Mémoire de Master Agrégation Mathématiques

Dorian Cacitti-Holland

Les Anneaux Principaux

Table des matières

Introduction.
Pour résoudre des équations diophantiennes, nous sommes souvent amenés à travailler dans des anneaux factoriels pour obtenir une unique décomposition en produits d'irréductibles de nos éléments considérés.
Cependant il est difficile de montrer qu'un anneau est factoriel. Nous sommes donc amenés à considérer une plus petite catégorie d'anneaux factoriels : les anneaux principaux. Ils nous permettent d'obtenir davantage de propriétés et il est plus aisé de montrer qu'un anneau est principal. De plus pour montrer qu'un anneau est principal, on peut montrer qu'il s'agit d'un anneau euclidien qui est une encore plus petite catégorie d'anneaux factoriels.
Par exemple nous allons pouvoir résoudre des équations de Mordell de type $y^2 = x^3 - k$ avec $k \in \mathbb{Z}$, ou l'équation de des deux carrés $n = x^2 + y^2$ avec $(n, x, y) \in \mathbb{N}^3$.

1 La principalité dans un anneau

On considère un anneau A unitaire commutatif. On supposera connu les notions d'anneaux, d'idéaux et d'anneaux quotients.

1.1 Les idéaux principaux

On considère un idéal I de notre anneau A.

Définition. On dit que I est principal s'il est engendré par un élément de A, ie s'il existe $a \in A$ tel que

$$I = (a) = aA$$

Exemple. Tous les ideaux de $\mathbb{Z}$ sont principaux.
En effet si I est un idéal de $\mathbb{Z}$ alors soit $I = \{0\}$ (engendré par 0) soit $I \neq \{0\}$.
Dans ce dernier cas, $I \cap N^*$ est un sous-ensemble non vide de $\mathbb{N}^*$, il admet donc un plus petit élément $x \in I \cap \mathbb{N}^*$.
Soit $y \in I$, on considère sa division euclidienne par x : il existe $(q, r) \in \mathbb{Z} \times [\![0, x-1]\!]$ tel que

$$y = qx + r$$

Donc, comme I est un idéal, $r = y - qx \in I$.
D'où, par minimalité de x, $r = 0$ et $y = qx \in (x)$.
Par conséquent $I \subset (x) \subset I$, puis $I = (x)$.

Remarque. Tous les idéaux d'un anneau ne sont pas principaux.

Exemple. L'idéal $I = (2, X)$ de l'anneau $\mathbb{Z}[X]$ n'est pas principal.
En effet si on suppose par l'absurde qu'il existe $P \in \mathbb{Z}[X]$ tel que $(P) = I = (2, X)$.
Alors, en particulier, $2 \in (P), X \in (P)$, d'où, dans $\mathbb{Z}[X]$, $P \mid 2, P \mid X$.
Ainsi $P \in \{-2, -1, 1, 2\} \cap \{-X, -1, 1, X\} = \{-1, 1\} = \mathbb{Z}^\times$, d'où $I = (P) = \mathbb{Z}[X]$.
Or, en particulier, $1 \in \mathbb{Z}[X]$, donc il existe $(U, V) \in (\mathbb{Z}[X])^2$ tel que $1 = 2U + XV$.
Ainsi, en évaluant en $0 \in \mathbb{Z}$, $1 = 2\overbrace{U(0)}^{\in\mathbb{Z}}$ ce qui est absurde car 2 ne divise pas 1 dans $\mathbb{Z}$.
Par conséquent $I = (2, X)$ n'est pas principal.

D'autres idéaux vont être importants pour la suite de notre étude des anneaux principaux, il s'agit des idéaux premiers et des idéaux maximaux

Définition. On dit que I est un idéal premier si

$$\forall (a, b) \in A^2, ab \in I \Rightarrow a \in I \text{ ou } b \in I$$

Exemple. L'idéal $\{0\}$ est premier si seulement si A est intègre.

Définition. On dit que I est un idéal maximal si $I \neq A$ et pour tout idéal J de A tel que $I \subset J$, on ait $J = I$.

Concernant ces types d'idéaux, nous avons des liens entre eux. Les résultats suivant peuvent être démontrés en revenant aux différentes définitions des notions utilisées.

Théorème. Si A intègre alors :

1. I est maximal dans A si et seulement si A/I est un corps
2. I est premier dans A si et seulement si A/I est un anneau intègre

Corollaire. Si I maximal et A intègre alors I est premier dans A.

Proposition. Soit $p \in A$ avec A intègre, alors p est premier si et seulement si l'idéal (p) est premier.

Corollaire. Soit $p \in A$ avec A intègre tel que (p) soit maximal alors p est irréductible.

1.2 Anneaux principaux

Définition. On dit que A est un anneau principal s'il est intègre et si tout idéal de A est principal.

Exemple. Un corps est un anneau principal car ses seuls idéaux sont $\{0\}$ et K.
En effet soit I idéal non réduit à 0 de K, alors il existe $x \in I \cap K^*$, d'où

$$\forall y \in K, y = yx^{-1}x \in Kx = (x) \subset I$$

Donc $K \subset I \subset K$ puis $K = I$.

Exemple. Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps, sont principaux. En effet, les idéaux de $\mathbb{Z}$ ont été détaillés dans la partie précédente et on obtient de la même manière les idéaux de $K[X]$ car il existe une division euclidienne dans $K[X]$ grâce au degré.

On a vu dans la partie précédente qu'un idéal maximal est premier, mais, dans un anneau principal, on a la proposition plus forte suivante :

Proposition. Soit $p \in A\backslash(\{0\} \cup A^\times)$, alors les assertions suivantes sont équivalentes :

1. L'idéal (p) est premier
2. p est premier
3. p est irréductible
4. L'idéal (p) est maximal.

Démonstration. On a déjà $1 \iff 2$, $2 \implies 3$ et $4 \implies 1$ dans un anneau intègre non nécessairement principal.
Sens $3 \implies 2$: On suppose p irréductible. Soit $(a, b) \in A^2$ tel que $p \mid ab$.
Alors, comme A est principale et (p, a) idéal de A, il existe $c \in A$ tel que $(p, a) = (c)$.
D'où $p \in (p) \subset (c)$ ie $c \mid p$.
Donc, comme p est irréductible, c est soit inversible soit associée à p (ie il existe $\alpha \in A^\times$ tel que $c = \alpha p$).

— Dans le premier cas on a $A = (c) = (p, a)$. En particulier $1 \in (p, a)$, donc il existe $(u, v) \in A^2$ tel que $1 = up + va$.
D'où $b = upb + vab$ avec $p \mid upb$ (car A commutatif), $p \mid ab \mid vab$.
Par conséquent

$$p \mid b$$

— Dans le second cas on a directement $p \mid a$.

Ainsi p est premier, ce qui montre $3 \Longrightarrow 2$.
Sens $3 \Longrightarrow 4$: On suppose p est irréductible. Comme p est non inversible,

$$(p) \neq A$$

De plus pour J idéal de A principal différent de A contenant (p), il existe $a \in A$ tel que $J = (a)$.
Or, en particulier, $p \in (p) \subset J = (a)$, donc $a \mid p$.
Comme p irréductible, a est soit inversible, soit associé à p.
Le premier cas est exclu car $(a) = J \neq A$, d'où a et p sont associés, ie il existe $\alpha \in A^\times$ tel que $a = \alpha p$, donc

$$J = (a) = Aa = A\alpha p = Ap = (p)$$

avec la pénultième égalité justifiée car l'application $x \in A \longmapsto x\alpha \in A$ est bijective.
Par conséquent (p) est maximal, ce qui montre $3 \Longrightarrow 4$.
On a donc montré les différentes équivalences de manière circulaire $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$. □

Remarque. Cette proposition est utile pour montrer qu'un anneau n'est pas principal en mettant en défaut l'une des assertions.

1.3 Cas particulier des anneaux euclidiens

Définition. On dit que A est un anneau euclidien s'il est intègre et s'il existe une application $\varphi : A\backslash\{0\} \longrightarrow \mathbb{N}$ telle que

$$\forall (a, b) \in A \times A\backslash\{0\}, \exists (q, r) \in A^2, \begin{cases} a = bq + r \\ r = 0 \text{ ou } \varphi(r) < \varphi(b) \end{cases}$$

Théorème. Si A est un anneau euclidien alors A est un anneau principal, plus précisément pour tout idéal I de A non réduit à 0, $I = (a_0)$ avec $a_0 \in A$ tel que $\varphi(a_0) = \min\limits_{a \in I\backslash\{0\}} \varphi(a)$.

Démonstration. On suppose que A est un anneau euclidien.
Soit I idéal de A.
Si $I = \{0\}$ alors I est principal.
Sinon $\varphi(I\backslash\{0\})$ est une partie non vide de $\mathbb{N}$, donc admet une borne inférieure atteinte en un élément $a_0 \in I\backslash\{0\}$: $n_0 := \varphi(a_0) = \min\limits_{a \in I\backslash\{0\}} \varphi(a)$.
Soit $a \in I$, alors, comme A est euclidien et $a_0 \neq 0$, il existe $(q, r) \in A^2$ tel que

$$\begin{cases} a = a_0 q + r \\ \varphi(r) < \varphi(a_0) \text{ ou } r = 0 \end{cases}$$

Or a_0 est de stathme minimal dans $I\backslash\{0\}$, donc $r = 0$ car $r = a - a_0 q \in I$.
Donc $I \subset (a_0) \subset I$, d'où $I = (a_0)$ est un idéal principal, ce qui montre que A est principal. □

Remarque. La réciproque est fausse, un anneau principal est non nécessairement euclidien.

Pour justifier cette remarque nous avons le contre-exemple suivant qui fait l'objet de notre premier développement.

Proposition. Pour $\omega = \frac{1+i\sqrt{19}}{2}$, l'anneau $Z[\omega] = \{a + b\omega, (a, b) \in \mathbb{Z}^2\}$ est prinipal et non euclidien.

Démonstration.
Etape 1 : Lemme intermédiaire : $(\mathbb{Z}[\omega])^\times = \{-1, 1\}$
Soit $u = a + b\omega \in \mathbb{Z}[\omega]\backslash\{0\}$ inversible, alors il existe $v \in \mathbb{Z}[\omega]$ tel que $uv = 1$.
En particulier, en notant $N(u) = |u|^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4}b^2 = a^2 + ab + 5b^2 \in \mathbb{N}$, on a dans $\mathbb{N}$

$$N(u)N(v) = N(uv) = N(1) = 1$$

Ainsi $1 = N(u) = a^2 + ab + 5b^2$.
Or $a^2 + ab + b^2 \geq a^2 - |a||b| + b^2 \geq (|a| - |b|)^2 \geq 0$, d'où $1 \geq 4b^2$.
Ainsi, nécessairement, $b = 0$ puis $a = \pm 1$.
Réciproquement ces deux éléments sont bien inversibles dans $\mathbb{Z}[\omega]$, d'inverses eux-mêmes.
Etape 1 : L'anneau $\mathbb{Z}[\omega]$ n'est pas euclidien
On suppose par l'absurde qu'il existe un stathme $\varphi : A\backslash\{0\} \longrightarrow \mathbb{N}$ dans $\mathbb{Z}[\omega]$.
Or $\{\varphi(u), u \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}\}$ est un ensemble non vide de $\mathbb{N}$, donc admet un minimum atteint en $u_0 \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}$: $\varphi(u_0) = \min\{\varphi(u), u \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}\}$.
Soit $u \in \mathbb{Z}[\omega]\backslash\{0\}$, par division euclidienne par u_0, il existe $(q, r) \in (\mathbb{Z}[\omega])^2$ tel que

$$\begin{cases} u = qu_0 + r \\ \varphi(r) < \varphi(u_0) \text{ ou } r = 0 \end{cases}$$

Si $r = 0$ alors $u_0 \mid u$, en particulier pour $u = 1$, $u_0 \mid 1$, ie $u_0 \in (\mathbb{Z}[\omega])^\times$ ce qui est exclu.
Donc $r \neq 0$ et $\varphi(r) < \varphi(u_0)$.
Or $r = u - qu_0 \in \mathbb{Z}[\omega]$, donc, par minimalité de $\varphi(u_0)$, $r \in \{-1, 1\}$, d'où

$$u_0 \mid u - 1 \text{ ou } u_0 \mid u + 1$$

Ainsi, dans $\mathbb{N}$,

$$N(u_0) \mid N(u - 1) \text{ ou } N(u_0) \mid N(u + 1)$$

En particulier pour $u = 2 \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}$,

$$N(u_0) \mid N(u - 1) = N(1) = 1 \text{ ou } N(u_0) \mid N(u + 1) = N(3) = 9$$

Et pour $u = \omega \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}$,

$$N(u_0) \mid N(u - 1) = 5 \text{ ou } N(u_0) \mid N(u + 1) = 7$$

Ainsi, la seule possibilité pour $N(u_0)$ est $N(u_0) = 1$, d'où $u \in \{-1, 1\}$ ce qui est exclu.
Par conséquent $\mathbb{Z}[\omega]$ n'est pas euclidien.
Etape 3 : Lemme intermédiaire : Pour $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[\omega]$ tel que $|z - u| < 1$ ou $|2z - u| < 1$

Soit $z \in \mathbb{C}$, alors il existe $(x, y) \in \mathbb{R}^2$ (unique) tel que $z = x + \omega y$, de plus il existe $(a, b) \in \mathbb{Z}^2$ (unique) tel que

$$(x, y) \in \left[a - \frac{1}{2}, a + \frac{1}{2}\right[\times \left[b - \frac{1}{2}, b + \frac{1}{2}\right[$$

(en considérant a partie entière de $x + \frac{1}{2}$ et b partie entière de $b + \frac{1}{2}$).
On considère donc $u = a + b\omega \in \mathbb{Z}[\omega]$.
Ainsi, comme $|x - a| \leq \frac{1}{2}$,

$$|z - u|^2 = (x - a)^2 + (x - a)(y - b) + 5(y - b)^2 \leq \frac{1}{4} + \frac{1}{2}|y - b| + 5(y - b)^2$$

Distinguons deux cas :

— Si $|y - b| \leq \frac{1}{3}$ alors $|z - u|^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$, d'où

$$|z - u| < 1$$

— Sinon $|y - b| \in \left]\frac{1}{3}, \frac{1}{2}\right]$, ainsi

$$\frac{1}{3} < y - b \leq \frac{1}{2} \text{ oou } -\frac{1}{2} \leq y - b < -\frac{1}{3}$$

D'où

$$2b + \frac{2}{3} < y \leq 2b + 1 \text{ ou } 2b - 1 \leq y < 2b - \frac{2}{3}$$

Donc en considérant

$$d := 2b + 1 \text{ ou } d := 2b - 1$$

On obtient $|2y - d| \leq \frac{1}{3}$.
Ainsi, avec c partie entière de $2x + \frac{1}{2}$ et $u' := c + d\omega \in \mathbb{Z}[\omega]$, on a, grâce au cas précédent,

$$|2z - u'| < 1$$

Etape 4 : L'idéal (2) est maximal dans $\mathbb{Z}[\omega]$
Par le morphisme d'anneaux $\text{ev}_\omega : P \in \mathbb{Z}[X] \longrightarrow P(\omega) \in \mathbb{Z}[\omega]$ de noyau $(X^2 - X + 5) \subset \mathbb{Z}[X]$.
En effet, pour $P \in \mathbb{Z}[X]$, si $P(\omega) = 0$ alors $P(\overline{\omega}) = 0$, d'où $X^2 - X + 5 = (X - \omega)(X - \overline{\omega}) \mid P$ dans $\mathbb{C}[X]$ car $X - \omega$ et $X - \overline{\omega}$ sont premiers entre eux dans $\mathbb{C}[X]$.
D'où, comme $X^2 - X + 5 \in \mathbb{Z}[X]$ unitaire et $P \in \mathbb{Z}[X]$, on a $X^2 - X + 5 \mid P$ dans $\mathbb{Z}[X]$, ie $P \in (X^2 - X + 5)$.
Réciproquement, pour $P \in (X^2 - X + 5) \subset \mathbb{Z}[X]$, alors $ev_\omega = P(\omega) = 0$.
De plus ev_ω est surjectif par définition de $\mathbb{Z}[\omega]$.
Donc par théorème d'isomorphisme d'anneaux on a $\mathbb{Z}[\omega] \simeq \mathbb{Z}[X]/(X^2 - X + 5)$.
Puis, encore par théorèmes d'isomorphismes d'anneaux,

$$\mathbb{Z}[\omega]/(2) \simeq \mathbb{Z}[X]/(2, X^2 - X + 5) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + X)$$

avec $X^2 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$ irréductible, d'où $\mathbb{Z}[\omega]/(2)$ est un corps, donc (2) est maximal.
Etape 5 : L'anneau $\mathbb{Z}[\omega]$ est principal
Soit I idéal de $\mathbb{Z}[\omega]$ non réduit à 0, alors $\{N(u), u \in I \backslash \{0\}\}$ est un ensemble non vide de $\mathbb{N}$,

donc admet un minimum atteint en $u_0 \in I\backslash\{0\}$: $N(u_0) = \min\{N(u), u \in I\backslash\{0\}\}$.
Soit $v \in I$ et $z = \frac{v}{u_0} \in \mathbb{C}$.
Or, d'après le lemme précédent, il existe $u \in \mathbb{Z}[\omega]$ tel que $|z - u| < 1$ ou $|2z - u| < 1$.
Distinguons les deux cas :

— Si $|z - u| < 1$ alors $|v - uu_0| < |u_0|$.
Ainsi, comme $v - uu_0 \in \mathbb{Z}[\omega]$, $N(v - uu_0) < N(u_0)$, d'où, comme $v - uu_0 \in I$ et par minimalité de $N(u_0)$ sur $I\backslash\{0\}$,

$$v = uu_0 \in (u_0)$$

— Si $|2z - u| < 1$ alors $|2v - uu_0| < |u_0|$.
Ainsi, comme $2v - uu_0 \in \mathbb{Z}[\omega]$, on a $N(2v - uu_0) < N(u_0)$.
D'où, comme $2v - uu_0 \in I$ et par minimalité de $N(u_0)$ sur $I\backslash\{0\}$,

$$2v = uu_0 \in (u_0)$$

De plus $uu_0 = 2v \in (2)$ avec (2) maximal d'après le lemme précédent, en particulier premier, donc $u \in (2)$ ou $u_0 \in (2)$.
— Si $u \in (2)$ alors $u = 2u'$ avec $u' \in \mathbb{Z}[\omega]$, d'où, comme $\mathbb{Z}[\omega]$ intègre et $2 \neq 0$,

$$v = u'u_0 \in (u_0)$$

— Sinon $u \notin (2)$ et $u_0 \in (2)$, alors $u_0 = 2u'_0$ avec $u'_0 \in \mathbb{Z}[\omega]$, donc $v = uu'_0$.
De plus $(u, 2) = \mathbb{Z}[\omega]$ car (2) est maximal et $u \notin (2)$.
En particulier il existe $(\lambda, \mu) \in (\mathbb{Z}[\omega])^2$ tel que $1 = 2\lambda + u\mu$.
D'où $u'_0 = 2u'_0\lambda + uu'_0\mu = u_0\lambda + v\mu \in I$ car $(u_0, v) \in I$.
Ainsi

$$v = uu'_0 \in I$$

Donc $I \subset (u_0) \subset I$, d'où $I = (u_0)$ est principal, ce qui montre que $\mathbb{Z}[\omega]$ est principal. □

2 L'arithmétique dans un anneau principal

2.1 L'existence de plus grand commun diviseur

Définition. Soit $(a, b) \in A^2$, on dit que a et b admettent un plus grand commun diviseur (PGCD) s'il existe $d \in A\backslash\{0\}$ tel que

$$d \mid a, d \mid b, \forall d' \in A\backslash\{0\}, [d' \mid a, d' \mid b] \Longrightarrow d' \mid d$$

Remarque. On peut définir la même notion pour une famille d'éléments $(a_1, ..., a_r) \in (A\backslash\{0\})^r$: on dit que $a_1, ..., a_r$ admettent un PGCD s'il existe $d \in A\backslash\{0\}$ tel que

$$\forall k \in [\![1, r]\!], d \mid a_k$$

Et

$$\forall d' \in A\backslash\{0\}, [\forall k \in [\![1, r]\!], d' \mid a_k] \Longrightarrow d' \mid d$$

Théorème. Soit a et b dans A principal, alors a et b admettent un PGCD, plus précisément il existe $d \in A\backslash\{0\}$ PGCD de a et b tel que

$$(a, b) = (d)$$

Et en particulier il existe $(u, v) \in A^2$ tel que

$$d = au + bv$$

Démonstration. On a (a, b) idéal de A principal, donc il existe $d \in A$ tel que $(d) = (a, b)$.
En particulier $a \in (d)$ et $b \in (d)$, d'où $d \mid a$ et $d \mid b$.
De plus si $d' \in A\backslash\{0\}$ tel que $d' \mid a$ et $d' \mid b$ alors $(d) = (a, b) \subset (d')$, d'où $d' \mid d$.
Par conséquent d est un PGCD de a et b. □

Remarque. Dans le cas d'une famille $(a_1, ..., a_r) \in (A\backslash\{0\})^r$ avec A principal, les $a_1, ..., a_r$ admettent un PGCD $d \in A\backslash\{0\}$ et il existe $(u_1, ..., u_r) \in A^r$ tel que

$$d = \sum_{k=1}^{r} u_k a_k$$

Remarque. Dans le cadre des anneaux euclidiens, l'algorithme d'Euclide permet de déterminer le PGCD entre deux éléments et l'algorithme d'Euclide étendu permet également de déterminer une relation du type $d = u_1 a_1 + u_2 a_2$ (appelé relation de Bézout).

On obtient le théorème de Bézout dans le cas particulier d'éléments premier entre eux dans leur ensemble :

Définition. Soit $(a_1, ..., a_r) \in A^r$, on dit que que $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si leur PGCD est dans $A^\times$.

Corollaire. Théorème de Bézout : Soit $(a_1, ..., a_r) \in A^r$, alors $a_1, ..., a_r$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $(u_1, ..., u_r) \in A^r$ tel que

$$1 = \sum_{k=1}^{r} u_k a_k$$

Comme $K[X]$, pour K un corps, est un anneau principal, on a le résultat suivant pour les polynômes d'endomorphismes d'un K-espace vectoriel. Il s'agit d'un résultat très utile en algèbre linéaire, par exemple dans l'étude de la diagonalisabilité d'endomorphismes ou de matrices.

Application. Lemme des noyaux : Soit K un corps, E un K-espace vectoriel, u dans $End_K(E)$ et $P = P_1...P_r \in K[X]$ avec $P_1, ..., P_r$ premiers entre eux deux à deux, alors

$$ker(P(u)) = \bigoplus_{k=1}^{r} ker(P_k(u))$$

Démonstration. On raisonne par récurrence sur $r \in [\![2, +\infty[\![$:

— Pour $r = 2$: Comme P_1 et P_2 sont premiers entre eux et $K[X]$ principal, d'après le théorème de Bézout, il existe $(U_1, U_2) \in (K[X])^2$ tel que $1 = U_1P_1 + U_2P_2$.
Soit $x \in ker(P_1(u)) \cap ker(P_2(u))$, alors

$$x = (U_1P_1 + U_2P_2)(u)(x) = U_1(u)(P_1(u)(x)) + U_2(u)(P_2(u)(x)) = 0$$

D'où $ker(P_1(u)) \oplus ker(P_2(u))$.
Soit $x \in ker(P(u))$, alors $x = (U_1P_1)(u)(x) + (U_2P_2)(u)(x)$.
Or, comme $x \in ker(P(u))$,

$$P_2(u)((U_1P_1)(u)(x)) = U_1(u)((P_1P_2)(u)(x)) = U_1(u)(P(u)(x)) = 0$$

et

$$P_1(u)((U_2P_2)(u)(x)) = U_2(u)((P_1P_2)(u)(x)) = U_2(u)(P(u)(x)) = 0$$

D'où $x \in ker(P_1(u)) + ker(P_2(u))$.
Ainsi $ker(P(u)) \subset ker(P_1(u)) + ker(P_2(u)) \subset ker(P(u))$.
Par conséquent

$$ker(P(u)) = ker(P_1(u)) \oplus ker(P_2(u))$$

ce qui initialise la récurrence.

— On suppose le résultat vrai au rang $r-1$ pour $r \in [\![3, +\infty[\![$. On a $P = P_1...P_r = Q_1Q_2$ avec $Q_1 = P_1...P_{r-1}$ et $Q_2 = P_r$.
Or, comme les $P_1, ..., P_r$ sont premiers entre eux deux à deux, Q_1 et Q_2 sont premiers entre eux, donc, d'après le cas précédent, on a

$$ker(P(u)) = ker(Q_1(u)) \oplus ker(Q_2(u))$$

D'où, par hypothèse de récurrence :

$$ker(P(u)) = \bigoplus_{k=1}^{r-1} ker(P_k(u)) \oplus ker(P_r(u)) = \bigoplus_{k=1}^{r} ker(P_k(u))$$

ce qui montre l'hérédité de la récurrence.

□

2.2 La factorialité d'un anneau principal

A partir de maintenant nous avons suffisamment de résultats pour montrer un résultat très important en arithmétique : Un anneau principal est factoriel, ce qui est très utile pour résoudre des équations diophantiennes.

Définition. On dit que A est un anneau factoriel si A est intègre et si tout élément non nul de A s'écrit de manière unique comme produit d'éléments irréductibles. Autrement dit, pour $a \in A\backslash\{0\}$:

— Il existe $u \in A^\times$ et $p_1, ..., p_r \in A$ irréductibles tels que $a = u\prod_{k=1}^{r} p_k$.

— Si $a = v\prod_{k=1}^{s} q_k$ avec $v \in A^\times$ et $q_1, ..., q_r$ irréductibles, alors $r = s$ et il existe $\sigma \in S(\llbracket 1, r \rrbracket)$ tel que pour tout $k \in \llbracket 1, r \rrbracket$, q_k et $p_{\sigma(k)}$ soient associés.

Pour montrer qu'un anneau principal est factoriel nous allons passer par la caractérisation suivante des anneaux factoriels dont la démonstration est assez longue et ne rentre pas dans le cadre de l'étude des anneaux principaux.

Lemme. Les assertions suivantes sont équivalentes :

1. A est un anneau factoriel
2. A est intègre et :
   — Toute suite croissante d'idéaux principaux de A est stationnaire.
   — Tout élément irréductible de A est premier.

Théorème. Un anneau principal est factoriel.

Démonstration. On suppose que A est principal.
En particulier A est intègre et on a vu précédemment que les éléments irréductible de A sont premiers. Il ne reste plus qu'à montrer que toute suite croissante d'idéaux principaux de A est stationnaire pour pouvoir conclure avec le lemme précédent.
Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux principaux de A, alors il existe $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ tel que $\forall n \in \mathbb{N}, I_n = (a_n)$.
On considère $I = \bigcup_{n\in\mathbb{N}} (a_n)$, alors I est un idéal de A comme réunion dénombrable d'idéaux.
Or A est principal, donc il existe $a \in A$ tel que $I = (a)$.
En particulier il existe $n \in \mathbb{N}$ tel que $a \in I_n = (a_n)$, et comme la suite $(I_n)_{n\in\mathbb{N}}$ est croissante, on peut considérer $n_0 \in \mathbb{N}$ le plus petit des $n \in \mathbb{N}$ tel que $a \in (a_n)$.
Ainsi $I = (a) \subset (a_{n_0}) \subset I$, d'où $I = (a_{n_0})$.
Ainsi $\forall p \in \mathbb{N}, a_{n_0+p} \in (a_{n_0})$, puis, par croissance des idéaux $\forall p \in \mathbb{N}, (a_{n_0+p}) \subset (a_{n_0}) \subset (a_{n_0+p})$ et

$$\forall p \in \mathbb{N}, I_{n_0+p} = (a_{n_0+p}) = (a_{n_0}) = I_{n_0}$$

Par conséquent la suite croissante d'idéaux principaux est stationnaire et le lemme précédent permet de conclure que A est factoriel. □

Remarque. La réciproque est fausse, un anneau factoriel est non nécessairement principal.

Proposition. L'anneau $\mathbb{Z}[X]$ est factoriel non principal.

Démonstration.
Etape 1 : L'anneau $\mathbb{Z}[X]$ est factoriel
En effet l'anneau $\mathbb{Z}$ est factoriel car prinicpal, donc par théorème de Gauss sur la factorialité, $\mathbb{Z}[X]$ est factoriel.
Etape 2 : L'anneau $\mathbb{Z}[X]$ n'est pas principal
L'idéal $I = (2, X) \subset \mathbb{Z}[X]$ n'est pas principal (détaillé en partie 1.1).
Par conséquent $\mathbb{Z}[X]$ n'est pas principal. □

De plus on a un résultat plus général sur les anneaux de polynômes à coefficients dans un anneau A commutatif, unitaire et intègre :

Proposition. Les assertions suivantes sont équivalentes :

1. $A[X]$ est euclidien.
2. $A[X]$ est principal.
3. A est un corps.

Démonstration.
Etape 1 : $1 \Longrightarrow 2$ D'après la partie 1.3, un anneau euclidien est principal.
Etape 2 : $2 \Longrightarrow 3$ On suppose que $A[X]$ est principal. Soit $\lambda \in A\backslash\{0\}$.
On considère l'idéal $I = (\lambda, X)$ dans $A[X]$ principal, alors il existe $P \in A[X]$ tel que $(\lambda, X) = I = (P)$.
En particulier $\lambda \in (P), X \in (P)$ et $P \in (\lambda, X)$, donc il existe $(Q, R, A, B) \in (A[X])^4$ tel que $\lambda = QP, X = RP$ et $P = \lambda A + XB$.
De la première égalité on en déduit en raisonnant sur les degrés que $P \in A\backslash\{0\}$. En évaluant la seconde égalité en 1 on a $1 = Q(1)P(1) = Q(1)P$, donc $P \in A^\times$. Puis en évaluant la dernière égalité en 0 on en déduit $P = P(0) = \lambda A(0) + 0$.
Ainsi

$$\lambda(A(0)P^{-1}) = 1$$

D'où λ est inversible, ce qui montre que A est un corps.
Etape 3 : $3 \Longrightarrow 1$ On suppose que A est un corps, alors $A[X]$ est euclidien avec pour stathme le degré comme détaillé précédemment. □

Par conséquent, comme un anneau principal est factoriel, on obtient les deux résultats suivants, très utiles en arithmétique.

Théorème. Théorème de Gauss : On suppose que A est principal, en particulier factoriel, soit $(a, b, c) \in A^3$ tel que $a \mid bc$ et a et b premiers entre eux, alors $a \mid c$.

Démonstration. Comme A est factoriel, on décompose a, b, c en produits d'irréductibles distincts :

$$a = u_a \prod_{k=1}^{r} p_k^{\nu_k(a)}, b = u_b \prod_{k=1}^{r} p_k^{\nu_k(b)}, c = u_c \prod_{k=1}^{r} p_k^{\nu_k(c)}$$

(quitte à rajouter des $\nu_k(a), \nu_k(b), \nu_k(c)$ nulles).
On suppose par l'absurde qu'il existe $k \in [\![1, r]\!]$ tel que $\nu_k(a) > \nu_k(c) > 0$.
Or $a \mid bc$, donc $\nu_k(a) \leq \nu_k(bc) = \nu_k(b) + \nu_k(c)$ (la dernière égalité étant justifiée par l'unicité de la décomposition en produit d'irréductibles de bc).
Ainsi $\nu_k(b) \geq \nu_k(a) - \nu_k(c) > 0$.
D'où $p_k \mid a$ et $p_k \mid b$ ce qui contredit le fait que a et b soient premiers entre eux.
Par conséquent $\forall k \in [\![1, r]\!], \nu_k(a) \leq \nu_k(c)$.
Ainsi $a \mid c$. □

Théorème. Théorème d'Euclide : On suppose que A est principal, en particulier factoriel, soit $(p, a, b) \in A^3$ avec p irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration. Si p ne divise pas a alors, comme p est irréductible, p et a sont premiers entre eux.
Or $p \mid ab$, donc, d'après le théorème de Gauss (car A principal), $p \mid b$. □

2.3 Un isomorphisme entre anneaux quotients

Quand il s'agit de résoudre un système de congruences, il est naturel de travailler dans un anneau produit d'anneaux quotients. Mais dans le cas où l'anneau est principal, on peut se ramener à l'étude dans un anneau quotient plus simple grâce au théorème des restes chinois.

Lemme. Soit $a_1, ..., a_r$ éléments deux à deux premiers entre eux dans A principal et pour tout k dans $[\![1, r]\!], b_k := \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ alors les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble.

Démonstration. On suppose par l'absurde qu'il existe $p \in A$ premier divisant tous les $b_1, ..., b_r$.
En particulier $p \mid b_1 = \prod_{j=2}^{r} a_i$, donc, comme p est premier, il existe $i \in [\![2, r]\!]$ tel que $p \mid a_i$.
Or, de plus, $p \mid b_i$, donc, comme p est premier, il existe $j \in [\![1, r]\!] \backslash \{i\}$ tel que $p \mid a_j$.
Par conséquent p divise a_i et a_j premiers entre eux, ce qui est absurde, ce qui montre que les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble. □

Théorème. Théorème des restes chinois (ou de Sun Zi) : Avec les notations du lemme précédent, en notant de plus $a := \prod_{k=1}^{r} a_k$ et les surjections canoniques $\pi : A \longrightarrow A/(a)$ et $\pi_k : A \longrightarrow A/(a_k)$ pour $k \in [\![1, r]\!]$, l'application

$$\varphi : \begin{array}{ccc} A & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$$

est un morphisme d'anneaux surjectif.
En particulier φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : \begin{array}{ccc} A/(a) & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$$

d'inverse

$$\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times ...A/(a_r) & \longrightarrow & A/(a) \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$$

avec $(u_1, ..., u_r) \in A^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$.

Démonstration. L'application φ est bien un morphisme d'anneaux.
De plus son noyau est formé des multiples de tous les a_j, donc de leur PPCM $a = \prod_{k=1}^{r} a_k$ car les $a_1, ..., a_r$ sont premiers entre eux deux à deux. Autrement dit

$$ker(\varphi) = (a)$$

Or, d'après le lemme précédent, les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble, donc, d'après le théorème de Bézout, il existe $(u_1, ..., u_r) \in A^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$.

Soit $k \in [\![1,r]\!]$, alors pour $i \in [\![1,r]\!]\backslash\{k\}$, comme b_i est un multiple de a_k car $k \neq i$, $\pi_k(b_i) = \pi_k(0)$.

Donc, comme π_k est un morphisme d'anneaux, $\pi_k(1) = \pi_k\left(\sum_{i=1}^{r} u_k b_k\right) = \pi_k(u_k)\pi_k(b_k)$.

Ainsi $\pi_k(b_k)$ est inversible dans $A/(a_k)$ d'inverse $\pi_k(u_k)$.

Soit $(\pi_1(x_1), ..., \pi_r(x_r)) \in A/(a_1) \times ... \times A/(a_r)$, on considère $x = \sum_{k=1}^{r} x_k u_k b_k$.

Alors, pour $k \in [\![1,r]\!]$, $\pi_k(x) = \pi_k(x_k)\pi_k(u_k)\pi_k(b_k) = \pi_k(x_k)$.

Autrement dit

$$\varphi(x) = (\pi_1(x_1), ..., \pi_r(x_r))$$

Ainsi φ est surjectif.

Puis, par propriété universelle sur les morpismes d'anneaux, φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : \begin{array}{ccc} A/(a) & \longrightarrow & A/(a_1) \times ... \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$$

De plus, d'après la démonstration de la surjectivité de φ, on a également

$$\overline{\varphi}^{-1} : \begin{array}{ccc} A/(a_1) \times ...A/(a_r) & \longrightarrow & A/(a) \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$$

□

Application. On considère le système de congruences $\begin{cases} x \equiv a[n] \\ x \equiv b[n] \end{cases}$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec n et m premiers entre eux, alors il existe une solution $x \in \mathbb{Z}$ (unique modulo nm) de ce système.

Exemple. Le système $\begin{cases} x \equiv 2[4] \\ x \equiv 3[5] \\ x \equiv 1[9] \end{cases}$ a pour ensemble de solutions $\{838 + 180k, k \in \mathbb{Z}\}$ car on a la relation de Bézout entre 4,5 et 9 : $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 - 22 \times 4 \times 5$.

3 Les entiers d'un corps quadratique

On peut obtenir des exemples utiles d'anneaux principaux grâce aux corps quadratiques, ie les sous-corps de $\mathbb{C}$ qui sont de dimension 2 sur $\mathbb{Q}$ sous-corps premier de $\mathbb{C}$. Il s'agit de sous-corps de $\mathbb{C}$ de la forme $\mathbb{Q}(\delta)$ où δ est une racine dans $\mathbb{C}$ de $X^2 - d$ avec $d \in \mathbb{Z}\backslash\{0, 1\}$ sans facteur carré (autre que 1). Plus particulièrement nous allons nous intéresser à certains éléments de $\mathbb{Q}(\delta)$ appelés entiers de $\mathbb{Q}(\delta)$.

3.1 Les entiers de $\mathbb{Q}(\delta)$

Définition. Soit $z \in \mathbb{Q}(\delta)$, alors on dit que z est un entier de $\mathbb{Q}(\delta)$ (ou entier quadratique) si z est racine d'un polynôme unitaire de degré 2 à coefficients dans $\mathbb{Z}$.

Et on note A_d l'ensemble des entiers de $\mathbb{Q}(\delta)$.

Exemple. Le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ est un entier de $\mathbb{Q}(\sqrt{5})$ car annulé par $X^2 - X - 1$ unitaire à coeffcients dans $\mathbb{Z}$.
Le nombre complexe i est un entier de $\mathbb{Q}(i)$ car annulé par $X^2 + 1$ unitaire à coefficients dans $\mathbb{Z}$.
Le nombre complexe $j = e^{i\frac{2\pi}{3}}$ est un entier de $\mathbb{Q}(i\sqrt{3})$ car annulé par $X^2 + X + 1$ unitaire à coeffcients dans $\mathbb{Z}$.

Définition. Soit $z \in \mathbb{Q}(\delta)$, alors, comme $[\mathbb{Q}(\delta) : \mathbb{Q}] = 2$ et $(1, \delta)$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\delta)$, il existe $(x, y) \in \mathbb{Q}^2$ tel que $z = x + \delta y$, ainsi on appelle :

1. Conjugué de z : $\overline{z} = x - \delta y$
2. Norme de z : $N(z) = z\overline{z} = x^2 - dy^2$
3. Trace de z : $tr(z) = z + \overline{z} = 2x$

Remarque. Si $d < 0$ alors $\overline{z}$ est également le conjugué complexe de $z \in \mathbb{C}$.

Lemme. Soit $z \in \mathbb{Q}(\delta)$, alors $z \in A_d \iff tr(z) \in \mathbb{Z}, N(z) \in \mathbb{Z}$

Démonstration.
Etape 1 : Sens direct
On suppose que $z \in A_d$, alors il existe $(a, b) \in \mathbb{Z}^2$ tel que $(X^2 + aX + b)(z) = 0$.
De même $(X^2 + aX + b)(\overline{z}) = \overline{(X^2 + aX + b)(x)} = 0$ car $(a, b) \in \mathbb{Z}^2$.
Donc $N(z) = x\overline{x} = b \in \mathbb{Z}$ et $tr(z) = z + \overline{z} = -a \in \mathbb{Z}$.
Etape 2 : Sens indirect
On suppose que $tr(z) \in \mathbb{Z}$ et $N(z) \in \mathbb{Z}$.
Or $(X^2 - tr(z)X + N(z))(z) = z^2 - tr(z)z + N(z) = z^2 - (z + \overline{z})z + z\overline{z} = 0$, d'où $z \in A_d$. □

Lemme. Soit $z = \frac{a}{b} + \frac{\alpha}{\beta}\delta \in A_d \subset Q(\delta)$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ premiers entre eux et (α, β) dans $\mathbb{Z} \times \mathbb{N}^*$ premiers entre eux, alors $b \in \{1, 2\}$, puis :
— Si $b = 1$ alors $z = a + \alpha\delta$
— Si $b = 2$ alors a, α impairs, $\beta = 2$ et $d \equiv 1[4]$.

Démonstration.
Comme $z \in A_d$, d'après le lemme précédent, $2\frac{a}{b} = tr(z) \in \mathbb{Z}$ avec a et b premiers entre eux, donc $2 \mid b$ puis $b \in \{1, 2\}$.
Si $b = 1$: On a $a^2 - \frac{\alpha^2}{\beta^2}d = N(z) \in \mathbb{Z}$, d'où $\beta^2 \mid d$.
Or d est sans facteur carré (autre que 1), donc $\beta = 1$ puis $z = a + \alpha\delta$.
Si $b = 2$: On $\frac{a^2}{4} - \frac{\alpha^2}{\beta^2}d = N(z) \in \mathbb{Z}$, d'où $4\beta^2 \mid a^2\beta^2 - 4\alpha^2 d$ puis $4 \mid 4\beta^2 + 4\alpha^2 d \mid a^2\beta^2$.
Or a et b (pair) sont premiers entre eux, donc a est impair, puis β est pair : $\beta = 2\beta'$.
Ainsi $\frac{a^2}{4} - \frac{\alpha^2}{4\delta'^2} = N(z) \in \mathbb{Z}$, d'où $4\beta'^2 \mid a^2\beta'^2 - \alpha^2 d$, puis $\beta'^2 \mid 4\beta'^2 + a^2\beta'^2 \mid \alpha^2 d$.
Or α et β premiers entre eux et d sans facteur carré, donc $\beta' = 1$, puis $\beta = 2$ et $4 \mid a^2 - \alpha^2 d$.
De plus a est impair donc α également, ainsi $a^2 \equiv 1[4]$ et $\alpha^2 \equiv 1[4]$.
Donc, comme $a^2 - \alpha^2 d \equiv 0[4]$, on a $d \equiv 1[4]$. □

Théorème. On a les deux cas suivants :

1. Si $d \equiv 2[4]$ ou $d \equiv 3[4]$ alors
$$A_d = \mathbb{Z} + \mathbb{Z}\delta = \mathbb{Z}[\delta]$$

2. Sinon $d \equiv 1[4]$ alors

$$A_d = \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2} = \mathbb{Z}\left[\frac{1+\delta}{2}\right]$$

Démonstration. Comme d est sans facteur carré, $d \equiv 1[4]$, $d \equiv 2[4]$ ou $d \equiv 3[4]$.
Etape 1 : Si $d \equiv 2[4]$ ou $d \equiv 3[4]$: Par le lemme précédent, on a $A_d \subset \mathbb{Z} + \mathbb{Z}\delta$.
Réciproquement si $z = a + \alpha\delta \in \mathbb{Z} + \mathbb{Z}\delta$ alors $tr(z) \in \mathbb{Z}$ et $N(z) \in \mathbb{Z}$, donc d'après un lemme précédent, $z \in A_d$, d'où $\mathbb{Z} + \mathbb{Z}\delta \subset A_d$, puis $A_d = \mathbb{Z} + \mathbb{Z}\delta$.
Etape 2 : Si $d \equiv 1[4]$: Par le lemme précédent, pour $z \in A_d$, on a $z = \frac{a+\alpha\delta}{2}$ avec a et α de même parité.
Réciproquement pour $z = \frac{a+\alpha\delta}{2}$ avec a et α de même parité, on a $tr(z) = \alpha \in \mathbb{Z}$ et $N(z) = \frac{a^2-d\alpha^2}{4} \in \mathbb{Z}$ car $d \equiv 1[4]$, d'où, d'après un lemme précédent, $z \in A_d$.
Ainsi $A_d = \left\{\frac{a+\alpha\delta}{2}, (a,\alpha) \in \mathbb{Z}^2, a \equiv \alpha[2]\right\} = \left\{\frac{a-\alpha}{2} + \alpha\frac{1+\delta}{2}, (a,\alpha) \in \mathbb{Z}^2, a \equiv \alpha[2]\right\} \subset \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2}$.
Réciproquement pour $z = a + \alpha\frac{1+\delta}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2}$, on a $z = a + \frac{\alpha}{2} + \frac{\alpha}{2}\delta$, donc on obtient $tr(z) = 2\left(a + \frac{\alpha}{2}\right) = 2a + \alpha \in \mathbb{Z}$ et $N(z) = \left(a + \frac{\alpha}{2}\right)^2 - d\frac{\alpha^2}{4} = a^2 + a\alpha + \frac{1-d}{4}\alpha^2 \in \mathbb{Z}$ car $d \equiv 1[4]$, d'où, d'après un lemme précédent, $z \in A_d$.
Par conséquent $A_d = \mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2}$. □

Corollaire. L'ensemble A_d est un sous-anneau de $\mathbb{Q}(\delta)$.

Démonstration. Comme $\mathbb{Z} + \mathbb{Z}\delta$ et $\mathbb{Z} + \mathbb{Z}\frac{1+\delta}{2}$ sont des sous-anneaux de $\mathbb{Q}(\delta)$, d'après le théorème précédent, A_d est un sous-anneau de $\mathbb{Q}(\delta)$. □

Théorème. Soit $z \in A_d$, alors $z \in A_d^\times \iff |N(z)| = 1$.

Démonstration.
Etape 1 : Sens direct On suppose $z \in A_d^\times$, alors il existe $w \in A_d$ tel que $1 = zw$, donc $1 = N(1) = N(zw) = N(z)N(w)$ dans $\mathbb{Z}$, d'où $|N(z)| = 1$.
Etape 2 : Sens indirect On suppose $|N(z)| = 1$, or $N(z) \in \mathbb{Z}$ car $z \in A_d$, donc $N(z) = \pm 1$, ie $z\overline{z} = \pm 1$ avec $\pm\overline{z} \in A_d$ car $tr(\overline{z}) = tr(z) \in \mathbb{Z}$ et $N(\overline{z}) = N(z) \in \mathbb{Z}$, d'où $z \in A_d^\times$. □

Théorème. L'anneau $A_{-1} = \mathbb{Z}[i]$ (car $-1 \equiv 3[4]$) est euclidien avec N comme stathme.

Démonstration. Soit $(z,w) \in \mathbb{Z}[i] \times \mathbb{Z}[i]\backslash\{0\}$, alors $\frac{z}{w} \in \mathbb{C}$, ainsi il existe $(x,y) \in \mathbb{R}^2$ tel que

$$\frac{z}{w} = x + iy$$

On considère $q = a + ib$ avec a et b les entiers les plus proches de x et y, d'où $\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{2}}{2} < 1$.
On considère de plus $r = z - qw \in \mathbb{Z}[i]$, ainsi $N(r) = N(w)N\left(\frac{z}{w} - q\right) < N(w)$.
D'où $z = qw + r$ est une division euclidienne de z par w, ce qui montre que $\mathbb{Z}[i]$ est euclidien. □

Remarque. Plus généralement l'application norme sur A_d est un stathme sur A_d si

$$d \in \{2, 3, 5, 13, -1, -2, -3, -7, -11\}$$

En particulier les anneaux correspondants A_d sont euclidiens donc principaux.

Application. (Question posée à l'oral) L'équation de Mordell (pour $k = 2$)

$$y^2 = x^3 - 2$$

d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour uniques solutions $(3, 5)$ et $(3, -5)$.

Démonstration.
Soit $(x, y) \in \mathbb{Z}^2$ tel que $x^3 = y^2 - 2$.
Etape 1 : x est impair
On suppose par l'absurde que x est pair, alors $y^2 \equiv -2[8] \equiv 6[8]$ ce qui n'est pas pas possible car dans $\mathbb{Z}/8\mathbb{Z}$, $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 1, 4^2 = 0, 5^2 = 1, 6^2 = 4, 7^2 = 1$.
D'où x est impair.
Etape 2 : Utilisation de $A_{-2} = \mathbb{Z}[i\sqrt{2}]$ On a

$$x^3 = y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2})$$

Etape 3 : $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$
Soit $p \in \mathbb{Z}[i\sqrt{2}]$ un diviseur commun à $y + i\sqrt{2}$ et $y - i\sqrt{2}$.
Donc $p \mid y + i\sqrt{2} - (y - i\sqrt{2}) = 2i\sqrt{2}$, ainsi dans $\mathbb{N}$ (car $d = -2 < 0$), $N(p) \mid N(2i\sqrt{2}) = 8$.
De plus dans $\mathbb{N}$, $N(p) \mid N(y + i\sqrt{2}) = y^2 + 2 = x^3$ impair d'après ce qui précède
D'où $N(p) = 1$ puis $p \in \mathbb{Z}[i\sqrt{2}]^\times$, ainsi $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux.
Etape 4 : Utilisation de la factorialité de $\mathbb{Z}[i\sqrt{2}]$
Comme $\mathbb{Z}[i\sqrt{2}]$ est euclidien, $\mathbb{Z}[i\sqrt{2}]$ est principal donc factoriel.
Ainsi, de $x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$, on en déduit qu'il existe $(u, v) \in (\mathbb{Z}[i\sqrt{2}]^\times)^2$ et $(\alpha, \beta) \in (\mathbb{Z}[i\sqrt{2})^2$ tel que $y + i\sqrt{2} = u\alpha^3$ et $y - i\sqrt{2} = v\beta^3$.
Or, d'après un théorème précédent, on a $N(u) = N(v) = 1$, puis en décomposant u et v en $a + bi\sqrt{2}$, on en déduit $u = \pm 1$ et $v = \pm 1$.
Ainsi on peut écrire $y + i\sqrt{2} = (m + ni\sqrt{2})^3$ pour $(m, n) \in \mathbb{Z}^2$.
D'où $y + i\sqrt{2} = m^3 - 6mn^2 + i\sqrt{2}(3m^2n - 2n^3)$, puis par unicité des parties réelle et imaginaire dans $\mathbb{C}$, $y = m^3 - 6mn^2 = m(m^2 - 6n^2)$ et $1 = 3m^2n - 2n^3 = (3m^2 - 2n^2)n$.
Ainsi, de la deuxième équation, on en déduit $n = \pm 1$.

- Si $n = 1$ alors $1 = 3m^2 - 2$, d'où $m = \pm 1$, puis $y = \pm 5$
- Si $n = -1$ alors $1 = -(3m^2 - 2)$, d'où $1 = 3m^2$ ce qui n'est pas possible dans $\mathbb{Z}$ car 3 ne divise pas 1 et $m^2 \in \mathbb{Z}$.

Par conséquent $y = \pm 5$ puis $x^3 = y^2 + 2 = 27$, d'où $x = 3$.
Etape 5 : Vérification
Réciproquement $(3, 5)$ et $(3, -5)$ vérifient $x^3 = y^2 + 2$. □

3.2 L'utilisation de l'anneau des entiers de Gauss $\mathbb{Z}[i]$

Définition. L'anneau des entiers de Gauss est l'anneau A_{-1} des entiers de $\mathbb{Q}(i)$, comme $-1 \equiv 3[4]$, il s'agit de $\mathbb{Z}[i]$.

Lemme. On a $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$.

Démonstration. On a d'après un lemme précédent $\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i], N(z) = 1\}$. Or, pour $z = a + ib \in \mathbb{Z}[i]$, $N(z) = 1 \iff a^2 + b^2 = 1 \iff (a, b) \in \{(0, 1), (1, 0), (0, -1), (-1, 0)\}$.
Donc $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$. □

Cet anneau, euclidien donc principal d'après ce qui précède, va nous aider à résoudre deux équations diophantiennes importantes : l'équation de Mordell (pour $k = 1$)

$$y^2 = x^3 - 1$$

et l'équation des deux carrés, pour $n \in \mathbb{N}$,

$$n = x^2 + y^2$$

Commençons par la première équation :

Théorème. L'équation de Mordell (pour $k = 1$) $y^2 = x^3 - 1$ admet pour une unique solution $(x, y) = (1, 0)$.

Démonstration. Procédons par analyse-synthèse : Soit $(x, y) \in \mathbb{Z}^2$ tel que $y^2 = x^3 - 1$.
Etape 1 : x est impair
On suppose par l'absurde que x est pair, alors $8 \mid x^3$, en particulier $4 \mid x^3$, d'où $x^3 \equiv 0[4]$.
Donc, comme (x, y) vérfie l'équation de Mordell, $y^2 \equiv -1[4] \equiv 3[4]$ ce qui est impossible car, dans $\mathbb{Z}/4\mathbb{Z}$, $0^2 = 0, 1^2 = 1, 2^2 = 0, 3^2 = 1$.
Par conséquent x est impair.
Etape 2 : $y + i$ et $y - i$ sont premiers entre eux dans $\mathbb{Z}[i]$
On écrit

$$x^3 = y^2 + 1 = (y - i)(y + i)$$

Soit $p \in \mathbb{Z}[i]$ irréductible tel que $p \mid y - i, p \mid y + i$, alors $p \mid y + i - (y - i) = 2i$.
Ainsi $N(p) \mid N(2i) = 4$.
Or p n'est pas inversible car irréductible, donc $N(p) = |N(p)| \neq 1$, ainsi $N(p) \in \{2, 4\}$.
En particulier $N(p)$ est pair.
De plus $N(p) \mid N(y + i) = y^2 + 1 = x^3$ ce qui est impossible car $N(p)$ est pair et x impair.
Par conséquent $y - i$ et $y + i$ sont premiers entre eux dans $\mathbb{Z}[i]$.
Etape 3 : Utilisation de la factorialté de $\mathbb{Z}[i]$
Comme $\mathbb{Z}[i]$ est euclidien donc principal donc factoriel, de la relation $x^3 = (y-i)(y+i)$ avec $y - i$ et $y + i$ premiers entre eux, on en déduit, par unicité de la décomposition en produits d'irréductibles de x, que

$$y + i = u(p_1...p_r)^3$$

avec $u \in \mathbb{Z}[i]^\times$ et $p_1, ..., p_r$ irréductibles dans $\mathbb{Z}[i]$.
Or $u = v^3$ avec $v \in \mathbb{Z}[i]^\times$ car $1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i = i^3$ et $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
Donc

$$y + i = (vp_1...p_r)^3 = (a + ib)^3 = (a^3 - 3ab^2) + i(3a^2b - b^3)$$

en écrivant $vp_1...p_r = a + ib$ avec $(a, b) \in \mathbb{Z}^2$.
Ainsi, par unicité des parties réelle et imaginaire dans $\mathbb{C}$:

$$y = a^3 - 3ab^2, 1 = 3a^2b - b^3 = (3a^2 - b^2)b$$

En particulier on a dans $\mathbb{Z}$ $b \mid 1$, d'où $b \in \{-1, 1\}$.
Donc :

— Si $b = 1$ alors $1 = 3a^2 - 1$ ie $3a^2 = 2$ ce qui n'est pas possible car 3 ne divise pas 2.
— Si $b = -1$ alors $1 = -3a^2 + 1$ ie $3a^2 = 0$, d'où par intégrité de $\mathbb{Z}$, $a = 0$.
Par conséquent on a

$$y = a^3 - 3ab^2 = 0$$

Puis $x^3 = y^2 + 1 = 1$ ie

$$x = 1$$

Réciproquement $(x, y) = (1, 0)$ vérifie bien l'équation de Mordell pour $k = 1$. □

Maintenant étudions l'équation des deux carrés qui fait l'objet de notre second développement. On cherche à déterminer les entiers $n \in \mathbb{N}$ tels qu'il existe $(x, y) \in \mathbb{N}^2$ tel que

$$n = x^2 + y^2$$

Nous avons restreint l'étude à $\mathbb{N}$ car $\forall (x, y) \in \mathbb{Z}^2, x^2 + y^2 = (-x)^2 + (-y)^2 \geq 0$.

Définition. On définit $\Sigma = \{n \in \mathbb{N}, \exists (x, y) \in \mathbb{N}^2, n = x^2 + y^2\}$.

Lemme. Soit $n \in \mathbb{N}$, alors $n \equiv 3[4] \Longrightarrow n \notin \Sigma$.

Démonstration. On suppose que $n \in \Sigma$. Alors il existe $(x, y) \in \mathbb{N}^2$ tel que $n = x^2 + y^2$.
Or pour tout $z \in \mathbb{N}, z \in 2\mathbb{N} \Rightarrow z^2 \equiv 0[4]$ et $z \in 2\mathbb{N} + 1 \Rightarrow z^2 \equiv 1[4]$.
Donc $n = x^2 + y^2 \equiv (0 \text{ } ou \text{ } 1) + (0 \text{ } ou \text{ } 1)[4] \equiv 0, 1 \text{ } ou \text{ } 2[4]$, d'où le résultat par contraposée. □

Lemme. Soit $n \in \mathbb{N}$, alors $n \in \Sigma \Longleftrightarrow \exists z \in \mathbb{Z}[i], n = N(z)$.

Démonstration. On a $n \in \Sigma \Longleftrightarrow \exists (x, y) \in \mathbb{N}^2, n = x^2 + y^2 = (x + iy)(x - iy) \Longleftrightarrow n = N(z)$ en posant $z = x + iy$ pour la dernière équivalence. □

Proposition. L'ensemble Σ est stable par multplication.

Démonstration. Soit $(n, n') \in \Sigma^2$, alorsn d'après le lemme précédent, il existe $(z, z') \in \mathbb{Z}[i]^2$ tel que $n = N(z), n' = N(z')$.
Donc $nn' = N(z)N(z') = z\overline{z}z'\overline{z'} = zz'\overline{zz'} = N(zz')$ avec $zz' \in \mathbb{Z}[i]$ car $\mathbb{Z}[i]$ est un anneau, d'où, d'après le lemme précédent, $nn' \in \Sigma$. □

Grâce à cette proposition, on peut restreindre l'étude aux éléments premiers de Σ pour ensuite étudier le cas général grâce à la factorialité de $\mathbb{Z}$.

Lemme. Soit $p \in \mathcal{P}$ (notation pour l'ensemble des nombres premiers dans $\mathbb{N}$), alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Démonstration.
Etape 1 : Sens direct
On suppose que $p \in \Sigma$. Alors il existe $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2 = (a + ib)(a - ib)$.
En particulier on a $a \neq 0$ et $b \neq 0$ car sinon p ne serait pas premier.
Or $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$, donc $a + ib$ et $a - ib$ ne sont pas inversible dans $\mathbb{Z}[i]$.
Par conséquent p n'est pas irréductible dans $\mathbb{Z}[i]$.
Etape 2 : Sens indirect

Réciproquement on suppose que p n'est pas irréductible dans $\mathbb{Z}[i]$, alors il existe (z, z') dans $(\mathbb{Z}[i]\backslash\mathbb{Z}[i]^\times)^2 = (\mathbb{Z}[i]\backslash\{1, -1, i, -i\})^2$ tel que $p = zz'$
Ainsi $p^2 = N(p) = N(z)N(z')$, donc, comme p est premier et z et z' non inversibles, on a $N(z) = N(z') = p$.
Or si on écrit $z = a + ib \in \mathbb{Z}[i]$, alors on a $p = N(z) = a^2 + b^2$.
D'où $p \in \Sigma$. □

Théorème. Soit $p \in \mathcal{P}$, alors

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1[4]$$

Démonstration.
Commençons par remarquer que $p = 2 = 1^2 + 1^2$, d'où $2 \in \Sigma$.
On suppose désormais $p \in \mathbb{N}$ premier distinct de 2.
Etape 1 : Sens direct
On suppose que $p \in \Sigma$, alors d'après une proposition précédente, p n'est pas congru à 3 modulo 4, d'où, comme $p \in \mathcal{P}\backslash\{2\}$, $p \equiv 1[4]$.
Etape 2 : Sens indirect
Réciproquement on suppose que $p \equiv 1[4]$.
Or en considérant le morphisme d'anneaux $ev_i : P \in \mathbb{Z}[X] \longmapsto P(i) \in \mathbb{Z}[i]$ surjectif de noyau $(X^2 + 1)$, on a l'isomorphisme d'anneaux $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$.
Puis par théorèmes d'isomorphismes : $\mathbb{Z}[i]/(p) \simeq Z[X]/(X^2 + 1, p) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2 + 1)$.
Or $p \equiv 1[4]$, donc le symbole de Legendre est $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \equiv 1$.
D'où, par définition du symbole de Legendre, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
Ainsi $X^2 + 1$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$, d'où $\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2 + 1)$ n'est pas un anneau intègre.
Par conséquent (p) n'est pas un idéal premier et p n'est pas irréductible.
D'où, d'après le lemme précédent, $p \in \Sigma$. □

Exemple. Les nombres premiers $41, 53$ et 61 sont congrus à 1 modulo 4, donc sont sommes de deux carrés, effectivement $41 = 5^2 + 4^2, 53 = 7^2 + 2^2, 61 = 6^2 + 5^2$.

Théorème. Soit $n \in \mathbb{N}$, alors :
- Si $n \in \{0, 1\}$ alors $n \in \Sigma$
- Sinon on décompose n en facteurs irréductibles (car $\mathbb{Z}$ factoriel) $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ et ainsi

$$n \in \Sigma \iff \forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$$

Démonstration.
Etape 1 : Sens direct
On montre par récurrence forte sur $n \in \mathbb{N}^*$ la propriété :

$$n \in \Sigma \Longrightarrow [\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}]$$

L'initialisation vient de $1 \in \Sigma$ et $\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(1) = 0 \in 2\mathbb{N}$.
Soit $n \in \mathbb{N}$ tel que $n > 1$ et $n \in \Sigma$. On suppose la propriété vraie pour tout $k \in [\![1, n-1]\!]$.
Soit $p \in \mathcal{P}$ tel que $p \equiv 3[4]$.

— Si $\nu_p(n) = 0$ alors $\nu_p(n) \in 2\mathbb{N}$.
— si $\nu_p(n) > 0$ alors $p \mid n = a^2 + b^2 = (a + ib)(a - ib)$.
Or $p \equiv 3[4]$, donc, d'après le théorème et le lemme précédent, on a p est irréductible dans $\mathbb{Z}[i]$.
D'où, par factorialité de $\mathbb{Z}[i]$, $p \mid a + ib$ ou $p \mid a - ib$.
Or $p \in \mathcal{P} \subset \mathbb{Z}$, donc $p \mid a$ et $p \mid b$, ainsi il existe $(a', b') \in \mathbb{N}^2$ tel que $a = a'p, b = b'p$ et de plus on a $p^2 \mid a^2 + b^2 = n$.
D'où, dans $\mathbb{N}$, $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$.
Or $\nu_p\left(\frac{n}{p^2}\right) = \nu_p(n) - 2$ et $\frac{n}{p^2} < n$, donc, par hypothèse de récurrence,

$$\nu_p(n) = \nu_p\left(\frac{n}{p^2}\right) + 2 \in 2\mathbb{N}$$

Ce qui achève la récurrence.
Etape 2 : Sens indirect
Réciproquement on suppose que

$$\forall p \in \mathcal{P}, p \equiv 3[4] \Rightarrow \nu_p(n) \in 2\mathbb{N}$$

Soit $p \in \mathcal{P}$ tel que $p \mid n$, alors si $p = 2$ ou $p \equiv 1[4]$ alors d'après le théorème précédent, $p \in \Sigma$.
Puis si $p \equiv 3[4]$ alors, par hypothèse, $\nu_p(n) \in 2\mathbb{N}$, d'où $p^{\nu_p(n)} = \left(p^{\frac{\nu_p(n)}{2}}\right)^2$ est un carré.
Donc on en déduit, d'après la stabilité de Σ par produit, que

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)} \in \Sigma$$

□

Conclusion.
Ainsi, nous avons vu que les anneaux principaux apportent beaucoup plus de structure qu'un anneau factoriel, ce qui permet de résoudre plus facilement les équations diophantiennes ou les systèmes de congruences. Cependant ces équations se résolvent encore plus facilement s'il existe un stathme sur notre anneau, dans le cadre des anneaux euclidiens, mais ceci n'est pas toujours possible pour les anneaux principaux comme nous l'avons vu.

Bibliographie.

1. Jean-Etienne Rombaldi, "Algèbre et Géométrie", Deboeck supérieur, 2017
2. Daniel Perrin, "Cours d'algèbre", Ellipses, 1996
3. Daniel Duverney, "Théorie des nombres", Dunod, 2007
4. Josette Calais, "Eléments de théorie des anneaux", Ellipses, 2006
5. Bertrand Hauchecorne, "Les contre-exemples en mathématiques", Ellipses, 2007