Leçon 122 : Anneaux principaux. Exemples et applications.

Soit $(A, +, .)$ un anneau commutatif intègre unitaire.

1 Un anneau particulier

1.1 Idéaux et anneaux principaux

Définition 1 (GOU 31)**.** Soit $I \subset A$. On dit que I est un idéal de l'anneau A si

1. $(I, +)$ est un sous-groupe de $(A, +)$
2. $\forall (x, a) \in I \times A$, $ax \in I$ et $xa \in I$.

Définition 2 (GOU 32)**.** Un idéal I de A est dit principal s'il existe $x \in A$ tel que $I = xA$. On note alors $I = (x)$ et on dit que I est engendré par x.

Exemple 3 (GOU 32)**.** Soit $n \in \mathbb{Z}$. $n\mathbb{Z}$ est un idéal principal de $(\mathbb{Z}, +, .)$.

Définition 4 (GOU 32)**.** Un anneau A est dit principal s'il est commutatif, unitaire, intègre et si tous les idéaux de A sont principaux.

Exemple 5 (BER405)**.** Les seuls sous-groupes de $(\mathbb{Z}, +)$ étant les $n\mathbb{Z}$, on en déduit que ce sont les seuls idéaux de $\mathbb{Z}$, qui sont des idéaux principaux. Ainsi $\mathbb{Z}$ est un anneau principal.

Définition 6 (ROM223)**.**

Un idéal de A est dit premier s'il est disctint de A et si on a $ab \in I \iff a \in I$ ou $b \in I$

Un idéal I de A est dit maximal s'il est distinct de A et si I et A sont les seuls idéaux de A qui contiennent I.

Proposition 7 (ROM 223)**.**
1. p est premier $\iff$ (p) premier.
2. Un idéal maximal est premier

Définition 8 (ROM 214 -215)**.**

$p \in A$ est dit irréductible si $p \neq 0$, p n'est pas inversible et $(p = ab) \implies$ (a ou b est inversible)

$p \in A$ est dit premier si $p \neq 0$, p n'est pas inversible et (p divise ab) $\implies$ (p divise a ou p divise b).

Proposition 9 (ROM 215)**.** Un élément premier dans un anneau intègre est irréductible.

Lemme 10 (ROM 241, ok , 2) à voir)**.** Supposons A principal.
1. Un élément $p \in A^* \setminus A^\times$ est irréductible si et seulement si il est premier.
2. Pour tout $p \in A^* \setminus A^\times$, on a : (p) premier $\iff$ p premier $\iff$ p irréductible $\iff$ (p) maximal

1.2 Cas particulier des anneaux euclidiens

Définition 11 (ROM 261)**.** L'anneau A est dit euclidien s'il existe un stathme $\varphi : A^* \to \mathbb{N}$ tel que pour tout $(a, b) \in A^2$ avevc $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0_A$ ou $r \neq 0_A$ et $\varphi(r) < \varphi(b)$.

Exemple 12 (ROM 266)**.** L'anneau $\mathbb{Z}$ est euclidien pour le stathme $\varphi : n \in \mathbb{Z}^* \mapsto |n|$.

Proposition 13 (ROM 261)**.** Un anneau euclidien est principal.

Remarque 14 (No ref). Pour montrer qu'un anneau est prinicipal on peut alors se ramener à montrer qu'il est euclidien.

Réciproque fausse : [ROM 272, 273] Soit $\omega = \frac{1+i\sqrt{19}}{2}$ et consiédrons l'anneau $\mathbb{Z}[\omega] = \{a+b\omega | (a,b) \in \mathbb{Z}^2\}$. $\mathbb{Z}[\omega]$ est principal mais pas euclidien

1.3 Lien avec les anneaux factoriels

Motivation de la partie : anneau principal est factoriel donc on hérite des bonnes propriétés

Définition 15 (ROM 224). On dit qu'un anneau A est factoriel s'il est intègre et si tout élément a non nul et non inversible s'écrit de manière unique comme produit d'éléments irréductibles. "c'est-à-dire..." garder pour question

Théorème 16 (ROM 225). A est factoriel si et seulement si :

1. toute suite croissante d'idéaux principaux de A est stationnaire
2. tout élément irréductible de A est premier

Corollaire 17 (ROM 227). Un anneau principal est factoriel.

Remarque 18. On a donc le schéma : euclidien $\implies$ principal $\implies$ factoriel

Lemme 19 (ROM 226). [d'Euclide] Dans un anneau factoriel, un élément est irréductible si et seulement si, il est premier. avoir version reformulé dans la tête

Théorème 20 (ROM 242). Soit A un anneau commutatif et unitaire. On a : $A[X]$ est euclidien $\iff$ $A[X]$ est principal $\iff$ A est un corps

Exemple 21 (No ref). $\mathbb{K}[X]$ est principal, et donc fatoriel, pour tout corps $\mathbb{K}$ commutatif.

Application 22 (ROM 604, 605). [Définition du polynôme minimal] Soit E un $\mathbb{K}-$ev ou $\mathbb{K}$ est un corps commutatif et $u \in \mathcal{L}(E)$. On définit le polynôme minimal de u, noté μ_u, par le générateur unitaire de l'idéal $I_u = \{P(u) | P \in \mathbb{K}[X]\}$. En particulier $dim(\mathbb{K}[u]) = deg(\mu_u)$

Ex non factoriel : $\mathbb{Z}[i\sqrt{n}]$

2 Arithmétique sur un anneau principal

2.1 Divisibilité, PGCD, PPCM

Définition 23 (BER 515). Soient $a, b \in A$. On dit que a divise b s'il existe $x \in A$ tel que $b = ax$. On le note $a|b$

Proposition 24 (BER 515). $a|b \iff (b) \subset (a)$

Définition 25 (ROM 242). On dit que $a_1, .., a_r$ admettent un plus grand commun diviseur s'il existe $\delta \in A^*$ tel que :

$$\begin{cases} \forall k \in \{1, ..., r\}, \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, .., a_r \text{ divise } \delta \end{cases}$$

Définition 26 (ROM 246). On dit que $a_1, .., a_r$ admettent un plus petit commun multiple s'il existe $\mu \in A^*$ tel que :

$$\begin{cases} \forall k \in \{1, ..., r\}, \mu \text{ est multiplie de } a_k \\ \text{tout multiple commun à } a_1, .., a_r \text{ multiple } \mu \end{cases}$$

Notation 27 (ROM). On note respectivement $pgcd(a_1, ..., a_r)$ (ou encore $a_1 \wedge ... \wedge a_r$) et $ppcm(a_1, ..., a_r)$ (ou encore $a_1 \vee ... \vee a_r$).

Proposition 28 (ROM). Le ppcm et le pgcd sont associatifs et commutatifs.

Contre-exemple 29 (No ref). Dans l'anneau, $\mathbb{Z}[i\sqrt{3}]$, $4 = (1+i\sqrt{3})(1-i\sqrt{3})$ et $2(1+i\sqrt{3})$ n'ont pas de pgcd. Ceci montre qu'il n'y a pas toujours existence du $pgcd$.

Proposition 30 (ROM 243). Dans un anneau principal A, on a toujours existence d'un pgcd. Plus précisément, il existe $\delta \in A^*$ tel que $(a_1, ..., a_r) = (\delta)$ et cet élément s'écrit $\delta = \sum_{i=1}^{r} u_k a_k$ où $u_1, .., u_r \in A$ et $\delta = pgcd(a_1, ..., a_r)$.

Théorème 31 (ROM 244). Dans un anneau factoriel A, on a toujours existence d'un pgcd. Plus précisément, pour $a = u \prod_{k=1}^{r} p_k^{m_k}$, et

$b = v \prod_{k=1}^{r} p_k^{n_k}$ dans $A^* \setminus A^\times$, où u, v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels. On a $a \wedge b = \prod_{k=1}^{r} p_k^{min(m_k,n_k)}$.

Définition 32 (ROM 245)**.** On dit que $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si leur pgcd est dans $A^\times$.

Proposition 33 (ROM 245)**.** Soit d un diviseur commun à $a_1, ..., a_r$. Pour tout k compris entre 1 et r, considérons $\alpha_k \in A$ tel que $a_k = d\alpha_k$. On a : $d = pgcd(a_1, ..., a_r) \iff pgcd(\alpha_1, .., \alpha_r) = 1$

2.2 Résultats importants des anneaux principaux

Désormais on considère que A est un anneau prinicipal.

Théorème 34 (ROM 247)**.** [Bézout] Les $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si et seulement si il existe $(u_1, ..., u_k) \in A^r$ tel que $\sum_{k=1}^{r} u_k a_k = 1$.

Application 35 (GOU 185)**.** [lemme des noyaux] Sot $\mathbb{K}$ un corps. Soient $P = P_1...P_r \in \mathbb{K}[X]$ où les P_i sont premiers entre eux deux à deux. Soit $f \in \mathcal{L}(E)$ où E est un $\mathbb{K}-$ev. On a :

$$ker(P(f)) = ker(P_1(f)) \oplus ... \oplus ker(P_k(f))$$

Théorème 36 (ROM 245)**.** [Gauss] Soit $a, b \in A$. a et b sont premier entre eux si et seulement si pour tout $c \in A^*$, $a|bc$ implique $a|c$.

THM suivants : Écrire avec A à la place de $\mathbb{Z}$ et dire que dev avec $\mathbb{Z}$

Théorème 37 (thm chinois)**.** [TL1 149, DEV 1] Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. Étant donné des entiers $a_1, .., a_r$, considérons le système de congruences :
$(S) : x \equiv a_i \ [m_i] \ (i = 1, ..., r)$
Ce système possède une solution $x \in \mathbb{Z}$ qui est unique modulo M.

Corollaire 38 (TL1 150)**.** Soient $m_1, .., m_r \geq 2$ des entiers premiers entre eux deux à deux ($r \geq 2$). On note M leur produit. On a alors :

$$\mathbb{Z}/M\mathbb{Z} \simeq \mathbb{Z}/m_i\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$$

Si time, mettre algorithme d'Euclide en annexe

3 Applications

3.1 Entiers de Gauss

Définition 39 (ROM 267)**.** On appelle anneau des entiers de Gauss l'ensemble $\mathbb{Z}[i] = \{a + ib | (a, b) \in \mathbb{Z}^2$. C'est un sous-anneau de $\mathbb{C}$

Proposition 40 (ROM 267)**.** $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe. Il est donc commutatif et intègre comme $\mathbb{C}$.

Proposition 41 (ROM 267)**.** $\mathbb{Z}[i]$ est euclidien (donc principal) pour le stathme $\varphi : a + ib \in \mathbb{Z}[i]^* \mapsto a^2 + b^2$

Application 42 (ROM 268, 269)**.** [théorème des deux carrés de Fermat, ADMIS]

Un nombre premier p est somme de deux carré si et seulement si il est égal à 2 modulo 4

Un entier $n \in \mathbb{N}^*$ est somme de deux carrés si et seulement si ses éventuels diviseurs premiers congrus à 3 modulo 4 qui apparaissent dans sa décomposition en facteurs premiers y figurente avec un exposant pair.

3.2 Polynômes cyclotomiques

Définition 43 (TL1 309)**.** Le $n-$ème polynôme cyclotomique est le polynôme unitaire ϕ_n dont les racines sont les racines primitives $n-$ème de l'unité : $\phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$

Proposition 44 (TL1 309, PER 80)**.** $deg(\phi_n) = \varphi(n)$

Exemple 45 (TL1 309)**.** 1. $\phi_1(X) = X - 1$

2. Si p est premier, $\phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + ... + X + 1$
3. $\phi_4(X) = X^2 + 1$

Proposition 46 (TL1 309)**.** Soit $n \geq 1$. Alors : $X^n - 1 = \prod_{d|n} \phi_d$

Théorème 47 (PER 82, DEV 1)**.** Pour $n \geq 1$, $\phi_n(X) \in \mathbb{Z}[X]$ est un polynôme irréductible et unitaire, donc irréductible dans $\mathbb{Q}[X]$ également.

3.3 Équations diophantiennes

On considère toujours n un entiers supérieur ou égal à 2.

Définition 48 (ROM 289)**.** Une équation diophantienne est une équation à solutions dans $\mathbb{Z}$ de la forme $ax \equiv b\ [n]$ où $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Exemple 49. Si $b = 1$, cette équation a des solutions si et seulement si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème 50 (ROM 290)**.** Soit $\delta = pgcd(a, n)$. L'équation diophantienne $ax \equiv b\ [n]$ a des solutions entières si et seulement si δ divise b. Dans ce cas, l'ensemble des solutions est $S = \{b'x'_0 + kn' | k \in \mathbb{Z}\}$ où x_0 est une solution particulière de $a'x \equiv 1\ [n]$.

Exemple 51 (No ref)**.** $9x \equiv 15\ [21]$ admet une unique solution modulo 21

Application 52 (un peu ROM 290, 291)**.** Le théorème chinois permet de résoudre des système d'équations diophantienne. Le système

$$\begin{cases} k \equiv a_1\ [n_1] \\ \quad ... \\ k \equiv a_r\ [n_r] \end{cases}$$

a toujours une infinité de solutions si la famile $(a_i)_{1 \leq i \leq r}$ est une famille d'éléments 2 à 2 premiers entre eux. Cette solution est unique modulo $n = n_1..n_r$.

Exemple 53 (BER 469, A voir selon place et temps)**.** Considérons le système d'équations diophantiennes :

$$\begin{cases} k \equiv 1\ [3] \\ k \equiv 2\ [4] \\ k \equiv -1\ [7] \end{cases}$$

$3, 4$ et 7 sont deux à deux premiers entre eux donc ce système a des solutions. La 1ère équation donne $x = 1 + 3y, y \in \mathbb{Z}$. En reportant dans la 2−ème, on obtient $3y \equiv 1[4]$. On a alors $y \equiv -1\ [4]$, soit $y = -1 + 4z, z \in \mathbb{Z}$ donc $x = 1 + 3(-1 + 4z) = -2 + 12z$ avec $z \in \mathbb{Z}$. En reportant dans la dernière égalité on a $12z \equiv 1\ [7]$ soit $5z \equiv 1[7]$ puis $z \equiv 3[7]$ car 3 est l'inverse de 5 modulo 7. Ainsi $z = 3 + 7t, t \in \mathbb{Z}$ et finalement $x =_2 +12(3 + 7t) = 34 + 84t, t \in \mathbb{Z}$.

Application 54 (ROM 291)**.**

$$\begin{cases} k \equiv a_1\ [n_1] \\ k \equiv a_2\ [n_2] \end{cases}$$

a des solutions si et seulement si $\delta = n_1 \wedge n_2$ divise $a_2 - a_1$

Une autre app du thm chinois : Si $n \geq 2$ avec $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, on a $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$.