

Résumé de cours:

Algèbre Générale

Blague du jour

L'ingénieur, dans l'entreprise n'a pratiquement rien à faire, si ce n'est

- De décider ce qu'il faut faire,
- De désigner quelqu'un pour le faire,
- D'écouter les raisons pour lesquelles la chose ne doit pas être faite,
- Ou doit être faite plus tard,
- Ou autrement,
- Ou par quelqu'un d'autre ;



Mathématicien du jour

Étienne Bézout, (1730-1783), est un mathématicien français, connu par le théorème d'arithmétique qui porte son nom. Il rédige *le Cours complet de mathématiques à l'usage de la marine et de l'artillerie*, qui devient plus tard le livre de chevet des candidats au concours d'entrée à l'École polytechnique.

Bezout

1 Notion d'idéal.

Dans toute cette partie A est un anneau commutatif.

Définition 1

On appelle idéal de A , toute partie $\mathcal{I} \neq \emptyset$ de A , vérifiant la propriété suivante

$$a \in \mathcal{I}, x \in A \implies a.x \in \mathcal{I}.$$

Remarque 1

- L'intersection et somme de deux idéaux de A est un idéal de A .
- Si $f : A \longrightarrow B$ est un morphisme d'anneau, alors $\ker f$ est un idéal de A .

Vocabulaire.

- Soit $a \in A$, alors l'ensemble $aA = \{a.x \text{ tel que } x \in A\}$ est un idéal de A , appelé *idéal engendré par a* .
- Un idéal \mathcal{I} est dit *principal* s'il est de la forme aA .
- Un anneau est dit *principal* si tous ses idéaux sont principaux.

Théorème 1

\mathbb{Z} et $\mathbb{K}[X]$ sont des anneaux principaux.

2 Arithmétique.

2.1 Théorèmes fondamentaux.

Théorème 2 *Caractérisation du pgcd.*

Soit $a, b \in \mathbb{Z}$ et $d \in \mathbb{N}^*$ alors :

$$d = a \wedge b \iff d \text{ divise } a \text{ et } b \\ \text{si } d' \in \mathbb{N}^* \text{ divise } a \text{ et } b \text{ alors } d' \text{ divise } d$$

Théorème 3 *Caractérisation du ppcm.*

Soit $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$ alors :

$$m = a \vee b \iff m \text{ multiple de } a \text{ et } b \\ \text{si } m' \in \mathbb{N}^* \text{ multiple de } a \text{ et } b \text{ alors } m' \text{ multiple de } m$$

Théorème 4 *Théorème de Bezout.*

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

$$a \wedge b = 1 \iff \exists u, v \in \mathbb{Z} \text{ tel que } au + bv = 1.$$

Remarque 2

Les 3 théorèmes précédents sont encore valables dans $\mathbb{K}[X]$.

2.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$.

Définition 2

– Soit $n \in \mathbb{N}^*$. Sur \mathbb{Z} , on définit la relation d'équivalence dite *congruence modulo n* par la relation

$$a \equiv b [n] \iff n \text{ divise } a - b.$$

– Pour tout $a \in \mathbb{Z}$, sa classe d'équivalence est l'ensemble $\dot{a} = a + n\mathbb{Z} = \{x = a + nk \text{ tel que } k \in \mathbb{Z}\}$.

– Cette relation admet exactement n classes d'équivalence $\dot{0}, \dots, \overline{n-1}$.

– L'ensemble formée par ses classes d'équivalence

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dots, \overline{n-1}\}$$

s'appelle *ensemble quotient*.

Théorème 5

Soit $n \in \mathbb{N}^*$. Sur $\mathbb{Z}/n\mathbb{Z}$, on définit les lois de compositions internes suivantes :

$$a \dot{+} b = \dot{a} + \dot{b} \quad , \quad \dot{a} \dot{b} = \dot{a} \cdot \dot{b}$$

Muni de ses LCI, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

Théorème 6

Soit $a, n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes :

- \dot{a} inversible dans $\mathbb{Z}/n\mathbb{Z}$.
- \dot{a} n'est pas un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.
- $a \wedge n = 1$.

Corollaire 1

Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes :

- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps.
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau intègre.
- n est premier.

Notation.

L'ensemble des éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$, se note $U(\mathbb{Z}/n\mathbb{Z})$ ou bien $(\mathbb{Z}/n\mathbb{Z})^*$, c'est un groupe pour la loi .

Définition 3 *Fonction indicatrice d'Euler.* Pour tout $n \in \mathbb{N}^*$, on pose

$$\varphi(n) = \text{card}\{k \text{ tel que } 1 \leq k \leq n \text{ et } k \wedge n = 1\}.$$

L'application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ s'appelle *la fonction indicatrice d'Euler.*

$$n \longmapsto \varphi(n)$$

Remarque 3
Soit $n \in \mathbb{N}^*$, alors $\varphi(n) = \text{card}(\mathbb{Z}/n\mathbb{Z})^*$.

Théorème 7 *Théorème des restes chinois.*
Soit $n, m \in \mathbb{Z}$ tel que $n \wedge m = 1$, soit $u, v \in \mathbb{Z}$ tel que $nu + mv = 1$, soit $a, b \in \mathbb{Z}$. On considère le système suivant d'inconnue $x \in \mathbb{Z}$:

$$S : \begin{cases} x \equiv a [n] \\ x \equiv b [m] \end{cases}$$

On a les résultats suivants :

- $x_0 = bnu + amv$ est une solution particulière de S .
- Toute autre solution de S est congrue à x_0 modulo nm .

Remarque 4
La forme originale du théorème, contenue dans un livre du mathématicien chinois *Qin Jiushao* publié en 1247, mais on trouve trace d'un problème analogue dans le livre de *Sun Zi*, le *Sunzi suanjing* datant du IIIe siècle :

Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

3 Polynôme minimal.

3.1 Généralités.

Introduction.

Soit \mathcal{A} une algèbre unitaire d'unité e , soit $a \in \mathcal{A}$ et $P(X) = \sum_{k=0}^n \alpha_k X^k \in \mathbb{K}[X]$.

- On pose $P(a) = \sum_{k=0}^n \alpha_k X^k \in \mathbb{K}[X]$, où $a^0 = e$.
- Si $P(a) = 0$, on dit que P est un polynôme annulateur de a .
- L'application $\varphi : \mathbb{K}[X] \longrightarrow \mathcal{A}$ est un morphisme d'algèbre.
 $a \longmapsto P(a)$
- On pose $\mathbb{K}[a] = \text{Im } \varphi = \{P(a) \text{ tel que } P \in \mathbb{K}[X]\}$.
- $\ker \varphi = \{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\}$ est un idéal de $\mathbb{K}[X]$ formé pas les polynômes annulateurs de a .

Théorème 8
Soit \mathcal{A} une algèbre unitaire et $a \in \mathcal{A}$, alors $\{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\}$ est un idéal principal de $\mathbb{K}[X]$. Si de plus $\{P \in \mathbb{K}[X] \text{ tel que } P(a) = 0\} \neq \{0\}$, alors il est engendré par un unique polynôme unitaire noté π_a , appelé *polynôme minimal* de a .

Remarque 5

Soit \mathcal{A} une algèbre unitaire et $a \in \mathcal{A}$ qui admet un polynôme annulateur non nul, alors :

- π_a est un polynôme annulateur de a qui divise tous les autres polynômes annulateurs de a .
- π_a est de degré minimal parmi les polynômes annulateurs de a .

Théorème 9

Soit \mathcal{A} une algèbre unitaire et $a \in \mathcal{A}$, alors a admet un polynôme annulateur non nul si et seulement si $\mathbb{K}[a]$ est de dimension finie et non nulle, dans ce cas

$$\dim \mathbb{K}[a] = \deg \pi_a.$$

3.2 Cas d'un endomorphisme.

Principe. Soit E un \mathbb{K} -espace vectoriel on prend $a = u \in \mathcal{L}(E) = \mathcal{A}$, les résultats précédents sont encore valables.

Définition 4

Soit E un \mathbb{K} -espace vectoriel, $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$.

- On dit que λ est une *valeur propre* de u s'il existe $x \in E$ tel que $x \neq 0$ et $u(x) = \lambda x$.
- x s'appelle alors *vecteur propre* de u associé à λ .
- L'ensemble des valeurs propres de u dans \mathbb{K} s'appelle *spectre* de u et se note $\text{Sp}_{\mathbb{K}}(u)$.

Théorème 10

Soit E un \mathbb{K} -espace vectoriel, $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$. Les propriétés suivantes sont équivalentes :

- λ est une valeur propre de u .
 - $u - \lambda \text{id}_E$ est non injective.
 - $\ker(u - \lambda \text{id}_E) \neq \{0_E\}$.
- $E_\lambda = \ker(u - \lambda \text{id}_E)$ s'appelle *sous-espace propre* de u , associé à λ .

Remarque 6

Soit E un \mathbb{K} -espace vectoriel, $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$ une valeur propre de u et x un vecteur propre associé, donc $u(x) = \lambda x$, dans ce cas on a les résultats suivants :

- $u^k(x) = \lambda^k x$, $\forall k \in \mathbb{N}$, en particulier λ^k est une valeur propre de u^k .
- $P(u)(x) = P(\lambda)x$, $\forall P \in \mathbb{K}[X]$, en particulier $P(u) = 0 \implies P(\lambda) = 0$.

Théorème 11

Soit E un \mathbb{K} -espace vectoriel, $u \in \mathcal{L}(E)$ et $\lambda \in \mathbb{K}$, alors λ une valeur propre de u si et seulement si λ est une racine de π_u .

i.e. les valeurs propres de u sont exactement les racines de π_u .

Fin
à la prochaine