Leçon 122 - Anneaux principaux. Applications.

Cadre : A désigne un anneau commutatif unitaure, et K un corps.

1. Notion de principalité. —

1. Idéaux et anneaux principaux. —

- Def : Un idéal I d'un anneau A est principal ssi il est non-trivial et engendré par un élément.
- Ex : Pour $n \geq 1$, $n\mathbb{Z}$ est principal.
- Contre-ex : Dans $\mathbb{Z}[X]$, $(2, X)$ n'est pas principal.
- Def : Un anneau intègre A est principal ssi tous ses idéaux non-triviaux sont principaux.
- Ex : Un corps est principal.
- Pro : $\mathbb{Z}$ est un anneau principal. Tous ses idéaux sont de la forme $n\mathbb{Z}$.
- Def : Un anneau intègre A est dit noethérien si tout idéal non-trivial de A est engendré par un nombre fini d'éléments.
- Pro : Un anneau intègre A est noethérien ssi toute suite croissante d'idéaux de A est stationnaire.
- Pro : Un anneau principal est noethérien.

2. Exemple des anneaux euclidiens. —

- Def : Un anneau intègre A est dit euclidien s'il existe une application $w : A-\{0\} \to \mathbb{N}$ telle que :
  ii) $\forall a, b \in A - \{0\}$, $w(b) \leq w(ab)$ i) $\forall a, b \in A - \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $w(r) < w(b)$.
- Pro : Pour tout $a, b \in A-\{0\}$ le couple q, r vérifiant la propriété ci-dessus est unique.
- Pro : Un anneau euclidien est principal.
- Ex : $\mathbb{Z}$ est euclidien pour $w(a) = |a|$. K est euclidien pour $w(a) = 0$.
- Pro : $A[X]$ est euclidien ssi A est un corps, et son stathme est $w(P) = deg(P)$.
  Si A n'est pas un corps, alors $A[X]$ n'est pas principal.
- Rem : Ainsi, $K[X_1, .., X_n]$ est principal ssi $n = 1$.
- Pro : Les éléments inversibles d'un anneau euclidien sont ceux de stathme minimal.
- Pro : L'anneau des séries formelles $K[[X]] := \{\sum_n a_n X^n \text{ tq } (a_n)_n \in K^{\mathbb{N}}\}$ est euclidien pour $w(S) = val(S) = \min(n \geq 0 \text{ tq } a_n \neq 0)$.
- Pro : Les inversibles de $K[[X]]$ sont les séries formelles avec $a_0 \neq 0$.
  Les idéaux non-triviaux de $K[[X]]$ sont de la forme (X^n) pour un $n \geq 1$.
- Ex : $\mathbb{Z}[i]$ est euclidien pour $w(a + ib) = \sqrt{a^2 + b^2}$.
- Pro : L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal non euclidien.

2. Arithmétique dans les anneaux principaux. —

1. Arithmétique dans $\mathbb{Z}$. —

- Def : Pour $a, b \in A$, on dit que $a|b$ si $b \in (a)$.
- Rem : $(a) = (b)$ ssi $\exists u \in A^\times$ tq $b = a.u$. On dit alors que a et b sont associés.
- Def : On dit qu'un élément c est irréductible ssi $a|c \Rightarrow$ a inversible ou a associé à c.
- Rem : Si c est irréductible, alors l'idéal (c) est maximal parmi les idéaux principaux de A.
- Cor : Les idéaux maximaux d'un anneau principal sont exactement les idéaux de la forme $I = (c)$ pour c un irréductible de A.
- Ex : Les éléments irréductibles de $K[[X]]$ sont les X^n à association près.
- Def : Soit L un corps contenant le corps K. Un élément $x \in L$ est algébrique sur K ssi il existe $P \in K[X]$ tel que $P(x) = 0$.
- Def+Pro : Pour x algébrique sur K, il existe un unique polynôme unitaire générateur de l'idéal des polynômes annulateurs de x. On le note μ_x et on l'appelle polynôme minimal de x sur $\mathbb{K}$.
- Pro : Pour tout $P \in K[X]$ tel que $P(x) = 0$, on a $\mu_x | P$. Ainsi, μ_x est irréductible sur K.
  De plus, le sous-corps de L engendré par K et x, $K(x)$, est isomorphe à $K[X]/(\mu_x)$ via l'isomorphisme qui à la classe de X modulo μ_x assoxie x. On appelle alors corps de rupture de x sur K le corps $K[X]/(\mu_x)$.
- Ex : $\sqrt[p]{n}$ est algébrique sur $\mathbb{Q}$, $exp^{i\pi\frac{k}{n}}$ est algébrique sur $\mathbb{Q}$, i est algébrique sur $\mathbb{R}$. $K \in K(X)$ est transcendant sur K.
- Ex : On a $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$.
- Def : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k\wedge n=1,\ k\leq n}(X - e^{2i\pi\frac{k}{n}}) \in \mathbb{C}[X]$, le n-ième polynôme cyclotomique.
- **Dev** : Pour tout $n \geq 1$, Φ_n est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$ et tel que $\Pi_{d|n}\Phi_d = X^n - 1$.
  On peut ainsi projeter les polynômes cyclotomiques dans $\mathbb{F}_p[X]$ et avoir une décomposition de $X^n - 1$. en produit de polynômes.
- Pro : Pour tout $n = p^s.m$ avec $m \wedge p = 1$, $\Phi_n(X) = \Phi_m(X)^{p^s - p^{s-1}}$ dans $\mathbb{F}_p[X]$.
  Si $n \wedge p = 1$, alors tous les facteurs irréductibles de Φ_n dans $\mathbb{F}_q[X]$ sont de degré égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Rem : Comme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est cyclique que si $n = \widetilde{p}$ ou $n = 2\widetilde{p}$ avec $\widetilde{p}$ premier, une grande partie des polynômes cyclotomiques n'est automatiquement pas irréductible sur les $\mathbb{F}_q$.

2. Héritage de la factorialité. —

- Def : Pour $a, b \in A - \{0\}$, on appelle pgcd de a et de b un élément $d \in A$ tel que $d|a$, $d|b$, et tel que $c|a$ et $c|b \Rightarrow c|d$.
  On appelle ppcm de a et de b un élément $d \in A$ tel que $a|d$, $b|d$, et tel que $a|c$ et $b|c \Rightarrow d|c$.
- Rem : Le ppcm et le pgcd de deux éléments n'existe pas forcément. Dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et 9 et $6 + 3i\sqrt{5}$ n'ont pas de pdcg.
  Si le pgcd/ppcm exisent, ils sont uniques à association près.
- Def : Système de représentant des irréductibles.

- Def : Un anneau A est facoriel ssi pour tout élément x il existe des $p_1, .., p_n$ du système de représentant des irréductibles, des indices $a_1, .., a_n$, et un inversible u, tel que $x = u.p_1^{a_1}..p_n^{a_n}$, et tel que cette écriture soit unique à permutation près des p_i.
- Ex : $\mathbb{Z}$ est factoriel. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$
- Pro : Un anneau principal est factoriel.
- Pro : Conditions pour être factoriel quand il y a existence de la décomposition en produit d'irréductibles.
- Pro : Soit A un anneau principal. Soient $a, b \in A - \{0\}$.
  Le pgcd de a et b est un $d \in A$ tel que $(d) = (a) + (b)$.
  Le ppcm de a et b est un $d \in A$ tel que $(d) = (a) \cap (b)$.
- Théorème de Bézout : Si A est principal, alors pour tous $a, b \in A - \{0\}$ il existe $u, v \in A$ tels que $au + bv = pgcd(a, b)$.
- App : Lemme des noyaux : Soit E un K-ev de dimension finie et $u \in End(E)$. Soit $P \in K[X]$ avec $P = P_1..P_r$ où les P_i sont premiers entre eux deux à deux.
  Alors $Ker(P(u)) = \oplus_i Ker(P_i(u))$.
- Thm : Un anneau factoriel qui vérifie le théorème de Bézout est principal.

3. Théorème chinois et polynômes d'endomorphismes. —

- Théorème chinois : Soit A un anneau principal, soit $a \in A - \{0\}$ avec $a = r_1..r_n$ où les r_i sont premiers entre eux deux à deux. Alors $A/(a) \simeq \Pi_i A/(r_i)$.
- Application à la résolution d'un système de congruences.
- Def+Pro : Soit E un K-ev de dimension finie. Pour $u \in End(E)$ on définit $\Phi_u : P \in K[X] \mapsto P(u) \in End(E)$ le morphisme d'évaluation en u.
  Son image, notée $K[u]$, est une sous-algèbre commutative de $End(E)$.
  Comme E est de dimension finie, Φ_u n'est pas injectif. On appelle alors polynôme minimal de u, noté μ_u, l'unique polynôme unitaire de $K[X]$ générateur de $Ker(\Phi_u)$.
- App : Pour $\mu_u = P_1^{a_1}..P_r^{a_r}$ la décomposition de μ_u en produit de facteurs irréductibles dans $K[X]$, on a alors $K[u] \simeq K[X]/(\mu_u) \simeq \Pi_i \mathbb{K}[X]/(P_i^{a_i})$.
- App : u est diagonalisable dans E ssi $K[u] \simeq K^r$ pour un $r \geq 1$, où K^r est muni du produit terme à terme.
- Def : Soit $\mathbb{K}$ un corps et E un $\mathbb{K} - ev$. Un endomorphisme f de E est dit semi-simple si pour tout s-ev F de E stable par f, il existe un supplémentaire V de F qui est lui aussi stable par f.
- **Dev** : Soit $f \in End(E)$. Alors f est semi-simple ssi son polynôme minimal est sans facteurs carrés.

3. Anneaux d'entiers de corps quadratiques. —
On se place ici dans $\mathbb{Q}(\sqrt{d})$, avec $d \in \mathbb{Z} - \{0, 1\}$ sans facteurs carrés.

- Rem : $\mathbb{Q}(\sqrt{d})$ est un corps.
- Def : Norme d'un élément de $\mathbb{Q}(\sqrt{d})$.
- Def : Trace d'un élément de $\mathbb{Q}(\sqrt{d})$.
- Def : Un élément de $\mathbb{Q}(\sqrt{d})$ est appelé un entier algébrique ssi son polynôme minimal sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$.
  On appelle O_d l'ensemble des entiers algébriques sur $\mathbb{Q}(\sqrt{d})$.
- Pro : O_d est un anneau intègre.
- Thm : $O_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1\ mod(4)$, et $O_d = \mathbb{Z}[\sqrt{d}]$ sinon.
- Thm : La norme sur O_d est un stathme si :
  $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13\}$.
- Rem : Les inversibles de A_d sont les éléments de norme 1. Si $d < 0$ ce sont ± 1 et $\pm i$.
- Thm : Caractérisation des inversibles de A_d pour $d > 1$.
- Application à la résolution de $x^2 - 3y^2 = 1$.
- Rem : On a déjà vu que $\mathbb{Z}[i]$ est un anneau euclidien, avec pour stathme sa norme. Ses inversibles sont ± 1 et $\pm i$.
- **Dev** : Théorème des deux carrés de Fermat : Les irréductibles de $\mathbb{Z}[i]$ sont : les p premiers tq $p \equiv 2, 3\ mod(4)$, et les $a + ib$ tels que $a^2 + b^2$ est premier.
  De plus, l'équation diophantienne $x^2 + y^2 = n$ admet des solutions si et seulement si pour tout p premier tq $p \equiv 3$ mod(4), on a $v_p(n)$ pair.

Références

Combes : Théorème chinois, résolution d'un système de congruences. Entiers quadratiques.
Perrin : Idéal principal, polynôme minimal d'un élément algébrique, corps de rupture. Anneau euclidien, propriétés, exemples. Divisibilité, via les idéaux, él associés, él irréductibles. Système de représentants des irréductibles, anneau factoriel, critères de Gauss/Euclide propriétés, exemples. Bézout, pgcd/ppcm dans un anneau principal. Th des deux carrés.(Dev)
Tauvel : Anneau principal, propriétés, exemples. Pgcd et ppcm, exemples.
Duverney : Unités dans les anneaux d'entiers quadratiques.
Gourdon : Polynôme minimal d'un endomorphisme. Lemme des noyaux. Endomorphismes semi-simples.(Dev)
FGN (Algèbre 1) : Etude des polynômes cyclotomiques.(Dev)

January 23, 2018

Vidal Agniel, École normale supérieure de Rennes