ENS de Lyon
2025-2026

Leçon Agreg

Leçon PGCD/PPCM

I. Thèmes pour le plan et de développements

Les éléments marqués « DEV » dans cette section sont des éléments qui peuvent être mis en item dans ce plan et réutilisés comme développements dans au moins une autre leçon. Attention, ce ne sont pas tous les meilleurs développements possibles pour cette leçon.

1. Choses obligatoires

- Définition abstraite du ppcm/pgcd dans un anneau commutatif intègre.
- Existence et formule pour le pgcd dans un anneau factoriel. Principal $\Longrightarrow$ Factoriel. Formules basiques du genre $(ca \wedge cb) = c(a \wedge b)$ et $(a \wedge b)(a \vee b) = ab$.
- Algorithme d'Euclide dans un anneau euclidien, exemple de $\mathbb{Z}$ et $\mathbb{K}[X]$.
- Lemme chinois (si vous voulez, vous avez le droit de l'énoncer dans un anneau principal car c'est déjà très bien et suffisant).
- Lemme des noyaux.
- Résolution de l'équation diophantienne linéaire à 2 inconnues. Donner l'algo.
- Interpolation de Lagrange = restes chinois.

2. Choses classiques

Je conseille de jeter au moins un coup d'œil à ces éléments.

- Pas mal d'exemples d'anneaux euclidiens : $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ (avec j d'ordre 3 dans $\mathbb{C}^\times$).
- Identités à mourir de rire : $(X^m - 1) \wedge (X^n - 1) = X^{m \wedge n} - 1$.
- pgcd dans $\mathbb{K}[X]$ c'est pareil que pgcd dans $\mathbb{L}[X]$, si $\mathbb{L}/\mathbb{K}$ est une extension (quelconque) de corps.
- Arithmétique dans des groupes. Par exemple : Ordre d'un élément dans un groupe cyclique. Exposant d'un groupe. Un sous-groupe fini d'un corps est cyclique.
- Algorithme d'Euclide binaire pour des pgcd dans $\mathbb{Z}$ (on divise par deux quand on peut).
- Exemples de pgcd qui n'existent pas (dans $\mathbb{Z}[\sqrt{-5}]$, c.f. Rombaldi) dans un anneau commutatif intègre. Existence du ppcm implique celle du pgcd, mais pas réciproquement (même référence).
- Etude de la complexité sur les bits des algos mentionnés (e.g. dans Demazure).
- Calcul de pgcd dans $\mathbb{K}[X, Y]$ ou dans $\mathbb{Z}[X]$: utiliser le contenu.
- Non classique mais devrait l'être : Lemme Chinois=Lemme des noyaux. Si $u \in \mathcal{L}(E)$ (E de dimension finie), il existe un diagramme commutatif d'isomorphismes de $\mathbb{K}$-algèbres (exo : les définir. Indication : ils sont naturels) :

$$\begin{array}{ccc} \mathbb{K}[X]/(\pi_u) & \xrightarrow{c} & \displaystyle\prod_{i=1}^{r} \mathbb{K}[X]/(P_i^{n_i}) \\ \Big\downarrow \text{can} & & \Big\downarrow \prod \text{can}_i \\ \mathbb{K}[u] & \xrightarrow[r]{} & \displaystyle\prod_{i=1}^{r} \mathbb{K}\Big[u_{|C_{P_i}(u)}\Big]. \end{array}$$

- Le diagramme précédent permet une preuve vraiment efficace de la liste des idempotents de $\mathbb{K}[u]$.

3. Pistes pour enrichir

Ces éléments sont très bien pour s'amuser un peu plus, rajouter du contenu. Ce genre de contenu de plan se recase bien.

- Anneaux à PGCD. $\mathbb{Z} + X\mathbb{Q}[X] \subset \mathbb{Q}[X]$ n'est pas factoriel mais a des pgcd. $\mathcal{H}(U)$ ($U \subset \mathbb{C}$ ouvert connexe) aussi ! On retrouve les lemmes d'Euclide, Gauss. La théorie du contenu se généralise parfaitement (pas aisément mais c'est sympa).
- Résultant. Conseillé si vous êtes en option C.

— Forme normale de Smith et structure des modules sur un anneau euclidien (ou même principal, mais attention la forme normale de smith est plus reloue). Oui, si ça vous plaît, allez-y. Application : structure des G.A.F, invariants de Frobenius.

II. Développements pour cette leçon

Ils font aussi de supers items de plans. Liste non exhaustive.

— Un scoop sur Cailey-Hamilton (voir exos ou c.f. chaîne YouTube de Caldero)

— Forme normale de Smith (présenter l'algo, et surtout montrer qu'il termine).

— Théorème de descente de Springer (très beau recasage notamment en formes quadratiques, c.f. CVAlgébrie de Caldero-Peronnier)

— Algorithme de Berlekamp.

— Idempotents de $\mathbb{K}[u]$, application à Dunford.

— Une forme faible du théorème de Bézout (intersection de courbes algébriques, attention, ça utilise le résultant)

III. Exercices

Exercice 1. (Définitions d'un entier algébrique) Montrer qu'un élément x est entier algébrique sur $\mathbb{Z}$ (i.e. annulé par un polynôme unitaire de $\mathbb{Z}[X]$) si et seulement s'il est algébrique sur $\mathbb{Q}$, de polynôme minimal à coefficients dans $\mathbb{Z}$.

Exercice 2. — Soit $\mathbb{K}$ corps, soit $A, B \in \mathbb{K}[X]$ premier entre eux, et $F = A/B$. Quel est le degré de l'élément X sur le corps $\mathbb{K}(F)$?

Exercice 3. — Soit $P \in \mathbb{Z}[X]$. Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux. Si $\frac{p}{q}$ est une racine de multiplicité d de P, montrer que q^d divise le coefficient dominant de P.

Exercice 4. (Un scoop sur Cailey-Hamilton) Soit $\mathbb{K}$ un corps. Si $A \in M_n(\mathbb{K})$, on note χ_A son polynôme caractéristique et π_A son polynôme minimal.

1. Soit $A \in M_n(\mathbb{K})$, $P \in \mathbb{K}[X]$, $B(X) \in M_n(\mathbb{K}[X])$ tels que $(XI_n - A)B(X) = P(X)I_n$. Montrer que $P(A) = 0$.

2. En déduire le théorème de Cailey-Hamilton.

3. Montrer que $\chi_A/\mu_A = \pi_A$, où π_A est le pgcd des coefficients de la matrice $C(X) = \mathrm{Com}(XI_n - A)$. Commencer par vérifier que $\pi_A \mid \chi_A$.

Exercice 5. (Théorème de l'élément primitif, à peu près la preuve par Galois) Soit $\mathbb{K}$ un corps infini. Le but est de montrer le théorème suivant : si $\mathbb{L}/\mathbb{K}$ est une extension finie, alors il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[x]$. Si x est un élément algébrique sur $\mathbb{K}$, on note $\Pi_{\mathbb{K},x}$ son polynôme minimal sur $\mathbb{K}$.

1. Montrer qu'il ne suffit de prouver ce théorème que pour les extensions de la forme $\mathbb{L} = \mathbb{K}[x, y]$, avec x, y algébriques sur $\mathbb{K}$.

2. Soit x, y algébriques sur $\mathbb{K}$, soit $x_1, \dots, x_n$ et $y_1, \dots, y_m$ les racines de $\Pi_{\mathbb{K},x}$ et $\Pi_{\mathbb{K},y}$ dans un corps de décomposition $\mathbb{M}$ assez grand.

a. Montrer qu'il existe $t \in \mathbb{K}$ tel que $\forall (i, j) \in [\![1, n]\!] \times [\![1, m]\!]$, $x + ty = x_i + ty_j \implies i = j = 1$.

b. Calculer le pgcd entre les polynômes $\Pi_{\mathbb{K},y}(X)$ et $\Pi_{\mathbb{K},x}(z - tX)$ comme éléments de l'anneau $\mathbb{M}[X]$.

c. En déduire que $y \in \mathbb{K}[z]$.

3. Conclure.