TD n°1 - Solutions.

Tous les anneaux sont supposés commutatifs et unitaires.

1 Entiers algébriques

Exercice 1. Montrer que dans $\mathbb{Z}[\sqrt{-5}]$, 3, 7, $2+\sqrt{-5}$, $4+\sqrt{-5}$ sont irréductibles.
Montrer que la décomposition de 21 en facteurs irréductibles dans $\mathbb{Z}[\sqrt{-5}]$ n'est pas unique ($\mathbb{Z}[\sqrt{-5}]$ n'est pas *factoriel*).

Solution. Les équations $a^2+5b^2)=3$ et $a^2+5b^2=7$ n'ont pas de solutions, donc il n'y a pas d'élément de $\mathbb{Z}[\sqrt{-5}]$ de norme 3 ou 7. En particulier, si z est de norme 9, 21 ou 49, un diviseur propre non inversible de z devrait être de norme 3 ou 7 : z est donc irréductible. Ici $N(3)=N(2+\sqrt{-5})=9$, $N(7)=49$ et $N(4+\sqrt{-5})=21$.
On a $21=3\cdot 7=(4+\sqrt{-5})\cdot(4-\sqrt{-5})$ et l'on obtient deux décompositions en facteurs irréductibles.

Exercice 2. Montrer que, si z est un élément irréductible de $\mathbb{Z}[i]$, alors $N(z)$ est un nombre premier ou le carré d'un nombre premier.

Solution. Comme z est irréductible, $barz$ aussi (l'irréductibilité est invariante par automorphisme d'anneau, en particulier par conjugaison complexe). On a $z\bar{z}=N(z)$ et z et $\bar{z}$ sont irréductibles. Par unicité de la décomposition en facteur irréductibles, la décomposition en facteur premiers de $N(z)$ contient au plus deux éléments. Si elle n'en contient qu'un, alors $N(z)$ est premier. Si elle en contient deux, $N(z)=pq$, et p et q doivent être associés à z et $\bar{z}$. Comme $p^2=N(z)=N(\bar{z})=q^2$, on obtient $p=q$ et $N(z)=p^2$ comme voulu.

Exercice 3. Montrer qu'un nombre rationnel est un entier algébrique si et seulement si il appartient à $\mathbb{Z}$.

Solution. Soit $x\in\mathbb{Q}$, qu'on peut supposer non nul, zéro d'un polynôme unitaire $P=X^N+\sum_{0\le n<N}a_nX^n$ de $\mathbb{Z}[X]$. Ecrivons x sous la forme p/q avec p et $q>0$ entiers premiers entre eux et multiplions par q^N l'égalité $P(p/q)=0$. On obtient

$$p^n=\sum_{0\le n<N}a_np^nq^{N-n}.$$

Le membre de gauche étant divisible par q, on en déduit que p^n est divisible par q. Or comme p et q sont premiers entre eux, $q=1$ et donc $x\in\mathbb{Z}$.

Exercice 4. Soit A un sous-anneau de $\mathbb{Q}$.

a) Montrer que si $p/q\in A$ avec p et q deux entiers premiers entre eux, alors $q\in A^\times$.

b) Montrer que A est un anneau principal.

c) Montrer que tout élément irréductible de A est associé (dans A) à un élément irréductible de $\mathbb{Z}$.

Solution. a) Comme A est unitaire, $1\in A$ et il en découle aisément que $\mathbb{Z}\in A$ (en fait pour tout anneau unitaire, il existe un unique morphisme d'anneau de $\mathbb{Z}$ vers cet anneau). Donc $q\in A$. Comme p et q sont premiers entre eux, il existe u et v tels que $up+vq=1$. Alors $1/q=v+up/q\in A$ car $v,u,p/q\in A$. Donc $q\in A^\times$.

b) . D'après la question précédente, tout élément de A est associé dans A à un entier, qui engendre donc le même idéal : on ne perd donc rien à chercher des familles génératrices d'idéaux constituées d'entiers. Soit I un idéal de A, et $J=I\cap\mathbb{Z}$. J est un idéal de $\mathbb{Z}$, donc il est monogène : $J=m\mathbb{Z}$. Soit $a=p/q\in I$, alors $p\in J$ donc il existe $n\in\mathbb{Z}$ tel que $p=mn$. Donc $a=m(n/q)$ avec $n/q\in A$ d'après la question précédente ; donc $a\in mA$, et donc $I=mA$.

c) Soit $a=p/q\in A$ un élément irréductible. Alors $p=u\prod_i p_i^{a_i}$ la factorisation en nombres premiers de p. Alors $a=u/q\prod_i p_i^{a_i}$ est une factorisation dans A de a, qui est irréductible, et donc un des facteurs doit être associé à a. C'est nécessairement l'un des p_i (u/q étant inversible).

Exercice 5. Soit $x=\sqrt{2}+\sqrt[3]{3}$ et $v=(1,\sqrt{2},\sqrt[3]{3},\sqrt{2}\sqrt[3]{3},\sqrt[3]{3}^2,\sqrt{2}\sqrt[3]{3}^2)\in\mathbb{C}^6$.

a) Montrer qu'il existe $M\in M_6(\mathbb{Z})$ telle que $Mv=xv$.

b) En déduire que x est un entier algébrique.

c) En généralisant la construction précédente, montrer que les entiers algébriques forment un sous-anneau de $\mathbb{C}$.

Solution. a) Notons v_i la $i$eme coordonnée de v. On a $xv_1 = v_2 + v_3$, $xv_2 = 2v_1 + v_4$, $xv_3 = v_4 + v_5$, $xv_4 = 2v_3 + v_6$, $xv_5 = v_6 + 3v_1$ et $xv_6 = 2v_5 + 3v_2$. Il suffit donc de prendre

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 & 0 \end{pmatrix}$$

b) Soit P le polynôme caractéristique de M (c'est un polynôme unitaire à coefficients entiers). On a $P(x) = 0$ car x est valeur propre de M.

c) On veut montrer que si x et y sont des entiers algébriques, alors $x + y$ et xy sont des entiers algébriques (les autres propriétés étant immédiates). Soit P, Q polynomes à coefficients entiers et unitaires annulant x et y. Soient n et m les degrés de P et Q. Considérons le vecteur v de taille mn tel que $v_{im+j} = x^i y^j$. Alors posons $M_{im+j,i'm+j'} = Aii'\delta_{jj'}$, où A est la matrice comagnon de P et δ le symbole de Kronecker, et $N_{im+j,i'm+j'} = \delta_{ii'}B_{jj'}$ où B est la matrice compagnon de Q. On a $Mv = xv$ et $Nv = yv$. Donc $(M + N)v = (x + y)v$ et $MNv = xyv$. Il suffit donc de prendre comme polynômes annulateurs les polynômes caractéristiques de $M + N$ et de MN.

Exercice 6. Soit d un nombre impair sans facteur carré. Montrer que, si $a, b \in \mathbb{Q}$, $a + b\sqrt{d}$ est un entier algébrique si et seulement si $2a$ et $a^2 + db^2$ sont entiers.
Montrer que l'anneau des entiers algébriques de $\mathbb{Q}\left[\sqrt{d}\right]$ est :

a) $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 3 \bmod 4$;

b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \bmod 4$.

Solution. Soit $z = a + b\sqrt{d}$ et soit $z' = a - b\sqrt{d}$. Si $P \in \mathbb{Q}[X]$, alors $P(z) \in \mathbb{Q}[\sqrt{d}]$ et s'écrit donc sous la forme $c + d\sqrt{d}$ avec $c, e \in \mathbb{Q}$. On vérifie facilement que $P(z') = c - e\sqrt{d}$ (l'application $c + d\sqrt{d} \mapsto c - e\sqrt{d}$ est un automorphisme d'anneau de $\mathbb{Q}[\sqrt{d}]$). En particulier z annule P si et seulement si z' annule P. Donc si z est un entier algébrique z' aussi. Comme les entier algébriques forment un anneau, $z + z' = 2a$ et $zz' = a^2 - db^2$ doivent aussi être des entiers algébriques, donc des entiers d'après l'exercice précédent.
Réciproquement si $2a$ et $a^2 - db^2$ sont entiers, le polynôme $X^2 - 2aX + a^2 - db^2$ est un polynome unitaire de $\mathbb{Z}[X]$ annulant z, et z est donc entier algébrique.
Donc si z est entier algébrique $a \in \frac{1}{2}\mathbb{Z}$ et l'on déduit de $a^2 - db^2 \in \mathbb{Z}$ que $db^2 \in \frac{1}{4}\mathbb{Z}$. Comme d est sans facteur carré, on obtient $b \in \frac{1}{2}\mathbb{Z}$. En posant $a' = 2a$ et $b' = 2b$, il suffit pour conclure de vérifier que $a'^2 - db'^2 \equiv 0 \bmod 4$ si et seulement si a' et b' sont pairs dans le cas $d \equiv 3 \bmod 4$ et si et seulement si a' et b' sont de même parité dans le cas $d \equiv 1 \bmod 4$.

Exercice 7. Parmi les nombres algébriques suivants, lesquels sont entiers ?

a) $\beta = \frac{\sqrt{11}+\sqrt{13}}{2}$,

b) $\gamma = \frac{\sqrt{5}+\sqrt{13}}{2}$,

c) $\delta = \frac{i+\sqrt{11}+\sqrt{13}}{2}$,

d) $\frac{1+\sqrt[4]{17}}{2}$.

Solution. a) On vérifie comme dans l'exercice précédent que si α était entier $\alpha' = \frac{1-\sqrt[4]{17}}{2}$ le serait aussi. Or $\alpha\alpha' = \frac{1-\sqrt{17}}{4}$, qui n'est pas entier d'après l'exercice précédent, donc α n'est pas entier.

b) On a $\beta^2 = 6 + \frac{\sqrt{143}}{2}$, qui n'est pas entier d'après l'exercice précédent donc, β n'est pas entier.

c) $\gamma = \frac{\sqrt{5}+1}{2} + \frac{-1+\sqrt{13}}{2}$ est entier comme somme de deux entiers.

d) Si δ était entier, $\delta\bar{\delta} = \frac{25+2\sqrt{143}}{4}$ le serait aussi, or ce n'est pas le cas d'après l'exercice précédent.

Exercice 8. Soit $A = \mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$, et $N : A \to \mathbb{R}$ définit par $N(z) = z\bar{z}$.
N est il un stathme euclidien quand $d = 3, 7, 11, 15, 19$?

Solution. N est un stathme si et seulement si pour tous $a, b \in A^\times$, il existe $q \in A$ et r avec $N(r) < N(b)$ tels que $a = bq + r$, c'est-à-dire $a/b = q + r'$ avec $N(r') < 1$.
Pour montrer que N est un stathme, il suffit donc de vérifier que pour tout $z \in \mathbb{C}$, $\inf_{q\in A} N(z - q) < 1$. Réciproquement, comme $\{a/b\}_{a,b\in A^\times}$ est dense dans $\mathbb{C}$, si il existe $z \in \mathbb{C}$ tel que $\inf_{q\in A} N(z - q) > N(a/b)$, alors N n'est pas un stathme.
Le plan $\mathbb{C}$ est pavé par des triangles isocèles de sommets $a, a + \frac{1+i\sqrt{d}}{2}$ et $a+1$ où $a \in A$ et $a, a + \frac{1-i\sqrt{d}}{2}$ et $a+1$ où $a \in A$. La distance à A est maximale au centre du cercle circonscrit du triangle (quand celui-ci est à l'intérieur du triangle, ce qui est le cas ici). Le centre du cercle est $1/2 + ix$ avec x tel que $N(1/2 + ix) = N(i\sqrt{d}/2 - ix)$, c'est à dire $x^2 + 1/4 = x^2 - \sqrt{d}x + d/4$, soit $x = (d - 1)/(4\sqrt{d})$ et alors $d(x, A)^2 = (d + 1)^2/(16d)$. On obtient facilement que $d(x, A) < 1$ pour $d = 3, 7, 11$ mais $d(x, A) > 1$ pour $d = 15, 19$.

Exercice 9. a) Soit R un anneau euclidien. Montrer qu'il existe $x \in R$ non inversible tel que $R^* \cup \{0\} \to R/(x)$ soit surjective.

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

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

d) Montrer que (2) est un idéal maximal de A.

e) Montrer que A est principal.

Solution. a) Soit $x \in R - (R^* \cap \{0\})$ 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 $r \in R^* \cap \{0\}$. Donc $\bar{y}$ est l'image de r par l'application $R^* \cup \{0\} \to R/(x)$

b) Soit $N(z) = z\bar{z} \in \mathbb{Z}$. Alors z est inversible si et seulement si $N(z) = 1$. Mais si $z = a + b\frac{1+i\sqrt{19}}{2}$, $N(z) \geq 19b^2/4 > 1$ dès que $b \neq 0$. On en déduit $R* = \{1, -1\}$.
Si x est tel que $R^* \cup \{0\} \to R/(x)$ est surjective, alors si $y \in R$, 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, $N(x) = 1$ ce qui contredit l'hypothèse que x n'est pas inversible. Donc R n'est pas euclidien.

c) Soit $x = a/b$. Il suffit de montrer qu'il existe $q \in A$ tel que $|x - q| < 1$ (on pose alors $r = b(x - q) = a - bq$) ou $|2x - q| < 1$ (on pose alors $r = b(2x - q) = 2a - bq$).
Soit u, v les parties réelles et imaginaires de $x : x = u + iv$. Soit $n \in \mathbb{Z}$ tel que $|4v/\sqrt{19} - n| \leq 1/2$. Quitte à remplacer x par $x - n\frac{1+i\sqrt{19}}{2}$, on peut supposer $|v| \leq \sqrt{19}/4$. Quitte à remplacer x par $-x$, on peut supposer que $0 \leq v \leq \sqrt{19}/4$.
Supposons momentanément $v \leq \sqrt{3}/2$ Soit $n \in \mathbb{Z}$ tel que $|u - n| \leq 1/2$. Alors $|x - n|^2 = |u - n|^2 + |v|^2 < 1/4 + 3/4 = 1$, et on est donc dans le premier cas en posant $q = n$
Supposons $\sqrt{3}/2 \leq v \leq \sqrt{19}/4$. Alors Comme $v \leq \sqrt{19}/4$, on a $\sqrt{3}/2 \geq \sqrt{19}/2 - \sqrt{3} \geq \sqrt{19}/2 - 2v \geq 0$. Donc $x' = \frac{1+i\sqrt{19}}{2} - 2x$ vérifie la condition étudiée juste au-dessus, d'où $n \in \mathbb{Z}$ tel que $|\frac{1+i\sqrt{19}}{2} - 2x - n| < 1$ et on est alors dans le deuxième cas en posant $q = \frac{1+i\sqrt{19}}{2} - n$.

d) 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.

e) Soit I un idéal de A. Soit $b \in I - \{0\}$ minimisant $|b|$ (comme $|z|^2 \in \mathbb{N}$ et que $\mathbb{N}$ est bien ordonné, il existe bien un tel b). Comme $b \in I$, $(b) \subset I$ et donc $(2b) \subset (2I)$. 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. Donc $2I \subset (b)$.
On a donc $(2b) \subset 2I \subset (b)$. L'ensemble $J = \{x \in A, bx \in 2I\}$ est un idéal de A contenant (2), donc par maximalité de (2) :
– Soit $J = A$ et alors $2I = (b)$ est principal. Comme A est intègre, I est principal aussi.
– Soit $J = (2)$ et alors $2I = (2b)$ et donc par intégrité, $I = (b)$ est principal.

2 Anneaux et idéaux

Si I, J sont deux idéaux de A, on note $(I : J) := \{a \in A, aJ \subset I\}$ (c'est un idéal de A).

Exercice 10. Montrer qu'il n'y a pas de morphisme d'anneaux :

a) de $\mathbb{C}$ dans $\mathbb{R}$,

b) de $\mathbb{R}$ dans $\mathbb{Q}$,

c) de $\mathbb{Q}$ dans $\mathbb{Z}$,

d) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$, pour tout $n > 0$.

Solution. (i) Soit f un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{R}$, on a

$$f(i)^2 = f(i^2) = f(-1) = -f(1) = -1.$$

Ainsi $f(i) \in \mathbb{R}$ et $f(i)^2 = -1$. C'est impossible.
(ii) Soit f un morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{Q}$, on a

$$f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2.$$

Ainsi $f(\sqrt{2}) \in \mathbb{Q}$ et $f(\sqrt{2})^2 = 2$. C'est impossible car $\sqrt{2}$ et $-\sqrt{2}$ ne sont pas rationnels.
(iii) Soit f un morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Z}$, on a

$$2 \cdot f(\frac{1}{2}) = (1+1)f(\frac{1}{2}) = (f(1) + f(1))f(\frac{1}{2}) = f(1+1)f(\frac{1}{2}) = f(2)f(\frac{1}{2}) = f(2 \cdot \frac{1}{2}) = f(1) = 1.$$

Ainsi $f(\frac{1}{2}) \in \mathbb{Z}$ et $2f(\frac{1}{2}) = 1$. C'est impossible.
(i) Soit f un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$ et notons $\overline{x}$ la classe dans $\mathbb{Z}/n\mathbb{Z}$ de $x \in \mathbb{Z}$. On a

$$0 = f(0) = f(\overline{n}) = f(\overline{1} + \cdots + \overline{1}) = f(\overline{1}) + \cdots + f(\overline{1}) = n \cdot f(\overline{1}) = n.$$

On trouve que $0 = n > 0$ dans $\mathbb{Z}$, c'est absurde.

Exercice 11. Montrer qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n. Montrer que dans ce cas il existe un unique morphisme d'anneau.

Solution. Soit f un morphisme d'anneau de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Nous noterons $\hat{x}$ et $\overline{x}$ respectivement les classes de $x \in \mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ et respectivement dans $\mathbb{Z}/m\mathbb{Z}$. Alors on a

$$0 = f(0) = f(\hat{n}) = f(\underbrace{\hat{1} + \cdots + \hat{1}}_{n \text{ fois}}) = \underbrace{f(\hat{1}) + \cdots + f(\hat{1})}_{n \text{ fois}} = n \cdot f(\hat{1}) = n \cdot \overline{1} = \overline{n}.$$

Ainsi pour que f existe, il faut que $\overline{n} = \overline{0} \in \mathbb{Z}/m\mathbb{Z}$ c'est-à-dire m divise n.
Définir un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est équivalent à définir un morphisme f de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ tel que $f(n) = \overline{0}$. Cependant on a nécessairement $f(1) = \overline{1}$ donc $f(n) = \overline{0} \Leftrightarrow \overline{n} = \overline{0}$ ce qui est équivalent au fait que m divise n. Par ailleurs le morphisme est unique car $f(x) = \overline{x}$ pour tout $x \in \mathbb{Z}$.

Exercice 12. Montrer qu'un anneau intègre A possédant un nombre fini d'idéaux est un corps.
Indice : prendre $x \in A$ et considérer les idéaux (x^n).

Solution. Soit A un anneau intègre ne possédant qu'un nombre fini d'idéaux et soit x non nul dans A. La suite décroissante d'idéaux $((x^n))_n$ n'est pas injective, donc il existe $n > m$ tel que $(x^n) = (x^m)$. En particulier $x^m \in x^n$, donc il existe $a \in A$ tel que $x^m = ax^n = ax^{n-m}x^m$. Comme A est intègre, on obtient $1 = ax^{n-m}$ et donc x est inversible d'inverse ax^{n-m-1}. Donc A est un corps.

Exercice 13. Soit A un anneau, montrer que l'ensemble R des éléments réguliers de A (c'est-à-dire non diviseurs de 0 dans A) est une partie multiplicative, c'est-à-dire : $1 \in R$ et si r et s sont des éléments de R alors $rs \in R$.

Solution. Supposons qu'il existe $x \in A$ tel que $1 \cdot x = 0$, alors $x = 0$ donc $1 \in R$.
Soient maintenant r et s deux éléments non diviseurs de 0. Supposons qu'il existe $x \in A$ tel que $x \cdot rs = 0$. On a alors $xr \cdot s = 0$ donc comme s n'est pas diviseur de 0, on a $xr = 0$ et comme r n'est pas diviseur de 0, on a $x = 0$. Ainsi $rs \in R$.

Exercice 14. Dans un anneau fini, tous les éléments réguliers sont inversibles.

Solution. Soit $a \in A$ un élément régulier (c'est-à-dire non diviseur de 0). On considère alors le morphisme d'anneau : $\mu_a : A \to A$ défini par $\mu_a(x) = ax$. Comme a est régulier cette application est injective. Mais comme A est fini, l'application est aussi surjective et donc il existe $b \in A$ tel que $\mu_a(b) = 1$ c'est-à-dire $ab = 1$ donc a est inversible.

Exercice 15. Soit $A = \mathbb{C}[X,Y]/(XY-1)$; on pose x l'image de X dans A.

a) Montrer que x est inversible et que tout élément a non nul de A peut s'écrire de façon unique sous la forme $a = x^m P(x)$ où $m \in \mathbb{Z}$ et P est un polynôme de terme constant non nul. On note $e(a) = \deg(P)$.

b) Soient $a, b \in A$ montrer qu'il existe $q, r \in A$ tels que $a = bq + r$ et : $r = 0$ ou $e(r) < e(b)$.

c) En déduire que A est principal.

Solution. a) Soit y l'image de Y. Alors $xy = 1$ donc x est inversible d'inverse y.
Soit $a = Q(x,y) \in A$, avec $Q = \sum_i \sum_j a_{ij} X^i Y^j$. Alors $a = \sum_i \sum_j a_{ij} x^{i-j} = \sum_k \sum_i a_{i,i-k} x^k$ en faisant le changement de variable $k = i - j$. Posons $b_k = \sum_i a_{i,i-k}$. La famille (b_k) est à support finie et soit $m = \inf\{k; b_k \neq 0\}$. Alors $a = x^m P(x)$ avec $P = \sum_{k \geq m} b_k X^{k-m}$.
Si $x^m P(x) = x^n Q(x)$, quitte à multiplier par x^N avec $N >> 0$, on obtient qu'un certain polynôme en x s'annule. Pour l'unicité, il suffit donc de prouver que le morphisme de k-algèbre $f : \mathbb{C}[X] \to A$ qui envoie X sur x est injectif. Notons que $f = \pi\iota$ où $\pi : \mathbb{C}[X,Y] \to A$ est la projection canonique et $\iota : k[X] \to \mathbb{C}[X, \ddot{Y}]$ est l'injection canonique. Soit $P \in \ker f$. Alors $\iota P \in (XY-1)$, c'est-à-dire $P(X) = (XY-1)R(X,Y)$. En évaluant en $(x, x^{-1}) \in \mathbb{C}^2$ pour $x \neq 0$, on obtient $P(x) = 0$. Donc P a une infinité de racine donc $P = 0$.

b) Soient $a = x^m A(x)$ et $b = x^n B(x)$ les décompositions comme dans la question a). Alors il existe $Q, R \in \mathbb{C}[X]$ tels que $A = BQ + R$ et $\deg R < \deg B$. Alors $a = bq + r$ avec $q = x^{m-n} Q(x)$ et $r = x^m R(x)$, et $e(r) \leq \deg R < \deg B = e(b)$.

c) e est un stathme euclidien, donc A est principal.

Exercice 16. Soit $A = A_1 \times \cdots \times A_n$ un produit d'anneaux et soit I un idéal de A.

a) Montrer que I est égal à un produit d'idéaux $I_1 \times \cdots \times I_n$.

b) Déterminer les idéaux premiers et maximaux de A.

c) Supposons que les A_i soient des corps, montrer que l'anneau A n'a qu'un nombre fini d'idéaux.

Solution. (i) Commençons par le cas $n = 2$, nous montrerons le cas général par récurrence. Soit I un idéal de A et notons I_1 et I_2 les images de I par les projections de $A_1 \times A_2 \to A_1$ (resp. $A_1 \times A_2 \to A_1$).
Montrons que I_1 est un idéal de A_1. Soient x_1 et y_1 dans I_1 et $a_1 \in A_1$, il existe x_2 et y_2 dans A_2 tels que $x = (x_1, x_2) \in I$ et $y = (y_1, y_2) \in I$. On a alors $x + y \in I$ donc $(x_1 + y_1, x_2 + y_2) \in I$ et donc $x_1 + y_1 \in I_1$. Par ailleurs, on a pour tout $a_2 \in A_2$, $(a_1, a_2) \cdot (x_1, x_2) \in I$ donc $(a_1 x_1, a_2 x_2) \in I$ et donc $a_1 x_1 \in I_1$. Par conséquent, I_1 est un idéal et de même I_2 aussi.
Montrons maintenant que $I = I_1 \times I_2$. Soit $x = (x_1, x_2) \in I$, alors $x_1 \in I_1$ et $x_2 \in I_2$ donc $I \subset I_1 \times I_2$. Réciproquement, soit $(x_1, x_2) \in I_1 \times I_2$, il existe alors $x_1' \in A_1$ et $x_2' \in A_2$ tels que $(x_1, x_2') \in I$ et $(x_1', x_2) \in I$. Mais alors on a

$$(x_1, x_2) = (1,0) \cdot (x_1, x_2') + (0,1)(x_1', x_2) \in I.$$

Lorsque $n \geq 2$, on procède par récurrence sur n : les idéaux de $A_1 \times \cdots \times A_n$ sont de la forme $I_1 \times J$ où J est un idéal de $A_2 \times \cdots \times A_n$. Par récurrence, on a $J = I_2 \times \cdots \times I_n$.
(ii) Soit $I = I_1 \times \cdots \times I_n$ un idéal de A, il est premier si et seulement si $A/I = A_1/I_1 \times \cdots \times A_n/I_n$ est intègre. Ce produit est intègre si et seulement s'il n'a qu'un terme (disons A_i/I_i) et que ce terme est intègre (c'est-à-dire I_i premier). Les idéaux premiers de A sont donc de la forme $A_1 \times \cdots \times I_i \times \cdots A_n$ avec I_i idéal premier de A_i. De même $I = I_1 \times \cdots \times I_n$ est maximal si et seulement si $A/I = A_1/I_1 \times \cdots \times A_n/I_n$ est un corps. Il doit donc être premier et le quotient A_i/I_i doit être un corps donc I_i est maximal. Les idéaux maximaux sont de la forme $A_1 \times \cdots \times I_i \times \cdots A_n$ avec I_i idéal maximal de A_i.
(iii) Si A_i est un corps, ses seuls idéaux sont (0) et A_i. Un idéal de A étant de la forme $I = I_1 \times \cdots \times I_n$, pour chaque indice i, on a deux possibilités : $I_i = (0)$ ou $I_i = A_i$. On a donc 2^n idéaux dans A. Il y en a n premiers qui sont aussi maximaux.

Exercice 17. Soient A un anneau et I, J et L des idéaux de A. Montrer les assertions suivantes :

a) $I \cdot J \subset I \cap J$,

b) $(I \cdot J) + (I \cdot L) = I \cdot (J + L)$,

c) $(I \cap J) + (I \cap L) \subset I \cap (J + L)$,

d) si A est principal, alors $(I \cap J) + (I \cap L) = I \cap (J + L)$,

e) si J est contenu dans I, alors $J + (I \cap L) = I \cap (J + L)$,

f) supposons que $A = k[X, Y]$ avec k un corps et posons $I = (X)$, $J = (Y)$ et $L = (X + Y)$. Calculer $(I \cap J) + (I \cap L)$ et $I \cap (J + L)$, puis les comparer.

Solution. (i) Soit $x \in I \cdot J$, alors $x = \sum a_i b_i$ avec $a_i \in I$ et $b_i \in J$. Comme I et J sont des idéaux, on a $a_i b_i \in I$ et $a_i b_i \in J$ donc $x \in I \cap J$.
(ii) On a $I \cdot J \subset I \cdot (J + L)$ et $I \cdot L \subset I \cdot (J + L)$ donc $(I \cdot J) + (I \cdot L) \subset I \cdot (J + L)$. Réciproquement, soit $x \in I \cdot (J + L)$. On a $x = \sum a_i(b_i + c_i)$ avec $a_i \in I$, $b_i \in J$ et $c_i \in L$. Mais alors $x = (\sum a_i b_i) + (\sum a_i c_i)$, on voit que $\sum a_i b_i \in I \cdot J$ et $\sum a_i c_i \in I \cdot L$. Ainsi $x \in (I \cdot J) + (I \cdot L)$.
(iii) Soit $x = y + z$ avec $y \in I \cap J$ et $z \in I \cap L$, alors $y + z \in I$ et $y + z \in J + L$ donc $x \in I \cdot (J + L)$.
(iv) Il s'agit de montrer la réciproque de (iii) en supposant A principal. Si x et y sont des éléments de A, on notera $x \wedge y$ le p.g.c.d de x et y et $x \vee y$ le p.p.c.m de x et y. Soient a, b et c dans A tels que $I = (a)$, $J = (b)$ et $L = (c)$, on a

$$I \cap (J + L) = (a \vee (b \wedge c)) = ((a \vee b) \wedge (a \vee c)) = ((a \vee b)) + ((a \vee c)) = I \cap J + I \cap L.$$

(v) Par (iii) on sait que $J + (I \cap L) \subset I \cap (J + L)$. Soit $x \in I \cap (J + L)$, on a $x \in I$ et $x = y + z$ avec $y \in J$ et $z \in L$. Comme $J \subset I$, on a $y \in I$, donc $z = x - y \in I$. Ainsi $y \in J$ et $z \in I \cap L$, donc $x \in J + (I \cap L)$.
(vi) On a $I \cap J = (XY)$ et $I \cap L = (X(X + Y))$. Ainsi

$$I \cap J + I \cap L = (XY) + (X(X + Y)) = (XY, X^2).$$

Par ailleurs, on a $J + L = (Y) + (X + Y) = (X, Y)$, donc

$$I \cap (J + L) = (X) \cap (X, Y) = (X).$$

Ainsi on a bien l'inclusion $I \cap J + I \cap L \subset I \cap (J + L)$ mais pas égalité.

Exercice 18. Soient I et J deux idéaux d'un anneau A. On suppose que $I + J = A$ (deux tels idéaux sont dits comaximaux), montrer que $I^n + J^n = A$.

Solution. On a $1 = i + j$ avec $i \in I$ et $j \in J$. Alors $1 = (i + j)^k = \sum_{r=0}^{k} \binom{k}{r} i^r j^{k-r}$, où les termes de la somme sont dans I^n quand $r \geq n$ et dans J^n quand $r \leq k - n$ On en déduit, en choisissant $k \geq 2n - 1$, que $1 \in I^n + J^n$. D'où le résultat.

Exercice 19. Soit I et J deux idéaux comaximaux de A (c'est-à-dire $I + J = A$). Montrer que $(I : J) = I$. Soit L un idéal tel que $I \cdot L \subset J$; montrer que $L \subset J$.

Solution. Si $a \in I$, $aJ \subset I$, donc $I \subset (I : J)$. Réciproquement, si $a \in (I : J)$, $aJ \subset I, aI \subset I$, donc $a(I+J) \subset I$. Or $I + J = A$, donc $a \in I$. D'où $(I : J) = I$.
$L = A \cdot L = (I + J) \cdot L = I \cdot L + J \cdot L$ d'après l'exo 17.b). Or $I \cdot L \subset J$ par hypothèse et $J \cdot L \subset J$. Donc $L \subset J$.

Exercice 20. Montrer à l'aide d'un contre-exemple, que si I et J sont des idéaux tels que $I \cap J = I \cdot J$, I et J ne sont pas nécessairement comaximaux.

Solution. Voici plusieurs contre exemples :
(i) Soient k un corps et $A = k[X, Y]$. On pose $I = (X)$ et $J = (Y)$. Si $P \in I \cap J$, alors X et Y divisent P. Comme X et Y sont irréductibles, on a XY divise P et $I \cap J = (XY) = I \cdot J$. Cependant $I + J = (X, Y) \subsetneq A$.
(ii) Soient k un corps et $A = k[X, X^{\frac{1}{2}}, X^{\frac{1}{3}}, \cdots, X^{\frac{1}{n}}, \cdots]$ l'anneau des polynômes en des puissances fractionnaires de X. Tout élément de A s'écrit de manière unique comme somme finie

$$\sum_{r \in \mathbb{Q}_+} a_r X^r.$$

L'ensemble des ""polynômes"" tels que $a_0 = 0$ est un idéal I de A et on a $I^2 = I$. En effet, tout élément

$$P = \sum_{r \in \mathbb{Q}_+^*} a_r X^r \in I$$

peut s'écrire sous la forme

$$P = X^a \sum_{r \in \mathbb{Q}_+^*} a_r X^{r-a}$$

où a est un rationnel strictement positif et strictement plus petit que tous les $r \in \mathbb{Q}_+^*$ tels que $a_r \neq 0$ (il n'y en a qu'un nombre fini).
On a donc $I \cdot I = I = I \cap I$ et pourtant $I + I = I \subsetneq A$.
(ıı) Soit $\mathcal{C}$ l'anneau des fonctions continues sur $\mathbb{R}$ et I l'idéal des fonctions qui s'annulent en 0. Si $f \in I$, on peut écrire

$$f(x) = \sqrt{|f(x)|} \cdot \sqrt{|f(x)|}\ \text{signe}(f(x))$$

avec $\sqrt{|f(x)|} \in I$ et $\sqrt{|f(x)|}\ \text{signe}(f(x)) \in I$. Ainsi $I \cdot I = I = I \cap I$ et pourtant $I + I = I \subsetneq A$.

Exercice 21. Étant donné I un idéal d'un anneau A, on note $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$ (vérifier que $\sqrt{I}$ est bien un idéal). Soient I, J et L des idéaux de A, montrer les assertions suivantes :

a) si $I \subset J$, alors $\sqrt{I} \subset \sqrt{J}$,
b) $\sqrt{I \cdot J} = \sqrt{I \cap J}$,
c) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$,
d) $\sqrt{\sqrt{I}} = \sqrt{I}$,
e) si $\mathfrak{p}$ est un idéal premier, alors $\sqrt{\mathfrak{p}} = \mathfrak{p}$,
f) $\sqrt{I} + \sqrt{J} \subset \sqrt{I + J}$,
g) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$,
h) $\sqrt{(I \cap J) + (I \cap L)} = \sqrt{I \cap (J + L)}$,
i) soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$ des idéaux premiers de A, supposons que

$$I \subset \bigcap_{i=1}^{n} \mathfrak{p}_i \subset \sqrt{I},$$

montrer que

$$\sqrt{I} = \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Exercice 22. Soit A un anneau factoriel et $a \in A$. Montrer que $\sqrt{aA}$ est un idéal principal.

Solution. Si $a = 0$, alors $\sqrt{(a)} = 0$ puisque A est intègre. Sinon, soit $a = \prod_i p_i^{n_i}$ la décomposition en facteurs irréductibles de a, avec $n_i \geq 1$. Soit $b = \prod_i p_i$. Alors $b^{\max_i n_i} \in (a)$ et donc $b \in \sqrt{(a)}$. Réciproquement si $c \in \sqrt{(a)}$, alors il existe n tel que a divise c^n. En particulier p_i divise c^n et donc p_i divise c d'après le lemme de Gauss. Donc $b = \prod_i p_i$divise c. Donc $\sqrt{(a)} = (b)$.

Exercice 23. Montrer que $A = k[X, Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$.

Solution. Soit $f : k[X, Y] \to k[T]$ l'unique morphisme de k-algèbres envoyant X sur T^3 et Y sur T^2. Alors $X^2 - Y^3 \in \ker f$, donc par factorisation f induit un morphisme $g : A \to k[T]$. Montrons que ce morphisme est injectif, c'est-à-dire $\ker f = (X^2 - Y^3)$.
Soit $P(X, Y) \in \ker f$. Comme $X^2 - Y^3$ est unitaire en X, on peut effectuer la division euclidienne dans $k[Y][X]$ de P par $X^2 - Y^3$. Le reste de la division euclidienne $R(X, Y)$ appartient également à $\ker f$ et est de degré au plus 1 en X : $R(X, Y) = A(Y)X + B(Y) = X \sum_i a_i Y^i + \sum_i b_i Y^i$. Alors $0 = f(R) = A(T^2)T^3 + B(T^2) = \sum_i a_i T^{2i+3} + \sum_i biT^{2i}$. T Tous les exposants de T apparaissant sont distincts (ils sont impairs dans la première somme et paire dans la deuxième). Donc pour tout i,$a_i = b_i = 0$, et donc $R = 0$ et $P \in X^2 - Y^3$. Ce qui prouve l'injectivité de g. Comme $k[T]$ est intègre, A aussi.

3 Idéaux premiers et maximaux

Exercice 24. Montrer qu'un élément x de A appartient à tous les idéaux maximaux de A si et seulement si pour tout $a \in A$, $1 - ax$ est inversible (l'intersection de tous les idéaux maximaux de$A$ est appelé le radical de Jacobson de A).

Solution. Supposons que x appartient à tout les idéaux maximaux. Soit $a \in A$. Si $1 - ax$ appartient à un idéal maximal $\mathfrak{m}$ alors $1 = (1 - ax) + ax$ appartiendrait aussi à cet idéal maximal, ce qui est impossible. Donc $1 - ax$ n'appartient à aucun idéal maximal (car tout idéal propre est contenu dans un idéal maximal donc $(1 - ax) = A$).
Réciproquement, soit $\mathfrak{m}$ un idéal maximal et supposons par contraposition que $x \notin \mathfrak{m}$. Alors $\bar{x}$ est inversible dans le corps $A/\mathfrak{m}$, donc il existe $a \in A$ tel que $\bar{a}/barx = \bar{1}$. Donc $\overline{1 - ax} = 0$, donc $1 - ax$ n'est pas inversible, ce qui prouve la réciproque.

Exercice 25. Soit A un anneau et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$.

a) Montrer que P est nilpotent si et seulement si pour tout $i \in \mathbb{N}$, a_i est nilpotent.

b) Soit x un élément nilpotent de A. Montrer que $1 + x$ est inversible.

c) Montrer que P est inversible dans $A[X]$ si et seulement si a_0 est inversible et pour tout $i \geq 1$, a_i est nilpotent.

Indice : si $Q = \sum_{i=0}^{m} b_i X^i$ est un inverse de P, on pourra commencer par montrer que que pour tout $r \geq 0$, $a_n^{r+1} b_{m-r} = 0$.

d) Montrer que P est dans l'intersection de tous les idéaux maximaux si et seulement si P est nilpotent (c'est-à-dire, dans $A[X]$, le radical de Jacobson est égal au nilradical).

Solution. a) Si a_i est nilpotent dans A pour tout i, il l'est aussi dans $A[X]$ et donc P, qui appartient à l'idéal de $A[X]$ engendré par les a_i l'est aussi (puisque les éléments nilpotents forment un idéal).

Réciproquement, on raisonne par récurrence sur le degré de P (c'est évident si P est un polynôme constant). Si $P^k = 0$, alors le coefficient en X^{nk} dans P^k, qui est a_n^k, doit être nul. Donc a_n est nilpotent. Donc $Q = P - a_n X^n$ est aussi nilpotent et $\deg Q < \deg P$. Donc les coefficients de Q sont nilpotents, or ce sont les coefficients de P (à l'exception de a_n). D'où le résultat.

b) Si $x^n = 0$, on pose $x' = \sum_{i=0}^{n-1} (-x)^i$ et on vérifie que $x'(1 + x) = 1$.

c) Si a_0 est inversible et a_i nilpotent pour $i \geq 1$, alors $P = a_0(1 + a_0^{-1} \sum_{i=1}^{n} a_i X^i)$. D'après a), $a_0^{-1} \sum_{i=1}^{n} a_i X^i$ est nilpotent, donc $(1 + a_0^{-1} \sum_{i=1}^{n} a_i X^i)$ est inversible d'après b), et donc P est inversible comme produit d'inversibles.

Réciproquement, soit $Q = \sum_{i=0}^{m} b_i X^i$ un inverse de P. Alors $1 = a_0 b_0$, donc a_0 et b_0 est inversible. Montrons par récurrence sur r que $a_n^{r+1} b_{m-r} = 0$.

Pour $r = 0$, il suffit de regarder le coefficient de X^{m+n} dans $PQ = 1$.

Pour $r \geq 1$ alors le coefficient de X^{m+n-r} dans $PQ = 1$ est $0 = a_n b_{m-r} + \sum_{k=0}^{r-1} a_k b_{m-k}$. En multipliant par a_n^r et puisque $0 = a_n^k b_{m-k} | a_k b_{m-k} a_n^r$ pour $k \leq r - 1$, il ne reste plus que $0 = a_n^{r+1} b_{m-r}$, comme voulu.

En prenant, $r = m$, on obtient $a_n^{m+1} b_0 = 0$, et donc a_n est nilpotent puisque b_0 est inversible.

Donc $P - a_n X^n$ est aussi inversible (par la question b)), et de degré strictement inférieur à P. Par récurrence sur le degré de P, on en déduit que $a_i = 0$ pour $1 \leq i \leq n - 1$.

d) Supposons que x appartienne à tous les idéaux maximaux de A. Si $1 - ax$ n'est pas inversible, $(1 - ax)$ est un idéal propre, donc contenu dans un idéal maximal $\mathfrak{m}$. Alors $1 = (1 - ax) + ax \in \mathfrak{m}$ comme combinaison linéaire d'éléments de $\mathfrak{m}$. D'où une contradiction.

Si $1 - ax$ est inversible pour tout a. Soit $\mathfrak{m}$ un idéal maximal de A ne contenant pas x. Alors l'image $\bar{x}$ de x dans $A/\mathfrak{m}$ est non nul donc inversible, d'inverse $\bar{x}'$. Alors $1 - xx' \in \mathfrak{m}$ ne peut pas être inversible contrairement à l'hypothèse.

e) Si P est dans tout idéal premier, a fortiori il est dans tout idéal maximal.

Réciproquement, si P est dans tout idéal maximal, alors d'après d), $1 + XP$ est inversible. On déduit donc de c), que les coefficients de P sont nilpotents, donc P est nilpotent d'après a). Il appartient donc à tout idéal premier.

Exercice 26. Soit $f : A \to B$ un morphisme d'anneaux.
(i) Montrer que l'image réciproque d'un idéal premier est encore un idéal premier.
(ii) Est-ce encore vrai pour les idéaux maximaux ? Et si f est surjectif ?

Solution. Remarque préliminaire :
Soit $\mathfrak{p}$ un idéal de B, alors comme $0 \in \mathfrak{p}$, alors $f^{-1}(\mathfrak{p}) \supset \ker f$. Ainsi le morphisme induit

$$\overline{f} : A/f^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$$

est injectif : si $\overline{x} \in \ker \overline{f}$, alors $f(x) \in \mathfrak{p}$ donc $x \in f^{-1}(\mathfrak{p})$ donc $\overline{x} = 0$. Ainsi $\overline{f}$ est toujours injectif.
(i) Si $\mathfrak{p}$ est premier, alors $B/\mathfrak{p}$ est intègre, mais comme $\overline{f} : A/f^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$ est injectif, $A/f^{-1}(\mathfrak{p})$ est aussi intègre donc $f^{-1}(\mathfrak{p})$ est premier.
(ii) Si f n'est pas surjectif, c'est faux. Par exemple considérons l'inclusion $\mathbb{Z} \to \mathbb{Q}$ et prenons $\mathfrak{p} = (0) \subset \mathbb{Q}$ qui est un idéal maximal de $\mathbb{Q}$. Alors $f^{-1}(\mathfrak{p}) = (0)$ qui est un idéal premier de $\mathbb{Z}$ (car $\mathbb{Z}/(0)$ est intègre) mais pas maximal (car $\mathbb{Z}/(0)$ n'est pas un corps).
Si par contre f est surjectif, alors $\overline{f}$ est surjectif. Or on a vu qu'il est injectif donc il est bijectif. Si $\mathfrak{p}$ est maximal, alors $B/\mathfrak{p}$ est un corps et donc $A/f^{-1}(\mathfrak{p})$ aussi (car $\overline{f}$ est bijective) et $f^{-1}(\mathfrak{p})$ est maximal.

Exercice 27. Soit A un anneau et I un idéal et soit $\pi : A \to A/I$. Montrer que :
(i) les idéaux de A/I sont en bijection avec les idéaux de A contenant I,
(ii) cette bijection induit une bijection sur les idéaux premiers et les idéaux maximaux.

Solution. (i) Soit $\mathcal{C} = \{J \subset A, \text{ idéal } / \ I \subset J\}$ et $\mathcal{E} = \{L \subset A/I \ / \ J \text{ est un idéal}\}$. Considérons les applications suivantes $f : \mathcal{C} \to \mathcal{E}$, $f(J) = \pi(J)$ ($\pi(J)$ est bien un idéal de A/I car il est stable par addition et si $\pi(a) \in A/I$ et $\pi(j) \in \pi(J)$, alors $\pi(a)\pi(j) = \pi(aj) \in \pi(J)$) et $g : \mathcal{E} \to \mathcal{C}$, $g(L) = \pi^{-1}(L)$ ($\pi^{-1}(L)$ contient bien I car $0 \in L$ et $\pi^{-1}(0) = I$).
Nous montrons que f et g sont des bijections réciproques. On a $f(g(L)) = \pi(\pi^{-1}(L)) \subset L$. Soit maintenant $x \in L$, comme π est surjective, on peut écrire $x = \pi(a)$, mais alors $a \in \pi^{-1}(L)$ et donc $x \in \pi(\pi^{-1}(L))$. On a bien $f \circ g = \mathrm{id}_{\mathcal{E}}$.
Par ailleurs, $g(f(J)) = \pi^{-1}(\pi(J)) = J + I = J$ car $I \subset J$. On a bien $g \circ f \mathrm{id}_{\mathcal{C}}$.
(ii) Supposons maintenant que $J \in \mathcal{C}$ est premier, c'est-à-dire A/J est intègre. Son image dans $\mathcal{E}$ est $\pi(J) = J/I$ et on a $(A/I)/(J/I) \simeq A/J$ est intègre donc $\pi(J)$ est premier.
Réciproquement, si $L \in \mathcal{E}$ est premier, c'est-à-dire $(A/I)/L$ est intègre. Son image dans $\mathcal{C}$ est $J = \pi^{-1}(L)$ et on a $A/L = (A/I)/(J/I) \simeq A/J$ est intègre donc J est premier.
De même en remplaçant premier par maximal et anneau intègre par corps, on a le résultat pour les idéaux maximaux.

Exercice 28. Soit $\mathfrak{p}$ un idéal premier d'un anneau A, et soient $(I_i)_{1 \leq i \leq n}$ des idéaux de A. Supposons que

$$\mathfrak{p} \supset \prod_{i=1}^{n} I_i,$$

montrer que $\mathfrak{p}$ contient l'un des idéaux I_i.

Solution. Supposons que $\mathfrak{p}$ ne contienne aucun des idéaux I_i, alors pour chaque i, il existe $x_i \in I_i$ tel que $x_i \notin \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, le produit de ces x_i n'est pas dans $\mathfrak{p}$. Cependant on a

$$\prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} I_i \subset \mathfrak{p}$$

ce qui est une contradiction.

Exercice 29. Soient $(\mathfrak{p}_i)_{1 \leq i \leq n}$ des idéaux premiers d'un anneau A, et soit I un idéal de A tel que

$$I \subset \cup_{i=1}^{n} \mathfrak{p}_i.$$

Montrer que I est contenu dans l'un des $\mathfrak{p}_i$.

Solution. Quitte à remplacer les $\mathfrak{p}_i$ par un sous-ensemble, on peut supposer qu'aucun des $\mathfrak{p}_i$ n'est contenu dans un $\mathfrak{p}_j$ (sinon on garde le plus grand, le plus petit ne sert à rien).
Remarquons que comme $\mathfrak{p}_j \not\subset \mathfrak{p}_1$ pour $j \geq 2$, on peut trouver $b_j \in \mathfrak{p}_j$ tel que $b_j \notin \mathfrak{p}_1$ et on a $a_1 = b_2 \cdots b_n \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ mais $a_1 \notin \mathfrak{p}_1$. De même on peut trouver des $a_j \notin \mathfrak{p}_j$ tels que a_j appartienne à tous les autres $\mathfrak{p}_i$.
Supposons que I n'est contenu dans aucun $\mathfrak{p}_i$, alors pour tout i, il existe $x_i \in I$ tel que $x_i \notin \mathfrak{p}_i$.
Considérons l'élément $x = \sum a_i x_i$. Comme $x_i \in I$ pour tout i, on a $x \in I$.
Par ailleurs, comme $a_1 \notin \mathfrak{p}_1$, $x_1 \notin \mathfrak{p}_1$ et que $\mathfrak{p}_1$ est premier on a $a_1 x_1 \notin \mathfrak{p}_1$. Mais on a $a_2 x_2 + \cdots a_n x_n \in \mathfrak{p}_1$ car tous les $a_i \in \mathfrak{p}_1$ pour $i \geq 2$, ainsi $x \notin \mathfrak{p}_1$. De même, $x \notin \mathfrak{p}_i$ pour tout i, donc

$$x \notin \cup_{i=1}^{n} \mathfrak{p}_i$$

ce qui est absurde.

Exercice 30. Soit A un anneau et nil(A) l'ensemble des éléments nilpotents de A.
(i) Montrer que nil(A) est un idéal.
(ii) Montrer que si $\mathfrak{p}$ est un idéal premier, alors nil(A) $\subset \mathfrak{p}$.
(iii) Soit $s \notin$ nil(A) et $S = \{1, s, \cdots, s^n, \cdots\}$. Montrer que l'ensemble des idéaux de A disjoints de S contient un élément maximal $\mathfrak{p}$ (utiliser le lemme de Zorn). Montrer que $\mathfrak{p}$ est premier. En déduire que

$$\mathrm{nil(A)} = \bigcap_{\mathfrak{p} \text{ idéal premier}} \mathfrak{p}.$$

Solution. Soient $a \in A$ et $x \in \text{nil(A)}$, alors il existe $n \in \mathbb{N}$ tel que $x^n = 0$, mais alors $(ax)^n = a^n x^n = 0$ donc $ax \in \text{nil(A)}$.
Soient x et y des éléments de nil(A), alors il existe $n \in \mathbb{N}$ tel que $x^n = 0$ et $m \in \mathbb{N}$ tel que $y^m = 0$. On calcule alors

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Si $k \in [0, n]$, alors $n + m - k \geq m$ donc $y^{n+m-k} = 0$ et si $k \in [n, n+m]$, alors $x^k = 0$. Ainsi $(x+y)^{n+m} = 0$ et $x + y \in \text{nil(A)}$.
(ii) Soit $\mathfrak{p}$ un idéal premier et $x \in \text{nil(A)}$, il existe alors $n \in \mathbb{N}$ tel que $x^n = 0 \in \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, ceci impose que $x \in \mathfrak{p}$.
(iii) Montrons que l'ensemble des idéaux de A disjoints de S vérifie les hypothèses du lemme de Zorn c'est-à-dire est inductif pour l'inclusion : pour toute suite croissante $(I_n)_{n\in\mathbb{N}}$ d'idéaux disjoints de S, alors la réunion I de ces idéaux est encore un idéal disjoint de S.
Il est clair que I est encore un idéal, en effet, si x et y sont dans I, alors il existe n et m tels que $x \in I_n$ et $y \in I_m$ et on a $x + y \in I_{\max(n,m)} \subset I$. De même si $a \in A$, alors $ax \in I_n \subset I$.
Il reste à voir que I ne rencontre pas S. Mais si I rencontrait S, alors il existerait $k \in \mathbb{N}$ tel que $s^k \in I$ ce qui signifie qu'alors il existerait un $n \in \mathbb{N}$ tel que $s^k \in I_n$, c'est-à-dire que I_n rencontrerait S, c'est absurde.
Ainsi par le lemme de Zorn, il existe un idéal maximal parmi les idéaux de A disjoints de S. Soit $\mathfrak{p}$ un tel idéal, montrons qu'il est premier. Soient donc x et y dans A tels que $xy \in \mathfrak{p}$. Il faut montrer que $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Si on a $x \notin \mathfrak{p}$ et $y \notin \mathfrak{p}$, alors les idéaux $\mathfrak{p} + (x)$ et $\mathfrak{p} + (y)$ rencontrent S. Il existent donc n et m des entiers tels que

$$s^n = p_1 + a_1 x \quad \text{et} \quad s^m = p_2 + a_2 y$$

avec $p_i \in \mathfrak{p}$ et $a_i \in A$. Alors on calcule le produit, on a

$$s^{n+m} = p_1 p_2 + p_1 a_2 y + p_2 a_1 x + a_1 a_2 xy \in \mathfrak{p}.$$

Ce qui est absurde car $\mathfrak{p}$ ne rencontre pas S. L'idéal $\mathfrak{p}$ est donc premier.
Montrons la dernière égalité. On a vu au (ii) que pour tout idéal premier, on a $\text{nil(A)} \subset \mathfrak{p}$ donc

$$\text{nil(A)} \subset \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}.$$

Réciproquement, soit $s \notin \text{nil(A)}$, d'après ce qu'on vient de montrer, il existe un idéal premier $\mathfrak{p}$ tel que $\mathfrak{p}$ ne rencontre pas S, en particulier $s \notin \mathfrak{p}$ ce qui montre que $s \notin \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.

Exercice 31. Montrer que dans un anneau principal A, les idéaux premiers sont maximaux.

Solution. Soit $\mathfrak{p}$ un idéal premier et soit $\mathfrak{m}$ un idéal le contenant. Comme l'anneau est principal, on peut écrire $\mathfrak{p} = (p)$ et $\mathfrak{m} = (m)$. Le fait que $\mathfrak{p} \subset \mathfrak{m}$ se traduit par : $p = am$ avec $a \in A$. Mais alors comme $\mathfrak{p}$ est premier, on a $a \in \mathfrak{p}$ ou $m \in \mathfrak{p}$. Si $m \in \mathfrak{p}$, alors $\mathfrak{p} = \mathfrak{m}$ et on a fini. Sinon, alors $a \in \mathfrak{p}$ donc il existe $u \in A$ tel que $a = up$ donc $p = upm$ et comme A est intègre (car principal) on a $1 = um$ donc m est inversible et $\mathfrak{m} = A$. L'idéal $\mathfrak{p}$ est donc maximal.