Leçon 141 : Polynômes Irréductibles à une indéterminée. Corps de rupture. Applications

Cadre : on considère par la suite (sauf mention contraire explicite) que les anneaux (notés A) et corps (notés K) sont commutatifs et que les anneaux sont intègres.

1. Rapport du jury. — 2017 : *Dans cette leçon on peut présenter des méthodes de résolution, de la théorie des corps, des notions de topologie (continuité des racines) ou même des formes quadratiques. Il peut être pertinent d'introduire la notion de polynôme scindé, de citer le théorème de d'Alembert-Gauss et des applications des racines (valeurs propres, etc.). Il est apprécié de faire apparaître le lien solide entre la recherche des racines d'un polynôme et la réduction des matrices ; l'étude des valeurs propres de la matrice compagnon d'un polynôme permet d'entretenir ce lien. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois ou s'intéresser à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin..*

2. Généralités. — On suppose connus les notions et résultats simples sur les groupes, anneaux, corps et espaces vectoriels.

A étant intègre, on aura affaire à des anneaux de polynômes intègres, ayant des corps de fractions (construits de manière formellement analogue à la construction de Q) et vérifiant $deg(PQ) = deg(P) + deg(Q)$ (le coefficient dominant étant le produit des deux autres).

1. *Définitions.* —

- Def : Un élément d'un anneau intègre est irréductible s'il n'est pas inversible et s'il n'est pas le produit de deux éléments non inversibles.
- Not : On note A^x l'ensemble des inversibles de A. C'était un corps inclus dans A qui a une structure d'espace vectoriel sur A^x.
- Def : Deux éléments a et b sont associés s'il existe un inversible λ tel que $a = \lambda b$. Il s'agit d'une relation d'équivalence.
- Prop. : a et b sont associés ssi $(a) = (b)$ ssi $a/b\&b/a$
- Def : Anneaux premier, principaux, euclidiens, factoriels.

Exemples :

- Ex : 0 n'est jamais irréductible puisque $0 = 0 * 0$.
- Ex : un corps n'a pas d'éléments irréductibles. $\mathbb{Z}$ a pour éléments irréductibles les nombres premiers (positifs et négatifs).
- Ex : $2(X + 1)$ n'est pas irréductible dans l'anneau des polynômes $\mathbb{Z}[X]$, mais l'est sur $\mathbb{Q}[X]$.

2. *PGCD et PPCM :.* —

- Pro et Def : Dans le cas d'un anneau factoriel, l'ensemble des idéaux monogènes est réticulé. On définit $c = ppcm(a, b)$ comme $(c) = inf((a), (b))$ et $d = pgcd(a, b)$ comme $(d) = sup((a), (b))$.
- Rem : On a donc que ppcm et pgcd sont définis à un multiple inversible près.
- Rem : Dans la mesure où $I = (a) + (b)$ ne serait pas monogène, I peut ne pas coïncider avec (d), qu'il contient.
- Pro : *Théorème de Bezout-Bachet* : si A est principal, $(pgcd(a, b)) = (a) + (b)$ et donc il existe λ, μ tels que $pgcd(a, b) = \lambda a + \mu b$.
- Pro : Dans tous les cas d'anneaux, si $c = ppcm(a, b)$ alors $(c) = (a) \cap (b)$

3. Anneau des polynômes sur un corps. — *Propriétés :*

- Pro : Si $\mathbb{K}$ est un corps, $\mathbb{K}[X]$ est intègre et $deg(PQ) = deg(P) + deg(Q)$.
- Pro : L'ensemble des inversibles est $\mathbb{K}[X] - \{0\}$. Les classes d'équivalence par rapport à la relation "associés" contiennent -et peuvent être représentées par- un unique polynôme unitaire. On pourra souvent prendre un tel polynôme sans perte de généralité.
- Pro : On dispose d'une division euclidienne avec pour stathme le degré d'un polynôme.
- Pro $\mathbb{K}[X]$ est euclidien, principal et factoriel.
- Pro : Puisque $\mathbb{K}[X]$ est principal, on a le théorème de Bézout $((a)+(b) = (pgcd(a, b))$.
- Pro : On a en particulier le lemme d'Euclide et les éléments premiers sont forcément irréductibles.
- Pro : les polynômes de degré 1 sont tous irréductibles.
- Thm : Théorème de d'Alembert-Gauss : Les seuls polynômes de $\mathbb{C}[X]$ sont ceux de degré 1.
- les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont alors de degré 1 (tous) ou de degré 2 (ceux dont le discriminant est strictement négatif).

4. Anneau des polynômes sur un anneau intègre. — Motivation en partant de l'exemple $2(X + 1)$ avec $2 \notin A^*$. *Définitions et propriétés 4 : éléments primitifs*

- Def : *élément primitif* P : les seuls éléments divisant tous ses coefficients sont les inversibles de A (noté A^*).
- Def : *contenu d'un polynôme* P, noté $co(P)$: élément $a \in A$ tel $\exists Q$ primitif $P = aQ$.
- Pro : $co(P)$ est unique modulo A^*.
- Rem : lorsque possible (et c'est toujours le cas pour $K[X]$) on retient les polynômes unitaires pour représenter $co(P)$.
- Lem : lemme de Gauss - Soit A un anneau factoriel. Alors, $\forall P, Q \in A[X]$, $co(PQ) = co(P)co(Q)$ modulo les inversibles de A.

Propiétés :

- Pro : si A est un intègre, $A[X]$ est intègre et $deg(PQ) = deg(P) + deg(Q)$.
- Pro : si A est un factoriel, $A[X]$ est factoriel.
- Rem : A peut être euclidien sans que $A[X]$ le soit. Si A est un corps, oui.
- Rem : $A[X]$ n'est pas forcément principal même si A l'est. On ne peut donc compter sur le théorème de Bézout.
- Pro : Les seuls éléments inversibles d'un anneau $A[X]$ sont les éléments inversibles de A.

– Pro : Les polynômes irréductibles de $A[X]$ sont exactement :
  • Les constantes (hors zéro) non inversibles.
  • Les polynômes *primitifs* irréductibles sur $\mathbb{K}[X]$, corps des fractions de $A[X]$

Propositions

– Pro : on a la division euclidienne dès lors que le coefficient dominant est inversible.
– *Cor.* : A étant intègre, un polynôme de degré n a au plus n racines.

Exemples 7 :

– Un irréductible de degré $ge2$ ne peut pas avoir de racine.
– Réciproque pour les degrés 2 et 3.
– Ceci est faux pour les degrés $ge4$ (cf famille $(X^2+1)^2P(X)$).
– $2(X+2)$ sur $\mathbb{Z}/4\mathbb{Z}$ (qui n'est pas intègre) : nous avons 0 et 2 comme racines

5. Polynômes dérivés. —

6. Critères d'irréductibilité. —

– The : *Critère d'Einseinstein* : si p premier divise les coefficients autres que dominant et p^2 ne divise pas pour autant le coefficient du terme constant, le polynôme est irréductible. Ex : $X^n - pc$ avec p premier et premier avec c.
– Pro : si $P(X)$ est irréductible, $P(X+1)$ l'est aussi. Ex: $X^n + \cdots + 1$
– Pro : soit $P(X) = \Sigma(a_k X)$ et si p ne divise a_n et si on considère $P_p$la réduction modulo p, alors si P_p est irréductible, P l'est aussi. Ex : $X^3+2712X^2+517X+111$, qui se réduit à X^3+X+1 sur F_2 où il est irréductible car de degré 3 et sans racine.
– Si P de degré n, il est irréductible s'il n'a pas aucune racine de degré $\leq \frac{n}{2}$.
– Pro : si P est irréductible sur $k[X]$, il l'est aussi sur toute extension K dont la dimension sur k est première avec le degré de P.
– Dév. : Berlekamp Trouver des facteurs d'un polynôme sur F_q.

7. Corps de rupture. — *Prop. : adjonction d'une racine* Pour tout corps k on peut créer ainsi un sur-corps m/k de k-dimension finie :

– Pro : si $f(X) \in k[X]$ est irréductible (et donc en particulier est sans racine dans k), alors (f) est maximal et $k[X]/f(X)$ est un corps.
– Pro : il vérifie que, si on note $\alpha = [X]$ alors $f(\alpha) = 0$.
– Pro : $[m:k] = deg(f)$
– Pro : on a $k \subseteq m$ via l'injection canonique d'un anneau dans son anneau des polynômes.
– *Nota :* on a donc "fabriqué" un nouvel élément α et un nouveau corps m de la forme $k(\alpha)$. Dans ce nouveau corps, f a une racine et n'est donc plus irréductible : on parle de "corps de rupture de f".

Développement 1 : *Berlekamp*

Développement 2 : *Irréductibilité des polynômes cyclotomiques*

Développement 3 : *Polynômes irréductibles de F_q*

.

Sources :

– *D. Perrin "Algèbre Générale"*
– *Dany-Jack Mercier "Corps Finis"*
– *J. Calais "Extension des corps - Théorie de Galois"*
– *Jeanneret - Lines "Invitation à l'Algèbre"*
– *Hauchecorne*

November 20, 2017

Bruno Nitrosso, EPP et indépendant