorname{Im}\varphi \implies \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{Im}\varphi$$

   ⌟

   Par contre, $\operatorname{Ker}\varphi$ n'est pas un sous-anneau de A! En effet $1_A \notin \operatorname{Ker}\varphi$ (puisque $\varphi(1_A) = 1_{A'} \neq 0$, sauf si $A' = 0$)
   On reviendra à la "nature" exacte des noyaux plus tard.

6. Un isomorphisme d'anneaux est un homomorphisme $\varphi : A \to A'$ tel qu'il existe un homomorphisme $\psi : A' \to A$ avec $\psi \circ \varphi = id_{[}A]$ et $\varphi \circ \psi = id_{[}A']$.
   (C'est équivalent à : φ est un homomorphisme bijectif, comme pour les groupes)

   Si $\varphi : A \to A'$ est un isomorphisme d'anneaux, alors $\varphi|_{A^*}: A^* \to (A')^*$ est un isomorphisme de groupes.
   Toutes les remarques sur les isomorphismes de groupes se transposent aux isomorphismes d'anneaux.

Exemples d'homomorphismes (d'anneaux)

1. $id_{[}A] : A \to A$ est un homomorphisme.

2. Si $B \subset A$ est un sous-anneau, l'inclusion $\varphi : \begin{array}{ccc} B & \longrightarrow & A \\ b & \longmapsto & \varphi(b) \end{array}$ est un homomorphisme.
   En particulier, on a des homomorphismes $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ donnés par les inclusions.

3. $\varphi : \begin{array}{ccc} \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ dérivable } \} & \longrightarrow & \mathbb{R} \\ f & \longmapsto & \varphi(f) = f(x_0) \end{array}$, pour $x_0 \in \mathbb{R}$ fixé.
   φ est un homomorphisme:
   - $\varphi(f+g) = (f+g)(x_0) = f(x_0) + g(x_0) = \varphi(f) + \varphi(g)$
   - Idem pour la multiplication.
   - $1_A(x) = 1 \; \forall x \in \mathbb{R} \implies \varphi(1_A) = 1_A(x_0) = 1$

   Son noyau: $\operatorname{Ker} \varphi = \{f \mid f(x_0) = 0\}$.

4. $A = M_n(\mathbb{K})$, $P \in \mathrm{GL}(n, \mathbb{K})$ fixé, alors $\varphi : \begin{array}{ccc} A & \longrightarrow & A \\ M & \longmapsto & PMP^{-1} \end{array}$ est un isomorphisme (ex5, S7).
   On dit que φ est un <u>automorphisme</u> de A.

5. $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ a & \longmapsto & [a] \end{array}$ est un homomorphisme d'anneaux.

Proposition II.1

Pour tout anneau A, il existe un unique homomorphisme d'anneaux $\varphi : \mathbb{Z} \to A$.

<u>Preuve:</u>
Soit A un anneau, et $\varphi : \mathbb{Z} \to A$ un homomorphisme.

Pour $n \in \mathbb{Z}_{>0}$, on a $\varphi(n) = \varphi(\overbrace{1 + \cdots + 1}^{n}) = \overbrace{\varphi(1) + \cdots + \varphi(1)}^{n} = \overbrace{1_A + \cdots + 1_A}^{n} \overset{\text{not.}}{=:} n \cdot 1_A$
Pour $n \in \mathbb{Z}_{<0}$, on a $\varphi(n) = \varphi\big(\underbrace{(-1) + \cdots + (-1)}_{|n|}\big) = \underbrace{\varphi(-1) + \cdots + \varphi(-1)}_{|n|} = \underbrace{(-1_A) + \cdots + (-1_A)}_{|n|} \overset{\text{not.}}{=:} n \cdot 1_A$
Pour $n = 0$, $\varphi(0) = 0_A = 0 \cdot 1_A$

Ainsi, si $\varphi : \mathbb{Z} \to A$ est un homomorphisme, on a forcément $\varphi(n) = n \cdot 1_A \quad \forall n \in \mathbb{Z}$.
Vérifions encore que cette formule définit bien un homomorphisme d'anneau. Cela découle de la remarque 7 après la définition d'un anneau:

$$\begin{aligned} \varphi(n+m) &= (n+m) \cdot 1_A \overset{\text{rem. } 7}{=} n \cdot 1_A + m \cdot 1_A = \varphi(n) + \varphi(m) \\ \varphi(nm) &= (nm)1_A \overset{\text{rem. } 7}{=} n(m \cdot 1_A) = n \cdot \varphi(m) = n \cdot (1_A \varphi(m)) \overset{\text{rem. } 7}{=} (n1_A)\varphi(m) = \varphi(n)\varphi(m) \\ \varphi(1) &= 1 \cdot 1_A = 1_A \end{aligned}$$

□

Ainsi, tout anneau A possède un unique homomorphisme $\varphi : \mathbb{Z} \to A$, d'où un noyau $\operatorname{Ker} \varphi < \mathbb{Z}$ uniquement associé à A, d'où un entrier $n \in \{0, 1, 2, \ldots\}$ uniquement associé à A!

Terminologie

Cet entier n est appelé la caractéristique de A, noté $\text{car}(A)$.

En clair

- $\star$ $\text{car}(A) = 0 \iff \text{Ker}\,\varphi = \{0\} \iff \varphi : \mathbb{Z} \to A$ injectif

  Dans ce cas, $\overbrace{1_A + \cdots + 1_A}^{n} \neq 0 \quad \forall n > 0$

- $\star$ $\text{car}(A) = n > 0 \iff \underbrace{1_A + \cdots + 1_A}_{n} = 0$ pour $n = \text{car}(A)$, et c'est le plus petit entier tel que c'est le cas.

Exemples

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ont caractéristique 0.
2. $\mathbb{Z}/n\mathbb{Z}$ a caractéristique n: $\underbrace{[1] + \cdots + [1]}_{n} = [n] = [0]$

Proposition II.2

Si A est un anneau intègre, alors $\text{car}(A)$ est soit nulle, soit un nombre premier.

Preuve:
Supposons que $n = \text{car}(A) > 0$, mais pas premier. A voir: A n'est pas intègre.

Si $n > 0$ n'est n'est pas premier, il existe $1 < r,\ s < n$ tels que $r \cdot s = n$

Calculons: $0 = n \cdot 1_A = (rs) \cdot 1_A = (\overbrace{1_A + \cdots + 1_A}^{r \cdot s}) = (\overbrace{1_A + \cdots + 1_A}^{r}) \cdot (\overbrace{1_A + \cdots + 1_A}^{s}) = \underbrace{(r1_A)}_{=:a} \cdot \underbrace{(s1_A)}_{=:b}$

On a donc $ab = 0$, mais $a \neq 0$ car $r < n$ et n est le plus petit entier tel que $n \cdot 1_A = 0$ et $b \neq 0$ pour la même raison. Donc, A n'est pas intègre.

□

Corollaire II.3

Un corps a caractéristique nulle ou un premier.

Démonstration:
Direct par Proposition précédente.

□

Proposition II.4

Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors la caractéristique de A' divise celle de A.

Preuve:
Soit donc $\varphi : A \to A'$ un homomorphisme d'anneaux, et $\varepsilon : \mathbb{Z} \to A$, $\varepsilon' : \mathbb{Z} \to A'$
φ et ε sont des homomorphismes $\implies \varphi \circ \varepsilon : \mathbb{Z} \to A'$ est un homomorphisme $\overset{\text{Prop II.1}}{\implies} \varphi \circ \varepsilon = \varepsilon'$, par unicité.

Si l'on note $n := \text{car}(A),\ n' := \text{car}(A')$, et obtient $n'\mathbb{Z} = \text{Ker}(\varepsilon') = \text{Ker}(\varphi \circ \varepsilon) \supset \text{Ker}(\varepsilon) = n\mathbb{Z}$
On a donc $n\mathbb{Z} \subset n'\mathbb{Z} \implies n \in n'\mathbb{Z} \iff \exists k \in \mathbb{Z}$ tel que $n = n'k \iff n' \mid n$

□

Conséquence

$$A \cong A' \implies \text{car}(A) = \text{car}(A')$$

2.3 Idéaux et anneaux quotients

Au Chapitre I, on a vu que les sous-groupes normaux sont importants. Ils coïncident avec les noyaux d'homomorphisme de groupes. Qu'en est-il pour les anneaux ? Etudions les noyaux d'homomorphisme d'anneaux.

Lemme II.5

Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors $I := \operatorname{Ker}\varphi$ satisfait:

(i) I est un sous-groupe de $(A, +)$

(ii) Si $x \in I$ et $a \in A$, alors $ax \in I$ et $xa \in I$.

Preuve:

(i) Vu, découle du Chapitre I.

(ii) Soit $x \in I = \operatorname{Ker}\varphi$, et $a \in A$: $\quad \varphi(ax) = \varphi(a)\varphi(x) \overset{x\in\operatorname{Ker}\varphi}{=} \varphi(a)\cdot 0 = 0 \implies ax \in I$ et de même: $xa \in I$.

□

Définition

Soit A un anneau. Un sous-ensemble $I < A$ est appelé un idéal de A si:

(i) I est un sous-groupe de $(A, +)$.

(ii) $\forall x \in I,\ \forall a \in A, \quad ax \in I$ et $xa \in I$.

Exemples d'idéaux

1. Tout anneaux A possède les idéaux suivants: $I = \{0\}$ et $I = A$
   (Un anneau commutatif non-nul est un corps $\iff$ ses seuls idéaux sont ceux-là (Série 8))

2. $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

3. Dans A commutatif. $\forall x \in A,\ I := (x) = \{xa \mid a \in A\} = xA$ est un idéal de A, appelé l'idéal principal engendré par x

   ⌜

   (i) $0 = x \cdot 0 \in I$

   $xa, xb \in I \implies xa - xb \overset{(A4)}{=} x(\overbrace{a-b}^{\in A}) \in I$

   (ii) $xa \in I, a' \in A \implies a'(xa) \overset{A \text{ comm.}}{=} x(\overbrace{a'a}^{\in A}) \in I$
   idem pour $(xa)\cdot a' = x(aa') \in I$

   ⌟

Par exemple, si $A = \mathbb{Z}$ et $x = n$, on obtient $(x) = n\mathbb{Z}$, l'exemple 2. Pour $x = 0$, on a $(0) = \{0\}$; pour $x = 1_A$ on a $(1) = A$ (exemple 1).

4. Par le Lemme II.5, si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors $I = \operatorname{Ker}\varphi$ est un idéal de A.

Remarque

1. Un idéal n'est en général pas un sous-anneau (par ex: $I = 2\mathbb{Z}$ pas un sous-anneau de $\mathbb{Z}$ car $1 \notin 2\mathbb{Z}$)

2. Un sous-anneau n'est en général pas un idéal.

3. Si φ est un homomorphisme, $\operatorname{Im}(\varphi)$ n'est pas un idéal.

Exemple pour (2, 3): $\varphi : \mathbb{Z} \to \mathbb{Q}$ l'inclusion $\operatorname{Im}\varphi = \mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, mais pas un idéal!
$n \in \mathbb{Z},\ a \in \mathbb{Q} \not\Rightarrow an \in \mathbb{Z}$

Comme un idéal $I \subset A$ est un sous-groupe de $(A, +)$ abélien, on a le groupe quotient:

$$A/I := \{a + I \mid a \in A\} = \{[a] \mid a \in A\}, \quad \text{où} \quad a \sim b \iff a - b \in I$$

Par le théorie du Chapitre I, on sait que A/I est un groupe abélien pour $[a]+[b] := [a+b]$, et $\pi : A \to A/I$, $\pi(a) = [a]$, est un homomorphisme de groupes.
De plus:

Proposition II.6

Si I est un idéal de A, alors A/I est un anneau pour $[a]+[b] := [a+b]$ et $[a]\cdot[b] := [a\cdot b]$. De plus, $\pi : A \to A/I$ est un homomorphisme d'anneaux.

Preuve:
Le fait que A/I est un groupe abélien est déjà connu, mais on va refaire la preuve que $+$ est bien définie.

$$\begin{array}{rcl} [a] = [a'] \\ [b] = [b'] \end{array} \iff \begin{array}{rcl} a' - a \in I \\ b' - b \in I \end{array} \implies (a' + b') - (a + b) = \overbrace{(a' - a)}^{\in I} + \overbrace{(b' - b)}^{\in I} \in I$$

$$\iff [a' + b'] = [a + b] \implies [a] + [b] := [a + b] \quad \text{est bien définie}$$

On obtient immédiatement que $\left(A/I\ , +\right)$ est un groupe abélien et π est un homomorphisme de groupes.

Vérifions que la multiplication est bien définie:

$$\begin{array}{ccccc} [a] & = & [a'] & \iff & a'-a \in I \\ [b] & = & [b'] & & b'-b \in I \end{array} \iff \exists x,y \in I \text{ tq. } a'=a+x,\ b'=b+y \quad \text{à voir:} \quad [ab]=[a'b']$$

$$\begin{aligned} a'b'-ab &= (a+x)(b+y)-ab \overset{(A4)}{=} a(b+y)+x(b+y)-ab \overset{(A4)}{=} ab+ay+xb+xy-ab \\ &= ay+xb+xy \in I \quad \text{par l'axiome (ii)} \end{aligned}$$

Les axiomes $(A2)$, $(A3)$, $(A4)$ se traduisent directement de A à A/I
Par exemple: $1_{A/I} = [1_A]$ car $1_{A/I} \cdot [a] = [1_A] \cdot [a] = [1_A \cdot a] = [a]$
Finalement, π est un homomorphisme d'anneaux, car:

$$\pi(a \cdot b) \overset{def.}{=} [a \cdot b] = [a][b] \overset{def.}{=} \pi(a) \cdot \pi(b) \quad \forall a,b \in A$$

et:

$$\pi(1_A) = [1_A] = 1_{A/I}$$

□

Remarque

Les ideaux de A sont exactement les noyaux d'homomorphisme d'anneaux $A \to A'$.

Exemples d'anneaux quotients

1. $I = \{0\} \subset A \implies A/I = A/\{0\} = A \qquad ([a]=[b] \iff a \sim b \iff a-b \in \{0\} \iff a=b)$
2. $I = A \implies A/I = A/A = 0$, l'anneau trivial ($[a]=[b] \iff a-b \in A$, toujours vrai)
3. $I = n\mathbb{Z} \subset \mathbb{Z} = A \implies A/I = \mathbb{Z}/n\mathbb{Z}$ l'anneau des entiers modulo n.
4. Plus genéralement: si A est commutatif, $x \in A$, $I = (x)$, on obtient l'anneau commutatif $A/(x)$, où $[a]=[b] \iff a-b \in xA$
   (source très riche de nouveaux anneaux)

Proposition II.7

Soit $\varphi : A \to A'$ un homomorphisme d'anneaux, $I \subset A$ un idéal, tel que $I \subset \operatorname{Ker}\varphi$. Alors, il existe un unique homomorphisme d'anneaux $\overline{\varphi} : A/I \to A'$ tel que $\overline{\varphi}([a]) = \varphi(a)$, $\forall a \in A$.

Preuve:
Par Proposition I.8, il existe un unique homomorphisme de groupes $\overline{\varphi} : A/I \to A'$ tel que $\overline{\varphi}([a]) = \varphi(a)$ $(\overline{\varphi} \circ \pi = \varphi)$
Reste à verifier que $\overline{\varphi}$ est un homomorphisme d'anneaux:

$$\overline{\varphi}([a] \cdot [b]) = \overline{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}([a])\overline{\varphi}([b])$$

et pour l'élement neutre: $\overline{\varphi}(1_{A/I}) = \overline{\varphi}([1_A]) = \varphi(1_A) = 1_{A'}$

□

Proposition II.8

Tout homomorphisme d'anneaux $\varphi : A \to A'$ définit un isomorphisme d'anneaux

$$\overline{\varphi} : {}^{A}\!\Big/_{\operatorname{Ker}\varphi} \to \operatorname{Im}\varphi$$

Preuve:
Par Prop I.9, on sait que φ définit $\overline{\varphi}$ isomorphisme de groupes.
Par Prop II.7, $\overline{\varphi}$ est un homomorphisme d'anneaux
$\Longrightarrow$ $\overline{\varphi}$ homomorphisme d'anneaux bijectif $\Longleftrightarrow$ $\overline{\varphi}$ isomorphisme d'anneaux.

□

Exemple

Soit A un anneau quelconque, et $\varphi : \mathbb{Z} \to A$ l'homomorphisme donné en Prop II.1

- ⋆ Si $\operatorname{car}(A) = 0$, alors $\operatorname{Ker}\varphi = 0 \implies \varphi$ injectif $\implies \varphi : \mathbb{Z} \to \varphi(\mathbb{Z})$ est un isomorphisme d'anneaux
  $\implies A$ contient un sous-anneau isomorphe à $\mathbb{Z}$ (le sous anneau $\varphi(\mathbb{Z})$)

- ⋆ Si $\operatorname{car}(A) = n > 0$, alors $\operatorname{Ker}\varphi = n\mathbb{Z}$.
  Par la Prop II.8, on a un isomorphisme d'anneaux $\overline{\varphi} : {}^{\mathbb{Z}}\!\Big/_{n\mathbb{Z}} \to \varphi(\mathbb{Z}) \subset A \implies A$ contient un sous-anneau isomorphe à ${}^{\mathbb{Z}}\!\Big/_{n\mathbb{Z}}$

2.4 Corps des fractions d'un anneau intègre

L'anneau intègre $A = \mathbb{Z}$ n'est pas un corps. Mais, il existe un corps $K = \mathbb{Q}$ et un homomorphisme d'anneaux injectif $\mathbb{Z} \to \mathbb{Q}$ (l'inclusion); on parle de plongement: $A \to K$.

Notons que s'il existe un plongement de $A \neq 0$ dans un corps K, alors A est intègre! Et en fait, c'est possible dès que A est intègre!

Théorème II.9

Pour tout anneau intègre A, il existe un corps $Q(A)$ et un homomorphisme d'anneaux injectif (=plongement) $i : A \to Q(A)$

Réfléchissons à la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ (vu en logique), et tentons de l'étendre.

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} - \{0\}) \Big/ \sim$$

où $(a,b) \sim (c,d) \iff ad = bc$: penser à (a,b) comme $\frac{a}{b}$ $\left(\frac{a}{b} = \frac{c}{d} \iff ad = bc\right)$.
Notons $[a,b]$ la classe de (a,b). On définit les opérations:
$[a,b] + [c,d] = [ad + bc, bd] \rightsquigarrow \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
$[a,b] \cdot [c,d] = [ac, bd] \rightsquigarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
On vérifie que c'est bien défini, et que cela donne un corps.

Preuve du théorème II.9
Soit A un anneau intègre. Posons $X := A \times (A - \{0\})$, et $(a,b) \sim (c,d) \in X \iff ad = bc \in A$
C'est une relation d'équivalence:

- $(a,b) \sim (a,b) \iff ab = ba \in A$: ✓car A commutatif
- $\left.\begin{array}{l}(a,b) \sim (c,d) \iff ad = bc \\ (c,d) \sim (a,b) \iff cb = da\end{array}\right\}$, équations équivalentes dans A commutatif.
- $$\left.\begin{array}{l}(a,b) \sim (c,d) \iff ad = bc \\ (c,d) \sim (e,f) \iff cf = de\end{array}\right\} \implies b(de) = b(cf) = (bc)f = (ad)f$$
$$\iff d(be) = d(af) \underset{\substack{d \neq 0 \\ A \text{ intègre}}}{\implies} be = af \iff (a,b) \sim (e,f)$$

C'est bien une relation d'équivalence.

Posons $Q(A) := X \Big/ \sim \; = \{[a,b] \mid (a,b) \in X\}$ et notons $[a,b] \in Q(A)$ la classe d'équivalence de $(a,b) \in X$ (y penser comme $\frac{a}{b}$).

- L'addition dans $Q(A)$ est définie par $[a,b] + [c,d] := [ad + bc, bd]$
  C'est bien défini: $b \neq 0,\ d \neq 0 \implies bd \neq 0$ car A est intègre.

$$\left.\begin{array}{l}[a',b']=[a,b] \iff a'b=b'a\\ [c',d']=[c,d] \iff c'd=d'c\end{array}\right\} \overset{?}{\implies} [a'd'+b'c',b'd']=[ad+bc,bd]$$

$$\iff (a'd'+b'c')bd=b'd'(ad+bc)$$

$$a'd'bd+b'c'bd=(a'b)dd'+(c'd)bb'=(b'a)dd'+(d'c)bb'=b'd'ad+b'd'ad+b'd'bc$$

Donc ça marche

- $(Q(A),+)$ est un groupe abélien:
  - Associativité, Ex 4, S8
  - Le neutre est $0=[0,1]$ $(=[0,b],\ b\neq 0)$: $[0,1]+[a,b]=[0\cdot b+1\cdot a,1\cdot b]=[a,b]$
  - L'inverse additif de $[a,b]$ est $[-a,b]$: $[a,b]+[-a,b]=[ab+b(-a),b^2]=[0,b^2]=[0,1]$
  - $[a,b]+[c,d]=[c,d]+[a,b]$: Par simple définition.
- La Multiplication dans $Q(A)$ est définie par $[a,b]\cdot[c,d]=[ac,bd]$
  <u>C'est bien défini:</u> $b\neq 0,\ d\neq 0 \implies bd\neq 0$ car A intègre.

$$\left.\begin{array}{l}[a',b']=[a,b] \iff a'b=b'a\\ [c',d']=[c,d] \iff c'd=d'c\end{array}\right\} \overset{?}{\implies} [a'c',b'd']=[ac,bd]$$

$$\iff a'c'bd=b'd'ac$$

$$a'c'bd=(a'b)(c'd)=(b'a)(d'c)=b'd'ac$$

Donc ça marche.

- $(Q(A),+,\cdot)$ est un anneau commutatif

(A1) Vu.

(A2) Découle de (A2) pour l'anneau A.

(A3) L'unité est $1_{Q(A)}:=[1_A,1_A]$ $(=[b,b],\ b\neq 0)$: $[a,b]\cdot[1,1]=[a\cdot 1,b\cdot 1]=[a,b]$

(A4) Découle de (A4) pour A.

<u>Commutatif:</u> Car A est commutatif.

<u>C'est un corps:</u> Si $[a,b]\neq 0\in Q(A)$, cela signifie $[a,b]\neq[0,1]$ ic: $a\cdot 1\neq b\cdot 0=0$ ie: $a\neq 0$
Son inverse est $[b,a]$ (possible car $a\neq 0$): $[a,b]\cdot[b,a]=[ab,ab]=1_{Q(A)}$

<u>On a un plongement $i:\ A\to Q(A)$:</u> $i(a)=[a,1]$ C'est un plongement:

- $i(a+b)=[a+b,1]=[a,1]+[b,1]=i(a)+i(b)$
- $i(a\cdot b)=[ab,1]=[a,1]\cdot[b,1]=i(a)\cdot i(b)$
- $i(1_A)=[1_A,1_A]=1_{Q(A)}$

<u>i est injective:</u> Soient $a,b\in A$ tels que $i(a)=i(b)$, ie: $[a,1]=[b,1] \iff a\cdot 1=1\cdot b \iff a=b$

□

Terminologie

$Q(A)$ est le corps des fractions de A.

Exemples

1. $A = \mathbb{Z} \implies Q(A) = \mathbb{Q}$

2. Si A est un corps, alors $i : A \to Q(A)$ est un isomorphisme d'anneaux (corps).
   En effet: Soit $[a, b] \in Q(A)$; $b \neq 0 \in A$ un corps $\implies \exists b^{-1} \in A$ tel que $b^{-1}b = 1$. On a donc $ab^{-1} \in A$ tel que $i(ab^{-1}) = [ab^{-1}, 1] = [a, b]$ car $ab^{-1} \cdot b = a \cdot 1$.
   $\implies i$ est surjectif $\implies i$ bijectif $\implies i$ isomorphisme.

3. D'autres exemples à venir.

Remarque (Ex.5, S.8)

$\forall$ plongement $\varphi : A \to K$, K un corps, il existe un plongement $\overline{\varphi} : Q(A) \to K$ tel que $\overline{\varphi} \circ i = \varphi$

2.5 Anneaux euclidiens

Définition

Un anneau intègre A est un anneau euclidien s'il existe une application $f : A - \{0\} \to \{1, 2, 3, \ldots\}$ telle que:

1. $f(a) \leq f(ab) \quad \forall a, b \in A - \{0\}$

2. Pour tous $a, b \in A - \{0\}$, il existe $q, r \in A$ tel que $a = qb + r$ avec $r = 0$ ou $f(r) < f(b)$.

Remarque

Voir ex.6, S.8: Le point 2 est le point crucial.

Exemples

1. $A = \mathbb{Z}$ avec $f : \begin{array}{ccc} \mathbb{Z} - \{0\} & \longrightarrow & \{1, 2, 3, \ldots\} \\ n & \longmapsto & |n| \end{array}$. C'est l'algorithme de division euclidienne !

2. Si A est un corps, c'est un anneau euclidien (pour $f \equiv 1$):
   $\forall a, b \in A - \{0\}$, on pose $q = ab^{-1}$ et $r = 0$: $(a = q \cdot b + e)$

3. D'autres exemples plus tard.

En Prop I.10, on avait utilisé la division euclidienne (dans $\mathbb{Z}$) pour montrer:
Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$. Voici la généralisation (même preuve).

Proposition II.10

Soit I un idéal dans un anneau euclidien A. Alors, il existe $x \in A$ tel que $I = (x) := \{xa \mid a \in A\}$.

Preuve:
Soit donc $I \subset A$ un idéal. Si $I = \{0\}$, on choisit $x = 0$, OK.

On suppose donc $I \neq \{0\}$.
Choisissons $x \in I - \{0\}$ qui minimise f sur $I - \{0\}$ ($\forall y \in I - \{0\}$, $f(x) \leq f(y)$)
Affirmation: $I = (x)$
En effet:

$[\supset]$ $x \in I \overset{I \text{ idéal}}{\Longrightarrow} xa \in I \quad \forall a \in A \implies (x) \subset I$.

$[\subset]$ Soit donc $y \in I$, $y \neq 0$. Par l'axiome 2 d'un anneau euclidien, $\exists q, r \in A$ tel que $y = qx + r$ avec $r = 0$ ou $f(r) < f(x)$.

$x \in I$, $q \in A \implies \left.\begin{array}{c} qx \in I \\ y \in I \end{array}\right\} \implies r = y - qx \in I \implies r = 0$, car $f(r) < f(x)$ est impossible par minimalité.

Ainsi, $r = 0 \implies y = qx$, et donc $y \in (x)$.

□

Remarque

Un anneau intègre tel que tout idéal est de la forme (x) est un anneau principal.
Ainsi, cette proposition dit: A euclidien $\implies$ A principal.
(On verra un anneau non-principal en fin de Chapitre II)

On va généraliser et étudier les notions suivantes:

(A) Divisibilité

(B) pgcd

(C) élément premier

(A) Terminologie

Soient $a, b \in A$ avec A commutatif. On dit que a divise b, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. Dans le cas contraire, on note $a \nmid b$

Exemples

1. Dans $A = \mathbb{Z}$, on a $2 \nmid 3$, car il n'existe pas $n \in \mathbb{Z}$ tel que $3 = 2 \cdot n$. Mais dans $A = \mathbb{Q}$, on a $2 \mid 3$, car il existe $c = \dfrac{3}{2} \in \mathbb{Q}$ tel que $3 = 2 \cdot c$.

2. Si $A = K$ est un corps, alors tout $a \neq 0$ divise tout b! On pose $c = a^{-1}b$.

Remarques

1. $a \mid b,\ b \mid c \implies a \mid c$

2. $a \mid b,\ a \mid c \implies a \mid (b + c)$

3. $a \mid b \implies a \mid bx \quad \forall x \in A$

4. $a \mid b,\ u \in A^* \implies au \mid b$

5. $a \mid b \iff (b) \subset (a)$

(Voir ex. 7, S.8)

Proposition II.11

Pour $a, b \in A$ avec A intègre, les énoncés suivants sont équivalents:

(i) $a \mid b$ et $b \mid a$

(ii) $(a) = (b)$

(iii) $\exists u \in A^*$ tel que $b = au$

(On dit alors que a et b sont associés, voir ex.8, S.8)

Preuve:
(i) $\iff$ (ii): Par la remarque 5 ci-dessus.
(iii) $\implies$ (i): Supposons $b = a \cdot u$ avec $u \in A^*$. Alors $a \mid b$ par définition et $a = b \cdot u^{-1} \implies b \mid a$
(i) $\implies$ (iii): Supposons $a \mid b$ et $b \mid a$, donc $\exists c, d \in A$ tels que $b = ac$ et $a = bd$.

$$\implies a = bd = (ac)d \implies 0 = a - acd = a(1 - cd)$$

A intègre $\implies$

- soit $a = 0$, et alors $b = 0$ et (iii) est vérifié.
- soit $1 - cd = 0$, et alors $cd = 1$, d'où $c, d \in A^*$, d'où $b = ac$ avec $c \in A^*$, et (iii) est vérifié.

□

Exemple

1. Dans $A = \mathbb{Z}$, m, n sont associés $\iff m = \pm n$

2. Dans $A = K$ corps ?

(B) Terminologie

Si on a deux éléments $a, b \in A$ anneau commutatif, alors un plus grand commun diviseur de a et b, noté $\text{pgcd}(a, b)$ est un élément $d \in A$ tel que:

- $d \mid a$ et $d \mid b$

- Si $c \in A$ est tel que $c \mid a$ et $c \mid b$ alors $c \mid d$

Remarques

1. Si d est un pgcd de a et b, alors $d \cdot u$ aussi $\forall u \in A^*$

   ⌜

   $$d \mid a,\ d \mid b \quad u \in A^* \implies du \mid a,\ du \mid b$$

   Et si $c \in A$ tel que $c \mid a$:

   $$c \mid b \implies c \mid d \implies c \mid du$$

   ⌟

2. Réciproquement si A est intègre alors deux pgcd d et d' de a et b sont forcément associés ($\exists u \in A^*$ tel que $d' = d \cdot u$)

$$\left.\begin{array}{lll} d \mid a,\ d \mid b & \Longrightarrow & d \mid d' \\ d' \mid a,\ d' \mid b & \Longrightarrow & d' \mid d \end{array}\right\} \Longrightarrow d \text{ et } d' \text{ sont associés.}$$

Exemple

Dans $\mathbb{Z}$, deux pgcd de $a, b \in \mathbb{Z}$ fixés sont égaux a multiplication par élément de $\mathbb{Z}^* = \{-1, 1\}$ près ! (Donc au signe près)
Dans ce cas il est naturel de définir le pgcd comme celui qui est ≥ 0. Mais cela ne fait pas de sens sur A quelconque qui n'est pas forcément muni d'un ordre "$\geq$", d'où "un" pgcd.

Qu'en est-il de l'existence d'un pgcd ?
Dans un anneau euclidien, on a la généralisation suivante de I.12 (Bézout):

Proposition II.12

Soit A un anneau euclidien et $a, b \in A$ fixés.
Alors il existe un pgcd $d \in A$ et a et b. Il existe de plus $\lambda, \mu \in A$ tels que $\lambda a + \mu b = d$

Preuve:
Soient donc $a, b \in A$ fixés. Considérons

$$I := \{ra + s \cdot b \mid r, s \in A\} \subset A$$

C'est un idéal de A:

- $0 = 0 \cdot a + a \cdot b \in I$, d'où $I \neq \varnothing$

- $\left.\begin{array}{ll} ra + sb & \in I \\ r'a + s'b & \in I \end{array}\right\} \Longrightarrow (ra + sb) - (r'a + s'b) = (\underbrace{r - r'}_{\in A})a + (\underbrace{s - s'}_{\in A})b \in I$

Ainsi $I < (A, +)$

- Si $ra + sb \in I$ et $x \in A$ alors $x \cdot (ra + sb) = (\underbrace{xr}_{\in A})a + (\underbrace{xs}_{\in A})b \in I$

C'est donc bien un idéal de A. Comme A est euclidien par Prop II.10, il existe $d \in A$ tel que $I = (d) = \{xd \mid x \in A\}$
Affirmation: d est un pgcd de a et b.

$$\left.\begin{array}{l} a = 1 \cdot 1 + 0 \cdot b \ \in \ I = (d) \Longrightarrow d \mid a \\ b = 0 \cdot a + 1 \cdot b \ \in \ I = (d) \Longrightarrow d \mid b \\ \text{Soit } c \in A \text{ tq } c \mid a \text{ et } c \mid b \Longrightarrow c \mid (ra + sb)\ \forall r, s \in A \Longrightarrow c \mid x\ \forall x \in I \Longrightarrow c \mid d \end{array}\right\} \ d \text{ est un pgcd de } a \text{ et } b.$$

Finalement, $d \in (d) = I = \{ra + sb \mid r, s \in A\} \Longrightarrow \exists \lambda, \mu \in A$ tels que $d = \lambda a + \mu b$

□

(C) Terminologie

Soit A un anneau intègre et $p \in A$, $p \neq 0$, $p \notin A^*$

- p est irréductible dans A si $p = a \cdot b$ avec $a, b \in A \implies a \in A^*$ ou $b \in A^*$

- p est premier dans A si $p \mid ab$ avec $a, b \in A \implies p \mid a$ ou $p \mid b$.

Exemples

1. Dans $\mathbb{Z}$, $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ est premier $\iff$ p est irréductible $\iff$ les diviseurs de p sont ± 1 et $\pm p$.
   Ainsi ces notions sont des générateurs naturels de la notion de "nombres premiers" dans $\mathbb{Z}$.

2. Dans un corps, comme $A^* \cup \{0\} = A$ on a aucun éléments premier/irreductible.

Proposition II.13

Si $p \in A$ est premier, alors p est irréductible. Réciproquement si A est euclidien, alors p irréductible implique p premier.

Preuve:
Soit donc $p \in A$, $p \neq 0$, $p \notin A^*$ avec p premier.

Soient $a, b \in A$ tels que $p = ab$.
A voir: $a \in A^*$ ou $b \in A^*$

On a $p \mid p \implies p \mid ab \implies p \mid a$ ou $p \mid b$. Supposons sans perte de généralité que $p \mid a$: Donc $\exists c \in A$ tel que $a = pc \implies a = pc = (ab)c = a(bc) \implies 1 = bc \implies b \in A^*$
Cela montre que p est irréductible.
Réciproquement supposons $p \in A$ irréductible, avec A euclidien. Soient $a, b \in A$ tels que $p \mid ab$.
A voir: $p \mid a$ ou $p \mid b$

Supposons sans perte de généralité que $p \nmid a$. Alors tout pgcd de a et p est une unité.

⌜

Soit donc $d \in A$ tel que $d \mid a$ et $d \mid p$, donc $\exists c \in A$ tel que $p = dc \implies c \in A^*$ ou $d \in A^*$
Si $c \in A^*$ alors $d = pc^{-1}$ donc $p \mid d \underset{d \mid a}{\implies} p \mid a$ une contradiction.
On a donc bien $d \in A^*$

⌟

Comme A abélien, par Prop II.12, $\exists \lambda, \mu \in A$ tels que $\lambda a + \mu p = 1$
Ecrivons $b = 1b = (\lambda a + \mu p) \cdot b = \lambda ab + \mu pb$.

$$p \mid ab \implies \left.\begin{matrix} p \mid \lambda ab \\ p \mid \mu pb \end{matrix}\right\} \implies p \mid \big(\lambda ab + \mu pb\big) = b \quad \text{d'où} \quad p \mid b$$

□

But

Nous voulons tenter de généraliser le Théorème fondamental de l'arithémtique aux anneaux euclidiens.

Lemme II.14

Dans un anneau euclidien, la fonction $f: A - \{0\} \to \{1, 2, \ldots\}$ satisfait:

$$f(ab) > f(a) \qquad \forall a, b \in A - \{0\} \quad \text{et} \quad b \notin A^*$$

Preuve:
Par la première condition dans la définition d'un anneau euclidien on a:

$$f(a) \leq f(ax) \qquad \forall ax \neq 0$$

Fixons $a \neq 0 \in A$, on a donc si l'on pose $I := (a)$, $f(a) = \min\{f(ax) \mid x \in A - \{0\}\}$ i.e: $f(a) = \min\{f(y) \mid y \in I, y \neq 0\}$
Comme $ab \in I$ on a $f(a) \leq f(ab)$. Supposons par l'absurde que $f(a) = f(ab)$:
Donc on a: $f(ab) = f(a) = \min\{f(y) \mid y \in I - \{0\}\}$
Par l'argument dans la preuve de la propostition II.10: $I = (ab)$
On a donc $(a) = (ab) \implies \exists x \in A$ tel que $a = abx \implies bx = 1 \implies b \in A^* \implies$ ↯

□

Théorème II.15

Soit A un anneau euclidien, et soit $a \in A$, $a \neq 0$ et $a \notin A^*$.
Il existe des éléments irréductibles $p_1, \ldots, p_n \in A$ tels que $a = p_1 \cdot \cdots \cdot p_n$.
De plus, si $a = p_1 \cdots p_n = q_1 \cdots q_m$ avec p_i, q_j irréductibles, alors $m = n$ et pout tout $i = 1, \ldots, n$, p_i est associé à $q_{\sigma(i)}$ par une permutation $\sigma \in S_n$

Exemple

$A = \mathbb{Z}$, on obtient alors:
Tout $n > 1$ est produits de nombres premiers, produit unique à l'ordre des facteurs près.

Preuve du Théorème II.15:
Soit donc $a \in A$, $a \neq 0$, $a \notin A^*$, A euclidien.
L'existence d'un décomposition découle immédiatement de:
Affirmation: Tout $a \in A - \{0\}$ est soit une unité, soit le produit d'un nombre fini d'éléments irréductible dans A.

⌜

En effet: On démontre l'affirmation par récurrence sur $f(a) \in \{1, 2, 3, \ldots\}$
Supposons $f(a) = 1$. Alors $a \in A^*$. En effet, si $a \notin A^*$, alors par le lemme II.14:

$$f(a) = f(1 \cdot a) \underset{\text{II.14}}{\overset{a \notin A^*}{>}} f(1) \geq 1 \implies f(a) > 1$$

On a donc $a \notin A^* \implies f(a) > 1$, ce qui est équivalent à $f(a) = 1 \implies a \in A^*$
Supposons l'affirmation vraie pour tout $a' \in A - \{0\}$ tel que $f(a') < f(a)$. Si a est une unité ou un élément irréductible, on a fini !

On peut donc supposer $a \notin A^*$, a non-irreductible. Ainsi, il existe $b, c \in A - \{0\}$ tels que $a = bc$ et

$b \notin A^*$, $c \notin A^*$
Par le lemme II.14, on a $f(b) < f(a)$, $f(c) < f(a)$.
Par hypothèse de récurrence, b et c sont produits d'irréductibles. Ainsi, $a = bc$ est un produit d'irreductible.

⌟

Pour l'unicité, supposons $a = p_1 \cdots p_n = q_1 \cdots q_m$ avec p_i et q_j irréductibles, et donc premiers.
Considérons $p_1 \mid p_1 \cdots p_n = q_1 \cdots q_m$
p_1 premier $\implies \exists j$ tel que $p_1 \mid q_j \implies \exists v_1 \in A$ tel que $q_j = u_1 \cdot p_i$
q_j irréductible $\implies p_1 \in A^*$ ou $u_1 \in A^*$, p_1 irréductible $\implies p_1 \notin A^*$, et donc $u_1 \in A^*$
Ainsi, p_1 est associé à $q_j = q_{\sigma(1)}$.
On a:

$$p_1 p_2 \cdots p_n = q_1 \cdots q_{j-1} u_1 \cdot p_1 q_{j+1} \cdots q_m \overset{\substack{A \text{ intègre} \\ p_1 \neq 0}}{\implies} p_2 \cdots p_n = u_1 \cdot q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$$

On continue, $p_2 = u_2 q_{\sigma(2)}$, $\ldots$, $u_2 \in A^*$, $p_3 = \ldots etc \ldots$

Comme $m \geq n$, on finit avec $1 = u_1 u_2 \ldots u_n q_{jl} q_{jm-n}$ $u_j \in A^*, a_j$ irréductible $\implies$ $q_{jl} \in A^*$, impossible $\implies m - n = 0$, ie: $m = n$

On a donc $m = n$ et $p_i = u_i q_{\sigma(i)}$ $\forall i = 1, \ldots, n$ avec $u_i \in A^*$, $\sigma \in S_n$

□

Remarques

1. Un anneau intègre dans lequel le Théorème II.15 est valide s'appelle un anneau factoriel. Ainsi, ce théorème dit: A euclidien $\implies$ A factoriel.

2. En fait, le théorème plus général suivant est valide:
   A principale $\implies$ A factoriel.

   On a donc les inclusions suivantes:

   $$\{\text{corps}\} \subsetneq \{\text{anneaux euclidiens}\} \subsetneq \{\text{anneaux principaux}\} \subsetneq \{\text{anneaux factoriels}\} \subsetneq \{\text{anneaux intègres}\}$$

2.6 Les entiers de Gauss

Posons:

$$\mathbb{Z}[i] := \{x + iy \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$$

Par l'ex 7, Série 9: c'est un sous-anneau de $\mathbb{C}$, donc un anneau intègre et $\mathbb{Z}[i]^* = \{1, i, -1, -i\}$.
C'est l'anneau des entiers de Gauss.

Théorème II.16

L'anneau $\mathbb{Z}[i]$ est euclidien.

Preuve:

Posons $f : \begin{array}{ccc} \mathbb{Z}[i] - \{0\} & \longrightarrow & \{1, 2, 3, \ldots\} \\ x + iy & \longmapsto & \|x + iy\|^2 = x^2 + y^2 \end{array}$.

On a bien $f(x+iy) \geq 1 \quad \forall x+iy \neq 0$. De plus, pour $a, b \in \mathbb{Z}[i]-\{0\}$, $f(ab) = \|ab\|^2 = \|a\|^2 \cdot \|b\|^2 = f(a)\overbrace{f(b)}^{\geq 1} \geq f(a)$ ce qiu vérifie le premier point. Voyons le second.

Fixons $a, b \in \mathbb{Z} - \{0\}$; on veut trouver $q, r \in \mathbb{Z}[i]$ tels que $a = qb + r$ et $f(r) < f(b)$, ou $r = 0$.
On a $a, b \in (\mathbb{Z}[i] - \{0\}) \subset \mathbb{C}^*$, considérons $\dfrac{a}{b} \in \mathbb{C}^*$, $\dfrac{a}{b} = u + iv$ avec $u, v \in \mathbb{R}$.
$u \in \mathbb{R} \implies \exists x \in \mathbb{Z}$ tel que $|x - u| \leq 1/2$; $v \in \mathbb{R} \implies \exists x \in \mathbb{Z}$ tel que $|y - v| \leq 1/2$.
Posons $q := x + iy \in \mathbb{Z}[i]$ et $r := a - qb \in \mathbb{Z}[i]$
$r = a - qb = b\left(\dfrac{a}{b} - q\right) = b\big((u + iv) - (x + iy)\big) = b\big((u - x) + i(v - y)\big) \implies$ soit $r = 0$, soit:

$$\begin{aligned} f(r) &= f(b) \cdot f\big((u - x) + i(v - y)\big) \\ &= f(b) \cdot \big(\underbrace{(u - x)^2}_{\leq 1/4} + \underbrace{(v - y)^2}_{\leq 1/4}\big) \leq \frac{1}{2} f(b) < f(b) \end{aligned}$$

□

Conséquence

Tout le paragraphe II.5 s'applique à $A = \mathbb{Z}[i]$. Cela implique une preuve d'un théorème de Fermat.

On a besoin de:

Lemme II.17

Soit p un premier de la forme $p = 4n + 1$, $n \in \mathbb{N}$. Alors, il existe $m \in \mathbb{Z}$ tel que $m^2 \equiv -1 \pmod{p}$

Preuve:

Soit donc $p \in \mathbb{N}$ un premier de la forme $p = 4n + 1$, et posons $m := \left(\dfrac{p-1}{2}\right)! \in \mathbb{Z}$. Notons que $\dfrac{p-1}{2}$ est un entier pair.

Calculons $m^2 \pmod p$:

$$\begin{aligned} m^2 &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot (-1)(-2)(-3) \cdots \left(-\frac{p-1}{2}\right) \\ \text{(Par } -k \equiv p-k \pmod p\text{)} &\equiv 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)(p-1)(p-2)(p-3) \cdots \underbrace{\left(p-\left(\frac{p-1}{2}\right)\right)}_{\frac{p+1}{2}=\frac{p-1}{2}+1} \pmod p \\ &= 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right) \cdots (p-3)(p-2)(p-1) = (p-1)! \\ &\equiv (-1) \pmod p \quad \text{Par Wilson, puisque } p \text{ est premier.} \end{aligned}$$

□

Théorème des deux carrés de Fermat

Un premier impair est somme de deux carrés si et seulement si il est congru à 1 modulo 4.

Exemples

$3 \neq x^2+y^2$, $5 = 1^2+2^2, 7 \neq x^2+y^2, 11 \neq x^2+y^2, 13 = 2^2+3^2, \ldots$

Preuve:
[$\Longrightarrow$] : Très facile, voir ex. 2,S. 10.

[$\Longleftarrow$] : [Preuve de Dedekind, 1894]
Soit donc p un premier, $p \equiv 1 \pmod 4$. A voir: $\exists x, y \in \mathbb{Z}$ tels que $p = x^2+y^2$.
Par Lemme II.17, il existe $m \in \mathbb{Z}$ tel que $p \mid m^2+1$ dans $\mathbb{Z}$.
Dans $\mathbb{Z}[i]$, on a $m^2+1 = (m+i)(m-i)$. On a $p \mid (m^2+1) = (m+i)(m-i) \in \mathbb{Z}[i]$, mais $p \nmid m+i$, $p \nmid m-i$ ($p \mid m \pm i \implies \exists x, y \in \mathbb{Z}$ tels que $m \pm i = p(x+iy) \implies \pm i = py$, impossible)
Cela signifie que $p \in \mathbb{Z}[i]$ n'est pas premier ($\Longleftrightarrow$ par irréductible, car $\mathbb{Z}[i]$ euclidien)
$\mathbb{Z}[i]$ euclidien $\implies$ on peut appliquer le Théorème II.15 à l'élément $p \in \mathbb{Z}[i]$. Ainsi, il existe $p_1, \ldots, p_n \in \mathbb{Z}[i]$ irréductibles tels que $p = p_1 p_2 \cdots p_n$, $n \geq 2$ (p par premier dans $\mathbb{Z}[i]$)
Appliquons f à cette égalité:

$$p^2 = f(p) = f(p_1 \cdots p_n) = f(p_1) \cdots f(p_n) \in \mathbb{Z}$$

De plus, $f(p_i) > 1 \quad \forall i$, car $f(p_i) = 1 \implies p_i \in \mathbb{Z}[i]^*$, impossible car p_i est premier.
Comme $p \in \mathbb{Z}$ est premier, l'unicité de la décomposition en premier dans $\mathbb{Z}$ implique $n \leq 2$. On a donc $n = 2$, et $f(p_1) = f(p_2) = p$.

$$p_1 = x + iy \implies p = f(p_1) = x^2+y^2$$

□

2.7 Anneaux de polynômes

Dans tout ce paragraphe, A est un anneau commutatif.
Notons $A[X]$ l'ensembles des symboles $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, avec $a_i \in A$.
Avec $P = a_0 + a_1X + \cdots + a_nX^n$ et $Q = b_0 + b_1X + \cdots + b_mX^m$ qui coïncident si et seulement si $a_i = b_i$, $\forall i \geq 0$.
P est souvent noté: $P = \sum_{i\geq 0} a_iX^i$

- Sur $A[X]$, on définit une addition comme suit:

$$P = \sum_{i\geq 0} a_iX^i,\ Q = \sum_{i\geq 0} b_iX^i \implies P + Q = \sum_{i\geq 0} c_iX^i \quad \text{avec} \quad c_i = a_i + b_i$$

- Sur $A[X]$ on définit une multiplication comme suit:

$$P = \sum_{i\geq 0} a_iX^i,\ Q = \sum_{j\geq 0} b_jX^j \implies PQ = \sum_{k\geq 0} c_kX^k \quad \text{avec} \quad c_k = \sum_{i+j=k} a_ib_j$$

(En clair: on multiplie formellement, et on remplace X^iX^j par X^{i+j}.)

Exemple

$P = 2 + 3X - X^2$, $Q = 1 + 4X + X^2 \in \mathbb{Z}[X]$

$$\begin{aligned} P \cdot Q &= (2 + 3X - X^2)(1 + 4X + X^2) = (2 \cdot 1)(3 \cdot 1 + 2 \cdot 4)X + (2 \cdot 1 + 3 \cdot 4 + (-1)1)X^2 + (3 \cdot 1 + (-1)4)X^3 + ((-1)1)X^4 \\ &= 2 + 11X + 13X^2 - X^3 - X^4 \end{aligned}$$

En exercice: $(A[X], +, \cdot)$ est un anneau commutatif.

Définition

L'anneau $A[X]$ est l'anneau des polynômes (en X) à coefficients dans A.

Terminologie

– Si $P = a_0 + a_1X + \cdots + a_nX^n$ avec $a_n \neq 0$, on dit que $\deg(P) = n$ (si $P = 0$, $\deg(P) = -\infty$)

– Le coefficient a_n est appelé le <u>coefficient dominant</u> de P.

Remarques

1. A est un sous-anneau de $A[X]$, via : $\begin{array}{ccc} A & \longrightarrow & A[X] \\ a & \longmapsto & P = a,\ \text{poly. de degré } 0 \end{array}$, d'où:
   – A^* est un sous-groupe de $A[X]^*$
   – $A[X]$ intègre $\implies$ A intègre.
2. $\deg(P + Q) \leq \max\{\deg P, \deg Q\}$.
3. $\deg(P \cdot Q) \leq \deg(P) + \deg(Q)$
   (Dans $\mathbb{Z}/4\mathbb{Z}\ [X]$, $P = [2]X = Q$, $\deg P = \deg Q = 1$, mais $P \cdot Q = [2][2]X^2 = 0$, donc il n'y a <u>pas</u> d'égalité en général!)

Proposition II.18

Soit A un anneau intègre. Alors:

(i) $A[X]^* = A^*$

(ii) $A[X]$ est intègre.

(iii) $\deg(P \cdot Q) = \deg P + \deg Q$.

Preuve:

(iii) Soient $P = \sum_{i=0}^{n} a_i X^i$, $a_n \neq 0$, $Q = \sum_{j=0}^{m} b_X^j$, $b_m \neq 0$.
$P \cdot Q = \sum_{k \geq 0} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i b_j$.
$\implies c_{n+m} = a_n \cdot b_m$ car $a_i = 0 \; \forall i > n$, $b_j = 0 \; \forall j > m$.
$a_n \neq 0$, $b_m \neq 0$, A intègre $\implies c_{n+m} \neq 0 \implies \deg(P \cdot Q) \geq n + m = \deg(P) + \deg(Q)$.
Comme $\deg(P \cdot Q) \leq \deg P + \deg Q$, on a gagné.

(ii) Soient $P, Q \in A[X]$ avec $P \neq 0$ et $Q \neq 0$.

$\implies \deg(P) \geq 0, \; \deg(Q) \geq 0$
$\overset{(ii)}{\implies} \deg(PQ) = \deg(P) + \deg(Q) \geq 0 \implies PQ \neq 0.$

(i) On a toujours $A^* \subset A[X]^*$; voyons l'autre inclusion.
Soit $P \in A[X]^*$, il existe donc $Q \in A[X]$ tel que $P \cdot Q = 1$.
On a donc:
$0 = \deg(1) \overset{(iii)}{=} \deg P + \deg Q \implies \deg P = \deg Q = 0 \implies P, Q \in A$ tels que $PQ = 1 \implies P \in A^*$

□

Conséquences

1. Ainsi, si A est intègre, $A[X]$ est intègre. Par le paragraphe II.4, on a que $A[X]$ se plonge dans son corps des fraction $Q(A[X])$: le corps des fonctions rationnels (à coefficients dans A).

2. Si $A = K$ est un corps, alors $K[X]^* = K^* = K - \{0\}$, Les polynômes de degré 0.
Ainsi, tout polynôme de degré 1 dans $K[X]$ est irréductible.
En effet: Si $P \in K[X]$, $\deg P = 1$, et $P = QT$, alors:

$$1 = \deg P = \deg(QT) = \deg Q + \deg T \implies \deg Q = 0 \text{ ou } \deg T = 0 \iff Q \in K[X]^* \text{ ou } T \in K[X]^*$$

Ainsi, P est irréductible. (Faux dans $\mathbb{Z}[X]$: $P = 2X$, par irréductible)

Théorème II.19

Si K est un corps, alors $K[X]$ est euclidien pour $\deg : K[X] \to \{0, 1, 2, \ldots\}$

Preuve:

Pour $P, Q \in K[X] - \{0\}$, $\deg(PQ) \overset{(iii)}{=} \deg P + \overbrace{\deg Q}^{\geq 0} \geq \deg P$
Soient $P, Q \in K[X] - \{0\}$; on doit trouver $T, R \in K[X]$ tels que $P = T \cdot Q + R$ avec $R = 0$ ou $\deg R < \deg Q$.
Fixons $Q = \sum j = 0^m b_j X^j$ avec $b_m \neq 0$ (d'où $\deg Q = m \geq 0$).
Procédons par récurrence sur $n = \deg P \geq 0$

- Si $n < m$, alors, on pose $T = 0$ et $R = P$. Cela donne le départ de la récurrence, sauf si $m = 0$, auquel cas: On a $Q = b_0 \in K^*$, et l'on pose $R = 0$, $T = P \cdot b_0^{-1}$

- Soit $P = \sum_{i=0}^{n} a_i X^i$, avec $a_n \neq 0$, et supposons $n \geq m$.
  Posons $P_1 := P - a_n \cdot b_m^{-1} X^{n-m} \cdot Q$
  (Rappel: $b_m \in K - \{0\} = K^*$, donc inversible car dans un corps); le coefficient de degré n de P_1 est égal à: $a_n - a_n b_m^{-1} b_m = 0$
  Ainsi, $\deg P_1 < n = \deg P$. Par l'hypothèse de récurrence:

$\exists\, T_1,\ R \in K[X]$ tels que $P_1 = T_1 Q + R,\ R = 0$ ou $\deg R < \deg Q$
$\implies P = P_1 + a_n b_m^{-1} X^{n-m} \cdot Q = \big(T_1 Q R\big) + a_n b_m^{-1} X^{n-m} Q = \underbrace{\big(T_1 + a_n b_m^{-1} X^{n-m}\big)}_{=:T} Q + R$

□

Remarques

1. C'est faux si A n'est pas un corps (en général). Par exemple, $\mathbb{Z}[X]$ n'est pas euclidien (ex. 4, S. 10)

2. En fait, la preuve montre que la division euclidienne est possible dans $A[X]$ dès que le coefficient dominant de Q eest inversible ($b_m \in A^*$).

Exemple

$P = X^3 + 3X^4 + X^3 - 6X^2 - X + 1,\ Q = X^3 + 2X^2 + X - 1$

	X^3	$+$	$3X^4$	$+$	X^3	$-$	$6X^2$	$-$	X	$+$	1	$\underline{X^3 + 2X^2 + X - 1}$
$-$	X^5	$-$	$2X^4$	$-$	X^3	$+$	$6X^2$					$X^2 + X - 2 =: T$
			X^4			$-$	$5X^2$	$-$	X	$+$	1	
		$-$	X^4	$-$	$2X^3$	$-$	X^2	$+$	X			
				$-$	$2X^3$	$-$	$6X^2$			$+$	1	
					$2X^3$	$+$	$4X^2$	$+$	$2X$	$-$	2	
						$-$	$2X^2$	$+$	$2X$	$-$	1	

Si Y est un ensemble quelconque et A un anneau, alors $A^Y = \{f : Y \to A\}$ est un anneau, pour: $\begin{array}{lcl} (f+g)(x) & = & f(x) + g(x) \\ (f \cdot g)(x) & = & f(x) g(x) \end{array}$
En particulier, $A^A = \{f :\ A \to A\}$ est un anneau.

Tout $P = \sum_{i\geq 0} a_i X^i \in A[X]$ définit $\overline{P} : A \to A$, $\overline{P}(x) := \sum_{i\geq 0} a_i x^i$; l'application polynomiale associée. De plus, l'application $\varphi : \begin{array}{ccc} A[X] & \longrightarrow & A^A \\ P & \longmapsto & \overline{P} \end{array}$, est un homomorphisme d'anneaux.

Terminologie

$a \in A$ est une racine de $P \in A[X]$ si $\overline{P}(a) = 0$.

Proposition II.20

$a \in A$ est une racine de $P \in A[X] \iff (X - a) \mid P$ dans $A[X]$.

Preuve:
$[\Longleftarrow] : (X-a) \mid P \iff \exists T \in A[X]$ tel que $P = T \cdot (X - a)$. Comme $P \mapsto \overline{P}$ est un homomorphisme:
$\overline{P} = \overline{T} \cdot (X - a) \implies \overline{P}(a) = \overline{T}(a) \cdot (a - a) = \overline{T}(a) \cdot 0 = 0 \iff a$ est une racine de P.

$[\Longrightarrow]$: Supposons $a \in A$ racine de P, ie: $\overline{P}(a) = 0$.
Faisons la division euclidienne de P par $Q := X - a \in A[X]$ (OK, car coefficient dominant $= 1$). Donc, il existe $T, R \in A[X]$ tels que $P = TQ + R$, $R = 0$ ou $\deg R < \deg Q = 1 \implies R \in A$ ($R = 0$, ou $\deg R = 0$)
Comme $P \mapsto \overline{P}$ est un homomorphisme, on a: $\overline{P} = \overline{T} \cdot \overline{Q} + \overline{R}$
Par hypothèse: $0 = \overline{P}(a) = \overline{T}(a) \cdot \underbrace{\overline{Q}(a)}_{=0} + \overline{R}(a) = \overline{R}(a) \overset{R \in A}{\Longrightarrow} R = 0 \implies P = TQ$, donc $Q \mid P$.

□

Exemple

Les éléments irréductibles ($\iff$ premier) de $\mathbb{C}[X]$ sont les polynômes de degré 1. Par conséquent, tout $P \in \mathbb{C}[X]$ irréductible est associé à un unique $X - \lambda \in \mathbb{C}[X]$.

⌜

En effet: On a déjà vu: $P \in C[X]$, $\deg P = 1 \implies P$ irréductible.
Reste à voir:

- $\deg P \neq 1 \implies P$ non irréductible.
- $\deg P = 0 \iff P \in \mathbb{C}[X]^* \implies P$ par irréductible.
- $\deg P \geq 2 \implies P$ admet au moins une racine $a \in \mathbb{C}$ (Théorème fondamental de l'algèbre)
  $\overset{II.20}{\Longrightarrow} (X - a) \mid P \implies \exists T \in \mathbb{C}[X]$ tel que $P = (X - a)T$, $\deg T = \deg P - 1 \geq 1 \implies P$ par irréductible.
  Par conséquent: $P \in \mathbb{C}[X]$ irréductible $\iff \deg P = 1$.
  $\deg P = 1 \iff P = a_0 + a_1 X$, $a_1 \neq 0 \implies P$ est associé à $X + a_1^{-1} a_0 =: X - \lambda$.

⌟

La décomposition en irréductible de $P \in \mathbb{C}[X]$ est: $P = a(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n)$, où $a \in C^*$ est le coefficient dominant de P, et $\lambda_1, \ldots, \lambda_n$ sont les racines.

3 Espaces vectoriels et modules

3.1 Espaces vectoriels et applications linéaires

Définition

Soit K un corps. Un ensemble E muni de deux lois $+ : \begin{array}{ccc} E\times E & \longrightarrow & E \\ (v,w) & \longmapsto & v+w \end{array}$, et $\bullet : \begin{array}{ccc} K\times E & \longrightarrow & E \\ (\lambda, v) & \longmapsto & \lambda\cdot v = \lambda v \end{array}$ est appelé un espace vectoriel sur K (ou K-espace vectoriel) si ($\forall \lambda, \mu \in K$, $\forall v, w \in E$):

(E1) $(E, +)$ est un groupe abélien.

(E2) $\lambda(\mu v) = (\lambda\mu)v$

(E3) $(\lambda + \mu)v = \lambda v + \mu v$

(E4) $\lambda(v + w) = \lambda v + \lambda w$

(E5) $1_K \cdot v = v$

Remarques/terminologie

1. Les élémetns de K sont appelés des scalaires, et ceux de E des vecteurs.

2. C'est la définition du 1er semestre, mais avec K un corps quelconque, par exemple: $K = \mathbb{R}, \mathbb{C}$, $K = \mathbb{Q}$, $K = \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$, $K = Q(\mathbb{Z}[x])$,...

3. On a les "règles de calcul" suivantes:
   (i) $0_k \cdot v = 0_E \qquad \forall v \in E$
   (ii) $\lambda \cdot 0_E = 0_E \qquad \forall \lambda \in K$
   (iii) $\lambda v = 0 \implies \lambda = 0_k$ ou $v = 0_E$
   (iv) $(-\lambda)v = -(\lambda v) = \lambda(-v)$, qu'on note $-\lambda v$

Exemples d'espaces vectoriels

1. Un $\mathbb{F}_2$-espace vectoriel est exactement un groupe abélien où tout élément non-trivial est d'ordre 2.

2. Soit K un sous-corps d'un corps L (ie: K sous-anneau de L, K, L corps). Alors, L est un espace vectoriel sur K:
   $(E1) \iff (A1)$
   $(E2) \iff (A2)$
   $(E3), (E4) \iff (A3)$
   $(E5) \iff (A4)$
   Par exemple: $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel, $\mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel, tout corps de caractéristique 0 est un $\mathbb{Q}$-espace vectoriel, tout corps de caractéristique p est un $\mathbb{F}_p$-espace vectoriel.
   En particulier, K est un K-espace vectoriel.

3. $E = K^n = \overbrace{K \times \cdots \times K}^{n}$ $(n \geq 1)$ est un espace vectoriel pour:
   $(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n)$, $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$

4. Pour K un corps, $E = K[X]$ est un espace vectoriel sur K. via $P + Q$, et $\lambda P = \lambda \left(\sum_i a_i X^i \right) = \sum_i (\lambda a_i) X^i$
   De même, $K_n[X] := \{P \in K[X] \mid \deg P < n\}$ est un K-espace vectoriel.

5. Pour K un corps et $n \geq 1$, l'ensemble $M_n(K)$ des matrices $n \times n$ à coefficients dans K est un K-espace vectoriel.

6. Si $E_1, \ldots, E_n$ sont des K-espaces vectoriels, alors, $E := E_1 \times \cdots \times E_n$ est un K-espaces vectoriel via:
   $(v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n)$ et $\lambda(v_1, \ldots, v_n) = (\lambda v_1, \ldots, \lambda v_n)$
   On le note $E = E_1 \oplus \cdots \oplus E_n$ appelé la <u>somme directe</u> (externe) de $E_1, \ldots, E_n$.
   Par exemple si $E_1 = \cdots = E_n = K$, on retrouve $E = K^n$

Terminologie

Un sous-ensemble $F \neq \varnothing$ d'un espace vectoriel E est un <u>sous-espace vectoriel</u> de E si:

$$v, w \in F \implies v + w \in F, \text{ et } \lambda \in K, v \in F \implies \lambda v \in F$$

(équivalent: F est un espace vectoriel pour la restriction des 2 lois de E à F)

Exemples de sous-espaces vectoriels

1. Tout espace vectoriel E admet les sous-espaces vectoriels $F = \{0\}$ et $F = E$

2. Si on a une suite de sous-corps $K \subset L \subset M$, alors L et M sont des K-espaces vectoriels, et L est un sous-espace vectoriel de M.

3. $K_n[X] := \{P \in K[X] \mid \deg P < n\}$ est un sous-espace vectoriel de $K_m[X]$ $\forall m \geq n$, et de $K[X]$

4. F_1, F_2 sous-espaces vectoriels de $E \implies F_1 \cap F_2$ est aussi un sous-espace vectoriel de E.

5. F_1, F_2 sous-espaces vectoriels de E, alors $F_1 + F_2 := \{v_1 + v_2 \mid v_1 \in F_1,\ v_2 \in F_2\}$ est un sous-espace vectoriel de E

Définition

Soient E, E' deux espaces vectoriels sur un même corps K. Une application $f : E \to E'$ est dite <u>linéaire</u> (ou K-linéaire) si:

$$f(v + w) = f(v) + f(w) \quad \forall v, w \in E, \text{ et } f(\lambda v) = \lambda f(v) \quad \forall v \in E$$

Remarques et terminologie

1. On note habituellement $\mathcal{L}(E, E')$ $(= \mathcal{L}_K(E, E'))$ l'ensemble des $f : E \to E'$ linéaires.

2. Comme d'habitude, on peut considérer $\mathrm{Ker}(f) = \{v \in E \mid f(v) = 0\} \subset E$ et $\mathrm{Im}(f) \subset E'$
   Ce sont des sous-espaces vectoriels. On a toujours: $\mathrm{Ker}(f) = \{0\} \iff f$ est injective.

3. $\left.\begin{array}{ll} f : E \to E' & \text{linéaire} \\ g : E' \to E'' & \text{linéaire} \end{array}\right\} \implies g \circ f : E \to E''$ est linéaire.

4. Un <u>isomorphisme</u> (linéaire, ou isomorphisme d'espaces vectoriels) est une application linéaire $f : E \to E'$ bijective (d'inverse linéaire, mais c'est une conséquence).
   On dit que E, E' sont <u>isomorphe</u>, noté $E \cong E'$.

Exemples d'applications linéaires

1. L'application nulle $f : \begin{array}{ccc} E & \longrightarrow & E' \\ v & \longmapsto & 0 \end{array}$, est linéaire. (avec $\mathrm{Ker}(f) = E$, et $\mathrm{Im}(f) = \{0\}$)

2. Si F est un sous-espace vectoriel de E, alors l'inclusion $f : \begin{array}{ccc} F & \longrightarrow & E \\ v & \longmapsto & v \end{array}$ est linéaire. (avec $\mathrm{Ker}(f) = \{0\}$ (fini) et $\mathrm{Im}(f) = F$). En particulier, $f = id_{[}E]$ est linéaire.

3. Pour $\lambda \in K$, l'application $ev_\lambda : K[X] \to K$ définie par $ev_\lambda \left(\sum_i a_i X^i \right) = \sum_i a_i X^i$, est linéaire.
(avec $\mathrm{Ker}(ev_\lambda) = \{P \in K[X] \mid \lambda \text{ est racine de } P\}$, $\mathrm{Im}(ev_\lambda) = K$)

Terminologie

Soit E un espace vectoriel, et $F_1, \ldots, F_n$ des sous-espaces vectoriels de E. On dit que E est la somme directe (interne) de $F_1, \ldots, F_n$ si tout $v \in E$ s'écrit de manière unique $v = v_1 + \cdots + v_n,\ v_i \in F_i \quad \forall i = 1, \ldots, n.$

Remarque

E est somme directe interne de $F_1, \ldots, F_n$ si et seulement si $E = F_1 + \cdots + F_n$ et $F_i \cap (F_1 + \cdots + F_{i-1}) = \{0\} \quad \forall i \leq n$.
(Tout élément $v \in E$ s'écrit $v = v_1 + \cdots + v_n,\ v_i \in F_i \iff E = F_1 + \cdots + F_n$ L'unicité de l'écriture $\iff F_i \cap F_j = \{0\} \quad \forall i \neq j$)

Proposition III.1

Si E est somme directe (interne) de $F_1, \ldots, F_n \subset E$ alors, $E \cong F_1 \oplus \cdot \oplus F_n$: E est isomorphe à la somme direct (externe) des espaces vectoriels $F_1, \ldots, F_n$.

Preuve:
Soit E somme directe (interne) de $F_1, \ldots, F_n$. Posons $f : F_1 \oplus \cdots \oplus F_n \to E$ définie par $f(v_1, \ldots, v_n) = v_1 + \cdots + v_n$.
f est linéaire:

$$\begin{aligned} f\big((v_1, \ldots, v_n) + (w_1, \ldots, w_n)\big) &= f(v_1 + w_1, \ldots, v_n + w_n) = (v_1 + w_n) + \cdots + (v_n + w_n) = (v_1 + \cdots + v_n) + (w_1 + \cdots + w_n) \\ &= f(v_1, \ldots, v_n) + f(w_1, \ldots, w_n) \end{aligned}$$

$$f\big(\lambda(v_1, \ldots, v_n)\big) = f(\lambda v_1, \ldots, \lambda v_n) = \lambda v_1 + \cdots + \lambda v_n = \lambda(v_1 + \cdots + v_n) = \lambda f(v_1, \ldots, v_n)$$

Donc, f est linéaire.
Finalement, f est surjective car tout $v \in E$ s'écrit $v = v_1 + \cdots v_n$ avec $v_i \in F_i$ et f est injective, car cette écriture est unique (par définition de somme directe interne).

Le tout implique que f est un isomorphisme.

□

Remarque (voir ex.4,S. 11)

Si F est un sous-espace vectoriel de E, alors $(F, +)$ est un sous-groupe de $(E, +)$, et on peut donc condidérer le groupe quotient E/F, muni de l'addition $[v] + [w] := [v + w]$ (par le Chapitre I).

De plus, on peut munir E/F d'une loi $K \times E/F \longrightarrow E/F$ via:

$$\lambda \in K,\ [v] \in E/F \implies \lambda \cdot [v] = [\lambda \cdot v]$$

Cela munit E/F d'une structure d'espace vectoriel, et tous les résultats vus au Chapitre I s'étendent (voir ex.4, S. 11).

3.2 Indépendance linéaire, bases, dimension

Terminologie

- Si E est un K-espace vectoriel, et $v_1, \ldots, v_n \in E$, alors tout élément $v = \lambda_1 v_1 + \cdots + \lambda_n v_n \in E$ avec $\lambda_i \in K$ est une combinaison linéaire de $v_1, \ldots, v_n$.

- Pour $\varnothing \neq S \subset E$ un sous-ensemble non-vide de E, on pose $L(S) := \{$ combinaisons linéaires d'un nombre fini d'éléments de $S\} = \{\lambda_1 v_1 + \cdots + \lambda_n v_n \mid n \geq 0, \lambda_i \in K, v_i \in S\}$
  $L(S)$ est le sous-espace vectoriel engendré par S.

- Par convention, $L(\varnothing) = \{0\}$

Lemme III.2

(i) $L(S)$ est un sous-espace vectoriel de E, le plus petit contenant S (d'où le nom).

(ii) $S \subset T \subset E \implies L(S) \subset L(T)$

(iii) $L(S \cup T) = L(S) + L(T)$ pour $S, T \subset E$.

Preuve:

(ii) Trivial.

(iii) Ex. 5, S. 11

(i) Si $v, w \in L(S)$, alors:

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n, w = \mu_1 w_1 + \cdots + \mu_m w_m, v_i, w_j \in S, \lambda_i, \mu_j \in K$$
$$\implies v + w = \lambda_1 v_1 + \cdots \lambda_n v_n + \mu_1 w_1 + \cdots + \mu_m w_m \in L(S)$$

et

$$\lambda v = \lambda(\lambda_1 v_1 + \cdots + \lambda_n v_n) = (\lambda\lambda_1)v_1 + \cdots + (\lambda\lambda_n)v_n \in L(S)$$

Soit finalement $F \subset E$ un sous-espace vectoriel, avec $F \supset S$. $F \supset S$,
F sous-espace vectoriel $\implies F \supset \{\lambda v \mid \lambda \in K, v \in S\}$
F sous-espace vectoriel $\implies F \supset \{$somme de $\lambda_i v_i, \lambda_i \in K, v_i \in S\} = L(S)$
Ainsi, $L(S)$ est le plus petit sous-espace vectoriel de E contenant S

□

Terminologie

Un espace vectoriel E est dit de dimension finie sur K s'il existe S fini$\subset E$ tel que $E = L(S)$

Exemples

1. $\mathbb{C} = L(\{1, 2\})$ est de dimension finie sur $\mathbb{R}$

2. $K^n = L\big(\overbrace{(1, 0, \ldots, 0)}^{:=e_1}, \ldots, \overbrace{(0, \ldots, 0, 1)}^{:=e_n}\big)$ est de dimension finie sur K.

3. $K_n[X] = L(\{1, X, X^2, \ldots, X^{n-1}\})$ est de dimension finie sur K $\forall n$.

4. $K[X]$ n'est <u>pas</u> de dimension finie sur K.

   ⌜

   Si $S \subset K[X]$ est fini, $L(S)$ ne continet que ds polynômes de degré $\leq \max\{\deg P \mid P \in S\}$, d'où $L(S) \neq K[X]$

   ⌟

Définition

Soit E un espace vectoriel sur K, et $v_1, \ldots, v_n \in E$. On dit que $v_1, \ldots, v_n$ sont <u>linéairement indépendant</u> (ou: <u>famille libre</u>) si:

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0,\ \lambda_1, \ldots, \lambda_n \in K \implies \lambda_1 = \cdots = \lambda_n = 0$$

Sinon, ils sont dits <u>linéairement dépendant</u> (ou: <u>famille liée</u>).

Exemples

1. $\{1, 2\} \subset \mathbb{C}$ est une faille libre sur $\mathbb{R}$ $\left(\begin{matrix} a \cdot 1 + b \cdot 2 = 0 \\ a, b \in \mathbb{R} \end{matrix}\right\} \implies a = b = 0\Bigg)$, mais liée sur $\mathbb{C}$ ($(-i)1 + 1i = 0$)

2. $e_1, \ldots, e_n \in K^n$ sont linéairement indépendant sur K.

3. $\{1, X, \ldots, X^{n-1}\}$ est une famille libre de $K_n[X]$ sur K.

Remarque

Si $v_1, \ldots, v_n \in E$ est une famille libre, alors tout élément de $L(\{v_1, \ldots, v_n\})$ s'écrit de manière unique comme combinaison linéaire des $v_1, \ldots, v_n$

⌜

Si $v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \lambda'_1 v_1 + \cdots + \lambda'_n v_n \qquad \lambda_i, \lambda'_i \in K$
$\implies 0 = v - v = (\lambda_1 v_1 + \cdots + \lambda_n v_n) - (\lambda'_1 v_n + \cdots + \lambda'_n v_n) = (\lambda_1 - \lambda'_1)v_1 + \cdots + (\lambda_n - \lambda'_n)v_n$
Comme $v_1, \ldots, v_n$ est libre, on a $\lambda_i - \lambda'_i = 0 \quad \forall i$, donc $\lambda_i = \lambda'_i$.

⌟

Proposition III.3

Soit $v_1, \ldots, v_n \in E$ une famille liée. Alors, il existe $j \in \{1, \ldots, n\}$ tel que v_j est combinaison linéaire de $v_1, \ldots, v_{j-1}$.

Preuve:
Par hypothèse, il existe $\lambda_1, \ldots, \lambda_n \in K$, non-tous nuls, tels que $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. Posons $j := \max\{i \mid \lambda_i \neq 0\}$

$$0 = \lambda_1 v_1 + \cdots + \lambda_n v_n = \lambda_1 v_1 + \cdots + \lambda_j v_j \quad \text{car} \quad i > j \implies \lambda_i = 0$$
$$\lambda_j v_j = -(\lambda_1 v_1 + \cdots + \lambda_{j-1} v_{j-1}) \underset{\lambda_j \neq 0}{\implies} v_j = (-\lambda_j^{-1}\lambda_1)v_1 + \cdots + (-\lambda_j^{-1} v_{j-1})v_{j-1}$$

Remarque: On utilise ici le fait que l'on travail sur un corps, $\lambda_j \in K$ implique qu'il existe un inverse λ_j^{-1}

□

Corollaire III.4

Soient $v_1, \ldots, v_n \in E$ avec $v_1, \ldots, v_k$ linéairement indépendants ($k \in \{0, 1, \ldots, n\}$)
Alors, il existe $\{i, \ldots, i_r\} \subset \{k+1, \ldots, n\}$ tel que $v_1, \ldots, v_k, v_{i1}, \ldots, v_{ir}$ est linéairement indépendant, et:

$$L(\{v_1, \ldots, v_k, v_{i1}, \ldots, v_{ir}\}) = L(\{v_1, \ldots, v_n\})$$

Preuve:
Soit $S = \{v_1, \ldots, v_n\} \subset E$, avec $v_1, \ldots, v_k$ linéairements indépendants.
Supposons qu'il n'existe pas de $v_j \in S$ combinaison linéaire des $v_1, \ldots, v_{j-1}$. Dans ce cas, par la contraposée à la Proposition III.3, la famille S est libre. Dans ce cas, on pose $\{i_1, \ldots, i_r\} = \{k+1, \ldots, n\}$, il n'y a rien à faire.

Dans le cas contraire, il existe v_j combinaison linéaire de $v_1, \ldots, v_{j-1}$. Prenons le plus grand tel j, et posons $S' := S - \{v_j\}$. (Notons que $j > k$, car $v_1, \ldots, v_k$ est libre)
On a $L(S') = L(S)$:

- $L(S') \subset L(S)$: $S' \subset S \implies L(S') \subset L(S)$
- $L(S) \subset L(S')$: car v_j est combinaison linéaire des $v_1, \ldots, v_{j-1}$

On recommence, supposons qu'aucun $v_l \in S'$ n'est combinaison linéaire des précédents. Par Proposition III.3, S' est libre et $L(S') = L(S)$.
On pose $\{i_1, \ldots, i_r\} = \{k+1, \ldots, n\} \setminus \{j\}$.
Sinon, on enlève le plus grand $v_e \in S'$ combinaison linéaire des précédents. On continue cette procédure jusqu'à obtenir:

$$T = \{v_1, \ldots, v_k, v_{i1}, \ldots, v_{ir}\} \subset S \quad \text{tel que} \quad L(T) = L(S)$$

et aucun v_j n'est combinaison linéaire des précédents. Par III.3, T est libre, et on a fini.

□

Définition

Soit $S \subset E$ un espace vectoriel. L'ensemble S est une base de E si:

(i) $L(S) = E$

(ii) Toute famille finie $\{v_1, \ldots, v_n\} \subset S$ est libre

Remarque

De manière équivalente: tout élément de E s'écrit de façon unique comme combinaison linéaire finie d'éléments de S.

Théorème III.5

Tout espace vectoriel de-dimension-finie admet une base.

Preuve:
Soit E un espace vectoriel de dimension finie. Donc, il existe $S := \{v_1, \ldots, v_n\} \subset E$ tel que $E = L(S)$. Appliquons Corollaire III.4 dans le cas $k = 0$:
$\exists \{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$ tel que $v_{i1}, \ldots, v_{ir}$ est libre, et $L(\{v_{i1}, \ldots, v_{ir}\}) = L(S) = E$. Donc $v_{i1}, \ldots, v_{ir}$ est une base de E.

□

Exemples de bases

1. $\{1, i\}$ est une base de $\mathbb{C}$ sur $\mathbb{R}$.

2. $\{e_1, \ldots, e_n\}$ est une base de K^n (où $e_i := (0, \ldots, 0, \overset{i\text{ème}}{1}, 0, \ldots, 0)$)

3. $\{1, X, X^2, \ldots, X^{n-1}\}$ est une base de $K_n[X]$.

4. $\{1, X, X^2, \ldots\}$ est une base infine de $K[X]$

Remarque

Tout espace vectoriel admet une base. Mais la preuve repose sur le "Lemme de Zorn" (axiome du Choix), et n'est donc pas constructible. (voir aussi ex. 7, S. 11)

Lemme III.6

Si $v_1, \ldots, v_n$ engendrent E, et $w_1, \ldots, w_m$ sont linéairement indépendants, alors $m \leq n$.

Preuve:
Soit donc $v_1, \ldots, v_n \in E$ qui engendrent E, et $w_1, \ldots, w_m \in E$ liinéairement indépendants. A voir: $m \leq n$.

Considérons la famille $w_m, v_1, \ldots, v_n$: cette famille engendre E, mais est liée, car $v_1, \ldots, v_n$ engendrent E.
Appliquons Corollaire III.4 à $w_m, v_1, \ldots, v_n$ (w_m libre):
$\exists \{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$, avec $r \leq n-1$, tel que $w_m, v_{i1}, \ldots, v_{ir}$ est une base de E.

On recommence avec $w_{m-1}, w_m, v_{i1}, \ldots, v_{ir}$: engendre E, mais liée, comme avant. On applique à nouveau Corollaire III.4 à $W_{m-1}, w_m, v_{i1}, \ldots, v_{ir}$ (w_{m-1}, w_m libre):
$\exists \{j, \ldots, j_s\} \subset \{i_1, \ldots, i_r\}$, avec $s \leq r-1 \leq n-2$ tel que $w_{m-1}, w_m, v_{j1}, \ldots, v_{js}$ est une base. Etc...

Après $m-1$ itérations de ce processus, on obtient une base de E de la forme $w_2, \ldots, w_m, v_{k1}, \ldots, v_{kl}$ avec $l \leq n-(m-1) = n-m+1$.

Finalement, comme $w_1 \in E$, w_1 est combinaison linéaire de $w_2, \ldots, w_m, v_{k1}, \ldots, v_{kl}$, et comme $w_1, \ldots, w_m$ est

libre, un des v_{kj} apparait dans cette combinaison linéaire.
Cela donne donc $l \geq 1$.

On obtient ainsi: $n - m + 1 \geq l \geq 1 \implies m \leq n$

□

Théorème III.7

Deux bases pour un espace vectoriel de dimension finie ont même cardinal.

Preuve:
Soient $\{v_1, \ldots, v_n\}$ et $\{w_1, \ldots, w_m\}$ deux bases pour E.
Comme $v_1, \ldots, v_n$ engendrent E et $w_1, \ldots, w_m$ est libre, on a $m \leq n$ par Lemme III.6. On échange les rôles: $n \leq m$.
Ainsi, $m = n$.

□

Définition

Soit E un espace vectoriel de dimension finie. La dimension de E, notée $\dim(E)$, est le nombre d'éléments d'une base quelconque de E.

Remarques

1. Ainsi, si E est de dimension finie, on a que $\dim(E)$ est finie. Cela justifie la terminologie, et l'on peut abeandonner les tirets.

2. Ce théorème est valable pour tout espace vectoriel, et l'on peut définir la dimension de E comme le cardinal (peut-être infini) d'une base quelconque de E.

Exemples

1 $\dim_{\mathbb{R}}(\mathbb{C}) = 2$

2 $\dim(K^n) = n$

3 $\dim\big(K_n[X]\big) = n$

Théorème III.8

Deux espaces vectoriels de dimension finie E et E' sont isomorphes si et seulement si $\dim(E) = \dim(E')$.

Preuve:

[$\Longleftarrow$] : Soit E de dimension n. On va montrer rque $E \cong K^n$.
Du coup, si E' est un autre espace vectoriel de dimension n, on a $E' \cong K^n$, d'où $E \cong E'$, et on a fini.

Soit donc E de $\dim n$. Il existe donc une base $v_1, \ldots, v_n$ de E.
Soit $f: K^n \to E$, $f(x_1, \ldots, x_n) = x_1 v_1 + \cdots + x_n v_n = \sum_{i=1}^{n} x_i v_i$.
f est linéaire:

(1)

$$f\big((x_1,\dots,x_n)+(y_1,\dots,y_n)\big) = f(x_1+y_1,\dots,x_n+y_n) = \sum_{i=1}^{n}(x_i+y_i)v_i = \sum_{i=1}^{n} x_i v_i + \sum_{i=1}^{n} y_i v_i$$
$$= f(x_1,\dots,x_n) + f(y_1,\dots,y_n)$$

(2)

$$f\big(\lambda(x_1,\dots,x_n)\big) = f(\lambda x_1,\dots,\lambda x_n) = \sum_{i=1}^{n}(\lambda x_i)v_i = \sum_{i=1}^{n}\lambda(x_i v_i) = \lambda\sum_{i=1}^{n} x_i v_i = \lambda f(x_1,\dots,x_n)$$

f est surjective car $v_1,\dots,v_n$ engendre E; f inj $\iff$ $\operatorname{Ker} f = 0$ $\iff$ $v_1,\dots,v_n$ linéairement indépendants.

[$\Longrightarrow$] : Soit $f : E \to E'$ un isomorphisme, et soit S une base de E. On va montrer que $f(S)$ est une base de E'. (Du coup, comme $f : S \to f(S)$ est une bijection, on aura: $\dim(E) = \#S = \#f(S) = \dim(E')$, et on aura fini.)

Vérifions donc (i) et (ii) pour $f(S)$ base de E'

(i) Soit $v' \in E'$; f surjective $\implies$ $\exists v \in E$ tel que $v' = f(v)$.
Comme $E = L(S)$, $\exists v_1,\dots,v_n \in S, \lambda_1,\dots,\lambda_n \in K$ tels que $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$
$\implies$ $v' = f(v) = f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n)$, avec $f(v_i) \in f(S)$.
On a donc $v' \in L\big(f(S)\big)$, d'où $E' = L\big(f(S)\big)$

(ii) Soient $v'_1,\dots,v'_n \in f(S)$, et $\lambda_1,\dots,\lambda_n \in K$ tels que $\lambda_1 v'_1 + \cdots + \lambda_n v'_n = 0$, à voir: $\lambda_1 = \cdots = \lambda_n = 0$

$$v'_i \in f(S) \implies \exists v_i \in S \quad \text{tels que} \quad v' = f(v_i)$$
$$\implies 0 = \lambda_1 v'_1 + \cdots + \lambda_n v'_n = \lambda_1 f(v_1) + \cdots + \lambda_n f(v_n) = f(\lambda_1 v_1 + \cdots + \lambda_n v_n)$$

Comme f est injective, cela implique $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$

Comme $v_i \in S$, S base on a $\{v_1,\dots,v_n\}$ est libre, d'où $\lambda_1 = \cdots = \lambda_n = 0$.

□

Exemples

1. $\mathbb{C} \cong \mathbb{R}^2$
2. $K_n[X] \cong K^n$
3. $\mathbb{R}^n \ncong \mathbb{R}^m$ pour $n \neq m$

Lemme III.9

Soit E un espace vectoriel de dimension finie, et F un sous-espace de E. Alors:
F est de dimension finie, $\dim F \leq \dim E$, et $\dim\left({}^{E}\big/_{F} \right) = \dim(E) - \dim(F)$.

Preuve:
Soit donc E de dimension finie, $\dim(E) = n$, et F un sous-espace.

- Par le Lemme III.6, toute famille de $n+1$ éléments de F est liée. (contraposée du Lemme III.6)
  Soit $w_1, \dots, w_m$ une famille libre de taille maximale dans F. On a donc $m \leq n$
  Affirmation: $w_1, \dots, w_m$ engendrent F ($\implies w_1, \dots, w_m$ base $\implies \dim(F) = m \leq n = \dim(E)$)
  En effet: Soit $w \in F$ un élément quelconque. Par maximalité de $w_1, \dots, w_m$, la famille $w_1, \dots, w_m, w$ est liée.
  Ainsi, il existe $\lambda_1, \dots, \lambda_m, \lambda \in K$, non-tous nuls, tels que $\lambda_1 w_1 + \cdots + \lambda_m w_m + \lambda w = 0$.
  On a $\lambda \neq 0$, car si $\lambda = 0$, on a $\lambda_1, \dots, \lambda_m$ non-tous nuls tels que $\lambda_1 w_1 + \cdots + \lambda_m w_m = 0$, ie: $w_1, \dots, w_m$ est liée, une contradiction.
  Ainsi, $\lambda \neq 0 \in K$, d'où:
  $\lambda w = -(\lambda_1 w_1 + \cdots + \lambda_m w_m) \implies w = (-\lambda^{-1}\lambda_1)w_1 + \cdots + (-\lambda^{-1}\lambda_m)w_m \in L(\{w_1, \dots, w_m\})$, on a fini.

- Soit $w_1, \dots, w_m$ une base de F.
  Comme $\dim(E) = n$, il existe une base $v_1, \dots, v_n$ de E.
  Appliquons le corolalire III.4 à la famille $w_1, \dots, w_m, v_1, \dots, v_n$, avec $w_1, \dots, w_m$ est libre:
  Il existe $\{i_1, \dots, i_r\} \subset \{1, \dots, n\}$ tel que $w_1, \dots, w_m, v_{i1}, \dots, v_{ir}$ est une base de E (avec $m + r = n$)
  Affirmation: $[v_{i1}], \dots, [v_{ir}] \in E/F$ est une base de E/F ($\implies \dim\left(E/F\right) = r = n - m = \dim E - \dim F$)

  En effet: Démontrons les 2 points dans la définition d'une base:

  (i) Un élément quelconque de E/F est de la fomre $[v] = \pi(v) \in E/F$, avec $v \in E$ et $\pi : E \to E/F$.
  Comme $w_1, \dots, w_m, v_{i1}, \dots, v_{ir}$ engendre E, il existe $\lambda_1, \dots, \lambda_m, \mu_1, \dots, \mu_r$ tels que:

  $$v = \lambda_1 w_1 + \cdots + \lambda_m w_m + \mu_1 v_{i1} + \cdots + \mu_r v_{ir}$$

  On applique π:

  $$[v] = \pi(v) = \lambda_1 \underbrace{\pi(w_1)}_{=0} + \cdots + \lambda_m \underbrace{\pi(w_m)}_{=0} + \mu_1 \pi(v_{i1}) + \cdots + \mu_r \pi(v_{ir}) = \mu_1 [v_{i1}] + \cdots + [v_{ir}]$$

  $w_i \in F = \mathrm{Ker}(\pi)$. Donc, cette famille engendre E/F

  (ii) Soient $\alpha_1, \dots, \alpha_r \in K$ tels que $\alpha_1[v_{i1}] + \cdots + \alpha_r[v_{ir}] = 0 \in E/F$.
  A voir: $\alpha_1 = \cdots = \alpha_r = 0$, et on aura terminé.

  On a $E/F \ni 0 = \alpha_1[v_{i1}] + \cdots + \alpha_r[v_{ir}] = [\alpha_1 v_{i1} + \cdots + \alpha_r v_{ir}] = \alpha_1 v_{i1} + \cdots + \alpha_r v_{ir} \in F = L(\{w_1, \dots, w_m\})$
  Ainsi, il existe $\beta_1, \dots, \beta_m \in K$ tels que $\alpha_1 v_{i1} + \cdots + \alpha_r v_{ir} = \beta_1 w_1 + \cdots + \beta_m w_m$.

  $$\implies 0 = \beta_1 w_1 + \cdots + \beta_m w_m - \alpha_1 v_{i1} - \cdots - \alpha_r v_{ir} \underset{\text{Famille libre}}{\implies} \beta_1 = \cdots = \beta_m = \alpha_1 = \cdots = \alpha_r = 0$$

□

Théorème III.10: Théorème du Rang

Si $f : E \to E'$ est une application linéaire aec E de dimension finie, alors:

$$\dim(E) = \dim(\mathrm{Ker}(f)) + \dim(\mathrm{Im}(f))$$

Preuve:

Soit donc $f : E \to E'$ linéaire, avec $\dim(E) < \infty$. Cela définit un isomorphisme $E/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. On a donc:

$$\dim\left(\mathrm{Im}(f)\right) \overset{\text{Thm III.8}}{=} \dim\left(E/\mathrm{Ker}(f)\right) \overset{\text{Lemme III.9}}{=} \dim(E) - \dim(\mathrm{Ker}(f))$$

□

Terminologie

Une suite $0 \overset{f_0}{\to} E_1 \overset{f_1}{\to} E_2 \overset{f_2}{\to} E_3 \overset{f_3}{\to} \cdots \overset{f_{n-2}}{\to} E_{n-1} \overset{f_{n-1}}{\to} E_n \overset{f_n}{\to} 0$ d'applications linéaires est dite <u>exacte</u> si $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \quad \forall i$.

Corollaire III.11

Dans une suite exacte d'espaces vectoriels de dimension finie, on a:

$$\sum_{i=1}^{n} (-1)^i \dim(E_i) = 0$$

<u>Preuve:</u>
Appliquons le théorème du rang à $f_i : E_i \to E_{i+1}$:

$$\begin{aligned}
\sum_{i=1}^{n} (-1)^i \dim(E_i) &= \sum_{i=1}^{n} (-1)^i \left(\dim\left(\mathrm{Ker}(f_i)\right) + \dim\left(\mathrm{Im}(f_i)\right)\right) \\
&= \sum_{i=1}^{n} (-1)^i \left(\dim\left(\mathrm{Ker}(f_i)\right) + \dim\left(\mathrm{Ker}(f_{i+1})\right)\right) \\
&= -(\dim \underbrace{\mathrm{Ker}(f_1)}_{=\mathrm{Im}(f_0)=0} + \cancel{\dim \mathrm{Ker}(f_2)}) + (\cancel{\dim \mathrm{Ker}(f_2)} + \cancel{\dim \mathrm{Ker}(f_3)}) - \\
&\qquad \cdots + (-1)^n (\cancel{\dim \mathrm{Ker}(f_n)} + \dim \underbrace{\mathrm{Ker}(f_{n+1})}_{=\mathrm{Im}(f_n)=0}) = 0
\end{aligned}$$

□

3.3 Application aux polyèdres

On considère un polyèdre. On note: S :=#sommets de P
A :=#arêtes de P
F :=#faces de P

Existe-t-il une relation entre S, A et F ?

Exemples

	pyra	cube	octa.	dodéca.	icosa.
S	4	8	6	20	12
A	6	12	12	30	30
F	4	6	8	12	20

Euler[1758]: Pour tout polyèdre P, on a $S-A+F=2$ (sans preuve). Mais cette formule est-elle toujours valide ?

Définition (Möbius, 1867)

Un polyère est une collecitn finie de polygones (faces) telle que:

(i) Si deux faces se rencontrent, c'est en un sommet ou en une arrête.

(ii) Chaque arête borde exactement 2 faces, dites adjacentes.

(iii) Pour toute paire de faces, f, f', il existe des faces $f_1, f_2, \ldots, f_n$ telles que $f = f_1$, $f_n = f'$, et f_{i+1} est adjacente à f_i $\forall i$.

Théorème III.12: Poincaré, 1899

Soit P un polyèdre tel que toute boucle formée d'arêtes borde une collection de faces. Alors, $S - A + F = 2$.

Préliminaires à la preuve

- On va appeler:
  - un sommet: un 0-polytope
  - une arête: un 1-polytope
  - une face: un 2-polytope
  - un polyèdre: un 3-polytope
  - $\varnothing$: un (-1)-polytope
- Soit P un polyèdre fixé. Pour $n = -1, 0, 1, 2, 3$, on note $C_n(P)$ le $\mathbb{F}_2$-espace vectoriel de base donnée par l'ensemble des n-polytopes de P.

Remarques

1. Par définition de la base:
   Tout élément de $C_n(P)$ s'écrit de manière unique comme combinaison $\mathbb{F}_2$-linéaire de n-polytopes de P, ie: comme somme de n-polytopes de P.

2. L'addition dans $C_n(P)$ est donnée comme suit:
   On additionne les 2 sommes, et on efface chaque élément qui apparait 2 fois.

- Pour σ un n-polytope, on pose $\delta_n(\sigma) \in C_{n-1}(P)$, la somme des $(n-1)$-polytopes dans le bord de σ.
  Cela définit de manière unique une application linéaire $\delta_n : C_n(P) \to C_{n-1}(P)$, appelée l'application bord, via :
  $$\delta_n(\sigma_1 + \cdots + \sigma_r) = \delta_n(\sigma_1) + \cdots + \delta_n(\sigma_r)$$

  Par convention: $\delta(\cdot) = \varnothing \in C_{-1}(P)$, $\delta_{-1}(\varnothing) = 0$

  On a donc une suite de $\mathbb{F}_2$-espaces vectoriels:
  $$0 \to \underset{\#\{3-\text{polytopes}\}=1}{C_3(P)} \xrightarrow{\delta_3} \underset{F}{C_2(P)} \xrightarrow{\delta_2} \underset{A}{C_1(P)} \xrightarrow{\delta_1} \underset{S}{C_0(P)} \xrightarrow{\delta_0} \underset{1}{C_{-1}(P)} \to 0$$
  Par le Corollaire III.11; il reste à voir que la suite est exacte, et l'on aura: $0 = 1 - F + A - S + 1 \iff S - A + F = 2$

Preuve de l'exactitude
($\implies$ théorème III.12):
Notons tout d'abord que $\forall n$, on a $\delta_{n-1} \circ \delta_n = 0$. Cela implique $\mathrm{Im}(\delta_n) \subset \mathrm{Ker}(\delta_{n-1}) \quad \forall n$.

En effet: Si $x \in \mathrm{Im}(\delta_n)$, $\exists y$ tel que $x = \delta_n(y) \implies \delta_{n-1}(x) = \delta_{n-1}\big(\delta_n(y)\big) = (\delta_{n-1} \circ \delta_n)(y) = 0$.
$\implies x \in \mathrm{Ker}(\delta_{n-1})$

Vérifions que $\delta_{n-1} \circ \delta_n = 0 \quad \forall n$. Il suffit de le voir pour les éléments de la base.

- $\delta_0\big(\delta_1($  $)\big) = \delta_0(v_1 + v_2) = \varnothing + \varnothing = 0$

- $\delta_1\big(\delta_2($  $)\big) = \delta_1($  $) = 0$
- $\delta_2\big(\delta_3(P)\big) = \delta_2(\text{somme de toutes les faces}) = 2 \cdot \text{ chaque arête} = 0$

Reste à voir: $\mathrm{Ker}(\delta_{n-1}) \subset \mathrm{Im}(\delta_n) \quad \forall n$.

- $\mathrm{Ker}(\delta_{-1}) = C_{-1}(P) = \mathbb{F}_2\varnothing = \{0, \varnothing\} \overset{?}{\subset} \mathrm{Im}(\delta_0)$: OK, car $\delta_0(v) = \varnothing$ pour tout sommet v. Donc, ça montre que P contient au moins un sommet.
- $\mathrm{Ker}(\delta_0) \subset \mathrm{Im}(\delta_1)$: $\begin{matrix}\mathrm{Ker}(\delta_0) = & \text{somme d'un nombre pair de sommets.} \\ \mathrm{Im}(\delta_1) = & \text{bord d'une famille d'arêtes.}\end{matrix}$

  Cette inclusion dit: $\forall v_1, v_2$ sommets, il existe un chemin formé d'arête, qui joint v_1 à v_2. C'est une conséquence des points (ii) et (iii) dans la définition de Möbius.
- $\mathrm{Ker}(\delta_1) \subset \mathrm{Im}(\delta_2) \iff$ toute boucle formés d'arêtes borde une collection de faces: c'est l'hypothèse du théorème !

– $\mathrm{Ker}(\delta_2) \subset \mathrm{Im}(\delta_3) = \{0$, somme de toutes les faces $\}$: ça découle de la condition (iii)

– $\mathrm{Ker}(\delta_3) \subset \mathrm{Im}(\delta_4) = 0 \iff \delta_3$ inj. $\iff \delta_3(P) \neq 0$, clair.

□

3.4 Modules axiomes et exemples

Définition

Soit A un anneau. Un ensemble M muni d'une loi $+ : \begin{array}{ccc} M \times M & \longrightarrow & M \\ (x,y) & \longmapsto & x+y \end{array}$ et d'une loi $\bullet : \begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,x) & \longmapsto & a \cdot x = ax \end{array}$ est appelé un <u>module sur A</u> (ou <u>A-module</u>) si $(\forall a, b \in A,\ \forall x, y \in M)$:

(M1) $(M, +)$ est un groupe abélien

(M2) $a(bx) = (ab)x$

(M3) $(a+b)x = ax + bx$

(M4) $a(x+y) = ax + ay$

(M5) $1_A \cdot x = x$

Exemples

1) Si $A = K$ est un corps, alors un A-module coïncident avec les K-espaces vectoriels $\implies$ les modules généralisent les espaces vectoriels.

2) Si $A = \mathbb{Z}$, alors les $\mathbb{Z}$-modules coïncident avec les groupes abéliens.
En effet, un $\mathbb{Z}$-module est un groupe abélien par (M1). Réciproquement, soit $(G, +)$ un groupe abélien.
Il est muni de la loi $\bullet : \begin{array}{ccc} \mathbb{Z} \times G & \longrightarrow & G \\ (n,x) & \longmapsto & nx \end{array}$, où $n \cdot x = \begin{cases} \overbrace{x + \cdots + x}^{n} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-x) + \cdots + (-x)}_{|x|} & n < 0 \end{cases}$
Et les axiomes sont verifiés:
(M2) : $n \cdot (m \cdot x) = (nm) \cdot x$
(M3) : $(n+m)x = nx + mx$
(M4) : $n(x+y) = nx + ny$
(M5) : $1 \cdot x = x$

Ainsi: les modules généralisent les groupes abéliens !

3) Un anneau A est un A-module. ((M1)=(A1), (M2)-(M5) $\iff$ (A2)-(A4))
Ainsi, les modules généralisent aussi les anneaux !

4) Soit E un K-espace vectoriel, et $f : E \to E$ un endomorphisme. Cela définit une structure de $K[X]$-module sur E, via:

$$P = \sum_{i=0}^{n} \lambda_i X^i \in K[X],\ v \in E \implies P \cdot v := \sum_{i=0}^{n} \lambda_i f^i(v),\ \text{où } f^i := \overbrace{f \circ \cdots \circ f}^{i}$$

(M1) OK car E est un espace vectoriel
(M2) OK par définition de $P \cdot Q$
(M3) OK par définition de $P + Q$
(M4) OK par linéarité de f
(M5) OK par définition.

On obtient donc un $K[X]$-module qui dépend de f; on le notera E_f.
Réciproquement, si M est un module sur $K[X]$, alors M est un K-espace vectoriel (restriction de la loi externe à $K \subset K[X]$), et l'application $f : M \to M$, $f(x) = X \cdot x$ est linéaire.

$$f(x+y) = X(x+y) \overset{(M4)}{=} X\cdot x + X\cdot y = f(x) + f(y)$$
$$f(\lambda x) = X\cdot(\lambda x) \overset{(M2)}{=} (X\lambda)\cdot x \overset{(M2)}{=} \lambda(X\cdot x) = \lambda f(x)$$

Ainsi, les modules généralisent aussi les espaces vectoriels munis d'un endomorphisme !

5) Si $M_1, \dots, M_n$ sont des A-modules, alors $M_1 \times \cdots \times M_n$ est aussi un A-module via:
$$\begin{array}{ll}(x_1,\dots,x_n)+(y_1,\dots,y_n) & := (x_1+y_1,\dots,x_n+y_n) \\ a(x_1,\dots,x_n) & := (ax_1,\dots,ax_n)\end{array}, \text{ où } x_i, y_i \in M_i \quad \forall i, \text{ et } a \in A.$$
Le résultat est noté $M_1 \oplus \cdots \oplus M_n$, la somme directe de $M_1, \dots, M_n$. Si $M_i = M \quad \forall i$, on le note M^n.

Remarques

Comme pour les espaces vectoriels, on a les "règles de calcul" suivantes, avec les mêmes preuves:

(i) $0_A \cdot x = 0_M \quad \forall x \in M,\ a \cdot 0_M = 0_M \quad \forall a \in A$

(ii) $(-a)x = a(-x) = -(ax) \quad \forall a \in A,\ \forall x \in M$

En revanche, l'égalité $a \cdot x = 0_M$ avec $a \in A,\ x \in M$, n'implique pas $a = 0_A$ ou $x = 0_m$!
Par exemple, prenons $A = \mathbb{Z}$, et $M = \mathbb{Z}/2\mathbb{Z}$: soit $a = 2 \in \mathbb{Z}$, $x = [1] \in \mathbb{Z}/2\mathbb{Z}$; on a $a \neq 0,\ x \neq 0$ mais $a \cdot x = 2 \cdot [1] = [1] + [1] = [0] = 0_{\mathbb{Z}/2\mathbb{Z}}$

Terminologie

Un sous-ensemble $N \neq \varnothing$ d'un A-module M est un sous-module de M si:

$$x, y \in N \implies x + y \in N, \text{ et } x \in N,\ a \in A \implies ax \in N$$

Exemples

1. Si $A = K$ est un corps, c'est la notion de sous-espace vectoriel.

2. Si $A = \mathbb{Z}$, un sous $\mathbb{Z}$-module est un sous-groupe (abélien).

3. Soit A un anneau commutatif. Un sous-module du A-module $M = A$ est un idéal de A.

4. Soit E un K-espace vectoriel, et $f \in \mathrm{End}(E)$. Cela définit une structure de $K[X]$-module sur E, noté E_f.
Un sous-module du $K[X]$-module E_f est sous-espace vectoriel $F \subset E$ stable par f, ie: tel que $f(F) \subset F$.

$\ulcorner$

$F \subset E_f$ sous-module $\iff (x, y \in F \implies x + y \in F$, et $x \in F$, $P = \sum_i \lambda_i X^i \in K[X] \implies P \cdot x \in F)$

$\iff (x, y \in F \implies x + y \in F,\ x \in F \implies \lambda \cdot x \in F\ \forall \lambda \in K$, et $X \cdot x \in F)$

$\iff F \subset E$ est un sous-espace vectoriel, et $x \in F \implies X \cdot x \overset{\text{déf.}}{=} f(x) \in F$

$\iff F \subset E$ est un sous-espace vectoriel tel que $f(F) \subset F$.

$\lrcorner$

5. Si $M_1, M_2 \subset M$ sont deux sous-modules de M, alors $M_1 + M_2 := \{x_1 + x_2 \mid x_i \in M_i\}$ est aussi un sous-module de M.

Définition

Une application $\varphi : M \to M'$ entre deux modules sur A est un homomorphisme de A-modules (ou application A-linéaire) si:

$$\varphi(x + y) = \varphi(x) + \varphi(y) \qquad \forall x, y \in M \quad \text{et} \quad \varphi(a \cdot x) = a \cdot \varphi(x) \qquad \forall a \in A,\ \forall x \in M$$

Exemples

1. Si $A = K$ un corps, c'est la notion d'application linéaire.

2. Si $A = \mathbb{Z}$, une application $\mathbb{Z}$-linéarie est un homomorphisme de groupes (abéliens)

   $(\varphi(x + y) = \varphi(x) + \varphi(y) \iff$ homo. de groupes, et $\varphi(n \cdot x) = \varphi(\overbrace{x + \cdots + x}^{n}) = \overbrace{\varphi(x) + \cdots + \varphi(x)}^{n} = n \cdot \varphi(x)$ si $n > 0$, idem pour $n \leq 0)$

3. Si $A = K[X]$: Soient $E_f, E'_{f'}$ deux $K[X]$-modules (avec $f \in \mathrm{End}(E)$, $f' \in \mathrm{End}(E')$).
   Une application $\varphi : E_f \to E'_{f'}$ est $K[X]$-linéaire $\iff \varphi$ est K-linéaire, et $\varphi \circ f = f' \circ \varphi$.
   (Comme si-dessu, φ est $K[X]$-linéaire $\iff \begin{matrix} \varphi(x + y) = \varphi(x) + \varphi(y) \\ \varphi(\lambda x) = \lambda \varphi(x) \quad \forall \lambda \in K \end{matrix}$ et $\varphi\big(f(x)\big) = \varphi(X \cdot x) = X \cdot \varphi(x) = f'\big(\varphi(x)\big)$ et ce $\forall x \in E$.) Imagé:

$$\begin{array}{ccc} E & \xrightarrow{f} & E \\ \varphi \downarrow & & \downarrow \varphi \\ E' & \xrightarrow[f']{} & E' \end{array}$$

Remarque

Si M est un A-module et $N \subset M$ un sous-module, N est un sous-groupe (abélien) $\implies$ on a un groupe abéline quotient M/N .
De plus, M/N est un A-module pour la loi externe suivante:

$$a \in A,\ [x] \in M/N \implies a \cdot [x] := [a \cdot x]$$

Comme dans le cas des espaces vectoriels, tout se généralise, en particulier le théorème d'isomorphisme: Tout $\varphi : M \to M'$ application A-linéarie définit un isomorphisme $\overline{\varphi} : {}^{M}\!/_{\mathrm{Ker}(\varphi)} \to \mathrm{Im}(\varphi)$

3.5 Classification des modules de génération finie sur un anneau euclidien

Terminologie

Un A-module M est somme directe (interne) de sous-modules $M_1, \dots, M_n$ si tout $x \in M$ s'écrit de manière unique $x = x_1 + \cdots + x_n$, $x_i \in M_i \quad \forall i$.

Remarque

1. La Proposition III.1 s'étend verbatim: $M \cong M_1 \oplus \cdots \oplus M_n$.

2. M est somme diecte de M_1 et $M_2 \iff M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$

Exemple

Soit E_f un $K[X]$-module somme directe de $F_1, \dots, F_n \subset E_f$.
On a donc $E_f \cong F_1 \oplus \cdots \oplus F_n$ comme $K[X]$-module. Cela signifie:

1) $E \cong F_1 \oplus \cdots \oplus F_n$ comme K-espace vectoriel (φ $K[X]$-lin. $\implies$ φ K-linéaire).
Ainsi, si S_i est une base de F_i, alors $S = S_1 \cup \cdots \cup S_n$ est une base de E (sur K).

2) $F_i \subset E_f$ sous $K[X]$-module $\implies f(F_i) \subset F_i$.

ainsi, dans une base de la forme $S = S_1 \cup \cdots \cup S_n$, une amtrice pour f sera:

$$\mathrm{Mat}_f = \begin{pmatrix} \mathrm{Mat}_{f_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \mathrm{Mat}_{f_n} \end{pmatrix}, \quad \text{où} \quad f_i = f|_{F_i} \in \mathrm{End}(F_i)$$

Terminologie

Un A-module M est dit cyclique si:

$$\exists x_0 \in M \quad \text{tel que} \quad \forall x \in M,\ x = a \cdot x_0 \quad \text{pour un } a \in A$$

Exemples

1. Un K-module cyclique est soit $M = \{0\}$, soit $M = K$.

2. Un $\mathbb{Z}$-module cyclique est un groupe cyclique (ie: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$).

3. $M = A$ est un A-module cyclique. (prendre $x_0 = 1_A$).
Plus généralement, si I est un idéal de A, A/I est un A-module cyclique.
(Posons $x_0 = [1_A]$: Tout $x \in A/I$ s'écrit $x = [a]$ pour $a \in A$, et on a: $x = [a] = [a \cdot 1_A] = a \cdot [1_A] = a \cdot x_0$)
Pour $A = K$ et $\mathbb{Z}$, on retrouve les exemples 1 et 2. En fait, tous les modules cycliques sont de cette forme !

Proposition III.12

Soit A un anneau commutatif. Alors, si M est un A-module cyclique, il existe un idéal $I \subset A$ tel que $M \cong A/I$.

Preuve:
Soit M un A-module cyclique, engendré par $x_0 \in M$.
Posons $\varphi : A \to M$, $\varphi(a) = a \cdot x_0$. C'est une application A-linéaire:

$$\varphi(a+b) = (a+b)x_0 \overset{(M3)}{=} ax_0 + bx_0 = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = (ab)x_0 \overset{(M2)}{=} a(bx_0) = a\varphi(b)$$

De plus, φ est surjective car x_0 engendre M. Finalement, $\operatorname{Ker}\varphi$ est un sous-module de A, donc un idéal I car A commutatif.
Par le Théorème d'isomorphisme, on a un isomorphise $\underline{\varphi} : {}^{A}\!/_{I} \to M$.

□

Corollaire III.13

Si A est euclidien, tout A-module cyclique est isomorphe à ${}^{A}\!/_{(x)}$ pour un certain $x \in A$.

Preuve:
Découle de Proposition III.12 et Proposition II.10.

□

Terminologie

Un A-module M est dit degénération finie s'il existe $x_1, \ldots, x_n \in M$ tesl que tout $x \in M$ s'écrit $x = a_1x_1 + \cdots + a_nx_n$ avec $a_i \in A$.

Exemples

1. Pour $A = K$ un corps, un K espace vectoriel est de génération finie $\iff$ il est de dimension finie.

2. Pour $A = \mathbb{Z}$, si un groupe abélien est fini, alros il est de génération finie.

Théorème III.14

Soit A un anneau euclidien. Tout A-module de génération finie est somme direct d'un nombre fini de sous-modules cycliques.

Théorème III.15: Classification des modules de génération finie sur A euclidien

Soit A un anneau euclidien, et M un A-module de génération finie. Alors, il existe des entiers $r, n \geq 0$, des éléments premiers $p_1, \ldots, p_n \in A$ (pas forcément distincts) et des entiers $\nu_1, \ldots, \nu_n \geq 1$ tels que:

$$M \cong A^r \oplus {}^{A}\!/_{(p_1{}^{\nu_1})} \oplus \cdots \oplus {}^{A}\!/_{(p_n{}^{\nu_n})}$$

Preuve:
Soit donc M un A-module de génération finie.
Par le Théorème III.14 (A euclidien), il existe $M_1, \ldots, M_m$ sous-modules cycliques de M tels que $M \cong M_1 \oplus \cdots \oplus M_m$.
Par corollaire III.13 (A euclidien), il existe $x_1, \ldots, x_m \in A$ tels que $M_i \cong {}^{A}\!/_{(x_i)} \quad \forall i$.

On a donc: $M \cong {}^{A}\!/_{(x_1)} \oplus \cdots \oplus {}^{A}\!/_{(x_m)}$.

- Si $x_i = 0$, on a $M_i \cong {}^{A}\!/_{(0)} = A$, qui contribue à A^r.
- Si $x_i \in A^*$, on a $M_i \cong {}^{A}\!/_{A} = \{0\}$, qui ne contribue pas.
- Si $x \in A$, $x \notin A^*$, $x \neq 0$, alors , par le théorème II.15 (A euclidien), il existe des premiers $P_1, \ldots, p_l$, des entiers $\mu_1, \ldots, \mu_l \geq 1$ et $u \in A^*$ tels que $x = up_1^{\mu_1} \cdots p_l^{\mu_l}$.

$$\Longrightarrow \quad {}^{A}\!/_{(x)} \;=\; {}^{A}\!/_{(p_1^{\mu_1} \cdots p_l^{\mu_l})} \;\cong\; {}^{A}\!/_{(p_1^{\mu_1})} \oplus \cdots \oplus {}^{A}\!/_{(p_l^{\mu_l})}$$

Par le Théorème des restes chinois (ex. 7, S. 10).

(Vu pour $l = 2$, mais le cas général est par induction)
(Vu comme isomophisme d'anneaux, mais c'est trivialement un isomorphisme de A-module).

□

Remarques

1. En fait, les données du théorème (les entiers, les premiers etc) sont uniques ! Mais on ne le démontrera pas.
2. C'est vrai pour tout anneau A principal.

Exemples

1. $A = K$ un corps: Il n'existe pas de premiers dans K, et l'on obtinet donc:
   Tout espace vectoriel de dimension finie sur K est isomorphe à K^r pour un $r \geq 0$.
   (On ne démontre pas ici l'unicité de ce $r \geq 0$, qui repose sur la notion de dimension.)
2. $A = \mathbb{Z}$. Comme tout groupe abélien fini est un $\mathbb{Z}$-module de génération finie, et que la somme directe de $\mathbb{Z}$-module est notée $\times$ pour les groupes abéliens, on obtient donc:

   Théorème III.16

   Tout groupe abélien fini est isomorphe à ${}^{\mathbb{Z}}\!/_{p_1^{\nu_1}\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{p_n^{\nu_n}\mathbb{Z}}$, pour certains premiers $p_1, \ldots, p_n \in \mathbb{Z}$ (pas distincts à priori), et entiers $\nu_1, \ldots, \nu_n \geq 1$.

   Remarque

   C'est le théorème énoncé au paragraphe I.8, sans l'unicité (et avec une "forme normale" différente).

3. $A = \mathbb{C}[X]$. Soit E un espace vectoriel sur $\mathbb{C}$ de dimension finie, et soit $f \in \mathrm{End}(E)$. Cela définit une structure de $\mathbb{C}[X]$-module sur E, noté E_f, via: $X \cdot v = f(v) \quad \forall v \in E$.
   E est de dimension finie sur $\mathbb{C} \implies E$ enendré sur $\mathbb{C}[X]$ par ces m'emes éléments. On peut donc appliquer le théorème III.15 à E_f:

   Il existe $r, n \geq 0$, une suite $p_1, \ldots, p_n$ de premiers $\in \mathbb{C}[X]$, et des entiers $\nu_1, \ldots, \nu_n \geq 1$ tels que:

$$E_f \cong \mathbb{C}[X]^r \oplus {}^{\mathbb{C}[X]}\!/_{(p_1^{\nu_1})} \oplus \cdots \oplus {}^{\mathbb{C}[X]}\!/_{(p_n^{\nu_n})}$$

Observations

- $\dim_{\mathbb{C}} \mathbb{C}[X] = \infty$, $\dim_{\mathbb{C}} E < \infty \implies r = 0$.

- Comme on l'avait vu en fin de Chapitre II: Les premiers de $\mathbb{C}[X]$ sont de la forme $X - \lambda$, avec $\lambda \in \mathbb{C}$.
  $\implies$ il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ et des entiers $\nu_1, \ldots, \nu_n \geq 1$ (pas forcément distincts) tels que

$$E_f \cong \mathbb{C}[X]\Big/((X-\lambda_1)^{\nu_1}) \oplus \cdots \oplus \mathbb{C}[X]\Big/((X-\lambda_n)^{\nu_n})$$

- Par l'exemple vu au début du paragraphe III.5, $\mathrm{Mat}_f = \begin{pmatrix} \mathrm{Mat}_{f_1} & & 0 \\ & \ddots & \\ 0 & & \mathrm{Mat}_{f_n} \end{pmatrix}$,
  où $f_i := f|_{\mathbb{C}[X]\Big/((X-\lambda_i)^{\nu_i})}$, $i = 1, \ldots, n$. et f est donnée par la multiplication par $X \in \mathbb{C}[X]$.

- Tentons donc de calculer une matrice pour la multiplication par X dans le $\mathbb{C}$-espace vectoriel.
  $\mathbb{C}[X]\Big/((X-\lambda)^{\nu})$, où $\lambda \in \mathbb{C}$, $\nu \geq 1$.
  Une base du $\mathbb{C}$-espace vectoriel $\mathbb{C}[X]\Big/((X-\lambda)^{\nu})$ est donnée par:

$$e_1 = [(X-\lambda)^{\nu-1}],\ e_2 = [(X-\lambda)^{\nu-2}], \ldots,\ e_{\nu-1} = [(X-\lambda)],\ e_\nu = [1]$$

  Calculons la matrice de la multiplication par X dans la base $e_1, \ldots, e_\nu$, matrice notée $J_\nu(\lambda)$:

$$0 = [(X-\lambda)^{\nu}] = [(X-\lambda)(X-\lambda)^{\nu-1}] = (X-\lambda)[(X-\lambda)^{\nu-1}] = (X-\lambda)\cdot e_1 = Xe_1 - \lambda e_1 \implies X \cdot e_1 = \lambda e_1$$
$$e_1 = [(X-\lambda)^{\nu-1}] = (X-\lambda)[(X-\lambda)^{\nu-2}] = (X-\lambda)e_2 = Xe_2 - \lambda e_2 \implies Xe_2 = \lambda e_2 + e_1$$

$$J_\nu(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ \vdots & 0 & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix} \quad \text{de taille} \quad \nu \times \nu$$

Conclusion

Si E est un espace vectoriel de dimention finie sur $\mathbb{C}$ et $f \in \mathrm{End}(E)$, alors il existe une base de E dans laquelle $\mathrm{Mat}_f = F_{\nu_1}(\lambda_1) \oplus \cdots \oplus J_{\nu_n}(\lambda_n)$, pour des $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ et $\nu_1, \ldots, \nu_n \geq 1$.
C'est la forme normale de Jordan.

Remarque

On peut faire de même sur $\mathbb{R}$, en utilisant la caractésisation des premiers $\in \mathbb{R}[X]$ vue à l'ex. 6, S. 10.