DEUXIÈME PARTIE : ANNEAUX

Cette partie est consacrée à l'étude des anneaux. Au premier semestre ont été vues les notions d'anneaux principaux et euclidiens. Le théorème de *décomposition en produits d'irréductibles* dans un anneau principal unifie les situations déjà connues dans $\mathbf{Z}$ et $k[X]$. Ce résultat invite à étudier les propriétés des anneaux jouissant de cette propriété, les anneaux *factoriels*.

0. Rappels et compléments

0.1. Anneaux, idéaux.

Définition 0.1.1. Un *anneau unitaire* $(A, +, \times)$ est un ensemble non vide muni de deux lois internes $+$ et $\times$ qui vérifient les propriétés suivantes :
— $(A, +)$ est un groupe abélien d'élément neutre 0, ou 0_A ;
— la multiplication $\times$ est associative et possède un élément neutre 1, ou 1_A ;
— la loi $\times$ est distributive par rapport à l'addition $+$.
Un *anneau commutatif unitaire* est un anneau unitaire dont le produit est commutatif.

Remarque 0.1.2. L'anneau nul $\{0\}$ est un anneau commutatif unitaire, dans lequel $1_{\{0\}} = 0_{\{0\}}$.

Convention : dans toute la suite, les anneaux considérés seront commutatifs et unitaires. Nous supposerons de plus que les morphismes d'anneaux conservent les éléments unités : ainsi, un morphisme d'anneaux $f\colon A \to B$ est une application si $f(x +_A y) = f(x) +_B f(y)$, $f(x \cdot_A y) = f(x) \cdot_B f(y)$ et $f(1_A) = 1_B$.

Définition 0.1.3. On appelle *élément inversible*, ou *unité*[1], tout élément a tel qu'il existe $b \in A$ tel que $ab = 1$. On note $A^\times$ (ou A^*) l'ensemble des inversibles. C'est un groupe, appelé *groupe des unités* : $A^\times = \{a \in A | \exists b \in A, ab = 1\}$.

Exemple 0.1.4. Dans $\mathbf{Z}$, les unités sont 1 et -1 : $\mathbf{Z}^\times = \{1, -1\}$. Dans $\mathbf{Z}/n\mathbf{Z}$, $(\mathbf{Z}/n\mathbf{Z})^\times = \{\bar{k} | 1 \leqslant k \leqslant n-1, (k, n) = 1\}$.

Définition 0.1.5. Un anneau (commutatif) est un *corps* (commutatif), si tout élément non nul est inversible, autrement dit si $A^\times = A \setminus \{0\}$.

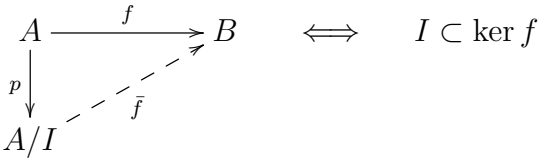
Définition 0.1.6. Un *idéal* de A est un sous-ensemble $I \subset A$ qui est un sous-groupe pour l'addition et vérifie : $\forall a \in A, aI \subset I$.

Exemple 0.1.7. Les idéaux de $\mathbf{Z}$ sont les $a\mathbf{Z}$, $a \in \mathbf{Z}$: en effet, ce sont des idéaux, et, inversement, tout sous-groupe additif de $\mathbf{Z}$ est de cette forme.
Le noyau de tout morphisme d'anneaux est un idéal.

Proposition-Définition 0.1.8 (Quotient et propriété universelle)**.** *Soit $I \subset A$ un idéal d'un anneau A. Alors il existe sur A/I une unique structure d'anneau faisant de la surjection canonique $p_I\colon A \to A/I$ un morphisme d'anneaux.*
On appelle anneau quotient *et on note encore A/I l'anneau ainsi défini.*

Date: 11 mars 2021.
1. Attention à ne pas confondre unité, et élément unité.

Ce quotient jouit de la propriété universelle *suivante : un morphisme d'anneaux $f\colon A \to B$ se factorise via $p\colon A \to A/I$ (i.e. il existe un morphisme d'anneaux $\bar{f}\colon A/I \to B$ tel que $f = \bar{f} \circ p$) si et seulement si $I \subset \ker f$:*



$\iff \quad I \subset \ker f$

et $\operatorname{im} \bar{f} = \operatorname{im} f$, $\ker \bar{f} = \ker f/I$.

Pour tout anneau unitaire A on dispose d'un morphisme canonique $\iota_A\colon \mathbf{Z} \to A$ défini par $k \to k1_A$. Son noyau est un idéal de $\mathbf{Z}$, de la forme $m_A\mathbf{Z}$ avec $m_A \geqslant 0$. D'après la proposition précédente, $\iota_A(\mathbf{Z})$ est un sous-anneau de A, isomorphe à l'anneau $\mathbf{Z}/m_A\mathbf{Z}$. L'entier m_A s'appelle la *caractéristique* de l'anneau A. La caractéristique de l'anneau nul est égale à 1.

On définit plusieurs opérations sur les idéaux :

— **intersection** : l'*intersection* $I \cap J$ de deux idéaux de A est encore un idéal. Plus généralement, l'intersection $\bigcap_{\lambda\in\Lambda} I_\lambda$ d'une famille quelconque d'idéaux $\{I_\lambda\}_{\lambda\in\Lambda}$ est un idéal ;

— **idéal engendré par un élément** : si $a \in A$, l'ensemble $aA = \{ax, x \in A\}$ est un idéal de A : c'est l'idéal engendré par a (i.e. le plus petit idéal engendré par a). On appelle *idéal principal* un idéal engendré par un élément ;

— **somme** : la *somme* de deux idéaux I et J est l'idéal $I + J = \{i+j, i \in I, j \in J\}$, c'est le plus petit idéal contenant I et J. La somme d'une famille quelconque d'idéaux I_λ est l'ensemble des sommes finies $\sum x_\lambda$ d'éléments $x_\lambda \in I_\lambda$;

— **idéal engendré par une famille finie d'éléments** : l'idéal engendré par une famille finie $a_1, \ldots, a_n$ d'éléments est $(a_1) + (a_2) + \cdots + (a_n) = \{\sum_i a_i x_i, x_i \in A\}$. C'est le plus petit idéal contenant les a_i, on le note $(a_1, \ldots, a_n)$. Un idéal est dit *de type fini* s'il est engendré par un nombre fini d'éléments ;

— **produit** : l'*idéal produit* IJ est l'idéal engendré par les produits ij pour $i \in I$ et $j \in J$:

$$\{i_1j_1 + i_2j_2 + \cdots + i_mj_m, m \in \mathbf{N}, i_k \in I, j_k \in J\}.$$

Lemme 0.1.9. *Soient I et J deux idéaux. Alors $IJ \subset I \cap J$.*

La réciproque est fausse en général : dans $\mathbf{Z}$, $2\mathbf{Z} \cap 2\mathbf{Z} = 2\mathbf{Z} \supsetneq 4\mathbf{Z} = (2\mathbf{Z})(2\mathbf{Z})$.

Proposition 0.1.10 (Lemme chinois)**.** *Soient I, J deux idéaux de A tels que $I + J = A$. Alors $IJ = I \cap J$ et on a un isomorphisme d'anneaux*

$$A/IJ \simeq A/I \times A/J.$$

Démonstration. Soit $f\colon x \in A \mapsto (p_I(x), p_J(x))$ où $p_I\colon A \to A/I$ et $p_J\colon A \to A/J$ sont les projections canoniques. Alors $\ker f = I \cap J$. Par ailleurs, f est surjective. En effet, soit $(\bar{a}, \bar{b}) \in A/I \times A/J$. Par hypothèse, il existe $i \in I$ et $j \in J$ tels que $i + j = 1$. Considérons, si a et $b \in A$ vérifient $p_I(a) = \bar{a}$ et $p_J(b) = \bar{b}$, l'élément [2] $x = aj + bi$. Alors $f(x) = (\bar{a}, \bar{b})$: en effet, $x = aj + bi =$

2. Il convient de motiver le choix de cet élément : pour montrer la surjectivité, il suffit en fait de relever dans A les éléments $(1_{A/I}, 0_{A/J})$ et $(0_{A/I}, 1_{A/J})$. Or, l'égalité $i+j = 1$ permet d'écrire $j = 1-i$, ce qui signifie que $f(j) = (1, 0)$. Elle permet aussi d'écrire $i = 1 - j$, ce qui signifie $f(i) = (0, 1)$. Pour relever $(\bar{a}, \bar{b})$, on est donc naturellement amené à considérer $aj + bi$.

$a(1-i)+bi = a+(b-a)i \in a+I$ et $x = aj+b(1-j) \in b+J$. Donc f induit un isomorphisme d'anneaux $A/IJ \xrightarrow{\sim} A/I \times A/J$.

Par ailleurs, on a toujours $IJ \subset I \cap J$ et, si $x \in I \cap J$, alors $x = x \cdot 1 = x(i+j) = xi+xj$, et $x \in J \Rightarrow xi \in IJ$ et $x \in I \Rightarrow xj \in IJ$ assurent $x \in IJ$. □

— **image réciproque** : si $f\colon A \to B$ morphisme d'anneaux, alors l'*image réciproque* $f^{-1}(I)$ de tout idéal I de B est un idéal de A :

$$I \subset B \text{ idéal } \implies f^{-1}(I) \text{ idéal de } A.$$

En général l'image directe d'un idéal n'est pas un idéal. C'est vrai pour les morphismes surjectifs. En particulier, pour la projection canonique $A \to A/I$, on obtient ainsi une description des idéaux du quotient A/I :

Proposition 0.1.11 (Idéaux d'un anneau quotient)**.** *Soient A un anneau, I un idéal. Alors les idéaux de A/I sont en bijection avec les idéaux de A contenant I via les deux applications*

$$\begin{array}{ccc} \{ \text{ idéaux de } A \text{ contenant } I\} & \overset{\sim}{\longleftrightarrow} & \{ \text{ idéaux de } A/I\} \\ J & \longmapsto & p(J) \\ p^{-1}(K) & \longleftarrow\!\shortmid & K \end{array}$$

où $p\colon A \to A/I$ est la projection canonique.

— **anneaux de polynômes à coefficients dans un anneau** : soit A un anneau. L'*anneau des polynômes à une indéterminée à coefficients dans A*, noté $A[X]$, est l'ensemble des suites $(a_n)_{n\in\mathbf{N}}$ presque nulles d'éléments de A (i.e. telles que $a_n = 0$ pour n assez grand) muni des lois $(a_n)_n + (b_n)_n = (a_n+b_n)_n$ et $(a_n)_n \cdot (b_n)_n = (\sum_{k=0}^n a_k b_{n-k})_n$.

L'anneau A s'identifie au sous-anneau $\{(a,0,0,\ldots), a \in A\}$: on notera encore $a = (a,0,0,\ldots)$.

Posons $X = (0,1,0,\ldots,0,\ldots)$. On vérifie par récurrence que X^k est la suite $(a_n)_{n\in\mathbf{N}}$ dont le seul terme non nul est $a_{k+1} = 1_A$. On peut ainsi écrire $P = (a_n)_n$ sous la forme usuelle $P = a_0 + a_1X + a_2X^2 + \cdots a_dX^d$ et effectuer les calculs comme on en a l'habitude (puisque $X^kX^l = X^{k+l}$).

On appelle *degré* d'un polynôme non nul $P = \sum_{n\geqslant 0} a_nX^n$ l'entier $\deg P = \max\{d \in \mathbf{N}, a_d \neq 0\}$. Par convention on pose $\deg 0 = -\infty$.

Proposition 0.1.12. *Soient $P, Q \in A[X]$:*

(i) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$*, avec égalité si* $\deg P \neq \deg Q$ *;*

(ii) $\deg(PQ) \leqslant \deg P + \deg Q$*, avec égalité si le produit des coefficients dominants de P et Q est non nul.*

Proposition 0.1.13 (Propriété universelle de $A[X]$)**.** *Un morphisme d'anneau $f\colon A[X] \to B$ est caractérisé par sa restriction $f_{|A}\colon A \to B$ à A et par l'image $f(X)$ de X. Autrement dit, se donner un morphisme d'anneaux $A[X] \to B$ revient à se donner un morphisme d'anneaux $A \to B$ et un élément de B.*

Remarque 0.1.14 (Anneau $A[X_1, X_2, \ldots, X_n]$)**.** On peut considérer l'anneau $A[X][Y]$ des polynômes en l'indéterminée Y à coefficients dans l'anneau $A[X]$, mais également l'anneau $A[Y][X]$ des polynômes en X à coefficients dans $A[Y]$. Ces deux anneaux sont canoniquement isomorphes : c'est, par exemple et par *abstract nonsense*, une conséquence de la propriété universelle. L'unique morphisme d'anneaux $A[X][Y] \to A[Y][X]$ correspondant au morphisme $A[X] \to A[Y][X]$

défini par $A \subset A[Y][X]$ et X, et à l'élément Y, et le morphisme $A[Y][X] \to A[X][Y]$ analogue sont des morphismes réciproques l'un de l'autre.

On note $A[X,Y] = A[X][Y] (= A[Y][X])$ l'anneau ainsi défini. Un morphisme d'anneaux $A[X,Y] \to B$ est la donnée d'un morphisme $A \to B$ et de deux éléments de B.

En répétant cette construction on définit l'anneau $A[X_1, X_2, \ldots, X_n]$ des polynômes à n indéterminées à coefficients dans A.

Enfin, on peut considérer la réunion croissante (ou, plus exactement, la limite inductive) $\bigcup_{n \geqslant 1} A[X_1, \ldots, X_n]$, pour les inclusions canoniques $A[X_1, \ldots, X_n] \subset A[X_1, \ldots, X_n][X_{n+1}] = A[X_1, \ldots, X_{n+1}]$. On obtient ainsi un anneau de polynômes à coefficients dans A à une infinité (dénombrable) d'indéterminées, noté $A[X_1, \ldots, X_n, \ldots]$ ou $A[X_n, n \geqslant 1]$.

0.2. **Intégrité, idéaux premiers, idéaux maximaux.**

Définition 0.2.1 (Anneau intègre)**.** Un *anneau intègre* est un anneau non nul dans lequel $ab = 0$ entraîne $a = 0$ ou $b = 0$:

$$\begin{cases} A \neq \{0\}, \\ \forall a, b \in A, ab = 0 \Longrightarrow a = 0 \text{ ou } b = 0. \end{cases}$$

Si A est non intègre, on appelle *diviseur de zéro* tout élément a non nul tel qu'il existe $b \neq 0$ vérifiant $ab = 0$.

Exemple 0.2.2. Un corps est un anneau intègre ; $\mathbf{Z}$ est intègre ; $\mathbf{Z}/4\mathbf{Z}$ ne l'est pas : $\bar{2}$ y est un diviseur de zéro.

Proposition 0.2.3. *Soit A un anneau intègre. Alors*

(i) $A[X]$ *est intègre,*

(ii) $\forall P, Q \in A[X]$, $\deg(PQ) = \deg P + \deg Q$,

(iii) $A[X]^\times = A^\times$.

Démonstration. L'anneau A étant non nul, $A[X]$ est aussi non nul. Soient P et Q deux polynômes non nuls. Ils s'écrivent $P = \sum_{k=0}^{d} a_k X^k$, avec $a_d \neq 0$, et $Q = \sum_{k=0}^{e} b_k X^k$, avec $b_e \neq 0$. On a donc $PQ = a_d b_e X^{d+e} + \underbrace{\cdots\cdots\cdots}_{\text{termes de degrés} < de}$. L'intégrité de A assure alors que $a_d b_e \neq 0$. On a donc $PQ \neq 0$ et de degré $\deg(PQ) = \deg P + \deg Q$. Cela prouve *(i)* et *(ii)*.

Soit $P \in A[X]^\times$. Il existe alors $Q \in A[X]$ tel que $PQ = 1$. On a donc $\deg P + \deg Q = \deg(PQ) = 0$ d'où $\deg P = 0 = \deg Q$. Ainsi P et Q sont constants, d'où $P \in A^\times$. □

Remarque 0.2.4. Si A n'est pas intègre, l'inclusion $A^\times \subset A[X]^\times$ peut être stricte. Ainsi, le polynôme non constant $1+2X \in (\mathbf{Z}/4\mathbf{Z})[X]$ est inversible (égal à son inverse).

Une des notions les plus essentielles est celle d'idéal premier.

Définition 0.2.5 (Idéal premier)**.** Soit A un anneau.

Un idéal $I \subset A$ est *premier* si A/I intègre.

Proposition 0.2.6. *Un idéal $I \subset A$ est premier si et seulement si*

$$\begin{cases} I \neq A, \\ ab \in I \Longrightarrow a \in I \text{ ou } b \in I. \end{cases}$$

Remarque 0.2.7. A intègre $\iff \{0\}$ est premier.

Exemple 0.2.8. Si $A = \mathbf{Z}$, $I = n\mathbf{Z}$ est premier si et seulement si $\pm n$ est premier ou $n = 0$.

Proposition 0.2.9. *Soit $f\colon A \to B$ un morphisme d'anneaux. L'image réciproque de tout idéal premier de B est un idéal premier de A :*

$$I \subset B \text{ premier } \implies f^{-1}(I) \subset A \text{ premier.}$$

Définition 0.2.10. Soit A un anneau. Un idéal I est *maximal* si $I \neq A$ et s'il est maximal (relativement à l'inclusion) parmi les idéaux différents de A : si $I \subset J$ et $J \neq A$, alors $J = I$.

Proposition 0.2.11. *Soit A un anneau. Pour tout idéal $I \subset A$, on a :*

$$I \text{ est maximal } \iff A/I \text{ est un corps.}$$

Corollaire 0.2.12. *Tout idéal maximal est premier.*

Démonstration (de 0.2.11). Supposons I maximal. Soit $\bar{x} \in A/I$ la classe d'un élément $x \in A$. Supposons $\bar{x} \neq 0$ (i.e. $x \notin I$). L'idéal $I + (x)$ contient alors strictement I, donc est égal à A. En particulier, il existe $i \in I$ et $a \in A$ tels que $1 = i + ax$. Ainsi $\bar{x}$ est inversible dans A/I, d'inverse $\bar{a}$. Le quotient A/I est donc un corps.

Réciproquement, supposons que A/I est un corps. Puisqu'un corps a au moins deux éléments, on a $I \neq A$. Soit $J \supsetneq I$. Si $x \in J \setminus I$, alors $\bar{x} \in A/I$ est non nul, donc inversible : il existe donc $a \in A$ tel que $ax \in 1 + I$. Alors $1 \in ax + I \subset J$, ce qui entraîne $J = A$. L'idéal I est donc maximal. □

Théorème 0.2.13 (Krull)**.** *Soit I un idéal de A, $I \neq A$. Alors il existe un idéal maximal $\mathfrak{m} \subset A$ contenant I :*

$$I \neq A \implies \exists \mathfrak{m} \text{ maximal}, I \subset \mathfrak{m}.$$

En particulier, tout anneau non nul possède un idéal maximal.

Démonstration. C'est une conséquence du lemme de Zorn (équivalent à l'axiome du choix) :

Tout ensemble inductif admet au moins un élément maximal.

Un *ensemble inductif* est un ensemble ordonné dans lequel tout sous-ensemble totalement ordonné possède un majorant.

Un sous-ensemble inductif est donc non vide, puisque le sous-ensemble vide possède un majorant. On reformule couramment la définition ainsi : un ensemble inductif est un ensemble non vide dans lequel tout sous-ensemble totalement ordonné non vide admet un majorant.

Soit donc I idéal de A, distinct de A. Considérons l'ensemble

$$\mathscr{J} = \{J \subset A \text{ idéal }, J \neq A, J \supset I\}$$

des idéaux de A distincts de A contenant I. C'est un ensemble ordonné par $\subset$, et tout sous-ensemble $(J_\lambda)_{\lambda\in\Lambda} \subset \mathscr{J}$ totalement ordonné possède un majorant $I \cup \bigcup_{\lambda\in\Lambda} J_\lambda$ (en effet, $I \cup \bigcup_{\lambda\in\Lambda} J_\lambda$ est un idéal, car le sous-ensemble est totalement ordonné, contient I, et est $\neq A$, puisqu'il ne peut contenir 1 ; il appartient donc à $\mathscr{J}$, et contient chacun des J_λ). C'est donc un ensemble inductif et, d'après le lemme de Zorn, il admet un élément maximal $\mathfrak{m}$. Cet élément est un idéal contenant I, et, tout idéal J tel que $\mathfrak{m} \subset J \subsetneq A$ appartient à $\mathscr{J}$, donc, par maximalité, est égal à $\mathfrak{m}$. Ainsi, $\mathfrak{m}$ est un idéal maximal, contenant I.

En appliquant ce résultat à l'idéal nul, on obtient l'existence d'un idéal maximal dans tout anneau non nul. □

1. Anneaux noethériens, théorème de la base de Hilbert

Si elle a un rôle tout à fait dispensable dans ce cours, la notion de *noethériannité* est une *condition de finitude* capitale en algèbre commutative.

Proposition-Définition 1.1 (Anneau noethérien)**.** *Soit A un anneau. Les propriétés suivantes sont équivalentes :*

(i) Tout idéal de A est de type fini.

(ii) Toute suite croissante $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ d'idéaux de A est stationaire (i.e. $\exists N, n \geqslant N \Rightarrow I_n = I_N$).

(iii) Tout ensemble non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Un anneau qui vérifie ces conditions est dit noethérien.

Démonstration.

$(i) \Rightarrow (ii)$: soit $(I_n)_{n\in\mathbf{N}}$ une suite croissante d'idéaux. Puisque la suite est croissante, la réunion $I = \bigcup_{n\in\mathbf{N}} I_n$ est un idéal, et, par hypothèse, il est de type fini, soit de la forme $I = (a_1, \ldots, a_r)$. Il existe alors N tel que $a_1, \ldots, a_r \in I_N$, et pour tout $n \geqslant N$, $I = (a_1, \ldots, a_r) \subset I_N \subset I_n \subset I$, d'où $I_n = I_N$.

$(ii) \Rightarrow (iii)$: soit $\mathscr{E}$ un ensemble non vide d'idéaux. Supposons que cet ensemble ne possède pas d'élément maximal. Construisons alors une suite (I_n) strictement croissante d'idéaux, qui contredit (ii). Soit $I_0 \in \mathscr{E}$ quelconque. Soit $n \geqslant 1$, et supposons construite $I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_{n-1}$, avec $I_k \in \mathscr{E}$. Puisque I_{n-1} n'est pas maximal dans $\mathscr{E}$, il existe $I_n \in \mathscr{E}$, $I_n \supsetneq I_{n-1}$. On construit ainsi une suite d'idéaux de A (appartenant à l'ensemble $\mathscr{E}$), strictement croissante, donc non stationnaire.

$(iii) \Rightarrow (i)$: soit I un idéal de A, et $\mathscr{E} = \{J \subset A \text{ idéal de type fini}, J \subset I\}$. C'est un ensemble d'idéaux non vide, car il contient (0). Soit J un idéal maximal de $\mathscr{E}$. Si $a \in I$, alors $J + (a) \in \mathscr{E}$ et $J + (a) \supset J$, donc, par maximalité de J, on a $J + (a) = J$, i.e. $a \in J$. On a donc $I \subset J$, et, puisque $J \subset I$, $I = J$, et I est donc de type fini. □

Remarque 1.2. Puisqu'un idéal principal est de type fini, un anneau principal (dont on rappelle la définition plus loin) est noethérien.

Cette notion est stable par passage au quotient :

Proposition 1.3. *Soient A un anneau noethérien, et I un idéal de A. Alors l'anneau quotient A/I est encore noethérien :*

$$A \text{ noethérien } \Longrightarrow A/I \text{ noethérien } .$$

Remarque 1.4. L'anneau des polynômes à une infinité (dénombrable) d'indéterminées $k[X_1, X_2, \ldots, X_n, \ldots]$ n'est pas noethérien.

L'anneau $\mathscr{O}(\mathbf{C})$ des fonctions *entières* (i.e. holomorphes dans tout le plan complexe) n'est pas noethérien.

Remarque 1.5. Un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien : si k est intègre, $k[X_i, i \in \mathbf{N}]$ est intègre, donc contenu (comme sous-anneau) dans son corps des fractions.

Le *théorème de la base* de Hilbert est un résultat fondamental, qui assure la noethériannité d'une très large classe d'anneaux.

Théorème 1.6 (Théorème de la base de Hilbert)**.** *Si A est noethérien, $A[X]$ l'est aussi :*

$$A \text{ noethérien } \Longrightarrow A[X] \text{ noethérien } .$$

Démonstration. Montrons que si $A[X]$ n'est pas noethérien, alors A non plus.

Soit donc $I \subset A[X]$ un idéal qui n'est pas de type fini. Construisons par récurrence une suite $(P_n)_{\in \mathbf{N}}$ d'éléments de I tels que pour tout $n \in \mathbf{N}$, $P_n \in I \setminus (P_0, \dots, P_{n-1})$ et $\deg P_n = \min\{\deg P, P \in I \setminus (P_0, \dots, P_{n-1})\}$. Puisque I est non nul, choisissons $P_0 \in I$ de degré d_0 minimal parmi les polynômes non nul appartenant à I : $d_0 = \min\{\deg P, P \in I \setminus \{0\}\}$. Puis, I étant différent de l'idéal principal (P_0), $P_1 \in I \setminus (P_0)$ de degré d_1 minimal dans $I \setminus (P_0)$. Supposons ainsi construits $P_0, P_1, \dots, P_n$ avec, pour tout $k = 0, \dots, n$, $P_k \in I \setminus (P_0, \dots, P_{k-1})$ de degré d_k minimal dans $I \setminus (P_0, \dots, P_{k-1})$. Alors, I n'étant pas de type fini, $I \supsetneq (P_0, \dots, P_n)$, et il existe donc $P_{n+1} \in I \setminus (P_0, \dots, P_n)$ de degré minimal $d_{n+1} = \min\{\deg P, P \in I \setminus (P_0, \dots, P_n)\}$.

On obtient ainsi une suite $(P_n)_{n \in \mathbf{N}}$ d'éléments de I comme annoncée. Notons que les degrés de ces polynômes forment une suite $(d_n)_n$ croissante.

Soit a_n le coefficient dominant de P_n. On a alors $a_{n+1} \notin (a_0, \dots, a_n)$ pour tout entier n : en effet, si $a_{n+1} = \sum_{i=0}^{n} b_i a_i$, alors $P_{n+1} - \sum_{i=0}^{n} b_i X^{d_{n+1}-d_i} P_i$ est un polynôme de degré $< d_{n+1}$ appartenant à $I \setminus (P_0, \dots, P_n)$, ce qui n'est pas.

La suite d'idéaux $\big((a_0, \dots, a_n)\big)_n$ est donc une suite strictement croissante d'idéaux de A, qui n'est ainsi pas noethérien. □

Corollaire 1.7. *Si A est noethérien, $A[X_1, \dots, X_n]$ l'est aussi.*

Rappelons qu'une A-algèbre est un anneau B muni d'un morphisme d'anneaux $f \colon A \to B$. Ce morphisme (non nécessairement injectif) revient à munir B d'une loi externe de multiplication scalaire $A \times B \to B, (a, b) \mapsto f(a)b$.

Une *A-algèbre de type fini* est une algèbre engendrée, comme A-algèbre, par un nombre fini d'éléments. Cela signifie qu'il existe $x_1, \dots, x_n \in B$ tels que B soit la plus petite sous-A-algèbre de B contenant les x_i, soit encore que tout élément de B s'écrive comme un polynôme $\displaystyle\sum_{I=(i_1,\dots,i_n)\in\mathbf{N}^n} a_I \prod_{k=1}^{n} x_k^{i_k}$ en les x_i à coefficients a_I dans A.

Ainsi, B est une A-algèbre de type fini si et seulement si c'est un quotient de l'anneau $A[X_1, \dots, X_n]$ pour un certain $n \in \mathbf{N}$, donc isomorphe à $A[X_1, \dots, X_n]/I$ pour un idéal I de $A[X_1, \dots, X_n]$.

Corollaire 1.8. *Si A est noethérien, toute A-algèbre de type fini*

$$A[X_1, \dots, X_n]/I$$

est noethérienne. En particulier, si k est un corps, toute k-algèbre de type fini est noethérienne.

Remarque 1.9. Soit k un corps. Le sous-anneau $A = \{a_{00} + \sum_{i>j} a_{ij} X^i Y^j, a_{ij} \in k\}$ de l'anneau noethérien $k[X, Y]$ n'est pas noethérien : en effet, l'idéal maximal noyau de l'évaluation $P \mapsto P(0)$ en 0 n'est pas de type fini (ou la suite $(X) \subsetneq (X, X^2Y) \subsetneq (X, X^2Y, X^3Y^2) \subsetneq \cdots \subsetneq (X, X^2Y, \dots, X^{n+1}Y^n) \subsetneq \cdots$ est strictement croissante).

C'est un nouvel exemple de sous-anneau non noethérien d'un anneau noethérien.

2. Propriétés arithmétiques : anneaux factoriels, principaux, euclidiens

Par propriétés *arithmétiques* d'un anneau, on entend celles relatives à la relation de divisibilité.

2.1. **Divisibilité.**

Définition 2.1.1 (Divisibilité)**.** Soient $a, b \in A$. On dit que a divise b, et on écrit $a|b$, si et seulement si il existe $c \in A$ tel que $b = ac$. On dit également que b est un multiple de a.

Cela admet une traduction essentielle en termes d'inclusion d'idéaux principaux :

Proposition 2.1.2. *Si $a, b \in A$, on a*

$$a|b \iff (b) \subset (a).$$

On peut également noter les traductions suivantes : pour tout $a \in A$, l'inclusion $\{0\} \subset (a)$ exprime que tout élément $a \in A$ divise 0, et, si $u \in A^\times$, l'égalité $(u) = A$ signifie qu'un inversible divise tout élément de A.

Remarque 2.1.3. La relation $b|a$ est un préordre (i.e. c'est une relation réflexive et transitive, mais pas antisymétrique en général). On lui associe la relation d'équivalence :

$$a\mathscr{R}b \Leftrightarrow a|b \text{ et } b|a \Leftrightarrow (a) = (b).$$

Proposition 2.1.4. *On suppose A intègre. Alors $a|b$ et $b|a$ si et seulement si il existe $u \in A^\times$ tel que $b = ua$.*

Démonstration. En effet, si $b = ca$ et $a = db$, alors $b = ca = cdb$, donc $b(1 - cd) = 0$. Puisque A est intègre, ou bien $b = 0$, auquel cas $a = 0$, ou bien $1 - cd = 0$, i.e. $c, d \in A^\times$ et $b = ca \in aA^\times$. □

Remarque 2.1.5. Si A n'est pas intègre, ce résultat tombe en défaut : soit $A = k[X, Y, Z]/X(1 - YZ)$ (k étant un corps, ou un anneau intègre), et x, y, z les images de X, Y et Z. On a $x = xyz$, donc $x|xy$ et $xy|x$. Mais il n'existe pas $u \in A^\times$ tel que $xy = ux$.

Montrons d'abord que $A^\times = k^\times$. Soit $p \in A^\times$ la classe d'un polynôme $P \in k[X, Y, Z]$. Il existe alors $Q \in k[X, Y, Z]$ tel que $X - XYZ|PQ - 1$. On a alors, modulo X, $\bar{P}\bar{Q} - 1 = 0$ dans $k[X, Y, Z]/X \simeq k[Y, Z]$. Comme $k[Y, Z]^\times = k^*$, on a $P = a + XP_1$ et $Q = a^{-1} + XQ_1$ avec $a \in k^\times$ et $P_1, Q_1 \in k[X, Y, Z]$. Alors $1 - YZ|aQ_1 + a^{-1}P_1 + XP_1Q_1$ dans $k[X, Y, Z]$. En considérant cette égalité dans $k[Y, Z][X]/(1 - YZ) \xrightarrow{\sim} (k[Y, Z]/(1 - YZ))[X]$, on obtient que $1 - YZ$ divise P_1 et Q_1 : en effet, $k[Y, Z]/(1 - YZ)$ est intègre (ce qu'on peut établir en constatant que le morphisme d'anneaux $k[Y, Z] \to k(T)$, $Y \to T$, $Z \to T^{-1}$ réalise $k[Y, Z]/(YZ - 1)$ comme un sous-anneau du corps des fractions rationnelles $k(T)$, ce qui en assure l'intégrité), et $\deg(aQ_1 + a^{-1}P_1 + XP_1Q_1) \geqslant \max(\deg P_1, \deg Q_1)$. Ainsi, $P, Q \in k^\times + (X - XYZ)$, d'où $p \in k^\times$.

On vérifie alors que, pour tout $u \in k^*$, $xy \neq ux$: on aurait sinon, dans $k[X, Y, Z]$, $(X - XYZ)|(XY - uX)$, ce qui est impossible pour des raisons de degré.

On suppose désormais A **intègre**.

Définition 2.1.6 (Éléments associés)**.** On dit que $a, b \in A$ sont *associés* si et seulement si il existe $u \in A^\times$ tel que $b = ua$.

Remarque 2.1.7. Ainsi a et b sont associés si et seulement si $a\mathscr{R}b$. L'application $a \longmapsto (a)$ induit une bijection strictement décroissante d'ensembles ordonnés de $A/\mathscr{R}$ muni de la relation de divisibilité sur l'ensemble $\mathscr{I}(A)$ des idéaux principaux de A muni de l'inclusion.

Définition 2.1.8 (Élément irréductible)**.** On dit qu'un élément $p \in A$ est *irréductible* s'il vérifie : $\begin{cases} p \notin A^\times, \\ p = ab \Longrightarrow a \in A^\times \text{ ou } b \in A^\times. \end{cases}$

Remarque 2.1.9.

(i) 0 n'est pas irréductible

(ii) Si A n'est pas un corps, p irréductible $\iff (p)$ maximal dans l'ensemble $\mathscr{I}(A) \setminus \{A\}$ des idéaux principaux de A distincts de A.

(iii) Dans $\mathbf{Z}$, les irréductibles sont les nombres premiers (et leurs opposés).

Définition 2.1.10 (Éléments premiers entre eux)**.** Soient $a, b \in A$. On dit que a et b sont *premiers entre eux* (ou *étrangers*) si et seulement si

$$\forall d \in A, d|a \text{ et } d|b \Longrightarrow d \in A^\times.$$

Définition 2.1.11 (Élément premier)**.** Un élément $p \in A$ est dit *premier* si l'idéal (p) est un idéal premier non nul. Autrement dit, si et seulement si

$$p \neq 0, p \notin A^\times \text{ et } p|ab \Longrightarrow p|a \text{ ou } p|b.$$

Proposition 2.1.12. *Dans un anneau intègre, tout élément premier est irréductible :*

$$p \text{ premier } \Longrightarrow p \text{ irréductible.}$$

Démonstration. Soit p premier. Alors p est non inversible. Supposons $p = ab$. Alors $p|ab$, donc $p|a$ ou $p|b$. Si $p|a$, alors $a = cp$, d'où $p = ab = bcp$ et, par intégrité, $bc = 1$, d'où $b \in A^\times$. De même, $p|b \Rightarrow a \in A^\times$. Ainsi p est irréductible. □

2.2. **Anneaux factoriels.** La notion de *factorialité* correspond à la propriété de décomposition, unique, en produit de facteurs premiers dans $\mathbf{Z}$. Mais toutes les propriétés de $\mathbf{Z}$ ne sont pas satisfaites dans un anneau factoriel général ; en particulier, le théorème de Bézout n'y a en général pas lieu.

Définition 2.2.1. Un anneau A est *factoriel* si

(O) A est intègre,

(E) tout élément $a \neq 0$ de A s'écrit $a = up_1 \cdots p_r$ avec $u \in A^\times$ et $p_1, \ldots, p_r$ irréductibles,

(U) cette décomposition est unique, à permutation près et à inversible près : si $a = up_1 \cdots p_r = vq_1 \cdots q_s$, alors $s = r$ et il existe $\sigma \in S_r$ tel que p_i et $q_{\sigma(i)}$ sont associés.

On peut reformuler cette définition de façon plus concrète en introduisant un *système de représentants des irréductibles* de A, c'est-à-dire un ensemble $\mathscr{P}$ d'irréductibles tel que pour tout irréductible p de A il existe un unique $q \in \mathscr{P}$ associé à p. Alors :

Définition 2.2.1 bis. Un anneau A est factoriel s'il est intègre et si tout élément $a \neq 0$ de A s'écrit de manière unique

$$a = u \prod_{p \in \mathscr{P}} p^{v_p(a)} \text{ avec } u \in A^\times \text{ et } v_p(a) \in \mathbf{N}.$$

On appelle l'entier $v_p(a)$ *valuation p-adique de a.*

Exemple 2.2.2. Dans $\mathbf{Z}$ on peut prendre comme système de représentants des irréductibles les nombres premiers.

Remarque 2.2.3. La valuation p-adique de a est le plus grand entier k tel que $p^k|a$, soit encore l'entier défini par $a \in (p^{v_p(a)}) \setminus (p^{v_p(a)+1})$.

Considérons la condition d'existence *(E)* : un élément $a \neq 0, \notin A^\times$ non irréductible peut s'écrire $a = bc$ avec b et c non associés à a. S'ils sont tous les deux irréductibles, on a une décomposition de a en produits d'irréductibles. Sinon, on peut réitérer l'opération. La question est de savoir si le processus s'arrête.

C'est le cas pour tout élément (non nul ni inversible) dans un anneau (intègre) noethérien :

Proposition 2.2.4. *Dans un anneau noethérien intègre, la condition (E) est vérifiée.*

Démonstration. On peut tout simplement suivre l'idée précédente : soit $a \in A$, $a \neq 0$. Si a est inversible, il s'écrit $a = a$ avec $a \in A^\times$. Sinon, remarquons d'abord que *dans un anneau noethérien intègre, tout élément $a \neq 0$ non inversible est divisible par un élément irréductible* : supposons en effet $a \neq 0$ non inversible, et sans diviseur irréductible, et écrivons a, qui n'est alors pas irréductible, ni inversible, $a = a_1 b_1$ avec a_1 et b_1 non associés à a (i.e. $(a) \subsetneq (a_1) \neq A$: en effet, si $(a) = (a_1)$, alors il existe $u \in A^\times$ tel que $a = a_1 u$, d'où $a = a_1 u = a_1 b_1 \overset{A \text{ intègre}}{\Longrightarrow} b_1 = u \in A^\times$) ; comme a_1 ne peut être irréductible, par hypothèse, et est non inversible, on peut l'écrire $a_1 = a_2 b_2$ avec $(a_1) \subsetneq (a_2) \neq A$, de sorte qu'on obtient ainsi une suite $((a_i))_{i \in \mathbf{N}^*}$ d'idéaux strictement croissante, qui contredit la noethérianité de A (pour un argument plus élégant, on peut considérer l'ensemble $\mathscr{E} = \{I \in \mathscr{I}(A) \setminus \{A\}, I \supset (a)\}$ des idéaux principaux de A, distincts de A, contenant a : c'est un ensemble d'idéaux non vide, car il contient (a) puisque $a \notin A^\times$, et il admet donc un élément maximal I ; un générateur p de l'idéal principal I est alors un irréductible divisant a, cf. Remarque 2.1.9 (ii)).

Il existe donc un irréductible $p_1 \in A$ qui divise a. Alors $a = p a_1$. Si $a_1 \in A^\times$, a s'écrit sous la forme attendue. Sinon, a_1 est à son tour divisible par un irréductible p_2 : $a_1 = p_2 a_2$. Le processus s'arrête, à nouveau par noethérianité : on construirait sinon une suite d'idéaux strictement croissante $((a_i))_i$.

Voici une autre démonstration, plus élégante, illustrant le *principe de récurrence noethérienne* : considérons l'ensemble d'idéaux

$$\mathscr{F} = \{(a) \in \mathscr{I}(A), a \neq 0 \text{ et } a \text{ n'est pas de la forme } a = u p_1 \cdots p_r\}.$$

En particulier, si $(a) \in \mathscr{F}$, a n'est ni inversible, ni irréductible.

Supposons $\mathscr{F}$ non vide, et soit (a) un élément maximal de $\mathscr{F}$ (qui existe car A est noethérien). Comme a n'est pas irréductible (ni inversible), il s'écrit $a = bc$ avec $b, c \notin A^\times$. On a donc $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$ (en effet, si par exemple $(a) = (b)$, alors $a = bu$ avec u inversible, puis $a = bu = bc$ entraîne, dans A intègre, $c = u \in A^\times$, ce qui n'est pas).

Alors, (a) étant maximal dans $\mathscr{F}$, les idéaux (b) et (c) ne sont pas dans $\mathscr{F}$, et on peut écrire $b = u p_1 \cdots p_r$ et $c = v q_1 \cdots q_s$ avec $u, v \in A^\times$ et $p_1, \ldots, p_r, q_1, \ldots, q_s$ irréductibles. On a ainsi $a = uv \cdot p_1 \cdots p_r q_1 \cdots q_s$ produit d'une unité uv et des irréductibles $p_1, \ldots, p_r, q_1, \ldots, q_s$, ce qui contredit l'appartenance de (a) à $\mathscr{F}$.

On en déduit que $\mathscr{F}$ est vide, ce qui signifie que tout élément non nul de A est produit d'un inversible et d'irréductibles : l'anneau A satisfait donc la condition *(E)*. □

Remarque 2.2.5.

(i) Factoriel n'implique pas noethérien (a fortiori, *(E)* n'entraîne pas noethérien). Par exemple l'anneau $k[X_1, \ldots, X_n, \ldots]$ des polynômes à une infinité d'indéterminées n'est pas noethérien, mais on verra plus loin qu'il est factoriel. En fait, on voit assez facilement qu'il satisfait la condition *(E)* : si $P \in k[X_i, i \in \mathbf{N}]$, il existe n tel que $P \in k[X_1, \ldots, X_n]$. Puisque $k[X_1, \ldots, X_n]$ est noethérien, donc P se décompose en irréductibles dans $k[X_1, \ldots, X_n]$. Il suffit de vérifier qu'un irréductible dans $k[X_1, \ldots, X_n]$ reste irréductible dans $k[X_i, i \in \mathbf{N}]$, mais cela résulte immédiatement de l'observation suivante : si $P, Q \in k[X_i, i \in \mathbf{N}]$ vérifient $PQ \in k[X_1, \ldots, X_n]$, alors $P, Q \in k[X_1, \ldots, X_n]$ (si $m > n$, on peut considérer PQ dans $k[X_1, \ldots, X_{m-1}][X_m]$, où on a alors $0 = \deg_{X_m}(PQ) = \deg_{X_m}(P) + \deg_{X_m}(Q)$, ce qui signifie que X_m n'apparaît dans aucun monôme de P ni de Q.

(ii) L'anneau $\mathscr{O}(\mathbf{C})$ des fonctions entières est un exemple d'anneau intègre qui ne vérifie pas la condition *(E)*. Remarquons d'abord que l'intégrité de $\mathscr{O}(\mathbf{C})$ (ou plus généralement de l'anneau $\mathscr{O}(U)$ des fonctions holomorphes sur un ouvert U

connexe non vide) résulte du principe des zéros isolés. Dans $\mathscr{O}(\mathbf{C})$, les inversibles sont les fonctions sans zéro, les irréductibles sont les fonctions admettant un seul zéro, simple, et les produits finis d'irréductibles et d'inversibles ont donc un nombre fini de zéros. Ainsi, sin ne peut s'écrire sous la forme $up_1 \cdots p_r$ attendue.

(iii) Dans un anneau intègre non noethérien, un élément peut être divisible par une infinité d'irréductibles deux à deux non associés. C'est par exemple à nouveau le cas de sin dans l'anneau $\mathscr{O}(\mathbf{C})$: elle est divisible par tous les irréductibles $z - k\pi$, $k \in \mathbf{Z}$.

(iv) Nous avons vu au cours de la démonstration que, dans un anneau noethérien intègre, tout élément $a \notin \{0\} \cup A^\times$ est divisible par un irréductible. Cela ne reste pas toujours vrai dans un anneau non noethérien : *il existe des anneaux intègres, qui ne sont pas des corps, ne possédant aucun irréductible*. C'est par exemple le cas de l'anneau des entiers algébriques $\mathfrak{O}_{\overline{\mathbf{Q}}} = \{x \in \mathbf{C}, \exists n \in \mathbf{N}, \exists a_1, \ldots, a_n \in \mathbf{Z}, x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0\}$.

(v) Par ailleurs, noethérien et intègre n'entraînent pas factoriel. Considérons $\mathbf{Z}[i\sqrt{5}]$. Cet anneau est intègre (car inclus dans $\mathbf{C}$) et noethérien (il est isomorphe au quotient $\mathbf{Z}[X]/(X^2+5)$ de l'anneau noethérien $\mathbf{Z}[X]$), donc satisfait *(E)*, mais l'unicité est en défaut. On a en effet, dans $\mathbf{Z}[i\sqrt{5}]$:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}),$$

et on vérifie que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles et que 2 et 3 ne sont associés ni à $1 + i\sqrt{5}$, ni à $1 - i\sqrt{5}$, par exemple en introduisant la *norme* d'un élément $z = a + ib\sqrt{5}$ définie ici par $N(z) = z\overline{z} = a^2 + 5b^2$. On a en effet $z \in \mathbf{Z}[i\sqrt{5}]^\times$ si et seulement si $N(z) = 1$, de sorte que $\mathbf{Z}[i\sqrt{5}]^\times = \{\pm 1\}$, ce qui montre que les éléments considérés sont deux à deux non associés. Par ailleurs, la considération de la norme permet de vérifier l'irréductibilité de certains éléments : ici, puisque $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = 6 = N(1 - i\sqrt{5})$, et qu'il ne peut exister d'éléments de norme 2 ou 3, ces quatre éléments sont irréductibles.

Tournons-nous maintenant vers la condition d'unicité *(U)*.

Proposition 2.2.6. *Soit A un anneau intègre vérifiant la condition (E). Les conditions suivantes sont équivalentes :*

(i) A vérifie la condition (U) (et donc A est factoriel),

(ii) **lemme d'Euclide** *: si p irréductible divise ab, alors p divise a ou p divise b,*

(iii) p irréductible $\iff$ p premier (rappelons que p premier signifie (p) premier non nul),

(iv) **théorème de Gauss** *: si a divise bc et a premier avec b, alors a divise c.*

Démonstration. Dans un anneau intègre, premier $\Rightarrow$ irréductible.

Le lemme d'Euclide *(ii)* signifie irréductible $\Rightarrow$ premier : ainsi $(ii) \Leftrightarrow (iii)$, sans l'hypothèse *(E)*.

Toujours sans *(E)*, *(iv)* entraîne clairement *(ii)*, et *(ii)* entraîne *(i)* : en effet, si a non nul s'écrit $a = u\prod_{p\in\mathscr{P}} p^{v_p} = v\prod_{p\in\mathscr{P}} p^{w_p}$ où $\mathscr{P}$ est un système de représentants des irréductibles de A, alors ou bien $a \in A^\times$ et $v_p = w_p = 0$ pour tout p et $u = a = v$, ou bien a non inversible et il existe $p \in \mathscr{P}$ tel que $v_p > 0$. Alors l'irréductible p divise $v\prod_{q\in\mathscr{P}} q^{w_q}$, et, d'après *(ii)*, on a $w_p > 0$. En divisant les deux membres par p, on conclut par récurrence sur $\sum_p v_p$.

Prouvons maintenant *(i)* $\Rightarrow$ *(iv)*, en utilisant *(E)*. Décomposons a, b et c en produits de facteurs irréductibles : $a = u\prod_p p^{v_p(a)}$, $b = v\prod_p p^{v_p(b)}$ et $c = w\prod_p p^{v_p(c)}$. On a

donc, pour tout p, $v_p(a) \leqslant v_p(b) + v_p(c)$. Mais, pour tout p, ou bien $v_p(a) > 0$ ($\Leftrightarrow p|a$), et a et b premiers entre eux entraîne $p \not| b$, i.e. $v_p(b) = 0$, d'où $v_p(a) \leqslant v_p(c)$, ou bien $v_p(a) = 0 \leqslant v_p(c)$. Ainsi, pour tout p, $v_p(a) \leqslant v_p(c)$, i.e. a divise c. □

Cet énoncé entraîne le critère de factorialité suivant, dont l'utilisation est très courante :

Corollaire 2.2.7. *Un anneau intègre noethérien dans lequel tout élément irréductible est premier est factoriel.*

Dans un anneau factoriel, on dispose des notions de *pgcd* et *ppcm*.

Définition 2.2.8 (pgcd, ppcm)**.** Soient a et b deux éléments de A intègre.

Un *plus grand commun diviseur* de a et b est un élément d tel que $d|a$, $d|b$ et, pour tout $c \in A$, $c|a$ et $c|b \Rightarrow c|d$. On note alors $d = \mathrm{pgcd}(a, b)$.

Un *plus petit commun multiple* de a et b est un élément m tel que $a|m$, $b|m$ et, pour tout $c \in A$, $a|c$ et $b|c \Rightarrow m|c$. On note alors $m = \mathrm{ppcm}(a, b)$.

Remarque 2.2.9. Dans un anneau intègre, pgcd et ppcm ne sont définis qu'à inversible près.

Proposition 2.2.10. *Dans un anneau factoriel,* pgcd *et* ppcm *sont bien définis.*

Démonstration. Soit $\mathscr{P}$ un système de représentants des irréductibles de A. Si a ou b est nul, le résultat est clair. Sinon, si $a = u \prod_{p \in \mathscr{P}} p^{v_p(a)}$ et $b = v \prod_{p \in \mathscr{P}} p^{v_p(b)}$, alors un pgcd de a et b est donné par $d = \prod_p p^{\min(v_p(a), v_p(b))}$ et un ppcm par $m = \prod_p p^{\min(v_p(a), v_p(b))}$. □

Remarque 2.2.11.

(i) Il convient de traduire ces définitions et la proposition précédente en termes d'idéaux : d est un pgcd de a et b si et seulement si $(a) \subset (d)$, $(b) \subset (d)$, et $\big((a) \subset (c)$ et $(b) \subset (c) \Rightarrow (d) \subset (c)\big)$, autrement dit si et seulement si $(d) = \sup((a), (b))$ dans l'ensemble $\mathscr{I}(A)$ des idéaux principaux de A ordonné par l'inclusion ; de même, m est un ppcm de a et b si et seulement si $(m) = \inf((a), (b))$ dans $(\mathscr{I}(A), \subset)$.

La proposition se reformule alors ainsi : dans un anneau factoriel, l'ensemble $\mathscr{I}(A)$ des idéaux principaux ordonné par l'inclusion est réticulé, c'est-à-dire que deux éléments quelconques ont un sup et un inf. On a en fait $\sup((a), (b)) = (\mathrm{pgcd}(a, b))$ et $\inf((a), (b)) = (\mathrm{ppcm}(a, b))$.

(ii) Dans un anneau factoriel, on a $(a) \cap (b) = (\mathrm{ppcm}(a, b))$. En revanche, en général $(a) + (b) \neq (\mathrm{pgcd}(a, b))$. C'est le cas si (et seulement si) tout idéal de type fini est principal.

2.3. **Anneaux principaux.** Les anneaux principaux fournissent un exemple important d'anneaux factoriels.

Définition 2.3.1 (Anneau principal)**.** Un *anneau principal* est un anneau intègre dans lequel tous les idéaux sont principaux.

Exemple 2.3.2. $\mathbf{Z}$ est principal.

Remarque 2.3.3. Un anneau principal est bien évidemment noethérien. Mais $\mathbf{Z}[X]$ (ou $k[X, Y]$) est noethérien (d'après le théorème de la base de Hilbert) mais non principal : l'idéal $(2, X)$ de $\mathbf{Z}[X]$ (ou (X, Y) de $k[X, Y]$) n'est pas principal.

Proposition 2.3.4. *Un anneau principal est factoriel.*

Démonstration. Un anneau principal est noethérien, donc vérifie la condition d'existence *(E)* d'après 2.2.4.

Si p est irréductible, l'idéal (p) est maximal parmi les idéaux principaux distincts de A (cf. Remarque 2.1.9 (ii)), donc maximal tout court dans A principal, donc premier. La proposition 2.2.6 assure alors que A est factoriel. □

Proposition 2.3.5. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Démonstration. Un idéal premier non nul est engendré par un irréductible (cf. 2.1.12), et on vient de voir dans la démonstration précédente qu'un idéal engendré par un irréductible est maximal.

Donnons-en une démonstration directe. Soit $\mathfrak{p} = (p)$ un idéal premier non nul. Soit $I = (x)$ un idéal tel que $(p) \subsetneq I$. Alors $p \in (x)$, i.e. il existe $a \in A$ tel que $p = ax$. Mais $x \notin (p)$, et (p) premier entraîne alors $a \in (p)$: il existe $b \in A$ tel que $a = pb$. Finalement $p = ax = pbx$ d'où, par intégrité de A, $bx = 1$. Ainsi $x \in A^\times$, et $I = (x) = A$. L'idéal (p) est donc maximal. □

Remarque 2.3.6. La proposition précédente décrit l'ensemble des idéaux premiers d'un anneau principal A : si A n'est pas un corps, ses idéaux premiers sont l'idéal nul (0) et les idéaux maximaux, qui sont exactement les idéaux (p) engendrés par les irréductibles p.

Dans un anneau principal, on retrouve le théorème de Bézout :

Proposition 2.3.7 (Théorème de Bézout)**.** *Soit A un anneau principal. Soient $a, b \in A$, et soit $d = \mathrm{pgcd}(a, b)$. On a alors $(a) + (b) = (d)$. En particulier, il existe $r, s \in A$ tels que $ra + vb = d$.*

Démonstration. On a remarqué en 2.2.11 (i) que l'idéal (d) est le sup des idéaux (a) et (b) dans l'ensemble des idéaux principaux de A, donc ici, puisque A est principal, dans l'ensemble des idéaux tout court. C'est donc $(a) + (b)$. □

Corollaire 2.3.8. *Soit A un anneau principal. Si a et b sont premiers entre eux, alors $(a) + (b) = 1$, i.e. il existe $r, s \in A$ tels que $ra + sb = 1$.*

Remarque 2.3.9. Le théorème de Bézout tombe en défaut dans un anneau factoriel non principal : par exemple dans l'anneau $k[X, Y]$ (dont on verra plus loin la factorialité), les éléments X et Y sont premiers entre eux, mais $1 \notin (X, Y)$.

En fait, on peut montrer qu'un anneau factoriel satisfaisant le théorème de Bézout (i.e. tel que (a, b) est principal pour tous $a, b \in A$, ou encore tel que tout idéal de type fini est principal) est un anneau principal.

2.4. **Anneaux euclidiens.** Les anneaux euclidiens constituent une classe importante d'anneaux principaux.

Définition 2.4.1 (Anneau euclidien)**.** Un *anneau euclidien* est un anneau intègre muni d'une *division euclidienne*, c'est-à-dire muni d'une fonction $v \colon A \setminus \{0\} \longrightarrow \mathbf{N}$ telle que pour tous $a, b \in A \setminus \{0\}$ il existe $q, r \in A$ avec $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

Exemple 2.4.2. L'anneau $\mathbf{Z}$ muni de la fonction valeur absolue $n \mapsto |n|$ est euclidien.

Remarque 2.4.3. En général, il n'y a pas unicité du quotient q ni du reste r. C'est déjà le cas dans $(\mathbf{Z}, |\cdot|)$. Pour retrouver la division euclidienne des écoliers, il faut ajouter la condition $r \geqslant 0$.

2.4.4. Un second exemple très important d'anneau euclidien est l'anneau $k[X]$ des polynômes à coefficients dans un corps k. Profitons de cet exemple pour établir un résultat important qui précise ce que devient la division euclidienne dans l'anneau $A[X]$ des polynômes à coefficients dans un anneau A :

Lemme 2.4.5 (division euclidienne dans $A[X]$)**.** *Soit A un anneau quelconque. Soit $U \in A[X]$, $U \neq 0$, de* coefficient dominant inversible*. Alors, pour tout $T \in A[X]$, il existe $Q, R \in A[X]$ tels que* $\begin{cases} T = QU + R \\ R = 0 \text{ ou } \deg R < \deg U. \end{cases}$

Démonstration. On peut supposer U unitaire. Écrivons $U = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ avec $a_0, a_1, \ldots, a_{d-1} \in A$.

On montre par récurrence sur $\deg T$ que tout polynôme T non nul (le résultat étant évident pour le polynôme nul) s'écrit $T = QU + R$ avec $R = 0$ ou $\deg R < \deg U$. Si T est de degré $< \deg U$, alors $Q = 0$ et $R = T$, de degré $\deg T < \deg U$. Sinon, écrivons $T = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_0$, avec $n = \deg T \geqslant \deg U = d$. On a donc $T = b_nX^{n-d}U + (T - b_nX^{n-d}U)$, et, $T - b_nX^{n-d}U$ étant de degré $\leqslant n-1$, il s'écrit par récurrence $T - b_nX^{n-d}U = QU + R$ avec $R = 0$ ou $\deg R < d$. Ainsi $T = (b_nX^{n-d} + Q)U + R$ où $R = 0$ ou $\deg R < d$, comme attendu. □

Corollaire 2.4.6. *Si k est un corps, l'anneau $k[X]$ est euclidien (avec la fonction* $\deg\colon k[X] \setminus \{0\} \longrightarrow \mathbf{N}$*).*

Exemple 2.4.7 (Autres exemples d'anneaux euclidiens)**.** L'*anneau des entiers de Gauss* $\mathbf{Z}[i] = \{P(i) \in \mathbf{C}, P \in \mathbf{Z}[X]\} = \{a + ib \in \mathbf{C}, a, b \in \mathbf{Z}\}$ est euclidien. L'*anneau* $\mathbf{D}$ *des nombres décimaux* (qui est le sous-anneau de $\mathbf{Q}$ engendré par $\mathbf{Z}$ et $\frac{1}{10}$) est également euclidien. Citons également l'anneau des *séries formelles* $k[[X]]$ à coefficient dans un corps k.

Théorème 2.4.8. *Un anneau euclidien est principal.*

Démonstration. On suit l'argument usuel pour établir que $\mathbf{Z}$ ou $k[X]$ est principal.

Il s'agit de vérifier que tout idéal de A est principal.

Soit I un idéal non nul de A (l'idéal nul étant bien évidemment principal). Soit $b \in I$ tel que $v(b) = \min\{v(x), x \in I \setminus \{0\}\}$. Montrons que $I = (b)$. On a évidemment $(b) \subset I$.

Soit $a \in I$. Effectuons une division euclidienne de a par b : il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Alors $r = a - bq \in I$, et, comme $v(b)$ est le minimum de v sur les éléments non nuls de I, on a $r = 0$, d'où $a \in (b)$. Ainsi $I \subset (b)$, d'où $I = (b)$. □

On obtient en corollaire que l'anneau des polynômes $k[X]$ sur un corps k est principal. On a déjà vu que $k[X][Y]$ et $\mathbf{Z}[X]$ ne le sont pas. On peut préciser cette observation :

Proposition 2.4.9. *Soit A un anneau. L'anneau $A[X]$ est principal si et seulement si A est un corps :*

$$A[X] \text{ principal} \iff A \text{ corps.}$$

Démonstration. Si A est un corps, $A[X]$ est euclidien, donc principal.

Réciproquement, si $A[X]$ est principal, alors il est en particulier intègre, et $A \subset A[X]$ aussi. Montrons que l'idéal (X) est premier [3]. Soient $P, Q \notin (X)$. Alors $P = \underbrace{a_0}_{\neq 0} + XP_1$

3. On peut aussi démontrer que A est un corps en revenant à la définition : si $a \in A \setminus \{0\}$, considérons l'idéal (a, X). Comme $A[X]$ est principal, il existe P tel que $(a, X) = (P)$. On a donc

et $Q = \underbrace{b_0}_{\neq 0} + XQ_1$. Ainsi $PQ = \underbrace{a_0 b_0}_{\neq 0} + X(b_0 P_1 + a_0 Q_1 + X P_1 Q_1) \notin (X)$ (le terme constant $a_0 b_0$ est non nul par intégrité de A). Donc (X) est un idéal premier non nul, donc maximal dans l'anneau principal $A[X]$. On conclut en considérant l'isomorphisme $\underbrace{A[X]/(X)}_{\text{corps}} \longrightarrow A$ (donné par l'évaluation $P \mapsto P(0)$). □

Remarque 2.4.10. En particulier, $A[X]$ principal $\Leftrightarrow$ $A[X]$ euclidien.

2.4.11. Donnons à présent un exemple d'anneau principal non euclidien. Pour reconnaître qu'un anneau n'est pas euclidien, le critère suivant est utile (en particulier lorsqu'il n'y a pas beaucoup d'unités) :

Proposition 2.4.12. *Dans un anneau euclidien A, il existe $x \in A \setminus A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique $A \longrightarrow A/(x)$ soit surjective.*

Démonstration. Si A est un corps, $x = 0$ convient. Sinon, on choisit $x \notin A^\times \cup \{0\}$ tel que $v(x)$ est minimal : $v(x) = \min\{v(y), y \notin A^\times \cup \{0\}\}$. Soit alors $a \in A$. Effectuons la division euclidienne de a par x : $a = qx + r$ avec $r = 0$ ou $v(r) < v(x)$. Ainsi a et r ont même image dans $A/(x)$. Mais, si $r \neq 0$, la condition $v(r) < v(x) = \min\{v(y), y \notin A^\times \cup \{0\}\}$ assure que r est inversible. Ainsi, $r \in \{0\} \cup A^\times$, et $a \bmod (x)$ est dans l'image de $\{0\} \cup A^\times$ par la projection $A \to A/(x)$. □

Remarque 2.4.13. L'image d'un inversible étant inversible, le quotient $A/(x)$ est un corps. En particulier, (x) est maximal, et x est irréductible.

Exemple 2.4.14. Donnons quelques exemples :
- dans $A = \mathbf{Z}$, $\mathbf{Z}^\times = \{1, -1\}$, et $x = \pm 2$ ou ± 3 conviennent ;
- dans $A = k[X]$, $k[X]^\times = k^\times$, et les polynômes $x = X - a$, $a \in k$, conviennent ;
- dans $A = \mathbf{Z}[i]$, $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$, et on peut prendre $x = 1 - i$, car $\mathbf{Z}[i]/(1-i) \simeq \mathbf{Z}/2\mathbf{Z}$ (en effet, en utilisant l'isomorphisme $\mathbf{Z}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{Z}[i]$ déduit, par division euclidienne dans $\mathbf{Z}[X]$ par le polynôme unitaire $X^2 + 1$, du morphisme surjectif $P \in \mathbf{Z}[X] \mapsto P(i) \in \mathbf{Z}[i]$, on montre que la composée $\mathbf{Z}[X] \to \mathbf{Z}[i] \to \mathbf{Z}[i]/(1-i)$ a pour noyau $(X^2+1, 1-X)$, idéal encore égal à $(2, 1-X)$, puisque $X^2 + 1 = (1-X)^2 - 2X$ et $2 = 2(1-X) - (1-X)^2 + (1+X^2)$; on conclut alors en constatant, à l'aide de la division euclidienne par $X - 1$, que $\mathbf{Z}[X] \to \mathbf{Z}/2\mathbf{Z}, P \mapsto P(1) \bmod 2$ est un morphisme surjectif de noyau $(2, 1-X)$).

Considérons maintenant l'anneau $\mathbf{Z}[\frac{1+i\sqrt{19}}{2}]$ (i.e. $\{P(\frac{1+i\sqrt{19}}{2}) \in \mathbf{C}, P \in \mathbf{Z}[X]\}$), et montrons que cet anneau n'est pas euclidien.

Posons $\omega = \dfrac{1+i\sqrt{19}}{2}$. On a $\omega + \overline{\omega} = 1$ et $\omega\overline{\omega} = 5$, de sorte que ω satisfait $\omega^2 - \omega + 5 = 0$. Ainsi $\mathbf{Z}[\omega] = \{z \in \mathbf{C}, z = a + b\omega, a, b \in \mathbf{Z}\}$. Comme sous-anneau de $\mathbf{C}$, c'est un anneau intègre.

Afin d'étudier son arithmétique, introduisons pour $z = a + b\omega \in \mathbf{Z}[\omega]$ la *norme* $N(z) = z\overline{z} = a^2 + ab + 5b^2$. On a $N(z) \in \mathbf{N}$, $N(zz') = N(z)N(z')$ et $N(z) \neq 0$ si $z = 0$.

Cette norme permet de déterminer le groupe des unités $\mathbf{Z}[\omega]^\times$. En effet, si $z \in \mathbf{Z}[\omega]^\times$, alors $1 = N(zz^{-1}) = N(z)N(z^{-1})$, avec $N(z), N(z^{-1}) \in \mathbf{N}$, de sorte que $N(z) = 1$ (remarquons que, puisque $\mathbf{Z}[\omega]$ est stable par la conjugaison, on a $N(z) = 1 \Rightarrow z \in \mathbf{Z}[\omega]^\times$, puisque alors $z\overline{z} = 1$ et $\overline{z} \in \mathbf{Z}[\omega]$; on n'utilise cette observation que dans la note

$a = RP$ et $X = SP$ avec $R, S \in A[X]$. Puisque A est intègre, on a $\deg R = \deg P = 0$, i.e. R et P sont des polynômes constants. Donc $P = p \in A$. Le polynôme S s'écrit alors $S = sX$ avec $sp = 1$, de sorte que p est inversible. Enfin, comme $(p) = (a, X)$, il existe $T, U \in A[X]$ tels que $p = aT + XU$, et, en évaluant en 0, $aT(0) = p$. Comme p est inversible, a l'est aussi.

5). En écrivant $z = a + b\omega$, on a donc $1 = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 \geqslant \frac{19}{4}b^2$. Ainsi l'entier $b \in \mathbf{Z}$ vérifie $\frac{19}{4}b^2 \leqslant 1$. On en déduit $b = 0$, puis $a = \pm 1$. Donc $\mathbf{Z}[\omega]^\times \subset \{1, -1\}$. Puisque 1 et -1 sont évidemment inversibles, on a égalité : $\mathbf{Z}[\omega]^\times = \{1, -1\}$.

Ainsi $\mathbf{Z}[\omega]^\times \cup 0$ contient trois éléments. Si $\mathbf{Z}[\omega]$ était euclidien, il existerait d'après 2.4.12 un élément $x \in \mathbf{Z}[\omega]$ tel que $\mathbf{Z}[\omega]/(x)$ soit un corps k à 2 ou 3 éléments. Il n'existe qu'un seul corps à 2 éléments (c'est $\mathbf{Z}/2\mathbf{Z}$, et c'est évident), et qu'un seul corps à 3 éléments (c'est $\mathbf{Z}/3\mathbf{Z}$, et c'est également évident) [4]. La restriction à $\mathbf{Z} \subset \mathbf{Z}[\omega]$ de la projection $\mathbf{Z}[\omega] \to \mathbf{Z}[\omega]/(x)$ envoie 1 sur 1. C'est donc exactement la projection canonique de $\mathbf{Z}$ sur $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$. Mais alors, l'image β de ω dans $k = \mathbf{Z}[\omega]/(x)$ vérifie $\beta^2 - \beta + 5 = 0$, i.e. est racine dans k du polynôme $X^2 - X + 5$. Or, si $k = \mathbf{Z}/2\mathbf{Z}$, ce polynôme, qui devient $X^2 + X + 1$, n'a pas de racine dans $\mathbf{Z}/2\mathbf{Z}$, et, si $k = \mathbf{Z}/3\mathbf{Z}$, il devient $X^2 - X - 1$, qui n'a pas de racine dans $\mathbf{Z}/3\mathbf{Z}$. L'anneau $\mathbf{Z}[\omega]$ n'est donc pas euclidien [5].

Montrons maintenant que $\mathbf{Z}[\omega]$ est principal.

Pour ce faire, utilisons le fait suivant, parfois appelé *pseudo division euclidienne* : pour tous $a, b \in \mathbf{Z}[\omega] \setminus \{0\}$, il existe $q, r \in \mathbf{Z}[\omega]$ tels que

— $N(r) < N(b)$,

— $a = bq + r$ ou $2a = bq + r$.

En effet, $z = \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} \in \mathbf{C}$ s'écrit $z = x + iy$ avec $x, y \in \mathbf{Q}$. Choisissons m et n des entiers aussi proches que possible de x et y respectivement (i.e. $|x - m| \leqslant \frac{1}{2}$ et $|y - n| \leqslant \frac{1}{2}$). Si $|y - n| \leqslant \frac{1}{3}$, alors, puisque $|x - m| \leqslant \frac{1}{2}$, on a, en posant $q = m + n\omega \in \mathbf{Z}[\omega]$, $N(z - q) = |z - q|^2 = (x - m)^2 + (x - m)(y - n) + 5(y - n)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$, d'où $N(a - bq) = N(b)N(x - q) < N(b)$. Sinon, $\frac{1}{3} < |y - n| \leqslant \frac{1}{2}$, et il existe alors $n' \in \{2n - 1, 2n + 1\}$ tel que $|y - \frac{n'}{2}| < \frac{1}{6}$. On a alors $\frac{2a}{b} = 2x + i2y$ avec $2x, 2y \in \mathbf{Q}$ avec $|2y - n'| < \frac{1}{3}$. On est ainsi ramené au cas précédent : si m' est un entier tel que $|2x - m'| \leqslant \frac{1}{2}$, alors, en posant $q = m' + n'\omega$, on a $N(2a - bq) < N(b)$.

Déduisons-en que $\mathbf{Z}[\omega]$ est principal : remarquons d'abord que l'idéal (2) engendré par 2 est maximal. En effet, en utilisant la division euclidienne dans $\mathbf{Z}[X]$ par le polynôme unitaire $X^2 - X + 5$, on montre que le morphisme surjectif $P \in \mathbf{Z}[X] \mapsto P(\omega) \in \mathbf{Z}[\omega]$ passe au quotient pour induire un isomorphisme $\mathbf{Z}[X]/(X^2 - X + 5) \xrightarrow{\sim} \mathbf{Z}[\omega]$. On a donc

$$\mathbf{Z}[\omega]/(2) \xleftarrow{\sim} \mathbf{Z}[X]/(2, X^2 - X + 5) \xrightarrow{\sim} (\mathbf{Z}/2\mathbf{Z})[X]/(X^2 + X + 1).$$

Mais $\mathbf{Z}/2\mathbf{Z}$ est un corps, donc $(\mathbf{Z}/2\mathbf{Z})[X]$ est euclidien, donc principal. Comme $X^2 + X + 1$ est irréductible (pour un raison de degré, il serait sinon divisible par un polynôme de degré 1, or il n'a pas de racine dans $\mathbf{Z}/2\mathbf{Z}$), il engendre dans l'anneau principal $(\mathbf{Z}/2\mathbf{Z})[X]$ un idéal maximal (cf. 2.3.6), et $\mathbf{Z}[\omega]/(2) \simeq (\mathbf{Z}/2\mathbf{Z})[X]/(X^2 + X + 1)$ est alors un corps. L'idéal (2) est ainsi un idéal maximal dans $\mathbf{Z}[\omega]$.

Soit alors I un idéal non nul de $\mathbf{Z}[\omega]$, et soit $a \in I$, $a \neq 0$ de norme $N(a)$ minimale. Montrons que $I = (a)$. Effectuons, pour $x \in I$ la pseudo division euclidienne de x par a : il existe q et r avec $N(r) < N(a)$ tels que $aq + r = x$ ou $2x$. Dans le premier cas, $r \in I$, et $N(r) < N(a)$ entraîne donc $r = 0$, d'où $x = aq \in (a)$. Dans le second

4. Nous verrons plus tard qu'il existe un corps de cardinal $n = p^k$ pour tout premier p et tout entier $k \in \mathbf{N}^*$, unique à isomorphisme non unique près. Mais pour $n = 2$ ou 3, c'est évident.

5. On peut donner un argument beaucoup plus naïf : puisque $\mathbf{Z}[\omega]^\times = \{1, -1\}$, la proposition 2.4.12 signifie que tout élément de $\mathbf{Z}[\omega]$ serait congru à $-1, 0$ ou 1 modulo x. Autrement dit, pour tout $a \in A$, x diviserait $a - 1$,a ou $a + 1$, et donc $N(x)$ diviserait $N(a - 1)$, $N(a)$ ou $N(a + 1)$. Avec $a = 2$, $N(x)$ diviserait $N(1) = 1$, ou $N(2) = 4$, ou $N(3) = 9$. Avec $a = \omega$, $N(x)$ diviserait également $N(\omega - 1) = 5$, $N(\omega) = 5$ ou $N(\omega + 1) = 7$. On aurait donc $N(x) = 1$. Mais x serait alors inversible, contradiction.

cas, on a encore $r \in I$, donc $r = 0$ et $2x = aq$. Montrons que 2 divise alors q, ce qui entraîne évidemment $x \in (a)$. Sinon, (2) étant premier (car maximal), 2 divise a, i.e. $a = 2a'$. De plus, (2) étant maximal, $q \notin (2) \Rightarrow (2, q) = 1$: il existe donc $u, v \in \mathbf{Z}[\omega]$ tels que $2u + qv = 1$. On en tire $a' = 2ua' + qva' = ua + vx \in I$. Mais alors $N(a') = \frac{1}{4}N(a) < N(a)$, ce qui contredit le choix de a de norme minimale dans $I \setminus \{0\}$. On a donc $I = (a)$. L'anneau $\mathbf{Z}[\omega]$ est donc principal.