106 : PGCD dans $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps commutatif, théorème de Bézout. Applications.

Prérequis : Arithmétique dans $\mathbb{Z}$.
Division euclidienne dans $\mathbb{K}[X]$.

I- PGCD

Th : $\mathbb{K}[X]$ est un anneau principal.

Coro : $\forall P_1,\dots,P_n \in \mathbb{K}[X] \quad \exists!\, P$ unitaire tq. : $(P_1)+\cdots+(P_n)=(P)$

Déf : On dira que P est le PGCD de $(P_1,\dots,P_n)$ et on notera : $P = P_1 \wedge \cdots \wedge P_n$

Prop : Soit $P = P_1 \wedge \cdots \wedge P_n$, si $A \in \mathbb{K}[X]$ tel que : $\forall i \in \{1,\dots,n\}$ $A|P_i$ alors $A|P$.

Prop : $\wedge$ est associative, commutative et la multiplication est distributive par rapport à $\wedge$.

Exo : Calculer $(X^m-1)\wedge(X^n-1)$ pour $m,n \in \mathbb{N}^*$ Arn p. 266

Prop : Soit $A = BQ+R$ la div. eucl. de A par B. On a alors : $A \wedge B = B \wedge R$

Appli : Algo. d'euclide pour le calcul du PGCD.

Exo : Mq $\left(X^5+X+1\right)\wedge\left(X^4-2X^3-X+2\right) = X^2+X+1$ dans $\mathbb{R}[X]$ Mo p.140

Exo : Calculer $\left(X^5-X+1\right)\wedge\left(X^2+1\right)$ dans $\mathbb{Z}/5\mathbb{Z}[X]$

II- Bézout

Déf : On dit que $P_1,\dots,P_n$ sont premiers entre eux si $P_1 \wedge \cdots \wedge P_n = 1$

Exo : Pour quelles valeurs de $p \in \mathbb{P}$ et $a \in \mathbb{Z}/p\mathbb{Z}$ (X^p+X+2a) et $\left(X^2+1\right)$ sont-ils premiers entre eux dans $\mathbb{Z}/p\mathbb{Z}[X]$?

Prop (Bézout) : $P_1 \wedge \cdots \wedge P_n = 1 \Leftrightarrow \exists U_1,\dots,U_n$ tq $\sum_{i=1}^{n} P_iU_i = 1$ (Les U_i peuvent être trouvés par l'algorithme d'euclide.)

Prop (Gauss) : Si $A \wedge B = 1$ alors $A|BC \Rightarrow A|C$

Exo : $a,b \in \mathbb{N}\backslash\{0,1\}$ $\quad P,Q \in \mathbb{C}[X]$ tq $P^a - Q^b = 1$ Montrer que P et Q sont constants. Mo p. 145

Déf : $P \in \mathbb{K}[X]$ est irréductible si $deg(P) \geqslant 1$ et si : $Q|P \Rightarrow \quad Q = a$ ou $Q = aP$ avec $a \in \mathbb{K}$

Prop : P irréductible $\Rightarrow \quad P \wedge Q = 1$ ou $P|Q$

Th : Tout polynôme P non constant s'écrit de manière unique à l'ordre près sous la forme : $P = a\prod_{i=1}^{n} P_i$ avec $a \in \mathbb{K}$ et P_i irréductible $\forall i$.

Appli : $A \wedge B = \prod_{i=1}^{n} P_i^{\min(a_i,b_i)}$ ou $A = \prod_{i=1}^{n} P_i^{a_i}$ et $B = \prod_{i=1}^{n} P_i^{b_i}$ (décomposition primaire de A et B)

Exo : A,B,C 2 à 2 premiers entre eux. Mq $(AB+BC+CA)\wedge(ABC) = 1$ Mo p. 146

Exo : Soit $(b,c) \in \mathbb{N}^2$, $b \wedge c = 1$. Montrer que : $\left(P^b-1\right)\left(P^c-1\right) | \left(P-1\right)\left(P^{bc}-1\right)$ Arn p. 269

III- Applications

Th (décomposition des noyaux) : Si $P = \prod_{i=1}^{n} P_i$ où les P_i sont 2 à 2 premiers entre eux.
E e.v. et $u \in \mathcal{L}(E)$ alors $\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{n} \mathrm{Ker}P_i(u)$
Gd p.173

Appli 1 : Résolution des équations différentielles linéaires à coefficients constants du type : $\sum_{i=0}^{n} a_i f^{(i)} = 0$ Gd p. 359
ou suites Ro p. 128-309

Appli 2 : $u \in \mathcal{L}(E)$ est diagonalisable $\Leftrightarrow \quad \exists P \in \mathbb{K}[X]$ scindé à racines simples tq $P(u) = 0$.
Gd p.173

Exo : Montrer que les symétries et projections sont diagonalisables.

Th (Liouville) : $n \in \mathbb{N}$, $n \geqslant 3$. Si $P^n+Q^n+R^n = 0$ dans $\mathbb{C}[X]$ alors P,Q et R sont égaux à une constante multiplicative près. X-ENS p. 179

Th : $A \in \mathbb{K}[X]$, $\quad S_1,\dots,S_n \in \mathbb{K}[X]\backslash\{0\}$ 2 à 2 premiers entre eux. $\exists!\,(E,R_1,\dots,R_n) \in (\mathbb{K}[X])^{n+1}$ $\dfrac{A}{S_1\dots S_n} = E + \sum_{i=1}^{n}\dfrac{R_i}{S_i}$ avec $deg(R_i) < deg(S_i)$
Mo p. 166

Appli : Décomposition en éléments simples ; calcul de primitives Mo p.171 So p. 238

José Gregorio : http://agregorio.net