Cadre : A un anneau commutatif unitaire, $\mathbb{K}$ un corps.

I Notion de principalité

1) Idéaux

Définition 1. Un idéal I de A es un sous-groupe de $(A,+)$ tel que pour tout $i \in I$ et tout $a \in A$, $ai \in I$.

Définition 2. Un idéal I de A est dit principal s'il est monogène, i.e. engendré par un élément $x \in A$. On note $I = (x) = xA$.

Exemple 3. *Tout idéal de $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$ pour p premier est principal.*

Exemple 4. *Dans $\mathbb{Z}[X]$, $(2,X)$ n'est pas principal*

Définition 5. Un idéal I de A est dit premier si $A \neq I$ et pour tous $a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

Proposition 6. *I est idéal premier si, et seulement si, A/I est intègre.*

Exemple 7. *L'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ est premier ssi $n = 0$ ou n est premier.*

Définition 8. Un idéal I de A est dit maximal si $A \neq I$ et pour tout J idéal de A, $I \subset J \subset A \Rightarrow J = I$ ou $J = A$.

Proposition 9. *I est idéal maximal si, et seulement si, A/I est un corps.*

Exemple 10. *Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premier.*

Remarque 11. *Tout idéal maximal est premier. La réciproque est fausse. En effet, dans $\mathbb{Z}[X]$, (X) est premier, mais non maximal ($\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ est intègre mais ce n'est pas un corps).*

2) Anneaux principaux

Définition 12. Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.

Exemple 13. *L'anneau $\mathbb{Z}$ est principal, ainsi que $\mathbb{K}[X]$, mais pas $\mathbb{Z}[X]$. $\mathbb{Z}/n\mathbb{Z}$ est principal si, et seulement si, n est premier.*

Application 14. *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, et soit $u \in \mathcal{L}(E)$. On note ϕ_u l'évaluation en u. L'anneau $\mathbb{K}[X]$ étant principal, $\operatorname{Ker}\phi_u$ est monogène. On appelle polynôme minimal de u l'unique générateur unitaire de $\operatorname{Ker}\phi_u$.*

Application 15. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps, et soit $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Un même raisonnement avec l'évaluation des polynômes en α donne l'existence du polynôme minimal en α.*

Définition 16. Soit $p \in A$, p est dit irréductible si $p \notin A^\times$ et si $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

Exemple 17. *Les irréductibles de $\mathbb{Z}$ sont les nombres premiers.*

Proposition 18. *Si A est principal, alors :*

$$p \text{ est irréductible} \Leftrightarrow (p) \text{ est premier} \Leftrightarrow (p) \text{ est maximal}$$

Proposition 19. *Si A est un corps, alors $A[X]$ est principal.*

3) Cas des anneaux euclidiens

Définition 20. Un stathme d'un anneau intègre est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a,b \in A \setminus \{0\}$, il existe $q,r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$).
Un anneau intègre possédant un stathme est dit euclidien.

Exemple 21. *$\mathbb{Z}$ muni de la valeur absolue est euclidien.*

Théorème 22. *Un anneau euclidien est principal.*

Proposition 23. *Soit $P \in A[X] \setminus \{0\}$ de coefficient dominant inversible, et $F \in A[X]$. Alors il existe $Q,R \in A[X]$ tels que $F = PQ + R$ et ($R = 0$ ou $\deg R < \deg P$).*

Corollaire 24. *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien.*

Proposition 25. *A corps $\Leftrightarrow$ $A[X]$ euclidien $\Leftrightarrow$ $A[X]$ principal*

Exemple 26. *$\mathbb{Z}[i] = \{z = a + ib \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$ est un anneau euclidien.*

Lemme 27. *Soit A un anneau euclidien. Il existe $x \in A \setminus A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Exemple 28. *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non-euclidien.*

II Arithmétique et anneaux principaux

1) Divisibilité

Définition 29. Soient $a, b \in A$. On dit que a divise b, noté $a|b$, s'il existe $c \in A$ tel que $b = ac$.

Remarque 30. $a|b \Leftrightarrow (b) \subseteq (a)$

Définition 31. a et b sont dits associés si $(a) = (b)$.

Proposition 32. *Si A est intègre, a et b sont associés si, et seulement si, il existe $u \in A^\times$ tel que $b = au$.*

Définition 33. On dit que a et b sont premiers entre eux, noté $a \wedge b = 1$, si $(d|a$ et $d|b) \Rightarrow d \in A^\times$.

Définition 34. $p \in A \setminus \{0\}$ est premier si $p \notin A^\times$ et si $p|ab \Rightarrow p|a$ ou $p|b$.

Définition 35. Si A est principal, pour $a, b \in A$, on pose :

(i) $\text{pgcd}(a, b)$ tout générateur de l'idéal $((a) \cup (b))$.

(ii) $\text{ppcm}(a, b)$ tout générateur de l'idéal $(a) \cap (b)$

On note $\text{pgcd}(a, b) = a \wedge b$ et $\text{ppcm}(a, b) = a \vee b$.

Exemple 36. *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* pgcd*.*

Théorème 37 (Bézout)**.** *Soit A principal, alors pour tous $a, b \in A \setminus \{0\}$, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = a \wedge b$.*

Lemme 38 (Gauss)**.** *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Lemme 39 (Euclide)**.** *Soit $p \in A$ irréductible, et soit $a, b \in A$, alors $p|ab \Rightarrow p|a$ ou $p|b$.*

Proposition 40. *Si A est principal, et $a, b, c, d \in A$, alors :*

(i) $(a|c$ *et* $b|c) \Leftrightarrow a \vee b|c$

(ii) $(d|a$ *et* $d|b) \Leftrightarrow d|a \wedge b$

Proposition 41. *Les éléments iréductibles d'un anneau principal sont exactement les éléments premiers.*

2) Factorialité

On suppose que A est intègre.

Définition 42. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 43. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 44. Un anneau A est dit factoriel si tout $a \in A \setminus \{0\}$ se décompose sous la forme $a = u \prod_{p \in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles.

Exemple 45. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

Proposition 46. *Tout anneau principal est factoriel.*

Proposition 47. *Dans un anneau factoriel, les* pgcd *et* ppcm *existent.*

3) Théorème des restes chinois

Lemme 48. *Soient I et J des idéaux de A tels que $A = (I, J)$. On a alors $A/(IJ) \cong A/I \times A/J$.*

Corollaire 49. *Soit A un anneau principal, et soient $a_1, \ldots, a_n \in A \setminus \{0\}$ non-inversibles et premiers entre eux deux à deux. Alors $A/(a_1 \ldots a_n)$ est isomorphe à $A/(a_1) \times \ldots \times A/(a_n)$.*

Application 50. $\begin{cases} x \equiv 2 \ [4] \\ x \equiv 3 \ [5] \\ x \equiv 1 \ [9] \end{cases} \Leftrightarrow x = 118 + 180k$ *pour* $k \in \mathbb{Z}$.

III Entiers de corps quadratiques

1) Généralités

Définition 51. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ et sans facteur carré, et soit $\sqrt{d}$ une racine carrée de d dans $\mathbb{C}$. $\mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Q} \right\}$ est un sous-corps de $\mathbb{C}$, appelé corps quadratique. On note $\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Z} \right\}$. C'est un sous-anneau de $\mathbb{Q}[\sqrt{d}]$.

Définition 52. Soit $z = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. On définit :

(i) son conjugué par $\overline{z} = a - b\sqrt{d}$.

(ii) sa trace par $\mathrm{tr}(z) = z + \overline{z} = 2a$.

(iii) sa norme par $N(z) = z\overline{z} = a^2 - db^2$.

Définition 53. On dit que $z = a + b\sqrt{d}$ est un entier de $\mathbb{Q}[\sqrt{d}]$ si a et b sont des entiers. On note A_d l'ensemble des entiers de $\mathbb{Q}[\sqrt{d}]$.

Définition 54. z est entier si, et seulement si, $\mathrm{tr}(z)$ et $N(z)$ sont entiers.

Proposition 55. *A_d est un anneau intègre.*

Théorème 56. $A_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *si* $d \equiv 1[4]$.
$A_d = \mathbb{Z}[\sqrt{d}]$ *si* $d \equiv 2[4]$ *ou* $d \equiv 3[4]$.

2) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss

Proposition 57. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 58. $\mathbb{Z}[i]$ *est un anneau euclidien.*

Définition 59. On note $\Sigma = \left\{n = a^2 + b^2 \,\middle|\, a, b \in \mathbb{N}\right\}$.

Lemme 60. *Soit p premier impair. Alors $p \in \Sigma$ si, et seulement si, p est réductible dans $\mathbb{Z}[i]$.*

Lemme 61. Σ *est stable par multiplication.*

Théorème 62. *Soit p premier impair. Alors $p \in \Sigma$ ssi $p \equiv 1[4]$.*

Corollaire 63 (Théorème des deux carrés)**.** *Soit $n \in \mathbb{N}*$. On le décompose en produit de facteurs premiers : $n = \prod_{p\in\mathbb{P}} p^{v_p n}$. Alors :*

$$n \in \Sigma \Leftrightarrow (\forall p \in \mathbb{P}, p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$$

IV Irréductibilité des polynômes de $\mathbb{Z}[X]$

On suppose que A est factoriel. On considère $\mathbb{K} = \mathrm{Frac}(A)$.

Définition 64. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 65. *Le produit de deux polynômes primitifs est primitif.*

Lemme 66. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 67. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 68 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 69. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

Développements

— Théorème des deux carrés (57,58,60,61,62,63) [Per96]

— Critère d'Eisenstein (65,66,67,68) [FGN13a]

Références

[Com98] F. Combes. *Algèbre et géométrie.* Bréal
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini