Maths

Algèbre
Vocabulaire d'ensemble structuré

Algèbre Linéaire
Algorithme du pivot de Gauss
Base duale, antéduale
Condition de liberté d'une forme linéaire à une famille
Développement du déterminant par ligne ou par colonne
Endomorphismes nilpotents
Espaces supplémentaires
Intersection d'hyperplans
Lemme de factorisation
Liberté d'une famille de l'espace dual
Notations de matrices
Somme directe de sous espaces vectoriels
Théorème de la base téléscopique
Vandermonde, interpolation de Lagrange

Algèbres
Algèbre engendrée
Algèbres
Algèbres commutatives intègres de dimension finie
Algèbres et extensions de corps
Clôture algébrique des rationnels
Condition d'intégrité d'une sous-algèbre engendrée
Morphisme d'algèbre
Nombres algébriques
Sous algèbres
inversibilité des éléments d'une sous-algèbre engendrée

Anneaux et Corps
Irréductibles d'un anneau

Anneaux et corps
Axiomes d'un anneau
Axiomes d'un corps
Axiomes d'un sous-corps
Corps des fractions
Corps gauche, anneau à division
Diviseur de zéro
Groupe des inversibles
Idéal d'un anneau
Idéaux maximaux, anneaux quotientés
Intégrité d'un anneau
Primalité de la caracèristique d'un corps

Arithmétique
Fonctions arithmétiques : Möbius et indicatrice d'Euler
Formule du nombre de diviseurs
Indicatrice d'Euler
Lemme d'Euclide
Nombres de Fermat
Petit théorème de Fermat
Propriétés diviseurs communs
Théorème de Bézout
Théorème de Gauss
Théorème de Wilson
Théorème des restes chinois
Équations diophantiennes

Ensembles
Formule du crible

Espaces Vectoriels
Axiomes d'un espace vectoriel
Formes lineaires et hyperplans
Théorème de caractérisation du rang

Groupes
Actions de groupe
Axiomes d'un groupe
Axiomes d'un sous-groupe
Démonstration du Théorème de Lagrange
Dévissage de groupes
Exercice : Les p-groupes
Exercice : élément d'ordre p dans un groupe d'ordre divisé par p
Formule des classes
Groupe Diédral
Groupes quotientés
Relation de cardinal pour un morphisme de groupe
Signature d'une permutation
Théorème de Burnside
Théorème de Lagrange
Éxistence et unicité des sous groupes de groupe cyclique

Matrices
Matrices sembables
Théorème de caractérisation des matrices inversibles

Polynômes
Contenus d'un polynôme à coéfficients entiers
Critère d'Eisenstein
Décomposition en éléments simples
Entiers algébriques
Fonctions symétriques des racines
Formule de Taylor-Langrange formelle
Multiplicité d'une racine
Polynômes associés
Polynômes cyclotomiques
Polynômes de Tchebycheff
Polynômes en caractèristique strictement positive
Polynômes irréductibles
Polynômes scindés
Propriétés des fractions rationelles
Propriétés des racines d'un polynôme

Relations
Majorant, borne supérieure, élément maximale

Calculs
Formule de newton
Formules sur les coéfficients binomiaux

Exercice

Algèbre Générale
Dévissage de groupes
Exercice : Cyclicité des sous-groupes finis des inversibles d'un corps
Exercice : Dénombrement de morphismes
Exercice : Groupe d'éléments d'ordre inférieur à deux
Exercice : Les carrés de Fp
Exercice : Les p-groupes
Exercice : existence d'un élément d'ordre du ppcm de deux autres
Exercice : élément d'ordre p dans un groupe d'ordre divisé par p

Algèbre Linéaire
Exercice : Noyaux et images itérées
Exercice : Union de sous espaces vectoriels
Exercice : endomorphisme qui stabilise toutes les droites
Exercice : rang d'une comatrice

Polynômes
Exercice : Gauss-Lucas
Exercice : Irréductibilité dans les rationels
Exercice : Polynômes à coéfficients entiers
Exercice : Produit de polynômes de rationels unitaire entier
Exercice : rationalité d'une racine de haute multiplicité

Formule de newton

Soit $n \in \mathbb{N}, x, a, b \in \mathbb{C}$

$$x^n - 1 = ?$$

$$a^n - b^n = ?$$

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

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-k-1}$$

Formules sur les coéfficients binomiaux

Soit $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = ? \qquad \binom{n}{n} = ?$$

$$\sum_{k=0}^{n} \binom{n}{k} = ? \qquad k\binom{n}{k} = ?$$

$$\binom{n}{n-k} = ? \qquad \binom{k}{p}\binom{n}{k} = ?$$

$$\binom{n}{k} + \binom{n}{k+1} = ?$$

Soit $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = \binom{n}{n} = 1$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$\binom{n}{n-k} = \binom{n}{k}$$

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

$$\binom{k}{p}\binom{n}{k} = \binom{n}{p}\binom{n-p}{k-p}$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Formule du crible

Formule du crible : soit $A_1, \dots, A_n \subseteq E$

$$\left|\bigcup_{k=1}^{n} A_k\right| = ?$$

Soit $A_1, \dots, A_n \subseteq E$

$$\begin{aligned}\left|\bigcup_{k=1}^{n} A_k\right| &= |A_1|+|A_2|+\cdots+|A_n| \\ &\quad - |A_1\cap A_2|-\cdots-|A_{n-1}\cap A_n| \\ &\quad + |A_1\cap A_2\cap A_3|+\cdots+|A_{n-2}\cap A_{n-1}\cap A_n| \\ &\quad \vdots \\ &\quad + (-1)^n |A_1\cap A_2\cap\cdots\cap A_n|\end{aligned}$$

$$= \sum_{k=1}^{n} (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} \left|\bigcap_{j=1}^{k} A_{i_j}\right|$$

Majorant, borne supérieure, élément maximale

Soit $(E, \leq)$ un ensemble ordonné et $A \subseteq E$, définitions de

- Majorant
- Maximum
- Borne supérieure
- Élément maximale

Soit $(E, \leq)$ un ensemble ordonné et $A \subseteq E$.

Majorant $M \in E$ est un majorant de A si $\forall x \in A, x \leq M$

Maximum M est le maximum de A si M est un majorant de A et $M \in A$. S'il existe il est unique.

Borne supérieure B est la borne supérieure de A si B est le plus petit majorant de A : $\forall M \in E, (\forall x \in A, x \leq M) \Rightarrow B \leq M$. Si elle existe elle est unique.

Élément maximale M est un élément maximale de A si M n'est plus petit que personne : $\nexists x \in A, M \leq x$. Dans le cas d'un ensemble totalement ordonné, seul un maximum est élément maximale, dans le cas d'un ensemble non totalement ordonné, il peut en exister plusieurs.

Axiomes d'un groupe

Soit G un ensemble muni d'une opération interne $*$, quels axiomes pour que $(G, *)$ ait une structure de groupe ?

Soit G un ensemble et $*$ une opération interne, $(G, *)$ forme un groupe si

i) Associativité :

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

ii) Existence d'un neutre :

$$\exists e \in G, \forall x \in G, x * e = e * x = x$$

iii) Existence d'inverse :

$$\forall x \in G, \exists y \in G, x * y = y * x = e$$

Vocabulaire d'ensemble structuré

Définitions du vocabulaire suivant

- Magma
- Semi-groupe
- Monoïde
- Groupe

Ensemble	Loi interne	Associative	Neutre	Inverse	Nom
×	×				Magma
×	×	×			Semi-groupe
×	×	×	×		Monoïde
×	×	×	×	×	Groupe

Axiomes d'un sous-groupe

Soit $(G, *)$ un groupe, quels axiome pour que $H \subseteq G$ soit un sous-groupe ?

Soit $(G, *)$ un groupe et $H \subseteq G$, H est un sous-groupe de G si

i) Présence du neutre :

$$e \in H$$

ii) Stable par $*$:

$$\forall x, y \in H, x * y \in H$$

iii) Stable par inverse :

$$\forall x \in H, x^{-1} \in H$$

Théorème de Lagrange

Énoncer le théorème de Lagrange sur les groupes.

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G

$$|H| \mid |G|$$

Démonstration du Théorème de Lagrange

Démonstration du théorème de Lagrange

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe.

- Relation quotienté par H : $x \mathcal{R} y$ si $yx^{-1} \in H$ (relation d'équivalence). On note G/H l'ensemble des classes d'équivalences.
- Soit $x \in G$, $\bar{x}$ sa classe d'équivalence pour $\mathcal{R}$. $\bar{x} = Hx = \{hx, h \in H\}$.

  Par double inclusion :
  - $Hx \subseteq \bar{x}$: Soit $y \in Hx$, $y = hx$ avec $h \in H$, donc $yx^{-1} = h \in H$ d'où $y \mathcal{R} x$ et $y \in \bar{x}$.
  - $\bar{x} \subseteq Hx$: Soit $y \in \bar{x}$, $yx^{-1} = h \in H$, donc $y = hx \in Hx$.
- Donc $\forall x \in G, \bar{x} = Hx \simeq H$ d'où $|\bar{x}| = |H|$.
- Enfin par le lemme du berger : $|G/H| = \frac{|G|}{|H|}$ et donc $|H| \mid |G|$.

Relation de cardinal pour un morphisme de groupe

Soient $(G_1, +), (G_2, \cdot)$ des groupes et $\varphi : G_1 \to G_2$ un morphisme, avec G_1 fini. Que peut on dire de $|G_1|$?

Soient $(G_1, +), (G_2, \cdot)$ des groupes et $\varphi : G_1 \to G_2$ un morphisme, avec G_1 fini.

$$|G_1| = |\ker \varphi| \cdot |\operatorname{im} \varphi|$$

Axiomes d'un anneau

Soit A muni de deux opérations internes $+$ et $\cdot$, quels axiomes pour que $(A, +, \cdot)$ soit un anneau ?

$(A, +, \cdot)$ est un anneau si :

i) $(A, +)$ est un groupe abélien
   a) Associativité de $+$
   b) Existence d'un neutre additif (0_A)
   c) Existence d'opposés $(-x)$
   d) Commutativité de $+$
ii) Associativité de $\cdot$
iii) Existence d'un neutre multiplicatif (1_A)
iv) Distributivité de $\cdot$ sur $+$

$$x(y+z) = xy + xz$$
$$(x+y)z = xz + yz$$

Diviseur de zéro

Définition de diviseur de 0 dans un anneau.

Soit $(A, +, \cdot)$ un anneau, $x \in A$ est dit diviseur de 0 (à gauche) si $x \neq 0$ et $\exists y \neq 0, \quad xy = 0$

Intégrité d'un anneau

Définition d'un anneau intègre.

Un anneau $(A, +, \cdot)$ est dit intègre si

- A est commutatif
- A n'admet aucun diviseur de 0

Groupe des inversibles

Définition de groupe des inversibles d'un anneau.

Le groupe des inversibles d'un anneau $(A, +, \cdot)$, est le groupe $(A^\times, \cdot)$.

Idéal d'un anneau

Définition d'un idéal d'un anneau, propriétés élémentaires.

Soit $(A, +, \cdot)$ un anneau et $I \subseteq A$, I est un idéal de A si

- I est un sous-groupe additif de A
- I est stable par produit externe : $\forall x \in I, \forall a \in A, ax \in I$

Propriétés :

- Si $1 \in I$ idéal de A, alors $I = A$.
- Plus généralement s'il existe $x \in I$ inversible, $I = A$.
- Une intersection quelconque d'idéaux est un idéal.
- Une somme finie d'idéaux est un idéal.
- Si $\varphi : A_1 \to A_2$ un morphisme d'anneau avec A_1 commutatif, $\ker \varphi$ est un idéal de A_1.
- Pour tout $b \in A$, bA est un idéal de A.
- Un idéal engendré par un ensemble est le plus petit idéal le contenant, dans le cas d'un singleton $\{a\} \subset A$, il s'agit de aA.

Axiomes d'un corps

Soit K muni de deux opérations internes $+$ et $\cdot$, quels axiomes pour que $(K, +, \cdot)$ soit un corps ?

$(K, +, \cdot)$ est un corps si :

i) $(K, +)$ est un groupe abélien
   a) Associativité de $+$
   b) Existence d'un neutre additif (0)
   c) Existence d'opposés $(-x)$
   d) Commutativité de $+$
ii) Associativité de $\cdot$
iii) Commutativité de $\cdot$
iv) Existence d'un neutre multiplicatif (1)
v) Distributivité de $\cdot$ sur $+$
vi) Existence d'inverses (sauf pour 0)

$$\forall x \in K \setminus \{0\}, \exists x^{-1} \in K$$
$$x x^{-1} = x^{-1} x = 1$$

Corps gauche, anneau à division

Qu’est-ce qu’un “corps gauche” ou “anneau à division” ?

Un corps gauche ou anneau a division et un anneau non commutatif dont tous les éléments sont inversible sauf 0. C’est un corps dont le produit n’est pas commutatif.

Axiomes d'un sous-corps

Soit $(K, +, \times)$ un corps, axiomes pour que $L \subseteq K$ soit un sous-corps ?

$(K, +, \times)$ un corps, $L \subseteq K$ est un sous-corps si :

i) $0 \in L$
ii) $1 \in L$
iii) Stable par $+$
iv) Stable par $-$ ou stable par opposé
v) Stable par $\times$
vi) Stable par $\nabla \cdot$ ou stable par inverse

Primalité de la caracèristique d'un corps

Si $(K, +, \cdot)$ est un corps de caractèristique non nulle, que peut-on dire sur celle ci ?

$(K, +, \cdot)$ un corps, notons p sa caractèristique, si $p \neq 0$ alors p est premier

Démonstration:

Notons $p = ab$ avec $a, b \in \mathbb{N}$

$$\begin{aligned}\left(\sum_{k=1}^{a} 1\right)\left(\sum_{k=1}^{b} 1\right) &= \sum_{k=1}^{a}\sum_{k=1}^{b} 1 \\ &= \sum_{k=1}^{ab=p} 1 \\ &= 0\end{aligned}$$

Or un corps n'admet pas de diviseurs de 0, donc $\sum_{k=1}^{a} 1 = 0$ ou $\sum_{k=1}^{b} 1 = 0$, d'où

$$\text{ou} \quad \begin{matrix} a = p, b = 1 \\ p = b, a = 1 \end{matrix}$$

Donc p est premier.

Corps des fractions

Définition du corps des fractions d'un anneau intègre.

$(A, +', \cdot)$ un anneau intègre.

- Soit $(a, b), (c, d) \in A \times A \setminus \{0\}$, on définit la relation d'équivalence suivante :

$$(a, b)\ \mathcal{R}\ (d, c) \text{ si } ad = bc$$

- On note $\frac{a}{b}$ la classe d'équivalence de (a, b).
- On définit les opérations $+, \times$ sur les fractions

$$\frac{a}{b} + \frac{c}{d} = \frac{ad +' cb}{bd}$$
$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Le corps des fractions de A est le corps

$$(A \times A \setminus \{0\}, +, \times)$$

Théorème de Gauss

Théorème de Gauss.

Soit $a, b, c \in \mathbb{N}$, si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$

Équations diophantiennes

Résolutions d'une équation de la forme $ax + by = c$ dans $\mathbb{Z}$.

Soit $a, b, c \in \mathbb{Z}$

$$(E) : \quad ax + by = c$$

- Solution homogène : On cherche un couple $(u, v) \in \mathbb{Z}^2$ (Bézout) tel que

$$au + bv = c$$

- Solution particulière : il en existe si

$$a \wedge b \mid c$$

- Les solutions sont

$$S = \begin{cases} x = x_p - kb' \\ y = y_p + ka' \end{cases}$$

avec (x_p, y_p) solution particulière

$$\text{et } a' = \frac{a}{a \wedge b}, \quad b' = \frac{b}{a \wedge b}$$

Nombres de Fermat

Que sont les nombres de Fermat, et quelques propriétés.

Le n-ème nombre de Fermat est

$$F_n = 2^{2^n} + 1$$

Ils sont impaires et premier entre eux :

Soit $n < m \in \mathbb{N}$,

$$\begin{aligned}
&\left(2^{2^n} - 1\right) \cdot F_n && \cdot F_{n+1} \cdots F_{m-1} \\
&\left(2^{2^n} - 1\right) \cdot \left(2^{2^n} + 1\right) && \cdot F_{n+1} \cdots F_{m-1} \\
&\left(2^{2^{n+1}} - 1\right) && \cdot F_{n+1} \cdots F_{m-1} \\
&\vdots \\
&2^{2^m} - 1 = F_m - 2
\end{aligned}$$

Donc $F_n \mid F_m - 2$, d'où $F_m \wedge F_n \mid F_m - 2$, donc $F_m \wedge F_n \mid 2$, mais ils sont impaire donc premier entre eux.

Lemme d'Euclide

Théorème du lemme d'Euclide.

Soit $p \in \mathbb{P}, a, b \in \mathbb{Z}$,

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b$$

Plus algébriquement :

$\mathbb{Z}/p\mathbb{Z}$ est un anneaux intègre :

$$ab \equiv 0\ [p] \Rightarrow a \equiv 0\ [p] \text{ ou } b \equiv 0\ [p]$$

Formule du nombre de diviseurs

Formule du nombre de diviseurs d'un entier.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\text{nombre de diviseurs} = \prod_{i=1}^{k} (\alpha_k + 1)$$

Théorème des restes chinois

Théorème des restes chinois.

Soit $n, m \in \mathbb{N}^*$ premiers entre eux

- Formulation arithmétique :

$$\forall a \in [\![0, m-1]\!], \forall b \in [\![0, n-1]\!],$$
$$\exists! x \in [\![0, nm-1]\!],$$
$$x \equiv a\ [m] \text{ et } x \equiv b\ [n]$$

- Formulation algébrique :

$$\varphi : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & \binom{x\ [m]}{x\ [n]} \end{array}$$

  est un isomorphisme d'anneaux.
- Structure de preuve : injectivité par $\ker \varphi$ + argument de cardinal.

Petit théorème de Fermat

Petit théorème de Fermat.

- Première formulation :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$
$$a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 \ [p]$$

- Deuxième formulation (moins forte) :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$
$$a^p \equiv a \ [p]$$

- Démo : On étudie $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$$
$$\text{ord}(a) \mid p - 1 \text{ (Lagrange)}$$
$$\text{donc } a^{p-1} \equiv 1 \ [p]$$

Indicatrice d'Euler

Définition de l'indicatrice d'Euler, et propriétés.

La fonction indicatrice d'Euler est

$$\varphi : \begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{N} \\ n & \mapsto & \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \end{array}$$

Quelques propriétés :

$$\varphi(p) = p - 1$$

$$\varphi(p^a) = p^a - p^{a-1}$$

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi\left(n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = \prod_{i=1}^{k} \left(p_i^{\alpha} - p_i^{\alpha-1}\right)$$

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

$$\sum_{d \in \mathrm{Div}(n)} \varphi(d) = n$$

Pour se convaincre de la dernière :

$$\frac{1}{n} + \frac{2}{n} + \cdots + \frac{n}{n}$$

Sous formes irréductibles ($p_i \wedge q_i = 1$)

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} + \cdots + \frac{p_n}{q_n}$$

Il y a n fractions, les $q_i \in \mathrm{Div}(n)$, et pour chaque q_i, on a tous les $p_i \leq q_i$, qui sont premiers avec eux :

$$\underbrace{\sum_{d \in \mathrm{Div}(n)}}_{\substack{\text{somme sur} \\ \text{tous les} \\ \text{dénominateur}}} \underbrace{\varphi(d)}_{\substack{\text{nombre de} \\ \text{fractions pour le} \\ \text{dénominateur } d}} = \underbrace{n}_{\substack{\text{nombre de} \\ \text{fractions}}}$$

Enfin, une généralisation du petit théorème de Fermat :

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \ [n]$$

Théorème de Bézout

Énoncé et preuve du théorème de Bézout.

- Soient $a, b \in \mathbb{N}$ et $d = a \wedge b$ alors il existe $u, v \in \mathbb{Z}$ tel que $au + bv = d$.
- Preuve : Soit $I = \{au + bv, (u, v) \in \mathbb{Z}\}$

  I est un idéal de $\mathbb{Z}$, donc $\exists d \in \mathbb{Z}, I = d\mathbb{Z}$ (principalité de $\mathbb{Z}$). Donc $d \mid a$ et $d \mid b$.

  Soit ∂ tel que $\partial \mid a$ et $\partial \mid b$. $\forall x \in I, \partial \mid x$, en particulier $\partial \mid d$ d'où $\partial \leq d$.

  $a \wedge b = d \in I$ d'où $\exists u, v \in \mathbb{Z}, d = au + bv$

Propriétés diviseurs communs

Soit $a, b \in \mathbb{Z}$

$$x \mid a \text{ et } x \mid b \text{ ssi } ?$$

$$a \mid y \text{ et } b \mid y \text{ ssi } ?$$

$$a\mathbb{Z} + b\mathbb{Z} = ?$$

$$a\mathbb{Z} \cap b\mathbb{Z} = ?$$

Soit $a, b \in \mathbb{Z}$

$$x \mid a \text{ et } x \mid b \text{ ssi } x \mid (a \wedge b)$$

$$a \mid y \text{ et } b \mid y \text{ ssi } m \mid (a \vee b)$$

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$$

Théorème de caractérisation des matrices inversibles

Énoncé du théorème de caractérisation des matrices inversibles.

Soit $A \in M_n(\mathbb{R})$, les assertions suivantes sont équivalentes :

- A est inversible.
- $A \overset{L}{\sim} I_n$.
- $\text{rg}\, A = n$.
- Le système homogène $AX = 0$ admet une seule solution.
- $\forall Y \in \mathbb{R}^n$ le système homogène $AX = Y$ admet au plus une solution.
- $\forall Y \in \mathbb{R}^n$ le système homogène $AX = Y$ admet au moins une solution.

Polynômes associés

Définition et propriétés des polynômes associés.

Soit $P, Q \in \mathbb{K}[X]$, P et Q sont dit associé si $P \mid Q$ et $Q \mid P$.

P, Q sont associés ssi $\exists \lambda \in \mathbb{K}^\star, A = \lambda B$. Toute class de polynômes associés contient un unique polynôme unitaire (à l'exception de $\{0\}$).

Propriétés des racines d'un polynôme

Propriétés des racines d'un polynôme.

Soit $P \in \mathbb{K}[X]$, $n = \deg P$

En général

1. Si $P \neq 0$, P à au plus n racines (comptées avec multiplicités).
2. L'unique polynôme qui à une infinité de racines est $P = 0$.
3. Si $Q \in \mathbb{K}_n[X]$ et $\exists a_1, ..., a_{n+1} \in \mathbb{K}$ tels que $\forall k \in [\![1, n+1]\!], P(a_k) = Q(a_k)$, alors $P = Q$.

En caractèristique nulle

4. $a \in \mathbb{K}$ est racine de P avec multiplicité m ssi

$$\forall k \in [\![0, m-1]\!], P^{(k)}(a) = 0$$
$$\text{et } P^{(m)}(a) \neq 0$$

Démonstration

1. Si $a_1, ..., a_N \in \mathbb{K}$ sont des racines distinctes de P, et $m_1, ..., m_N \in \mathbb{N}^*$ leurs multiplicités.

   Pour tout $k \in [\![1, N]\!], (X - a_k)^{m_k} \mid P$

   Or pour $i < j \in [\![1, n]\!]$

   $$(X - a_i) - (X - a_j) = a_j - a_i$$

   Relation de Bézout ($a_j - a_i$ associé à 1) donc premiers entre eux deux à deux.

   D'où $\prod_{k\in 1}^{N} (X - a_k)^{m_k} \mid P$ et $n \geq \sum_{k=1}^{N} m_k$.

2. Par la propriétés précedente, si P à une infinité de racine distincte il ne peut être de degré positif (ou il serait infini) donc il est nul.

4. Par Taylor-Langrange formel, pour tout $j \in [\![1, m-1]\!]$

$$P = \underbrace{\sum_{k=0}^{j-1} P^{(k)}(a)\frac{(X-a)^k}{k!}}_{R_j(X)\,(\deg < j)} + \underbrace{\sum_{k=j}^{n} P^{(k)}(a)\frac{(X-a)^k}{k!}}_{(X-a)^j Q(X)}$$

   D'où R_j le reste de la division euclidienne de P par $(X - a)^j$. Or a est une racine de multiplicité m ssi

$$\begin{cases} R_m = 0 \\ R_{m+1} \neq 0 \end{cases}$$
$$\Leftrightarrow \begin{cases} \forall k \in [\![0, m-1]\!], \frac{P^{(k)}(a)}{k!} = 0 \\ \exists k \in [\![0, m]\!], \frac{P^{(k)}(a)}{k!} \neq 0 \end{cases}$$
$$\Leftrightarrow \begin{cases} \forall k \in [\![0, m-1]\!], (P^{(k)}(a)) = 0 \\ P^{(m)}(a) \neq 0 \end{cases}$$

Multiplicité d'une racine

Définition de multiplicité d'une racine.

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ une racine et $n \in \mathbb{N}^\star$. On dit que α est de multiplicité n si (l'un ou l'autre) :

- $(X - \alpha)^n \mid P$ mais $(X - \alpha)^{n+1} \nmid P$.
- $\forall k \in [\![0, n-1]\!], P^{(k)}(\alpha) = 0$

Polynômes scindés

Définition et propriétés des polynôme scindés.

Soit $P \in \mathbb{K}[X]$, $a_1, ..., a_k$ ses racines et $m_1, ..., m_k$ leur multiplicités.

- P est scindé si $\deg P = \sum_{i=1}^{k} m_k$.
- P est scindé racines simples si P scindé et $\forall i \in [\![1, k]\!], m_i = 1$.

Propriétés :

- Si P est scindé racines simples sur $\mathbb{R}$, P' aussi.
- Si P est scindé sur $\mathbb{R}$, P' aussi.
- Tout polynôme P est scindé sur $\mathbb{C}$: théorème de Gauss-d'Alembert.

Polynômes irréductibles

Définition et propriétés des polynômes irréductibles.

Soit $P \in \mathbb{K}[X]$, P est dit irréductible si ses seuls diviseurs sont P, 1 et leurs associés.

1. Dans $\mathbb{C}$, les polynômes irréductibles sont les monômes (théorème de Gauss-d'Alembert).
2. Dans $\mathbb{R}$, les polynômes irréductibles sont les monômes et les polŷnomes de degré 2 avec $\Delta < 0$.
3. En général, un polynôme de degré 1 est toujours irréductible.
4. Dans $\mathbb{K}[X]$, un polynôme de degré 2 ou 3 est irréductible ssi il n'admet pas de racine dans $\mathbb{K}$.
5. Dans $\mathbb{K}[X]$, un polynôme de degré ≥ 2 ne peut être irréductible s'il admet une racine dans $\mathbb{K}$.
6. ($\text{car}(\mathbb{K}) = 0$) Un polynôme $P \in \mathbb{K}[X] \subset \mathbb{L}[X]$ irréductible ($\mathbb{L}$ extension de corps de $\mathbb{K}$) n'admet que des racines simples dans $\mathbb{L}$ (et à fortiori dans $\mathbb{K}$).

Démonstration

2. Par les propriétés 3 et 4, on sait que ces polynômes sont irréductibles, montrons que ce sont les seuls.

   Soit $P \in \mathbb{R}[X]$ irréductible de degré ≥ 2.

   $P \in \mathbb{C}[X]$ donc on dispose de $\lambda \in \mathbb{C} \setminus \mathbb{R}$ racine de P.

   $$P\left(\overline{\lambda}\right) = \overline{P}\left(\overline{\lambda}\right) = \overline{P(\lambda)} = 0$$

   D'où ($\text{car } (X - \lambda) \wedge \left(X - \overline{\lambda}\right) = 1$)

   $$Q = \underbrace{X^2 - 2\,\mathrm{Re}(\lambda)X + |\lambda|^2}_{\in \mathbb{R}[X]} \mid P$$

   Comme P est irréductible, P et Q sont associés et $\deg P = 2$.

4. Soit $P \in \mathbb{K}_3[X] \setminus \mathbb{K}_1[X]$
   - S'il est irréductible il n'admet pas de racine.
   - S'il n'est pas irréductible,

     $$P = QR$$

     - Soit $\deg Q = 1$, $Q = X - \alpha$ et α racine de P.
     - Soit $\deg R = 1$, $R = X - \beta$ et β racine de P.

6. $0 \leq \deg P' \leq \deg P - 1$ et par irréductibilité de P dans $\mathbb{K}[X]$

   $$P \wedge P' = 1$$

   Or le PGCD se conserve sur les extensions de corps, ils n'ont donc pas de racine communes (dans $\mathbb{K}$ et $\mathbb{L}$).

Fonctions symétriques des racines

Définition des fonctions symétriques des racines et formules de Viete.

Soit $a_1, ..., a_k \in \mathbb{C}$ et $k \in [\![0, n]\!]$, la k-ème fonction symétrique des élémentaire de $a_1, ..., a_n$ est

$$\sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^{k} a_{i_j}$$

On remarque que $\sigma_0 = 1$.

Soit $P = a_0 + a_1 X + \cdots + a_n X^n$ scindé, on note $a_1, ..., a_n$ ses racines (non distinctes).

Formule de Viete :

$$\forall k \in [\![0, n]\!], \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

Polynômes de Tchebycheff

Définition et propriétés des polynômes de Tchebycheff.

Le n-ème polynôme de Tchebycheff est le polynôme tel que

$$\forall \theta \in \mathbb{R}, T_n(\cos\theta) = \cos(n\theta)$$

Propriétés :

1. Formule de récurrence :
$$T_{n+1} + T_{n-1} = 2XT_n$$
2. $\deg T_n = n$, coéfficient dominant : 2^{n-1}, sauf pour $n = 0$, $T_0 = 1$.
3. T_n est scindé racines simples sur $\mathbb{R}$:
$$T_n(X) = 2^{n-1}\prod_{k=0}^{n-1}\left(X - \cos\frac{(2k+1)\pi}{2n}\right)$$
4. Orthogonalité : si $n \neq p$
$$\int_{-1}^{1} T_n(x)T_p(x)\frac{\mathrm{d}x}{\sqrt{1-x^2}} = 0$$
5. Minimalité en norme :
$$\|P\| = \max_{t\in[-1,1]}|P(t)|$$
Si P unitaire de degré n, alors $\|P\| \geq \frac{1}{2^{n-1}}$.
Avec cas d'égalité si $P(X) = \frac{T_n(X)}{2^{n-1}}$

Preuves :

1. Formules de trigonométrie :
$$\cos((n+1)\theta)+\cos((n-1)\theta)=2\cos\theta\cos(n\theta)$$
$$T_{n+1}(\cos\theta)+T_{n-1}(\cos\theta)=2(\cos\theta)T_n(\cos\theta)$$
Donc ils coincident en une infinité de valeurs $[-1, 1]$, et sont donc égaux.
2. Par récurrence avec la relation de récurrence.
3. On résout $\cos(n\theta) = 0$, on fait attention à distingué les racines.
4. Changement de variable $x = \cos\theta$, puis formules de trigonométrie.
5. Par contraposé : On prend P unitare de degré n tel que $\|P\| \leq \frac{1}{2^{n-1}}$.
   - $P = \frac{1}{2^{n-1}}T_n + Q, \quad \deg Q \leq n-1$.
   - On regarde les y_k quand $T_n(y_k) = \pm 1$.
   - On en déduis le signe de Q
   - Par le TVI Q à n racines donc $Q = 0$.
   - Donc $P(X) = \frac{T_n(X)}{2^{n-1}}$.

Propriétés des fractions rationelles

Propriétés des fractions rationelles

- Si on dit que $\frac{P}{Q}$ est scindé, c'est que Q est scindé.
- Si F admet une infinité de racines alors $F = 0$.
- Si F et G coincident en une infinité de points alors $F = G$.

Décomposition en éléments simples

Formules, propriétés de la décomposition en éléments simples.

Soit $F \in \mathbb{K}(X)$, F se décompose de façon uniqe sous la forme

$F = E + G$ avec $E \in \mathbb{K}[X]$ et $\deg G < 0$

On appelle E la partie entière de F et G la partie pôlaire.

- Si $F = \frac{P}{Q}$ sindé racines simples : soit $a_1, ..., a_n$ les pôles et $Q(X) = (X - a_k)R_k(X)$ pour tout $k \in [\![1, n]\!]$:

  $$F = E + \frac{\lambda_1}{X - a_1} + \cdots + \frac{\lambda_n}{X - a_n}$$

  Avec

  $$\lambda_k = \frac{P(a)}{R_k(a)} = \frac{P(a)}{Q'(a)}$$

- Si F est scindé pôles multiples, on fait la même chose en retranchant les décompositions à chaques fois.

Décomposition en éléments simples de $\frac{P'}{P}$:

$$P(X) = \lambda(X - a_1)^{m_1}...\cdots\cdot(X - a_k)^{m_k}$$

$$\frac{P'(X)}{P(X)} = \frac{m_1}{X - a_1} + \cdots + \frac{m_k}{X - a_k}$$

Axiomes d'un espace vectoriel

Axiomes d'un espace vectoriel.

Sois $\mathbb{K}$ un corps, E muni de la somme interne $+$ et du produit externe $\cdot$ est un $\mathbb{K}$-ev si

1. $(E, +)$ est un groupe abélien.
2. $\forall x \in E, 1 \cdot x = x$.
3. $\forall \lambda \in \mathbb{K}, \forall x, y \in E, \lambda(x + y) = \lambda x + \lambda y$.
4. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, (\lambda + \mu)x = \lambda x + \mu x$.
5. $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, \lambda(\mu x) = (\lambda\mu)x$

Théorème de caractérisation du rang

Énoncé du théorème de caractérisation du rang.

Soit $A \in M_{np}(\mathbb{K})$, $r \in \mathbb{N}$, les assertions suivantes sont équivalentes

- A équivalente par ligne à une matrice échelonné avec r lignes non nulles.
- $\operatorname{rg} \varphi_A = r$
- $\operatorname{rg}\left(C_1, ..., C_p\right) = r$ (avec C_i la i-ème colonne de A)
- $\operatorname{rg}(L_1, ..., L_n) = r$ (avec L_i la i-ème ligne de A)
- $A \overset{L,C}{\sim} J_r$

On dit alors que $\operatorname{rg} A = r$.

On a aussi

$$A \overset{L,C}{\sim} B \text{ ssi } \operatorname{rg} A = \operatorname{rg} B$$

$$\operatorname{rg}(\varphi \circ \psi) = \operatorname{rg} \psi - \dim(\ker \varphi \cap \operatorname{im} \varphi) \leq \min(\operatorname{rg} \varphi, \operatorname{rg} \psi)$$

Formes lineaires et hyperplans

Formes lineaires et hyperplans.

Soit E un $\mathbb{K}$-ev

Un hyperplan de E est un sev de codimension 1, c'est à dire qui admet un supplémentaire de dimension 1.

- Si $a \in E^* \setminus \{0\}$, alors $\ker a$ est un hyperplan.
- Si H est un hyperplan de E, il existe une forme linéaire a unique à constante multiplicative prés tel que $H = \ker a$.

Deux hyperplans on toujours un supplémentaire commun.

Démonstration

- Si H_1 et H_2 sont des hyperplans, $H_1 \cup H_2 \neq E$
  - Par l'absurde : supposons $H_1 \cup H_2 = E$ sev de E

    Or $H_1 \cup H_2 = (H_1$ ou $H_2) = E$ (cf unions de sev) qui est absurde.

  Donc on dispose de $x_0 \in E \setminus (H_1 \cup H_2)$

  Ainsi $\text{Vect}(x_0)$ est un supplémentaire de H_1 et H_2

Matrices sembables

Définition de matrices sembables.

Soit $A, B \in M_{n(\mathbb{K})}$, A est dite sembable à B si

$$\exists P \in \mathrm{GL}_n(\mathbb{K}),\ B = P^{-1}AP$$

Invariants :

- $\mathrm{rg}\, A = \mathrm{rg}\, B$
- $\mathrm{tr}\, A = \mathrm{tr}\, B$
- $\det A = \det B$
- $\chi_A = \chi_B$
- $\mu_A = \mu_B$

Fonctions arithmétiques : Möbius et indicatrice d'Euler

Définition, contexte et démonstration de la fonction de Möbius et la formule d'inversion.

Pour $A = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$ on définit $(*)$, pour $f, g \in A$

$$f * g = \begin{cases} \mathbb{N}^* & \to & \mathbb{C} \\ n & \mapsto & \displaystyle\sum_{d \mid n} f(d) g\left(\frac{n}{d}\right) \end{cases}$$

Qui est une loi de composition interne sur A. On montre que
- $\mathbb{1}_{\{1\}}$ est l'élément neutre.
- $(*)$ est commutatif
- $(*)$ est associatif

On définit la fonction de Möbius, on note $\pi(n) = |\{p \in \mathbb{P}, p \mid n\}|$

$$\begin{array}{rcl} 1 & \mapsto & 1 \\ \mu : n \mid \nexists p \in \mathbb{P}, p^2 \mid n & \mapsto & (-1)^{\pi(n)} \\ n \mid \exists p \in \mathbb{P}, p^2 \mid n & \mapsto & 0 \end{array}$$

On montre de plus

$$\mu * \mathbb{1}_{\mathbb{N}} = \mathbb{1}_{\{1\}}$$

Pour $n \geq 2$ on écrit $n = \prod_{j=1}^{k} p_j^{a_j}$. Un diviseur d s'écrit $\prod_{j=1}^{k} p_j^{\beta_j}$ avec $\beta_j \leq a_j$. Donc

$$\mu(d) \neq 0 \iff \forall j \in [\![1, k]\!], \beta_j \in \{0, 1\}$$

Ainsi

$$\begin{aligned} \sum_{d \mid n} \mu(d) &= \sum_{\beta_1, \ldots, \beta_k \in \{0,0\}} \mu\left(\prod_{j=1}^{k} p_j^{\beta_j}\right) \\ &= \sum_{q=0}^{k} \sum_{I \subset [\![1,q]\!]} (-1)^{|I|} \\ &= \sum_{q=0}^{k} (-1)^q \binom{k}{q} \\ &= 0 \end{aligned}$$

On en déduit la formule d'inversion de Möbius : soit $f : \mathbb{N}^* \to \mathbb{C}$, on pose $g : n \mapsto \sum_{n \mid d} f(d)$ $(g = f * \mathbb{1}_{\mathbb{N}})$, on a alors pour tout $n \in \mathbb{N}$

$$f(n) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right)$$

C'est à dire $f = g * \mu = f * \underbrace{\mathbb{1}_{\mathbb{N}} * \mu}_{\mathbb{1}_{\{1\}}}$.

De plus μ est multiplicative.

Existence et unicité des sous groupes de groupe cyclique

Soit G un groupe cyclique d'ordre n, et $d \mid n$, montrer l'éxistence et l'unicité d'un sous groupe d'ordre d.

Soit G cyclique d'ordre n.

Par isomorphisme à $(\mathbb{Z}/n\mathbb{Z}, +)$, on se ramène à l'étude de $(\mathbb{U}_n, \cdot)$.

Soit H sous groupe de $\mathbb{U}_n$, $|H| = d$.

Pour tout $x \in H$, $x^d = 1$ donc $H \subset \mathbb{U}_d$, par égalité des cardinaux, $H = \mathbb{U}_d$.

Polynômes cyclotomiques

Définitions et propriétés des polynômes cyclotomiques.

Pour $n \in \mathbb{N}^*$ on note

$$\begin{aligned}\mathbb{V}_n &= \{z \in \mathbb{U}_n \mid \text{ord}(z) = n\} \\ &= \left\{e^{\frac{2ki\pi}{n}}, k \in (\mathbb{Z}/n\mathbb{Z})^\times\right\}\end{aligned}$$

On définit de n-ème polynôme cyclotomique

$$\Phi_n(X) = \prod_{\xi \in \mathbb{V}_n} (X - \xi)$$

$$\deg(\Phi_n) = \varphi(n)$$

On montre

$$X^n - 1 = \prod_{d \mid n} \Phi_d$$

$$\Phi_n \in \mathbb{Z}[X]$$

Φ_p irréductible

Démonstration

- Pour $d \mid n$, on a

  $$\mathbb{V}_d = \{z \in \mathbb{U}_n \mid \text{ord}(n) = d\}$$

  Car si $z \in \mathbb{U}_n$ d'ordre d, $z \in <z>$ sous groupe de $\mathbb{U}_n$ de cardinal d, qui est unique car $\mathbb{U}_n$ est cyclique. D'où $z \in \mathbb{U}_d$ et à fortiori $z \in \mathbb{V}_d$.

- On a donc

  $$\mathbb{U}_n = \biguplus_{d \mid n} \mathbb{V}_d$$

  $$\begin{aligned}X^n - 1 &= \prod_{\xi \in \mathbb{U}_n} (X - \xi) \\ &= \prod_{d \mid n} \left(\prod_{\xi \in \mathbb{V}_n} (X - \xi) \right) \\ &= \prod_{d \mid n} \Phi_d\end{aligned}$$

- On montre que la division euclidienne dans $\mathbb{Z}[X]$ par un polynôme unitaire donnent un polynôme dans $\mathbb{Z}[X]$. On refait la démonstration de la division euclidienne (récurrence).

- Récurrence forte sur n pour montrer que $\Phi_n \in \mathbb{Z}[X]$

  $$X^n - 1 = \Phi_n \cdot \left(\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d \right)$$

- Soit $p \in \mathbb{P}$

  $$\begin{aligned}\Phi_p &= \prod_{\substack{\omega \in \mathbb{U}_p \\ \text{ord}(\omega) = p}} (X - \omega) \\ &= \frac{X^p - 1}{X - 1} = \sum_{k=0}^{p-1} X^k\end{aligned}$$

  Remarquons que

  $$\tau : \begin{cases} \mathbb{Q}[X] & \to & \mathbb{Q}[X] \\ P(X) & \mapsto & P(X+1) \end{cases}$$

  est un automorphisme d'anneau.

  D'où $\Phi_p(X)$ irréductible ssi $\Phi_p(X+1)$ irréductible.

  $$\begin{aligned}\Phi_p(X+1) &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \sum_{k=1}^{p-1} \underbrace{\binom{k}{p}}_{\text{divisible par } p} X^{k-1}\end{aligned}$$

  et le coéfficient constant est $\binom{p}{1}$ qui n'est pas divisible par p^2, d'où par le critère d'Eisenstein, Φ_p irréductible dans $\mathbb{Q}[X]$.

Démonstration de $n = \sum_{d \mid n} \varphi(d)$:

$$\begin{aligned}n &= |\mathbb{U}_n| \\ &= \sum_{d \mid n} |\mathbb{V}_d| \\ &= \sum_{d \mid n} \varphi(d)\end{aligned}$$

Groupes quotientés

Définitions et propriétés des groupes quotientés.

Soit G un groupe, H sous-groupe.

On définit la relation d'équivalence

$$\forall (x, y) \in G^2,\ x \sim y \text{ ssi } y \in xH$$

On obtient ainsi les classes à gauche gH pour tout $g \in G$, dont l'ensemble est noté G/H.

H est dit distingué si

$$\forall g \in G,\ gHg^{-1} = H$$

Et dans ce cas G/H à une structure de groupe muni de la multiplication sur les classes

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Et on pose

$$f : \begin{array}{ccc} G & \to & G/H \\ g & \mapsto & gH \end{array}$$

qui est un morphisme de groupe surjectif appelé projection cannonique de G sur G/H dont le noyau est H.

Cas particuliers

- Tous noyau de morphisme est un sous groupe distingué.
- Tous sous-groupe d'indice 2 ($\frac{|G|}{|H|} = 2$) est distingué.

Idéaux maximaux, anneaux quotientés

Définitions d'idéal maximale, anneau quotienté, propriétés.

Soit $(A, +, \cdot)$ un anneau et I idéal de A.

Idéal maximale

Un idéal I de A est dit maximale si pour tout J idéal de A

$$I \subsetneq J \Rightarrow J = A$$

Anneau quotienté

On définit sur A la relation d'équivalence

$$\forall (x, y) \in A^2,\ x \sim y \text{ ssi } x - y \in I$$

On note A/I l'ensemble des classes d'équivalences par cette relation qu'on muni d'une structure de groupe en définissant les loi suivantes

$$\overline{x} + \overline{y} = \overline{x + y}$$
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Qui ne dépend pas du représentant choisis.

Propriétés

- I est maximale ssi tous les éléments non nuls de A/I sont inversibles.
- Si A commutatif, I maximale, alors I est premier (A/I est intègre).

Démonstration :

- On suppose I maximale. Soit $x \in A \setminus I$ c'est à dire $x \notin \overline{0_A}$, montrons que $\overline{x}$ est inversible.

  $I \subseteq xA + I = J$ est un idéal, or I maximale d'où $1_A \in A = J$, d'où l'existence de $y \in A$ et $z \in I$ tel que

  $$xy + z = 1_A$$
  $$\overline{xy} = \overline{1_A}$$
- On suppose les éléments non nuls de I/A inversibles.

  Soit $J \supsetneq I$ idéal de A, donc il existe $x \in J$ tel que $x \notin I$.

  $\overline{x} \neq \overline{0}$ donc $\overline{x}^{-1} = \overline{y}$ existe.

  $$\overline{xy} = \overline{xy} = \overline{1_A}$$
  $$\exists z \in I,\ \underbrace{xy + z}_{\in J} = 1_A$$

  $1_A \in J$ donc $J = A$, I est maximale.
- Soit $x, y \in A$ tels que $xy \in I$, supposons que $x \notin I$. Donc $\overline{x}$ inversible : on dispose de $x' \in A$ et $z \in I$ tels que

  $$xx' + z = 1_A$$
  $$\overbrace{\underbrace{xyx'}_{\in I} + zy}^{\in I} = y \in I$$

Signature d'une permutation

Définitions et propriétés de la signature dans $\mathfrak{S}_n$.

Plusieurs définitions alternatives.

- $\varepsilon : (\mathfrak{S}_n, \circ) \to (\mathbb{Z}^\times, \cdot)$ est l'unique morphisme non triviale.

Pour $\sigma \in \mathfrak{S}_n$:

$$\begin{aligned}\varepsilon(\sigma) &= \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= (-1)^{N_\sigma} \\ &= (-1)^{n - |\mathrm{Orb}(\sigma)|}\end{aligned}$$

Où $N_\sigma = |\{(i, j) \mid i < j \text{ et } \sigma(i) > \sigma(j)\}|$.

Actions de groupe

Définitions et exemples usuels, propriétés des actions de groupes.

Soit G un groupe, X un ensemble. Une action de groupe est la donnée d'un morphisme de groupe

$$\varphi : \begin{cases} G \to \mathfrak{S}(X) \\ g \mapsto \rho_g : \begin{cases} X \to X \\ x \mapsto \rho_g(X) = g.x \end{cases} \end{cases}$$

Ainsi tout groupe fini de cardinal $n \in \mathbb{N}$ est isomorphe à un sous groupe de $\mathfrak{S}_n$.

Démonstration

Grâce à l'action de groupe φ

$$\varphi : \begin{cases} G \to \mathfrak{S}(G) \simeq \mathfrak{S}_n \\ a \mapsto \rho : \begin{cases} G \to G \\ g \mapsto ag \end{cases} \end{cases}$$

Qui est un morphisme de groupe (car $\rho_a \circ \rho_b = \rho_{a,b}$), injectif (car $\ker \varphi = e_G$), d'où $\varphi|_{\varphi(G)}$ isomorphisme de $G \to \varphi(G)$, avec $\varphi(G)$ sous groupe de $\mathfrak{S}(G) \simeq \mathfrak{S}_n$.

Autre action classique

On peut aussi considérer l'action de conjugaison

$$\theta : \begin{cases} G \to \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \to G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On a

$$\begin{aligned} \ker \theta &= \{g \in G \mid \theta(g) = \mathrm{id}\} \\ &= \{g \in G \mid \forall x \in G, gxg^{-1} = x\} \\ &= \{g \in G \mid \forall x \in G, gx = xg\} \\ &= Z(G) \end{aligned}$$

Formule des classes

Énoncé, démonstration et définitions de la formule des classes.

Soit G un groupe et φ une action de G sur un ensemble X. On définit pour tout $x \in X$

$$\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}$$

C'est un sous groupe de G :
- $e.x = x$ d'où $e \in \mathrm{Stab}(x)$
- $\forall g \in \mathrm{Stab}(x), g^{-1}.x = g^{-1}.g.x = x$
- $\forall g, h \in \mathrm{Stab}(x), (gh).x = g.h.x = x$

On définit également

$$\mathrm{Orb}(x) = \{g.x, g \in G\}$$

Qui est la classe d'équivalence de x pour la relation d'équivalence

$$x \sim y \text{ si } \exists g \in G, y = g.x$$

Donc les orbites forment une partition de X.

Formule des classes

Pour tout $x \in X$ fini et G fini

$$|\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)| = |G|$$

Démonstration

Soit $x \in X$, pour $y \in \mathrm{Orb}(x)$, on dispose de $g_0 \in G$ tel que $g_0.x = y$.

Étudions $\{g \in G \mid g.x = y\}$:

$$\begin{aligned} g.x = y &\iff g.x = g_0.x \\ &\iff (g_0^{-1}g).x = x \\ &\iff g_0^{-1}g \in \mathrm{Stab}(x) \\ &\iff g \in g_0\,\mathrm{Stab}\,(x) \end{aligned}$$

D'où

$$G = \biguplus_{y \in \mathrm{Orb}(x)} \{g \in G \mid g.x = y\}$$

$$\begin{aligned} |G| &= \sum_{y \in \mathrm{Orb}(x)} |g_0\,\mathrm{Stab}\,(x)| \\ &= \sum_{y \in \mathrm{Orb}(x)} |\mathrm{Stab}\,(x)| \\ &= |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}\,(x)| \end{aligned}$$

Exercice : Les p-groupes

Définitions d'un p-groupe, et démonstration de

1. Pour G p-groupe, $|Z(G)| = p^\alpha$ avec $\alpha \in \mathbb{N}^*$.
2. Tout groupe G d'ordre p^2 est abélien

Un p-groupe est un groupe dont tout les éléments sont d'odre p^ν avec $p \in \mathbb{P}$. A fortiori, il s'agit d'un groupe de cardinal p^α.

1. On étudie l'action de groupe

$$\varphi : \begin{cases} G \to \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \to G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On montre que

$$x \in Z(G) \text{ ssi } \mathrm{Orb}(x) = \{e_G\}$$

Et par la formule des classes on a pour tout $x \in G$:

$$p^\alpha = |G| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)|$$

Donc $|\mathrm{Orb}(x)| \mid p^\alpha$ d'où si $|\mathrm{Orb}(x)| > 0, p \mid |\mathrm{Orb}(x)|$.

Or les $\mathrm{Orb}(x)$ forment une partition de G donc

$$\begin{aligned} p^\alpha = |G| &= \sum_{x \in G} |\mathrm{Orb}(x)| \\ &= |Z(G)| + \underbrace{\sum_{\substack{x \in G/\sim \\ |\mathrm{Orb}(x)|>1}} |\mathrm{Orb}(x)|}_{\text{divisible par } p} \end{aligned}$$

Donc $p \mid |Z(G)|$ mais $e_G \in Z(G)$ donc $|Z(G)| > 0$ d'où $|Z(G)| \geq p$.

2. Par l'exercice ci dessus

$$Z(G) \in \{p, p^2\}$$

Supposons qu'il existe $x \in G \setminus Z(G)$, alors

$$Z(G) \subset \mathrm{Stab}(x) \text{ et } x \in \mathrm{Stab}(x)$$

Donc $|\mathrm{Stab}(x)| \geq p + 1$ sous-groupe de G donc

$$\mathrm{Stab}(x) = G$$

D'où $x \in Z(G)$, absurde.

Exercice : élément d'ordre p dans un groupe d'ordre divisé par p

Soit G un groupe d'ordre pq avec $p \in \mathbb{P}$ et $q \in \mathbb{N}^*$, démonstration de l'existence d'un élémént d'ordre p.

Soit G d'odre $n = pq$ avec $(p, q) \in \mathbb{P} \times \mathbb{N}^*$.

On pose

$$\Gamma = \{(x_1, ..., x_p) \in G^p \mid x_1 \cdots x_n = e_G\}$$
$$\sigma = (1\ 2 \cdots p) \in \mathfrak{S}_p$$

On considère $H = <\sigma>$ qui agit sur Γ via

$$\varphi : \begin{cases} H & \to & \mathfrak{S}(\Gamma) \\ \sigma^k & \mapsto & \rho_{\sigma^k} \end{cases}$$

Où

$$\rho_{\sigma^k} : \begin{cases} \Gamma & \to & \Gamma \\ (x_1, ..., x_p) & \mapsto & (x_{\sigma^k(1)}, ..., x_{\sigma^k(p)}) \end{cases}$$

(On montre par récurrence sur k que ρ_{σ^k} à bien valeur dans Γ).

On remarque que $|H| = p$ et

$$\forall X = (x_1, ..., x_p) \in G^p,$$
$$X \in \Gamma \Leftrightarrow x_p^{-1} = x_1 \cdots x_{p-1}$$
$$\Gamma \simeq G^{p-1} \text{ donc } |\Gamma| = n^{p-1}$$

Pour tout $x \in \Gamma$ (par la formule des classes)

$$p = |H| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)|$$
$$\text{donc } |\mathrm{Orb}(x)| \in \{1, p\}$$

$$\mathrm{Orb}(x) = \{x\} \Leftrightarrow x_1 = x_2 = \cdots = x_p$$
$$\Leftrightarrow x_1^p = e_G$$

Et

$$n^{p-1} = |\Gamma| = \sum_{x \in \Gamma/\sim} |\mathrm{Orb}(x)|$$
$$= \sum_{\substack{x \in \Gamma/\sim \\ |\mathrm{Orb}(x)| = 1}} 1 + \sum_{\substack{x \in \Gamma/\sim \\ |\mathrm{Orb}(x)| > 1}} p$$
$$= |\{x \in G \mid x^p = e_G\}| + kp$$

Avec $k \in \mathbb{N}$. Or $p \mid n$ donc

$$p \mid |\{x \in G \mid x^p = e_G\}| \geq 1$$

Donc il existe au moins $p - 1$ éléménts d'ordre p.

Cas $n = 2$:

On regroupe les éléments avec leurs inverse, ce qui montre par la parité du cardinale l'éxistence d'un élémént d'ordre 2.

Théorème de Burnside

Énoncer et démonstration du théorème de Burnside.

Soit G un groupe fini qui agit sur un ensemble X fini par φ.

On définit pour $g \in G$

$$\mathrm{Fix}(g) = \{x \in X, g.x = x\}$$

Notons N le nombre d'orbites :

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Démonstration

On étudie

$$\begin{aligned}\Gamma &= \{(g,x) \in G \times X \mid g.x = x\} \\ &= \biguplus_{x \in X} \{(g,x), g \in \mathrm{Stab}(x)\} \\ &= \biguplus_{g \in G} \{(g,x), x \in \mathrm{Fix}(g)\}\end{aligned}$$

Or par la formule des classes

$$|\mathrm{Stab}(x)| = \frac{|G|}{|\mathrm{Orb}(x)|}$$

D'où (en notant x_i représentant du i-ème orbite)

$$\begin{aligned}|\Gamma| &= \sum_{x \in X} |\mathrm{Stab}(x)| \\ &= \sum_{j=1}^{N} \sum_{x \in \overline{x_j}} |\mathrm{Stab}(x)| \\ &= \sum_{j=1}^{N} \sum_{x \in \overline{x_j}} \frac{|G|}{|\mathrm{Orb}(x_j)|} \\ &= N\,|G|\end{aligned}$$

Or

$$|\Gamma| = \sum_{g \in G} |\mathrm{Fix}(g)|$$

D'où

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Exercice : Groupe d'éléments d'ordre inférieur à deux

Propriétés du groupe G tel que $\forall x \in G, x^2 = 1$

On a immédiatement

$$\forall x \in G, x = x^{-1}$$

- G est abélien, soit $x, y \in G$:

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

- Si G fini, $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ et $|G| = 2^n$ pour un $n \in \mathbb{N}$.

  Passons en notation additive pour plus de caireté :

  Faison de G un $\mathbb{F}_2$-ev :

$$\begin{aligned} \mathbb{F}_2 \times G &\to G \\ \left(\overline{k}, g\right) &\mapsto kg \end{aligned}$$

  Qui ne dépend pas du représentant car $2G = \{0\}$.

G un $\mathbb{F}_2$-ev de dimension finie, donc isomorphe à $\mathbb{F}_2^n$ en tant qu'éspace vectoriel, et à fortiori en tant que groupe.

Irréductibles d'un anneau

Définition, propriétés élémentaires sur les irréductibles dans un anneau principal.

Soit $(A, +, \cdot)$ un anneau principal.

- Dans un anneau principal on a un PGCD

  Pour tout $a, b \in A$, il existe $d \in A$ tel que $aA + bA = dA$, unique (à associés près), qu'on appelle PGCD de a et b ($a \wedge b = d$).

  On a aussi Bézout car $d \in dA = aA + bA$ d'où $\exists (u, v) \in A^2, d = au + bv$.
- Un élément de A est dit irréductible si ses seuls diviseurs sont ses associés et les inversibles.
- Pour tout $a \in A$, il existe une unique (à permutation et multiplication par des inversibles près) décomposition de a en irréductibles.

Démonstration de la décomposition

- Toute suite croissante d'idéaux est stationnaire.

  $(I_i)_{i \in \mathbb{N}}$ suite d'idéaux de A croissante au sens de l'inclusion.

  $$K = \bigcup_{i \in \mathbb{N}} I_i$$

  Est encore un idéal car union croissante d'idéaux

  Par principalité de A, $K = zA$ avec $z \in K$ donc on dispose de $k \in \mathbb{N}$ tel que $z \in I_k$ d'où

  $$K = zA \subseteq I_k \subseteq K$$
- Tout élément de A admet au moins un diviseur irréductible dans A.

  Soit $x \in A$, on construit la suite (x_n) par récurrence : $x_0 = x$ et pour $n \in \mathbb{N}$
  - Si x_n irréductible, $x_{n+1} = x_n$
  - Sinon on prend x_{n+1} diviseur de x_n non associés et non inversible.

  Par définition de la divisibilité, $(x_n A)_n$ est une suite croissante d'idéaux, et est donc stationnaire.

  Soit k le rang à partir du quel c'est le cas, x_k est donc un diviseur irréductible de x.
- Existence de la décomposition : récurrence avec la propriété ci dessus.
- Unicité de la décomposition : on prend deux décomposition on montre que chaque irréductible est présent à la même puissance dans les deux.

Polynômes en caractèristique strictement positive

Remarques et mises en gardes à propos de $\mathbb{K}[X]$ quand $\text{car}(\mathbb{K}) > 0$

Soit $\mathbb{K}$ un corps tel que $\text{car}(\mathbb{K}) > 0$

- Le morphisme d'évaluation $\theta : \mathbb{K}[X] \to \mathcal{F}(\mathbb{K}, \mathbb{K})$ n'est pas forcément injectif.

  Dans $\mathbb{F}_p$, $\theta(X^p - X) = \theta(0) = 0_{\mathcal{F}(\mathbb{F}_p, \mathbb{F}_p)}$ or $X^p - 1 \neq 0$.

- Il n'y a pas équivalence entre multiplicité d'une racine et les valeurs des dérivées succéssives.

  Pour $\text{car}(\mathbb{K}) = p \in \mathbb{P}$

  Pour $k \in [\![1, p-1]\!]$

$$\binom{k}{p} = \frac{\overbrace{p(p-1)\cdot\cdots\cdot(p-k+1)}^{p \text{ divise}}}{\underbrace{k!}_{p \text{ ne divise pas}}}$$

  D'où $\binom{k}{p}$ nul dans $\mathbb{K}$.

  Ainsi pour tout $a, b \in \mathbb{K}$

$$\begin{aligned}(a+b)^p &= a^p + b^p + \sum_{k=1}^{p-1}\binom{k}{p}a^k b^{p-k} \\ &= a^p + b^p\end{aligned}$$

  Et on peut définir le morphisme de corps de Frobenius

$$\sigma : \begin{cases} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{cases}$$

  Donc dans $\mathbb{F}_p[X]$

$$Q = (X-1)^p = X^p - 1$$

  1 est racine de multiplicité p de Q or $Q' = 0$ d'où pour tout $k \in \mathbb{N}$, $Q^{(k)}(1) = 0$.

Théorème de Wilson

Énoncer et démonstration du théorème de Wilson.

Pour tout $p \in \mathbb{N}^*$, p est premier ssi $(p-1)! \equiv -1[p]$.

Démonstration

- Soit $n \in \mathbb{N}^*$ non premier.
  - Si $3 \leq n = m^2$ avec $m \in \mathbb{N}^*$. $2m \cdot m \mid (n-1)!$ d'où $(n-1)! \equiv 0[n]$
  - Sinon on dispose de $1 \leq p, q < n$ tels que $n = pq$ d'où $n = pq \mid (n-1)!$ et $(n-1)! \equiv 0[n]$.
- Soit $p \in \mathbb{P}$, étudions $(p-1)!$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$

  Soit $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $x^2 = 1$

  $$(x+1)(x-1) = 0$$

  Donc $x = \{1, -1\}$.

  On peut donc regrouper les éléments du produit $(p-1)!$ avec leurs inverses (qui sont dans le produit), à l'éxception de 1 et -1 d'où

  $$\begin{aligned}(p-1)! &= (p-1)(p-2)\cdot\dots\cdot 1 \\ &= -1 \cdot 1 = 1\end{aligned}$$

  Dans $\mathbb{Z}/p\mathbb{Z}$.

Autre démonstration horrible pour le deuxième sens

Soit $p \in \mathbb{P}$, on étudie $R = X^p - X$ dans $\mathbb{F}_p[X]$.

Pour tout $x \in \mathbb{F}_p$, $R(x) = 0$ donc $(X-x) \mid R$ et premiers entre eux deu x à deux d'où

$$\prod_{x \in \mathbb{F}_p} (X-x) \mid R$$

Et par égalité des degrés on a égalité des polynômes.

Considèrons maintenant le morphisme d'anneau suivant :

$$\pi : \begin{cases} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] \\ \sum_{k=0}^n a_k X^k & \mapsto & \sum_{k=0}^n \overline{a_k} X^k \end{cases}$$

$$Q = \prod_{k=0}^{p-1} (X-k) = X^p + \sum_{k=0}^{p-1} a_k X^k$$

$$\pi(Q) = \prod_{k=0}^{p-1} \left(X - \overline{k}\right) = R$$

$$\begin{aligned} a_1 &= (-1)^{p-1} \sum_{\substack{I \subset [\![0, p-1]\!] \\ |I| = p-1}} \prod_{i \in I} i \\ &= (p-1)! \end{aligned}$$

$$\overline{a}_1 = \overline{(p-1)!} = -1$$

Formule de Taylor-Langrange formelle

Formule de Taylor-Langrange formelle sur $\mathbb{K}[X]$, démonstration.

Soit $\mathbb{K}$ un corps tel que $\text{car}(\mathbb{K}) = 0$, $P \in \mathbb{K}[X]$, $N \geq \deg P$ et $a \in \mathbb{K}$.

$$P = \sum_{k=0}^{N} P^{(k)}(a) \frac{(X-a)^k}{k!}$$

Démonstration

Notons $E = \mathbb{K}_N[X]$ qui est un $\mathbb{K}$-ev de dimension $N+1$.

La famille $\left((X-a)^k\right)_{k \in [\![0,N]\!]}$ est libre car échelonné en degré, c'est donc une base de E, et comme $P \in E$, et comme $P \in E$

$$P = \sum_{k=0}^{N} \lambda_k (X-a)^k$$

Pour $j \in [\![0, N]\!]$

$$\begin{aligned} P^{(j)}(a) &= \sum_{k=j}^{N} \frac{\lambda_k k!}{(k-j)!} (a-a)^{k-j} \\ &= \lambda_j j! \\ \lambda_j &= \frac{P^{(j)}(a)}{j!} \end{aligned}$$

Contenus d'un polynôme à coéfficients entiers

Définitions, propriétés, et démonstrations à propos du contenu dans $\mathbb{Z}[X]$.

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$, on définit le contenu de P comme

$$c(P) = \bigwedge_{k=0}^{d} a_k$$

Et on dit qu'un polynôme P est primitif si $c(P) = 1$.

- Soient $P, Q \in \mathbb{Z}[X]$ tels que $c(P) = c(Q) = 1$, alors $c(PQ) = 1$.A
- Pour tout $P, Q \in \mathbb{Z}[X]$, $c(PQ) = c(P)c(Q)$.

Démonstration

- Soit $p \in \mathbb{P}$, posons le morphisme d'anneau

$$\pi : \begin{cases} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] \\ \sum_{k=0}^{d} a_k X^k & \mapsto & \sum_{k=0}^{d} \overline{a_k} X^k \end{cases}$$

  $c(P) = 1$ donc P admet au moins un coéfficient non divisible par p et de même pour Q.

$$\pi(P) \neq 0 \text{ et } \pi(Q) \neq 0$$
$$\pi(PQ) = \pi(P)\pi(Q) \neq 0$$

  Donc p ne divise pas tous les coéfficients de PQ pour tout $p \in \mathbb{P}$, d'où $c(PQ) = 1$.
- On remarque que pour $P \in \mathbb{Z}[X]$ et $k \in \mathbb{Z}$, $c(kP) = kc(P)$ et on étudie $\tilde{P} = \frac{P}{c(P)}$ et $\tilde{Q} = \frac{Q}{c(Q)}$.

Exercice : Produit de polynômes de rationels unitaire entier

Soient $P, Q \in \mathbb{Q}[X]$ unitaires, montrer que si $PQ \in \mathbb{Z}[X]$ alors $P, Q \in \mathbb{Z}[X]$.

$P, Q \in \mathbb{Q}[X]$ unitaires, $PQ \in \mathbb{Z}[X]$.

Comme PQ unitaire $c(PQ) = 1$. On trouve $a, b \in \mathbb{Z}$ tels que $aP, bQ \in \mathbb{Z}[X]$.

$$c(aP)c(bQ) = abc(PQ) = ab$$

Or P et Q étant unitaires

$$\begin{cases} c(aP) \mid a \\ c(bQ) \mid b \end{cases} \text{ donc } \begin{cases} a = k_a c(aP) \\ b = k_b c(bQ) \end{cases}$$

$$c(aP)c(bQ) = ab = k_a k_b c(aP)c(bQ)$$

$$\text{d'où } k_a = k_b = 1 \text{ et } \begin{cases} a = c(aP) \\ b = c(bQ) \end{cases}$$

Ainsi

$$\begin{cases} P = a\frac{P}{a} \in \mathbb{Z}[X] \\ Q = b\frac{Q}{b} \in \mathbb{Z}[X] \end{cases}$$

Exercice : Irréductibilité dans les rationels

Soit $P \in \mathbb{Z}[X]$ dont les seuls diviseurs dans $\mathbb{Z}[X]$ sont de degré 0 ou $\deg P$, montrer que P est irréductible dans $\mathbb{Q}[X]$.

On suppose par contraposé que P n'est pas irréductible dans $\mathbb{Q}$.

$$P = QR$$
$$1 \leq \deg Q, \deg R \leq \deg P - 1$$

On introduit $a, b \in \mathbb{Z}$ tels que $aQ, bR \in \mathbb{Z}[X]$.

$$\begin{aligned} abc(P) &= c(aQbR) \\ &= c(aQ)c(bR) \end{aligned}$$

$$\begin{aligned} P &= \frac{aQbR}{ab} \\ &= \frac{(aQ)(bR)}{\frac{c(aQ)c(bR)}{c(P)}} \\ &= c(P) \cdot \underbrace{\frac{aQ}{c(aQ)}}_{Q_0} \cdot \underbrace{\frac{bR}{c(bR)}}_{R_0} \in \mathbb{Z}[X] \end{aligned}$$

Avec Q_0 et R_0 diviseurs de P dans $\mathbb{Z}[X]$ de degrés compris dans $[\![1, \deg P - 1]\!]$.

Entiers algébriques

Définition d'entier algébrique.

Soit $\alpha \in \mathbb{C}$, on dit que α est un entier algébrique s'il existe $Q \in \mathbb{Z}[X]$ unitaire tel que $Q(\alpha) = 0$.

1. α est donc aussi algébrique dans $\mathbb{Q}$, et son polynôme minimal est aussi dans $\mathbb{Z}[X]$.

Entiers algébrique de degré 2

2. $\alpha \in \mathbb{C}$ entier algébrique de degré 2 : on dispose de $\pi_\alpha \in \mathbb{Z}[X]$ unitaire de degré 2 qui annule α. $\mathbb{Z}[\alpha] = \operatorname{im} \theta_\alpha$ est un sous-anneau de $\mathbb{R}$ (et donc de $\mathbb{C}$).
3. $\mathbb{Z}[\alpha] = \{x + \alpha y, (x, y) \in \mathbb{Z}^2\}$ et tout élément s'écrite de manière unique sous cette forme.
4. On peut écrire

   $$\pi_\alpha = (X - \alpha)(X - \beta)$$

   On remarque que $\beta \in \mathbb{Z}[\alpha]$ car $\alpha + \beta = a \in \mathbb{Z}$ d'où $\beta = a - \alpha \in \mathbb{Z}[\alpha]$.

   On définit

   $$\tau : \begin{cases} \mathbb{Z}[\alpha] & \to & \mathbb{Z}[\alpha] \\ x + \alpha y & \mapsto & x + \beta y \end{cases}$$

   On a alors

   $$\forall z, z' \in \mathbb{Z}[\alpha],\ \tau(zz') = \tau(z)\tau(z')$$

5. Et on peut alors définir

   $$N : \begin{cases} \mathbb{Z}[\alpha] & \to & \mathbb{Z} \\ z = x + \alpha y & \mapsto & z\tau(z) \end{cases}$$

   Qui est aussi multiplicatif.
6. $z \in \mathbb{Z}[\alpha]$ est inversible ssi $N(z) = |1|$.

Démonstration

1. Notons P_α ce polynôme, comme $Q(\alpha) = 0$, $P_\alpha \mid Q$ dans $\mathbb{Q}[X]$, d'où

   $$\mathbb{Z}[X] \ni Q = P_\alpha R \in \mathbb{Q}[X]$$

   Et donc $P_\alpha, R \in \mathbb{Z}[X]$ car Q unitaire (cf. exercices sur le contenu).
3. α de degré 2 donc

   $$\pi_\alpha(X) = X^2 + aX + b$$

   - On a déjà $\{x + \alpha y, (x, y) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[\alpha]$.
   - Soit $x = P(\alpha) \in \mathbb{Z}[\alpha]$, $P = Q\pi_\alpha + R$ avec $Q \in \mathbb{K}[X], R \in \mathbb{K}_1[X]$.

     Donc

     $$R = yX + x \in \mathbb{Z}[X]$$
     $$P(\alpha) = \underbrace{Q(\alpha)\pi_{\alpha(\alpha)}}_{0} + y\alpha + x$$

   - Soit $x_1 + \alpha y_1 = x_2 + \alpha y_2$ avec $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

     $$x_1 - x_2 = (y_2 - y_1)\alpha$$

     Par l'absurde, si $y_1 \neq y_2$:

     $$\alpha = \frac{x_1 - x_2}{y_2 - y_1} \in \mathbb{Q}[X]$$

     Qui est absurde car π_α serait de degré 1.
4. Soit $z = x + \alpha y, z' = x' + \alpha y'$

   On a $\alpha^2 = a\alpha - b$ et $\beta^2 = a\beta - b$ donc

$$\begin{aligned}\tau(zz') &= \tau\big(xx' + \alpha(xy' + x'y) + \alpha^2 yy'\big) \\ &= \tau(xx' - byy' + \alpha(xy' + xy' + ayy' \\ &= xx' - byy' + \beta(xy' + x'y + ayy') \\ &= (x + \beta y)(x' + \beta y) \\ &= \tau(z)\tau(z')\end{aligned}$$

5. Soit $z = x + \alpha y \in \mathbb{Z}[\alpha]$

$$\begin{aligned}N(z) = z\tau(z) &= (x + \alpha y)(x + \beta y) \\ &= x^2 + (\alpha + \beta)xy + \alpha\beta y^2 \\ &= x^2 = axy + by^2 \in \mathbb{Z}\end{aligned}$$

6. - Soit $z \in \mathbb{Z}[\alpha]$ inversible, on dispose de $z' \in \mathbb{Z}[\alpha]$ tel que $zz' = 1$.

     $$N(zz') = N(1) = 1 = N(z)N(z')$$

     Donc $|N(z)| = 1$
   - Soit $z \in \mathbb{Z}[\alpha]$ tel que $N(z) = \varepsilon \in \{1, -1\}$

     $$(x + \alpha y)(x + \beta y) = \varepsilon$$
     $$z(\varepsilon x + \varepsilon\beta y) = 1 = \varepsilon^2$$
     $$z^{-1} = \varepsilon(x + \beta y)$$

Exercice : Polynômes à coéfficients entiers

1. Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$, montrer que si P admet une racine rationelle $\frac{p}{q}$ avec $p \wedge q = 1$, alors $q \mid a_d$ et $p \mid a_0$.

1.

$$0 = P\left(\frac{p}{q}\right) = \sum_{k=0}^{d} a_k p^k q^{d-k}$$

$$\underbrace{-\sum_{k=0}^{d-1} a_k p^k q^{d-k}}_{\text{divisible par } q} = a_d p^d$$

$$\underbrace{-\sum_{k=1}^{d} a_k p^k q^{d-k}}_{\text{divisible par } p} = a_0 q^d$$

D'où $\begin{cases} q \mid a_d p^d \\ p \mid a_0 q^d \end{cases}$ or $q \wedge p = 1$ donc par le théorème de Gauss, $\begin{cases} q \mid a_d \\ p \mid a_0 \end{cases}$.

On en déduis que si $P \in \mathbb{Z}[X]$ est unitaire et admet une racine rationelle, alors elle est entière.

Critère d'Eisenstein

Énoncé et démonstration du critère d'Eisenstein.

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$ tel qu'il existe $p \in \mathbb{P}$ et

$$\begin{cases} \forall k \in [\![0, d-1]\!], p \mid a_k \\ p \nmid a_d \\ p^2 \nmid a_0 \end{cases}$$

Alors P n'a pas de diviseurs dans $\mathbb{Z}[X]$ de degré compris dans $[\![1, d-1]\!]$, et est donc irréductible dans $\mathbb{Q}[X]$ (cf. exercices sur le contenu).

Démonstration

On considère le morphisme d'anneau suivant

$$\pi : \begin{cases} \mathbb{Z}[X] & \to & \mathbb{F}_p[X] \\ \sum_{k=0}^{d} a_k X^k & \mapsto & \sum_{k=0}^{d} \overline{a_k} X^k \end{cases}$$

Supposons par l'absurde que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$

$$\overline{0} \neq \overline{a_d} X^d = \pi(P) = \pi(Q)\pi(R)$$

Par unicité de la décomposition en irréductibles dans $\mathbb{F}_p[X]$

$$\pi(Q) = \alpha X^k \quad \pi(R) = \beta X^l$$
$$k + l = d \quad \deg Q \geq k \quad \deg R \geq l$$

Or $\deg Q + \deg R = d$ d'où

$$Q = \sum_{i=0}^{k} b_i X^i \text{ avec } \begin{cases} \overline{b_k} = \alpha \neq 0 \\ \overline{b_0} = 0 \end{cases}$$

$$R = \sum_{i=0}^{l} c_i X^i \text{ avec } \begin{cases} \overline{c_l} = \beta \neq 0 \\ \overline{c_0} = 0 \end{cases}$$

D'où $a_0 = b_0 c_0$ est divisible par p^2, absurde.

Exercice : rationalité d'une racine de haute multiplicité

Soit $P \in \mathbb{Q}[X]$ de degré n et α racine de P de multiplicité $m_\alpha > \frac{n}{2}$, montrer que $\alpha \in \mathbb{Q}$.

Soit $P \in \mathbb{Q}[X]$ de degré n et α racine de P de multiplicité $m_\alpha > \frac{n}{2}$.

$$P = \prod_{k=0}^{N} Q_k^{p_k}$$

Décomposition en irréductibles de P dans $\mathbb{Q}[X]$. Pour tout $i \neq j, P_i \wedge P_j = 1$ dans $\mathbb{Q}[X]$ et donc dans $\mathbb{C}[X]$.

Ainsi α n'est racine que d'un des P_i, notons $P_1(\alpha) = 0$.

C'est une racine simple car P_1 irréductible, d'où

$$p_1 \geq m_\alpha > \frac{n}{2}$$
$$2p_1 > n \geq p_1 \deg(P_1)$$
$$2 > \deg(P_1) = 1$$

Donc $P_1 = \lambda(X - \alpha) \in \mathbb{Q}[X]$ d'où $\alpha \in \mathbb{Q}$.

Algèbres

Définition d'une $\mathbb{K}$-Algèbre avec $\mathbb{K}$ un corps.

Une $\mathbb{K}$-Algèbre est un ensemble A muni de deux lois de composition internes $(+)$, $(\times)$ et d'une loi de composition externe $(\cdot)$ tel que

- $(A, +, \times)$ est un anneau
- $(A, +, \cdot)$ est un $\mathbb{K}$-ev
- $\forall (a, x, y) \in \mathbb{K} \times A^2$

$$a(x \times y) = (ax) \times y = x \times (ay)$$

Exemples

- $\mathbb{K}$ est une $\mathbb{K}$-Algèbre
- $(\mathbb{K}[X], +, \times, \cdot)$ est une $\mathbb{K}$-Algèbre
- Pour E un $\mathbb{K}$-ev, $(\mathcal{L}(E), +, \circ, \cdot)$ est une $\mathbb{K}$-Algèbre.

Exercice : existence d'un élément d'ordre du ppcm de deux autres

1. Soit G un groupe abélien fini, montrer que pour tout $x, y \in G$, il existe un élément $z \in G$ tel que $\mathrm{ord}(z) = \mathrm{ord}(x) \vee \mathrm{ord}(y)$.
2. En déduire que

$$\max_{g \in G} \mathrm{ord}(g) = \bigvee_{g \in G} \mathrm{ord}(g)$$

---

1. Soit G un groupe abélien, $x, y \in G$ qui admettent un ordre.

$$\mathrm{ord}(x) = \prod_{i=1}^{N} p_i^{\alpha_i}$$

$$\mathrm{ord}(y) = \prod_{i=1}^{N} p_i^{\beta_i}$$

Pour tout $k \in [\![1, N]\!]$

$$\mathrm{ord}\left(x^{\prod_{i \neq k} p_i^{\alpha_i}}\right) = p_k^{\alpha_k}$$

$$\mathrm{ord}\left(y^{\prod_{i \neq k} p_i^{\beta_i}}\right) = p_k^{\beta_k}$$

On pose alors

$$z_k = \begin{cases} x^{\prod_{i \neq k} p_i^{\alpha_i}} \text{ si } \alpha_k \geq \beta_k \\ y^{\prod_{i \neq k} p_i^{\beta_i}} \text{ sinon} \end{cases}$$

D'où $\mathrm{ord}(z_k) = p_k^{\max(\alpha_k, \beta_k)}$

Ainsi en posant $z = \prod_{k=1}^{N} z_k$:

$$\begin{aligned} \mathrm{ord}(z) &= \prod_{k=1}^{N} p_k^{\max(\alpha_k, \beta_k)} \\ &= \mathrm{ord}(x) \vee \mathrm{ord}(y) \end{aligned}$$

(Car G est abélien).

2. Par récurrence (car G fini) on dispose de $h \in G$ tel que

$$\mathrm{ord}(h) = \bigvee_{g \in G} \mathrm{ord}(g) = m$$

Posons $g_0 \in G$ d'ordre $\max_{g \in G} \mathrm{ord}(g)$.

On a donc

$$\begin{aligned} m \leq \mathrm{ord}(g_0) \mid m \\ m = \mathrm{ord}(g_0) \end{aligned}$$

Exercice : Cyclicité des sous-groupes finis des inversibles d'un corps

Soit $\mathbb{K}$ un corps, et $G \leq \mathbb{K}^\times$ fini. Montrer que G est cyclique.

Première méthode

On utilise la propriété suivante (à redémontrer) : si G abélien fini

$$\max_{g \in G} \operatorname{ord}(g) = \bigvee_{g \in G} \operatorname{ord}(g)$$

Or pour tout $g \in G, g^m = 1$ d'où

$$G \subset \{\text{racines de } X^m - 1 \text{ dans } \mathbb{K}[X]\}$$

D'où $|G| \leq m$ car $\mathbb{K}$ est un corps et ainsi l'élément d'ordre maximale est d'ordre supérieure ou égal au cardinal de G, d'où G cyclique.

Deuxième méthode

Pour $d \mid n = |G|$ on pose

$$\Gamma_d = \{g \in G \mid \operatorname{ord}(g) = d\}$$

$$G = \biguplus_{d \mid n} \Gamma_d$$

$$n = \sum_{d \mid n} |\Gamma_d|$$

On pose aussi

$$\begin{aligned} A_d &= \{g \in G \mid g^d = 1\} \\ &= \{\text{racines de } X^d - 1\} \cap G \\ |A_d| &\leq d \end{aligned}$$

Pour $d \mid n$ on a

- $\Gamma_d = \varnothing$ et $|\Gamma_d| = 0$
- Ou il existe $x \in \Gamma_d$, d'où $\langle x \rangle \subset A_d$ et $d \leq |A_d| \leq d$.

  Ainsi

$$\begin{aligned} \Gamma_d &= \{g \in A_d = \langle x \rangle \mid \operatorname{ord}(g) = d\} \\ |\Gamma_d| &= \varphi(d) \end{aligned}$$

Finalement

$$\sum_{d \mid n} \varphi(d) = n = \sum_{d \mid n} \underbrace{|\Gamma_d|}_{\in \{0, \varphi(d)\}}$$

D'où nécéssairement $|\Gamma_d| = \varphi(d)$ pour tout $d \mid n$, en particulier pour $|\Gamma_n| = \varphi(n) > 0$: il existe $\varphi(n)$ éléments d'ordre n.

Exercice : Les carrés de Fp

Notons $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \{x^2, x \in \mathbb{F}_p^*\}$.

1. Montrer que $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$ et $\left|\mathbb{F}_p^{*2}\right| = \frac{p-1}{2}$.
2. Montrer que pour $x \in \mathbb{F}_p^*$, $x \in \mathbb{F}_p^{*2}$ ssi $x^{\frac{p-1}{2}} = \overline{1}$.
3. En déduire que pour $p \geq 3$, -1 est un carré ssi $p \equiv 1[4]$.
4. On suppose $p \equiv 3[4]$, pour $x \in \mathbb{F}_p^*$ montrer que x est un carré ssi $-x$ n'en est pas un.
5. Soit $p \in \mathbb{P} \mid p \equiv -1[4]$, pour tout $r \in \mathbb{F}_p^*$ montrer que $\Gamma_r = \left\{(x, y) \in \left(\mathbb{F}_p^*\right)^2 \mid x^2 - y^2 = r\right\}$ est de cardinal $p - 3$.

---

1. On étudie le morphisme de groupe

$$\theta : \begin{cases} \mathbb{F}_p^* & \to & \mathbb{F}_p^{*2} \\ x & \mapsto & x^2 \end{cases}$$

$$\begin{aligned} \ker\theta &= \{x \in \mathbb{F}_p^*, x^2 = 1\} \\ &= \{x \in \mathbb{F}_p^*, (x-1)(x+1) = 0\} \\ &= \{-1, 1\} \end{aligned}$$

$$\underbrace{|\ker\theta|}_{2} \cdot \underbrace{(\operatorname{im}\theta)}_{|\mathbb{F}_p^{*2}|} = p - 1$$

D'où $\left|\mathbb{F}_p^{*2}\right| = \frac{p-1}{2}$.

Et $\mathbb{F}_p = \mathbb{F}_p^* \cup \{0\}$ d'où

$$\left|\mathbb{F}_p^2\right| = \left|\mathbb{F}_p^{*2}\right| + 1 = \frac{p+1}{2}$$

2. Soit $x \in \mathbb{F}_p^{*2}$, on écrit $x = y^2$ avec $y \in \mathbb{F}_p^*$.

$$x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$$

D'où

$$\underbrace{\mathbb{F}_p^{*2}}_{\frac{p-1}{2}} \subset \underbrace{\left\{\text{racines de } X^{\frac{p-1}{2}} - 1\right\}}_{\leq \frac{p-1}{2}}$$

D'où l'égalité des ensembles.

3.
$$\begin{aligned} \overline{-1} \in \mathbb{F}_p^{*2} &\Leftrightarrow (-1)^{\frac{p-1}{2}} = \overline{1} \\ &\Leftrightarrow \frac{p-1}{2} \in 2\mathbb{Z} \\ &\Leftrightarrow p \equiv 1[4] \end{aligned}$$

4. On suppose $p \equiv 3[4]$

$$(-1) \notin \mathbb{F}_p^{*2} \quad \text{car } (-1)^{\frac{p-1}{2}} = -1$$

$$\begin{aligned} x \in \mathbb{F}_p^{*2} &\Leftrightarrow x^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow (-x)^{\frac{p-1}{2}} = -1 \\ &\Leftrightarrow -x \notin \mathbb{F}_p^{*2} \end{aligned}$$

5. • Si r est un carré, $r = a^2$ avec $a \in \mathbb{F}_p^*$

$$\begin{aligned} (x, y) \in \Gamma_r &\Leftrightarrow x^2 - y^2 = a^2 \\ &\Leftrightarrow \left(xa^{-1}\right)^2 - \left(ya^{-1}\right)^2 = 1 \\ &\Leftrightarrow \left(xa^{-1}, ya^{-1}\right) \in \Gamma_1 \end{aligned}$$

D'où $|\Gamma_r| = |\Gamma_1|$

• Si r n'est pas un carré, $-r$ en est un.

$$(x, y) \in \Gamma_r \Leftrightarrow y^2 - x^2 = -r$$

Et on se ramène au cas précédent.

$$|\Gamma_r| = |\Gamma_1|$$

Dénombrons Γ_1.

$$\begin{aligned} (x, y) \in \Gamma_1 &\Leftrightarrow x^2 - y^2 = 1 \\ &\Leftrightarrow (x - y)(x + y) = 1 \end{aligned}$$

Posons $a = x + y$, $b = x - y$ (p impair d'où $2 \in \mathbb{F}_p^*$)

$$x = a + \frac{b}{2}$$
$$y = a - \frac{b}{2}$$

$$(x, y) \in \Gamma_1 \Leftrightarrow b = a^{-1}$$

On a $(p - 1)$ choix pour a, et b déterminé par a, d'où au plus $(p - 1)$ couples.

Il faut exclure les cas où notre choix de a permet $x, y \notin \mathbb{F}_p^*$:

$$\begin{aligned} x = \overline{0} &\Leftrightarrow a = -a^{-1} \\ &\Leftrightarrow a^2 = -1 \\ y = \overline{0} &\Leftrightarrow a = a^{-1} \\ &\Leftrightarrow a^2 = 1 \end{aligned}$$

Ainsi $|\Gamma_r| = |\Gamma_1| = p - 3$.

Sous algèbres

Définition, propriétés des sous-algèbres.

Soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre, $B \subset A$ est une sous-algèbre de A si c'est un sous-anneau et un sev de A.

De plus si B est de dimension finie

$$B^\times = B \cap A^\times$$

Démonstration

On a évidement $B^\times \subset B \cap A^\times$.

On suppose $b \in B \cap A^\times$, on dispose de $a \in A$, $ab = ba = 1$.

On pose

$$\varphi_b = \begin{cases} B & \to & B \\ x & \mapsto & bx \end{cases} \in \mathcal{L}(B)$$

Soit $x \in \ker \varphi_b$, on a $bx = 0$ donc $(ab)x = x = 0$.

Donc φ_b bijectif (argument dimensionnel), et $\varphi_b^{-1}(1) = a$ existe et $a \in B$.

Algèbres commutatives intègres de dimension finie

Que peut-on dire d'une algèbre $(A, +, \times, \cdot)$ commutative et intègre de dimension finie ?

Si $(A, +, \times, \cdot)$ est commutative, intègre et de dimension finie, alors c'est un corps.

Démonstration

Soit $a \in A \setminus \{0\}$, étudions

$$\varphi_a : \begin{cases} A & \to & A \\ x & \mapsto & ax \end{cases} \in \mathcal{L}(A)$$

$$\begin{aligned} \ker \varphi_a &= \{x \in A \mid ax = 0\} \\ &= \{x \in A \mid x = 0\} \quad \text{(par integrité)} \\ &= \{0\} \end{aligned}$$

Et par argument dimensionnel, φ_a bijectif, d'où $\varphi_a^{-1}(a) = a^{-1}$ existe.

Morphisme d'algèbre

Définition, propriétés des morphismes d'algèbres.

Pour A, B deux $\mathbb{K}$-algèbre, une application $\varphi : A \to B$ est un morphisme d'algèbre si c'est un morphisme d'anneau linéaire.

Et dans ce cas $\operatorname{im} \varphi$ est une sous-algèbre de B et $\ker \varphi$ est un idéal et un sev de A.

Dévissage de groupes

Propriétés, outils du dévissage de groupes.

---

1. Soient G et H deux groupes cycliques de cardinaux n et p, $G \times H$ est cyclique ssi $n \wedge p = 1$.
2.

Démonstration

1. • Par contraposé, supposons que $n \wedge p = d > 1$, ainsi $m = n \vee p < np$.

   Pour tout $(x, y) \in G \times H$,

   $$(x, y)^m = (x^m, y^m) = (e_G, e_H)$$

   donc $\mathrm{ord}((x, y)) \mid m < |G \times H|$ qui ne peut être cyclique.

   • Soit $x \in G$ d'ordre n et $y \in H$ d'ordre p. Pour $k \in \mathbb{N}^*$

   $$\begin{aligned}(x, y)^k &\iff \left(x^k, y^k\right) = (e_G, e_H)\\ &\iff \begin{cases} n \mid k \\ p \mid k \end{cases} \iff np \mid k\\ &\iff G \times H \text{ cyclique}\end{aligned}$$

   • Autre méthode :

   $$\begin{aligned}G &\simeq \mathbb{Z}/n\mathbb{Z}\\ H &\simeq \mathbb{Z}/p\mathbb{Z}\end{aligned}$$

   $$\begin{aligned}G \times H &\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\\ &\simeq \mathbb{Z}/(np)\mathbb{Z} \quad \text{cyclique}\end{aligned}$$

2. Soient H, K sous-groupes de G et φ (qui n'est pas forcément un morphisme) tel que

   $$\varphi : \begin{cases} H \times K & \to & G \\ (h, k) & \mapsto & hk \end{cases}$$

   On note $HK = \varphi(H \times K)$. Soient $(h, k), (h_0, k_0) \in H \times K$

   $$\begin{aligned}&\varphi(h, k) = \varphi(h_0, k_0)\\ \iff &hk = h_0k_0\\ \iff &h_0^{-1}h = k_0k^{-1} = t \in H \cap K\\ \iff &\exists t \in H \cap K, \begin{cases} h = k_0t \\ k = t^{-1}h_0 \end{cases}\end{aligned}$$

   φ est injectif ssi $H \cap K = \{e_G\}$, c'est automatique si $|H| \wedge |K| = 1$ (en étudiant les ordres et les divisibilités de ceux-ci).

   Dans ce cas $|HK| = |\mathrm{im}\,\varphi| = |H| \cdot |K|$

   Dans le cas général

   $$\left|\varphi^{-1}\{\varphi(h_0, k_0)\}\right| = |H \cap K|$$

Groupe Diédral

Construction et propriétés du groupe diédral.

Construction

Soient $n \geq 2$ et $A_0, \ldots, A_{n-1}$ des points de $\mathbb{R}^2$ d'afixes

$$\forall i \in [\![0, n-1]\!], A_i : e^{\frac{2ik\pi}{n}}$$

On considère Γ l'ensemble des isométries qui préservent le polygone $A_0, \ldots, A_{n-1}$.

Comme une transformation affine préserve les barycentres, tout élément de Γ préserve l'isobarycentre (l'origine).

On a alors

$$\Gamma \in O(\mathbb{R}^2)$$

Et donc tout $\gamma \in \Gamma$, est soit une rotation ou une réflexion.

- Si γ est une rotation : $\gamma(A_0) \in \{A_0, \ldots, A_{n-1}\}$ d'où $\gamma = \text{rot}\left(\frac{2k\pi}{n}\right)$ pour un $k \in [\![0, n-1]\!]$.

  On note r la rotation d'angle $\frac{2\pi}{n}$

  $$\gamma = r^k$$

- Si γ est une réflexion

  Soit s la réflexion à l'axe des abscices, $s \in \Gamma$.

  $s \circ \gamma \in \Gamma$ est une rotation car

  $$\det(s \circ \gamma) = (-1)^2 = 1$$

  Ainsi $\exists k \in [\![0, n-1]\!]$ tel que

  $$s \circ \gamma = r^k \iff \gamma = s \circ r^k$$

Donc

$$\Gamma = \bigcup_{k=0}^{n-1} \{r^k, sr^k\}$$

Groupe

Γ est un sous-groupe de $O(\mathbb{R}^2)$.

- $|\Gamma| = 2n$
- $\Gamma = \langle s, r \rangle$

Algèbre engendrée

Pour $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre et $a \in A$, définition et propriétés de $\mathbb{K}[a]$.

Soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre et $a \in A$. Si on pose le morphisme d'algèbre

$$\theta_a : \begin{cases} \mathbb{K}[X] & \to & A \\ P = \sum_{k=0}^{d} a_k X^k & \mapsto & \sum_{k=0}^{d} a_k a^k \end{cases}$$

On note $\mathbb{K}[a] = \operatorname{im} \theta_a$ qui est la plus petite sous-algèbre de A contenant a.

De plus $\ker \theta_a$ est un idéal de $\mathbb{K}[X]$.

- Si θ_a est injectif et $\mathbb{K}[a] \simeq \mathbb{K}[X]$ qui est donc de dimension infinie.
- Sinon on dispose d'un unique polynôme π_a unitaire tel que $\ker \theta_a = \pi_a \mathbb{K}[X]$ (par principalité).

  π_a est appelé polynôme minimal de a, $\mathbb{K}[a]$ est de dimension $d = \deg \pi_a$ et $(1, a, ..., a^{d-1})$ en est une base.

Démonstration

- Soit $B \in \mathbb{K}[X] \setminus \{0\}$ et $d = \deg B$, par l'éxistence et l'unicité de la division euclidienne on a

$$\mathbb{K}[X] = B\mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

- Soit $u \in \mathcal{L}(E, F)$ et G un supplémentaire de $\ker u$, montrons que $u|_G$ est un isomorphisme de $G \to \operatorname{im} u$.

  $\ker u|_G = \ker u \cap G = \{0\}$ par supplémentarité.

  Soit $y \in \operatorname{im} u$, $y = u(x)$, $x = a + b$ avec $(a, b) \in \ker u \times G$.

$$u(x) = \underbrace{(a)}_{0} + u(b)$$

$$y = u|_G(b)$$

  Soit $y \in \operatorname{im} u|_G$, $y = u|_G(x) = u(x)$.

  D'où $\operatorname{im} u = \operatorname{im} u|_G$.

- Si θ_a est injectif, c'est un isomorphisme de $\mathbb{K}[X]$ sur $\operatorname{im} \theta_a = \mathbb{K}[a]$.
- Sinon on a π_a de degré d et

$$\mathbb{K}[X] = \pi_a \mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

  $\mathbb{K}_{d-1}$ est un supplémentaire de $\ker \theta_a$, ainsi $\theta_a|_{\mathbb{K}_{d-1}[X]}$ est un isomorphisme de $\mathbb{K}_{d-1}[X] \to \mathbb{K}[a]$, d'où

$$\dim \mathbb{K}[a] = d$$

  Et l'image de la base cannonique de $\mathbb{K}_{d-1}[X]$ par $\theta|_{\mathbb{K}_{d-1}[X]}$ est

$$(1, a, ..., a^{d-1})$$

  Qui est donc une base de $\mathbb{K}[a]$.

Condition d'intégrité d'une sous-algèbre engendrée

Pour A une $\mathbb{K}$-algèbre et $a \in A$ tel que θ_a n'est pas injectif, sous quelle condition $\mathbb{K}[a]$ est elle intègre ?

Soit A une $\mathbb{K}$-algèbre et $a \in A$ tel que θ_a n'est pas injectif.

$\mathbb{K}[a]$ est intègre ssi π_a est irréductible.

Démonstration

- Si π_a irréductible, soit $x = P(a)$, $y = Q(a) \in \mathbb{K}[a]$ tels que $xy = 0$.

$$PQ(a) = 0$$
$$\pi_a \mid PQ$$

Donc par le lemme d'Euclide,

$$\text{ou} \quad \begin{matrix} \pi_a \mid P \iff x = 0 \\ \pi_a \mid Q \iff y = 0 \end{matrix}$$

- Par contraposé, si π_a non irréductible, $\pi_a = PQ$ avec $P, Q \in \mathbb{K}[X]$ non inversible ou associé à π_a.

$$\underbrace{P(a)}_{\neq 0}\underbrace{Q(a)}_{\neq 0} = \pi_a(a) = 0$$

D'où $\mathbb{K}[a]$ non intègre.

inversibilité des éléments d'une sous-algèbre engendrée

Soit $\mathbb{K}[a]$ une sous-algèbre de A de dimension finie pour $a \in A$, sous quelle condition $x \in \mathbb{K}[a]$ est il inversible ?

Soit $\mathbb{K}[a]$ une sous-algèbre de A de dimension finie pour $a \in A$. Soit $x = P(a) \in \mathbb{K}[a]$.

$$x \in \mathbb{K}[a]^\times \text{ ssi } P \wedge \pi_a = 1$$

On en déduit que $\mathbb{K}[a]$ est un corps ssi π_a est irréductible.

Démonstration

Par propriété de sous-algèbre

$$\mathbb{K}[a]^\times = A^\times \cap \mathbb{K}[a]$$

Ainsi

$$\begin{aligned} x \in \mathbb{K}[a]^\times &\iff \exists y \in \mathbb{K}[a], xy = 1 \\ &\iff \exists Q \in \mathbb{K}[X], PQ(a) = 1 \\ &\iff \exists Q \in \mathbb{K}[X], \pi_a \mid (PQ - 1) \\ &\iff \exists Q, V \in \mathbb{K}[X], PQ - 1 = \pi_a V \\ &\iff \exists Q, V \in \mathbb{K}[X], PQ - \pi_a V = 1 \\ &\iff P \wedge \pi_a = 1 \end{aligned}$$

Ainsi si π_a irréductible, pour tout $x = P(a) \in \mathbb{K}[a] \setminus \{0\}$, $P \wedge \pi_a = 1$ d'où x inversible et $\mathbb{K}[a]$ est un corps.

Et si $\mathbb{K}[a]$ est un corps, alors il est intègre et π_a irréductible.

Algèbres et extensions de corps

Propriétés des algèbres en lien avec les extensions de corps.

Soient $\mathbb{K} \subseteq \mathbb{L}$ deux corps. On remarque que $\mathbb{L}$ est une $\mathbb{K}$-algèbre.

1. Soit $a \in \mathbb{L}$ qui admet un polynôme annulateur dans $\mathbb{K}[X]$ et π_a son polynôme minimal.

   π_a est irréductible dans $\mathbb{K}[X]$ et $\mathbb{K}[a]$ est un corps.

Démonstration

1. $P, Q \in \mathbb{K}[X]$ tels que $\pi_a = PQ$.

   Dans $\mathbb{L}$

   $$P(a)Q(a) = \pi_a(a) = 0$$

   Donc $P(a) = 0 \iff \pi_a \mid P$ ou $Q(a) = 0 \iff \pi_a \mid Q$ donc π_a irréductible.

   Ainsi $\mathbb{K}[a]$ est un corps.

Nombres algébriques

Définitions et propriétés des nombres algébriques sur un corps $\mathbb{K}$.

Soit $a \in A$ une $\mathbb{K}$-algèbre, on dit que a est algébrique sur $\mathbb{K}$ s'il admet un polynôme annulateur dans $\mathbb{K}[X]$.

Par défaut a algébrique veut dire algébrique sur $\mathbb{Q}$., quitte à les échangers prenons $P(a) = 0, P \in \ker \theta_a = \pi_a \mathbb{K}[X]$.

Propriété

1. Soit $a \in \mathbb{L}$ une extension de corps de $\mathbb{K}$, a algébrique sur $\mathbb{K}$.

   Pour tout $P \in \mathbb{K}[X]$ unitaire, $P = \pi_a$ ssi $P(a) = 0$ et P irréductible sur $\mathbb{K}[X]$.

Démonstration

1. Sens directe connus. Soit $P \in \mathbb{K}[X]$ unitaire, irréductible et annulateur de a.

   On a $\pi_a \mid P$, or P irréductible donc P et π_a sont associé, or tout deux unitaires donc $P = \pi_a$.

Théorème de la base téléscopique

Énoncer et démonstration du théorème de la base téléscopique.

Soit $\mathbb{K} \subseteq \mathbb{L}$ deux corps tel que $\mathbb{L}$ est de dimension finie sur $\mathbb{K}$.

Soient
- E un $\mathbb{L}$-ev, (et donc un $\mathbb{K}$-ev).
- $e = (e_1, ..., e_n)$ base de E sur $\mathbb{L}$.
- $z = (z_1, ..., z_p)$ base de $\mathbb{L}$ sur $\mathbb{K}$.

Alors $F = \left(z_i e_j\right)_{\substack{i \in [\![1,p]\!] \\ j \in [\![1,n]\!]}}$ est une base de E sur $\mathbb{K}$

Ainsi $\dim_{\mathbb{K}} E = \dim_{\mathbb{L}} E \cdot \dim_{\mathbb{K}} \mathbb{L}$.

Démonstration

- Soit $\omega \in E$, on dispose de $\lambda_1, ..., \lambda_n \in \mathbb{L}$ tels que

  $$\omega = \sum_{j=1}^{n} \lambda_j e_j$$

  On dispose de $\left(a_{ij}\right)_{ij} \in \mathbb{K}^{[\![1,p]\!]^{[\![1,n]\!]}}$

  $$\forall j \in [\![1, n]\!], \lambda_j = \sum_{i=1}^{p} a_{ij} z_i$$

  Ainsi

  $$\omega = \sum_{j=1}^{n} \sum_{i=1}^{p} a_{ij} z_i e_j$$

- Soit $\left(a_{ij}\right)_{ij} \in \mathbb{K}^{[\![1,p]\!]^{[\![1,n]\!]}}$ tel que

  $$\sum_{j=1}^{n} \underbrace{\sum_{i=1}^{p} a_{ij} z_i}_{\lambda_j \in \mathbb{L}} e_j = 0$$

  $$\sum_{j=1}^{n} \lambda_j e_j = 0$$

  Donc pour tout $j \in [\![1, n]\!], \lambda_j = 0$.

  $$\lambda_j = \sum_{i=1}^{p} a_{ij} z_i = 0$$

  Donc par liberté de z, $a_{ij} = 0$ pour tout i, j.

Clôture algébrique des rationnels

Propriétés de la clôture algébrique de $\mathbb{Q}$.

Notons $\mathbb{K}$ l'ensemble des $a \in \mathbb{C}$ algébriques sur $\mathbb{Q}$.

$\mathbb{K}$ est un corps algébriquement clos.

Démonstration : corps

- Soit $a, \beta \in \mathbb{K}$, montrons que $a\beta, a+\beta \in \mathbb{K}$.

  On utilise le fait que z algébrique dans $\mathbb{L}$ ssi $\mathbb{L}[z]$ de dimension finie sur $\mathbb{L}$ (car z admet un polynôme annulateur dans $\mathbb{L}[X]$).

  - Donc $\mathbb{Q}[a]$ est de dimension finie sur $\mathbb{Q}$,
  - β algébrique sur $\mathbb{Q} \subset \mathbb{Q}[a]$ donc algébrique sur $\mathbb{Q}[a]$.
  - Donc $\mathbb{Q}[a][\beta]$ est de dimension finie sur $\mathbb{Q}[a]$, et donc par le théorème de la base téléscopique, sur $\mathbb{Q}$.
  - Or $\mathbb{Q}[a+\beta], \mathbb{Q}[a\beta] \subseteq \mathbb{Q}[a][\beta]$, donc $\mathbb{Q}[a+\beta]$ et $\mathbb{Q}[a\beta]$ sont de dimension finie sur $\mathbb{Q}$.
- Soit $a \in \mathbb{K} \setminus \{0\}$, soit π_a son polynôme minimal et $d = \deg \pi_a$.

  $$\underbrace{X^d \pi_a\left(\frac{1}{X}\right)}_{\in \mathbb{Q}[X]} \text{ annule } \frac{1}{a}$$

  Donc $\frac{1}{a} \in \mathbb{K}$
- $1 \in \mathbb{K}$ car $\mathbb{Q} \subseteq \mathbb{K}$.

Démonstration : clôture

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$. Soit $a \in \mathbb{C}$ racine de $\mathbb{K}$, montrons que $a \in \mathbb{K}$.

Pour tout $k \in [\![0, d]\!]$, $a_k \in \mathbb{K}$ donc $\mathbb{Q}[a_k]$ de dimension finie sur $\mathbb{Q}$.

Par récurrence on a

$$\mathbb{L} = \mathbb{Q}[a_0][a_1]\cdots[a_d]$$

De dimension finie sur $\mathbb{Q}$.

Comme $P \in \mathbb{L}[X]$ annule a, $\mathbb{L}[a]$ est de dimension finie sur $\mathbb{L}$ et donc sur $\mathbb{Q}$, id est $a \in \mathbb{K}$.

Exercice : Gauss-Lucas

Soit $P \in \mathbb{C}[X]$, montrer que les racines de P' sont dans l'enveloppe convexe des racines de P.

Soit $P \in \mathbb{C}[X]$, montrer que les racines de P' sont dans l'enveloppe convexe des racines de P.

On écris

$$P = c\prod_{k=1}^{N}(X - a_k)^{m_k}$$

Soit b une racine de P'.

Si $b \in \{a_1, ..., a_N\}$, b est nécéssairement dans leur enveloppe convexe.

Sinon

$$\frac{P'}{P} = \sum_{k=1}^{n}\frac{m_k}{X - a_k}$$

$$0 = \frac{P'}{P}(b) = \sum_{k=1}^{N}\frac{m_k}{b - a_k} = \sum_{k=1}^{N}\frac{m_k}{\overline{b - a_k}}$$

$$= \sum_{k=1}^{N}\frac{m_k}{|b - a_k|^2}(b - a_k)$$

$$b = \frac{\sum_{k=1}^{N}\frac{a_k m_k}{|b-a_k|^2}}{\sum_{k=1}^{N}\frac{m_k}{|b-a_k|^2}}$$

$$= \sum_{k=1}^{N}\lambda_k a_k$$

Où $\lambda_k = \frac{\frac{a_k m_k}{|b-a_k|^2}}{\sum_{i=1}^{N}\frac{m_i}{|b-a_i|^2}}$ (on a alors $\sum_{k=1}^{N}\lambda_k = 1$).

b est donc un barycentre à coéfficients positifs des $a_1, ..., a_n$ et est donc dans leur enveloppe convexe.

Exercice : Dénombrement de morphismes

1. Dénombrer les morphismes de G_1 vers G_2, avec $|G_1| \wedge |G_2| = 1$.
2. Dénombrer les morphismes de G_1 vers G_2 où G_1 et G_2 sont cyclique.
3. Même chose avec les injections et les surjections.

Remarque générale

Soit $\varphi : G_1 \to G_2$ morphisme de groupe, $x \in G_1$

$$\varphi(x)^{\mathrm{ord}(x)} = e_{G_2}$$
$$\text{donc } \mathrm{ord}(\varphi(x)) \mid |G_2|$$
$$\text{et } \mathrm{ord}(\varphi(x)) \mid |G_1|$$

Ainsi $\mathrm{ord}(\varphi(x)) \mid |G_1| \wedge |G_2|$.

Exercices

1. Soit $\varphi : G_1 \to G_2$ morphisme, $x \in G_1$. Par la remarque ci dessus $\mathrm{ord}(\varphi(x)) \mid p \wedge q = 1$ donc $\varphi(x) = 0$, il n'y a donc que morphisme le morphisme triviale.
2. Notons $G_1 = \langle a \rangle$, posons

$$\theta : \begin{cases} \hom(G_1, G_2) & \to & G_2 \\ \varphi & \mapsto & \varphi(a) \end{cases}$$

Qui est injectif car tout morphisme est uniquement déterminé par son image du générateur a.

Pour tout $\varphi \in \hom(G_1, G_2)$ on a

$$\varphi(a)^{|G_1|} = \varphi\left(a^{|G_1|}\right) = \varphi\left(e_{G_1}\right) = e_{G_2}$$

D'où

$$\mathrm{im}\,\theta \subset \left\{y \in G_2 \mid y^{|G_1|} = e_{G_2}\right\}$$

Soit $y \in \mathrm{im}\,\theta$ posons

$$\varphi : \begin{cases} G_1 & \to & G_2 \\ x = a^k & \mapsto & y^k \end{cases}$$

Qui ne dépend pas du k choisi, soit $x = a^k = a^l$:

$$a^{k-l} = e_{G_1}$$
$$\text{donc } |G_1| \mid k - l$$
$$\text{et } y^{k-l} = e_{G_2}$$
$$\text{d'où } y^k = y^l$$

Donc $\theta(\varphi) = y$.

$$\begin{aligned} &|\hom(G_1, G_2)| \\ &= |\mathrm{im}\,\theta| \\ &= \left|\left\{y \in G_2 \mid y^{|G_1|} = e_{G_2}\right\}\right| \\ &= |\{y \in G_2 \mid \mathrm{ord}(y) \mid |G_1|\}| \\ &= \biguplus_{d \mid |G_1|} \{y \in G_2 \mid \mathrm{ord}(y) = d\} \\ &= \sum_{d \mid |G_1| \wedge |G_2|} \varphi(d) \\ &= |G_1| \wedge |G_2| \end{aligned}$$

3. • Pour les injections on veut $\varphi \in \hom(G_1, G_2)$ tels que $\ker \varphi = \{e_{G_1}\}$.

Pour $k \in [\![1, |G_1| - 1]\!]$,

$$\varphi(a)^k = \varphi\left(a^k\right) \neq 0$$
$$\mathrm{ord}\,\varphi(a) = |G_1|$$

Si $|G_1| \nmid |G_2|$, G_2 ne contient pas éléments d'ordre $|G_1|$ donc auncune injection.

Si $|G_1| \mid |G_2|$, il y a $\varphi(|G_1|)$ éléments d'ordre $|G_1|$, donc autant d'injections.

• Pour les surjections on veut $\mathrm{ord}\,\varphi(a) = |G_2|$, donc

$$\begin{cases} 0 & \text{si } |G_2| \nmid |G_1| \\ \varphi(|G_2|) & \text{sinon} \end{cases}$$

Exercice : Union de sous espaces vectoriels

E un $\mathbb{K}$ espace vectoriel.

1. Soit F, G deux sev de E, montrer que $F \cup G$ sev ssi $F \subseteq G$ ou $G \subseteq F$.
2. Supposons $\mathbb{K}$ infini, soit $F_1, ..., F_n$ n sevs, montrer que si $\bigcup_{k=1}^{n} F_k$ est un sev, alors il existe $i \in [\![1, n]\!]$ tel que

$$\bigcup_{k=1}^{n} F_k = F_i$$

---

1. Soit F, G sevs de E un $\mathbb{K}$-ev tel que $F \cup G$ est un sev.

   Si $F \not\subseteq G$, on pose $z \in F \setminus G$, soit $x \in G$.

   $$x + z \in F \cup G$$

   $x + z \notin G$ car sinon

   $$F \setminus G \ni z = \underbrace{(x+z)}_{\in G} - \underbrace{x}_{\in G} \in G$$

   Donc $x + z \in F$ d'où

   $$x = (x+z) - z \in F$$

   Et $G \subseteq F$.

2. Soient $F_1, ..., F_n$ sevs de E tels que $\bigcup_{k=1}^{n} F_k$ est un sev.

   Notons $U_m = \bigcup_{k=1}^{m} F_k$ pour $m \in \mathbb{N}$.

   On à déjà fait le cas $n = 2$ et le cas $n = 1$ est trivial.

   Supposons la propriété vraie pour un $n \in \mathbb{N}$.

   Si $U_n \subseteq F_{n+1}$ alors on a fini.

   Si $F_{n+1} \subseteq U_n$ alors par hypothèse de récurrence, on dispose de $i \in [\![1, n]\!]$

   $$U_{n+1} = U_n = F_i$$

   Sinon, on dispose de

   $$x \in F_{n+1} \setminus U_n \subseteq U_{n+1}$$
   $$y \in U_n \setminus F_{n+1} \subseteq U_{n+1}$$

   Soient $\lambda_0, ..., \lambda_{n+1} \in \mathbb{K}$ deux à deux distincts.

   $$z_k = x + \lambda_k y$$

   Par le lemme des tiroirs, on dispose de $k \neq l$ et j tel que $z_k, z_l \in F_j$

   Si $j = n + 1$

   $$z_k - z_l = \underbrace{(\lambda_k - \lambda_l)}_{\neq 0} y \in F_{n+1}$$

   Et $y \in F_{n+1}$ impossible.

   Si $j \in [\![1, n]\!]$

   $$\lambda_l z_k - \lambda_k z_l = \underbrace{(\lambda_l - \lambda_k)}_{\neq 0} x \in F_j$$

   Et $x \in F_j$ impossible.

Somme directe de sous espaces vectoriels

Définition et propriétés de somme directe de sev.

Soient $F_1, ..., F_n$ sev de E un $\mathbb{K}$-ev. On dit qu'ils sont en somme directe si pour tout $x \in \sum_{k=1}^{n} F_k$

$$\exists!(x_1, ..., x_n) \in \prod_{k=1}^{n} F_k,\ x = \sum_{k=1}^{n} x_k$$

Il y a équivalence entre $F_1, ..., F_n$ en somme directe et

1. $\forall (x_1, ..., x_n) \in \prod_{k=1}^{n} F_k,\ \sum_{k=1}^{n} x_k = 0 \Rightarrow \forall k \in [\![1, n]\!],\ x_k = 0.$
2. $\forall i \in [\![1, n]\!],\ F_i \cap \left(\sum_{i \neq k}^{n} F_k\right) = \{0\}$
3. $F_n \cap \bigoplus_{k=1}^{n-1} F_k = \{0\}$

En dimension finie

4. $\dim \sum_{k=1}^{n} F_n \leq \sum_{k=1}^{n} \dim F_n$ avec égalité ssi les $F_1, ..., F_n$ sont en somme directe.

Démonstration

1. $\Rightarrow$ il s'agit d'un cas particulier pour $x = 0$.

   $\Leftarrow$ Supposons $\sum_{k=1}^{n} x_k = \sum_{k=1}^{n} x'_k$

   Alors $\sum_{k=1}^{n} (x_k - x'_k) = 0$ donc $x_k = x'_k$ pour tout $k \in [\![1, n]\!]$.

3. $\Rightarrow$ Soit $x \in F_n \cap \bigoplus_{k=1}^{n} F_k$

$$\begin{aligned} x &= \sum_{k=1}^{n-1} 0 + x \\ &= \sum_{k=1}^{n-1} x_k + 0 \quad \text{car } x \in \bigoplus_{k=1}^{n-1} F_k \end{aligned}$$

   Donc par unicité de la décomposition $x = \sum_{k=1}^{n} 0 = 0$.

   $\Leftarrow$ Soit $x_1, ..., x_n \in E$ tels que

$$\sum_{k=1}^{n} x_k = 0$$

$$-x_n = \sum_{k=1}^{n-1} x_k \in F_n \cap \bigoplus_{k=1}^{n-1} F_k$$

   Donc $x_n = 0$ et $\sum_{k=1}^{n-1} x_k = 0$ donc $x_1 = x_2 = \cdots = x_n = 0$.

Espaces supplémentaires

Définition, propriétés des espaces supplémentaires.

Soient $F_1, ..., F_n$ sevs de E un $\mathbb{K}$-ev. On dit qu'ils sont supplémentaires si

$$E = \bigoplus_{k=1}^{n} F_k$$

Et on a

$$E = \bigoplus_{k=1}^{n} F_k$$

$$\Leftrightarrow \begin{cases} E = \sum_{k=1}^{n} F_k \\ \dim(E) = \sum_{k=1}^{n} \dim(F_k) \end{cases}$$

$$\Leftrightarrow \begin{cases} \sum_{k=1}^{n} F_k = \bigoplus_{k=1}^{n} F_k \\ \dim(E) = \sum_{k=1}^{n} \dim(F_k) \end{cases}$$

Notations de matrices

Notations de matrices : changements de bases, matrices d'un endomorphisme, ...

Soit $u \in \mathcal{L}(E,F)$, $e = (e_1, ..., e_n)$, $e' = (e'_1, ..., e'_n)$ bases de E et $f = (f_1, ..., f_p)$ base de F.

Applications linéaires

$$\mathcal{M}_{e,f}(u) = \mathcal{M}_{e\leftarrow f}(u) = \mathcal{M}_e^f(u) \in M_{pn}(\mathbb{K})$$

Et la matrice est alors

$$\mathcal{M}_{f\leftarrow e}(u) = \begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_p \end{array} \begin{array}{c} \begin{array}{cccc} u(e_1) & u(e_2) & \cdots & u(e_n) \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pn} \end{pmatrix} \end{array}$$

Où pour $j \in [\![1, n]\!]$

$$u(e_j) = \sum_{k=1}^{p} a_{kj} f_k$$

Endomorphismes

$$\mathcal{M}_e(u) = \mathcal{M}_{e\leftarrow e}(u) = \mathcal{M}_e^e(u)$$

$$u(e_j) = \sum_{k=1}^{p} a_{kj} f_k$$

Changement de base

$$P_{e\to e'} = \mathcal{M}_e(e') = \mathcal{M}_{e\leftarrow e'}(\mathrm{id})$$

Exercice : Noyaux et images itérées

Soit $u \in \mathcal{L}(E)$ avec E un $\mathbb{K}$-ev. Que peut on dire des suites $\left(\ker u^k\right)_k$ et $\left(\operatorname{im} u^k\right)_k$?

Soit $u \in \mathcal{L}(E)$ avec E un $\mathbb{K}$-ev.

Dimension quelconque

- Si $\ker u^k = \ker u^{k+1}$ pour un $k \in \mathbb{N}$ alors pour tout $n \geq k$, $\ker u^k = \ker u^n$.
- De même pour les images.

Dimension finie

En notant $n = \dim E$ on a

$$d_k = \dim \ker u^k \in [\![0, n]\!] \nearrow$$
$$r_k = \operatorname{rg} u^k \in [\![0, n]\!] \searrow$$

Ces deux suites sont donc stationnaires, on peut poser

$$m_K = \min\{k \in \mathbb{N} \mid \ker u^k = \ker u^{k+1}\}$$
$$m_I = \min\{k \in \mathbb{N} \mid \operatorname{im} u^k = \operatorname{im} u^{k+1}\}$$

On a de plus $m_K = m_I = m$.

Et en notant

$$K = \bigcup_{k \in \mathbb{N}} \ker u^k = \ker u^m$$
$$I = \bigcap_{k \in \mathbb{N}} \operatorname{im} u^k = \operatorname{im} u^m$$

Qui sont les valeurs auquelles les suites stationnent, on a

- $K \oplus I = E$
- K, I stables par u
- $u|_K^K$ est nilpotent
- $u|_I^I$ est inversible.
- Si $E = K' \oplus I'$ avec K', I' stables par u, $u|_{K'}^{K'}$ nilpotent et $u|_{I'}^{I'}$ inversible, alors $K' = K$ et $I' = I$.

Démonstration

- Soit $l \geq k$, on a évidement $\ker u^l \subseteq \ker u^{l+1}$.

  Soit $x \in \ker u^{l+1}$:

  $$u^{k+1}\left(u^{l-k}(x)\right) = 0$$
  $$u^{l-k}(x) \in \ker u^{k+1} = \ker u^k$$
  $$u^k\left(u^{l-k}(x)\right) = 0$$
  $$x \in \ker u^l$$

- Soit $l \geq k$, on a évidement $\operatorname{im} u^{l+1} \subseteq \operatorname{im} u^l$.

  Soit $u^l(x) = y \in \operatorname{im} u^l$:

  $$u^{l-k}\left(u^k(x)\right) = y$$
  $$u^k(x) \in \operatorname{im} u^k = \operatorname{im} u^{k+1}$$
  $$u^k(x) = u^{k+1}(x')$$
  $$u^{l-k}\left(u^{k+1}(x')\right) = y$$
  $$y \in \operatorname{im} u^{l+1}$$

Dimension finie

- Par le théorème de rang on a $d_k = n - r_k$, donc si r_k est constante à partire du rang m_I, alors d_k est aussi constante a partire de ce rang, donc $m_K = m_I$.
- Soit $y \in K \cap I$, on dispose de $x \in E$ tel que

  $$u^m(x) = y$$
  $$u^m(y) = 0$$
  $$u^{2m}(x) = 0$$
  $$x \in \ker u^{2m} = \ker u^m$$
  $$u^m(x) = y = 0$$

  donc $K \oplus I = E$.

- Soit $x \in K = \ker u^m$

  $$u^m(u(x)) = u^{m+1}(x) = 0$$

  donc $u(x) \in K$.

- Soit $y \in I = \operatorname{im} u^m$, on dispose de $x \in E$ tel que

  $$u^m(x) = y$$
  $$u^{m+1}(x) = u(y) \in \operatorname{im} u^m$$
  $$u(y) = u^m(x')$$

  et $u(y) \in I$.

- Notons $\tilde{u} = u|_K^K$ l'endomorphisme induit par u sur K.

  $$\tilde{u}^m(K) = u^m(K) = \{0\}$$

  Donc $\tilde{u}$ est nilpotent d'indice m.

- Notons $\tilde{u} = u\,|_I^I$ l'endomorphisme induit par u sur I.

  $$\tilde{u}(I) = u(\operatorname{im} u^m) = \operatorname{im} u^{m+1}$$
  $$= \operatorname{im} u^m = I$$

  Donc $\tilde{u}$ est inversible.

- Soit $K' \oplus I' = E$ qui respectent les hypothèses.

  On dispose de $d \in \mathbb{N}^*$ tel que

  $$u^d(K') = \{0\}$$
  $$K' \subseteq \ker u^d \subset K = \bigcup_{k \in \mathbb{N}} \ker u^k$$

  Et on a

  $$u(I') = I'$$
  $$u^m(I') = I'$$
  $$I' \subseteq \operatorname{im} u^m = I$$

  Donc

  $$\dim K' \leq \dim K$$
  $$\dim I' \leq \dim I$$

  Et on obtient l'égalité par supplémentarité, d'où $K' = K$ et $I' = I$.

Développement du déterminant par ligne ou par colonne

Formules et définitions du développement du déterminant par ligne ou par colonne.

Soit $A \in M_n(\mathbb{K})$

- pour tout $j \in [\![1, n]\!]$:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

- pour tout $i \in [\![1, n]\!]$:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

Où $\tilde{A}_{ij} \in M_{n-1}(\mathbb{K})$ est la matrice A privée de sa $i^{\text{ème}}$ ligne et $j^{\text{ème}}$ colonne.

On appelle $\hat{A}_{ij} = (-1)^{i+j} \det(\tilde{A}_{ij})$ cofacteur.

On appelle $\text{com}(A)$ la matrice des cofacteurs.

Et on a

$$A \cdot \text{com}(A)^T = \det(A) I_n$$

Exercice : rang d'une comatrice

Soit $A \in M_n(\mathbb{K})$ ($n \geq 3$), calculer $\operatorname{rg} \operatorname{com}(A)$ en fonction de $\operatorname{rg} A$.

Soit $A \in M_n(\mathbb{K})$ avec $n \geq 3$.

- Si $\operatorname{rg} A = n$, $A \in \mathrm{GL}_n(\mathbb{K})$ donc $\operatorname{com} A \in \mathrm{GL}_n(\mathbb{K})$ et $\operatorname{rg} \operatorname{com}(A) = n$.
- Si $\operatorname{rg} A \leq n-2$, pour tout $i, j \in [\![1, n]\!]$ la matrice $\tilde{A}_{ij}$ extraite de A privée de sa $i^{\text{ème}}$ ligne et $j^{\text{ème}}$ colonne est de rang inférieur à $n-2$ et n'est donc pas inversible, $\operatorname{com} A = 0$ et $\operatorname{rg} \operatorname{com}(A) = 0$.
- Si $\operatorname{rg} A = n-1$, on dispose d'une matrice éxtraite de taille $n-1$ inversible, donc au moins un des cofacteur est non nul d'où $\operatorname{rg} \operatorname{com}(A) \geq 1$.

  De plus

  $$A_T \operatorname{com}(A) = \det(A) I_n = 0$$

  Donc $\operatorname{im} \operatorname{com}(A) \subseteq \ker A^T$ et $\dim \ker A^T = 1$ d'où $\operatorname{rg} \operatorname{com}(A) \leq 1$.

Algorithme du pivot de Gauss

Déscription de l'algorithme du pivot de Gauss, et propriétés qui en découlent.

Opérations, représentation matricielle

Notons $(E_{ij})_{ij}$ la base cannonique de $M_n(\mathbb{K})$. On a

$$E_{ik}E_{lj} = \delta_{kl}E_{ij}$$

Pour $A \in M_{np}(\mathbb{K})$

$$E_{kl}^{(n)}A = \begin{pmatrix} & 1 \\ & \vdots \\ L_l & k \\ & \vdots \\ & n \end{pmatrix}$$

$$AE_{kl}^{(p)} = \begin{pmatrix} & C_k & \\ 1 & \cdots & l & \cdots & n \end{pmatrix}$$

Ainsi on peut définir

- $T_{kl}(\lambda) = I_n + \lambda E_{kl}^{(n)}$ la transvection sur les lignes ($L_k \leftarrow L_k + \lambda L_l$)
- $T'_{kl}(\lambda) = I_p + \lambda E_{kl}^{(p)}$ la transvection sur les colonnes ($C_l \leftarrow C_l + \lambda C_k$)
- $P_{kl} = I_n - E_{kk}^{(n)} - E_{ll}^{(n)} + E_{kl}^{(n)} + E_{lk}^{(n)}$ la transposition de lignes ($L_l \leftrightarrow L_k$)
- $P_{kl} = I_p - E_{kk}^{(p)} - E_{ll}^{(p)} + E_{kl}^{(p)} + E_{lk}^{(p)}$ la transposition de colonnes ($C_l \leftrightarrow C_k$)

Algorithme

Prenons $A = (c_1 \ \cdots \ c_n) \in M_n(\mathbb{K})$

- Si $A = 0$ fini.
- Soit $j = \min\{k \in [\![1, n]\!] \mid C_k \neq 0\}$

$$A^{(1)} : \quad C_j \leftrightarrow C_1$$

- Soit $i = \min\{k \in [\![1, n]\!] \mid a_{i1} \neq 0\}$
  - Si $i = 1$ on effectue $L_2 \leftarrow L_2 + L_1$ et on prend $i = 2$.

$$A^{(2)} : \quad L_1 \leftarrow L_1 + \left(1 - \frac{a_{11}}{a_{i1}}\right)L_i$$

$$A^{(2)} = \left(\begin{array}{c|ccc} 1 & * & \cdots & * \\ \hline * & & & \\ \vdots & & * & \\ * & & & \end{array}\right)$$

- Pour tout $i \in [\![2, n]\!]$ on effectue

$$A^{(i+1)} : \quad L_i \leftarrow L_i - a_{i1}L_1$$

Ainsi

$$A^{(n+1)} = \left(\begin{array}{c|ccc} 1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array}\right)$$

On repète l'algorithme sur $\tilde{A}$, on obtient alors

$$\tilde{\tilde{A}} = \left(\begin{array}{ccc|c|ccc} 1 & & (*) & * & & & \\ & \ddots & & \vdots & & (*) & \\ & & 1 & * & & & \\ \hline & & & \mu & * & \cdots & * \\ \hline & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{array}\right)$$

Avec $\mu \neq 1$ ssi le blocs de zéros à la fin est de taille nulles (on ne dispose pas des lignes nécéssaires pour se ramener à $\mu = 1$).

On peut alors finalement effectuer pour tout $i \in [\![1, \operatorname{rg} A]\!]$, puis pour $j \in [\![i+1, n]\!]$

$$\tilde{\tilde{A}} : \quad C_j \leftarrow C_j - \frac{\tilde{\tilde{A}}_{ij}}{\tilde{\tilde{A}}_{ii}}C_i$$

$$\tilde{\tilde{\tilde{A}}} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \mu & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}$$

On remarque que si A est inversible, les transpositions sont inutiles car il n'éxiste pas de colonnes nulles.

Propriétés

- Les transvections engendrent $\mathrm{SL}_n(\mathbb{K})$.
- Les transvections et une dilatation (pour atteindre n'importe quel déterminant) suffisent à engendrer $\mathrm{GL}_n(\mathbb{K})$.

Intersection d'hyperplans

Propriétés sur les intersections d'hyperplans.

Soient $(\varphi_1, ..., \varphi_p) \in \mathcal{L}(E, \mathbb{K})^p$

$$\dim \bigcap_{k=1}^{p} \ker \varphi_k = n - \operatorname{rg}(\varphi_1, ..., \varphi_p)$$
$$\geq n - p$$

Démonstration

On montre l'inégalité par récurrence sur p.

Montrons l'égalité.

Quitte à extraire et renuméroter, $(\varphi_1, ..., \varphi_r)$ est libre.

Or pour tout $k \in [\![r+1, p]\!]$,

$$\varphi_k \in \operatorname{Vect}(\varphi_1, ..., \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^{r} \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^{p} \ker \varphi_k = \bigcap_{k=1}^{r} \ker \varphi_k$$

Donc (cf. lemme sur la liberté d'une famille de formes linéaires)

$$\theta : \begin{cases} E & \to & \mathbb{K}^r \\ x & \mapsto & \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \quad \text{surjective}$$

$$\ker \theta = \bigcap_{k=1}^{r} \ker \varphi_k$$

Donc par le théorème du rang

$$\dim\left(\bigcap_{k=1}^{p} \ker \varphi_k\right) = n - \operatorname{rg}(\varphi_1, ..., \varphi_p)$$

Liberté d'une famille de l'espace dual

Démonstration d'une CNS pour la liberté d'une famille de $\mathcal{L}(E, \mathbb{K})$ où E est un $\mathbb{K}$-ev.

Soient $\varphi_1, ..., \varphi_p \in \mathcal{L}(E, \mathbb{K})$.

La famille $(\varphi_1, ..., \varphi_p)$ est libre ssi

$$\theta : \begin{cases} E & \to & \mathbb{K}^p \\ x & \mapsto & \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \end{cases} \quad \text{surjective}$$

Démonstration

- Supposons θ surjective, on considère $\lambda_1, ..., \lambda_p \in \mathbb{K}$ tels que

$$\sum_{k=1}^{p} \lambda_k \varphi_k = 0$$

Soit $i \in [\![1, p]\!]$, on dispose de $x \in E$ tel que

$$\theta(x) = \left(\begin{array}{c|c} 1 & \begin{matrix} 1 \\ \vdots \\ i \\ \vdots \\ p \end{matrix} \end{array}\right) = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_i(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix}$$

Ainsi

$$\left(\sum_{k=1}^{p} \lambda_k \varphi_k\right)(x) = 0 = \lambda_i$$

- Par contraposé supposons θ non surjective : $\operatorname{rg} \theta \leq p - 1$.

On dispose de H hyperplan tel que $\operatorname{im} \theta \subseteq H$. Donc on dispose de $(a_1, ..., a_p) \in \mathbb{K}^p \setminus \{0\}$ tels que

$$H = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p \;\middle|\; \sum_{k=1}^{p} a_k x_k = 0 \right\}$$

Donc pour tout $x \in E$,

$$\theta(x) = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \in \operatorname{im} \theta \subseteq H$$

$$\sum_{k=1}^{p} a_k \varphi_k(x) = 0$$

Donc $\sum_{k=1}^{p} a_k \varphi_k = 0$ et la famille est liée

Condition de liberté d'une forme linéaire à une famille

Soit $\varphi_1, ..., \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$.

Démonstration d'une CNS pour que $\psi \in \text{Vect}(\varphi_1, ..., \varphi_p)$.

Soit $\varphi_1, ..., \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$.

Pour tout $\psi \in \mathcal{L}(E, \mathbb{K})$

$$\varphi \in \text{Vect}(\varphi_1, ..., \varphi_p)$$

$$\text{ssi } \bigcap_{k=1}^{p} \ker \varphi_k \subseteq \ker \psi$$

Démonstration

- Si $\varphi \in \text{Vect}(\varphi_1, ..., \varphi_p)$, on dispose de $\lambda_1, ..., \lambda_p \in \mathbb{K}$ tels que

$$\psi = \sum_{k=1}^{p} \lambda_k \varphi_k$$

D'où

$$\psi\left(\bigcap_{k=1}^{p} \ker \psi_p\right) = \sum_{k=1}^{p} \lambda_k \varphi_k\left(\bigcap_{i=1}^{p} \ker \varphi_p\right) = \{0\}$$

Et donc $\bigcap_{k=1}^{p} \ker \varphi_p \subseteq \ker \psi$.

- Supposons $\bigcap_{k=1}^{p} \ker \varphi_p \subseteq \ker \psi$.

Quitte à extraire et renuméroter, $(\varphi_1, ..., \varphi_r)$ est libre.

Or pour tout $k \in [\![r+1, p]\!]$,

$$\varphi_k \in \text{Vect}\,(\varphi_1, ..., \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^{r} \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^{p} \ker \varphi_k = \bigcap_{k=1}^{r} \ker \varphi_k$$

Donc

$$\theta : \begin{cases} E \to \mathbb{K}^r \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Posons alors

$$\theta' : \begin{cases} E \to \mathbb{K}^{r+1} \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \\ \psi(x) \end{pmatrix} \end{cases}$$

Or

$$\bigcap_{k=1}^{r} \ker \varphi_k = \bigcap_{k=1}^{p} \ker \varphi_k \subseteq \ker \psi$$

$$\text{Donc } \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \notin \text{im}\,\theta'$$

La famille $(\varphi_1, ..., \varphi_r, \psi)$ est liée d'où $\psi \in \text{Vect}(\varphi_1, ..., \varphi_p)$.

Base duale, antéduale

Définitions, propriétés, démonstrations autours des bases duals.

Base duale

Soit E un $\mathbb{K}$-ev de dimension finie, $e = (e_1, ..., e_n)$ une base de e.

Il existe une unique famille $(\varphi_1, ..., \varphi_n) \in \mathcal{L}(E, \mathbb{K})^n$ tel que

$$\forall i, j \in [\![1, n]\!],\ \varphi_i(e_j) = \delta_{ij}$$

Cette famille est appelée base duale de e et est une base de $\mathcal{L}(E, \mathbb{K})$.

Dans ce cas

$$\forall x \in E,\ x = \sum_{k=1}^{n} \varphi_k(x) e_k$$

$$\forall \psi \in \mathcal{L}(E, \mathbb{K}),\ \psi = \sum_{k=1}^{n} \psi(e_k) \varphi_k$$

Base antéduale

Pour toute base $(\varphi_1, ..., \varphi_n)$ de $\mathcal{L}(E, \mathbb{K})$, il existe une unique base $(e_1, ..., e_n)$ de E tel que $(\varphi_1, ..., \varphi_n)$ en est la base duale.

Démonstration

- Existence / Unicité : car les formes linéaire sont uniquement déterminés par leurs image d'une base.
- Génératrice : Soit $\psi \in \mathcal{L}(E, \mathbb{K})$

  pour tout $i \in [\![1, n]\!]$

  $$\left(\sum_{k=1}^{n} \psi(e_k)\varphi_k\right)(e_i) = \sum_{k=1}^{n} \psi(e_k)\varphi_k(e_i)$$
  $$= \psi(e_k)$$

  $$\text{Donc } \psi = \sum_{k=1}^{n} \psi(e_k)\varphi_k$$

  Donc $(\varphi_1, ..., \varphi_n)$ est une base.
- Soit $x = \sum_{k=1}^{n} x_k e_k \in E, i \in [\![1, n]\!]$

  $$\varphi_i(x) = \varphi_i\left(\sum_{k=1}^{n} x_k e_k\right)$$
  $$= \sum_{k=1}^{n} x_k \delta_{ik} = x_i$$
- Soit $(\varphi_1, ..., \varphi_n)$ base de $\mathcal{L}(E, \mathbb{K})$

  $$\theta : \begin{cases} E \to \mathbb{K}^n \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_n(x) \end{pmatrix} \end{cases} \text{ surjective}$$

  Par liberté de la famille, donc bijective par argument dimensionnel.

  Notons $(b_1, ..., b_n)$ la base cannonique de $\mathbb{K}^n$.

  La famille $\left(e_k = \theta^{-1}(b_k)\right)_{k \in [\![1,n]\!]}$ est l'unique base de E tel que

  $$\forall i, j \in [\![1, n]\!],\ \varphi_i(e_j) = \delta_{ij}$$

Lemme de factorisation

Énoncé et démonstration du lemme de factorisation en algèbre linéaire.

Soient E, F, G trois $\mathbb{K}$-ev

1. Soient $u \in \mathcal{L}(E,F), v \in \mathcal{L}(E,G)$, dans ce cas

$$\ker u \subseteq \ker v$$
$$\iff \exists w \in \mathcal{L}(F,G),\ v = w \circ u$$

(Si u est inversible $w = v \circ u^{-1}$).

2. Soient $u \in \mathcal{L}(E,F), v \in \mathcal{L}(G,F)$, dans ce cas

$$\operatorname{im} v \subseteq \operatorname{im} u$$
$$\iff \exists w \in \mathcal{L}(G,E), v = u \circ w$$

Démonstration

1. • Supposons qu'il existe $w \in \mathcal{L}(F,G)$ tel que $v = w \circ u$.

$$\begin{aligned} v(\ker u) &= w(u(\ker u)) \\ &= w(\{0\}) = 0 \end{aligned}$$

D'où $\ker u \subseteq \ker v$.

• Supposons que $\ker u \subseteq \ker v$.

Soient H, K tels que

$$\ker u \oplus H = E$$
$$\operatorname{im} u \oplus K = F$$

Posons

$$\tilde{u} : \begin{cases} H & \to & \operatorname{im} u \\ x & \mapsto & u(x) \end{cases}$$
$$\ker \tilde{u} = \ker u \cap H = \{0\}$$
$$\dim H = \operatorname{rg} u$$

Donc $\tilde{u}$ inversible.

On peut donc écrire

$$w : \begin{cases} F = \operatorname{im} u \oplus K & \to & G \\ x = y \quad +z & \mapsto & v \circ \tilde{u}^{-1}(y) \end{cases}$$

Soit $x = y + z \in E = \ker u \oplus H$.

$$\begin{aligned} w \circ u(x) &= v\left(\tilde{u}^{-1}(u(z))\right) \\ &= v(z) \\ v(x) &= \underbrace{v(y)}_{0} + v(z) \end{aligned}$$

2. • Supposons qu'il existe $w \in \mathcal{L}(G,E)$ tel que $v = u \circ w$

$$v(E) = u \circ w(E) \subseteq u(E)$$

D'où $\operatorname{im} v \subseteq \operatorname{im} u$.

• Supposons que $\operatorname{im} v \subseteq \operatorname{im} u$.

Soit H tel que $\ker u \oplus H = E$.

$$\tilde{u} : \begin{cases} H & \to & \operatorname{im} u \\ x & \mapsto & u(x) \end{cases}$$
$$w : \begin{cases} G & \to & E \\ x & \mapsto & \tilde{u}^{-1} \circ v(x) \end{cases}$$

On a bien pour $x \in E$

$$u \circ w(x) = \tilde{u}\left(\tilde{u}^{-1}(v(x))\right) = v(x)$$

Vandermonde, interpolation de Lagrange

Définitions, propriétés et démonstrations de l'interpolation de Lagrange et des matrices des Vandermonde.

Soit $\mathbb{K}$ un corps, $n \in \mathbb{N}$, $a_0, ..., a_n \in \mathbb{K}$ deux à deux distincts.

$$\theta : \begin{cases} \mathbb{K}_n[X] & \to & \mathbb{K}^{n+1} \\ P & \mapsto & \begin{pmatrix} P(a_0) \\ \vdots \\ P(a_n) \end{pmatrix} \end{cases} \in \mathcal{L}\left(\mathbb{K}_n[X], \mathbb{K}^{n+1}\right)$$

Pour tout $P \in \ker \theta$,

$$P(a_0) = P(a_1) = \cdots = P(a_n) = 0$$

Donc P est de degré n avec $n+1$ racines distinctes, d'où $P = 0$.

Donc θ est un isomorphisme.

Notons

$$e = (e_0, ..., e_n)$$
$$c = (1, X, ..., X^n)$$

Les bases cannoniques de $\mathbb{K}^{n+1}$ et $\mathbb{K}_n[X]$.

$$\forall k \in [\![0, n]\!],\ \theta^{-1}(e_k) = \prod_{\substack{i=0 \\ i \neq k}}^{n} \frac{X - a_i}{a_k - a_i} = L_k(X)$$

La matrice de θ dans les bases cannoniques est appelée matrice de Vandermonde de $a_0, ..., a_n$.

$$\mathcal{M}_{e \leftarrow c}(\theta) = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^n \end{pmatrix}$$

Sont déterminant vaut

$$V(a_0, ..., a_n) = \det\left(\mathcal{M}_{e \leftarrow c}(\theta)\right) = \prod_{0 \leq i < j \leq n} \left(a_j - a_i\right)$$

Démonstration

Par récurrence sur n, initialisée aisément pour $n = 1$.

On suppose la formule pour un $n \in \mathbb{N}$.

$$P(X) = V(a_0, ..., a_n, X) = \begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n+1} \\ 1 & X & X^2 & \cdots & X^{n+1} \end{vmatrix} = \sum_{j=0}^{n+1} (-1)^{n+j} X^j V_j$$

Où V_j est le déterminant mineur en $(n+2, j+1)$. De plus

$$\deg P \leq n + 1$$
$$\text{cd } P = V(a_0, ..., a_n) \neq 0$$

De plus pour tout $k \in [\![0, n]\!]$, $P(a_k) = 0$ donc

$$P = V(a_0, ..., a_n) \prod_{k=0}^{n} (X - a_k) = \prod_{0 \leq i < j \leq n} \left(a_j - a_i\right) \prod_{k=0}^{n} (X - a_k)$$

Ainsi on peut calculer

$$P(a_{n+1}) = V(a_0, ..., a_{n+1}) = \prod_{0 \leq i < j \leq n} \left(a_j - a_i\right) \prod_{k=0}^{n} (a_{n+1} - a_k) = \prod_{0 \leq i < j \leq n+1} \left(a_j - a_i\right)$$

Exercice : endomorphisme qui stabilise toutes les droites

Soit $u \in \mathcal{L}(E)$ qui stabilise toute les droites, qui dire de u ?

Par définition pour tout $x \in E,\ u(x) = \lambda_x x$ avec $\lambda_x \in \mathbb{K}$.

Soit $x, y \in E \setminus \{0\}$.

- Si (x, y) est liée, $y = ax$

$$\lambda_y ax = u(y) = au(x) = \lambda_x ax$$
$$\lambda_y = \lambda_x$$

- Sinon (x, y) est libre

$$\lambda_{x+y}(x + y) = u(x + y) = u(x) + u(y)$$
$$\lambda_{x+y}x + \lambda_{x+y}y = \lambda_x x + \lambda_y y$$
$$\lambda_x = \lambda_{x+y} = \lambda_y$$

Donc pour tout $x \in E, \lambda_x = \lambda$ et $u = \lambda\,\mathrm{id}$.

Endomorphismes nilpotents

Définition d'un endomorphisme nilpotent et inégalité sur son indice.

Soit $u \in \mathcal{L}(E)$, u est dit nilpotent s'il existe $q \in \mathbb{N}^*$ tel que $u^q = 0$.

On appelle indice de nilpotence la valeur

$$d = \min\{q \in \mathbb{N}^* \mid u^q = 0\}$$

On a toujours $d \leq \dim E$.

Démonstration

Comme $u^{d-1} \neq 0$ on dispose de $x \in E$ tel que $u^{d-1} \neq 0$.

Considèrons la famille $\big(x, u(x), ..., u^{d-1}(x)\big)$, soient $\lambda_0, ..., \lambda_{d-1}$ tels que

$$\sum_{k=0}^{d-1} \lambda_k u^k(x) = 0$$

$$u^{d-1}\left(\sum_{k=0}^{d-1} \lambda_k u^k(x)\right) = \lambda_0 u^{d-1}(x) = 0$$

$$\Rightarrow \lambda_0 = 0$$

$$u^{d-2}\left(\sum_{k=1}^{d-1} \lambda_k u^k(x)\right) = \lambda_1 u^{d-1}(x) = 0$$

$$\Rightarrow \lambda_1 = 0$$

$$\vdots$$

$$\lambda_0 = \lambda_1 = \cdots = \lambda_{d-1} = 0$$

D'où $d \leq n$.