TD n°3.

1 Anneaux noethériens

Exercice 1. Soit A un anneau. Si $A[X]$ est noethérien, A est-il nécessairement noethérien ? Si $A[X]$ est principal, que peut-on dire de A ?

Solution. On sait que tout anneau quotient d'un anneau noethérien est encore noethérien (cours). Or $A = A[X]/(X)$ donc A est noethérien si $A[X]$ l'est. Supposons maintenant $A[X]$ principal, et montrons que A est un corps. Notons déjà que principal implique intègre, donc $A[X]$ est intègre, donc A aussi (contenu dans $A[X]$), et donc $A[X]/(X) \simeq A$ aussi. Il s'ensuit que (X) est un idéal premier de $A[X]$. Or, dans un anneau principal, on sait que les idéaux premiers non nuls sont maximaux. Donc A est un corps. *Autre possibilité pour montrer que A est un corps :* soit $a \in A$ non nul, et considérons l'idéal (a, X) de $A[X]$. Le terme constant d'un élément $af + Xg$ est visiblement dans (a), donc on a $(a, X) \cap A = aA$. Par hypothèse, (a, X) est principal, engendré par un polynôme $f \in A[X]$. Ce polynôme divise a donc son degré est nul, car $fg = a \Rightarrow \deg(f) + \deg(g) = 0$ par intégrité de A. Donc $f \in A$ et, par ci-dessus, $f \in aA$. Par ailleurs, f divise X, donc $f \in A$ divise le coefficient dominant de X qui est 1, i.e. f est inversible dans A. Comme $f \in aA$, il s'ensuit que a est aussi inversible dans A.

Exercice 2. Soit A un anneau commutatif.

a) Pour $a \in A$ et I un idéal de A, montrer que si les idéaux $I + (a)$ et $(I : a) = \{x \in A,\ ax \in I\}$ sont de type fini, alors I l'est.

b) Montrer que A est noethérien si et seulement si tous ses idéaux premiers sont de type fini.
Indication : Considérer un idéal maximal parmi ceux qui ne sont pas de type fini.

Solution. a) Soient $z_1, \cdots, z_n$ des générateurs de $I + (a)$. Alors on peut écrire $z_i = x_i + aa_i$ avec $x_i \in I$ et $a_i \in A$. On constate alors que l'idéal engendré par a et les x_i est contenu dans $I + (a)$ et contient les z_i, c'est donc $I + (a)$.
Soient $y_1, \cdots, y_m$ des générateurs de $(I : a)$, on a $ay_i \in I$. Montrons que l'on a

$$I = (x_1, \cdots, x_n, ay_1, \cdots, ay_m).$$

L'inclusion $(x_1, \cdots, x_n, ay_1, \cdots, ay_m) \subset I$ est évidente. Soit $u \in I$, on a $u \in I + (a)$ donc $u = \sum u_i x_i + ta$ avec $t \in A$. Mais alors $ta = u - \sum u_i x_i \in I$ donc $t \in (I : a)$. On peut donc écrire $t = \sum t_j y_j$. On a donc

$$u = \sum u_i x_i + \sum t_j (ay_j) \in (x_1, \cdots, x_n, ay_1, \cdots, ay_m).$$

b) Si A est noethérien, tous ses idéaux et donc en particulier les idéaux premiers sont de type fini.
Réciproquement, supposons que tous les idéaux premiers soient de type fini et soit E l'ensemble des idéaux de A qui ne sont pas de type fini. On veut montrer que $E = \emptyset$. Supposons que ce n'est pas le cas.
L'ensemble E est ordonné par l'inclusion et est inductif : si (I_n) est une suite croissante d'idéaux qui ne sont pas de type fini, alors $I = \bigcup I_n$ n'est pas de type fini (si c'était le cas on aurait $I = (a_1, \cdots, a_k)$ et il existerait n tel que $a_i \in I_n$ pour tout i donc $I = I_n$ qui serait de type fini, c'est absurde).
D'après le lemme de Zorn, il existe donc un (ou des) élément(s) maximal (maximaux) dans E. Soit I un tel élément maximal, il n'est pas de type fini donc n'est pas premier. Il existe donc a et $b \notin I$ tels que $ab \in I$.
On a alors $I \subsetneq I + (a)$, donc $I + (a)$ est de type fini. De plus $I \subsetneq (I : a)$ (car il est clair que $I \subset (I : a)$ et $b \in (I : a)$, $b \notin I$) donc $(I : a)$ est de type fini. Le (a) nous dit que I est de type fini, c'est une contradiction donc $E = \emptyset$ et A est noethérien.

Exercice 3. Soit A un anneau local dont l'idéal maximal $\mathfrak{m}$ est principal, engendré par a.

a) Montrer que $u \in A$ est inversible si et seulement si $u \notin \mathfrak{m}$.

b) Supposons que $\bigcap_{n>0} \mathfrak{m}^n = 0$.

i) Montrer que tout $x \in A$ *non nul* s'écrit sous la forme $x = ua^n$ où $u \in A^\times$ et $n \in \mathbb{N}$, et que cette écriture est unique si A est intègre.

ii) Montrer que tout idéal I est de la forme (a^n). En conclure que A est noethérien, et même principal s'il est intègre.

iii) Montrer que l'anneau de séries formelles $\mathbb{Q}[[X]] := \{f = \sum_{n\in\mathbb{N}} a_n X^n\}$ est noethérien.

c) Supposons maintenant A noethérien

i) Montrer que si I est un idéal tel que $\mathfrak{m}.I = I$, alors $I = 0$. On pourra raisonner par l'absurde sur un ensemble minimal $x_1, \cdots, x_n$ de générateurs de I et écrire que $x_n \in \mathfrak{m}.I$ pour aboutir à une contradiction.

ii) Montrer que $\bigcap_{n>0} \mathfrak{m}^n = 0$.

Solution. a) Si u est inversible, alors $(u) = A$ donc $u \notin \mathfrak{m}$. Si par contre u n'est pas inversible, alors $(u) \neq A$ donc il existe un idéal maximal contenant (u). Mais il y a un unique idéal maximal $\mathfrak{m}$ donc $u \in \mathfrak{m}$.

b) i) Soit $x \in A$ non nul. Par hypothèse on a donc un $k \in \mathbb{N}$ tel que $x \notin \mathfrak{m}^k$. Soit $n \in \mathbb{N}$ le plus grand entier tel que $x \in \mathfrak{m}^n$. On a alors $x = ua^n$ et $u \notin \mathfrak{m}$ (sinon $x \in \mathfrak{m}^{n+1}$). Ainsi u est inversible. On a donc toujours une écriture $x = ua^n$ et il reste à prouver l'unicité lorsque A est intègre. Soient deux écritures $x = ua^n = va^m$ avec u et v inversibles et supposons par exemple que $m \geqslant n$. On a alors $u = va^{m-n}$ et comme u est inversible, ceci impose $m = n$ puis $u = v$.

ii) Soit I un idéal, pour tout $x \in I$, on définit n_x le plus grand entier tel que $x \in \mathfrak{m}^{n_x}$. Soit alors $n_I = \min\{n_x \ / \ x \in I\}$. On a alors $I = (a^{n_I})$. En effet, si $x \in I$, alors $x = ua^{n_x}$ avec u inversible et $n_x \geqslant n_I$, on a donc $x = ua^{n_x - n_I}a^{n_I}$ donc $x \in (a^{n_I})$. Ainsi $I \subset (a^{n_I})$. Par ailleurs, comme $n_I = \min\{n_x \ / \ x \in I\}$, il existe $x \in I$ tel que $n_x = n_I$. Ainsi $x = ua^{n_I}$ avec u inversible. L'idéal I contient donc a^{n_I}. On vient de voir que tout idéal de A est principal, donc de type fini, l'anneau A est donc noethérien, et même principal s'il est intègre.

iii) Montrons d'abord que l'idéal (X) est l'unique idéal maximal de $\mathbb{Q}[[X]]$. Puisque X n'est pas inversible, c'est au moins un idéal propre, et il suffit de prouver que son complémentaire ne contient que des éléments inversibles, i.e. que toute série formelle de terme constant non nul est inversible. Écrivons une telle série formelle sous la forme $f = a(1 + a_1X + \cdots a_nX^n + \cdots) = a(1 + n(X))$. Alors $g := a^{-1}(1 - n(X) + n(X)^2 - \cdots + (-1)^n n(X)^n + \cdots)$ est une série formelle bien définie. Plus précisément, on a $g = a^{-1}(1 + \sum_{d\geqslant 1} b_d X^d)$ avec b_d le coefficient de X^d dans le polynôme $\sum_{i=1}^{d}(-1)^i n(X)^i$.
Maintenant, on remarque que $\bigcap_{n\in\mathbb{N}}(X)^n = 0$ car c'est l'ensemble des séries formelles dont tous les coefficients sont nuls. Pour appliquer (b), il reste donc à montrer que $\mathbb{Q}[[X]]$ est intègre et, vu (a), il suffit de montrer que X n'est pas diviseur de 0, ce qui est clair puisque la multiplication par X revient à décaler les coefficients d'un degré.

c) i) Soit $(x_1, \cdots, x_n)$ comme dans l'indication. Puisque $I = \mathfrak{m}.I$, on peut écrire x_n (entre autres) sous la forme $x_n = m_1x_1 + \cdots + m_nx_n$ avec $m_i \in \mathfrak{m} = (a)$. Il s'ensuit que $(1 - m_n)x_n = m_1x_1 + \cdots + m_{n-1}x_{n-1}$. Or, $1 - m_n$ n'est pas dans $\mathfrak{m}$ donc est inversible. Si a est son inverse, on a donc $x_n = am_1x_1 + \cdots + am_{n-1}x_{n-1}$, donc I est engendré par $x_1, \cdots, x_{n-1}$, contredisant la minimalité de la famille $(x_1, \cdots, x_n)$.

ii) Soit $I := \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$. On a $\mathfrak{m}.I = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^{n+1} = I$. Donc $I = 0$ par la question précédente.

Exercice 4. Soit $\varphi : A \to A$ un morphisme d'anneaux.

a) On suppose A noethérien, montrer qu'il existe un entier $n \geqslant 1$ tel que $\mathrm{Ker}(\varphi^n) = \mathrm{Ker}(\varphi^{n+1})$. En déduire que l'application

$$\varphi : \mathrm{Im}(\varphi^n) \to \mathrm{Im}(\varphi^{n+1})$$

est injective.

b) Montrer que si φ est surjective et A noethérien, alors elle est bijective.

c) Montrer qu'on ne peut remplacer dans la question précédente l'hypothèse « surjective » par « injective ».

d) Montrer que l'on ne peut se passer de l'hypothèse noethérien (considérer par exemple $A = k[X_1, \cdots, X_n, \cdots]$ un anneau de polynômes à une infinité de variables et φ convenable).

Solution. a) Considérons la suite des noyaux $(\mathrm{Ker}(\varphi^n))_{n\in\mathbb{N}}$. C'est une suite croissante d'idéaux de A. En effet, si $x \in \mathrm{Ker}(\varphi^n)$, alors $\varphi^{n+1}(x) = \varphi(\varphi^n(x)) = \varphi(0) = 0$ donc $x \in \mathrm{Ker}(\varphi^{n+1})$.

Comme A est noethérien, cette suite croissante d'idéaux est stationnaire donc il existe un $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0$ on ait

$$\mathrm{Ker}(\varphi^n) = \mathrm{Ker}(\varphi^{n_0}).$$

On considère alors l'application

$$\varphi : \mathrm{Im}(\varphi^{n_0}) \to \mathrm{Im}(\varphi^{n_0+1})$$

dont le noyau est $\mathrm{Ker}(\varphi) \cap \mathrm{Im}(\varphi^{n_0})$. Un point du noyau est alors de la forme $x = \varphi^{n_0}(y)$ et vérifie $\varphi(x) = 0$ donc $\varphi^{n_0+1}(y) = 0$. On a donc $y \in \mathrm{Ker}(\varphi^{n_0} + 1) = \mathrm{Ker}(\varphi^{n_0})$. Ainsi $x = \varphi^{n_0}(y) = 0$ donc la flèche est injective.

b) Si on suppose de plus φ surjective, alors on voit que φ^{n0} et φ^{n_0+1} sont aussi surjectives et l'application

$$\varphi : \mathrm{Im}(\varphi^{n_0}) \to \mathrm{Im}(\varphi^{n_0+1})$$

devient la flèche

$$\varphi : A \to A.$$

Elle est injective d'après ce qui précède, comme elle est surjectve par hypothèse, c'est un isomorphisme.

c) Prenons $A = k[X]$ et le morphisme de k-algèbres de A dans lui-même définit par $X \mapsto X^2$. Il est évidement injectif, mais n'est pas surjectif car X n'est pas dans l'image.

d) Considérons $A = k[X_1, \cdots, X_n, \cdots]$ un anneau de polynômes à une infinité de variables et définissons le morphisme de k-algèbres $\varphi : A \to A$ par l'image des générateurs :

$$\varphi(X_1) = 0 \quad \text{et} \quad \varphi(X_{i+1}) = X_i \quad \text{pour} \quad i \geqslant 1.$$

On voit alors que tous les X_i pour $i \geqslant 1$ sont dans l'image de φ donc φ est surjective alors que X_1 est dans le noyau de φ donc φ n'est pas injective.

2 Entiers algébriques

Exercice 5. On dit qu'un complexe $z \in \mathbb{C}$ est un entier algébrique s'il existe $f \in \mathbb{Z}[X]$ unitaire tel que $f(z) = 0$.

a) Montrer que $\alpha \in \mathbb{C}$ est entier algébrique si et seulement si le sous-anneau $\mathbb{Z}[\alpha]$ engendré par α est un $\mathbb{Z}$-module de type fini.

b) Soit $\alpha \in \mathbb{N}$ un nombre algébrique et $f_\alpha \in \mathbb{Q}[X]$ son polynôme minimal (i.e. le générateur unitaire de l'idéal annulateur de α dans l'anneau principal $\mathbb{Q}[X]$). Montrer que α est entier algébrique si et seulement si $f_\alpha \in \mathbb{Z}[X]$.

c) Montrer que les entiers algébriques forment un sous-anneau de $\mathbb{C}$.

Solution. On rappelle que $\mathbb{Z}[\alpha]$ est l'image de l'unique morphisme d'anneau $\mathbb{Z}[X] \longrightarrow \mathbb{C}$ qui envoie X sur α. On peut donc le voir concrètement comme :

— le sous-ensemble des éléments de la forme $g(\alpha)$ pour $g \in \mathbb{Z}[X]$

— le sous-$\mathbb{Z}$-module de $\mathbb{C}$ engendré par la famille $\{1, \alpha, \cdots, \alpha^n, \cdots\}$ des puissances de α.

a) Supposons α entier algébrique et soit $f \in \mathbb{Z}[X]$ un polynôme annulateur unitaire. Soit $\beta \in \mathbb{Z}[\alpha]$. Il existe donc $g \in \mathbb{Z}[X]$ tel que $\beta = g(\alpha)$. Comme f est unitaire, on peut faire la division euclidienne de g par f pour trouver $q, r \in \mathbb{Z}[X]$ tels que $g = qf + r$ avec $\deg(r) < n := \deg(f)$. Il s'ensuit que $\beta = r(\alpha)$ appartient au sous-$\mathbb{Z}$-module engendré par $1, \alpha, \cdots, \alpha^{n-1}$. Ceci étant vrai pour tout β dans $\mathbb{Z}[\alpha]$, on en déduit que $\mathbb{Z}[\alpha]$ est engendré, comme $\mathbb{Z}$-module par $1, \alpha, \cdots, \alpha^{n-1}$.

Supposons maintenant $\mathbb{Z}[\alpha]$ de type fini, engendré par $\beta_1, \cdots, \beta_m$. Il existe des polynômes $g_1, \cdots, g_m \in \mathbb{Z}[X]$ tels que $\beta_i = g_i(\alpha)$. Soit N le max des degrés des g_i. Alors chaque β_i est combinaison $\mathbb{Z}$-linéaire des α^j, $0 \leqslant j \leqslant N$, donc $\mathbb{Z}[\alpha]$ est engendré par ces mêmes α^j.

b) Il est clair que $f_\alpha \in \mathbb{Z}[X] \Rightarrow \alpha$ entier algébrique. Supposons α entier algébrique, et soit $f \in \mathbb{Z}[X]$ unitaire tel que $f(\alpha) = 0$. Alors f_α divise f dans $\mathbb{Q}[X]$, et il existe donc $g \in \mathbb{Q}[X]$ unitaire tel que $f = gf_\alpha$. Comme g et f_α sont unitaires, ils sont de contenu $\leqslant 1$. Mais alors l'égalité $1 = C(f) = C(f_\alpha)C(g)$ implique que ces contenus sont égaux à 1, i.e. que f_α et g sont dans $\mathbb{Z}[X]$.

c) Soient α, β deux entiers algébriques et n, m les degrés respectifs de f_α et f_β. Alors $\mathbb{Z}[\alpha, \beta]$ est de type fini, engendré par les $\alpha^i \beta^j$ pour $0 \leqslant i < n$ et $0 \leqslant j < m$.

Argument rapide : puisque $\mathbb{Z}$ est noethérien, le sous-module $\mathbb{Z}[\alpha + \beta]$ de $\mathbb{Z}[\alpha, \beta]$ est aussi de type fini, donc $\alpha + \beta$ est un entier algébrique d'après a). Idem pour $\alpha\beta$.

Argument constructif : Soit $M_\alpha \in \mathcal{M}_{nm}(\mathbb{Z})$ la matrice carrée de taille nm constituée de m blocs diagonaux de taille n égaux à la matrice compagnon de f_α. C'est la matrice de la multiplication par α dans la famille génératrice des $\alpha^i \beta^j$ ordonnée lexicographiquement. Par ailleurs, soit M_β la matrice carrée de taille nm obtenue en remplaçant les scalaires a_{kl} par des matrices diagonales $a_{kl} I_n$ de taille n dans la matrice compagnon de f_β. Alors M_β est la matrice de la multiplication par β dans la famille génératrice des $\alpha^i \beta^j$ ordonnée lexicographiquement. On a donc des diagrammes commutatifs

$$\begin{array}{ccc} \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \\ {\scriptstyle M_\alpha}\downarrow & & \downarrow{\scriptstyle \times\alpha} \\ \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \\ {\scriptstyle M_\beta}\downarrow & & \downarrow{\scriptstyle \times\beta} \\ \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \end{array}$$

dans lequel les flèches horizontales envoient l'élément e_k, $0 \leqslant k < nm$, de la base canonique de $\mathbb{Z}^{nm}$ sur $\alpha^i \beta^j$ si $k = i + nj$. On en déduit que pour tout polynôme $f \in \mathbb{Z}[X]$, la multiplication par $f(\alpha + \beta)$ est donnée par la matrice $f(M_\alpha + M_\beta) \in \mathcal{M}_{nm}(\mathbb{Z})$ dans la famille génératrice des $\alpha^i \beta^j$ ordonnée lexicographiquement, au sens où le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \\ {\scriptstyle f(M_\alpha+M_\beta)}\downarrow & & \downarrow{\scriptstyle \times f(\alpha+\beta)} \\ \mathbb{Z}^{nm} & \twoheadrightarrow & \mathbb{Z}[\alpha,\beta] \end{array} .$$

Appliquons ce diagramme au polynôme caractéristique f de la matrice $M_\alpha + M_\beta$, qui est bien unitaire et dans $\mathbb{Z}[X]$. Par le théorème de Cayley-Hamilton, on a $f(M_\alpha + M_\beta) = 0$ donc la multiplication par $f(\alpha + \beta)$ sur $\mathbb{Z}[\alpha, \beta]$ est nulle. Par intégrité, on a donc $f(\alpha + \beta) = 0$ et $\alpha + \beta$ est bien entier algébrique. Idem pour $\alpha\beta$ en utilisant $M_\alpha M_\beta$.

Exercice 6. Montrer qu'un rationnel $z \in \mathbb{Q}$ est entier algébrique si et seulement si il est entier.

Exercice 7. (Corps quadratiques)

a) Soit $D \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré et $\sqrt{D}$ une racine carrée de D dans $\mathbb{C}$. Montrer que $\mathbb{Q}[\sqrt{D}]$ est un sous-corps de $\mathbb{C}$ qui est de dimension 2 sur $\mathbb{Q}$.

b) Soit F un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$. Montrer qu'il existe D comme au (a) tel que $F = \mathbb{Q}[\sqrt{D}]$.

c) Soit $\mathcal{O}_D$ l'anneau des entiers algébriques de $\mathbb{Q}[\sqrt{D}]$. Montrer que

$$\mathcal{O}_D = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{si } D \equiv 2, 3[4] \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{si } D \equiv 1[4] \end{cases}$$

Solution. a) Le polynôme minimal de $\sqrt{D}$ étant de degré 2, on a $\mathbb{Q}[\sqrt{D}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$. En particulier, c'est une algèbre intègre de dimension finie sur $\mathbb{Q}$, donc un corps.

b) Soit $\alpha \in F \setminus \mathbb{Q}$. Alors $(1, \alpha)$ est une famille $\mathbb{Q}$-libre de F et donc une $\mathbb{Q}$-base. Il existe donc $a, b \in \mathbb{Q}$ tels que $\alpha^2 = a\alpha + b$. Écrivons cette égalité sous la forme $(\alpha - \frac{a}{2})^2 = \frac{a^2}{4} + b = \frac{r}{s}$ avec $r, s \in \mathbb{Z}$ premiers entre eux. En posant $\beta := s(\alpha - \frac{a}{2})$, on a $\beta^2 = rs$ et $F = \mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$. Soit alors D l'unique entier sans facteur carré tel que rs/D soit un carré d'entier, disons N^2. On a $F = \mathbb{Q}[N\sqrt{D}] = \mathbb{Q}[\sqrt{D}]$.

c) Remarquons que $\sqrt{D}$ est évidemment un entier algébrique, donc $\mathbb{Z}[\sqrt{D}] \subset \mathcal{O}_D$. Soit $\alpha = a + b\sqrt{D}$ un élément de $F \setminus \mathbb{Q}$ (donc $b \neq 0$). Alors f_α est de degré 2 et l'égalité $(\alpha - a)^2 = b^2 D$ nous donne $f_\alpha = X^2 - 2aX + (a^2 - b^2 D)$. D'après la question b) de l'exercice précédent, α est entier algébrique si et seulement si on a $2a \in \mathbb{Z}$ et $(a^2 - b^2 D) \in \mathbb{Z}$. Deux cas se présentent :
— Si $a \in \mathbb{Z}$, alors $b^2 D \in \mathbb{Z}$. Mais comme D est sans facteur carré, cela implique que $b \in \mathbb{Z}$, i.e. $\alpha \in \mathbb{Z}[\sqrt{D}]$.

— Si $a \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$, alors posons $a' := 2a$ et $b' := 2b$. On a $a' \in \mathbb{Z}$, donc $(b')^2 D \in \mathbb{Z}$ et, comme ci-dessus, $b' \in \mathbb{Z}$. Notons que b ne peut être entier car $a = \alpha - b\sqrt{D}$ ne l'est pas. Donc b' et a' sont impairs, et il s'ensuit que $(a')^2$ et $(b')^2$ sons congrus à 1 modulo 4. Or, $(a')^2 - (b')^2 D \in 4\mathbb{Z}$, donc $D \equiv 1[4]$. Dans ce cas, le nombre $\alpha_D := \frac{1+\sqrt{D}}{2}$ est dans $\mathcal{O}_D$ car son polynôme minimal $X^2 - X + \frac{1+\sqrt{D}}{2}$ est dans $\mathbb{Z}[X]$. On a alors $\alpha - \alpha_0 = (a - \frac{1}{2}) + (b - \frac{1}{2})\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ par l'alinea précédent. Il s'ensuit que $\alpha \in \alpha_D + \mathbb{Z}[\sqrt{D}]$.

On trouve ainsi que $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}]$ si D n'est pas congru à 1 modulo 4, et $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}] \cup (\alpha_D + \mathbb{Z}[\sqrt{D}]) = \mathbb{Z}[\alpha_D]$ si $D \equiv 1[4]$.

3 Anneaux euclidiens, principaux, factoriels

Exercice 8. Montrer que le polynôme $X_1^2 + \cdots + X_n^2$ est irréductible pour $n \geqslant 2$ dans $\mathbb{R}[X_1, \cdots, X_n]$ et pour $n \geqslant 3$ dans $\mathbb{C}[X_1, \cdots, X_n]$.

Solution. Posons $A = \mathbb{R}[X_1, \cdots, X_{n-1}]$ et regardons le polynôme $X_1^2 + \cdots + X_n^2$ comme un élément $P(X_n)$ dans $A[X_n] = \mathbb{R}[X_1, \cdots, X_n]$. On sait que A est factoriel et que $A^\times = \mathbb{R}^\times$ (car B intègre $\Rightarrow B[X]^\times = B^\times$). Donnons-nous une factorisation $P = QR$ dans $A[X_n]$. Comme P est unitaire, on peut supposer Q et R unitaires, quittes à multiplier P par un inversible de A (donc dans $\mathbb{R}^\times$) et Q par son inverse. On a $\deg_{X_n}(Q) + \deg_{X_n}(R) = 2$, donc si $\deg_{X_n}(Q) = 0$, alors Q est dans A et unitaire donc $Q = 1$. De même pour R. On en déduit que toute factorisation non triviale est de la forme $P = (f + X_n)(g + X_n)$ avec $f, g \in A$. En regardant le terme de degré 1 du produit on a $f = -g$, et on en déduit l'équation $f^2 = -(X_1^2 + \cdots + X_{n-1}^2)$. Pour des raisons de degré et de terme constant, un tel f est de la forme $a_1 X_1 + \cdots + a_{n-1} X_{n-1}$. En effet, si un monôme $X_1^{n_1} \cdots X_{n-1}^{n_{n-1}}$ de degré total $\sum_i n_i > 1$ apparaît avec coefficient $\alpha_{n_1, \cdots, n_{n-1}}$ non nul dans f, on peut en trouver un maximal pour un ordre lexicographique bien choisi sur le multi-degré $(n_1, \cdots, n_{n-1})$, et on voit alors que le coefficient de $X_1^{2n_1} \cdots X_{n-1}^{2n_{n_1}}$ dans f^2 est $(\alpha_{n_1, \cdots, n_{n-1}})^2$ qui est non nul, ce qui est incompatible avec l'équation $f^2 = -(X_1^2 + \cdots + X_{n-1}^2)$. En développant, on constate que $a_i^2 = -1$ et $a_i a_j = 0$ si $i \neq j$. Ceci n'est possible que si $1 = n - 1$ et -1 est un carré.

Exercice 9. Soit $P = a_n X^n + \cdots + a_0$ un élément de $\mathbb{Z}[X]$. Et soit $r = \frac{p}{q} \in \mathbb{Q}$ une racine de P (avec $p \wedge q = 1$).

a) Montrer que $qX - p$ divise P dans $\mathbb{Z}[X]$.

b) En déduire que $p | a_0$, $q | a_n$, $(p - q) | P(1)$ et $(p + q) | P(-1)$.

c) Trouver les racines rationnelles de $A(x) = x^3 - 6x^2 + 15x - 14$ et $B(x) = x^4 - 2x^3 - 8x^2 + 13x - 24$.

Exercice 10. a) Trouver un pgcd de $X^6 - 1$ et de $X^4 - 1$ dans $\mathbb{C}[X]$, par factorisation et par l'algorithme d'Euclide.

b) Résoudre dans $\mathbb{C}[X]^2$, l'équation $P(X)(X^6 - 1) + Q(X)(X^4 - 1) = X^3 + 2X^2 - X - 2$.

c) Résoudre la même équation dans $\mathbb{R}[X]$.

Exercice 11. Soit p un nombre premier.

a) Montrer que $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2 + 1)$.

b) En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.

Exercice 12. Factorisations et congruences

a) Soit $P(X) = X^4 + 1$. Décomposer P dans $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ en produits de facteurs irréductibles.

b) Montrer que -1 ou 2 ou -2 est un carré dans $\mathbb{F}_p$ pour tout p.

c) Montrer que $X^4 + 1$ est factorisable dans $\mathbb{F}_p$ pour tout p (on utilisera les égalités $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2 = (X^2)^2 - (-1)$).

Exercice 13. Montrer que $P(X) = (X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbb{Q}[X]$ si les a_i sont des entiers distincts.

Exercice 14. a) Montrer que $\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{-2}]$ sont euclidiens avec stathme $z \mapsto |z|^2$.

b) Montrer que $\mathbb{Z}[\sqrt{-3}]$ n'est pas principal, mais que $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ est euclidien.

Solution. a) Pour $\mathbb{Z}[i]$, le point clef est le suivant : pour tout $z \in \mathbb{C}$, il existe un élément $q_1 \in \mathbb{Z}[i]$ (pas nécessairement unique) tel que z appartienne au carré de sommets $q_1, q_1+1, q_1+i, q_1+1+i$. Soit alors q l'un des sommets de ce carré le plus proche de z. On a $|z-q|^2 \leqslant \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$. Soient maintenant $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, posons $z := a/b$ et choisissons q comme ci-dessus. On a $|a-bq|^2 \leqslant \frac{1}{2}|b|^2$, donc $|.|^2$ est bien un stathme euclidien.

Pour $\mathbb{Z}[\sqrt{-2}]$, on raisonne de même : pour tout $z \in \mathbb{C}$, il existe un élément $q_1 \in \mathbb{Z}[\sqrt{-2}]$ (pas nécessairement unique) tel que z appartienne au rectangle de sommets $q_1, q_1+1, q_1+i\sqrt{2}, q_1+1+i\sqrt{2}$. Soit alors q l'un des sommets de ce rectangle le plus proche de z. On a $|z-q|^2 \leqslant \frac{1}{4}+\frac{1}{2} = \frac{3}{4}$. Comme ci-dessus, en appliquant ceci à $z := a/b$ avec $a, b \in \mathbb{Z}[i]$, on a $|a-bq|^2 \leqslant \frac{3}{4}|b|^2$, donc $|.|^2$ est bien un stathme euclidien.

b) Posons maintenant $A = \mathbb{Z}[\sqrt{-3}]$ et suivons la même stratégie. Pour tout $z \in \mathbb{C}$ il existe bien q_1 dans A tel que z appartienne au rectangle de sommets $q_1, q_1+1, q_1+i\sqrt{3}, q_1+1+i\sqrt{3}$. Si q_2 désigne le sommet le plus proche de z, on a $|z-q_2|^2 \leqslant \frac{1}{4}+\frac{3}{4} = 1$, l'égalité étant atteinte si et seulement si z est au centre du rectangle. Le fait que l'inégalité stricte ne soit pas toujours vraie montre que $|.|^2$ n'est pas un stathme sur A. En revanche, posons $A' := \mathbb{Z}[j] = \mathbb{Z} \oplus \mathbb{Z}j$ avec $j = \frac{1+i\sqrt{3}}{2}$. Le centre du rectangle est justement $q_1 + j$, donc est dans A'. Il s'ensuit que le point q de A' le plus proche de z vérifie l'inégalité *stricte* $|z-q|^2 < 1$. On en déduit comme au (a) que $|.|^2$ est bien un stathme euclidien sur A'.

Montrons maintenant que A n'est pas factoriel (et donc pas principal, et encore moins euclidien). Pour cela, considérons l'égalité $(1+i\sqrt{3})(1-i\sqrt{3}) = 4 = 2.2$. Pour que cette égalité contredise l'unicité des décompositions en produit d'irréductibles, il faut vérifier que 2 et $(1 \pm i\sqrt{3})$ sont irréductibles et non associés. Supposons que $1+i\sqrt{3} = xy$ avec $x, y \in A$. Alors $|xy|^2 = 4$. En écrivant $x = a+ib\sqrt{3}$ avec $a, b \in \mathbb{Z}$, on voit que $|x|^2 = a^2+3b^2$ ne peut pas être égal à 2. Si $|x|^2 = 1$, alors x est inversible dans A d'inverse $\bar{x}$, et si $|x|^2 = 4$ alors c'est y qui est inversible. D'où l'irréductibilité de $1+i\sqrt{3}$. De même pour celle de $1-i\sqrt{3}$ et celle de 2. Reste à voir que 2 et $1 \pm i\sqrt{3}$ ne sont pas associés, mais c'est clair car $A^\times = \{\pm 1\}$. Donc A n'est pas factoriel. Remarquons que la même égalité $(1+i\sqrt{3})(1-i\sqrt{3}) = 4 = 2.2$ reste évidemment vraie dans A' et que 2 et $1 \pm i\sqrt{3}$ sont toujours irréductibles, *mais* les égalités $2j = 1+i\sqrt{3}$ et $2\bar{j} = 1-i\sqrt{3}$ montrent que 2 et $1 \pm i\sqrt{3}$ sont associés car j est inversible dans A' (d'inverse $\bar{j}$). Donc cette égalité ne contredit pas l'unicité des décompositions (heureusement, puisqu'on a prouvé au-dessus que A' est euclidien).

Exercice 15. a) Soit R un anneau euclidien. Montrer qu'il existe $x \in R$ non inversible tel que $R^\times \cup \{0\} \to R/(x)$ soit surjective.

b) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer $A^\times$ et montrer que A n'est pas euclidien.

c) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x-q| < 1$ ou $|2x-q| < 1$. On pose $x = u+iv$ avec $u, v \in \mathbb{R}$.

i) Se ramener au cas où $v \in [0, \sqrt{19}/4]$.

ii) Montrer que si $v \in [0, \sqrt{3}/2[$, il existe $q \in \mathbb{Z}$ tel que $|x-q] < 1$.

iii) Montrer que si $v \in [\sqrt{3}/2, \sqrt{19}/4]$, $\sqrt{19}/2 - 2v \in [0, \sqrt{3}/2[$ et en déduire $q \in A$ tel que $|2x-q| < 1$.

d) Soient $a, b \in A \backslash 0$. Montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq+r$, soit $2a = bq+r$.

e) Montrer que (2) est un idéal maximal de A (on pourra soit écrire la table de multiplication de $A/(2)$, soit vérifier que X^2+X+5 est un polynôme irréductible de $\mathbb{Z}/(2)[X]$).

f) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Montrer que $2I \subset (b) \subset I$.

g) Montrer que A est principal.

Solution. a) Soit $x \in R - (R^\times \cup \{0\})$ tel que $v(x)$ soit minimal. Alors si $y \in R$, il existe $q, r \in R$ tel que $y = qx+r$ (et donc $\bar{y} = \bar{r}$) et $v(r) < v(x)$, donc $r \in R^\times \cup \{0\}$. Donc $\bar{y}$ est l'image de r par l'application $R^\times \cup \{0\} \to R/(x)$

b) Soit $N(z) = z\bar{z} \in \mathbb{Z}$. Alors z est inversible si et seulement si $N(z) = 1$. Mais si $z = a+b\frac{1+i\sqrt{19}}{2}$, $N(z) \geqslant 19b^2/4 > 1$ dès que $b \neq 0$. On en déduit $R^\times = \{1, -1\}$.

Soit maintenant $x \in A$ tel que $A^\times \cup \{0\} \to A/(x)$ est surjective. Alors si $y \in A$, x divise y, $y+1$ ou $y-1$, et donc $N(x)$ divise $N(y)$, $N(y+1)$ ou $N(y-1)$. En prenant $y = 2$, on obtient $N(x)$ divise 1, 4 ou 9 et en prenant $y = (1+i\sqrt{19})/2$, on obtient $N(x)$ divise 5 ou 7. Comme $1 \times 4 \times 9$ et 5×7 sont premiers entre eux, $N(x) = 1$, donc x est inversible. D'après la question précédente, A n'est donc pas euclidien.

c) i) Soit $n \in \mathbb{Z}$ tel que $|4v/\sqrt{19} - n| \leqslant 1/2$. Soit $x' = x - n\frac{1+i\sqrt{19}}{2}$. Il suffit de résoudre le problème pour x'. On pose $x' = u' + iv'$. On a $v' \in [-\sqrt{19}/4, \sqrt{19}/4]$. Si $v' \geqslant 0$, on s'est ramené au cas voulu ; sinon, on remplace x' par $-x'$.

ii) Soit $n \in \mathbb{Z}$ tel que $|u - n| \leqslant 1/2$. Alors $|x - n|^2 = |u - n|^2 + |v|^2 < 1/4 + 3/4 = 1$.

iii) Comme $v \leqslant \sqrt{19}/4$, on a $\sqrt{19}/2 - 2v \geqslant 0$. Pour l'autre inégalité, il suffit de vérifier que $3\sqrt{3}/2 \geqslant \sqrt{19}/2$,ce qui provient du fait que $27 \geqslant 19$. Du coup, $\frac{1+i\sqrt{19}}{2} - 2x$ vérifie les conditions de ii), d'où $n \in \mathbb{Z}$ tel que $|\frac{1+i\sqrt{19}}{2} - 2x - n| < 1$ et il suffit de poser $q = \frac{1+i\sqrt{19}}{2} - n$.

d) On applique c) à $x = a/b$ et on pose $r = b(x - q) = a - bq$ ou $r = b(2x - q) = 2a - bq$ en fonction des cas.

e) Le nombre $\frac{-1+i\sqrt{19}}{2}$ est racine de $X^2 + X + 5$, d'où un morphisme surjectif $f : \mathbb{Z}[X]/(X^2 + X + 5) \to \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ envoyant X sur $\frac{1+i\sqrt{19}}{2}$. Comme les deux sont des $\mathbb{Z}$-modules libres de rang 2, et que f envoie la base $(1, X)$ sur la base $(1, \frac{1+i\sqrt{19}}{2})$, c'est un isomorphisme.
Il suffit donc de montrer que $A/(2) = \mathbb{Z}[X]/(X^2 + X + 5, 2) = \mathbb{F}_2[X]/(X^2 + X + 5)$ est un corps, et donc de montrer que $P = X^2 + X + 5$ est irréductible sur $\mathbb{F}_2$. Comme le degré de P est 2 il suffit de vérifier qu'il n'y a pas de racines dans $\mathbb{F}_2$, ce qui est immédiat.

f) Remarquons que $|z|^2 \in \mathbb{N}$ donc il existe bien $b \in I - \{0\}$ minimisant $|b|^2$. Comme $b \in I$, $(b) \subset I$. Si $a \in I$. On applique c) : si $a = bq + r$, alors $r = a - bq \in I$ et par minimalité de $|b|$, $r = 0$, donc $a \in (b)$ et donc $2a \in (b)$. Si $2a = bq + r$ alors $2a \in (b)$ par le même argument.

g) Soit, I un idéal de A. On a $(2b) \subset 2I \subset (b)$. Or, d'après la question (e), $(2b)$ est maximal parmi les idéaux de A contenus dans (b) (car la multiplication par b induit une bijection croissante des idéaux de A vers les idéaux de A contenant b). Il s'ensuit que $2I = (b)$ ou $(2b)$ est principal. Comme A est intègre, I est principal aussi.