ANNEAUX EUCLIDIENS, PRINCIPAUX, FACTORIELS

Chapitre 6

Ce polycopié est très largement inspiré du polycopié utilisé par mon prédécesseur K. Koufany, que je remercie pour son travail de rédaction.

Table des matières

Dans ce chapitre les anneaux considérés seront commutatifs et unitaires.

1. Anneaux euclidiens

***Définition 1.1* (Anneau euclidien).** — *On appelle* **anneau euclidien**, *un anneau A intègre, possédant une division euclidienne, dans le sens suivant : il existe une application θ, appelée stathme euclidien, de A dans $\mathbb{N}$, telle que pour tout $a \in A$ et pour tout $b \in A \setminus \{0_A\}$, il existe $q, r \in A$, tel que*

$$a = bq + r \text{ avec } \theta(r) < \theta(b). \tag{1}$$

Exemples 1.2. — (a) L'anneau $\mathbb{Z}$ est euclidien pour le stathme $\theta : n \mapsto |n|$ de $\mathbb{Z}$ dans $\mathbb{N}$.

(b) Les anneaux de polynômes $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont euclidiens pour le stathme $\theta : P \mapsto \mathrm{d}^\circ(P) + 1$ (avec la convention que le polynôme nul est de degré -1).

(c) L'anneau des **entiers de Gauss**, $\mathbb{Z}[i] = \{a+ib,\ \ a, b \in \mathbb{Z}\}$, est euclidien pour le stathme $\theta(z) = |z|^2$.

(d) L'anneau $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2},\ \ a, b \in \mathbb{Z}\}$ est euclidien pour le stathme $\theta(z) = |z|^2$.

Démonstration. — Les points (a) et (b) sont faciles à vérifier. Nous montrons (d), et laissons le soin à l'étudiant d'adapter cette preuve pour (c). Comme $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de $\mathbb{C}$, il est donc commutatif, unitaire ($1 = 1 + 0 \times i \times \sqrt{2}$) et intègre.

Pour $z = a + ib\sqrt{2}$, on pose $\theta(z) = |z|^2 = a^2 + 2b^2$. Il est clair que $\theta : \mathbb{Z}[i\sqrt{2}] \to \mathbb{N}$ et que θ est une application multiplicative : $\forall z, w \in \mathbb{Z}[i\sqrt{2}]$, $\theta(zw) = \theta(z)\theta(w)$.

Soit $z, w \in \mathbb{Z}[i\sqrt{2}]$ avec $w \neq 0$. Montrons qu'il existe $q, r \in \mathbb{Z}[i\sqrt{2}]$ tels que $z = qw + r$ avec $\theta(r) < \theta(w)$. Cette dernière inégalité est équivalente à $\frac{\theta(r)}{\theta(w)} < 1$ ou encore à $\left|\frac{r}{w}\right| < 1$, soit $\left|\frac{z}{w} - q\right| < 1$.

Le quotient z/w peut s'écrire $\frac{z}{w} = u + iv\sqrt{2}$, avec $u, v \in \mathbb{Q}$. Il existe $x \in \mathbb{Z}$ tel que $|u - x| < \frac{1}{2}$, pour cela il suffit de prendre

$$x = \begin{cases} \lfloor u \rfloor & \text{si } \ \lfloor u \rfloor \leq u \leq \lfloor u \rfloor + \frac{1}{2} \\ \lfloor u \rfloor + 1 & \text{si } \ \lfloor u \rfloor + \frac{1}{2} \leq u < \lfloor u \rfloor + 1 \end{cases}$$

De même, il existe $y \in \mathbb{Z}$ tel que $|v - y| < \frac{1}{2}$.

Posons alors $q = x + iy\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$. On a

$$\begin{aligned} \theta(\frac{z}{w} - q) = \left|\frac{z}{w} - q\right|^2 &= \left|(u + iv\sqrt{2}) - (x + iy\sqrt{2})\right|^2 \\ &= \left|(u - x) + i(v - y)\sqrt{2}\right|^2 \\ &= (u - x)^2 + 2(v - y)^2 \\ &\leq \frac{1}{4} + 2 \times \frac{1}{4} = \frac{3}{4} \\ &< 1 \end{aligned}$$

Posons maintenant $r = z - wq$. C'est aussi un élément de $\mathbb{Z}[i\sqrt{2}]$. Donc $z = wq + r$ et $\theta(r) = \theta(z - wq) = \theta(w)\theta(\frac{z}{w} - q) < \theta(w)$. □

Remarque 1.3. — *Il faut noter que q et r ne sont pas en général uniques. Par exemple, il existe quatre divisions possibles de $19 + 76i\sqrt{2}$ par $50 + 2i\sqrt{2}$. En effet,*

$$\frac{19 + 76i\sqrt{2}}{50 + 2i\sqrt{2}} = \frac{1}{2} + \frac{3}{2}i\sqrt{2}$$

On peut prendre $q = 0 + i\sqrt{2}$ *ou* $q = 0 + 2i\sqrt{2}$ *ou* $q = 1 + i\sqrt{2}$ *ou* $q = 1 + 2i\sqrt{2}$ *et les restes correspondants.*

2. Anneaux principaux

Soit A un anneau commutatif unitaire. L'idéal engendré par un élément a de A est l'ensemble $aA = \{ax \mid x \in A\}$ des multiples de a, d'après la Proposition 4.6 du chapître sur les anneaux en général. Supposons A intègre. Les générateurs de l'idéal aA sont les éléments associés à a, de la forme au où $u \in A^\times$. En effet le cas où $aA = \{0\}$ est trivial. Supposons $aA \neq \{0\}$, alors $a \neq 0$. Si $aA = bA$, il existe $u \in A$ tel que $b = au$ et il existe $v \in A$ tel que $a = bv$. On en déduit que $a = auv$ et ensuite que $1 = uv$ car A est intègre. Ainsi $u \in A^\times$ et a et b sont associés.

***Définition 2.1* (Anneau principal).** — *Soit A un anneau commutatif avec unité.*
Un idéal I de A est dit **principal***, s'il existe $a \in A$ tel que $I = aA$.*
L'anneau A est dit **principal** *s'il est intègre et si tout idéal de A est principal.*

Dans un anneau commutatif unitaire A, les idéaux $\{0\} = 0A$ et $A = 1A$ sont principaux. Un corps commutatif K est un anneau principal, car $\{0\}$ et K sont ses seuls idéaux.

Exemple 2.2. — L'anneau $\mathbb{Z}$ est intègre. De plus nous avons vu que ses seuls idéaux sont de la forme $n\mathbb{Z}$, donc sont principaux. On en déduit l'anneau $\mathbb{Z}$ est principal.

Théorème 2.3. — *Tout anneau euclidien est principal.*

Démonstration. — Si l'anneau est euclidien, il est intègre. Montrons que tout idéal I de A est principal. Si $I = \{0\}$, alors I est principal. Supposons $I \neq \{0\}$. Il existe $b \in I$ tel que $\theta(b)$ soit le plus petit élément de $\{\theta(x) \mid x \in I \setminus \{0\}\}$. On a $bA \subset I$. D'autre part, pour tout $a \in I$, la division euclidienne de a par b donne $q, r \in A$ tels que $a = bq + r$ et $\theta(r) < \theta(b)$. On a $r = bq - a \in I$. Le minimum de θ sur les éléments non nuls de I étant $\theta(b)$, on obtient $r = 0$, $a = bq \in bA$ et donc $I = bA$. □

Exemples 2.4. — (a) Les anneaux $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[i]$ sont principaux, car euclidiens.

(b) La réciproque du Théorème 2.3 n'est en général pas vraie. Il existe des anneaux principaux qui ne sont pas euclidiens. Par exemple, l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien. Voir la feuille d'exercices.

(c) L'anneau $\mathbb{Z}[X]$, des polynômes à coefficients entiers, n'est pas principal.

Démonstration. — En effet, considérons l'idéal de $\mathbb{Z}[X]$ donné par

$$I = \langle 2\rangle + \langle X\rangle = \{2P + XQ,\ P, Q \in \mathbb{Z}[X]\}$$

et montrons qu'il n'est pas principal. Pour cela, on observe d'abord que

$$I = \{A \in \mathbb{Z}[X],\ A(0) \text{ est pair}\}.$$

En effet, soit $A \in I$, alors il existe $P, Q \in \mathbb{Z}[X]$ tels que $A(X) = 2P(X) + XQ(X)$. En particulier $A(0) = 2P(0)$ est un entier pair. Réciproquement, si $A \in \mathbb{Z}[X]$ est tel que $A(0)$ est pair, alors en écrivant $A(X) = a_0 + a_1X + \cdots + a_nX^n$ on a $a_0 = 2k$ est un entier pair et $A(X) = 2k + X(a_1 + a_2X + \cdots + a_nX^{n-1}) \in \langle 2\rangle + \langle X\rangle$.

Supposons maintenant que I est principal, alors il existe $P_0 \in \mathbb{Z}[X]$ tel que $I = \langle P_0\rangle = P_0\mathbb{Z}[X]$. Or 2 et X appartiennent à I, donc $2 = P_0Q_1$ et $X = P_0Q_2$ avec $Q_1, Q_2 \in \mathbb{Z}[X]$. On en déduit que P_0 divise 2 et X. Mais les seuls polynômes de $\mathbb{Z}[X]$ qui divisent 2 sont les polynômes constants ± 1 ou ± 2 et parmi ceux-là seuls ± 1 divisent X. Par conséquent $P_0 = \pm 1$, mais ces polynômes ne vérifient pas $P_0(0)$ pair, ce qui est absurde.

En conclusion I n'est pas un idéal principal. □

3. Divisibilité dans un anneau intègre général

Soit A un anneau unitaire et intègre.

Définition 3.1. — *Soient a, b deux éléments de A. On dit que a* **divise** *b, ou que b est* **multiple** *de a, s'il existe $c \in A$ tel que $b = ac$, ce qui est équivalent à $bA \subset aA$. On notera $a|b$.*

On dit qu'un élément $p \in A$ est **irréductible** *dans A, si p n'est pas nul, n'est pas inversible, et si tout diviseur de p est soit inversible soit associé à p, i.e. pour tout $a, b \in A$,*

$$p = ab \Rightarrow a \in A^\times \text{ ou } b \in A^\times$$

Un élément $p \in A$ est **premier** *s'il est non nul, non inversible et si, pour tout $a, b \in A$,*

$$p|ab \Rightarrow p|a \quad ou \quad p|b$$

Remarque 3.2. —

(a) Si $p \in A$ est irréductible dans A, alors up est irréductible dans A pour tout $u \in A^\times$.

(b) Dans un anneau intègre, tout élément premier est irréductible.

Démonstration. — Pour le point (b), soit p premier, et supposons qu'on peut écrire $p = ab$, avec a et b des éléments de A. Alors, comme p est premier et que $p|p = ab$, on a $p|a$ ou $p|b$. Supposons que $p|a$. Alors on écrit $a = pa'$, de sorte que $p = ab = pa'b$. Par intégrité, $a'b = 1$, donc b est inversible. □

La propriété pour p d'être irréductible ou premier s'énonce en termes de l'idéal engendré par p.

Lemme 3.3. — *Soit $p \in A$.*

1. *p est premier si et seulement si l'idéal pA est premier.*
2. *p est irréductible dans A si et seulement si il n'existe pas d'idéal principal distinct de A qui contient strictement l'idéal pA.*

Démonstration. — Supposons p premier, et soit $a, b \in A$ tels que $ab \in pA$. Alors $p|ab$, et puisque p est premier, p divise a ou p divise b. Donc $a \in pA$ ou $b \in pA$. Réciproquement, si pA est premier, soit $a, b \in A$ tels que $p|ab$. Alors $ab \in pA$, et puisque pA est premier, on a $a \in pA$ ou $b \in pA$, ce qui implique $p|a$ ou $p|b$.

Supposons p irréductible et soit $I = aA$ un idéal principal contenant strictement pA. Alors a divise p, donc soit $b \in A$ tel que $p = ab$. Par irréductibilité de p, on a a inversible (et $I = A$) ou b inversible (et $I = pA$). Réciproquement, si la condition est vérifiée, montrons que p est irréductible. Soit donc $a, b \in A$ tels que $p = ab$. L'idéal aA contient pA, il est donc soit égal à pA (auquel cas a et p sont associés, donc b est inversible), soit égal à A (auquel cas a est inversible). □

Il existe des éléments irréductibles non premiers. Par exemple, dans l'anneau $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible (car le carré de sa norme complexe est égal à 4) mais pas premier. En effet, $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, mais 2 ne divise pas $1 \pm i\sqrt{5}$.

Définition 3.4 **(ppcm, pgcd)**. — *Soit $(a_i)_{i \in I}$ des éléments de A.*

1. *On dit que m est un plus petit commun multiple (ppcm) des éléments a_i si $\forall i \in I, a_i|m$, et si pour tout $m' \in A$ tel que $\forall i \in I, a_i|m'$, on a $m|m'$.*
2. *On dit que d est un plus grand commun diviseur (pgcd) des éléments a_i si $\forall i \in I, d|a_i$, et si pour tout $d' \in A$ tel que $\forall i \in I, a_i|m'$, on a $d'|d$.*

Deux ppcm, resp. pgcd, des éléments a_i, sont associés. "Le" ppcm resp. pgcd des éléments a_i est donc bien défini à un inversible près.

Il n'a donc pas de raison a priori pour qu'un ppcm ou un pgcd existe, mais s'il existe, il est unique (à un inversible près).

Démonstration. — Soit m_1 et m_2 deux ppcm des éléments a_i. En appliquant la définition avec $m = m_1$ et $m' = m_2$, on trouve que $m|m'$. Symétriquement, on obtient $m'|m$. Soit donc u et u' tels que $m' = mu$ et $m = m'u'$: on obtient $m = m'u' = muu'$, et par intégrité $uu' = 1$, de sorte que u et u' sont inversibles.

La preuve pour le pgcd est similaire. □

Définition 3.5. — *Des éléments $a_1, \dots, a_k$ de A sont dits* premiers dans leur ensemble *si les seuls diviseurs communs de $a_1, \dots, a_k$ sont les éléments de $A^\times$. De manière équivalente, les éléments $a_1, \dots, a_k$ ont 1 comme pgcd.*

Remarque 3.6. — *Des éléments $a_1, \dots, a_k$ premiers dans leur ensemble ne sont pas forcément deux à deux premiers entre eux. Par exemple les entiers 6, 10 et 15 sont premiers dans leur ensemble car leur seul diviseur commun est 1, mais ne sont pas deux à deux premiers entre eux.*

On peut caractériser le fait d'être un pgcd ou un ppcm en termes d'idéaux :

Proposition 3.7. — *Soit $(a_i)_{i\in I}$ des éléments non nuls de A, et soit $d, m \in A$.*

1. *m est un plus petit commun multiple des éléments a_i si et seulement si m est un générateur de l'idéal $\cap_i a_i A$.*
2. *Si d est un générateur de l'idéal $\sum_i a_i A$, alors d est un plus grand commun diviseur des éléments a_i.*

Démonstration. —
1. Supposons que m est un ppcm des éléments a_i. Alors m est un multiple de chacun des a_i, donc $mA \subset \cap_i a_i A$. De plus, étant donné un élément m' de $\cap_i a_i A$, m' est un multiple de chacun des a_i, et par définition du ppcm, $m' \in mA$. Donc $mA = \cap_i a_i A$. Réciproquement, si $mA = \cap_i a_i A$, alors m est un multiple de chacun des a_i, et il divise tout tel multiple commun. C'est donc un ppcm des a_i.
2. Supposons que $dA = \sum_i a_i A$. Alors, d divise chacun des a_i. De plus, soit d' qui divise chacun des a_i : écrivons $a_i = d'a'_i$. Ecrivons aussi $d = \sum a_i u_i$. Alors $d = \sum a_i u_i = \sum d' a'_i u_i = d' \sum a'_i u_i$, de sorte que d' divise d. Ainsi d est bien un pgcd des a_i. □

Exemple 3.8. — *Soit $A = \mathbb{R}[X, Y]$ un anneau de polynômes à deux indéterminées. Alors le ppcm de X et de Y est XY, et c'est aussi un générateur de $XA \cap YA$. Le pgcd de X et de Y est 1, mais il n'est pas dans $XA + YA$.*

4. Divisibilité dans un anneau principal

Dans la suite de ce paragraphe, A est un anneau principal. Nous montrons d'abord qu'un élément est irréductible si et seulement si il est premier :

Proposition 4.1. — *Soit $p \in A$. Les trois conditions sur p suivantes sont équivalentes :*

1. *p est premier ;*
2. *p est irréductible ;*
3. *l'idéal pA est maximal.*

Démonstration. — L'implication (1) ⇒ (2) est valable dans un anneau intègre général, cf Remarque 3.2. L'implication (3) ⇒ (1) est aussi valable en général, et résulte du fait que p est premier si et seulement si l'idéal pA est premier, par le Lemme 3.3, et du fait que I maximal implique I premier (cf chapitre sur les anneaux).

Montrons (2) ⇒ (3). Soit donc J un idéal contenant (p), avec p irréductible. Puisque A est principal, soit a tel que $J = (a)$. Puisque $J = (a) \supset (p)$, a divise p : soit donc $x \in A$ tel que $p = ax$. Par irréductibilité de p, on a a inversible (et $J = A$) ou x inversible (et $J = (p)$). Donc (p) est bien maximal. □

Théorème 4.2. — *Dans un anneau principal A, toute famille d'éléments non nuls $(a_i)_{i\in I}$ admet un pgcd et un ppcm. Par ailleurs, d est un pgcd des a_i si et seulement si il engendre $\sum a_i A$.*

Démonstration. — L'existence du pgcd et du ppcm résulte de la Proposition 3.7 et du fait que tout idéal de A admet un générateur. Montrons que si d est un pgcd des a_i alors il engendre l'idéal $\sum a_i A$. Soit en effet d' un générateur de $\sum a_i A$. On sait que d' est un pgcd des a_i. Mais donc d et d' sont associés, comme il est indiqué dans la Définition **??**. Ils engendrent donc le même idéal, donc d est aussi un générateur de $\sum a_i A$. □

***Corollaire 4.3* (Relation de Bezout).** — *Soient $a_1, \ldots, a_k$ des éléments de A. Un diviseur commun d de $a_1, \ldots, a_k$ est pgcd de $a_1, \ldots, a_k$, si et seulement si, il existe $u_1, \ldots, u_k \in A$ tels que*

$$d = a_1 u_1 + \cdots + a_k u_k \tag{2}$$

Démonstration. — Si d est un pgcd, alors $d \in dA = a_1 A + \cdots + a_k A$, d'où l'existence de $u_1, \ldots, u_k \in A$ tels que $d = a_1 u_1 + \cdots + a_k u_k$. Réciproquement, supposons que $d = a_1 u_1 + \ldots a_k u_k$. Soit d' un diviseur de chacun des éléments a_i : écrivons $a_i = d' b_i$. On a alors

$$d = \sum_i a_i u_i = \sum_i d' b_i u_i = d' \sum_i b_i u_i,$$

ce qui montre que $d' | d$. On a donc montré que d est un plus grand commun diviseur. □

***Corollaire 4.4* (Théorème de Bezout).** — *Pour que des éléments a_1, …, a_k de A soient premiers dans leur ensemble, il faut et il suffit qu'il existe $u_1, \ldots, u_k \in A$ tels que*

$$1 = a_1 u_1 + \ldots a_k u_k \tag{3}$$

Démonstration. — C'est une conséquence du Corollaire **??** : des éléments $a_1, \ldots a_k$ d'un anneau principal A sont premiers dans leur ensemble si et seulement si 1 est un pgcd de $a_1, \ldots a_k$. □

On donne maintenant une généralisation de la caractérisation des éléments inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$: $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow k \wedge n = 1$.

Corollaire 4.5. — *Soit a un élément non nul et non inversible d'un anneau principal A. Soit $b \in A$. Pour que $\bar{b} \in A/aA$ soit inversible dans l'anneau A/aA, il faut et il suffit que a et b soient premiers entre aux.*

Démonstration. — On a $\bar{b} \in (A/aA)^\times \Leftrightarrow \exists v \in A,\ \bar{v}\bar{b} = \bar{1}$. Or $\bar{v}\bar{b} = \bar{1} \Leftrightarrow \overline{1 - vb} = \bar{0} = aA \Leftrightarrow 1 - vb \in aA \Leftrightarrow \exists u \in A,\ 1 = ua + vb \Leftrightarrow a \wedge b = 1$. □

Corollaire 4.6 **(Lemme de Gauss)**. — *Soient $a, b, c \in A$. Si $a|bc$ et si $a \wedge b = 1$, alors $a|c$.*

Démonstration. — Il existe $q \in A$ tel que $bc = aq$ et $u, v \in A$ tels que $1 = ua + vb$. Donc $c = uac + vbc = a(uc + vq)$ et par suite $a|c$. □

Corollaire 4.7. — *Soient $a, b, c \in A$. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$. En particulier si $a \wedge b = 1$, alors $a^m \wedge b^n = 1$ pour tout $m, n \in \mathbb{N}^*$.*

Démonstration. — Il existe $u, v \in A$ tels que $1 = ua + vb$ et $x, y \in A$ tels que $1 = xa + yc$. En multipliant membre à membre ces deux égalités on obtient $1 = (uxa + uyc + vxb)a + (vy)bc$, d'où d'après le théorème de Bezout $a \wedge bc = 1$. □

On montre un résultat préliminaire en vue du Corollaire 4.9 (exceptionnellement, on ne suppose pas A principal dans cet énoncé) :

Proposition 4.8. — *Soient A un anneau commutatif unitaire, I et J des idéaux de A tels que $I + J = A$. Alors les deux anneaux $A/(I \cap J)$ et $A/I \times A/J$ sont isomorphes.*

Démonstration. — Si $x \in A$ on notera $[x]_{IJ}$ (respectivement $[x]_I$ et $[x]_J$) la classe de x modulo $I \cap J$ (respectivement I et J). Considérons l'application $f : A \to A/I \times A/J$ définie par $f : x \mapsto ([x]_I, [x]_J)$. Il est clair que f est un morphisme d'anneaux.

De plus, $x \in \mathrm{Ker}(f) \iff [x]_I = [0]_I$ et $[x]_J = [0]_J \iff x \in I$ et $x \in J \iff x \in I \cap J$. D'où $\mathrm{Ker}(f) = I \cap J$ et par factorisation de f, il existe un isomorphisme d'anneaux $\overline{f}$ de $A/(I \cap J)$ sur $f(A)$. Or $I + J = A$ donc il existe $u \in I$ et $v \in J$ tels que $1 = u + v$. Soit $([a]_I, [b]_J) \in A/I \times A/J$ et posons $x = va + ub$. On a $[x]_I = [va]_I = [ua + va]_U = [a]_I$, de même $[x]_J = [b]_J$. Ainsi $\overline{f}([x]_{I \cap J}) = f(x) = ([a]_I, [b]_J)$ et par suite f est surjectif. Finalement $A/(I \cap J) \simeq A/I \times A/J$. □

Corollaire 4.9 **(Théorème des restes chinois)**. — *Soit A un anneau principal, $m \in A$ et $n \in A$ premiers entre eux. Considérons $u \in A$, $v \in A$ tels que $1 = um + vn$. L'application $f : [x]_{mn} \mapsto ([x]_m, [x]_n)$ est un isomorphisme*

de l'anneau A/mnA sur l'anneau $A/mA \times A/nA$. L'isomorphisme réciproque associe à $([a]_m, [b]_m) \in A/mA \times A/nA$ la classe $[vna + umb]_{mn} \in A/mnA$.

Démonstration. — On applique la proposition précédente à $I = mA$ et $J = nA$. Puisque $m \wedge n = 1$, il existe $u, v \in A$ tels que $1 = mu + nv$, d'où $A = I + J$. De plus $mn = \text{ppcm}(m, n)$ est un générateur de $I \cap J$, donc $I \cap J = mnA$. □

5. Propriétés des anneaux principaux : noetherialité et factorialité

Définition 5.1. — *Un anneau A est dit Noetherien si toute suite croissante d'idéaux est stationnaire. Cela signifie que si on a une suite d'idéaux $(I_n)_{n\in\mathbb{N}}$ telle que $I_n \subset I_{n+1}$, alors il existe n_0 tel que $\forall n \geq n_0$, $I_n = I_{n_0}$.*

Exemple 5.2. — *L'anneau $\mathbb{Z}$ est Noetherien.*

Démonstration. — Soit (I_n) une suite croissante d'idéaux de $\mathbb{Z}$. Ecrivons $I_n = a_n\mathbb{Z}$ (les idéaux de $\mathbb{Z}$ sont de la formev $a\mathbb{Z}$). Puisque $I_n \subset I_{n+1}$, on a $a_{n+1}|a_n$. La suite des entiers (a_n) est donc décroissante et positive, elle est donc stationnaire, ce qui montre que la suite des idéaux (I_n) est aussi stationnaire. □

Plus généralement, on a :

Proposition 5.3. — *Tout anneau principal est Noetherien.*

Démonstration. — Soit (I_n) une suite croissante d'idéaux et soit $I = \cup_{n\in\mathbb{N}} I_n$. Alors I est un idéal. Comme A est principal, on peut écrire $I = aA$, avec $a \in I = \cup_n I_n$. Il existe donc un entier n_0 tel que $a \in I_{n_0}$.

Montrons que $\forall n \geq n_0$, $I = I_n = I_{n_0}$. En effet, on a les inclusions évidentes $I \supset I_n \supset I_{n_0} \supset aA = I$. Ceci conclut la preuve. □

Définition 5.4. — *Soit A un anneau commutatif et unitaire et intègre. Supposons que tout $a \in A$ non nul, non inversible, admet une décomposition $a = p_1 \cdots p_k$, où $k \in \mathbb{N}$ et où $p_1, \cdots, p_k$ sont irréductibles dans A. Supposons de plus que cette décomposition est unique dans le sens suivant : si $a = q_1 \cdots q_m$ est une autre décomposition de ce type, alors $k = m$ et il existe une permutation $\sigma \in \mathfrak{S}_k$ telle que p_i et $q_{\sigma(i)}$ soient associés pour $i = 1, \ldots, k$.*

Alors, on dit que A est factoriel.

On rappelle qu'un élément irréductible est non nul et non inversible par définition (cf Définition 3.1).

Exemple 5.5. — *$\mathbb{Z}$ et $\mathbb{R}[X]$ sont des anneaux factoriels.*

D'une manière générale, on a :

Théorème 5.6. — *Tout anneau principal est factoriel.*

Démonstration. — *Existence.* Soit $a \in A$ non nul et non inversible. Montrons d'abord que a possède un diviseur irréductible. Comme a est non inversible, l'idéal aA est strictement contenu dans A. D'après le théorème de Krull, il est inclus dans un idéal maximal, qu'on note M. Comme A est principal, il existe $p_1 \in A$ tel que $M = p_1 A$. Par la Remarque 3.2, p_1 est irréductible. Comme $aA \subset p_1 A$, p_1 divise a.

On a donc $a = p_1 a_1$ avec p_1 irréductible. Si $a_1 \in A^\times$, alors $p_1 a_1$ est irréductible. Si $a_1 \notin A^\times$, de même $a_1 = p_2 a_2$ avec p_2 irréductible. On continue ainsi par récurrence. Observons qu'on a à chaque étape, $a_i A \subsetneq a_{i+1} A$, puisque $a_i = a_{i+1} p_{i+1}$ avec p_{i+1} non inversible. Ce processus s'arrête après un nombre fini k d'étapes, par Noetherialité de A, et l'élément a_k est alors inversible. Donc $a = p_1 p_2 \cdots p_k a_k$ où $p_1, \ldots, p_{k-1}, p_k a_k$ sont irréductibles.

Unicité. Supposons qu'on ait $a = p_1 \cdots p_k = q_1 \cdots q_m$. Si p_1 était premier avec tous les q_i, alors il serait premier avec le produit des q_i, par le Corollaire 4.7, et il serait donc premier avec a ce qui est absurde. Quitte à appliquer une permutation des q_i, on peut donc supposer que p_1 n'est pas premier avec q_1. Soit alors d un diviseur commun de p_1 et q_1, non inversible. On peut écrire $p_1 = du$ et $q_1 = dv$, avec $u, v \in A$. Par irréductibilité de p_1 et q_1, u et v sont inversibles, de sorte que p_1 et q_1 sont associés. De plus, par intégrité, la relation $dup_2 \cdots p_k = dvq_2 \cdots q_m$ donne l'égalité $(up_2)p_3 \cdots p_k = (vq_2)q_3 \cdots q_m$ impliquant un nombre moindre d'irréductibles, et par récurrence on obtient le résultat souhaité. □

Définition 5.7. — *On appelle* **système d'irréductibles** *dans un anneau principal A une famille $\mathcal{P}$ d'éléments irréductibles de A telle que tout élément irréductible de A soit associé à un élément de $\mathcal{P}$ et un seul.*

On se fixe dorénavant un anneau principal A, et un système d'irréductibles $\mathcal{P}$ de A.

Corollaire 5.8. — *Soit a un élément non nul de A. Alors a s'écrit de manière unique sous la forme*

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k} \tag{4}$$

avec $u \in A^\times$, $k \geq 0$, $p_1, \ldots, p_k \in \mathcal{P}$ distincts et $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$.

Corollaire 5.9. — *Soit $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ un élément non nul de A, avec $u \in A^\times$, $p_1, \ldots, p_k \in \mathcal{P}$ distincts et $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$. Les diviseurs de a sont de la forme $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ où $\beta_1, \ldots \beta_k \in \mathbb{N}^*$ vérifiant $\beta_i \leq \alpha_i$ pour $i = 1, \ldots, k$.*

Démonstration. — Si b divise a alors il existe $c \in A$ tel que $a = bc$. Ecrivons $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ et $c = wp_1^{\gamma_1} \cdots p_k^{\gamma_k}$, où $v, w \in A^\times$ et $p_1, \ldots, p_k \in \mathcal{P}$. Le produit $uwp_1^{\beta_1+\gamma_1} \cdots p_k^{\beta_1\gamma_k}$ doit coïncider avec la décomposition

de a. D'après l'unicité de cette décomposition on a alors $\alpha_i = \beta_i + \gamma_i$, ce qui implique le résultat. □

Corollaire 5.10. — *Soit $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$ deux éléments non nul de A décomposés en produit de facteurs irréductibles de $\mathcal{P}$, où $\alpha_i > 0$, $\beta_i > 0$ et $u, v \in A^\times$. Pour $i = 1, \ldots, k$ posons $\gamma_i = \min(\alpha_i, \beta_i)$ et $\eta_i = \max(\alpha_i, \beta_i)$. Alors $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ est un pgcd de a et b et $m = p_1^{\eta_1} \cdots p_k^{\eta_k}$ est un ppcm de a et b. Il existe $w \in A^\times$ tel que $ab = wdm$.*

Démonstration. — Les expressions du pgcd et ppcm découlent du corollaire précédent. La relation $ab = wdm$ résulte de la propriété : $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$. □