122 ANNEAUX PRINCIPAUX. APPLICATIONS.

Soit A un anneau unitaire commutatif intègre et $\mathbb{K}$ un corps commutatif.

I. Arithmétique dans les anneaux

I. A. Vocabulaire

[Per96, §II.3, p45] [Rom17, Ch7, p205]

Définition 1. [Idéal]
$I \subset A$ est un idéal si $(I,+)$ est un sous-groupe de $(A,+)$ et si $\forall (a,i) \in A \times I, ai \in I$.

Exemple 2. Pour $a \in A$, $(a) = aA$ le plus petit idéal contenant a est dit principal.

Définition 3. [Divisibilité]
Pour $a, b \in A$, on dit que a divise b et on note $a \mid b$ si $\exists c \in A \mid b = ac$, ou encore $(b) \subset (a)$.

Définition 4. [Éléments associés]
$a, b \in A$ sont dits associés si $a \mid b$ et $b \mid a$ (ou s'il existe $u \in A^\times$ tel que $a = ub$).

Remarque 5. C'est une relation d'équivalence (notée $\sim$). Deux éléments associés sont indiscernables du point de vue de la divisibilité.

Définition 6. [Premier, irréductible] $a \in A$ non inversible et non nul est dit :
- premier si pour tout $b, c \in A$ tels que $a \mid bc$, alors $a \mid b$ ou $a \mid c$,
- irréductible si pour tout $b, c \in A$ tels que $a = bc$, alors $b \in A^\times$ ou $c \in A^\times$.

Proposition 7. *Si $a \in A$ est premier alors a est irréductible.*

Exemple 8. Dans $\mathbb{Z}$, les éléments premiers sont les nombres premiers et leurs opposés, tout comme les irréductibles (on a équivalence dans ce cas, comme on le verra plus loin).

Définition 9. [PGCD, PPCM] Soient $a, b \in A$. On dit que
- $d \in A$ est un PGCD de a et b et on note $d = a \wedge b$ si $\forall c \in A, c \mid a$ et $c \mid b \implies c \mid d$,
- $m \in A$ est un PPCM de a et b et on note $m = a \vee b$ si $\forall c \in A, a \mid c$ et $b \mid c \implies m \mid c$.

a et b sont dits premiers entre eux si $a \wedge b = 1$.

Remarque 10. L'existence de PGCD et PPCM n'est pas garantie en général. S'ils existent, ils sont définis à un inversible près. On peut généraliser à une famille quelconque d'éléments.

Proposition 11. *Deux PGCD (resp. PPCM) de $a, b \in A$ sont associés.*

I. B. Anneaux principaux

[Per96, §2.3-4, p49–51] [Rom17, Ch8, p231] [Com98, Ch11, p237]

Définition 12. [Anneau principal]
A est dit principal si tous ses idéaux sont principaux (engendrés par un élément).

Exemple 13. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

Proposition 14. *$A[X]$ est principal si et seulement si A est un corps.*

Soit désormais A principal.

Théorème 15. [Théorème de Bachet-Bézout]
Soient $a, b \in A^*$. Alors il existe $d \in A \mid (a,b) = (a) + (b) = (d)$. d est alors un PGCD de a et b et il existe $u, v \in A$ tels que $au + bv = d$.

Proposition 16. *Soient $a, b \in A^*$. Alors il existe $m \in A \mid (a) \cap (b) = (m)$. On a $m = a \vee b$.*

Remarque 17. On peut là encore généraliser à toute famille finie d'éléments.

Théorème 18. [Théorèmes de Gauss]
Soient $a, b, c \in A^*$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$. Si $ab \mid c$ et $b \wedge c = 1$, alors $a \mid c$.

Théorème 19. [Théorème des restes chinois]
Soient $a_1, \dots, a_r \in A$ deux à deux premiers. Alors l'application $\phi : x \mod a_1 \dots a_r \longmapsto (x \mod a_i)_{1 \le i \le r}$ est un isomorphisme d'anneaux de $A/(a_1 \dots a_r)$ sur $\prod_{i=1}^r A/(a_i)$.

Remarque 20. Si les $(a_i)_{1 \le i \le r}$ ne sont pas deux à deux premiers, le résultat est faux : par exemple $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Proposition 21. *Soit $p \in A^*$. Alors p est irréductible si et seulement si $A/(p)$ est intègre si et seulement si $A/(p)$ est un corps.*

Corollaire 22. *Dans un anneau principal, premier équivaut à irréductible.*

Proposition 23.
- *Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
- *Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 sans racines.*
- *$\mathbb{Q}[X]$ possède des irréductibles de degré arbitrairement grand.*

I. C. Anneau factoriel

[Per96, §2.3, p47] [Rom17, §7.6/8.2, p217/237]

Définition 24. [Anneau factoriel]
Un anneau A est factoriel si pour tout $a \in A^*$:
(E) il existe $n \in \mathbb{N}$, $p_1, \dots, p_n \in A$ irréductibles et $u \in A^\times$ tels que $a = up_1 \dots p_n$.
(U) si de plus on peut aussi écrire $a = vq_1 \dots q_r$ pour un $r \in \mathbb{N}$, $q_1, \dots, q_r \in A$ irréductibles et $v \in A^\times$, alors $r = n$ et il existe $\sigma \in \mathfrak{S}_n$ tel que $p_i \sim q_{\sigma(i)}$ pour tout $1 \leq i \leq n$.

Proposition 25. *Soit $\mathcal{P}$ un système de représentants d'éléments irréductibles à association près. Alors tout élément $a \in A^*$ s'écrit de manière unique sous la forme (le produit ne comporte qu'un nombre fini de termes distincts de 1) :*

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{où } u \in A^\times \text{ et } v_p(a) = \max\{n \in \mathbb{N} \mid p^n \mid a\}$$

Corollaire 26. *Soit $(a_i)_{i\in I}$ une famille d'éléments de A. Alors $(a_i)_{i\in I}$ possède un PGCD et si I est fini, $(a_i)_{i\in I}$ possède un PPCM. On a :*

$$\mathrm{PGCD}((a_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{\min_{i\in I} v_p(a_i)} \quad \text{et} \quad \mathrm{PPCM}((a_i)_{i\in I}) = \prod_{p\in\mathcal{P}} p^{\max_{i\in I} v_p(a_i)}$$

Corollaire 27. *Soient $a, b \in A^*$. Alors $a \mid b \iff \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$.*

Proposition 28. *Un anneau principal est factoriel.*

Exemple 29. $\mathbb{Z}$ est factoriel. Ainsi tout entier $n \in \mathbb{Z}^*$ s'écrit de manière unique $n = \varepsilon \prod_{p\in\mathcal{P}} p^{v_p(n)}$ où $\varepsilon = \pm 1$ et $\mathcal{P}$ est l'ensemble des nombres premiers.

Exemple 30. $\mathbb{K}[X]$ est factoriel. En particulier :

- pour $P \in \mathbb{C}[X]$, il existe $a \in \mathbb{C}$, $(\lambda_i)_{1\leq i\leq \ell} \in \mathbb{C}^\ell$ distincts et $(\alpha_i)_{1\leq i\leq \ell} \in (\mathbb{N}^*)^\ell$ tels que
$$P = a \prod_{i=1}^{\ell} (X - \lambda_i)^{\alpha_i}$$
- pour $P \in \mathbb{R}[X]$, il existe $a \in \mathbb{R}$,$(\lambda_i)_{1\leq i\leq \ell} \in \mathbb{R}^\ell$ distincts et $(\alpha_i)_{1\leq i\leq \ell} \in (\mathbb{N}^*)^\ell$, puis $(\mu_j, \nu_j)_{1\leq j\leq m} \in (\mathbb{R}^2)^m$ distincts et $(\beta_j)_{1\leq j\leq m} \in \mathbb{N}^*$ tels que $\mu_j^2 - 4\nu_j < 0$ pour tout j et
$$P = a \prod_{i=1}^{\ell} (X - \lambda_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + \mu_j X + \nu_j)^{\beta_j}$$

Théorème 31. [Théorème de Gauss] *Si A est factoriel, alors $A[X]$ factoriel.*

Corollaire 32. *Si A est factoriel alors pour tout $n \in \mathbb{N}$, $A[X_1, \dots X_n]$ est factoriel.*

Exemple 33. Un anneau factoriel n'est pas nécessairement principal ! Considérer par exemple $\mathbb{Z}[X]$ et $(2, X)$ qui n'est pas principal.

II. Applications aux anneaux euclidiens

II. A. Généralités

[Per96, §2.3-5, p50] [Rom17, Ch9, p257] [Com98, §11.2, p238]

Définition 34. [Stathme, anneau euclidien]
Un stathme sur A est une application $\varphi : A^* \longrightarrow \mathbb{N}$ telle que pour $a, b \in A \times A^*$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Exemple 35. $\mathbb{Z}$ muni de la valeur absolue et $\mathbb{K}[X]$ muni du degré sont euclidiens.

Proposition 36. *Un anneau euclidien est principal.*

Proposition 37. *$\mathbb{K}[X]$ est euclidien.*

Application 38. [Algorithme d'Euclide] Dans un anneau euclidien, il existe un algorithme permettant de trouver le PGCD de deux éléments.

Proposition 39. *$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.*

II. B. L'anneau des entiers de Gauss

[Per96, §2.3, p50] [Rom17, §9.4.3, p263] [Com98, §11.6, p246]

Définition 40. On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.

Proposition 41. *Muni du stathme $N(a + ib) = a^2 + b^2$, $\mathbb{Z}[i]$ est euclidien.*

Proposition 42. $\mathbb{Z}[i]^\times = N^{-1}(\{1\}) = \{\pm 1, \pm i\}$.

On définit $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \mid n = a^2 + b^2\}$. On cherche à quelle(s) condition(s) $n \in \Sigma$.

Exemple 43. $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ mais pas $3, 6, 7, 11$.

Lemme 44. *Σ est stable par produit.*

Lemme 45. *Si $p \in \mathcal{P}$, alors $p \in \Sigma \iff p \equiv 1, 2 \mod 4$.*

Théorème 46. [Théorème des deux carrés de Fermat]
$n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \mid 3 \mod 4$, alors $2 \mid v_p(n)$.

Proposition 47. *Les irréductibles de $\mathbb{Z}[i]$ sont :*
- *les $p \in \mathcal{P}$ tels que $p \equiv 3 \mod 4$,*
- *les $a + ib$ tels que $a^2 + b^2 \in \mathcal{P}$.*

III. Autres applications

III. A. Équations diophantiennes

[Rom17, §8.3/10.4, p243/288]

Théorème 48. *Dans le Théorème 19, l'isomorphisme réciproque est $\psi^{-1} : (x_i \mod a_i)_{1\le i\le r} \longmapsto \sum_{i=1}^r x_i u_i b_i \mod a_1 \dots a_r$ où $b_i = a/a_i$ et $\sum_{i=1}^r u_i b_i = 1$.*

Application 49. Soit $a, b, c \in A$ principal. On note $d = a \wedge b = au + bv$ et on écrit $a = da'$ et $b = db'$. L'équation $ax + bv = c$ admet une solution si et seulement si $d \mid c$, disons $c = dc'$ et dans ce cas les solutions sont de la forme $(c'u + kb', c'v - ka')_{k\in A}$.

Remarque 50. Dans le cas où l'anneau est euclidien, on peut déterminer u et v par l'algorithme d'Euclide.

Application 51. [Le cas de $\mathbb{Z}$] Soient $n, m \ge 2$. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations

$$\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$$

d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors
- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k\in\mathbb{Z}}$.

Exemple 52. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k\in\mathbb{Z}}$.

III. B. Algèbre linéaire

[MM16] [BMP05, §4.2.1, p158–161] [Gou09, §5.4, p224–226]

Soit $M \in \mathcal{M}_n(\mathbb{K})$.

Définition 53. [Polynôme minimal]
L'application $\varphi_M : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[M] \\ P & \longmapsto & P(M) \end{array}$ est un morphisme d'algèbres. Son noyau est un idéal de $\mathbb{K}[X]$ principal donc est engendré par un unique polynôme unitaire π_M appelé polynôme minimal de M.

Proposition 54. *On a $\dim(\mathbb{K}[M]) = \deg(\pi_M)$.*

Proposition 55. *$\mathbb{K}[M]$ est un corps si et seulement si π_M est irréductible dans $\mathbb{K}[X]$.*

Lemme 56. [Lemme des noyaux]
Soit $(P_i)_{1\le i\le r}$ une famille de polynômes deux à deux premiers entre eux et $f \in \mathcal{L}(E)$. Alors en posant $P = \prod_{i=1}^r P_k$, on a $\ker(P(f)) = \bigoplus_{i=1}^r \ker(P_i(f))$.
De plus, le projecteur de $\ker(P(f))$ sur l'un de ces sous-espaces parallèlement à la somme des autres est un polynôme en f.

Exemple 57. En pratique, on utilise souvent ce lemme avec P annulateur de E. On obtient alors une décomposition de E en sous-espaces stables, car $\ker(Q(f))$ est stable par f pour tout polynôme Q.

Proposition 58. *M est trigonalisable (resp. diagonalisable) si et seulement si π_M est scindé (resp. scindé racines simples).*

Théorème 59. [Décomposition de Dunford]
Supposons M de polynôme caractéristique scindé. Alors il existe un unique couple $(D, N) \in \mathcal{M}_n(\mathbb{K})^2$ tel que D est diagonalisable, N est nilpotente, $M = D + N$ et M commute avec N.
De plus, D et N sont des polynômes en M.

Définition 60. [Endomorphisme semi-simple]
M est dite semi-simple si tout sous-espace vectoriel de $\mathbb{K}^n$ M-stable admet un supplémentaire M-stable.

Théorème 61. *M est semi-simple si et seulement si π_m est sans facteur carré.*

Exemple 62. Si M est nilpotente, alors M est semi-simple si et seulement si $M = 0$.

ANNEXE

Algorithme d'EUCLIDE

Soit A un anneau euclidien. L'algorithme d'EUCLIDE détermine le PGCD de deux éléments :

Entrée : $a, b \in A, b \neq 0$

Sortie : d, u, v tels que $au + bv = d$ et $d = a \wedge b$

Algorithme : $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1, r_0 = a, r_1 = b, i = 1$

Tant que $r_i \neq 0$:

$r_{i+1} \leftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)

$u_{i+1} \leftarrow u_{i-1} - q_i u_i$

$v_{i+1} \leftarrow v_{i-1} - q_i v_i$

$i \leftarrow i + 1$

Renvoyer $r_{i-1}, u_{i-1}, v_{i-1}$

SPEECH

On souhaite généraliser les propriétés des anneaux classiques, et notamment de $\mathbb{Z}$ ($\mathbb{Z}$ notamment). *Avant de parler du plan écrire au tableau les implications entre anneaux : euclidien implique principal implique factoriel, puis expliquer que la notion de* PGCD *(et* PPCM*) définie sur un anneau factoriel va profiter des propriétés des autres types d'anneaux.*

Dans la première partie, on s'intéresse à l'arithmétique dans les anneaux, avec les définitions d'idéal, d'idéal principal, d'élément premier, irréductible, de PGCD et de PPCM. On regarde le cas des anneaux principaux avec le théorème de BACHET-BÉZOUT, l'existence d'un PPCM, mais aussi théorème chinois qui permet par exemple de simplifier la résolution de systèmes de congruences (cf troisième partie), mais aussi l'équivalence entre élément premier et irréductible. Enfin les anneaux factoriels permettent des manipulations algébriques plus simples, on a une décomposition en produits irréductibles et théorème de GAUSS.

Ensuite, on s'intéresse aux anneaux euclidiens qui sont des exemples d'anneaux principaux dans lesquels on a un algorithme permettant de trouver facilement le PGCD de deux éléments. Le cas particulier de l'anneau des entiers de GAUSS sera étudié.

La dernière partie s'intéresse aux applications des anneaux principaux, que ce soit pour la résolution d'équations diophantiennes via le théorème chinois dont on connaît la réciproque et qui devient effectif dans un anneau eucliden, mais aussi en algèbre linéaire avec le lemme des noyaux (principalité de $\mathbb{K}[X]$) qui mène par exemple à la décomposition de DUNFORD.

QUESTIONS

Q Résoudre $x^2 + y^2 = z^2$ d'inconnues $x, y, z \in \mathbb{N}$.

R On va regarder cette équation dans $\mathbb{Z}[i]$.
Comme $x, y, z \in \mathbb{N}$, on a $d = \mathrm{PGCD}_{\mathbb{Z}}(x, y, z) = \mathrm{PGCD}_{\mathbb{Z}[i]}(x, y, z)$ et on peut supposer que $d = 1$ quitte à diviser les trois inconnues par d.
Soit $z \in \mathbb{N}$ et $w = x + iy \in \mathbb{Z}[i]$ tels que $N(w) = z^2$. Soit a un diviseur de w et $\overline{w}$. Alors $a \mid 2x = w - \overline{w}$ et $a \mid 2y = (w + \overline{w})/i$.
On peut choisir a irréductible puisque x, y, z sont premiers entre eux, et alors $a \mid 2$ ou $a \mid x$. Si $a \mid 2$, on a $N(a) \in \{1, 2, 4\}$. [...] On finit par montrer que $w \wedge w' = 1$ et on conclut en considérant la décomposition de z en irréductibles de $\mathbb{Z}[i]$ [...].

Q Décomposer $3 + j$ en irréductibles de $\mathbb{Z}[j]$.

R Les irréductibles de $\mathbb{Z}[j]$ sont (aux inversibles $\{\pm 1, \pm j, \pm j^2\}$ près) :
- les $p \in \mathcal{P}$ tels que $p \equiv 2 \mod 3$,
- les $a + bj \in \mathbb{Z}[j]$ tels que $N(a + bj) \in \mathcal{P}$.

On calcule $N(3 + j) = 7 \in \mathcal{P}$ donc $3 + j$ est irréductible.

Q Soit A principal. Montrer qu'il existe $v : A \longrightarrow \mathbb{N}$ telle que
- $v(a) = 0 \iff a = 0$,
- $v(ab) \geq v(a)$ pour $a, b \in A, b \neq 0$,
- si $v(a) \geq v(b)$ pour $a, b \in A, b \neq 0$, alors $b \mid a$ ou $\exists q, d \in A \,|\, 0 < v(ad - bq) < v(b)$.

R On prend pour $v(a)$ le nombre de facteurs irréductibles comptés avec leur multiplicité. On démontre le dernier point par l'absurde en utilisant l'identité de BÉZOUT.

Q L'ensemble des fonctions holomorphes sur un ouvert U est un anneau satisfaisant une relation de BÉZOUT entre ses éléments. Montrer cependant qu'il n'est pas principal.

R On montre en fait qu'il n'est pas factoriel. On vérifie que si f holomorphe est irréductible, alors nécessairement f n'a qu'un seul 0. On en déduit que toute fonction possédant une infinité de 0 n'admet pas d'écriture finie en produit d'irréductibles (par exemple $\sin$).

Q Trouver les nombres premiers s'écrivant sous la forme $p = a^2 + 2b^2$.

R $a^2 + 2b^2 = (a + i\sqrt{2}b)(a - i\sqrt{2}b)$. On se place dans $A = \mathbb{Z}[i\sqrt{2}]$. Le stathme $N = |.|^2$ montre que A est principal. Puis on procède similairement au théorème des deux carrés.

Q $\mathbb{C}[X, Y]/(Y^2 - X^3)$ et $\mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ sont-ils principaux ?

R Seul le second l'est !

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[Com98] F. COMBES : *Algèbre et géométrie*. Bréal, 1998.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.