Leçon 101 : Groupe monogène, groupes cyclique, exemple.
Développement : (4) Description des groupes cyclique

$(G,*)$ groupe de neutre e

I. Groupes engendrés par une partie :

- **Théo 1 :** Si $(H_i)_{i\in I}$ est une famille de ss-groupe de G, alors $\bigcap_{i\in I} H_i$ est un ss-groupe de G.

- **Déf 2 :** Si A est une partie de G, alors l'intersection de tous les sous-groupes de G contenant A est un ss-groupe de G appelé sous-groupe engendré par A et noté $\langle A\rangle$

- **Prop 3 :** $\langle A\rangle = \{a_1 A \dots a_n a_n\}$ où $n\in\mathbb{N}$ et $a_i \in A\cup A'$
(A' : ens. des symétriques de A dans G.)

- **Exemples :** $(\mathbb{Z};+)$ engendré par $\{1\}$
$(\mathbb{C};+)$ engendré par $\{i\}\cup\mathbb{R}$

II. Groupes monogènes et groupes cycliques :

- **Déf 4 :** G est dit monogène s'il admet une partie génératrice à 1 élément

Si G est monogène et fini, on dit qu'il est cyclique

- **Rem :** un groupe monogène est abélien.

- **Exemple :** $(U_n;\times)$ groupe cyclique
$(\mathbb{Z};+)$ est monogène

- **Théo 5 :** Tout sous-groupe d'un groupe monogène est monogène.
(cyclique) (cyclique)

- **Exemple :** Les seuls sous-groupe de $(\mathbb{Z}/n\mathbb{Z};+)$ sont les ss-groupes $\langle\bar{q}\rangle$ où q/n.

II. Ordre d'un élément :

- **Déf 6 :** L'ordre de a de G est le plus petit entier naturel non nul, s'il existe, tel que $a^n = e$.
S'il n'existe pas, on dit qu'il est d'ordre infini.

- **Exemple :** Dans $(\mathbb{C};\times)$, 2 est d'ordre infini et j est d'ordre 3

- **Rem :** Si a est d'ordre n alors :
$\langle a\rangle = \{e; a; \dots; a^{n-1}\}$
. Ordre de G = Card(G)

- Théo 7 : Si a d'ordre n et $a^k = e$ pour k entier alors $n \mid k$.

- Cor 8 : Si $\mathrm{Card}(G) = n$ alors $\forall a \in G$: $\mathrm{Ordre}(a) \mid n$ (Lagrange) et $a^n = e$

- Théo 9 : Si $a \in G$.
  1) Si a est d'ordre infini alors : $\langle a \rangle \cong (\mathbb{Z}/n\mathbb{Z}; +)$
  2) Si a est d'ordre $n \in \mathbb{N}^*$ alors : $\langle a \rangle \cong (\mathbb{Z}/n\mathbb{Z}; +)$

- Ex : $(\mathbb{Z}/n\mathbb{Z}; +) \cong (\mathbb{U}_n; \times)$

III. Générateurs :

- Théo 10 : Si G cyclique d'ordre n et si a générateur de G (i.e. $G = \langle a \rangle$) alors :
  (i) $\forall d \mid n$ alors G contient $\varphi(d)$ éléments d'ordre d
  (ii) G contient $\varphi(n)$ générateurs : a^k tq $k \wedge n = 1$

- Rem : Si ordre de G est un nombre premier alors G cyclique engendré par tout a de G différent de e

- Exple : $(\mathbb{U}_n; \times)$ est engendré par les racines $n^{ièmes}$ primitives de l'unité.

V. Exemples :

1) Produit de groupes cycliques :

- Théo 11 : Si G_1 et G_2 cyclique d'ordre respectif n et m, alors : $n \wedge m = 1$ ssi $G_1 \times G_2$ cyclique

2) Sous-groupes additifs de $\mathbb{R}$:

- Théo 12 : Si G sous-groupe de $(\mathbb{R}; +)$, $G \neq \{0\}$ alors : $\exists m \in \mathbb{R}_+^*$ tq $G = m\mathbb{Z}$ ou G est dense dans $\mathbb{R}$

3) Groupe symétrique :

- Théo 13 : S_n est engendré par les transpositions du type $(i; i+1)$ où $i \in [\![1; n-1]\!]$

* Prérequis : Groupes, Anneaux pour, indicateur d'Euler, groupe de unités, groupe symétrique, morphisme de groupes, sous-groupes de $\mathbb{Z}$

* Livre : BURG 66 leçons

Compléments leçon 101 - Groupes monogènes, etc.

- Théo 5 : Soit $(G,*)$ un groupe monogène engendré par a.
Soit H un sous-groupe de G
Exple : Soit : $\varphi : (\mathbb{Z},+) \to G$, $n \mapsto a^n$
φ est un morphisme surjectif de groupes, donc $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$
donc $\exists$ un entier r tq $\varphi^{-1}(H) = r\mathbb{Z}$ (car les sous-groupes de $\mathbb{Z}$ sont de cette forme)
φ est surjective, donc $\varphi(\varphi^{-1}(H)) = H = \varphi(r\mathbb{Z})$
donc tout élément de H est de la forme a^{rk} où $k \in \mathbb{Z}$
donc a^r est un générateur de H.

- Les seuls sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ sont les ss-groupes $\langle \bar{q} \rangle$ où $q \mid n$:
Soit H un sous-groupe d'ordre k de $(\mathbb{Z}/n\mathbb{Z},+)$
Par le théorème de Lagrange on a donc : $k \mid n$
donc $n = kq$
Soit $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto m\bar{1}$
On a : $n \in \varphi^{-1}(H) = r\mathbb{Z}$, donc $r \mid n$ et $\exists$ p entier tq $n = rp$
Donc : $H = \varphi(r\mathbb{Z}) = \{\bar{0}; \bar{1}; 2\bar{1}; \dots; (p-1)\bar{1}\}$ de cardinal p
Mais $\mathrm{Card}\, H = k$
donc $k = p$ et donc $rp = qp$ donc $r = q$
d'où $H = \{\bar{0}; \bar{q}; 2\bar{q}; \dots; (k-1)\bar{q}\}$

- Rem : $\langle a \rangle = \{e; a; \dots; a^{n-1}\}$ si ordre de $a = n$:
On a : $\{1; a; \dots; a^{n-1}\} \subset \langle a \rangle$ et $\mathrm{Card}\langle a \rangle = n$

- Théo 7 : Soit $k \in \mathbb{N}^*$ tq $a^k = e$
division euclidienne de k par n : $k = nq + r$ avec $0 \le r < n$
donc : $e = a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r$
donc $r = 0$ (car n = ordre de a)
donc $k = nq$ et $n \mid k$

- Coro 8 : Soit $a \in G$ d'ordre k, alors $\langle a \rangle$ sous-groupe d'ordre k
donc $k \mid n$, $n = kq$
et $a^n = (a^k)^q = e^q = e$

Théo 10 :

1) $\text{Card}\langle a^k\rangle = \min\{m \in \mathbb{N}^* / (a^k)^m = 1\}$
$= \min\{m \in \mathbb{N}^* / a^{km} = 1\}$
$= \min\{m \in \mathbb{N}^* / n \mid km\}$

Posons $d = n \wedge k$, on a alors $n = dn'$ et $k = dk'$ avec n' et k' premiers entre eux (i.e. $n' \wedge k' = 1$)

d'où $n \mid km$ ssi $dn' \mid dk'm$ ssi $n' \mid k'm$ ssi $n' \mid m$ car $n' \wedge k' = 1$ (Gauss)

d'où $\text{Card}\langle a^k\rangle = \min\{m \in \mathbb{N}^* / n' \mid m\}$

or $\min\{m \in \mathbb{N}^* / n' \mid m\} = n'$, i.e. $\frac{n}{d}$

d'où $\text{Card}\langle a^k\rangle = \frac{n}{n \wedge k}$

2) $d \mid n \Rightarrow n = dq$

Soit $a^k \in \langle a\rangle$, alors $\text{Card}\langle a^k\rangle = d$ ssi $\frac{n}{n \wedge k} = d$

ssi $\frac{dq}{n \wedge k} = d$

ssi $\frac{q}{n \wedge k} = 1$

ssi $q = n \wedge k$

et $\exists k' \in \mathbb{N}$ tq $k = qk'$, d'où :

$\text{Card}\langle a^k\rangle = d$ ssi $dq \wedge qk' = q$ ssi $d \wedge k' = 1$

d'où $\text{Card}\langle a^k\rangle = \varphi(d)$

3) a^k engendre $\langle a\rangle$ ssi a^k d'ordre n

Mais a^k est d'ordre $\frac{n}{n \wedge k}$

donc a^k engendre $\langle a\rangle$ ssi $n \wedge k = 1$

il y en a donc $\varphi(n)$

Théo 12 : Formule de Möbius : (plus dans cette leçon refaite)

Soit $\langle a\rangle$ groupe cyclique d'ordre n

$\forall$ diviseur d de n, $\langle a\rangle$ contient $\varphi(d)$ éléments d'ordre d

Mais tout élément de $\langle a\rangle$ a un ordre qui divise n

d'où $n = \sum_{d \mid n} \varphi(d)$ car $\text{Card}\langle a\rangle = \sum_{d \mid n} \text{Card}\{a \in \langle a\rangle \text{ d'ordre } d\}$

Théo 11: Produit de groupes cycliques

$\Rightarrow$: Soit $f: (\mathbb{Z}/mn\mathbb{Z}; +) \to (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}; +)$

$\dot{k} \mapsto (\bar{k}; \tilde{k})$

f est un morphisme de groupes

On cherche $\ker(f)$:

Si $(\bar{k}; \tilde{k}) = (\bar{0}; \tilde{0})$ alors $m \mid k$ et $n \mid k$

mais $m \wedge n = 1$, donc $mn \mid k$

d'où $\dot{k} = \dot{0}$

donc $\ker(f) = \{\dot{0}\}$

et f est donc un monomorphisme

Mais $\text{Card}(\mathbb{Z}/mn\mathbb{Z}) = \text{Card}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$

donc f est un isomorphisme

$\Leftarrow$: On suppose $G_1 \times G_2$ cyclique d'ordre mn et raisonnons par l'absurde:

si $d = m \wedge n \geq 2$, alors $\exists m'$ et n' tq $m = dm'$ et $n = dn'$ avec $m' \wedge n' = 1$

Mais $(m \vee n)(m \wedge n) = mn$

d'où $m \vee n = dm'n' = m'n < mn$

Soit $(x; y) \in G_1 \times G_2$ alors: $(x; y)^{m \vee n} = (x^{m \vee n}; y^{m \vee n}) = (1; 1)$

donc tout $(x; y) \in G_1 \times G_2$ a un ordre $< mn$

impossible car $G_1 \times G_2$ cyclique d'ordre mn.

Sous-groupes additifs de $\mathbb{R}$:

Soit $E = \{x > 0 / x \in H\}$; E est non vide car $\exists h \in H$ avec $h \neq 0$

si $h > 0$ alors $h \in E$, sinon $-h \in E$

donc E est une partie non vide et minorée de $\mathbb{R}$, donc elle admet une borne inférieure.

$$\alpha = \text{Inf}\{x > 0 / x \in H\}$$

- Si $\alpha > 0$: on va montrer que $H = \alpha\mathbb{Z}$

on montre par l'absurde que $\alpha \in H$.

supposons que $\alpha \notin H$, alors par définition de la borne inférieure $\exists h_1, h_2 \in H$ avec $\alpha < h_1 < h_2 < (\alpha + \frac{\alpha}{2})$

On a $h_2 - h_1 \in H$ et $0 < h_2 - h_1 < \alpha$, contradiction avec la définition de α, donc $\alpha \in H$.

Donc $\alpha\mathbb{Z} \subset H$

Soit maintenant $h \in H$.

par division "euclidienne" de h par α on trouve: $h = \alpha q + r$

$r = h - \alpha q$

donc $r \in H$ et $0 \leq r < \alpha$

donc $r = 0$ par définition de α

d'où $h = \alpha q$ et donc $h \in \alpha\mathbb{Z}$ et $H \subset \alpha\mathbb{Z}$

d'où $H = \alpha\mathbb{Z}$

- si $\alpha = 0$: on montre que H est dense dans $\mathbb{R}$

Soit $x \in \mathbb{R}$ et $\varepsilon > 0$ fixés.

Par définition de α, $\exists\, h \in H$ tq $0 < h < \varepsilon$ et comme $\alpha = 0$

On a alors : $h - x > -\left\lfloor \frac{x}{h} \right\rfloor * h \geq -x$

car $h - x = h\left(1 - \frac{x}{h}\right) \Rightarrow \left\lfloor \frac{x}{h} \right\rfloor \leq \frac{x}{h} < \left\lfloor \frac{x}{h} \right\rfloor + 1$

$\Rightarrow -\left\lfloor \frac{x}{h} \right\rfloor \geq -\frac{x}{h} > -\left\lfloor \frac{x}{h} \right\rfloor - 1$

$\Rightarrow 1 - \left\lfloor \frac{x}{h} \right\rfloor \geq 1 - \frac{x}{h} > -\left\lfloor \frac{x}{h} \right\rfloor$

$\Rightarrow h - \left\lfloor \frac{x}{h} \right\rfloor * h \geq h - x > -\left\lfloor \frac{x}{h} \right\rfloor * h$

d'où $0 < x - \underbrace{\left\lfloor \frac{x}{h} \right\rfloor * h}_{\in H} < \varepsilon$

donc $\forall \varepsilon > 0$, $\exists\, y \in H$ tq $0 < y < \varepsilon$

et donc H est dense dans $\mathbb{R}$.

- Théo :

1) Soit l'application $\varphi : k \mapsto a^k$ de $(\mathbb{Z}; +)$ dans $(\langle a \rangle; *)$

On a $\forall (k, l) \in \mathbb{Z}^2$: $\varphi(k+l) = a^{k+l} = a^k * a^l = \varphi(k) * \varphi(l)$

donc φ est un morphisme de groupes.

Donc son noyau est un sous-groupe de $\mathbb{Z}$

donc ! $\exists\, m \in \mathbb{N}$ tq $\ker \varphi = m\mathbb{Z}$

Mais a est d'ordre infini. donc $m = 0$,

(car si $m \neq 0$, $\varphi(k+m) = \varphi(k) \Rightarrow a^{k+m} = a^k$ et a a un ordre fini)

Donc φ est injective.

On a $\operatorname{Im} \varphi = \langle a \rangle$ par construction, donc φ induit une bijection de $(\mathbb{Z}; +)$ sur $(\langle a \rangle; *)$.

Donc ces deux groupes sont isomorphes.

2) Supposons a d'ordre $n \in \mathbb{N}^*$.

Alors $\operatorname{Ker}\varphi = n\mathbb{Z}$

Considérons $\varphi : \mathbb{Z}/n\mathbb{Z} \to \langle a \rangle$

$\bar{k} \mapsto a^k$

On a : $\varphi(\bar{k}+\bar{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k * a^\ell$.

et : $\forall k, k' \in \mathbb{Z}$, on a : $a^k = a^{k'} \Leftrightarrow k \equiv k' \ [n]$

donc $\varphi(\bar{k}+\bar{\ell}) = a^k * a^\ell = \varphi(\bar{k}) * \varphi(\bar{\ell})$

Donc φ est un morphisme de groupes.

Par construction, $\operatorname{Im}\varphi = \langle a \rangle$

Cherchons $\operatorname{Ker}\varphi$:

on a : $\bar{k} \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(\bar{k}) = e \Leftrightarrow a^{\bar{k}} = e = a^0$

$\Leftrightarrow \bar{k} \equiv 0 \ [n]$

donc $\operatorname{Ker}\varphi = \{\bar{0}\}$

Donc φ est un isomorphisme entre le groupe $(\mathbb{Z}/n\mathbb{Z}; +)$ et $(\langle a \rangle; *)$

Leçon 108 : Permutation d'un ensemble fini, groupe symétrique
Développement : (1?) Décomposition permutation, famille minimale

I. Généralités :

- **Déf 1** : Soit $n \in \mathbb{N}^*$. On appelle permutation de $[\![1;n]\!]$ toute bijection de $[\![1;n]\!]$ dans lui-même.
  S_n : ensemble des permutations de $[\![1;n]\!]$
  Si $\sigma \in S_n$, on note :
  $$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$$
- **Prop 2** : * S_n est un groupe de cardinal $n!$
  * S_n est abélien ssi $n=1$ ou 2
- **Prop 3** : Si E ensemble de cardinal n et φ bijection de E sur $[\![1;n]\!]$ alors : $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ est un morphisme bijectif entre l'ensemble des bijections de E dans E ($S(E)$) et S_n.
  (Oral : on peut donc se limiter à l'étude de S_n)
- **Prop 4** : Soit $n \in \mathbb{N}^*$ et $\sigma \in (S_n;\circ)$.
  La relation R définie sur $[\![1;n]\!]$ par : $xRy \Leftrightarrow \exists k \in \mathbb{Z} / y = \sigma^k(x)$ est une relation d'équivalence.
  On appelle orbite de x la classe d'équivalence de x :
  $$Orb_\sigma(x) = \{\sigma^k(x) / k \in \mathbb{Z}\}$$
- **Exemple** : Si $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$
  $Orb_\sigma(1) = Orb_\sigma(3) = \{1;3\}$
  $Orb_\sigma(2) = \{2\}$

II. Cycles et transpositions :

Soit $n \in \mathbb{N}^* \setminus \{1\}$

- **Déf 5** : On dit que σ de $(S_n;\circ)$ est un cycle s'il existe une unique orbite non réduite à un point. On note :
  $\sigma = (a_1; a_2; \dots; a_p)$
  C'est un p-cycle et $l(\sigma) = p$ est sa longueur.
  Un cycle de longueur 2 est appelé transposition.
- **Exemple** : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = (1;4;5;2;3)$
- **Déf 6** : $Supp(\sigma) = \{x \in [\![1;n]\!] / \sigma(x) \neq x\}$
  $Fix(\sigma) = \{x \in [\![1;n]\!] / \sigma(x) = x\}$
- **Prop 7** : Soient n, p de $\mathbb{N}$ tq. $2 \leq p \leq n$.
  Soit $c = (a_1; a_2; \dots; a_n)$ un p-cycle de $(S_n;\circ)$. Alors on a :
  1) $\forall x \in Supp(c)$, $supp(x) = \{c^k(x) / k \in \mathbb{Z}\}$
  2) L'ordre de c dans $(S_n;\circ)$ est $l(c)$
  3) $\forall x \in Supp(c)$, $c = (x; c(x); \dots; c^{l-1}(x))$
- **Prop 8** : deux cycles de $(S_n;\circ)$ à supports disjoints commutent.

III. …
S…
- Thé…
Càl…
de c…
di…
e…
- …
- E…
- Re…

IV …
- …
- Re…
- P…

métrique. Application...
modulaire...

III. Décomposition:

Soit $n \in \mathbb{N}^*$, $n \geq 2$. de manière unique

- Théo 9: Tout σ de $(S_n;\circ)$ se décompose (à l'ordre de facteurs près) en produit de cycles à supports deux à deux disjoints. La partie $\{(1;i) / i \in [\![2;n]\!]\}$ est une famille minimale génératrice de S_n.
- Exemple: $\sigma_1 = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 4&3&1&7&6&5&2 \end{pmatrix} \in S_7$

$= (1;4;7;2;3) \circ (5;6)$

$= (5;6) \circ (1;4;7;2;3)$

$= (1;4) \circ (4;7) \circ (7;2) \circ (2;3) \circ (5;6)$

- Rem: décompo en transpositions en général pas unique! ORAL

IV. Signature:

Soit $\sigma \in (S_n;\circ)$ avec $n \in \mathbb{N}^* \setminus \{1\}$

- Déf 10: on appelle inversion tout couple $(i;j)$ de $[\![1;n]\!]^2$ tq $i<j$ et $\sigma(i) > \sigma(j)$

$I(\sigma)$: nombre d'inversions

$\varepsilon(\sigma) = (-1)^{I(\sigma)}$ signature de σ

si $\varepsilon(\sigma) = 1$, σ est paire, si $\varepsilon(\sigma) = -1$ σ est impaire.

- Rem: Une transposition est impaire.
- Prop 11: $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

- Théo 12: ε est un morphisme de groupe $(S_n;\circ)$ dans le groupe $\{-1;1\}$

- Déf-Théo 15: On appelle groupe alterné d'ordre n le sous-groupe de $(S_n;\circ)$, A_n, des permutations de signature 1. On a: $\text{Ordre}(A_n) = \frac{n!}{2}$ OPTION

V. Applications:

1) Algèbre linéaire:

- Théo 13: pour toute matrice $A = (a_{ij})$ de $\mathcal{M}_n(\mathbb{K})$, on appelle déterminant de A:

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{\sigma(1),1} \dots a_{\sigma(n),n}$$

l'application $\det : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$, $A \mapsto \det A$ est l'unique forme multilinéaire alternée en les colonnes de A valant 1 pour l'identité

2) Théorème de Cayley:

- Théo 14: Soit $(G;.)$ un groupe d'ordre $n \in \mathbb{N}^*$. Il existe un sous-groupe G' de $(S_n;\circ)$ isomorphe à G

3) Géométrie:

- Théo 15: Groupe de Isométries du tétraèdre.

* Prérequis: Morphisme de groupe, relation d'équivalence, composée application, bijective, matrice, ...

* Livre: 66 leçons / Cassor particulier / Oral en poche / BURG

Leçon 103 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Application.
Développement : (2) Indicatrice d'Euler

Prérequis : Arithmétique (Nbre premiers, Thé de Bezout, Gauss) groupes (Théo Lagrange) Anneaux

I. Congruence : Soit $n \in \mathbb{N}^*$

- **Déf 1 :** Si $(a;b) \in \mathbb{Z}^2$ on dit que a est congru à b modulo n ssi $n \mid a-b$ (i.e. $a-b \in n\mathbb{Z}$) et on note $a \equiv b \mod n$ ou $a \equiv b\ [n]$.
  [- Rem. la congruence modulo 0 est la relation d'égalité]
- **Prop 2** $\forall a \in \mathbb{Z}$, il existe un unique entier $r \in \{0; \dots; n-1\}$ tq $a \equiv r \mod n$.
- **Théo 3** Dans $\mathbb{Z}$, la relation $a \equiv b \mod n$ est une relation d'équivalence dont l'ensemble des classes d'équivalence, noté $\mathbb{Z}/n\mathbb{Z}$, est de cardinal n. Si on note $\bar{a}$ la classe d'un entier a on a :
  $$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\}$$
- **Théo 4 :** Soient a, b, a', b' des entiers tqs $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$ alors :
  $a+b \equiv a'+b'\ [n]$
  $ab \equiv a'b'\ [n]$
  $-a \equiv -a'\ [n]$
  et $\forall p \in \mathbb{N}^*$, $a^p \equiv a'^p\ [n]$
- **Applications :** Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

- **Propriétés :** $\forall a, b, c, d \in \mathbb{Z}$ et $\forall n \in \mathbb{N}$ on a :
  * si $a \equiv b\ [n]$ et si $d \mid n$ alors $a \equiv b\ [d]$
  * si P est un polynôme à coefficients entiers et si $a \equiv b\ [n]$ alors $P(a) \equiv P(b)\ [n]$

II. Anneau $\mathbb{Z}/n\mathbb{Z}$

- **Théo 7 :** L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition des classes d'équivalence a une structure de groupe commutatif.
- **Théo 8 :** $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ est un anneau commutatif d'élément neutre $\bar{0}$ et d'élément unité $\bar{1}$.
- **Prop 9 :** Soit $x \in \mathbb{Z}$. On a équivalence entre :
  i) $\bar{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
  ii) x et n premiers entre eux
  iii) $\bar{x}$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}; +)$
- **Rem.** On note $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles de l'anneau.
- **Théo 10 :** On a équivalence entre :
  i) n premier
  ii) L'anneau $(\mathbb{Z}/n\mathbb{Z}; +; \times)$ est un corps.

iii) L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre.

III. Applications :

1) Indicatrice d'Euler :

- Déf 11 : On appelle indicatrice d'Euler la fonction
$\varphi : \mathbb{N}^* \to \mathbb{N}^*$
$n \mapsto 1$ si $n=1$
$\mathrm{Card}(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}))$ sinon

- Rem : $\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

- Théorème 12 d'Euler :
$\forall \bar{a} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ on a : $\bar{a}^{\varphi(n)} = \bar{1}$

- Théorème 13 :
Si p premier alors $\varphi(p) = p-1$
et $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ $\forall \alpha \in \mathbb{N}^*$
Si $p_1, \dots, p_k$ sont les nombres premiers distincts dans la décomposition de n alors :
$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$
et $$n = \sum_{d \mid n} \varphi(d)$$

2) Théorème de Fermat :

- Thé 14 : Soit $a \in \mathbb{Z}$ et p premier
On a : $a^p \equiv a \ [p]$
et si p ne divise pas a on a : $a^{p-1} \equiv 1 \ [p]$

3) Théorème de Wilson :

- Thm 15 : Si p entier ≥ 2 alors on a :
p premier ssi $(p-1)! \equiv -1 \ [p]$

4) Théorème Chinois :

- Théo 16 : Si m et $n \in \mathbb{N}^*$ et $m \wedge n = 1$
alors les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}_m \times \mathbb{Z}_n$ sont isomorphes

- Exemple : Résoudre le système
$\begin{cases} x \equiv 4 \ [5] \\ x \equiv 2 \ [7] \end{cases}$

---

5) Critère d'Eisenstein :

- Théo 17 : Soit $A = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$
Si p divise tous les coefficients de A sauf a_n et si p^2 ne divise pas a_0 alors A est irréductible dans $\mathbb{Z}[X]$

- Ex : $P(X) = 3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$

---

* Prérequis : Arithmétique (Nbre premier, Théo de Bézout, etc), groupes (Théo de Lagrange), Anneaux

* Bibliographie : Buss + 66 leçons

103 : Anneaux Z/nZ - Compléments

Exemples sur les congruences

Exemples 3.8

1. Pour tout entier $n \in \mathbb{N}$, on a $4^n - 1 + 6n \equiv 0 \pmod 9$. En effet :
   - Pour $n = 0$, c'est trivial.
   - Soit $n \neq 0$. $4^n - 1 = (4-1)\left(4^{n-1} + \cdots + 4 + 1\right) = 3\left(1 + 4 + \cdots + 4^{n-1}\right)$: donc
     $4^n - 1 + 6n = 3\left(1 + 4 + \cdots + 4^{n-1} + 2n\right)$;
     or
     $4 \equiv 1 \pmod 3$, donc $1 + 4 + \cdots + 4^{n-1} + 2n \equiv n + 2n \equiv 3n \equiv 0 \pmod 3$.
   - Par conséquent $3\left(1 + 4 + \cdots + 4^{n-1} + 2n\right) \equiv 9n \equiv 0 \pmod 9$, par suite 9 divise $3\left(1 + 4 + \cdots + 4^{n-1} + 2n\right)$.

2. Montrons que $n = \sum_{k=0}^{p} a_k 10^k, a_p \neq 0$ est divisible par 3 si, et seulement si, $\sum_{k=0}^{p} a_k$ est divisible par 3.
   On a $10 \equiv 1 \pmod 3$, par conséquent, pour tout entier $k \in \mathbb{N}$, on a $10^k \equiv 1 \pmod 3$ et aussi $a_k 10^k \equiv a_k \pmod 3$. En utilisant la compatibilité de la congruence avec le produit et la somme on obtient :
   $$n = \sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k \pmod 3,$$
   donc $3 \mid n$ si, et seulement si, $3 \mid \sum_{k=0}^{p} a_k$.

3. Montrons que $7 \mid 3 \times 2^{101} + 9$.
   On décompose 2^{101} en puissances de 2 plus raisonnables. On a $2^{101} = (2^3)^{33} \times 2^2$.
   $$2^3 \equiv 1 \pmod 7 \quad \text{puis}$$
   $$(2^3)^{33} \equiv 1 \pmod 7 \quad \text{puis}$$
   $$3 \times (2^3)^{33} \times 2^2 \equiv 12 \pmod 7 \quad \text{d'où}$$
   $$3 \times 2^{101} + 9 \equiv 21 \equiv 0 \pmod 7.$$

Preuve de la propriété 6 :

Démonstration

1. On a d'une part $a \equiv b \pmod n$ donc pour tout $x \in \mathbb{Z}$ $ax \equiv bx \pmod n$ d'autre part $c \equiv d \pmod n$ donc pour tout $y \in \mathbb{Z}$ $cy \equiv dy \pmod n$ et on a la conclusion par la somme des congruences.
2. Si $n \mid a - b$ alors il existe $q \in \mathbb{Z}$ tel que $a - b = qn$: or il existe $q' \in \mathbb{Z}$ tel que $n = dq'$ par conséquent $a - b = dqq'$ avec $qq' \in \mathbb{Z}$ et $a \equiv b \pmod d$.
3. Posons $P = \sum_{k=0}^{m} c_k x^k$ où $m \in \mathbb{N}$ et $c_k \in \mathbb{Z}$. Or, pour tout entier $k \in [\![0, m]\!]$,
   $$a \equiv b \pmod n \Rightarrow c_k a^k \equiv c_k b^k \pmod n$$
   alors, par la propriété de la somme des congruences, on a :
   $$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod n$$
   ce qui donne la relation cherchée.

Preuve de la structure de groupe de Z/nZ :

Démonstration x, y, z désignent des entiers quelconques de $\mathbb{Z}$. Les propriétés de l'addition vont intervenir de façon essentielle.

Commutativité :

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

Associativité :

$$\overline{x} + (\overline{y} + \overline{z}) = \overline{x} + (\overline{y + z}) = \overline{x + (y + z)} = \overline{(x + y) + z}$$
$$= \overline{x + y} + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}.$$

Neutre : $\overline{0}$ est l'élément neutre pour l'addition :

$$\overline{x} = \overline{x + 0} = \overline{x} + \overline{0}.$$

Opposé : L'opposé de $\overline{x}$ est $\overline{-x}$:

$$\overline{0} = \overline{x + (-x)} = \overline{x} + \overline{-x}.$$

Preuve de la structure d'anneau de Z/nZ :

Démonstration. 1. Définissons la somme de deux classes α et β de $\mathbb{Z}/n\mathbb{Z}$. Soit x un représentant de α. Soit y un représentant de β. On peut alors former l'entier $x + y$ et sa classe associée $\overline{x + y}$. Soient x' un autre représentant de α et y' un autre représentant de β. On peut alors former l'entier $x' + y'$ et sa classe associée $\overline{x' + y'}$. Or $x \equiv x'[n]$ et $y \equiv y'[n]$. Donc, d'après la proposition 36, $x + y \equiv x' + y'[n]$, c'est-à-dire $\overline{x + y} \equiv \overline{x' + y'}$. Ainsi, la classe $\overline{x + y}$ est indépendante des représentants choisis. On dit que c'est la somme des classes $\overline{x}$ et $\overline{y}$. On pose donc $\overline{x} + \overline{y} := \overline{x + y}$.

2. On définit de la même manière $\overline{x} \times \overline{y} := \overline{x \times y}$.

3. On vérifie aisément que l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ remplissent les propriétés caractéristiques d'un anneau commutatif avec $\overline{0}$ l'élément neutre pour l'addition et $\overline{1}$ l'élément neutre pour la multiplication.

Propriété 3.19 Dans $\mathbb{Z}/n\mathbb{Z}$, la multiplication a les propriétés suivantes :

1. Le produit est commutatif. Pour tout x, y dans $\mathbb{Z}$, on a :
$$\overline{x}.\overline{y} = \overline{y}.\overline{x}.$$
2. La classe $\overline{1}$ est élément neutre. Pour tout x dans $\mathbb{Z}$, on a :
$$\overline{1}.\overline{x} = \overline{x}.\overline{1} = \overline{x}.$$
3. Le produit est associatif. Pour tout x, y, z dans $\mathbb{Z}$, on a :
$$(\overline{x}.\overline{y}).\overline{z} = \overline{x}.(\overline{y}.\overline{z}).$$
4. La multiplication est distributive sur l'addition. Pour tout x, y, z dans $\mathbb{Z}$, on a :
$$\overline{x}.(\overline{y} + \overline{z}) = \overline{x}.\overline{y} + \overline{x}.\overline{z}.$$

Preuve de la proposition 9 :

Démonstration. $1 \Rightarrow 2$: $\overline{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. Donc il existe $\overline{u} \in \mathbb{Z}/n\mathbb{Z}$, tel que $\overline{x}.\overline{u} = \overline{1}$. Ainsi, il existe un entier relatif q tel que $xu + nq = 1$. Par conséquent, d'après le théorème de Bézout, x et n sont premiers entre eux.

$2 \Rightarrow 3$: x et n sont premiers entre eux. Donc, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $xu + nv = 1$. Alors, $\overline{x}.\overline{u} = \overline{1}$. Soit $\overline{k} \in (\mathbb{Z}/n\mathbb{Z}, +)$, $\overline{k} = k\overline{1} = k\overline{xu} = ku\overline{x} = w\overline{x}$ avec $w \in \mathbb{Z}$. Donc $\overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$.

$3 \Rightarrow 1$: $\overline{x}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$. En particulier, il existe un entier relatif k tel que $k\overline{x} = \overline{1}$. D'où $\overline{kx} = \overline{1}$. Ainsi, $\overline{x}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. □

Remarque. L'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est noté $(\mathbb{Z}/n\mathbb{Z})^\times$. Alors $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe.

Preuve du théorème 10 :

Démonstration. $1 \Rightarrow 2$: n est premier donc $n \geqslant 2$ et $\mathbb{Z}/n\mathbb{Z} \neq \{\overline{0}\}$. Ainsi, il existe $\overline{r} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{r} \neq \overline{0}$. Nécessairement r est premier avec n, donc, d'après la proposition 38, $\overline{r} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Par conséquent, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.

$2 \Rightarrow 3$: Évident.

$3 \Rightarrow 1$: Supposons n non premier. Si $n = 1$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}\}$ et n'est pas intègre. Si $n \geqslant 2$, alors il existe deux entiers r et s dans $\{2; ...; n-1\}$ tels que $n = rs$. Alors, $\overline{r} \neq \overline{0}$ et $\overline{s} \neq \overline{0}$ mais $\overline{r}.\overline{s} = \overline{0}$. Donc $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ n'est pas intègre. □

Preuve du théorème de Fermat :

Démonstration Comme tout entier relatif admet un représentant positif modulo p, on se restreint au cas $a \in \mathbb{N}$.

- La relation $a^p \equiv a \pmod{p}$ est vraie pour $a = 0$.
  Supposons que $a^p \equiv a \pmod{p}$ soit vrai pour un entier a, et montrons-la pour l'entier $a + 1$. On a :

$$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k,$$

or, pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$, par conséquent :

$$(a+1)^p \equiv a^p + 1 \pmod{p},$$

donc, sachant que, par hypothèse de récurrence, $a^p \equiv a \pmod{p}$, on a :

$$(a+1)^p \equiv a + 1 \pmod{p},$$

ce qui prouve la relation pour tout entier $a \in \mathbb{N}$.

- Si $a^{p-1} \equiv 1 \pmod{p}$ alors, par multiplication par a, $a^p \equiv a \pmod{p}$.
  Réciproquement si $a^p \equiv a \pmod{p}$, alors p divise $a\,(a^{p-1} - 1)$. Comme $p \nmid a$, on a, sachant que p est premier, p et a premiers entre eux et, par le théorème de Gauss, p divise $(a^{p-1} - 1)$. Par conséquent $a^{p-1} \equiv 1 \pmod{p}$.

□

Preuve du théorème de Wilson :

Démonstration

— Si p est premier, alors $\mathbb{Z}/p\mathbb{Z}$ a une structure de corps. Les seules classes non nulles qui sont leur propre inverse sont $\overline{1}$ et $\overline{-1} = \overline{p-1}$ car l'équation $x^2 - 1 = 0$ n'a que ces deux solutions. Or $\overline{(p-1)!} = \overline{1} \times \overline{2} \times \cdots \overline{p-1}$ donc chaque facteur différent de $\overline{1}$ et de $\overline{p-1}$ s'élimine car son inverse fait partie du produit. Finalement $\overline{(p-1)!} = \overline{p-1} = \overline{-1}$, ce qui est la conclusion.

— Réciproquement, si p n'est pas premier, il existe $d \in]\!]1, p[\![$ tel que $d \mid p$. Par suite $d \mid (p-1)!$ et l'hypothèse implique que $d \mid (p-1)! + 1$ donc $d \mid 1$ ce qui est impossible.

□

Preuve du critère d'Einsenstein :

Démonstration. Soit $P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ un polynôme à coefficients dans $\mathbb{Z}$. Soit p un nombre premier vérifiant 1., 2. et 3. Supposons que $P(X)$ ne soit pas irréductible sur $(\mathbb{Z}[X], +, \times)$. Alors il existe deux polynômes non constants $B(X)$ et $C(X)$ de $(\mathbb{Z}[X], +, \times)$ tels que $P(X) = B(X) \times C(X)$. Par conséquent, il existe $k \in \{1; 2; \ldots; n-1\}$ et il existe $b_0, \ldots, b_k, c_0, \ldots, c_{n-k} \in \mathbb{Z}$ tels que :

$$\sum_{i=0}^{i=n} a_i X^i = \left(\sum_{i=0}^{i=k} b_i X^i\right)\left(\sum_{i=0}^{i=n-k} c_i X^i\right)$$

Égalité qui, dans $((\mathbb{Z}/p\mathbb{Z})[X], +, \times)$ devient :

$$\sum_{i=0}^{i=n} \overline{a_i} X^i = \left(\sum_{i=0}^{i=k} \overline{b_i} X^i\right)\left(\sum_{i=0}^{i=n-k} \overline{c_i} X^i\right)$$

Et donc, d'après 1. et 2. :

$$\overline{a_n} X^n = \left(\sum_{i=0}^{i=k} \overline{b_i} X^i\right)\left(\sum_{i=0}^{i=n-k} \overline{c_i} X^i\right)$$

Soit :

$$\overline{a_n} X^n = \overline{b_k} X^k \times \overline{c_{n-k}} X^{n-k}$$

Par conséquent, $\overline{b_0} = \overline{c_0} = \overline{0}$. Donc, p^2 divise $b_0 c_0$. Or $b_0 c_0 = a_0$. Donc p^2 divise a_0. Ce qui est en contradiction avec 3.

□

Exemple de résolution d'un système de congruence par le théorème chinois :

Exemple. Résolvons le système de congruences $\begin{cases} x \equiv 4[5] \\ x \equiv 2[7] \end{cases}$. Il existe deux entiers relatifs k et k' tels que $x = 4 + 5k$ et $x = 2 + 7k'$. Travaillons dans $(\mathbb{Z}/5\mathbb{Z}, +, \times)$. On a : $\overline{x} = \overline{4}$ et $\overline{x} = \overline{2} + \overline{7}\overline{k'}$. D'où : $\overline{7}\overline{k'} = \overline{2}$. Or, 7 est premier avec 5, donc $\overline{7}$ est inversible dans $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ d'après la proposition 38. Son inverse est $\overline{3}$ car $\overline{3} \times \overline{7} = \overline{21} = \overline{1}$. Ainsi, on a $\overline{7} \times \overline{3} = \overline{1}$ et $\overline{7}\overline{k'} = \overline{2}$, donc nécessairement, $\overline{k'} = \overline{2 \times 3} = \overline{6} = \overline{1}$. Et par conséquent, il existe un entier relatif l tel que $k' = 1 + 5l$. D'où $x = 2 + 7(1 + 5l) = 9 + 35l$. Ainsi, $\mathcal{S} = \{9 + 35l, l \in \mathbb{Z}\}$.

Leçon 105 : Nombres Premiers. Propriétés et applications.
Développement : (9) Théorème d'Euler

Prérequis : Nombres premiers entre eux, lemme de Gauss, anneaux $\mathbb{Z}/n\mathbb{Z}$, anneaux $\mathbb{K}[X]$, congruences

I. Définitions et propriétés

- Déf 1 : Soit $p \in \mathbb{N}$, $p \geq 2$. p est dit premier si ses seuls diviseurs sont 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers
- Rem : Un entier $p \geq 2$ non premier est dit composé.
- Déf 2 : Tout diviseur premier d'un entier composé n est appelé facteur premier de n.
- Prop 3 : Tout entier $n \geq 2$ admet au moins un facteur premier. Si n est composé alors il existe un diviseur premier p de n vérifiant : $2 \leq p \leq \sqrt{n}$
- Exemple : * si p et q premiers, alors $p|q \Rightarrow p = q$
  * Si p premier, alors $\forall k \in [\![1, p-1]\!]$, on a : $p \mid \binom{p}{k}$
  * Si $n \in \mathbb{N}^*$ est premier alors $M^n = 2^n - 1$ est premier (Nombre de Mersenne)
- Théo 4 : L'ensemble $\mathcal{P}$ est infini
- Théo 5 : Soient p premier et a, b des entiers non nuls.
  * si $p|ab$ alors $p|a$ ou $p|b$
  * $\forall n \in \mathbb{N}^*$, si $p|a^n$ alors $p|a$

II. Décomposition primaire

- Théo 6 : Théo. fondamental de l'arithmétique
  Soit n entier ≥ 2
  1) $\exists m \in \mathbb{N}^*, \exists p_1, \dots, p_m \in \mathcal{P}$ distincts deux à deux $\exists \alpha_1, \dots, \alpha_m \in \mathbb{N}^*$ tq : $n = \prod_{i=1}^{m} p_i^{\alpha_i}$
  2) Cette décomposition est unique à l'ordre des facteurs près
- Ex : $75 = 3 \times 5^2$
- Théo 7 : $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ admet $\prod_{i=1}^{m} (1 + \alpha_i)$ diviseurs
- Théo 8 : Si a et $b \in \mathbb{N}$, a et $b \geq 2$ de décompositions primaires :
  $a = p_1^{\alpha_1} \dots p_N^{\alpha_N}$
  $b = p_1^{\beta_1} \dots p_N^{\beta_N}$
  alors : $pgcd(a;b) = \prod_{i=1}^{N} p_i^{\min(\alpha_i, \beta_i)}$

$a^{p-1} \equiv 1 [p]$

sont et $\text{ppcm}(a;b) = \prod_{i=1}^{N} \max(\alpha_i; \beta_i)$

- Ex: $a = 24 = 2^3 \times 3$; $b = 36 = 2^2 \times 3^2$
$\Rightarrow a \wedge b = 2^2 \times 3 = 12$
$a \vee b = 2^3 \times 3^2 = 72$

III. Théorème d'Euler:

- Déf 9: On appelle indicatrice d'Euler la fonction:
$\varphi : \mathbb{N}^* \to \mathbb{N}^*$
$n \mapsto 1$ si $n = 1$
$\text{Card}\{k \in [\![1; n]\!] / k \wedge n = 1\}$ sinon

- Théo 10: Si $p_1, \dots, p_k$ sont les nombres premiers distincts dans la décomposition de n, alors
$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$
et $n = \sum_{d \mid n} \varphi(d)$

- ...

IV. Le corps $\mathbb{Z}/p\mathbb{Z}$:

- Théo 11: $(\mathbb{Z}/p\mathbb{Z}; +; \times)$ est un corps ssi p est premier.

- Théo 12: Petit théorème de Fermat.
Soient $a \in \mathbb{Z}$, $p \in \mathbb{P}$. on a:
$a^p \equiv a [p]$
et si p ne divise pas a,

- Théo 13: Théorème de Wilson:
Soit $p \in \mathbb{N}$ tq $p \geq 2$
Alors on a:
$p \in \mathbb{P}$ ssi $(p-1)! \equiv -1 [p]$

V. Critère d'Eisenstein:

- Théo 14: Soit $A = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$
si p divise tous les coefficients de A sauf a_n et si p^2 ne divise pas a_0, alors A est irréductible dans $\mathbb{Z}[X]$.

- Exemple: $P(X) = 5X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Z}[X]$

* Prérequis: Nbs premiers, pgcd, PPCM, Anneaux $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{K}[X]$, congruences

* Liens: 66 Lesage, Burg

Preuve du théorème fondamental de l'arithmétique :

Existence : Si n est premier, alors la preuve est terminée. Supposons que n ne soit pas premier et considérons l'ensemble

$$D = \{d\ ;\ d|n \ \text{ et } \ 1 < d < n\}.$$

D est une partie de $\mathbb{N}$, non vide car n est composé. D contient un plus petit élément p_1 qui est premier, sinon p_1 ne serait pas minimal. On peut alors écrire $n = p_1 n_1$. Si n_1 est premier alors la preuve est terminée, sinon, on répète le même processus que ci-dessus et on en déduit l'existence d'un nombre premier p_2, non nécessairement distinct de p_1, et d'un entier $n_2 < n_1$ tels que $n = p_1 p_2 n_2$. En poursuivant ainsi, on aboutit à la k-ième étape à :

$$n = p_1 p_2 \dots p_k n_k \ \text{ avec } \ n_1 > n_2 > \dots > n_k > 1.$$

Comme les entiers n_i sont strictement décroissants, le processus s'arrête à une k-ième étape où n_k est premier, soit en posant $n_k = p_{k+1}$, on a :

$$n = p_1 p_2 \dots p_{k+1},$$

et, en regroupant les facteurs premiers égaux, on a la relation.

Unicité à l'ordre près : Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N} = q_1^{\beta_1} p_2^{\beta_2} \dots q_M^{\alpha_M}$.

Pour tout $1 \leqslant i \leqslant N$, p_i divise l'un des q_j donc $p_i = q_j$, par conséquent

$$\{p_1, p_2, \dots, p_N\} \subset \{q_1, q_2, \dots, q_M\}.$$

On obtient de même l'inclusion inverse. Donc $M = N$ et en permutant les facteurs premiers, posons $q_i = p_i$ on a :

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N} = p_1^{\beta_1} p_2^{\beta_2} \dots p_N^{\beta_N}$$

Pour tout entier i, on a alors $p_i^{\alpha_i} | p_1^{\beta_1} p_2^{\beta_2} \dots p_N^{\beta_N}$ donc il existe un entier k tel que $p_i^{\alpha_i} | p_i^{\beta_i} k$ mais comme $p_i^{\alpha_i} \wedge k = 1$, on a $p_i^{\alpha_i} | p_i^{\beta_i}$, par conséquent $\alpha_i \leqslant \beta_i$. On obtient de même $\beta_i \leqslant \alpha_i$. Ainsi $\alpha_i = \beta_i$.

□

Preuve du PGCD et du PPCM

Démonstration

PGCD : Posons $d = a \wedge b$ et $\delta = \prod_{i=1}^{N} p_i^{\min(\alpha_i, \beta_i)}$.

D'une part on a $\delta | a$ et $\delta | b$ donc $\delta | d$.

D'autre part, $d | a$ et $d | b$ donc, par le théorème précédent, on a $d = \prod_{i=1}^{N} p_i^{\gamma_i}$

pour tout $i \leqslant N$, $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$, ce qui signifie que $\gamma_i \leqslant \min(\alpha_i, \beta_i)$. On en déduit que $d | \delta$.

Par conséquent, dans $\mathbb{N}^*$, on a $d | \delta$ et $\delta | d$ donc $d = \delta$.

PPCM : On utilise la relation $(a \wedge b)(a \vee b) = ab$. Cette relation s'écrit maintenant

$$\prod_{i=1}^{N} p_i^{\min(\alpha_i, \beta_i)} (a \vee b) = \prod_{i=1}^{N} p_i^{\alpha_i + \beta_i}, \quad \text{soit} \quad a \vee b = \prod_{i=1}^{N} p_i^{\alpha_i + \beta_i - \min(\alpha_i, \beta_i)}$$

or $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$, et nous obtenons la relation voulue.

Leçon 106 : Idéaux d'un anneau commutatif. Exemples.
Développement : Radical d'un Idéal

$(A;+;\times)$ anneau commutatif

I. Définitions :

- Déf 1 : Soit $I \subset A$. On dit que I est un idéal de A si :
  (i) $(I;+)$ sous-groupe de $(A;+)$
  (ii) $\forall (x;a) \in I \times A,\ ax \in I$

- Exple :
  * idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ ($n \in \mathbb{N}$)
  * $I = \{f \in \mathcal{C}(\mathbb{R};\mathbb{R}) / f(0) = 0\}$ est un idéal de $\mathcal{C}(\mathbb{R};\mathbb{R})$

- Prop 2 : Si A unitaire et si $1 \in I$ idéal de A, alors $I = A$.
  Si I possède un élément inversible de A alors $I = A$

- Prop 3 : Une intersection d'idéaux de A est un idéal de A.

- Prop 4 : Une somme finie d'idéaux de A est un idéal de A.

- Rem : Faux pour une union

- Exple : $\forall (a;b) \in \mathbb{N}$,
  $a\mathbb{Z} \cap b\mathbb{Z} = pgcd(a;b)\mathbb{Z}$
  $a\mathbb{Z} + b\mathbb{Z} = ppcm(a;b)\mathbb{Z}$

- Déf 5 : Soit X un sous-ensemble de A. On appelle idéal engendré par X le plus petit idéal contenant X. C'est l'intersection de tous les idéaux contenant X. On le note (X)

- Rem : si I, J idéaux de A :
  $I + J$ est l'idéal engendré par $I \cup J$.

II. Idéaux principaux :

- Déf 6 : Un idéal I de A est dit principal s'il existe $a \in A$ tq $I = aA = (a)$
  Un anneau A est dit principal s'il est commutatif, unitaire intègre et si tous ses idéaux sont principaux.

- Exple : $(\mathbb{Z};+;\times)$ est principal,
  * $\mathbb{Z}[X]$ n'est pas principal car $(X;2)$ est l'ensemble des polynômes de $\mathbb{Z}[X]$ tq $P(0) = 0$ et P pair.

- Prop 7 : Un anneau commutatif (intègre) est un corps si ses idéaux sont $\{0\}$ et A.

III. Anneau quotient :

- Déf 8 : Soit I idéal de A. La relation $\mathcal{R}$ définie sur A par :
  $a \mathcal{R} b$ ssi $b - a \in I$
  est une relation d'équivalence

- Prop

mple.

- Prop 9: A/R muni de loi $\bar{x}+\bar{y}=\overline{x+y}$ et $\bar{x}\cdot\bar{y}=\overline{x\cdot y}$ (où $\bar{x}$ désigne la classe de x) est un anneau appelé anneau quotient et noté A/I

IV. Idéaux et morphismes d'anneaux:

- Prop 10: Si A' anneau et $f: A \to A'$ morphisme d'anneaux alors:
  i) $\ker f$ idéal de A
  ii) si I idéal de A et f surjective alors $f(I)$ idéal de A
  iii) si I' idéal de A', alors $f^{-1}(I')$ est un idéal de A

- Prop 11: La caractéristique d'un anneau unitaire intègre est 0 ou un nombre premier.

V. Radical d'un idéal.

- Déf 12: Si A anneau commutatif unitaire et I idéal de A, on appelle radical de I l'ensemble: $\sqrt{I} = \{a \in A / \exists n \in \mathbb{N}^* \text{ tq } x^n \in I\}$

- Prop 13: $\sqrt{I}$ est un idéal de A

- Ex: Si $I = n\mathbb{Z}$ idéal de $\mathbb{Z}$ alors $\sqrt{I} = p_1 \dots p_k \mathbb{Z}$ où $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ décomposition en facteurs premiers de n

VII. Idéaux premiers, maximaux:

- Déf 14: Si A anneau commutatif intègre, un idéal P de A ($P \neq A$) est dit premier si $\forall x, y$ de A on a: $xy \in P \Rightarrow x \in P$ ou $y \in P$

- Prop 15: P idéal premier ssi A/p intègre

- Déf 16: Un idéal M de A ($M \neq A$) est dit maximal si les seuls idéaux contenant M sont M et A

- Prop 17: M maximal ssi A/M est un corps

- Prop 18: Tout idéal maximal est premier

* Compléments leçon 106 : Idéaux d'un anneau commutatif. Exemples.

(Toutes les preuves dans Goeurdon)

- Prop : si A unitaire et $1 \in I$, alors $I = A$

- Preuve : $\forall a \in A$, $1a \in I$, donc $A \subset I$ et $I = A$

- Prop : Si I possède un élément inversible alors $I = A$

- Preuve : si $x \in A$ inversible, alors $x \cdot x^{-1} \in I$, i.e. $1 \in I$ et donc $I = A$

- Prop : Une intersection d'idéaux de A est un idéal de A.

- Preuve : Si I, J deux idéaux de A, on a : $I \cap J = \{x / x \in I \text{ et } x \in J\}$

  - $0 \in I \cap J$ car $0 \in I$ et $0 \in J$ (I, J sous-groupes de A)
  - si $x \in I \cap J$ alors $x \in I$ et $x \in J$
    donc $x^{-1} \in I$ et $x^{-1} \in J$ (car sous-groupe)
    donc $x^{-1} \in I \cap J$

  } $I \cap J$ sous-groupe de A

  - Soit $a \in A$ et $x \in I \cap J$, alors $ax \in I$ et $ax \in J$ (car idéaux de A)
    donc $ax \in I \cap J$

  Donc $I \cap J$ idéal de A.

- Prop : Somme finie d'idéaux est un idéal.

- Preuve : Soit I, J idéaux de A, $I + J = \{x + y / x \in I \text{ et } y \in J\}$

  on a : $\cdot$ $0 \in I + J$ car $0 = 0 + 0$

  - Si $x \in I$, $x = x + 0 \in I + J$
    d'où $x^{-1} = x^{-1} + 0 \in I + J$
    (de même si $x \in J$)
  - Soit $a \in I + J$, $a = x + y$ avec $x \in I$ et $y \in J$
    $b \in I + J$, $b = x' + y'$ avec $x' \in I$ $y' \in J$
    } $a + b \in I + J$ (facile)

  donc $(I + J; +)$ est bien un sous-groupe de A

  - Soit $b \in I + J$ et $a \in A$. On a : $ab = a(x + y)$
    $= ax + ay \in I + J$

  Donc $I + J$ idéal de A

- Rem: $I+J$ idéal engendré par $I \cup J$.

- Preuve: Soit $K = \cap M$ tel que M idéal de A et $I \cup J \subset M$
  - On sait que $I \cup J \subset I+J$
    donc $I+J$ idéal contient $I \cup J$
    donc $K \subset I+J$
  - Tout idéal qui contient I et J contient $I+J$
    donc $I+J \subset K$

  Donc $K = I+J$

- Prop: La caractéristique d'un anneau unitaire intègre est 0 ou un nombre premier.

- Preuve: Soit c la caractéristique d'un anneau unitaire intègre.
  Si $c \neq 0$ et c non premier, alors on a: $c = ab$ avec $1<a<c$, $1<b<c$

  donc $0 = ce = (ae)(be)$
  Comme A est intègre on a alors: $ae = 0$ ou $be = 0$
  ce qui est absurde car c est le plus petit entier strictement positif tel que $ce = 0$.
  donc c non premier.

- Prop: Un anneau commutatif intègre est un corps ssi ses idéaux sont $\{0\}$ et A.

- Preuve: . Si A est un corps:
  A est alors intègre et tous ses éléments non nuls sont inversibles.
  Soit I un idéal de A.
  - Soit $I = \{0\}$
  - Soit $I \neq \{0\}$ et $\exists\, x \in I$ non nul et x admet un inverse
    donc $x x^{-1} = 1 \in I$ et $I = A$

  . Si A ne possède que deux idéaux, $\{0\}$ et A.
  Soit $x \in A$ et $I = (x)$ idéal engendré par x non nul
  on a donc $I = A$
  et donc $\exists\, y$ tel que $xy = 1$
  et x est donc inversible

  Donc A est un corps.

Prop: P idéal premier ssi A/p intègre

Preuve: • soit $x \in A$ et $\bar{x}$ sa classe dans A/p
alors on a: P premier $\Leftrightarrow$ $(xy \in P \Rightarrow x \in P$ ou $y \in P)$
$\Leftrightarrow$ $(\overline{xy} = \bar{0} \Rightarrow \bar{x} = \bar{0}$ ou $\bar{y} = \bar{0})$
$\Leftrightarrow$ $(\bar{x}\bar{y} = \bar{0} \Rightarrow \bar{x} = \bar{0}$ ou $\bar{y} = \bar{0})$
$\Leftrightarrow$ A/p est intègre

Prop: M maximal ssi A/M est un corps.

Preuve: • Si M est un idéal maximal de A:
Soit $x \in A$ tel que $\bar{x}$ sa classe dans A/M et tel que: $\bar{x} \neq \bar{0}$
alors $x \notin M$
On a: $I = M + (x)$ est un idéal de A contenant M et différent de M (car $x \notin M$)
donc $I = A$ par hypothèse (M est maximal)
donc: $\exists\, a \in A$ et $m \in M$ tel que $1 = m + ax$
i.e.t.q.: $\bar{1} = \bar{a}\bar{x}$
donc $\bar{x}$ est inversible et A est un corps.

• Si A/M est un corps:
Soit I idéal de A tel que $M \subset I$ et $M \neq I$
Soit $a \in I$ t.q. $a \notin M$, donc $\bar{a} \neq \bar{0}$
Comme A/I est un corps, on a: $\exists\, b \in A$ tel que $\bar{a}\bar{b} = \bar{1}$
donc: $\exists\, m \in M$ tel que $ab = 1 + m$
et $1 = ab - m$ $\in I$
$\in I$ $\in I$ car $M \subset I$
d'où $I = A$
et M est maximal.

Prop: Tout idéal maximal est premier

Preuve: Soit M un idéal maximal de A
donc A/M est un corps, donc un anneau intègre
donc M est un idéal premier.

Leçon 107 : PGCD dans $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps commutatif
Développement : (20) Lemme des Noyaux

$A = \mathbb{Z}$ ou $\mathbb{K}[X]$ avec $\mathbb{K}$ corps commutatif

I. Division euclidienne dans A :

- **Théo 1** : Si $(a;b) \in A^2$ et $b \neq 0$, il existe un unique couple $(q;r) \in A^2$ tq $a = bq + r$ et :
(oral : q quotient, r reste)
$\begin{cases} 0 \leq r < |b| \text{ si } A = \mathbb{Z} \\ \deg(r) < \deg(b) \text{ si } A = \mathbb{K}[X] \end{cases}$

- **Rem** : Si $r = 0$, on dit que b divise a ou que a est un multiple de b et on note a/b.

- **Exemples dans** $\mathbb{Z}$: $-21 = -9 \times 5 + 2$
* dans $\mathbb{K}[X]$: $X^3 + X^2 + 1 = (X^2 - 1)(X+1) + X + 2$
* $(X+1) / (X^2 - 1)$ dans $\mathbb{Z}[X]$

- **Théo 2** : L'anneau $(A; +; \times)$ est principal.

- **Cor 3** : Les idéaux de A sont les ensembles de la forme PA où $P \in A$

- on convient que si g générateur d'un idéal principal :
(ORAL : pour avoir unicité)
  - $g \geq 0$ si $A = \mathbb{Z}$
  - g unitaire si $A = \mathbb{K}[X]$ (et $g = 0$ si idéal nul)

II. PGCD :

- **Prop 4** : Soit $(a;b) \in A^2$. Il existe $d \in A$ tq $aA + bA = dA$ (avec d respectant la convention) d est appelé le plus grand commun diviseur de a et b et on note $d = a \wedge b$

- **Def 5** : Si $a \wedge b = 1$ on dit que a et b sont premiers entre eux.

- **Rem** : * $a \wedge 0 = a \quad \forall a \in A$
* si $d = a \wedge b$ alors : $\exists (u;v) \in A^2$ tq $d = au + bv$
(u;v : coefficients de Bézout, Non unique)

- **Prop 6** : Si q et r sont le quotient et le reste respectifs de a et b (avec $(a;b) \in A^2$ et $b \neq 0$), alors on a :
$a \wedge b = b \wedge r$
(- Rem : cette propriété permet de ORAL déterminer un pgcd par itération)

III. Algorithme d'Euclide :

Entrée : a, b
Tant que $b \neq 0$
  $q \leftarrow$ quotient de la div. eucl. de a par b
  $r \leftarrow$ reste
  $a \leftarrow b$
  $b \leftarrow r$
Fin
Afficher a

- Exemple
- Rem :
- Suite
- Prop 9 :
- Lemme
Soit
et
- Prop

…commutatif, théorème de Bézout. Algorithme d'Euclide. Applications.

- Exemple dans $\mathbb{Z}$: pgcd de 42 et 33

$42 = 1\times 33 + 9$
$33 = 3\times 9 + 6$
$9 = 1\times 6 + 3$
$6 = 2\times 3 + 0$
donc $42\wedge 33 = 3\wedge 0 = 3$

- Rem : en remontant l'algorithme d'Euclide on peut trouver des coefficients de Bézout.

- Suite exemple :

$3 = 9 - 1\times 6$
$3 = 9 - 1\times(33 - 3\times 9)$
$3 = 4\times 9 - 1\times 33$
$3 = 4\times(42 - 1\times 33) - 1\times 33$
$3 = \underline{4}\times 42 - \underline{5}\times 33$

IV. Théorème de Bézout et application

- Théo 8 : de Bézout
Soit $(a;b)\in A^2$. Alors on a :
$a\wedge b = 1$ ssi il existe $(u;v)\in A^2$ tq $au + bv = 1$

- Prop 9 : Soit $(a;b;c)\in A^3$ tq $a\wedge b = 1$ et $a\wedge c = 1$, alors : $a\wedge bc$

- Lemme 10 : de Gauss
Soit $(a;b;c)\in A^3$. Si $a\wedge b = 1$ et $a|bc$ alors $a|c$.

- Prop 11 : Soit $(a;b;c)\in A^3$ tel que $a\wedge b = 1$, $a|c$ et $b|c$. Alors on a : $ab|c$
(Gnal : de 9 à 10 : se généralisent par récurrence)

V. Applications :

1) Lemme des noyaux :

- Lemme 12 : Soit $u\in\mathcal{L}(E)$ où E est un $\mathbb{K}$-e.v. Soient $(P_1;\dots;P_n)\in\mathbb{K}[X]^n$ polynômes 2 à 2 premiers entre eux ($n\in\mathbb{N}^*$). Alors : $\mathrm{Ker}\left(\prod_{k=1}^{n} P_k(u)\right) = \bigoplus_{k=1}^{n}\mathrm{Ker}(P_k(u))$

2) Equation diophantienne $ax+by=c$

- Proposition 13 : Soient a,b,c dans $\mathbb{Z}$ tq. $a\neq 0$ et $b\neq 0$. L'équation $ax+by=c$ possède au moins une solution dans $\mathbb{Z}^2$ ssi $a\wedge b|c$

3) Théorème chinois :

- Théo 14 : Soient $(a;b)\in\mathbb{Z}^2$ et $(n;m)\in\mathbb{N}^2$ tels que $n\wedge m = 1$. Alors le système de congruences $\begin{cases} x\equiv a\,[n] \\ y\equiv b\,[m]\end{cases}$ admet une unique solution modulo nm

* Prérequis : anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, idéaux, polynômes, e.v, congruences

* Livres : Oral en poche (pour les $\mathbb{Z}$ et $\mathbb{K}[X]$), 66 leçons de BURG

* Compléments leçon 107 : PGCD dans $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps commutatif, théorème de Bézout. Algorithme d'Euclide. Application

→ Equation diophantienne $ax+by=c$

- Proposition : Soient a,b,c dans $\mathbb{Z}$ tq $(a;b)\neq(0;0)$ et $d=a\wedge b$.
L'équation $ax+by=c$ possède au moins une solution dans $\mathbb{Z}^2$ ssi $d|c$

- Preuve : • si $c=0$, alors $d|c$ et $(x;y)=(0;0)$ est une solution
(BURG) • si $c\neq 0$;
il existe alors $(u;v)\in\mathbb{Z}^2$ tq $d=au+bv$ (car $d=a\wedge b$)
- si d ne divise pas c et s'il existe une solution $(x;y)\in\mathbb{Z}^2$ de l'équation $ax+by=c$, alors $d|ax+by=c$ impossible.

- si $d|c$: soient $c'=\frac{c}{d}$, $a'=\frac{a}{d}$ et $b'=\frac{b}{d}$
L'équation est alors équivalente à : $a'x+b'y=c'$
avec $a'\wedge b'=1$
donc $\exists (u;v)\in\mathbb{Z}^2$ tq $a'u+b'v=1$
d'où $a'cu+b'cv=c$
i.e. $\frac{a}{d}cu+\frac{b}{d}cv=c$
i.e. $a\frac{cu}{d}+b\frac{cv}{d}=c$
et comme $d|c$, $\left(\frac{cu}{d};\frac{cv}{d}\right)\in\mathbb{Z}^2$
donc le couple $\left(\frac{cu}{d};\frac{cv}{d}\right)$ est solution de $ax+by=c$

- Ensemble des solutions :
Si $(x_0;y_0)$ est une solution particulière de l'équation $ax+by=c$ alors les solutions sont les couples $(x;y)$ de $\mathbb{Z}^2$ donnés par :

$$\begin{cases} x=x_0+\frac{kb}{d} \\ y=y_0-\frac{ka}{d} \end{cases} \quad \text{où } k\in\mathbb{Z}$$

- Preuve : $a = da'$, $b = db'$, $c = cd'$ avec $a' \wedge b' = 1$

On détermine une solution particulière de $a'x + b'y = 1$ en multipliant par c on trouve une solution particulière $(x_0; y_0)$ de $a'x + b'y = c$

S'il existe une autre solution $(x; y)$ de $a'x + b'y = c$

alors : $a'x + b'y = a'x_0 + b'y_0$

d'où $a'(x - x_0) = b'(y_0 - y)$

donc $a' \mid b'(y_0 - y)$. Mais comme $a' \wedge b' = 1$, alors par le théorème de Gauss : $a' \mid (y_0 - y)$

donc $\exists k \in \mathbb{Z}$ tq $y_0 - y = ka'$

i.e. $y = y_0 - ka'$

d'où $a'x = b'(y_0 - y_0 + ka') + a'x_0$

$a'x = a'b'k + a'x_0$

$x = x_0 + kb'$

La réciproque est évidente

→ Théorème Chinois :

Soient $(a; b) \in \mathbb{Z}^2$ et $(n; m) \in \mathbb{N}^2$ tq $n \wedge m = 1$. Alors le système de congruence $\begin{cases} x \equiv a\ [n] \\ y \equiv b\ [m] \end{cases}$ admet une unique solution modulo nm

- Preuve : (PURG)

. On a : $n \wedge m = 1$

donc par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tqs $un + vm = 1$, i.e. tq $un \equiv 1\ [m]$ et $vm \equiv 1\ [n]$

Bof Bof

Posons $x = bun + avm$

on a bien alors $x \equiv a\ [n]$ et $x \equiv b\ [m]$

. Unicité : Si y a une autre solution, alors : $x - y \equiv 0\ [n]$ et $x - y \equiv 0\ [m]$

Comme $n \wedge m = 1$ on a $x - y \equiv 0\ [nm]$.

Leçon 108 : Polynômes à une indéterminée à coefficients réels ou complexes.

Développements : *Théorème de d'Alembert Gauss*
Oral en poche (pour les trucs à mettre dedans !) + Algèbre et géométrie Burg

I. Définitions et structures :
Définition d'un polynôme coefficients, coefficients constants
Définition des opérations (addition, produit par un scalaire, produit)
Théo : sev de Kn et anneau commutatif
Notation usuelle

II. Degré d'un polynôme :
Définition du degré + coefficient dominant
Propriété des degrés de la somme et du produit de deux polynômes
Cor : Kn[X] sev de K[X] dont (1,X,...,X^n) est une base
Intégrité de K[X] et polynômes inversibles

III.Divisibilité dans K[X] :
Définition associés et diviseurs multiples
Théorème division euclidienne dans K[X]
Rem : détermination du PGCD

IV. Fonctions polynômiales et racines d'un polynôme :
Définition
Définition racines + propriétés des racines (divisibilité, conjugaison)
Propriétés sur le nombre de racines par rapport au degré, etc.
Théorème de d'Alembert Gauss
Définition et propriétés racines multiples

V. Dérivation d'un polynôme :
Définition + propriétés (degré, dérivation somme et produit)
Formule de Taylor
Théorème d'approximation de Weierstrass

II. Réductions :
1)Diagonalisation :
Définition + propriétés en lien avec valeurs propres, etc.
exemple
2) Trigonalisation :

Leçon 109 : Racines d'un polynôme à une indéterminée. Relation
Développement : (5) Théorème de d'Alembert-Gauss

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I. Division euclidienne :

- Théo 1 : Soient A et B de $\mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(Q;R) \in \mathbb{K}[X]^2$ tq : $A = BQ + R$ et $\deg R < \deg B$
  Q est le quotient de A par B et R est le reste de la division euclidienne de A par B.

- Exemple : $(X^4 + X^2 + X + 2) = (X^2 - 3)(X^2 + 4) + X + 14$

- Déf 2 : Si le reste est le polynôme nul, on dit que B divise A ou que A est multiple de B et on note $B \mid A$.

II. Racine d'un polynôme :

Soit P un polynôme de $\mathbb{K}[X]$

1) Notion sur les racines :

- Déf 3 : $x \in \mathbb{K}$ est racine de P si $P(x) = 0$.

- Exemple : $P = X^2 + X + 1$ n'a pas de racine dans $\mathbb{R}$ mais P a deux racines j et $\bar{j}$ dans $\mathbb{C}$
  (on a : $\mathbb{R}[X] \subset \mathbb{C}[X]$)

- Théo 4 : de d'Alembert-Gauss :
  Tout polynôme non constant admet au moins une racine dans $\mathbb{C}$.

- Théo 5 : Si $a \in \mathbb{K}$, il existe un unique polynôme Q de $\mathbb{K}[X]$ tel que
  $P = (X - a)Q + P(a)$

- Cor 6 : $a \in \mathbb{K}$ est racine de P ssi $(X - a) \mid P$

- Exemple : $(X - j) \mid X^2 + X + 1$

- Rem : i) si $Q \mid P$ alors toute racine de Q est racine de P
  ii) si $P \in \mathbb{R}[X]$ et si $z \in \mathbb{C}$ est racine de P, alors $\bar{z}$ racine de P

- Cor 7 : P de degré n admet au plus n racines distinctes

- Cor 8 : Si P de degré n admet n racines distinctes $a_1, \dots, a_n$ alors $\exists \lambda \in \mathbb{K}^*$ tq : $P = \lambda \prod_{i=1}^{n} (X - a_i)$

- Exemple : $X^n - 1 = \prod_{i=1}^{n} \left(X - e^{\frac{2i\pi}{n}}\right)$

- Rem : Si $\deg P \leq n$ et P possède au moins $n+1$ racines alors P est nul.

2) Racines multiples :

- Déf 9 : Si a racine de P, on dit que a est racine d'ordre $\alpha \in \mathbb{N}^*$

...inpé. Relation coefficient – racines. Application.

Si $(X-a)^n \mid P$ et si $(X-a)^{n+1}$ ne divise pas P

- Exemple: $P=(X-1)(X+2)^2$ a 1 comme racine simple et 2 comme racine double.

- Théo 10:
  1) a racine d'ordre $\geq$ de P si $P^{(k)}(a)=0 \ \forall k \in [\![0; n-1]\!]$ et $P^{(n)}(a) \neq 0$.
  2) Si $a_1, \dots, a_r$ racines distinctes de P d'ordres de multiplicité respectifs $n_1, \dots, n_r$ alors: $\prod_{k=1}^{r}(X-a_k)^{n_k} \mid P$

III. Relation entre les coefficients et les racines:

- Déf 11: P de degré $n \in \mathbb{N}^*$ alors scindé sur $\mathbb{K}$ s'il peut s'écrire $P=\lambda \prod_{k=1}^{n}(X-a_k)$ où $\lambda \in \mathbb{K}^*$ et $a_k \in \mathbb{K} \ \forall k$
- Exple: $P=(X^2+X+1)$ pas scindé sur $\mathbb{R}$ mais scindé sur $\mathbb{C}$.
- Déf 12: On appelle fonction symétrique élémentaire des racines $a_1, \dots, a_n$ de P scindé de degré n la somme:

$$\sigma_1 = \sum_{i=1}^{n} x_i = x_1 + \dots + x_n$$

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_n}$$

$$\sigma_n = \prod_{i=1}^{n} x_i$$

- Exple: $P=aX^2+bX+c=(X-a_1)(X-a_2)$

$$\sigma_1 = -\frac{b}{a} \qquad \sigma_2 = \frac{c}{a}$$

- Théo 13: $\forall P = \sum_{k=0}^{n} a_{n-k} X^{n-k} \in \mathbb{K}[X]$ scindé on a: $P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \dots + (-1)^n \sigma_n\right)$

IV. Application:

1) Calcul de fcts symétriques:

Si x_1, x_2, x_3 racines de $P=X^3+pX+q$ exprimer $S_2 = x_1^2 + x_2^2 + x_3^2$ et $S_3 = x_1^3 + x_2^3 + x_3^3$ en fonction de p et q.

2) Résolution d'un système d'équations algébriques symétriques:

Résoudre dans $\mathbb{C}^3$: $\begin{cases} x+y+z=11 \\ x^2+y^2+z^2=45 \\ x^{-1}+y^{-1}+z^{-1}=1 \end{cases}$

3) Algo. de Horner (?)

* Prérequis: Ring de polynômes, Polynôme dérivé

* Livre: 66 leçons / Berg

* Compléments leçon 109 :

- Formule de Taylor :

$\forall$ polynôme $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$ et $\forall a \in \mathbb{K}$ on a :

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

ou $P(a+X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k$

Preuve à partir de $P = \sum_{k=0}^{n} \lambda_k (X-a)^k$ car $\left((X-a)^k\right)_{0 \le k \le n}$ base de $\mathbb{K}^n[X]$
en dérivant et en utilisant $(X^n)^{(p)} = \frac{n!}{(n-p)!} X^{n-p}$

- Formule de Leibnitz : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$

Preuve par récurrence

- Caractérisation de l'ordre des racines :

- Théo : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $n \in \mathbb{N}^*$
Si a racine d'ordre n de P alors a racine d'ordre $n-1$ de P'.

- Preuve : On a : $P = (X-a)^n Q$ avec $Q(a) \neq 0$

d'où $P' = (X-a)^n Q' + n(X-a)^{n-1} Q$

$= (X-a)^{n-1}\underbrace{[(X-a)Q' + nQ]}_{R}$

et $R(a) = nQ(a) \neq 0$ donc a racine d'ordre $n-1$ de P'

- Théo : Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $n \in \mathbb{N}^*$. On a équivalence entre :
(i) a racine d'ordre n de P
(ii) $\forall k \in [\![0, n-1]\!]$ a racine de $P^{(k)}$ et a non racine de $P^{(n)}$

- Preuve : $*(i) \Rightarrow (ii)$: par le théorème précédent

$*(ii) \Rightarrow (i)$: Comme $P^{(n)}(a) \neq 0$ par hypothèse, on a : $n \geq n$
donc la formule de Taylor de P donne : $P = \sum_{k=n}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$

$= (X-a)^n \underbrace{\sum_{k=n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-n}}_{Q}$

et $Q(a) = \frac{P^{(n)}(a)}{n!} \neq 0$ donc a racine d'ordre n

* Calcul d'une fonction symétrique:

Soient x_1, x_2 et x_3 les racines d'un polynôme

$$P = X^3 + 2X^2 + pX + q$$

- Exprimer $S_2 = x_1^2 + x_2^2 + x_3^2$ et $S_3 = x_1^3 + x_2^3 + x_3^3$ en fonction de p et q:

* On a: $S_2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$

$$= \sigma_1^2 - 2\sigma_2$$

On : $P = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_1$

donc ici $\sigma_1 = -2$, $\sigma_2 = p$

d'où $S_2 = -2 - 2p$.

* On a: $S_3 = (x_1 + x_2 + x_3)^3 - 3\sigma_1\sigma_2$

car $(x_1 + x_2 + x_3)^3 = x_1^3 + 3x_1^2(x_2 + x_3) + 3x_1(x_2 + x_3)^2 + (x_2 + x_3)^3$

$$= x_1^3 + 3x_1^2x_2 + 3x_1^2x_3 + 3x_1(x_2^2 + 2x_2x_3 + x_3^2) + (x_2^3 + 3x_2^2x_3 + 3x_2x_3^2 + x_3^3)$$

$$= x_1^3 + x_2^3 + x_3^3 + 3x_1^2x_2 + 3x_1^2x_3 + 3x_1x_2^2 + 6x_1x_2x_3 + 3x_1x_3^2 + 3x_2^2x_3 + 3x_2x_3^2$$

$$= x_1^3 + x_2^3 + x_3^3 + 3\big(x_1(x_1x_2 + x_1x_3 + x_2x_3) + x_2(x_1x_2 + x_2x_3 + x_1x_3) + x_3(x_1x_3 + x_2x_3 + x_1x_2)\big)$$

$$= x_1^3 + x_2^3 + x_3^3 + 3\big((x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3)\big)$$

$$= x_1^3 + x_2^3 + x_3^3 + 3\sigma_1\sigma_2$$

d'où $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2$

$$= (-2)^3 - 3 \times (-2)p$$

$$= -8 + 6p$$

* Résolution d'un système d'équations algébriques

- Résoudre le système suivant d'inconnues $x,y,z \in \mathbb{C}$.

$$\begin{cases} x+y+z=11 \\ x^2+y^2+z^2=49 \\ x^{-1}+y^{-1}+z^{-1}=1 \end{cases}$$

* Soient $(x,y,z) \in \mathbb{C}^3$ une solution du système.
et considérons le polynôme

$$P=(X-x)(X-y)(X-z)=X^3-\underbrace{(x+y+z)}_{11}X^2+(xy+yz+xz)X-xyz$$

on a alors: $xy+yz+xz=\frac{1}{2}\left((x+y+z)^2-(x^2+y^2+z^2)\right)$

$$=\frac{1}{2}\left(11^2-49\right)=\frac{1}{2}(121-49)$$

$$=\frac{1}{2}\times 72=36$$

et on a: $1=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$ par hypothèse

$$=\frac{yz+xz+xy}{xyz}=\frac{36}{xyz} \text{ d'où } xyz=36$$

d'où $P=X^3-11X^2+36X-36$

2 est une racine évidente de P et on a par division euclidienne

$$X^3-11X^2+36X-36=(X-2)(X^2-9X+18)$$

$$=(X-2)(X-3)(X-6)$$

d'où $(x;y;z)=(2;3;6)$ ou $(x;y;z)$ est l'un de ceux obtenus par permutation de $(2;3;6)$

* on vérifie que ces triplets sont solutions du système.

* Algorithme de Horner:

Soit $P=a_nX^n+a_{n-1}X^{n-1}+\dots+a_0$

alors $\forall x_0$ on a: $P(x_0)=a_nx_0^n+a_{n-1}x_0^{n-1}+\dots+a_0$

où: $P(x_0)=\left(\left(\dots\left(a_nx_0+a_{n-1}\right)x_0+a_{n-2}\right)x_0+\dots\right)x_0+a_1\Big)x_0+a_0$

- Exemple :

Coefficient de $P = 4X^3 - 7X^2 + 3X - 5$	$a_n = 4$	$a_{n-1} = -7$	$a_{n-2} = 3$
Facteur $x_0 = 2$	$a_n = 4$	$a_n x_0 + a_{n-1}$ $= 4 \times 2 - 7$ $= 1$	$(a_n x_0 + a_{n-1}) x_0 + a_{n-2}$ $= 1 \times 2 + 3$ $= 5$

$a_0 = -5$
$5 \times 2 - 5$ $= 5$

d'où $P(2) = 5$ à chaque étape, on calcule $a_{n-k} \times x_0$ et on ajoute a_{n-k-1}

On obtient aussi le quotient de P par $(X - x_0)$:

on a : $P = (X - x_0) Q + P(x_0)$:

avec $Q = q_{n-1} X^{n-1} + \dots + q_1 X + q_0$

d'où $a_n X^n + \dots + a_1 X + a_0 = (X - x_0)(q_{n-1} X^{n-1} + \dots + q_1 X + q_0) + P(x_0)$

$= q_{n-1} X^n + X^{n-1}(q_{n-2} - x_0 q_{n-1}) + \dots$

donc $q_{n-1} = a_n$ et $a_k = q_{k-1} - x_0 q_k \quad \forall\ 0 < k < n$

i.e. $q_{k-1} = a_k + x_0 q_k$

donc les valeurs de la suite $(q_n)_n$ sont exactement celles calculées pour évaluer $P(x_0)$

Si on reprend l'exemple précédent on obtient :

$$P(X) = (X - 2)(4X^2 + 1X + 5) + 5$$

Leçon 110 : Dimension d'un espace vectoriel admettant une famille
Développement (15) Base incomplète, base et lemme de Steinitz

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
$(E, +, \cdot)$: $\mathbb{K}$-e.v.

I. Famille de vecteurs

- Déf 1 : Une famille $(e_i)_{i \in I}$ de vecteurs de E est
  - * génératrice si $\forall u \in E$, $\exists (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$ / $u = \sum_{i \in I} \lambda_i e_i$
  - * libre si : $\forall (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$, $\sum_{i \in I} \lambda_i e_i = 0 \Rightarrow \lambda_i = 0 \ \forall i \in I$
  - * une base si elle est génératrice et libre.

- Rem : une famille qui n'est pas libre est dite liée.
- Exemple : $(1, i)$ base de $\mathbb{R}$-e.v. $\mathbb{C}$.
  $(1, X, X^2)$ base de $\mathbb{K}^2[X]$.

- Théo 2 : Si $\mathcal{B} = (e_i)_{i \in I}$ est une base de E, alors : $\forall u \in E$, $\exists ! (\lambda_i)_{i \in I} \in \mathbb{K}^{(I)}$ tq : $u = \sum_{i \in I} \lambda_i e_i$

La famille $(\lambda_i)_{i \in I}$ est appelée famille des coordonnées de u dans la base $\mathcal{B}$ ORAL

II. Dimension :

- Déf 3 : On dit que E est de dimension finie s'il admet (au moins) une famille génératrice finie.
- Ex : $\mathbb{K}^n$, $\mathbb{C}$ de dim. finie. $\mathbb{K}[X]$ pas de dim. finie.

- Théo 4 : de la base incomplète :
  Soient $\mathcal{G}$ une famille génératrice finie de E et $\mathcal{L}$ une famille libre de E. Alors il existe $\mathcal{G}' \subset \mathcal{G}$ tq $\mathcal{L} \cap \mathcal{G}' = \emptyset$ et $\mathcal{B} = \mathcal{L} \cup \mathcal{G}'$ soit une base de E.

- Cor 5 : Dans tout $\mathbb{K}$-espace vectoriel de dim finie il existe (au moins) une base finie.

- Lemme 6 : (Lemme d'échange de Steinitz)
  Soit $\mathcal{G}$ une partie génératrice finie de E. Soient $x \in \mathcal{G}$ et $y = \sum_{z \in \mathcal{G}} \alpha_z z$:
  Si $\alpha_x \neq 0$, alors $(\mathcal{G} \setminus \{x\}) \cup \{y\}$ est une famille génératrice de E.

- Théo 7 : Soient $\mathcal{G}$ partie génératrice finie et $\mathcal{L}$ famille libre de E.

...une famille génératrice finie. Rang d'une famille de vecteurs.

Steinitz

Alors $\mathcal{L}$ est finie et $\text{Card}(\mathcal{L}) \leq \text{Card}(\mathcal{G})$

- Cor 8 : Dans un e.v. de dimension finie, toutes les bases sont finies et ont le même nombre d'éléments appelé dimension.
- Exemple : $\dim \mathbb{K}^n[X] = n+1$
- Théo 9 : Si E de dimension finie $n \geq 1$. Alors : * toutes les bases de E ont n éléments * toute famille libre a au plus n éléments * toute famille génératrice a au moins n éléments

- Cor 10 : base = fam. libre à n éléments = fam. génératrice à n éléments (ORAL)

III. Liens entre les dimensions

- Théo 11 : Si E est de dimension finie alors tout s.e.v. F de E est de dim. finie et $\dim F \leq \dim E$. Cas = : $F = E$ si $\dim F = \dim E$
- Cor 12 : Tout s.e.v. d'un $\mathbb{K}$-e.v. de dim. finie possède un supplémentaire. (ORAL)
- Prop 13 : Si E et F sont deux $\mathbb{K}$-e.v. de dim finies, alors $E \times F$ est de dim finie et $\dim_{\mathbb{K}}(E \times F) = \dim_{\mathbb{K}} E \times \dim_{\mathbb{K}} F$
- Prop 14 : Formule de Grassmann : Soit E est de dimension finie et E_1, E_2 deux s.e.v. de E. Alors : $\dim_{\mathbb{K}}(E_1 + E_2) = \dim_{\mathbb{K}}(E_1) + \dim_{\mathbb{K}}(E_2) - \dim_{\mathbb{K}}(E_1 \cap E_2)$
- Cor 15 : Si E_1 et E_2 deux s.e.v. supplémentaires de E de dim. finie n, alors : $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} E_1 + \dim_{\mathbb{K}} E_2$

IV. Rang d'une famille de vecteurs

- Déf 16 : Soit F une famille finie d'éléments de E. On appelle rang de la famille F la dimension du s.e.v. engendré par F. On note : $\text{Rg}(F) = \dim_{\mathbb{K}}(\text{Vect}(F))$
- Prop 17 : Si F famille finie d'élts de E, alors : * $\text{Rg}(F)$ est le plus grand cardinal des sous-familles libres de F * F libre ssi $\text{Card}(F) = \text{Rg}(F)$
- Prop 18 : $\text{Rg}(F)$ est inchangé par : (ORAL + Pivot Gauss) - permutation des vecteurs de F - addition à un vecteur d'une combinaison linéaire des autres - multiplication d'un vecteur par un scalaire non nul.

* Prérequis : e.v., supplémentaire, s.e.v. engendré par une partie, famille à rang fini
* Livres : Berg, Cours particulier, 66 leçons, Oral en Poche

Comp 1 to 1

* Compléments leçon 110 : Dimension d'un e.v. admettant une famille génératrice finie. Rang d'une famille de vecteurs.

- Théo 7 : $\mathcal{G}$ génératrice, $\mathcal{L}$ libre dans E, alors $\mathcal{L}$ est finie et $\text{Card}(\mathcal{L}) \leq \text{Card}(\mathcal{G})$

- Preuve : * si $\mathcal{L}$ infinie, alors $\mathcal{L}$ contient une partie finie de cardinal $\text{Card}(\mathcal{G})+1$ (car $\mathcal{G}$ finie) et cette partie n'est pas libre, donc $\mathcal{L}$ n'est pas libre.

Donc $\mathcal{L}$ est finie.

* Raisonnement par récurrence sur $n = \text{Card}(\mathcal{L} \setminus \mathcal{G})$

- si $n=0$: $\mathcal{L} \subset \mathcal{G}$ et $\text{Card}(\mathcal{L}) \leq \text{Card}(\mathcal{G})$
- supposons que pour $n \in \mathbb{N}$ tq $\text{Card}(\mathcal{L} \setminus \mathcal{G}) = n$ on ait $\text{Card}(\mathcal{L}) \leq \text{Card}(\mathcal{G})$

Soit $\mathcal{G}$ partie génératrice finie et $\mathcal{L}$ famille libre de E tq :

$$\text{Card}(\mathcal{L} \setminus \mathcal{G}) = n+1$$

Soit $\mathcal{L}_1 = \mathcal{G} \cap \mathcal{L}$ et $y \in \mathcal{L} \setminus \mathcal{G}$, alors :

$$y = \sum_{z \in \mathcal{G}} \alpha_z z \quad (\text{car } \mathcal{G} \text{ génératrice})$$

et $y \notin \text{Vect}(\mathcal{L}_1)$ (car $\mathcal{L}$ libre)

donc $\exists x \in \mathcal{L} \setminus \mathcal{G}_1$ tq $\alpha_x \neq 0$.

!!! -> Par le lemme d'échange on en déduit que $\mathcal{G}_1 = (\mathcal{G} \setminus \{x\}) \cup \{y\}$ génératrice

et $\text{Card}(\mathcal{L} \setminus \mathcal{G}_1) = n$

d'où par hyp. de récurrence : $\text{Card}(\mathcal{L}) \leq \text{Card}(\mathcal{G}_1)$

$\text{Card}(\mathcal{G})$

- Théo 8 : Si F s.e.v. de E alors $\dim F \leq \dim E$ et $\dim F = \dim E$ ssi $F = E$

- Preuve : * si $\mathcal{L}$ libre dans F, alors $\mathcal{L}$ libre dans E, et $\text{Card}(\mathcal{L}) \leq \dim(E) = n$

* soit p le plus grand nombre d'éléments d'une partie libre de F. Et soit $\mathcal{L}_0$ une telle partie libre (de cardinal p).

Lo étant libre maximale, c'est une base de F,
donc $\dim F = p \leq n$
Si $p = n$, & est alors une base de E et donc $F = E$.

- Prop 13 : $\dim(E \times F) = \dim E \times \dim F$

- Preuve : $(e_i)_{1 \leq i \leq n}$ base de E et $(f_j)_{1 \leq j \leq p}$ base de F.
et on démontre que $\mathcal{B} = \{(e_1;0); (e_2;0); \dots; (e_n;0); (0;f_1); \dots; (0;f_m)\}$
base de $E \times F$
(génératrice + libre)

- Prop 14 : Formule de Grassmann :
Si E_1 et E_2 deux s.e.v. de E de dim. finies, alors :
$$\dim(E_1 + E_2) = \dim(E_1) + \dim(E_2) - \dim(E_1 \cap E_2)$$

- Preuve : Soit $\phi : E_1 \times E_2 \to E_1 + E_2$
$(e_1; e_2) \mapsto e_1 + e_2$
ϕ est une application linéaire surjective
De plus : $(e_1; e_2) \in \ker(\phi)$ ssi $e_1 = -e_2$ et donc $e_1 \in E_1 \cap E_2$
donc $\Psi : E_1 \cap E_2 \to \ker\phi$ est un isomorphisme de $\mathbb{K}$-e.v.
$e_1 \mapsto (e_1; -e_1)$
d'où $\dim(\ker\phi) = \dim(E_1 \cap E_2)$
et par le théorème du rang :
$$\dim(E_1 \times E_2) = \operatorname{rg}(\phi) + \dim(\ker\phi)$$
d'où $\dim E_1 + \dim E_2 = \dim(E_1 + E_2) + \dim(E_1 \cap E_2)$
(Preuve à partir d'application linéaire et du théorème du rang)

ou : partir d'une base C de $E_1 \cap E_2$, la compléter en une base A de E_1
et en une base B de E_2
$A \cup B$ est alors une base de $F + G$, $A \cap B =$ base C de $E_1 \cap E_2$.

- Théorème du rang :

Si $u \in \mathcal{L}(E;F)$ et si V supplémentaire de $\ker(u)$, alors l'application $\tilde{u} : V \to \mathrm{Im}(u)$
$x \mapsto \tilde{u}(x) = u(x)$
est un isomorphisme d'e.v.
Si E est de dimension finie, alors on a le théorème du rang :
$$\dim(E) = \mathrm{rg}(u) + \dim(\ker(u))$$

- Preuve : * $\tilde{u}$ est linéaire et $\ker(\tilde{u}) = \ker(u) \cap V = \{0_E\}$
donc $\tilde{u}$ est injective.
Si $y \in \mathrm{Im}(u)$, alors $y = u(x)$ où $x \in E$ avec :
$x = v + z$ où $v \in V$ et $z \in \ker(u)$
d'où (u étant linéaire) $y = u(x) = u(v) + u(z) = \tilde{u}(v) \in \mathrm{Im}(\tilde{u})$
donc $\tilde{u}$ est surjective
donc $\tilde{u}$ est bijective.

* Soit $n = \dim E$.
V de dim. finie et u isomorphisme $\Rightarrow \dim(V) = \mathrm{rg}(u)$
Comme $E = V \oplus \ker(u)$ alors : $\dim E = \dim V + \dim \ker(u)$
$\dim E = \mathrm{rg}\, u + \dim \ker(u)$

- Corollaire : Soit E un $\mathbb{K}$-e.v. de dim. finie et F un s.e.v. de E.
Alors E/F est de dimension finie et :
$$\dim(E/F) = \dim E - \dim F$$

- Preuve : Soit $\pi : E \to E/F$
π est linéaire surjective, donc $\mathrm{rg}(\pi) = \dim(E/F)$
et on a : $\ker(\pi) = F$, donc par le théorème du rang :
$\dim E = \dim(\ker \pi) + \mathrm{rg}\, \pi$
$= \dim F + \dim(E/F)$

Leçon 112 : Déterminants. Applications.

Développements : *Déterminant de Vandermonde ou de Gram*
Algèbre & géométrie (Burg) + 66 leçons(pour quelques exemples)

I. Applications multilinéaires :

Déf + exemples
Propriétés
Définition alternée et symétrique
Propriété alternée et symétrique
Prop : f(x1,…,xn)=0 si (x1,..,xn) famille liée
Théo : unicité de la forme n linéaire alternée prenant la valeur 1 sur une base + proportionnalité des formes n linéaires alternées

II. Déterminants :

1) De n vecteurs :

Définition + notation
Théo de la relation de Chasles
Propriétés du déterminant
Exemple

2) D'un endomorphisme :

Théo et définition + formule det(u(x1),..,u(xn))=(det u)det(x1,…,xn)
Propriétés (en particulier det (u o v)=det u det v et det(u-1)=1/det u

3) D'une matrice carrée :

Définition + notation
Exemples : déterminant d'une matrice triangulaire supérieure
Exemple : déterminant d'une matrice de permutation
Théo : lien entre det et opérations sur les lignes ou les colonnes de la matrice
Théo : det(x1,…,xn)=det(aij) + det u = det M(u)
Cor : matrices semblables ont des déterminants égaux
Théo : det In= 1 et det M-1=1/det M

4) D'une matrice par bloc :

Proposition

5) Développement d'un déterminant :

Expression du det à partir des cofacteurs
Exemple : matrice de Vandermonde

IV. Applications :

1) Inverse d'une matrice :

Définition comatrice + A-1 = (1/det A)tcomA

2) Résolution d'un système de Cramer :

Définition + exemple

3) Equation de plans affines de R3 :

Exemple

4)Polynôme caractéristique :

Définition + prop sur les racines

5)Produit mixte et produit vectoriel :

Définition + orientation + obtention de base de sens positif

6) Matrice de Gram : Théo rang et déterminant

Leçon 117 : Valeurs propres et vecteurs propres. Recherche de valeurs propres. Application.
Développement : (16) Gerschgorin + Hadamard

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$
$(E, +, \cdot)$ un $\mathbb{K}$-e.v.
u : endomorphisme de E.

I. Éléments propres d'un endomorphisme (*)

- Déf 1 : * Un scalaire $\lambda \in \mathbb{K}$ est une valeur propre de u s'il existe un vecteur $x \neq 0_E$ tq : $u(x) = \lambda x$
  * Un tel x est appelé vecteur propre de u associé à la valeur propre λ.
  * On appelle sous-espace propre associé à la valeur propre λ le sous-espace : $E_\lambda(u) = \ker(u - \lambda Id_E)$
- Déf 2 : Si E de dimension finie, on appelle Spectre de u et on note $Sp(u)$ l'ensemble des valeurs propres de u.
- Rem : λ valeur propre de u ssi $u - \lambda Id_E$ non injectif.
- Exple : si u nilpotent : $Sp(u) = \{0\}$

II. Propriétés des éléments propres

- Prop 3 : Les sous-espaces propres de u sont stables par tout endom. v qui commute avec u.
- Prop 4 : Les sous-espaces propres de u associés à des valeurs propres deux à deux distincts sont en somme directe.
- Prop 5 : Soit $P \in \mathbb{K}[X]$. Si x vecteur propre de u associé à une valeur propre λ, alors x est vecteur propre de $P(u)$ associé à la valeur propre $P(\lambda)$.

III. Recherche de valeurs propres :

1) Lecture matricielle :

ORAL : endo. finie, A mat. diag. ou tri sup ou inf.

2) Polynôme annulateur :

- Prop 6 : Les valeurs propres de u sont racines de tout polynôme annulateur de u. (ORAL : poly. minimal + réciproque aussi)
- Exemple : si $u = 0$, $P = X^2 - X$ annulateur de u.

3) Polynôme caractéristique :

- Prop 7 : Si E de dimension finie, alors les valeurs propres de u sont les racines du polynôme $\chi_u(X) = \det(u - X I_n)$ appelé polynôme caractéristique de u.
- Exemple : $Sp(A)$ où $A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$
- Cor 8 : Si E de dimension n

(*) Notion valable pour les matrices carrées en dimension finie.

alors il y a au plus n valeurs propres distincts.
- Si $\mathbb{K}=\mathbb{C}$, il y a au moins une valeur propre.

4) Éléments caractéristiques de u

- Prop 9 : Si $A=\mathrm{Mat}(u)\in\mathcal{M}_n(\mathbb{K})$ et si u admet n valeurs propres $\lambda_1,\dots,\lambda_n$ (distincts ou non), alors : $\det A=\prod_{i=1}^{n}\lambda_i$ et $\mathrm{tr}\,A=\sum_{i=1}^{n}\lambda_i$

5) Localisation des valeurs propres :

Soit $A=(a_{ij})\in\mathcal{M}_n(\mathbb{K})$

- Théo 10 : de Gerschgorin :

On a : $Sp(A)\subset\bigcup_{i=1}^{n}\left\{z\in\mathbb{K} / |z-a_{ii}|\leq\sum_{j\neq i}|a_{ij}|\right\}$

- Théo 11 : de Hadamard

Si $\forall i\in[\![1,n]\!]$, $|a_{ii}|>\sum_{i\neq j}|a_{ij}|$ alors A est inversible.

III. Utilisation :

1) Réduction des endomorphismes :

E de dimension finie n.

- Prop 12 : u est diagonalisable (trigonalisable) ssi il existe une base $\mathcal{B}$ de E tq $\mathrm{Mat}_{\mathcal{B}}(u)$ diagonale (triangulaire)

- Prop 13 : Si u admet n valeurs propres distincts alors u est diagonalisable.

(**)

- Application : * Calcul de A^k et $\exp(A)$
  * Suite récurrente linéaire à coeff. constant

- Prop 14 : u est trigonalisable ssi χ_u est scindé (toujours vrai sur $\mathbb{C}$)

2) Endomorphisme symétrique :

- Théo 15 : théorème spectral

Si u endomorphisme de E espace euclidien, alors il existe une base orthonormée de E tq la matrice de u est diagonale.

---

* Prérequis : E.V., application linéaire, endomorphisme, endo. symétrique, matrice, polynôme, poly d'endomorphisme.
* Livre : BURG, 66 leçons, 31 leçons

(**) Parler aussi de autres caractérisations

Leçon 118 : Réduction d'un endomorphisme d'un e.v. de di
Développement : (1) Théorème spectral ou (8) Réduction Dun

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$
$(E, +, .)$ est un $\mathbb{K}$-e.v. de dimension finie $n \in \mathbb{N}^*$. Soit $u \in \mathcal{L}(E)$

I. Généralités :

1) Valeurs propres et espaces propres

- **Déf 1 :** • Un vecteur $x \neq 0$ de E est vecteur propre de u s'il existe un scalaire λ de $\mathbb{K}$ tel que $u(x) = \lambda x$.
  • Un scalaire λ est valeur propre de u s'il existe un vecteur $x \neq 0$ tel que $u(x) = \lambda x$.
  • Le sous-espace propre de u associé à la valeur propre λ est le sous-espace $\ker(u - \lambda Id_E)$ noté $E_\lambda(u)$
- **Propriété 2 :** * Les s.e. propres de u sont stables par tout endomorphisme v commutant avec u.
  * Des vecteurs propres associés à des valeurs propres deux à deux distincts forment une famille libre de E
  * Des s.e. propres associés à des valeurs propres deux à deux distincts sont en somme directe.
- **Rem :** En dimension finie, λ est valeur propre ssi $u - \lambda Id_E$ non inversible. On appelle spectre de u l'ensemble des valeurs propres de u : $Sp_{\mathbb{K}}(u)$
- **Rem :** Si $A = Mat_{\mathcal{B}}(u)$ où $\mathcal{B}$ base de E, les valeurs propres et les vecteurs propres de A sont ceux de u.

2) Polynôme caractéristique :

- **Théo 3 :** Soit $P \in \mathbb{K}[X]$. Si x vecteur propre de u associé à λ, alors x vecteur propre de $P(u)$ associé à la valeur propre $P(\lambda)$.
- **Cor 4 :** Les valeurs propres de u sont racines de tout polynôme annulateur de u.
- **Déf 5 :** On appelle polynôme caractéristique de u le polynôme : $\chi_u(X) = \det(u - X Id_E)$
- **Propo :** $\lambda \in Sp_{\mathbb{K}}(u)$ ssi λ racine de χ_u.
- **Rem :** $\chi_u(X)$ de degré n et $\chi_u(X) = X^n - \mathrm{tr}(u) X^{n-1} + \ldots + (-1)^n \det(u)$

II. Diagonalisation :

- **Déf :** u est diagonalisable s'il existe une base de E dans laquelle sa matrice est diagonale.
- **Ex :** homothéties, projecteurs et symétries vectorielles sont diagonalisables.
- **Propo :** Si u admet n valeurs propres deux à deux distinctes, alors u est diagonalisable.

e.v. de dimension finie. Applications.
Réduction Dunford

-Prop 9: Si χ_u est scindé à racines simples, alors u est diagonalisable

-Prop 10: On a équivalence entre
(1) u diagonalisable
(2) u admet un polynôme annulateur scindé à racines simples.
(3) χ_u est scindé et la dimension de chaque s.e. est égale à la multiplicité de la valeur propre dans χ_u
(4) la somme des dimension des s.e. propres est égale à n.

III. Trigonalisation:

-Def 11: u est trigonalisable si il existe une base de E dans laquelle sa matrice est triangulaire.

-Prop 12: Si u nilpotent d'indice $p \in \mathbb{N}^*$, alors il existe une base de E dans laquelle $Mat_{\mathcal{B}}(u)$ est triangulaire supérieure stricte.

-Théo 13: u trigonalisable ssi u admet un polynôme annulateur scindé.

-Rem: Si $\mathbb{K} = \mathbb{C}$, alors u est trigonalisable

III. Décomposition de Dunford:

-Théo 14: Si χ_u est scindé, alors il existe un couple (d, v) tq:
- $u = d + v$
- $v \circ d = d \circ v$
- v nilpotent
- d diagonalisable.

IV. Applications:

1) Théorème spectral: ($\mathbb{K} = \mathbb{R}$)

-Théo 15: Si $u \in \mathcal{S}(E)$, il existe une base $\mathcal{B}$ orthonormée de E dans laquelle $Mat_{\mathcal{B}}(u)$ est diagonale, i.e.
$\forall A \in \mathcal{S}_n(\mathbb{R}), \exists (\Omega, D) \in \mathcal{O}_n(\mathbb{R}) \times \mathcal{D}_n(\mathbb{R})$ tel que $S = \Omega D \Omega^{-1}$

2) Puissance de matrices: exemple

3) Suites récurrentes linéaires simultanées du 1° ordre à coefficient constant exemple

4) Système différentiel linéaire du 1° ordre à coefficients constants: exemple

* Livre: BURG & 66 leçons

* Prérequis: e.v., endomorphisme, matrice, endom. nilpotent, symétrique, matrice orthogonale, base de noyaux, polynôme d'endomorphisme, polynôme annulateur, déterminant.

Leçon 119 : Polynômes d'endomorphismes en dimension finie. Applications.
Développement : (20) Lemme des noyaux ou (21) Théorème de Cayley-Hamilton

E : e.v. sur $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

I. Définitions et propriétés :

- Déf 1 : Soient $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$. On note $P(u)$ l'endomorphisme $\sum_{k=0}^{p} a_k u^k$ (avec $u^0 = Id_E$; $u^2 = u \circ u$ ...)

- Exemple : Si $P = X^2 + 1$ alors $P(u) = u^2 + Id_E$

- Théo 2 : L'application $\Psi_u : \mathbb{K}[X] \to \mathcal{L}(E)$, $P \mapsto P(u)$ est un morphisme de $\mathbb{K}$-algèbre

- Rem : Si $A \in \mathcal{M}_n(\mathbb{K})$ et $P \in \mathbb{K}[X]$ on définit de même $P(A)$

- Exemple : Si $P = X^3 - 1$ alors $P(A) = A^3 + I_n$

- Rem : Si dans une base de E on a : $M = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ alors $P(M) = \mathrm{diag}(P(\lambda_1), \dots, P(\lambda_n))$

- Prop 3 : Si $P \in \mathbb{K}[X]$, $Q \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$, alors $P(u)$ et $Q(u)$ commutent et $\mathrm{Ker}(P(u))$ et $\mathrm{Im}(P(u))$ sont stables par u.

- Rem : * Si $v \in \mathcal{L}(E)$ commutent alors v commute avec $P(u)$ pour tout $P \in \mathbb{K}[X]$.

* $P({}^t A) = {}^t P(A)$; $\overline{P(A)} = P(\bar{A})$

- Déf 4 : On appelle polynôme annulateur d'un endomorphisme u tout polynôme P non nul tel que : $P(u) = 0$

- Prop 5 : Si E est de dimension finie, il existe au moins un polynôme annulateur de u

- Rem : Faux en dimension infinie. (ORAL : endom. de dérivation)

- Exemple : $P = X^2 - X$ est un polynôme annulateur d'un projecteur

II. Polynôme minimal :

Soit $u \in \mathcal{L}(E)$ et $\Psi_u : \mathbb{K}[X] \to \mathcal{L}(E)$, $P \mapsto P(u)$

- Théo 6 : Si $\mathrm{Ker}(\Psi_u) \neq 0$, alors il existe un unique polynôme unitaire M_u appelé polynôme minimal de u tel que $\mathrm{Ker}(\Psi_u) = (M_u)$

- Rem : On a : $\forall P \in \mathbb{K}[X]$, $M_u \mid P$ ssi $P(u) = 0$

- Théo 10 : $\mathrm{Ker}(\Psi_u) \neq 0$ ssi $\mathrm{Im}(\Psi_u)$ est de dimension finie. Dans ce cas la famille $(u^0, u^1, \dots, u^{n-1})$ est une base de $\mathrm{Im}(\Psi_u)$

où

- Rem :

- Exemple

- Lemme

- Corollaire

...Application... de Cayley-Hamilton

où $n = \deg(\Pi_u)$

- Rem: χ_A et ${}^tA$ ont le même polynôme minimal si $A \in \mathcal{M}_n(\mathbb{K})$
  * Si Π_A polynôme minimal de A alors Π_A polynôme minimal de $\bar{A}$

- Exemple: $X^2 - 1$ est le polynôme minimal d'une symétrie de E différente de $\pm Id_E$
  * Le polynôme minimal de la matrice compagnon C_P de $P = X^n - a_{n-1}X^{n-1} - \dots - a_0$ est P: (avec $C_P = \begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & & a_1 \\ 0 & \ddots & 0 & \vdots \\ \vdots & & 1 & a_{n-1} \end{pmatrix}$)

III. Lemme des noyaux:

- Lemme 11: Soit $u \in \mathcal{L}(E)$ et $P_1, \dots, P_n \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$, des polynômes 2a2 premiers entre eux 2a2. Alors on a:
$$\operatorname{Ker} \prod_{k=1}^{n} P_k(u) = \bigoplus_{k=1}^{n} \operatorname{Ker}(P_k(u))$$

- Corollaire 12: Si $P = \prod_{k=1}^{n} P_k$ annulateur de u alors:
$$E = \bigoplus_{k=1}^{n} \operatorname{Ker}(P_k(u))$$

- Exemple: Si $p \in \mathcal{L}(E)$ tel que $p^2 = p$ alors: $E = \operatorname{Ker}(p - Id_E) \oplus \operatorname{Ker} p$.

IV. Applications:

1) Puissances d'une matrice:

- Ex: Soit $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{pmatrix}$.
Déterminer A^k pour $k \in \mathbb{N}^*, k \geq 3$

2) Théorème de Cayley-Hamilton:

- Théorème: Si $u \in \mathcal{L}(E)$ et E de dimension finie, alors le polynôme caractéristique de u est annulateur de u: $\chi_u(u) = 0$

3) Equation différentielle (?)

---

* Prérequis: théorème incomplet, e.v., endomorphisme, valeur propre, vecteur propre, anneaux, idéaux, matrices, projecteur, polynôme, $\mathbb{K}[X]$, morphisme d'anneaux
* Livres: BURG & 66 leçons

Leçon 120 : Endomorphisme symétrique d'un espace vectoriel
Développement : (17) Réduction d'un endomorphisme symétrique

E : espace euclidien de dim $n \in \mathbb{N}^*$

I. Définition et propriétés :

- Déf 1 : Un endomorphisme $u \in \mathcal{L}(E)$ est symétrique si : $\forall (x,y) \in E^2, (u(x)|y) = (x|u(y))$
- Exple : * endomorphismes nul et identité sont symétriques
  * endomorphisme projection orthogonale et symétrie orthogonale aussi
- Théo 2 : Si $u \in \mathcal{L}(E)$, $\mathcal{B}$ b.o.n. de E et $A = M_{\mathcal{B}}(u)$ on a équivalence entre :
  (i) u symétrique
  (ii) A symétrique : $A = {}^tA$
- Prop 3 : Si $u \in \mathcal{L}(E)$ vérifie : $\forall (x,y) \in E^2, (u(x)|y) = -(x|u(y))$ on dit que u est antisymétrique. Cela revient à ${}^tA = -A$ si $A = \mathrm{Mat}_{\mathcal{B}}(u)$ — ORAL
- Théo 4 : L'ensemble $\mathcal{S}(E)$ des endomorphismes symétriques de E est un s.e.v. de $\mathcal{L}(E)$ de dimension $\frac{n(n+1)}{2}$
  L'ensemble $\mathcal{A}(E)$ des endomorphismes de $\mathcal{L}(E)$ antisymétriques est un s.e.v. de $\mathcal{L}(E)$ de dimension $\frac{n(n-1)}{2}$ — ORAL
- Théo 5 : L'endomorphisme induit sur un sous-espace stable par un endomorphisme u symétrique est aussi symétrique.
- Prop 6 : Si u et v endomorphismes symétriques de E, alors : $f \circ g$ symétrique ssi f et g symétriques

II. Réduction des endomorphismes symétriques.

- Théo 7 : Si $u \in \mathcal{S}(E)$, alors on a : $E = \ker u \oplus \mathrm{Im}\, u$
- Théo 8 : Si F est un sous-espace stable par $u \in \mathcal{S}(E)$, alors $F^\perp$ l'est aussi.
- Théo 9 : Le polynôme caractéristique d'un endomorphisme symétrique de E est scindé sur $\mathbb{R}$.
  Les sous-espaces propres associés à deux valeurs propres distinctes sont orthogonaux
- Théo 10 : Théorème spectral
  Tout endomorphisme symétrique de E est diagonalisable et il existe une base orthonormée de

...vectoriel euclidien de dimension finie. Application ...métrique (avec Théorème Spectral)

Vecteurs propres de u.

- Cor 11 : Traduction matricielle :
Si $A \in S_n(\mathbb{R})$ (ensemble des matrices symétriques réelles), alors :
$\exists P \in O_n(\mathbb{R}), \exists D \in D_n(\mathbb{R})$ tq $A = PDP^{-1} = PD\,{}^tP$

III. Norme d'un endomorphisme symétrique :

On munit l'algèbre $\mathcal{L}(E)$ de la norme subordonnée à la norme euclidienne de E :
$$\|u\| = \sup_{x \neq 0_E} \frac{\|u(x)\|}{\|x\|}$$

- Théo 12 : Si $u \in S(E)$ alors :
$$\|u\| = \sup_{\|x\|=1} |(u(x)|x)| = \underbrace{\max(|\lambda|, \lambda \in Sp(u))}_{r(u) : \text{rayon spectral de } u}$$

IV. Applications :

1) Endomorphismes symétriques positifs :

- Déf 13 : On définit :
1) $S^+(E) = \{u \in S(E) / \forall x \in E, (x|u(x)) \geq 0\}$
ens. des endomorphismes positifs de E

2) $S^{++}(E) = \{u \in S^+(E) / \forall x \in E, (x|u(x)) = 0 \Rightarrow x = 0\}$
ens. des endomorphismes symétriques définis positifs.

- Rem : on note aussi :
$$S_n^+(\mathbb{R}) = \{S \in S_n(\mathbb{R}) / \forall X \in \mathcal{M}_{n,1}(\mathbb{R}), {}^tXSX \geq 0\}$$
$$S_n^{++}(\mathbb{R}) = \{S \in S_n(\mathbb{R}) / \forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \setminus \{0\}, {}^tXSX > 0\}$$

- Théo 14 : Si $u \in S(E)$, on a :
1) $u \in S^+(E)$ ssi $Sp_{\mathbb{R}}(u) \subset \mathbb{R}_+$
2) $u \in S^{++}(E)$ ssi $Sp_{\mathbb{R}}(u) \subset \mathbb{R}_+^*$

2) Inégalité de Hadamard :

- Prop 15 : Si $S = (a_{ij}) \in S_n^{++}(\mathbb{R})$, $\lambda_1, \dots, \lambda_n$ valeurs propres de S et $f :]0; +\infty[\to \mathbb{R}$ une application convexe, alors : $\sum_{i=1}^n f(a_{ii}) \leq \sum_{k=1}^n f(\lambda_k)$

- Théo 16 : Si $S = (a_{ij}) \in S_n^+(\mathbb{R})$ alors :
(Hadamard) $\det S \leq \prod_{i=1}^n a_{ii}$

---

* Prérequis : espace euclidien, endomorphismes orthogonaux, diagonalisables, v.p., matrices, e.v., normes, fctions convexes, polynôme caractéristique
* Livre : BURG + 66 leçons (application)

* Compléments leçon 120 : Endomorphisme symétrique d'un e.v. euclidien de dimension finie. Application

- Matrice antisymétrique : $\forall (x,y) \in E^2$, $(u(x)|y) = -(x|u(y))$ ssi $\forall x \in E$, $(u(x)|x) = 0$

- Preuve : * si $\forall (x,y) \in E^2$, $(u(x)|y) = -(x|u(y))$
alors $\forall x \in E$: $(u(x)|x) = -(x|u(x)) = 0$

* si $\forall x \in E$, $(u(x)|x) = 0$
alors $\forall x,y \in E$: $(u(x+y)|x+y) = 0$
$= (u(x)|x) + (u(x)|y) + (u(y)|x) + (u(y)|y)$
$= 0 + (u(x)|y) + (u(y)|x) + 0$
$= 0$
d'où $(u(x)|y) = -(u(y)|x)$

- Exercice : si $u \in S(E) \cap A(E)$ alors $u = 0$

- Preuve : $\forall x,y \in E$ on a : $(u(x)|y) = (x|u(y)) = (x|-u(y))$
d'où : $2(x|u(y)) = 0$
d'où si $x = u(y)$ alors : $\forall y \in E$, $\|u(y)\|^2 = 0$
d'où $\|u(y)\| = 0$
et $u = 0$

- Proposition : $u \circ v$ symétrique ssi $u \circ v = v \circ u$

- Preuve : * $\forall (x,y) \in E^2$ on a : $(u \circ v(x)|y) = (x|v \circ u(y))$ (car u et v symétriques)
donc si $u \circ v = v \circ u$ alors $u \circ v$ est symétrique

* Si $u \circ v$ est symétrique, alors $\forall (x,y) \in E^2$ on a :
$(u \circ v(x)|y) = (x|u \circ v(y))$
et comme u et v sont symétriques on a :
$(u \circ v(x)|y) = (u(x)|v(y)) = (v \circ u(x)|y)$

d'où $\forall (x,y) \in E^2$ on a : $((u \circ v - v \circ u)(x)|y) = 0$

et donc $u \circ v = v \circ u$.

- Proposition : Soit $u \in S(E)$ tq : $\forall x \in E$, $(x|u(x)) = 0$.
Alors $u = 0$

- Preuve : u est diagonalisable (par le théorème spectral)
donc soit λ une valeur propre de u et x un vecteur propre associé.
On a alors : $(x|u(x)) = (x|\lambda x) = \lambda \|x\|^2 = 0$
Comme $x \neq 0_E$, alors $\lambda = 0$
Donc toutes les valeurs propres de u sont nulles, et $u = 0$.

- Exercice : Soit $A \in S_n(\mathbb{R})$ tq : $\exists k \in \mathbb{N}^* / A^k = I_n$
- Montrer que $A^2 = I_n$:
A est diagonalisable dans une base orthonormée de vecteurs propres, donc :
$\exists P \in O_n(\mathbb{R})$ et $D = Diag(\lambda_1, \dots, \lambda_n) \in D_n(\mathbb{R})$ tq :
$A = PDP^{-1}$
on a donc : $A^k = PD^kP^{-1} = I_n \left(\Rightarrow D^k P^{-1} = P^{-1} I_n = P^{-1} \right.$
$\left. \Rightarrow D^k = P^{-1}P = I_n \right)$
donc : $D^k = I_n$
Mais : $D^k = (\lambda_1^k, \dots, \lambda_n^k)$, donc $\forall i \in [\![1,n]\!]$, $\lambda_i^k = 1$
Comme $\lambda_i \in \mathbb{R}$ $\forall i \in [\![1,n]\!]$, alors $\lambda_i = \pm 1$ $\forall i \in [\![1,n]\!]$
d'où $D^2 = I_n$ et $A^2 = I_n$.

- Théorème : Si $u \in S(E)$ alors : $\|u\| = \sup_{\|x\|=1} |(u(x)|x)| = \underbrace{\max(|\lambda| / \lambda \in Sp(u))}_{r(u)}$

- Preuve : Soit $u \in S(E)$

* Soient $(\lambda_1, \dots, \lambda_p)$ les valeurs propres (distinctes ou non) et $(e_1, \dots, e_n)$ une base orthonormale de vecteurs propres.
On a : $\forall i \in [\![1, n]\!]$, $u(e_i) = \alpha_i e_i$ où α_i valeur propre.
Soit $x = \sum_{i=1}^{n} x_i e_i \in E$, alors :

$$\|u(x)\|^2 = \sum_{i=1}^{n} \alpha_i^2 x_i^2 \leq \max_{1 \leq i \leq n} (\alpha_i)^2 \|x\|^2$$

d'où $$\frac{\|u(x)\|}{\|x\|} \leq \max_{1 \leq i \leq n} |\alpha_i|$$

$$\leq \lambda(u)$$

Soit maintenant i_0 tq $|\lambda_{i_0}| = \lambda(u)$
Alors : $\|u(e_{i_0})\| = |\lambda_{i_0}| \cdot \|e_{i_0}\| = \lambda(u)$
d'où $\lambda(u) = \|u\|$

* Soit $x \in E$ tq $\|x\| = 1$, alors : $|(u(x)|x)| = \left| \sum_{i=1}^{n} \alpha_i x_i^2 \right|$

$$\leq \max_{1 \leq i \leq n} |\alpha_i| \cdot \|x\|^2$$

$$\leq \lambda(u)$$

et si $x = e_{i_0}$, alors : $|(u(e_{i_0}) | e_{i_0})| = |\lambda_{i_0}| \|e_{i_0}\| = \lambda(u)$

Théorème : 1) $s \in S^+(E)$ ssi $Sp_{\mathbb{R}}(s) \subset \mathbb{R}_+$
2) $s \in S^{++}(E)$ ssi $Sp_{\mathbb{R}}(s) \subset \mathbb{R}_+^*$

Preuve 1) * Si $\forall x \in E$, $(u(x)|x) \geq 0$
Soit λ valeur propre de u et x un vecteur propre associé.
On a donc : $(u(x)|x) = (\lambda x | x) = \lambda \|x\|^2 \geq 0$
Comme $x \neq 0_E$, alors $\lambda \geq 0$

* Supposons que les valeurs propres de u soient toutes positives ou nulles.

Comme u est symétrique, $\exists$ une base orthonormée $(e_1,\dots,e_n)$ formée de vecteurs propres de u.
Soit alors : $\forall i \in [\![1,n]\!]$, λ_i valeur propre associée à e_i
alors :
$\forall x \in E \left(x = \sum_{i=1}^{n} x_i e_i\right)$, on a :

$$u(x) = \sum_{i=1}^{n} \lambda_i x_i e_i$$

d'où $$(u(x)|x) = \underbrace{\sum_{i=1}^{n} \lambda_i x_i^2}_{\geq 0}$$ car $\lambda_i \geq 0 \ \forall i \in [\![1,n]\!]$

- Proposition : Soient $n \in \mathbb{N}^*$, $S = (a_{ij})_{1\leq i,j\leq n} \in S_n^{++}(\mathbb{R})$
Soient $\lambda_1,\dots,\lambda_n$ les valeurs propres de S (distinctes ou non)
Soit $f :]0,+\infty[\to \mathbb{R}$ une application convexe
Alors : $$\sum_{i=1}^{n} f(a_{ii}) \leq \sum_{k=1}^{n} f(\lambda_k)$$

- Preuve : $S \in S_n^{++}(\mathbb{R})$, donc par le théorème spectral :
$\exists P \in O_n(\mathbb{R})$ et $D \in \mathcal{D}_n(\mathbb{R})$ tq : $S = PDP^{-1}$
$(D = (\lambda_1,\dots,\lambda_n))$ $(P = (p_{ij})_{1\leq i,j\leq n})$
Alors : $\forall (i,j) \in [\![1,n]\!]^2$ on a :

$$a_{ij} = \sum_{k=1}^{n} p_{ik} \overbrace{\lambda_k p_{jk}}^{\alpha_{ki}}$$
$$= \sum_{k=1}^{n} p_{ik} p_{jk} \lambda_k$$

$$\begin{pmatrix} p_{11} & \cdots & p_{n1} \\ \vdots & & \vdots \\ p_{1n} & \cdots & p_{nn} \end{pmatrix} \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \begin{pmatrix} & j & \\ & \vdots & \\ i & \cdots & \alpha_{ij} \end{pmatrix}$$
$$\alpha_{ij} = \lambda_i p_{ji}$$

d'où $\forall i \in [\![1,n]\!]$ on a :

$$a_{ii} = \sum_{k=1}^{n} \underbrace{p_{ik}^2}_{>0} \lambda_k \quad \text{et} \quad \sum_{k=1}^{n} p_{ik}^2 = 1 \text{ car } P \in O_n(\mathbb{R})$$

Comme $S \in S_n^{++}(\mathbb{R})$, alors $\forall k \in [\![1,n]\!]$, $\lambda_k > 0$

d'où $\forall i \in [\![1;n]\!],\ a_{ii} > 0$

donc : $f(a_{ii}) = f\left(\sum_{k=1}^{n} p_{ik}^2 \lambda_k\right)$

$\leq \sum_{k=1}^{n} p_{ik}^2 f(\lambda_k)$ par l'inégalité de Jensen.

et donc : $\sum_{i=1}^{n} f(a_{ii}) \leq \sum_{i=1}^{n} \sum_{k=1}^{n} p_{ik}^2 f(\lambda_k)$

$\leq \sum_{k=1}^{n} \left(\underbrace{\sum_{i=1}^{n} p_{ik}^2}_{=1}\right) f(\lambda_k)$

$\leq \sum_{k=1}^{n} f(\lambda_k)$

- Théorème : Inegalité de Hadamard :

Soient $n \in \mathbb{N}^*$ et $S = (a_{ij})_{1 \leq i,j \leq n} \in S_n^+(\mathbb{R})$

Alors : $\det(S) \leq \prod_{i=1}^{n} a_{ii}$

- Preuve : * si $S \notin S_n^{++}(\mathbb{R})$, alors $\det(S) = 0$

donc : $0 = \det(S) \leq \prod_{i=1}^{n} a_{ii}$ (car $a_{ii} \geq 0\ \forall i \in [\![1;n]\!]$)

* si $S \in S_n^{++}(\mathbb{R})$:

$\forall i \in [\![1;n]\!],\ a_{ii} > 0$

donc par la proposition précédente appliquée à $f :]0;+\infty[\to \mathbb{R}$ définie par $f(x) = -\ln(x)$ (convexe)

on a : $\sum_{i=1}^{n} (-\ln(a_{ii})) \leq \sum_{k=1}^{n} (-\ln(\lambda_k))$

i.e. $-\ln\left(\prod_{i=1}^{n} a_{ii}\right) \leq -\ln\left(\prod_{k=1}^{n} \lambda_k\right)$

$\leq -\ln(\det(S))$

d'où $\det S \leq \prod_{i=1}^{n} a_{ii}$

Leçon 121: Endomorphismes diagonalisable, Exemple et applic
Développement : (17) Théorème spectral.

E : e.v. sur $\mathbb{K}$ ($=\mathbb{R}$ ou $\mathbb{C}$) de dim. $n \geq 1$
$u, v \in \mathcal{L}(E)$

I. Endomorphisme diagonalisable

(Oral: les notions vues ici s'appliquent aussi aux matrices carrés en considérant les endom. canoniques associés)

- Déf 1: u est diagonalisable s'il existe une base $\mathcal{B}$ de E dans laquelle la matrice de u est diagonale, i.e. s'il existe une base $\mathcal{B}$ de vecteurs propres de u.

(Exemples: les homothéties, projecteurs et symétries vectorielles sont diagonalisables. ORAL?)

- Prop 2: Si u admet n valeurs propres deux à deux distinctes, alors u est diagonalisable.

- Prop 3: Si le polynôme caractéristique χ_u de u est scindé à racines simples, alors u est diagonalisable

- Théo 4: u est diagonalisable si et seulement si u admet un polynôme annulateur scindé à racines simples.

- Théo 5: u est diagonalisable ssi son polynôme caractéristique χ_u est scindé et si pour tout λ espace propre E_λ, $\dim(E_\lambda)$ est égal à l'ordre de multiplicité de λ dans χ_u.

- Théo 6: u est diagonalisable ssi la somme des dimensions des sous-espaces propres est n.

- Théo 7: Si u est diagonalisable, alors il induit sur tout sous-espace stable par u un endomorphisme diagonalisable

- Prop 8: Soit $P \in \mathbb{K}[X]$. Si u est diagonalisable alors $P(u)$ est diagonalisable et toute base de vecteurs propres de u est une base de vecteurs propres de $P(u)$.

- Cas de matrices:
Si A matrice de u diagonalisable, alors si P est la matrice de passage de la base canonique à une base de diagonalisation de u, on a :

- Exe

- Prop
par
ssi

II. C

1) Dé

- Th
dé
alo
par
à

2) T

- Th
a

b

P

... et applications

$D = P^{-1}AP$ où $D \in \mathcal{D}_n(\mathbb{K})$

- Exemple : $J = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$ est diagonalisable
  * $A \in \mathcal{M}_n(\mathbb{K})$ tq $\operatorname{rg}(A) = 1$ diagonalisable ssi $\operatorname{tr}(A) \neq 0$.
  * Si $u \neq 0$ nilpotent alors u non diagonalisable.

- Prop 9 : Si $M \in \mathcal{M}_n(\mathbb{K})$ diagonale par blocs, alors M diagonalisable ssi chaque bloc est diagonalisable

II. Applications :

1) Diagonalisation simultanée :

- Théo 10 : Si u et v sont diagonalisables et commutent, alors il existe une base de E formée de vecteurs propres communs à u et v.

2) Théorème spectral :

- Théo 11 : Si E espace euclidien, alors tout endomorphisme symétrique de E admet une base orthonormale de vecteurs propres de u ;

si $A \in S_n$, alors $\exists P \in O(n)$, $D \in \mathcal{D}_n(\mathbb{R})$ tq $A = PD^tP$

3) Décomposition de Dunford :

- Théo 12 : Si $u \in \mathcal{L}(E)$ admet un polynôme caractéristique scindé, alors il existe $(d, v) \in (\mathcal{L}(E))^2$ tq
  * $u = v + d$
  * $v \circ d = d \circ v$
  * v nilpotent
  * d diagonalisable

4) Calcul de puissance d'une matrice carrée : exemple

~~5) Suite récurrente linéaire scalaire du 1° ordre à coeff. constant : exemple~~

6) Système différentiel linéaire du 1° ordre à coeff. constants : exemple.

---

* prérequis : matrice, ex. endomorphisme, endom. sym. et orthogonaux, valeur propre, vecteur propre, espace propre, polynôme (d'endomorphisme), poly. caractéristique
* BURG/66 le gen/Oral/en poche.

Lemme des noyaux, Cayley-Hamilton

* Compléments leçon 121 : Endomorphismes diagonalisables. Exemples et applications.

- Prop 2 : Si u admet n v.p. 2à2 distincts alors u diagonalisable.

- Preuve (66 leçon) raisonnons par récurrence sur le cardinal N de la famille de vecteurs propres ($N \in [\![1; n-1]\!]$)

* Si $N=1$: un seul vecteur non nul dans la famille, donc famille libre.

* On suppose que $\forall$ famille de vecteurs propres $\{x_1, \dots, x_N\}$ associés respectivement à N valeurs propres 2à2 distinctes $\{\lambda_1, \dots, \lambda_N\}$ est libre.

Soient $\{x_1, \dots, x_{N+1}\}$ une famille de $N+1$ vecteurs propres associés aux v.p. $\{\lambda_1, \dots, \lambda_{N+1}\}$ 2à2 distincts.

Considérons $\{\alpha_1, \dots \alpha_{N+1}\} \in \mathbb{K}^{N+1}$ tq : $\sum_{i=1}^{N+1} \alpha_i x_i = 0_E$ (*)

alors : $f\left(\sum_{i=1}^{N+1} \alpha_i x_i\right) = f(0_E) = 0_E$

d'où $\sum_{i=1}^{N+1} \alpha_i f(x_i) = 0_E$

i.e. $\sum_{i=1}^{N+1} \alpha_i \lambda_i x_i = 0_E$ (**)

de (*) on tire $\sum_{i=1}^{N+1} \lambda_{N+1} \alpha_i x_i = 0_E$

combiné avec (**) on a donc : $\sum_{i=1}^{N+1} (\lambda_{N+1} - \lambda_i) \alpha_i x_i = 0_E$

i.e. $\sum_{i=1}^{N} \underbrace{(\lambda_{N+1} - \lambda_i)}_{\neq 0 \ \forall i \in [\![1;N]\!]} \alpha_i x_i = 0_E$

d'où par l'hypothèse de récurrence, $\forall i \in [\![1;N]\!]$ $\alpha_i = 0$

d'où comme $x_{N+1} \neq 0_E$, $\alpha_{N+1} = 0$

donc $\{x_1, \dots, x_{N+1}\}$ est libre

et la propriété est donc vraie $\forall N \in [\![1; n]\!]$

- Prop 3: Si χ_u scindé simple alors u diagonalisable

- Preuve: (66 façons)
On a $\chi_u = \det(u - X Id_E)$
donc racines de χ_u = valeurs propres de u
donc si χ_u scindé à racines simples, alors u admet n valeurs propres 2à2 distinctes, et est donc diagonalisable.

- Théo 4: u diagonalisable ssi u admet un polynôme annulateur scindé à racines simples.

- Preuve: (66 façons)
  * Si u est diagonalisable:
  $\exists \mathcal{B}$ base de E t.q. $M = M_{\mathcal{B}}(u)$ diagonale
  Soit $(\alpha_k / k \in [\![1;m]\!])$ les elts diagonaux de M 2à2 distincts $(m \in [\![1;n]\!]_m)$ $(M = (m_{ij})_{1 \le i,j \le n})$
  - Montrons que $P(X) = \prod_{k=1}^{m} (X - \alpha_k)$ annule u (ou sa matrice):
  $A = \prod_{k=1}^{m} (M - \alpha_k I_n)$ est produit de matrices diagonales donc A est diagonale.
  et si $A = (a_{ij})_{1 \le i,j \le n}$ on a: $a_{ii} = \prod_{k=1}^{m} (m_{ii} - \alpha_k)$
  et $\forall i \in [\![1;n]\!], \exists k \in [\![1;m]\!]$ t.q. $m_{ii} = \alpha_k$
  donc $A = (0)_{1 \le i,j \le n}$ et $P(M) = 0$

  * si $\exists m \in [\![1;n]\!]$, $\lambda_1, \dots, \lambda_m \in \mathbb{K}$ 2à2 distincts t.q. $P(X) = \prod_{k=1}^{m} (X - \lambda_k)$ annule u:
  les polynômes $(X - \lambda_k)$, $k \in [\![1;m]\!]$ sont 2à2 premiers entre eux
  Donc, par le lemme des noyaux, on a:
  $E = \bigoplus_{k=1}^{m} \ker(u - \lambda Id)$

donc E est somme directe de sous-espaces propres de u
et u est donc diagonalisable.

- Théo 5 : u diagonalisable ssi χ_u scindé et $\dim(E_\lambda) = m_\lambda$

- Preuve : (66 leçon)

on a : $\chi_u = \det(u - X\mathrm{Id}_E)$

Soient $\{\lambda_k\}_{1 \le k \le m}$ les racines de χ_u où $m \in [\![1; n]\!]$

alors $\chi_u = \prod_{k=1}^{m} (X - \lambda_k)^{m_{\lambda_k}}$ où m_{λ_k} ordre de multiplicité

Par le lemme des noyaux et le théorème de Cayley-Hamilton

on a : $E = \bigoplus_{k=1}^{m} \mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)^{m_{\lambda_k}}$

et on a aussi : $\forall k \in [\![1; m]\!], \mathrm{Ker}(u - \lambda_k \mathrm{Id}_E) \subset \mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)^{m_{\lambda_k}}$

donc $E = \bigoplus_{k=1}^{m} \mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)$ ssi $\forall k \in [\![1; m]\!]$:

$$\mathrm{Ker}(u - \lambda_k \mathrm{Id}_E) = \mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)^{m_{\lambda_k}}$$

i.e. ssi ont même dimension

- Théo 6 : u diagonalisable ssi $\sum \dim E_\lambda = n$

- Preuve : (66 leçon) on a : $\sum_{k=1}^{m} \dim_{\mathbb{K}} \left(\mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)\right) \le \underbrace{\sum_{k=1}^{m} \dim_{\mathbb{K}} \left(\mathrm{Ker}(u - \lambda_k \mathrm{Id}_E)^{m_{\lambda_k}}\right)}_{n}$

donc égalité possible ssi $\sum \dim E_\lambda = n$

- Théo 7 : endom. induit sur sous-espace stable de diagonalisable

- Preuve : (BURG) Soit F s.e.v. de E et P un polynôme annulateur de u scindé à racines simples (existe car u diagonalisable)
Soit u_F l'endom. induit par u sur F

F est stable par u donc F stable aussi par $P(u)$

Ainsi : $P(u_F) = P(u)_F = 0$

donc u_F annule un polynôme à racines simples scindé

donc u_F est diagonalisable.

- **Prop 7 :** $P(u)$ diagonalisable

- **Preuve (BURG) :** Si $(e_1, \dots, e_m)$ base de vecteurs propres de u associés à $(\lambda_1, \dots, \lambda_m)$ valeurs propres de u, on a :

$$\forall i \in [\![1, n]\!] : (P(u))(e_i) = P(\lambda)(e_i)$$

(car $P(u)(e_i) = P(u(e_i)) = P(\lambda e_i)$)

donc $P(u)$ diagonalisable.

- **Prop 9 :** Si $M = \text{diag}(M_1, \dots, M_p)$ diagonale par blocs, alors :

M diagonalisable ssi $\forall i \in [\![1, p]\!]$, M_i diagonalisable.

- **Preuve (BURG) :** ✱ Si M est diagonalisable, les s.e. stables sont diagonalisables (Thm 7), donc M_i diagonalisable $\forall i \in [\![1, p]\!]$.

✱ Si $\forall i \in [\![1, p]\!]$, M_i est diagonalisable :

alors $M_i = P_i D_i P_i^{-1}$ où D_i diagonale et P_i inversible.

Soit $P = \text{diag}(P_1, \dots, P_p)$ diagonale par blocs

alors P est inversible d'inverse $P^{-1} = \text{diag}(P_1^{-1}, \dots, P_p^{-1})$

et : $P^{-1} M P = \text{diag}(P_1^{-1} M_1 P_1, \dots P_p^{-1} M_p P_p)$

$= \text{diag}(D_1, \dots, D_p)$

d'où M est diagonalisable.

Leçon 124 : Barycentres. Applications.

Développements : *Jensen*

Algèbre et géométrie (Burg) pour le début / 66 leçons en plus pour applications

I. Barycentre de points pondérés :

Définition du barycentre

Remarque : ordre pas important, homogénéité, si la somme est nulle vecteur constant

Remarque : isobarycentre

Exemple : milieu d'un segment, isobarycentre d'un triangle est sur chaque médiane, isobarycentre d'un parallélogramme est le point d'intersection des diagonales

Théo : barycentres et droites

Théo : barycentres et plans

Prop : une translation conserve les barycentres

II. Propriétés des barycentres :

1) Associativité :

Prop + exemple (tétraèdre)

2) Convexité :

Définition de la convexité + paramétrage segment

Théo enveloppe convexe et définition

Théo : Toute partie convexe est stable par passage au barycentre (coef positifs)

3) Stabilité des espaces affines :

Tout se affine est stable par barycentrisation

III. Applications :

1) Fonction scalaire de Leibnitz :

Théo

2) théorème de Gauss Lucas :

Théo

3) Inégalité de Jensen :

Définition fonction convexe + inégalité de Jensen

Leçon 125 : Applications affines en dimension finie. Propriétés et exemples.

Développements : *Rotation expression matricielle (exemple)*
66 leçons en plus pour applications + Algèbre et géo (Burg) pour la partie III

I. Généralités :

Définition application affine
Prop : affine ssi conservation barycentre
Théo divers
Déf GA(E) + image d'un sea par une application affine est un sea affine

II. Homothéties, translations et rotations :

1) Translations :

Définition + prop

2) Homothéties :

Définition + prop

3) Groupe des homothéties translations :

Déf théorème
Thé : description des homothéties translations

4) Rotations :

Définition rotation
Exemple : détermination d'une rotation par son expression matricielle

III. Projecteurs et symétries :

Déf projecteur + propositions sur les projecteurs
Caractérisation symétrie / droite avec produit scalaire
Caractérisation symétrie / plan avec produit scalaire
+ exemple : détermination d'une symétrie (ou projection) par son expression matricielle

IV. Points fixes d'une application affine :

Théorème

Leçon 126. : Espaces préhilbertiens réels. Orthogonalité, projection orthogonale
Développement : (7) Projection orthogonale

Soit $(E;+;\cdot)$ un $\mathbb{R}$-e.v.

I. Espaces préhilbertiens réels :

- Déf 1 : On appelle produit scalaire sur E toute application :
$\langle \cdot;\cdot \rangle : E\times E \to \mathbb{R}$
étant : 1) symétrique : $\forall (x;y)\in E^2$, $\langle x;y\rangle = \langle y;x\rangle$
2) linéaire à droite : $\forall (x;y;y')\in E^3$ et $\forall (\lambda;\mu)\in \mathbb{R}^2$:
$\langle x;\lambda y+\mu y'\rangle = \lambda\langle x;y\rangle + \mu\langle x;y'\rangle$
3) positive : $\forall x\in E$, $\langle x;x\rangle \geq 0$
4) définie : $\forall x\in E$, $\langle x;x\rangle = 0 \Rightarrow x = 0$

- Exemple :
1) Sur $\ell^2(\mathbb{R})$ e.v. des suites réelles $(u_n)_{n\in\mathbb{N}}$ vérifiant : $\sum_{n=0}^{+\infty} u_n^2 < +\infty$
$\langle (u_n);(v_n)\rangle = \sum_{n=0}^{+\infty} u_n v_n$ est un produit scalaire
2) Sur F e.v des fonctions continues sur $\mathbb{R}$ et 2π-périodiques
$\langle f;g\rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)g(x)dx$ est un produit scalaire

Simplifier à l'oral

- Déf 2 : Un e.v réel muni d'un produit scalaire est appelé espace préhilbertien réel (espace euclidien si E de dimension finie)

II. Propriétés des produit scalaire

E : espace préhilbertien réel.

- Prop 3 : L'application définie sur E à valeurs dans $\mathbb{R}$ définie par :
$x \mapsto \sqrt{\langle x;x\rangle}$ est une norme appelée norme euclidienne.
On note : $\|x\| = \sqrt{\langle x;x\rangle}$

- Prop 4 : Inégalité de Cauchy-Schwarz
$\forall (x;y)\in E^2$ on a : $|\langle x;y\rangle| \leq \|x\|\|y\|$

- Prop 5 : Inégalité de Minkowski
$\forall (x;y)\in E^2$ on a : $\|x+y\| \leq \|x\| + \|y\|$

- Prop 6 : Identité du parallélogramme
$\forall (x;y)\in E^2$ on a :
$\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$
ORAL : caractéristique d'une norme euclidienne.

III. Orthogonalité :

- Déf 7 : 1) Deux vecteurs x et y de E sont orthogonaux si $\langle x;y\rangle = 0$
2) Deux parties A et B de E sont orthogonales si $\forall x\in A, \forall y\in B$ on a $\langle x;y\rangle = 0$
3) une famille de vecteurs de E est orthogonale si ses vecteurs sont orthogonaux 2 à 2
4) une famille de vecteurs de E est orthonormale si elle est orthogonale et si ses vecteurs sont de norme 1.

... orthogonale sur un sous-espace de dim. finie Application.

- Déf 8 : Si A partie non vide de E, on appelle orthogonal de A la partie de E : $A^{\perp} = \{x \in E / \forall a \in A, \langle a; x \rangle = 0\}$
- Prop 9 : Si A non vide, $A^{\perp}$ est un s.e.v. de E
- Rem : Si $E = A \oplus A^{\perp}$, $A^{\perp}$ est un supplém. orthogonal de A
- Prop 10 : $\forall$ s.e.v. F d'un espace préhilbertien on a $F \subset F^{\perp\perp}$. Si $E = F \oplus F^{\perp}$ alors $F = F^{\perp\perp}$
- Théo 11 : Pythagore : Deux vecteurs x et y de E sont orthogonaux ssi $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.
- Prop 12 : Une famille orthogonale de vecteurs non nuls de E est libre
- Exemple : Sur l'espace F, la famille $\left(\frac{1}{\sqrt{2}}; \cos(nt); \sin(pt) / n, p \in \mathbb{N}^*\right)$ est orthonormée. à voir

IV Procédé d'orthonormalisation de Gram-Schmidt :

- Théo 13 : Si $(x_n)_{n \in [\![0;p]\!]}$ famille libre de E, alors $\exists$ une famille orthonormée $(e_n)_{n \in [\![0;p]\!]}$ tq $\forall m \in [\![0;p]\!]$ $\begin{cases} \text{Vect}(e_0; \dots; e_m) = \text{Vect}(x_0; \dots; x_m) \\ \langle e_m; x_m \rangle > 0 \end{cases}$
- Cor 14 : Si F s.e.v. de E de dim. finie (ou infinie dénombrable), alors $\exists$ une base orthonormée de F.

- Exemple : $(a_0; \dots; a_n) \in \mathbb{R}^{n+1}$, $E = \mathbb{R}_n[X]$, $\varphi : E \times E \to \mathbb{R} : (P; Q) \mapsto \sum_{k=0}^{n} P^{(k)}(a_k) Q^{(k)}(a_k)$
  - a) Mq φ est un produit scalaire
  - b) Si $n = 2$, $a_0 = -1$ et $a_1 = 0$ et $a_2 = 1$ trouver une base orthonormée pour φ.

V. Projection orthogonale :

- Prop 15 : Si F s.e.v. de E de dim finie et si $x \in E$, il existe un unique vecteur de F, noté $p_F(x)$, tq $x - p_F(x) \in F^{\perp}$ (projeté orthogonal de x sur F).
  On a : $d(x; F) = \inf_{y \in F}(x; y) = \min_{y \in F}(x; y) = \|x - p_F(x)\|$
  On a, $\forall x \in E$: $d^2(x; F) = \|x\|^2 - \|p_F(x)\|^2$
  Et si F n'est pas de dim finie, on peut avoir $E \neq F \oplus F^{\perp}$
- Rem : Si $(e_i)_{1 \leq i \leq n}$ b.o.n de F alors $x = \sum_{i=1}^{n} \langle x; e_i \rangle e_i$
- Exemple : Déterminer $d(X^3; \mathbb{R}_2[X])$
- Prop 16 : $\forall$ famille orthonormale $(e_i)_{1 \leq i \leq n}$ et $\forall x \in E$ on a : $\sum_{i=1}^{n} (e_i | x)^2 \leq \|x\|^2$
- Théo 17 : Si $(e_i)_{1 \leq i \leq n}$ famille orthonormée de E alors $\forall x \in E$ on a : $\sum_{i=0}^{+\infty} \langle e_i; x \rangle^2 = \|x\|^2$ ssi $x \in \overline{\text{Vect}((e_i))}$

Parseval ! → Bessel !

* Prérequis : normes, distances, suites, intégration, e.v.

* Livres : 66 leçons Dantzer | Méthodes MP Courpanticien

* Compléments leçon 126 : Espaces préhilbertiens réels...

- Exemple 1 : $\left(\frac{1}{\sqrt{2}}; \cos(nt), \sin(pt)\right)$ est orthonormée

$$\left\langle \frac{1}{\sqrt{2}}; \cos(nt) \right\rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1}{\sqrt{2}} \cos(nt)\,dt$$
$$= \frac{1}{\sqrt{2}\pi}\int_{-\pi}^{\pi} \cos(nt)\,dt$$
$$= \frac{1}{\sqrt{2}\pi}\left[\frac{\sin(nt)}{n}\right]_{-\pi}^{\pi}$$
$$= \frac{1}{\sqrt{2}\pi n}\left[\sin(n\pi) + \sin(-n\pi)\right]$$
$$= 0$$

$$\left\langle \frac{1}{\sqrt{2}}; \frac{1}{\sqrt{2}} \right\rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\,dt = \frac{1}{\sqrt{2}^2\pi}\left[\pi - (-\pi)\right] = \frac{2\pi}{2\pi} = 1$$

$$\langle \cos(nt); \cos(nt) \rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \cos(nt)\cos(nt)\,dt$$
$$= \frac{1}{\pi}\int_{-\pi}^{\pi} \cos^2(nt)\,dt$$
$$= \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{\cos(2nt)+1}{2}\,dt$$
$$= \frac{1}{2\pi}\left[\frac{1}{2}\sin(2nt) + t\right]_{-\pi}^{\pi}$$
$$= \frac{1}{2\pi}\left(\pi + \pi\right) = 1$$

$\cos(a+a) = \cos^2 a - \sin^2 a$
$= \cos^2 a + \cos^2 - 1$
$\Rightarrow \cos^2 a = \frac{\cos(2a)+1}{2}$

$$\langle \cos(nt); \sin(pt) \rangle = \frac{1}{\pi}\int_{-\pi}^{\pi} \cos(nt)\sin(pt)\,dt$$
$$= \frac{1}{\pi}\int_{-\pi}^{\pi} \frac{1}{2}\left(\sin(nt+pt) - \sin(nt-pt)\right)dt$$
$$= \frac{1}{2\pi}\left[\cos(nt+pt) - \cos(nt-pt)\right]_{-\pi}^{\pi}$$
$$= \frac{1}{2\pi}\left[\cos(n+p)t\,dt - \cos(n-p)t\right]_{-\pi}^{\pi}$$
$$= 0$$

$\cos(a)\cos(b) = \frac{1}{2}(\cos(a-b) + \cos(a+b))$

$\cos(a)\sin(b) = \frac{1}{2}(\sin(a+b) - \sin(b-a))$

$\sin(pt)\cos(nt) + \cos(pt)\sin(nt)$
$- \sin(pt)\cos(nt) + \cos(pt)\sin(nt)$

etc.

- Exemple 2 :

Soit $(a_0, \dots, a_m) \in \mathbb{R}^{m+1}$

$E = \mathbb{R}_m[X]$

$\varphi : E \times E \to \mathbb{R}$, $(P, Q) \mapsto \sum_{k=0}^{m} P^{(k)}(a_k) Q^{(k)}(a_k)$

a) Mq φ produit scalaire :

- φ est symétrique et bilinéaire à droite
- $\forall P \in E$, $\varphi(P, P) = \sum_{k=0}^{m} \underbrace{\left(P^{(k)}(a_k)\right)^2}_{\geq 0} \geq 0$
- Si P tel que $\varphi(P, P) = 0$, alors $\forall k \in [\![0, m]\!]$, $P^{(k)}(a_k) = 0$

  On a $P^{(m)}(a_m) = 0$ et $\deg(P) \leq m$, donc $\deg(P^{(m)}) \leq 0$

  donc $P^{(m)} = 0$, donc $\deg(P^{(m-1)}) \leq 0$

  on a : etc.

  on en déduit $P = 0$

donc φ est bien un produit scalaire sur E.

b) Si $m = 2$, $a_0 = -1$, $a_1 = 0$ et $a_2 = 1$, trouver une base orthonormée par φ :

On applique le procédé de Gram-Schmidt à la base canonique $(1, X, X^2)$

- $P_0 = 1$ et $U_0 = \frac{P_0}{\|P_0\|}$

  On a : $\|P_0\|^2 = \sum_{k=1}^{3} P_0(a_k)^2 = \sum_{k=1}^{3} 1 = 1$

  donc $\|P_0\| = 1$ et $U_0 = 1$

- Soit $P_1 = aX + b$ où $a, b \in \mathbb{R}$. On a :

  $\varphi(P_0, P_1) = 0$ ssi $P_0(-1)P_1(-1) + P_0'(0)P_1'(0) + P_0''(1)P_1'(1) = 0$

  ssi $1 \times (-a + b) + 0 \times \dots = 0$

  ssi $-a + b = 0$ ssi $a = b$

  d'où $P_1 = a(X + 1)$

  On a : $\|P_1\|^2 = (P_1(-1))^2 + (P_1''(0))^2 + (P_1'(1))^2$

  $= 0^2 + a^2 + 0 = a^2$

  d'où $\|P_1\| = a$ et $U_1 = \frac{P_1}{\|P_1\|} = \frac{(X+1)a}{a} = X + 1$

• Soit $P_2 = aX^2 + bX + c$ avec $a, b, c \in \mathbb{R}$

On a : $\varphi(P_0, P_2) = 0$ ssi $P_0(-1)P_2(-1) + P_0'(0)P_2'(0) + P_0''(1)P_2''(1) = 0$

ssi $1 \times (a - b + c) + 0 \times \ldots = 0$

ssi $a - b + c = 0$

$\varphi(P_1, P_2) = 0$ ssi $P_1(-1)P_2(-1) + P_1'(0)P_2'(0) + P_1''(1)P_2''(1) = 0$

ssi $0 \times \ldots + 1 \times (b) + 0 \times \ldots = 0$

ssi $b = 0$

d'où $\begin{cases} a - b + c = 0 \\ b = 0 \end{cases}$ ssi $\begin{cases} c = -a \\ b = 0 \end{cases}$

d'où $P_2 = a(X^2 - 1)$

On a : $\|P_2\|^2 = (P_2(-1))^2 + (P_2'(0))^2 + (P_2''(1))^2$

$= 0^2 + (0)^2 + (2a)^2 = 4a^2$

on peut prendre $a = \frac{1}{2}$

de $U_2 = \frac{P_2}{\|P_2\|} = \frac{1}{2}(X^2 - 1)$

Une base orthonormale de E pour φ est donc $(-1; X+1; \frac{1}{2}(X^2-1))$

c) Déterminons $d(X^3; \mathbb{R}_2[X])$:

Comme $(1; X+1; \frac{X^2-1}{2})$ est une b.o.n. de $\mathbb{R}_2[X]$ on a :

$$p_{\mathbb{R}_2[X]}(X^3) = \varphi(X^3; 1).1 + \varphi(X^3; X+1).(X+1) + \varphi(X^3; \tfrac{X^2-1}{2}).(\tfrac{X^2-1}{2})$$

avec : $\varphi(X^3; 1) = -1 \times 1 + 0 + 0 = -1$

$\varphi(X^3; X+1) = -1 \times 0 + 0 \times \ldots + 6 \times 0 = 0$

$\varphi(X^3; \frac{X^2-1}{2}) = -1 \times 0 + 0 \times \ldots + 6 \times 1 = 6$

d'où $p_{\mathbb{R}_2[X]}(X^3) = -1 + 6 \times \left(\frac{X^2-1}{2}\right) = 3X^2 - 4 = Q$

et $d(X^3; \mathbb{R}_2[X]) = \|X^3 - 3X^2 - 4\|$

$= \sqrt{Q(-1)^2 + Q'(0)^2 + Q''(1)^2}$

$= \sqrt{64 + 0^2 + (6-6)^2}$

$= \underline{8}$

Leçon 128 : Groupe orthogonal d'un espace vectoriel euclidien de dimension 2, de dimension 3.

Développements : *Décomposition endormorphismes orthogonaux (3)*
66 leçons mixé avec algèbre et géo (Burg)

I. Généralités :

1) Endormorphismes orthogonaux :
Déf endo orthogonal
Prop : conservation de la norme
Prop : conservation base orthonormée
Pro : groupe orthogonal

2) Matrices orthogonales :
Déf matrices orthogonales et On(R)
Prop : Caractérisation d'une matrice orthogonale
Prop : Groupe orthogonal
Prop : déterminant d'une matrice orthogonale
Pop : Les groupes SO(E) et SOn(R)

II. En dimension 2 :

Théo : caractérisation matrices de SO(2) et de o(2) de det -1
Prop : matrice de SO(2) s'écrit R(téta). Groupe SO(2) groupe des matrices de rotat.
Propriétés des rotations
Cor : morphisme surjectif du grp additif R vers SO(2)...
Prop : matrice de det -1 avec cos, sin... Matrice de symétrie
Propriétés des symétries

III. En dimension 3 :

Déf d'une rotation
Théo : classification des endormorphismes orthogonaux en dim 3
Théo : classification (suite)
Rem : une rotation d'axe D peut s'écrire comme produit de 2 réflexions
Les réflexions engendrent o(E)
Etude pratique d'une rotation + exemple
Prop : expression de u(x) à l'aide du produit vectoriel si u(x) image de x par une rotation