Leçon 122 : Anneaux principaux. Exemples et applications.

RM
2022-2023

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

1 Arithmétique dans les anneaux

1.1 idéal et divisibilité

Définition 1 : Un idéal de $\mathbb{A}$ est un sous groupe I de $(\mathbb{A},+)$ tel que $\forall (a,b)\in I\times\mathbb{A}, ab\in I$. On dit que I est absorbant pour le produit.

Exemple 2 : • $\{0\}$ et $\mathbb{A}$ sont des idéaux de $\mathbb{A}$.
- Si $(I_k)_{k\in K}$ est une famille d'idéaux de $\mathbb{A}$, $I=\cap_{k\in K}I_k$ est alors un idéal.
- Si $\varphi:\mathbb{A}\to\mathbb{B}$ est un morphisme d'anneaux, son noyau $ker(\varphi)$ est un idéal de $\mathbb{A}$.

Définition 3 : Pour tous $a\in\mathbb{A}$, l'ensemble $(a)=a.\mathbb{A}=\{qa|q\in\mathbb{A}\}$ des multiples de a dans $\mathbb{A}$ est un idéal. Un tel idéal est dit principal et on dit que c'est l'idéal engendré par a.

Remarque 4 : Si $a\in\mathbb{A}$ est inversible, alors $(a)=\mathbb{A}$.

Définition 5 : Un idéal I de $\mathbb{A}$ est dit premier s'il est distinct de $\mathbb{A}$ et si on a $ab\in I$ si et seulement si $a\in I$ ou $b\in I$.
Un idéal I de $\mathbb{A}$ est dit maximal s'il est distinct de $\mathbb{A}$ et si I et $\mathbb{A}$ sont les seuls idéaux de $\mathbb{A}$ qui contiennent I.

Exemple 6 : Si $\mathbb{A}=\mathbb{Z}$, $I=n\mathbb{Z}$ est premier si et seulement su $n=0$ ou n premier.
Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premiers.

Remarque 7 : On a qu'un idéal maximal est premier.

Théorème 8 : *i*) Un idéal I de $\mathbb{A}$ est maximal si et seulement si l'anneau quotient $\mathbb{A}/I$ est un corps.
ii) Un idéal I de $\mathbb{A}$ est premier si et seulement si l'anneau quotient $\mathbb{A}/I$ est intègre.

Définition 9 : Soient $a,b\in\mathbb{A}$. On dit que a divise b et on écrit $a|b$ si et seulement si il existe $c\in A$ avec $b=ca$.
Proposition 10 : On a : $b|a\Leftrightarrow(a)\subset(b)$.

Définition 11 : Soient $a,b\in A$, on dit que a et b sont associés si et seulement si il existe $u\in\mathbb{A}^\times$ tel que $a=ub$. C'est un relation d'équivalence.

Définition 12 : Un élément $p\in\mathbb{A}$ est dit irréductible si $p\neq 0$, p n'est pas inversible et $p=ab$ implique que a ou b est inversible.
Il est dit premier si $p\neq 0$, p n'est pas inversible et $p|ab$ implique que $p|a$ ou $p|b$.

Lemme 13 : Un élément premier est un élément irréductible.

Exemple 14 : Les irréductible de $\mathbb{Z}$ sont les nombres premiers.

Définition 15 : Soient $a,b\in\mathbb{A}$. On dit que
- $d\in\mathbb{A}$ est un pgcd de a et b noté $d=a\wedge b$ si $\forall c\in\mathbb{A}$ divisant a et b, alors c divise b.
- $m\in\mathbb{A}$ est un ppcm de a et b noté $a\vee b$ si $\forall c\in\mathbb{A}$ tel que a et b divise c, alors m divise c.

On dit que a et b sont premier entre eux si leurs pgcd est un inversible de $\mathbb{A}$.

Remarque 16 : On peut étendre cette définition à n éléments de $\mathbb{A}$. Il faut faire attention que dans le cas général, le pgcd et le ppcm n'existe pas toujours.

Proposition 17 : Deux pgcd (ppcm) de a et b sont associées.

1.2 Anneaux principaux

Définition 18 : On dit que l'anneau $\mathbb{A}$ est principal, s'il est intègre et si tout idéal de $\mathbb{A}$ est principal.

Exemple 19 : Un corps est un anneau principal. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont tous les deux principaux.

Proposition 20 : Soit A un anneau. Alors $\mathbb{A}[X]$ est principal si et seulement si A est un corps.

Remarque 21 : On en déduit que $\mathbb{Z}[X]$ n'est pas principal. En effet, l'idéal $(2,X)$ dans $\mathbb{Z}[X]$ n'est pas principal.

On considère maintenant que $\mathbb{A}$ est principal.

Théorème (de Bézout) 22 : Soit $a,b\in\mathbb{A}^*$. Alors il existe $d\in\mathbb{A}$ tel que $(d)=(a)+(b)$. On alors que d est un pgcd de a,b, et donc tout éléments dans un anneau principal admettent un pgcd. On en déduit qu'il existe $\lambda,\mu\in\mathbb{A}$ tel que $d=\lambda a+\mu b$.

Corollaire 23 : Si $a, b \in \mathbb{A}$ sont premiers entre eux, alors $(a) + (b) = (1)$, c'est-à-dire il existe $\lambda, \mu \in \mathbb{A}$ tel que $1 = \lambda a + \mu b$.

Théorème (de Gauss) 24 : Soient a, b, c dans $\mathbb{A}$ non nuls. Si a divise bc et a est premier avec b, alors a divise c.

Lemme 25 : Dans un anneau principal, on a équivalence entre être un élément premier et irréductible.

Développement 26 : Soit $\mathbb{A}$ un anneau unitaire principal. Soit $(a_j)_{1\leq j\leq r}$ des éléments non nuls inversibles deux à deux premiers entre eux avec $a = \prod_{i=1}^{r} a_j$. Alors l'application $\varphi : x \in \mathbb{A} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \prod_{i=1}^{r} \frac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux surjectif de noyau $Ker(\varphi) = (a)$. et φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : \pi(x) \in \frac{\mathbb{A}}{(a)} \mapsto (\pi_j(x))_{1\leq j\leq r} \in \prod_{i=1}^{r} \frac{\mathbb{A}}{(a_j)}$$

d'inverse

$$\overline{\varphi}^{-1} : (\pi_j(x_j))_{1\leq j\leq r} \in \prod_{i=1}^{r} \frac{\mathbb{A}}{(a_j)} \mapsto \overline{\sum_{i=1}^{r} x_i u_i b_i} \in \frac{\mathbb{A}}{(a)}$$

où $(u_j)_{1\leq j\leq r}$ est une suite d'éléments de $\mathbb{A}$ telle que $\sum_{i=1}^{r} u_j b_j = 1$.

Application (Calcul de $\varphi(n)$) 27 : Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < ... < p_r$ premiers et les α_i entiers naturels non nuls, on a alors :

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

1.3 Anneau factoriel

Définition 28 : L'anneau A est factoriel ssi :
- A est intègre.
- $\forall a \in A^*$, a s'écrit sous la forme $a = u \prod_{p\in P} p^{\nu_p(a)}$, avec $u \in A^\times$, $\nu_p(a) \in \mathbb{N}$ et les $\nu_p(a)$ nuls, sauf un nombre fini.
- cette écriture est unique à permutation près.

Exemple 29 : On peut prendre comme système de représentant pour $\mathbb{K}[X]$ les polynômes unitaires irréductibles.

Proposition 30 : Un anneau principal est factoriel.

Proposition 31 : Pour $a, b \neq 0$ on a :

$$a|b \Rightarrow \forall p \in P, \nu_p(a) \leq \nu_p(b)$$

Théorème 32 : Un anneau factoriel A est à pgcd. Plus précisément, pour a, b de A^* non inversible, avec $a = u \prod_{k=1}^{r} p_k^{\nu_{p_k}(a)}$, $b = v \prod_{k=1}^{r} p_k^{\nu_{p_k}(b)}$ avec u, v inversibles, on a :

$$a \wedge b = \prod_{k=1}^{r} p_k^{min(\nu_{p_k}(a), \nu_{p_k}(b))} \quad \text{et} \quad a \vee b = \prod_{k=1}^{r} p_k^{max(\nu_{p_k}(a), \nu_{p_k}(b))}$$

Exemple 33 : Dans $\mathbb{Z}$ on a $1350 = 2 \times 3^3 \times 5^2$ et $360 = 2^3 \times 3^2 \times 5$.
On en déduit que $1350 \wedge 360 = 2 \times 3^2 \times 5 = 90$ et $1350 \vee 360 = 2^3 \times 3^3 \times 5^2 = 5400$.

Remarque 34 : On déduit du théorème précédent que pour $\lambda \in A^*$, on a $pgcd(\lambda a, \lambda b) = \lambda pgcd(a, b)$. De même pour le ppcm.

Théorème (Gauss) 35 : Si A est factoriel, $A[X]$ est factoriel.

Dev 1

Lemme (Gauss) 36 : On pose pour $p \in A[X]$ non nul, le contenue de P noté $c(P) := pgcd(a_0, ..., a_n)$ pour $P = \sum_{i=0}^{n} a_i X^i$. On dit que P est primitif si $c(P) = 1$. On a alors $c(PQ) = c(P)c(Q)$ modulo A^*.

Proposition 37 : Les polynômes $P(X) \in A[X]$ irréductibles dans $A[X]$ sont :
- 1) les constantes $p \in A$, irréductibles dans A.
- 2) les polynômes $P(X)$, de degré supérieur ou égale à 1, primitifs et irréductibles dans $K[X]$.

2 Anneaux euclidien

Définition 38 : Un anneau commutatif et intègre A est dit euclidien, s'il existe un stathme $\varphi : A^* \mapsto \mathbb{N}$ tel que pour tout couple (a, b) d'éléments de A avec $b \neq 0_A$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0_1$ ou $r \neq 0_A$ et $\varphi(r) < \varphi(b)$.

Théorème 39 : Un anneau euclidien est principale, donc factoriel. On conserve alors tous les résultats précédent.

Remarque 40 : Un anneau principal n'est pas forcément euclidien, en prenant l'exemple de $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ qui est principal mais non euclidien.

Lemme 41 : Soient a, b dans A^* et r un reste dans la division euclidienne de a par b. On a alors $a \wedge b = b$ si $r = 0_A$ ou $a \wedge b = b \wedge r$ sinon.

Proposition (Algorithme d'Euclide étendue) 42 : L'algorithme d'Euclide étendue permet de trouver ces coefficients u et v dans la relation de bézout.
Soit a, b dans A non nuls. Pour $i \geq 0$, tant que $r_{i+1} \neq 0$:
- $r_{i+2} = reste(r_i, r_{i+1})$
- $q_{i+2} = quotient(r_i, r_{i+1})$
- $u_{i+2} = u_i - u_{i+1}q_{i+2}$
- $v_{i+2} = v_i - v_{i+1}q_{i+2}$

avec $(r_0, r_1) = (a, b)$,$(u_0, u_1) = (1, 0)$ et $(v_0, v_1) = (0, 1)$.
De la même manière que pour Euclide, on a $r_n = au_n + bv_n$ et donc comme $r_n = pgcd(a, b)$, on a bien les coefficients u et v voulus.

Exemple 43 : Les coefficients de Bézout pour 111 et 47 sont $u = -11$ et $v = 26$. On a bien $1 = 111u + 47v$.

2.1 Application aux théorèmes des deux carrés de Fermat

Définition 44 : On pose $\sum = \{n \in \mathbb{N} | n = a^2 + b^2; a, b \in \mathbb{N}\}$ et $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} | a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.
Exemple 45 : On a $0, 1, 2, 4, 5, 8, 9, 10$ dans $\sum$ mais pas $3, 6, 7, 11, 12$.

Remarque 46 : Si $n \equiv 3 \pmod 4$, alors $n \notin \sum$.

Proposition 47 : On a $\mathbb{Z}[i]^\times = \{-1, +1, -i, +i\}$.

Proposition 48 : L'ensemble $\sum$ des sommes de deux carrés est stable par multiplication.

Proposition 49 : L'anneau $\mathbb{Z}[i]$ est euclidien, donc principal.

Théorème 50 : Soit $p \in \mathbb{N}$ un nombre premier. On a alors que $p \in \sum$ si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.

Lemme 51 : On a que $p \in \sum$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Exemple 52 : On a bien que $41 = 5^2 + 4^2$,$53 = 7^2 + 2^2$,$61 = 6^2 + 5^2$ sont dans $\sum$.

Développement (Théorèmes des deux carrés de Fermat) 53 : Soit $n \in \mathbb{N}^*$ avec $n > 1$, on décompose n en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Alors on a $n \in \sum$ si et seulement si $v_p(n)$ pair pour $p \equiv 3 \pmod 4$.

Dev 2

3 Application à la résolution d'équations diophantiennes

Définition 54 : On appelle équation diophantienne une équation polynomiales à coefficients entiers telles que les solutions soit des solutions entières.

Exemple 55 : Soient $n \geq 2$ un entier, a un entier naturel non nul et b un entier relatif. Alors $ax \equiv b \pmod n$ est une équation diophantienne.

Proposition 56 : Dans le cas ou $b = 1$, alors cette équation a des solutions si et seulement si $\overline{a}$ est inversible dans dans $\mathbb{Z}/n\mathbb{Z}$, ie $a \wedge n = 1$.
L'algorithme d'Euclide nous permet alors de trouver une solutions particulière $x_0 \in \mathbb{Z}$.

Corollaire 57 : L'ensemble des solutions de $ax \equiv 1 \pmod n$ si $a \wedge n = 1$ est alors $S = \{x_0 + kn | k \in \mathbb{Z}\}$.

Proposition 58 : Si $a \wedge n = 1$ et $b \in \mathbb{Z}$, alors $u_0 = bx_0$ est solution particulière de $ax \equiv b \pmod n$ où x_0 est une solution particulière de $ax \equiv 1 \pmod n$. Les solutions sont alors $S = \{bx_0 + kn | k \in \mathbb{Z}\}$.

Proposition 59 : Dans le cas générale, on a pour $\delta = a \wedge n$ avec $a = \delta a'$,$n = \delta n'$ que a' et n' sont premiers entre eux. L'équation diophantienne à alors des solutions si et seulement si δ divise b. L'ensemble des solutions est $S = \{b'x'_0 + kn' | k \in \mathbb{Z}\}$, ou x'_0 est une solution particulière de $a'x \equiv 1 \pmod{n'}$ et $b = \delta b'$.

Remarque 60 : On peut ici remarquer que $ax \equiv b \pmod n$ revient à il existe $y \in \mathbb{Z}$ tel que $ax - ny = b$. Résoudre cette équation diophantienne est donc équivalente à résoudre $ax + by = c$ avec $a, b, c \in \mathbb{Z}$.

Remarque 61 : Le théorème chinois nous permet alors de résoudre certains systèmes de congruences. Il nous garantit alors une de l'existence d'une solution et même son unicité dans $\mathbb{Z}/n\mathbb{Z}$. On alors que toutes solutions sont de la $x_0 + kn$ ou x_0 est une solution particulière.

Exemple 62 : On considère le système suivant

$$\begin{cases} k \equiv 2 \pmod 4 \\ k \equiv 3 \pmod 5 \\ k \equiv 1 \pmod 9 \end{cases}.$$

On a alors comme solution $k = 118 + 180q$ ou $q \in \mathbb{Z}$.

Remarque 63 : Dans la pratique, pour trouver la solution de ce système, on pose $x = x_1 + 4x_2 + x_3 20$ et on cherche x_1, x_2, x_3 pour avoir une solution particulière.

Références :

1. Cours d'algèbre Perrin
2. Algèbre et géométrie Rombaldi
3. Algèbre Gourdon
4. Calcul formel Saux-Picard