TD n°2.

1 Arithmétique

Exercice 1. Soit n un entier supérieur ou égal à 1. Montrer que :

a) un élément $Cl(m) \in \mathbb{Z}/n\mathbb{Z}$ est une unité ssi m et n sont premiers entre eux,

b) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier,

c) l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'a pas d'élément nilpotent non nul ssi n n'a pas de facteur carré.

d) Déterminer l'idéal $\sqrt{n\mathbb{Z}}$ (rappelons que $\sqrt{I} = \{a \ / \exists k \in \mathbb{N} \ / \ a^k \in I\}$).

Solution. a) Soit $m \in \mathbb{Z}$, dire que $Cl(m)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ signifie qu'il existe $m' \in \mathbb{Z}$ tel que $Cl(m)Cl(m') = Cl(1)$ dans $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $n' \in \mathbb{Z}$ tel que $mm' = 1 + nn'$ ce qui signifie que m et n sont premiers entre eux.

Réciproquement si m et n sont premiers entre eux, il existe m' et n' dans $\mathbb{Z}$ tels que l'on ait $mm' + nn' = 1$ ce qui donne dans $\mathbb{Z}/n\mathbb{Z}$ la relation $Cl(m)Cl(m') = 1$ donc $Cl(m)$ est inversible.

b) Si n est premier, montrons que $\mathbb{Z}/n\mathbb{Z}$ est intègre. Soient a et b tels que $Cl(a)Cl(b) = 0$ dans $\mathbb{Z}/n\mathbb{Z}$, alors il existe $n' \in \mathbb{Z}$ tel que $ab = nn'$. Ainsi n divise le produit ab et comme n est premier, soit n divise a (c'est-à-dire $Cl(a) = 0$), soit n divise b (c'est-à-dire $Cl(b) = 0$).

Réciproquement, supposons que n n'est pas premier, alors on peut écrire $n = n_1 n_2$ avec n_1 et n_2 des entiers tels que $1 < n_1 < n$ et $1 < n_2 < n$. Alors on a $Cl(n_1) \neq 0$ et $Cl(n_2) \neq 0$ dans $\mathbb{Z}/n\mathbb{Z}$ alors que $Cl(n_1)Cl(n_2) = Cl(n_1 n_2) = Cl(n) = 0$. Dans ce cas $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

c) Écrivons la décomposition de n en facteurs premiers :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Supposons que pour tout i, on ait $\alpha_i = 1$ (c'est-à-dire n n'a pas de facteur carré). Soit alors $m \in \mathbb{Z}$ tel que $Cl(m)$ est nilpotent dans $\mathbb{Z}/n\mathbb{Z}$, il existe alors $k \geq 1$ tel que $Cl(m)^k = 0$. Il existe donc $n' \in \mathbb{Z}$ tel que $m^k = nn'$. Pour tout i, on a alors p_i divise m^k et comme p_i est premier, alors p_i divise m. Ainsi $n = \prod_{i=1}^{r} p_i$ divise m et $Cl(m) = 0$.

Réciproquement, supposons que l'un des α_i est différent de 1 (disons $\alpha_1 > 1$). Considérons alors

$$m = p_1^{\alpha_1 - 1} \prod_{i=2}^{r} p_i^{\alpha_i}.$$

On a $Cl(m) \neq 0$ et

$$m^2 = p_1^{2\alpha_1 - 2} \prod_{i=2}^{r} p_i^{2\alpha_i}.$$

Mais $2\alpha_i \geq \alpha_i$ et $2a_1 - 2 \geq \alpha_1$ (car $a_1 \geq 2$), donc n divise m^2, ainsi $Cl(m)^2 = 0$ donc m est nilpotent non nul dans $\mathbb{Z}/n\mathbb{Z}$.

d) Encore une fois on écrit la décomposition de n en facteurs premiers :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Si $m \in \sqrt{n\mathbb{Z}}$, alors il existe $k \in \mathbb{N}$ tel que $m^k \in n\mathbb{Z}$ c'est-à-dire n divise m^k. Mais alors pour tout facteur premier p_i de n, on a p_i divise m^k et donc p_i divise m. Ainsi l'entier

$$n' = \prod_{i=1}^{r} p_i$$

divise m. On a donc montré que $\sqrt{n\mathbb{Z}} \subset n'\mathbb{Z}$.

Réciproquement, soit $m \in n'\mathbb{Z}$, on a donc $m = an'$ avec $a \in \mathbb{Z}$. Soit alors $k = \max_{i\in[1,r]}(\alpha_i)$, on calcule m^k et on a

$$m^k = a\prod_{i=1}^{r} p_i^k.$$

Comme pour tout i, on a $k \geq \alpha_i$, alors n divise m^k et donc $m \in n\mathbb{Z}$ ou encore $m \in \sqrt{n\mathbb{Z}}$. On a donc $\sqrt{n\mathbb{Z}} = n'\mathbb{Z}$.

Exercice 2. Soit n un entier impair et x un entier premier avec n, on se propose de déterminer à quelle condition x est un carré dans $\mathbb{Z}/n\mathbb{Z}$.

a) Dans cette question on suppose que $n = p$ un nombre premier. Montrer que x est un carré non nul dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si on a

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Combien y'a-t-il de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

En déduire que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod 4$.

b) On décompose maintenant n en facteurs premiers : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Montrer que x est est un carré dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si pour tout $i \in [1, r]$, x est un carré dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

c) Montrer que x est un carré dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$si et seulement x est un carré dans $\mathbb{Z}/p_i^{\alpha_i-1}\mathbb{Z}$.

d) En déduire que x est un carré dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si c'est un carré dans $\mathbb{Z}/p_i\mathbb{Z}$ pour tout p_i facteur premier de n.

Solution. a) Considérons le morphisme

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

$$z \mapsto z^2$$

dont l'image est l'ensemble des carrés non nuls et le noyau est $\{\pm 1\}$. On en déduit que le nombre de carrés non nuls est $\frac{p-1}{2}$. Considérons maintenant le morphisme de groupes multiplicatifs :

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

$$z \mapsto z^{\frac{p-1}{2}}.$$

Comme pour tout élément x non nul de $\mathbb{Z}/p\mathbb{Z}$ on a $x^{p-1} = 1$, on voit que l'ensemble des carrés est contenu dans le noyau. Cependant le noyau est formé des racines de l'équation

$$X^{\frac{p-1}{2}} - 1 = 0.$$

Il y en a au plus $\frac{p-1}{2}$. Le noyau est donc formé uniquement des carrés et on a le résultat.

On a vu que le nombre de carrés non nuls est $\frac{p-1}{2}$. Comme 0 est u carré il y a donc $\frac{p+1}{2}$ carrés.

b) Le lemme chinois nous permet de dire qu'il y a un isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

$$Cl(x) \mapsto (Cl_1(x), \cdots, Cl_r(x))$$

où $Cl(x)$ est la classe de x dans $\mathbb{Z}/n\mathbb{Z}$ et $Cl_i(x)$ est la classe de x dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Ainsi, si $Cl(x) = Cl(y)^2$ est un carré alors $(Cl_1(x), \cdots, Cl_r(x)) = (Cl_1(y), \cdots, Cl_r(y))^2$ est un carré c'est-à-dire pour tout i, $Cl_i(x) = Cl_i(y)^2$ est un carré. Réciproquement si pour tout i, on a $Cl_i(x) = Cl_i(y_i)^2$ est un carré, alors il existe y tel que $Cl(y) \mapsto (Cl_1(y_1), \cdots, Cl_r(y_r))$ et donc $Cl(y)^2 = Cl(x)$ qui est donc un carré.

c) On écrit $p_i = p$. Si x est un carré dans $\mathbb{Z}/p^k\mathbb{Z}$, alors $x \equiv y^2 \pmod{p^k}$ donc $x \equiv y^2 \pmod{p^{k-1}}$ et x est un carré dans $\mathbb{Z}/p^{k-1}\mathbb{Z}$. Réciproquement, si $x \equiv y^2 \pmod{p^{k-1}}$, il existe alors $a \in \mathbb{Z}$ tel que $x = y^2 + ap^{k-1}$. Comme x est premier avec n, il est premier avec p. C'est aussi le cas de y donc y est inversible dans $\mathbb{Z}/p^k\mathbb{Z}$. On cherche z sous la forme $z = y + bp^{k-1}$ tel que $x \equiv z^2 \pmod{p^k}$. On a alors

$$z^2 \equiv y^2 + 2byp^{k-1} + b^2p^{2k-2} \pmod{p}.$$

Comme $k > 1$, on a $2k - 2 \geq k$, on a $b^2 p^{2k-2} \equiv 0 \pmod{p}$ et comme y et 2 (car n est impair donc les p_i sont disctincts de 2) sont inversibles dans $\mathbb{Z}/p^k\mathbb{Z}$, on peut poser

$$b \equiv \frac{a}{2y} \pmod{p}.$$

On a alors

$$z^2 \equiv y^2 + ap^{k-1} \equiv x \pmod{p}.$$

d) On voit par récurrence que x est un carré dans $\mathbb{Z}/p^{\alpha_i}\mathbb{Z}$ si et seulement si c'est un carré dans $\mathbb{Z}/p_i\mathbb{Z}$. Ainsi avec le b), on voit que x est un carré dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x est un carré dans $\mathbb{Z}/p_i\mathbb{Z}$ pour tout facteur premier p_i de n. Grâce au (ı), on a que x est un carré dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si pour tout facteur premier p_i de n, on a

$$x^{\frac{p_i-1}{2}} \equiv 1 \pmod{p_i}.$$

Exercice 3. Soit $A = \mathbb{Z}[i] = \{a + ib\}_{a,b\in\mathbb{Z}}$.

a) Montrer que si $\alpha, \beta \neq 0 \in A$, il existe $r, q \in A$ tels que $\alpha = q\beta + r$ avec $|r| < |\beta|$ (donc A est un anneau euclidien).

b) Montrer que si α divise $\beta\beta'$ dans A et α est irréductible, alors α divise β ou β'.

c) Montrer qu'un nombre premier p impair est somme de deux carrés si et seulement si $p \equiv 1 \pmod{4}$.

d) Montrer qu'un entier $n > 0$ est somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout $p \equiv 3 \pmod{4}$.

Exercice 4. a) Montrer que l'équation diophantienne (c'est-à-dire qu'on cherche des solutions qui sont des nombres entiers) $x^2 + y^2 = 3z^2$ n'a pas de solution non triviale (c'est-à-dire différente de $(0, 0, 0)$). On pourra raisonner par l'absurde en considérant une solution non triviale telle que x, y et z sont premiers entre eux et réduire modulo 3.

b) Même question pour les équations $x^2 + y^2 = 7z^2$ et $x^2 + y^2 = 11z^2$.

c) Montrer que les équations $x^2 + y^2 = 5z^2$ et $x^2 + y^2 = 13z^2$ ont des solutions non triviales.

d) Essayer de généraliser à certaines équations $x^2 + y^2 = pz^2$ pour certains nombre premiers p (on pourra étudier à quelle condition -1 est un carré dans $\mathbb{F}_p$).

Solution. Les cas a) et b) découlerons de l'étude du cas d).
c) On a la solution $(2, 1, 1)$ à la première équation et la solution $(3, 2, 1)$.
d) Plus généralement, si il existe deux entiers x et y tels que $p = x^2 + y^2$ ce qui est équivalent (cf. cours) à ce que $p \equiv -1 \pmod{4}$ ou encore à ce que -1 soit un carré dans $\mathbb{F}_p$, alors on a $(x, y, 1)$ est une solution non triviale de l'équation.
Réciproquement, supposons que $p \not\equiv -1 \pmod{4}$. Considérons une solution (x, y, z) non triviale de l'équation, quitte à diviser x, y et z, on peut supposer que x, y et z sont premiers entre eux (dans leur ensemble). Réduisons modulo p, on a alors $x^2 + y^2 \equiv 0 \pmod{p}$. Si $x \equiv 0 \pmod{p}$, alors $y \equiv 0 \pmod{p}$. Sinon, la classe de x est inversible dans $\mathbb{F}_p$ et on a $\frac{y}{x} \equiv -1 \pmod{p}$ ce qui est impossible car -1 n'est pas un carré dans $\mathbb{F}_p$. On doit donc avoir p qui divise x et y ce qui impose que p^2 divise pz^2 et donc p divise z. C'est absurde puisque x, y et z sont premiers entre eux.

Exercice 5. Montrer que dans un corps fini K (disons $\mathbb{Z}/p\mathbb{Z}$ avec p premier), tout élément est somme de eux carrés (on pourra compter le nombre de carrés et comparer si $a \in K$ est un élément fixé les ensembles $\{x^2 \ / \ x \in K\}$ et $\{a - y^2 \ / \ y \in K\}$).

Solution. C'est une application du principe des tiroirs. Fixons un élément a dans K quelconque. On sait cf. exercice 2 qu'il y a $\frac{q+1}{2}$ carrés dans K avec $q = \mathrm{Card}(K)$. Ainsi les deux ensembles de l'énoncé ont chacun $\frac{q+1}{2}$ éléments. S'il étaient disjoints, on aurait $q + 1$ éléments dans K ce qui est impossible. Ils ont donc un élément commun z qui s'écrit $z = x^2$ mais aussi $z = a - y^2$ pour un certain x et un certain y dans K. On a donc $a = x^2 + y^2$.

Exercice 6. Soit $d \in \mathbb{Z}$ sans facteur carré.

a) Soit K l'ensemble $K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \ / \ (a, b) \in \mathbb{Q}\}$. Montrer que K est un sous-corps de $\mathbb{C}$.

b) On note A l'ensemble des éléments de K qui sont entiers sur $\mathbb{Z}$, c'est-à-dire qui sont racines d'un polynôme unitaire de $\mathbb{Z}[X]$. Montrer que A est un sous-anneau de K.

c) Montrer que pour tout couple $(a, b) \in \mathbb{Z}^2$, l'élément $a + b\sqrt{d}$ de K est dans A.

d) Montrer que l'application $\sigma : K \to K$ définie par $\sigma(a+b\sqrt{d}) = a - b\sqrt{d}$ est un automorphisme de corps tels que $\sigma(x) = x$ si et seulement si $x \in \mathbb{Q}$. Montrer que si $x \in A$, alors $\sigma(x) \in A$ et que x et $\sigma(x)$ vérifient la même relation intégrale sur $\mathbb{Z}$.

e) Montrer que $T(x) = x + \sigma(x)$ (trace de x) et $N(x) = x\sigma(x)$ (norme de x) sont dans $\mathbb{Q}$.
En déduire que si $x \in A$, alors $T(x)$ et $N(x)$ sont dans $\mathbb{Z}$ puis expliciter une relation intégrale de x sur $\mathbb{Z}$ à l'aide de la trace et de la norme de x.

f) Déduire de ce qui précède que l'élément $x = a + b\sqrt{d}$ de K est dans A si et seulement si $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$.

g) On suppose maintenant les conditions $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$ vérifiée. Montrer qu'alors $2b \in \mathbb{Z}$. On peut donc poser $a = \frac{u}{2}$ et $b = \frac{v}{2}$ avec u et v dans $\mathbb{Z}$. Les conditions précédentes se résument en $u^2 - db^2 \in 4\mathbb{Z}$.

h) Montrer que v et u ont la même parité et que s'ils sont impairs, alors $d \equiv 1 \pmod 4$.

i) Conclure que si $d \equiv 1 \pmod 4$, alors $A = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et $A = \mathbb{Z}[\sqrt{d}]$ sinon.

Solution. a) Il est clair que somme et produit d'éléments de K sont encore dans K. Par ailleurs, l'inverse de l'élément $a + b\sqrt{d}$ non nul est $\frac{a-b\sqrt{d}}{a^2-db^2}$ qui existe toujours car le dénominateur ne peut s'annuler. En effet, si b est nul alors a aussi ce qui contredit le fait que $a + b\sqrt{d}$ est non nul. Si b est non nul, on aurait $d = \frac{a^2}{b^2}$ serait un carré ce qui est impossible.

b) On sait que si x et y sont dans A, alors $x + y$, $x - y$ et xy sont encore dans K (car c'est un corps) et sont encore des entiers algébriques (cf. le cours). Ils sont donc encore dans A.

c) Comme les éléments de $\mathbb{Z}$ sont des entiers algébriques et que l'ensembles des entiers algébriques est un anneau, il suffit de montrer que $\sqrt{d}$ est un entier algébrique ce qui est clair puisqu'il est racine du polynôme $X^2 - d$.

d) Il faut montrer que σ préserve l'addition et la multiplication. Prenons $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$. On a alors $x + y = (a + a') + (b + b')\sqrt{d}$ et $xy = (aa' + dbb') + (ab' + a'b)\sqrt{d}$. On calcule $\sigma(x + y) = (a + a') - (b + b')\sqrt{d} = \sigma(x) + \sigma(y)$ et $\sigma(xy) = (aa' + dbb') - (ab' + a'b)\sqrt{d} = \sigma(x)\sigma(y)$.
Supposons maintenant que $\sigma(x) = x$ c'est-à-dire que l'on a $a + b\sqrt{d} = a - b\sqrt{d}$ et donc $2b\sqrt{d} = 0$ ce qui impose $b = 0$ et $x \in \mathbb{Q}$. Réciproquement il est clair que si $x \in \mathbb{Q}$, alors $\sigma(x) = x$.
Supposons que x soit dans A. Il est donc racine d'un polynôme unitaire à coefficients entiers $P = X^n + a_1X^{n-1} + \cdots + a_n$ (pour tout i, on a $a_i \in \mathbb{Z}$) c'est-à-dire qu'on a $x^n + a_1x^{n-1} + \cdots + a_n = 0$. On applique σ à cette égalité et on obtient $\sigma(x)^n + \sigma(a_1)\sigma(x)^{n-1} + \cdots + \sigma(a_n) = 0$ mais comme les a_i sont dans $\mathbb{Z} \subset \mathbb{Q}$, on a $\sigma(a_i) = a_i$ donc $\sigma(x)^n + a_1\sigma(x)^{n-1} + \cdots + a_n = 0$ et x et $\sigma(x)$ vérifient la même relation.

e) Si $x = a + b\sqrt{d}$ alors $T(x) = 2a \in \mathbb{Q}$ et $N(x) = a^2 - db^2 \in \mathbb{Q}$. Si x est dans A, alors $\sigma(x)$ l'est aussi (cf. question précédente) et $T(x)$ et $N(x)$ sont aussi dans A car c'est un anneau. Mais alors $T(x)$ et $N(x)$ sont dans $\mathbb{Q}$ et entiers sur $\mathbb{Z}$. D'après l'exercice **??**, ils doivent être dans $\mathbb{Z}$. Par ailleurs, il est bien clair que l'on a la relation

$$(X - x)(X - \sigma(x)) = X^2 - T(x)X + N(x)$$

qui est un polynôme à coefficients entiers dont les racines sont exactement x et $\sigma(x)$.

f) On vient de voir que si x est dans A, alors $T(x)$ et $N(x)$ sont dans $\mathbb{Z}$ c'est-à-dire $2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$. Réciproquement si $T(x)$ et $N(x)$ sont dans $\mathbb{Z}$, le polynôme ci-dessus donne une relation intégrale pour x et $x \in A$.

g) On a $a^2 - db^2 \in \mathbb{Z}$ donc en multipliant par 4, on a $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ ce qui impose puisque $2a \in \mathbb{Z}$ que $d(2b)^2 \in \mathbb{Z}$. Supposons que $2b$ n'est pas entier, il s'écrit $\frac{r}{s}$ avec r et s premiers entre eux et $s > 0$. Soit p un facteur premier de s, alors on a $d(2b)^2 = N \in \mathbb{Z}$ donc $dr^2 = s^2$ et en paticulier p^2 divise d car r et s sont premiers entre eux. C'est impossible car d est sans facteur carré. On a donc $2b \in \mathbb{Z}$.
On peut donc poser $a = \frac{u}{2}$ et $b = \frac{v}{2}$ avec u et v dans $\mathbb{Z}$. Les conditions précédentes se résument en $u^2 - db^2 \in 4\mathbb{Z}$.

h) Supposons que u est pair, alors $u^2 \equiv 0 \pmod 4$ donc $dv^2 \equiv 0 \pmod 4$ et comme d n'a pas de facteur carré, on a $d \equiv \pm 1 \pmod 4$ ou $d \equiv 2 \pmod 4$. Ceci impose que $v^2 \equiv 2 \pmod 4$ donc 2 divise v^2 et donc v est pair.
Supposons maintenant u impair, on a alors nécessairement $u^2 \equiv 1 \pmod 4$ donc $dv^2 \equiv 1 \pmod 4$ et v ne peut être pair (sinon $v^2 \equiv 0 \pmod 4$). Mais alors si v est impairs, on a $v^2 \equiv 1 \pmod 4$ ce qui impose dans ce cas $d \equiv 1 \pmod 4$.

i) Réciproquement si u et v sont pair ou s'ils sont tous les deux impairs et que $d \equiv 1 \pmod 4$, on a toujours $u^2 - dv^2 \in 4\mathbb{Z}$. Ainsi l'élément

$$x = a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d}$$

est dans A si et seulement si u et v sont tous les deux pair ou s'ils sont tous les deux impairs et que $d \equiv 1 \pmod 4$.

Premier cas, si $d \not\equiv 1 \pmod 4$, alors les éléments de A sont de la forme $a + b\sqrt{d}$ avec a et b dans $\mathbb{Z}$ donc c'est exactement $\mathbb{Z}[\sqrt{d}]$.

Sinon, c'est-à-dire si $d \equiv 1 \pmod 4$, alors les éléments de A sont de la forme $a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d}$ avec u et u dans $\mathbb{Z}$. On a donc $A = \frac{1}{2}\mathbb{Z} + \frac{\sqrt{d}}{2}\mathbb{Z}$. Il reste à montrer que $A = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Il est clair que $\frac{1+\sqrt{d}}{2} \in \frac{1}{2}\mathbb{Z} + \frac{\sqrt{d}}{2}\mathbb{Z} = A$ donc on a l'inclusion $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset A$.

Réciproquement, commençons par remarquer que 1 et $\sqrt{d} = 2\frac{1+\sqrt{d}}{2} - 1$ sont dans $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ donc $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Soit maintenant $x = \frac{u}{2} + \frac{v}{2}\sqrt{d} \in A$. Si u et v sont pairs, alors $x \in \mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Sinon u et v sont impairs et $x + \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ et on a encore $x \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

2 Anneaux et idéaux

Exercice 7. 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. a) 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 $x \in I \cap J$.

b) 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 $x \in (I \cdot J) + (I \cdot L)$.

c) 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 $x \in I \cdot (J + L)$.

d) Il s'agit de montrer la réciproque de (m) 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

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

e) Par (m) 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 $x \in J + (I \cap L)$.

f) 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 8. Soient I et J deux idéaux d'un anneau A. On suppose que $I + J = A$ (deux tels idéaux sont dits comaximaux).

a) Montrer que $IJ = I \cap J$.

b) Montrer que $A \to A/I \times A/J$ est surjectif de noyau $I \cap J$.

c) Généraliser au cas de n idéaux comaximaux deux à deux.

Exercice 9. 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. Comme $I + J = A$, il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. En élevant à la puissance $2n$, on a alors

$$1 = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k}.$$

Cependant, si $k \in [0, n]$, alors $k \leq n$ donc $x^k \in I^n$ et si $k > n$, alors $2n - k \leq n$ donc $y^{2n-k} \in J^n$. Ainsi $1 \in I^n + J^n$ donc $I^n + J^n = A$.

Exercice 10. (ı) 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 $L \subset J$. "
(ıı) Soit $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers dont aucun n'est contenu dans l'autre. Montrer que $(\mathfrak{p} : \mathfrak{q}) = \mathfrak{p}$ et $(\mathfrak{q} : \mathfrak{p}) = \mathfrak{q}$. Donner un exemple de deux idéaux premiers dans $k[X, Y]$, où k est un corps, dont aucun n'est contenu dans l'autre et qui ne sont pas comaximaux.
(ıı) Soit a un élément non diviseur de 0 d'un anneau A. Montrer que si (a) est premier, la relation $(a) = I \cdot J$ pour deux idéaux I et J, entraine $I = A$ où $J = A$.
Indice : Commencer par montrer que $I = (a)$ ou $J = (a)$.

Solution. (ı) Soit $x \in I$ et soit $y \in J$, on a $xy \in I$ donc $I \subset (I : J)$. Réciproquement, soit $z \in (I : J)$. On sait que I et J sont comaximaux donc $I + J = A$ et en particulier, il existe $x \in I$ et $y \in J$ tels que $1 = x + y$. Mais alors comme $z \in (I : J)$, on a $zy \in I$. On a donc $z = zx + zy$ avec $zy \in I$ et $zx \in I$ car $x \in I$. Ainsi $z \in I$ et $(I : J) \subset I$, d'où l'égalité.
Soit L tel que $I \cdot L \subset J$. Soit $z \in L$, on réutilise les $x \in I$ et $y \in J$ tels que $x + y = 1$. On a alors $z = xz + yz$ or $xz \in I \cdot L \subset J$ et $yz \in J$ car $y \in J$. Ainsi $z \in J$.
(ıı) Comme précedement, on a $\mathfrak{p} \subset (\mathfrak{p} : \mathfrak{q})$. Soit $x \in (\mathfrak{p} : \mathfrak{q})$, et soit $y \in \mathfrak{q}$ tel que $y \notin \mathfrak{p}$ (ce qui est possible par hypothèse). On a alors $xy \in \mathfrak{p}$ et comme $\mathfrak{p}$ est premier, $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Comme $y \notin \mathfrak{p}$ c'est que $x \in \mathfrak{p}$ donc $(\mathfrak{p} : \mathfrak{q}) \subset \mathfrak{p}$, d'où l'égalité. De manière symétrique on a l'égalité $\mathfrak{q} = (\mathfrak{q} : \mathfrak{p})$.
Le premier exemple de l'exercice précédent convient : $\mathfrak{p} = (X)$ et $\mathfrak{q} = (Y)$. Alors $\mathfrak{p}$ et $\mathfrak{q}$ sont premiers, $\mathfrak{p} \cdot \mathfrak{q} = (XY) = \mathfrak{p} \cap \mathfrak{q}$ et $\mathfrak{p} + \mathfrak{q} = (X, Y) \subsetneq A$.
(ıı) Si $(a) = I \cdot J$, alors on peut écrire $a = \sum x_i y_i$ avec $x_i \in I$ et $y_i \in J$. Ainsi $a \in I$ et $a \in J$. Supposons que $I \not\subset (a)$ et $J \not\subset (a)$, soit alors $x \in I$ avec $x \notin (a)$ et $y \in J$ avec $y \notin (a)$. On a alors $xy \in I \cdot J = (a)$ ce qui est absurde car (a) est premier. Ainsi $I = (a)$ ou $J = (a)$. Disons par exemple que $I = (a)$ (l'autre cas est symétrique).
Dans l'écriture $a = \sum x_i y_i$ on a alors $x_i \in I = (a)$ donc $x_i = a x_i'$. On a donc $a = \sum a x_i' y_i$ et comme A est intègre $1 = \sum x_i' y_i \in J$, donc $J = A$.

Exercice 11. 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 :
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 $I + J = (X, Y) \subsetneq A$.
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

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

où α 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 $I + I = I \subsetneq A$.
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

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

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

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 $x \in A$ un élément non nul. Il faut montrer que x est inversible. Considérons la suite d'idéaux $(x) \supset (x^2) \supset \cdots \supset (x^n) \cdots$, il y en a une infinité et comme A n'a qu'un nombre fini d'idéaux, deux d'entre eux (au moins) sont égaux, disons $(x^n) = (x^m)$ avec $m > n \geq 1$. Il existe donc $a \in A$ tel que $x^n = ax^m$. On a donc $x^n(1 - ax^{m-n}) = 0$. Comme A est intègre et $x \neq 0$, on a $1 - ax^{m-n} = 0$. Mais alors on a $x \cdot ax^{m-n-1} = 1$ donc x est inversible (remarquons que $m - n - 1 \geq 0$).

Exercice 13. Soit $A = A_1 \times \cdots \times A_n$ un produit d'anneaux et soit I un idéal de A.
(i) Montrer que I est égal à un produit d'idéaux $I_1 \times \cdots \times I_n$.
(ii) Déterminer les idéaux premiers et maximaux de A.
(iii) 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 $(a_1x_1, a_2x_2) \in I$ et donc $a_1x_1 \in I_1$. 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 14. Soit A l'anneau des fonctions continues à valeur réelles sur un espace topologique compact K.

a) Soit I un idéal strict de A. Montrer qu'il existe $x \in K$ tel que pour tout $f \in I$, on ait $f(x) = 0$.

b) Déterminer les idéaux maximaux de A.

Solution. a) Supposons que pour tout $x \in K$, il existe $f \in I$ telle que $f(x) \neq 0$. On a alors

$$\bigcap_{f \in I} f^{-1}(0) = \emptyset.$$

Les complémentaires notés U_f des fermés $f^{-1}(0)$ sont ouverts et vérifient :

$$\bigcup_{f \in I} U_f = K.$$

Comme K est compact, on peut extraire un sous-recouvrement fini de ce recouvrement, il existe donc des éléments $f_1, \cdots, f_n$ de I tels que

$$\bigcup_{i=1}^{n} U_{f_i} = K.$$

Posons alors

$$f(x) = \sum_{i=1}^{n} f_i^2(x).$$

Pour tout $x \in K$, il existe i tel que $x \in U_{f_i}$ et donc $f_i(x) \neq 0$, ainsi pour tout $x \in K$, on a $f(x) > 0$. Mais alors f est inversible donc $I = A$, c'est absurde.

b) Soit $x \in K$, et considérons $I_x = \{f \in A \ / \ f(x) = 0\}$. Montrons que I_x est maximal. On a le morphisme $\varphi_x : A \to \mathbb{R}$ défini par $\varphi(f) = f(x)$. Ce morphisme est surjectif et son noyau est exactement I_x. Ainsi $A/I_x = \mathbb{R}$ qui est un corps donc I_x est maximal.

Réciproquement, soit I un idéal maximal. On a vu qu'il existe $x \in K$ tel que pour tout $f \in I$, on a $f(x) = 0$. Ainsi $I \subset I_x$. Mais comme I est maximal, on a nécessairement $I = I_x$.

Les idéaux maximaux sont donc les I_x pour $x \in K$. Enfin, remarquons que si $x \neq y$, alors $I_x \neq I_y$. En effet, il existe toujours $f \in A$ telle que $f(x) = 0 \neq f(y)$ (c'est le lemme de Tietze-Urysohn). Donc $K \simeq \text{Specmax}(A)$. De plus la topologie de K correspond à la topologie de Zariski de $\text{Specmax}(A)$.

Exercice 15. 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. a) Soit φ un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbb{R}$, on a

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1.$$

Ainsi $\varphi(i) \in \mathbb{R}$ et $\varphi(i)^2 = -1$. C'est impossible.

b) Soit φ un morphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{Q}$, on a

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

Ainsi $\varphi(\sqrt{2}) \in \mathbb{Q}$ et $\varphi(\sqrt{2})^2 = 2$. C'est impossible car $\sqrt{2}$ et $-\sqrt{2}$ ne sont pas rationnels.

c) Soit φ un morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Z}$, on a

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

Ainsi $\varphi(\frac{1}{2}) \in \mathbb{Z}$ et $2\varphi(\frac{1}{2}) = 1$. C'est impossible.

d) Soit φ 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

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

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

Exercice 16. 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 φ 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

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

Ainsi pour que φ 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 φ de $\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ tel que $\varphi(n) = \overline{0}$. Cependant on a nécessairement $\varphi(1) = \overline{1}$ donc $\varphi(n) = \overline{0} \Leftrightarrow \overline{n} = \overline{0}$ ce qui est équivalent au fait que m divise n. Par ailleurs le morphisme est unique car $\varphi(x) = \overline{x}$ pour tout $x \in \mathbb{Z}$.

Exercice 17. 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 18. 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 19. Soit A un anneau, $B = A[X]$ l'anneau des polynômes à coefficients dans A et $f = \sum_{i=0}^{n} a_i X^i$ un élément de B. Prouver les assertions suivantes :

a) f est nilpotent si et seulement si $a_0, \ldots, a_n$ sont nilpotents.

b) f est une unité de B si et seulement si a_0 est une unité de A et $a_1, \ldots, a_n$ sont nilpotents.
Indice : si $f^{-1} = g = \sum_{j=0}^{m} b_j X^j$ montrer par récurrence sur i que $a_n^{i+1} b_{m-i} = 0$.

c) f est diviseur de zéro si et seulement si $\exists a \in A$ tel que $a \neq 0$ et $af = 0$.
Indice : montrer que si $f \cdot g = 0$ avec $\deg(g)$ minimal alors $a_i . g = 0$ $\forall i$.

Solution. a) Si f est nilpotent, alors il existe $k \in \mathbb{N}$ tel que $f^k = 0$. Mais alors le terme dominant de f^k est a_n^k donc $a_n^k = 0$ et a_n nilpotent. Alors $f - a_n X^n$ est nilpotent et par récurrence sur le degré, tous les a_i sont nilpotents.

Réciproquement, si tous les a_i sont nilpotents, alors pour tout i, on a $a_i X^i$ est nilpotent donc f est somme de nilpotents donc est nilpotent.

b) Si a_0 est une unité de A et $a_1, \ldots, a_n$ sont nilpotents, alors $f = u - n$ où u est une unité et n est nilpotent. Alors f est inversible. En effet, il existe $k \in \mathbb{N}$ tel que $n^k = 0$, alors on a

$$(u - n)(u^{k-1} + u^{k-2}n + \cdots + un^{k-2} + n^{k-1}) = u^k - n^k = u^k.$$

Ainsi on a $(u - n)(u^{k-1} + u^{k-2}n + \cdots + un^{k-2} + n^{k-1})(u^{-1})^k = 1$ donc $u - n$ est inversible.
Réciproquement, si f est une unité, alors écrivons $f^{-1} = g = \sum_{j=0}^{m} b_j X^j$. On a

$$1 = fg = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j X^{i+j} = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j X^k.$$

Ainsi

$$\sum_{i+j=k} a_i b_j = 0 \quad \text{pour} \quad k \neq 0 \quad \text{et} \quad a_0 b_0 = 1,$$

ce qui prouve déjà que a_0 est inversible.
Si $n = 0$, on a fini. Sinon, montrons par récurrence sur k que $a_n^{k+1} b_{m-k} = 0$ pour $k \leq m$. Comme $n > 0$, on a $m + n > 0$ et $a_n b_m = 0$ ce qui prouve le cas $k = 0$.
Supposons que $a_n^{l+1} b_{m-l} = 0$ pour $l < k$, on a $m + n - k \geq n > 0$ donc $\sum_{i+j=m+n-k} a_i b_j = 0$ et en multipliant par a_n^k on a

$$0 = \sum_{i+j=m+n-k} a_i a_n^k b_j = a_n^{k+1} b_{m-k} + \sum_{i<n} a_i a_n^{n-1-i} \underbrace{a_n^{k+i-n+1} b_{m+n-k-i}}_{\text{nul par hyp. de récurrence}} = a_n^{k+1} b_{m-k}.$$

Pour $k = m$, on a $a_n^m b_0 = 0$ mais $a_0 b_0 = 1$ donc on en déduit $a_n^m = 0$ et a_n est nilpotent.
On a donc $f - a_n X^n$ encore inversible (car on l'a vu inversible + nilpotent = inversible) et par récurrence on en déduit que tous les a_i avec $i > 0$ sont nilpotents.

c) Si il existe $0 \neq a \in A$ tel que $af = 0$ alors f est évidement diviseur de 0.
Réciproquement, si f est diviseur de 0, alors il existe $0 \neq g \in A[X]$ tel que $fg = 0$. Prenons un tel g de degré minimal, on écrit $g = \sum_{j=0}^{m} b_j X^j$, si $m = 0$ c'est fini. Sinon, commençons par montrer que pour tout k, on a $a_k g = 0$.
L'assertion est vraie pour $k > n$. Supposons qu'elle est vraie pour tout $l > k$. Alors,

$$0 = fg = (a_0 + \cdots + a_n X^n)g = (a_0 + \cdots a_k X^k)g$$

et le coefficient dominant est $a_k b_m$ donc $a_k b_m = 0$. Mais alors $a_k g = \sum_{j=0}^{m-1} a_k b_j X^j$ est de degré inférieur à $m - 1$ et $f \cdot (a_k g) = 0$. Par minimalité du degré de g ceci impose que $a_k g = 0$.
Mais alors tous les produits $a_k b_l$ sont nuls. En particulier $b_l f = 0$ pour tout l et comme $g \neq 0$ l'un au moins de b_l est non nul ce qui prouve le résultat.

Exercice 20. Soit k un corps et A l'anneau quotient de $k[X,Y]$ par l'idéal engendré par X^2+5Y^2. L'anneau A est-il :

a) intègre ?

b) réduit ?

c) factoriel ?

Donner éventuellement des conditions sur k.

Solution. a) L'anneau A est intègre si et seulement si l'idéal (X^2+5Y^2) est premier. C'est le cas si et seulement si X^2+5Y^2 est irréductible. Ce polynômes est irréductible si et seulement si l'équation $x^2=-5$ n'a pas de solution dans k (c'est par exemple le cas sur $\mathbb{R}$ mais pas sur $\mathbb{C}$).

b) Remarquons tout d'abord que si A est intègre, alors il est réduit. Ainsi on peut se placer dans le cas A non intègre c'est-à-dire dans le cas où k contient $\sqrt{-5}$ et $-\sqrt{-5}$.
L'anneau A est réduit s'il n'existe pas d'élément $P\in k[X,Y]$ tel que $Cl(P)\in A$ est nilpotent (c'est-à-dire il exite $n\geq 2$ tel que $Cl(P)^n=0$). Si c'était le cas alors on aurait X^2+5Y^2 divise P^n. Ceci signifie donc que $(X+\sqrt{-5}Y)(X-\sqrt{-5}Y)$ divise P^n donc comme $X+\sqrt{-5}Y$ et $X-\sqrt{-5}Y$ sont irréductibles, ils divisent P.
Si $X+\sqrt{-5}Y$ et $X-\sqrt{-5}Y$ sont distincts, alors les deux divisent P donc leur produit divise P donc X^2+5Y^2 divise P et $Cl(P)=0$. Dans ce cas A est réduit.
Il reste le cas où $X+\sqrt{-5}Y=X-\sqrt{-5}Y$, c'est-à-dire $\sqrt{-5}=-\sqrt{-5}$ ou encore $2\sqrt{-5}=0$. Comme k est un corps, ceci n'arrive que si $2=0$ ou $\sqrt{-5}=0$ donc $5=0$. Ainsi si le corps k est de caractéristique 2 ou 5 (dans les deux cas $\sqrt{-5}$ existe), on a $X+\sqrt{-5}Y=X-\sqrt{-5}Y$ et $Cl(X+\sqrt{-5}Y)\neq 0$ alors que $Cl(X+\sqrt{-5}Y)^2=Cl(X^2+5Y^2)=0$. Dans ce cas A n'est pas réduit.

c) Un anneau factoriel étant intègre, on peut supposer que -5 n'est pas un carré dans k.
Il nous suffit montrer qu'il existe un élément irréductible u tel que $A/(u)$ n'est pas intègre. Prenons $u=y$ (la classe de Y dans A). On a alors $A/(y)=k[X,Y]/(X^2+5Y^2,Y)=k[X]/(X^2)$ qui n'est pas intègre. Il reste donc à montrer que y est irréductible.
Soient donc P_1 et P_2 dans $k[X,Y]$ tels que leurs classes p_1 et p_2 vérifient $y=p_1p_2$. Il faut montrer que l'un des p_i est inversible. La division euclidienne par X^2+5Y^2 permet de supposer que P_1 et P_2 sont de la forme $P_i=A_i(X)+YB_i(X)$ avec A_i et B_i des polynômes en X. On a alors

$$\begin{aligned}P_1(x,y)P_2(x,y)-y &= A_1(x)A_2(x)+(A_1(x)B_2(x)+A_2(x)B_1(x))y+B_1(x)B_2(x)y^2-y\\ &= (A_1(x)A_2(x)-\frac{1}{5}B_1(x)B_2(x)x^2)+(A_1(x)B_2(x)+A_2(x)B_1(x)-1)y.\end{aligned}$$

Ce terme doit être nul donc en relevant dans $k[X,Y]$ il est encore nul car le degré en Y est au plus 1 et qu'il doit être multiple de X^2+5Y^2.
On a donc les équations

$$5A_1A_2=B_1B_2X^2,\qquad \text{et}\qquad A_1B_2+A_2B_1=1.$$

On peut supposer qu'aucun de ces polynômes n'est nul : si par exemple A_1 est nul, alors l'un des B_i l'est aussi. Ce n'est pas B_1 d'après la seconde equation donc $B_2=0$. Mais alors on a $A_2B_1=1$ et $P_2=A_2$ est inversible.
Le polynômes X divise l'un des A_i. Si il divisait les deux alors il diviserait 1 ce qui est impossible. On peut donc supposer par exemple que X divise A_2 et pas A_1. On a alors $A_2=X^2A_2'$ et les équations :

$$5A_1A_2'=B_1B_2,\qquad \text{et}\qquad A_1B_2+X^2A_2'B_1=1.$$

Soit P un polynômes irréductible divisant A_1, alors P divise l'un des B_i. Ce n'est pas B_1 car sinon P diviserait 1 donc P divise B_2. De même si P divise B_2 il divise nécessairement A_1. Les polynômes A_1 et B_2 sont donc proportionnels. Il en va de même de A_2' et B_1. Il existe donc a et b dans k tels que $B_1=aA_2'$ et $B_2=bA_1$.
Les équiations précédentes deviennent

$$5=ab,\quad \text{et}\quad bA_1^2+\frac{1}{a}X^2B_1^2=1,$$

ce qui donne $5A_1^2+X^2B_1^2=a$. Mais alors on a la relation

$$5(A_1(x)+B_1(x)y)(A_1(x)-B_1(x)y)=5A_1(x)^2-5y^2B_1(x)^2=5A_1^2+X^2B_1^2=a$$

qui prouve que p_1 est inversible.

Exercice 21. 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 22. 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 23. Déterminer tous les idéaux premiers de :
(i) $\mathbb{C}[X]$,
(ii) $\mathbb{R}[X]/(X^2 + X + 1)$,
(iii) $\mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6)$,
(iv) $\mathbb{R}[X]/(X^4 - 1)$.
(v) Déterminer tous les morphismes de $\mathbb{R}$-algèbre de ces anneaux dans $\mathbb{R}$ et $\mathbb{C}$.

Solution. Rappelons les résultats suivants :
• si k est un corps, les idéaux premiers de $k[X]$ sont les (P) avec P irréductible. En effet, soit (P) un idéal premier (rappelons que $k[X]$ est euclidien donc principal ainsi tout idéal est de la forme (P)), si $P = P_1P_2$, alors $\overline{P}_1\overline{P}_2 = 0$ dans $k[X]/(P)$. Ceci impose comme (P) est premier que $\overline{P_1} = 0$ ou $\overline{P_2} = 0$ et donc P_1 ou P_2 est multiple de P, l'autre polynôme est donc constant. Ainsi P est irréductible.
Réciproquement, si P est irréductible et que P_1 et P_2 sont deux éléments de $k[X]$ tels que $\overline{P}_1\overline{P}_2 = 0$ dans $k[X]/(P)$, alors P divise le produit P_1P_2 et comme P est irréductible, il divise l'un ou l'autre c'est-à-dire $\overline{P_1} = 0$ ou $\overline{P_2} = 0$ donc (P) est premier.
• Si A est un anneau et I un idéal et soit $\pi : A \to A/I$. Les idéaux premiers de A/I sont en bijection (définie par $J \mapsto \pi(J)$ et de bijection réciproque $\overline{J} \mapsto \pi^{-1}(\overline{J})$) avec les idéaux premiers de A contenant I (cf. exercice précédent).

Nous pouvons maintenant résoudre l'exercice.

(i) Les idéaux premiers de $\mathbb{C}[X]$ sont les (P) avec P irréductible. Or sur $\mathbb{C}$ qui est algébriquement clos, les polynômes irréductibles sont les $X - a$ avec $a \in \mathbb{C}$. Les idéaux premiers de $\mathbb{C}[X]$ sont donc les $(X - a)$ avec $a \in \mathbb{C}$.

(ii) Les idéaux premiers de $\mathbb{R}[X]/(X^2+X+1)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent (X^2+X+1). Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^2+X+1)\subset(P)$ alors P divise X^2+X+1. Comme X^2+X+1 est irréductible, ceci impose que $P=a(X^2+X+1)$ avec $0\neq a\in\mathbb{R}$. Ainsi il y a un unique idéal premier contenant (X^2+X+1) c'est (X^2+X+1) lui-même. L'anneau $\mathbb{R}[X]/(X^2+X+1)$ a donc un unique idéal premier : (0).
(iii) Les idéaux premiers de $\mathbb{R}[X]/(X^3-6X^2+11X-6)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent $(X^3-6X^2+11X-6)$. Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^3-6X^2+11X-6)\subset(P)$ alors P divise le polynôme $X^3-6X^2+11X-6$. On écrit la décomposition de $X^3-6X^2+11X-6$ dans $\mathbb{R}[X]$:

$$X^3-6X^2+11X-6=(X-1)(X^2-5X+6)=(X-1)(X-2)(X-3).$$

Les polynômes irréductibles qui divisent $X^3-6X^2+11X-6$ sont donc $X-1$, $X-2$ et $X-3$. Il y a donc trois idéaux premiers dans $\mathbb{R}[X]/(X^3-6X^2+11X-6)$ qui sont $(X-1)/(X^3-6X^2+11X-6)$, $(X-2)/(X^3-6X^2+11X-6)$ et $(X-3)/(X^3-6X^2+11X-6)$.
(iv) Les idéaux premiers de $\mathbb{R}[X]/(X^4-1)$ sont en bijection avec les idéaux premiers de $\mathbb{R}[X]$ qui contiennent (X^4). Les idéaux premiers de $\mathbb{R}[X]$ sont les (P) avec P irréductible. Si de plus on a $(X^4-1)\subset(P)$ alors P divise le polynôme X^4-1. On écrit la décomposition de X^4-1 dans $\mathbb{R}[X]$:

$$X^4-1=(X-1)(X+1)(X^2+1).$$

Les polynômes irréductibles qui divisent X^4-1 sont donc $X-1$, $X+1$ et X^2+1. Il y a donc trois idéaux premiers dans $\mathbb{R}[X]/(X^4-1)$ qui sont $(X-1)/(X^4-1)$, $(X+1)/(X^4-1)$ et $(X^2+1)/(X^4-1)$.
(v) Cas (i) : soit $\varphi:\mathbb{C}[X]\to\mathbb{C}$ un morphisme de $\mathbb{R}$-algèbres, on a

$$\varphi(i)^2=\varphi(i^2)=\varphi(-1)=-\varphi(1)=-1,$$

donc $\varphi(i)=\pm i$. Soit $\alpha\in\mathbb{C}$ l'image de X et soit $P\in\mathbb{C}[X]$ avec $P=\sum a_nX^n+i\sum b_nX^n$ où a_n et b_n sont dans $\mathbb{R}$, on a :

$$\varphi(P)=\sum a_n\alpha^n+\varphi(i)\sum b_n\alpha^n.$$

Ainsi si $\varphi(i)=i$, alors $\varphi(P)=P(\alpha)$ et si $\varphi(i)=-i$, alors $\varphi(P)=\overline{P}(\alpha)$. Aucun de ces morphismes n'a son image contenue dans $\mathbb{R}$.
Cas (ii) : les morphismes φ de $\mathbb{R}$-algèbre de $\mathbb{R}[X]/(X^2+X+1)$ dans $\mathbb{C}$ sont les morphismes φ de $\mathbb{R}$-algèbre de $\mathbb{R}[X]$ dans $\mathbb{C}$ qui envoient X^2+X+1 sur 0. Le raisonnement précédent montre que $\varphi(P)=P(\alpha)$ pour un certain $\alpha=\varphi(X)$ (ici il n'y a pas le problème avec i). Par ailleurs, il faut que $0=\varphi(X^2+X+1)=\alpha^2+\alpha+1$. On a donc $\alpha=j$ ou $\alpha=j^2$. Il y a donc deux morphismes dans $\mathbb{C}$ donnés par $\varphi(P)=P(j)$ et $\varphi(P)=P(j^2)$. Aucun de ces morphismes n'a son image contenue dans $\mathbb{R}$.
Cas (iii) : le même raisonnement montre que les morphismes de $\mathbb{R}$-algèbre dans $\mathbb{C}$ sont donnés par $\varphi(P)=P(1)$, $\varphi(P)=P(2)$ ou $\varphi(P)=P(3)$. Tous ces morphismes sont à valeurs dans $\mathbb{R}$.
Cas (iv) : cette fois-ci les morphismes de $\mathbb{R}$-algèbre dans $\mathbb{C}$ sont donnés par $\varphi(P)=P(1)$, $\varphi(P)=P(-1)$, $\varphi(P)=P(i)$ ou $\varphi(P)=P(-i)$. Les deux premiers sont à valeurs dans $\mathbb{R}$ et pas les deux derniers.

Exercice 24. 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 25. 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 26. 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

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

Solution. Soient $a \in A$ et $x \in$ nil(A), alors il existe $n \in \mathbb{N}$ tel que $x^n = 0$, mais alors $(ax)^n = a^n x^n = 0$ donc $ax \in$ 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 $x + y \in$ nil(A).
(ii) Soit $\mathfrak{p}$ un idéal premier et $x \in$ 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 nil(A) $\subset \mathfrak{p}$ donc

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

Réciproquement, soit $s \notin$ 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 27. 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.

Exercice 28. Montrer que l'anneau $\dfrac{\mathbb{C}[X,Y]}{(Y-X^2)}$ est principal.

Solution. On montre que $\mathbb{C}[X,Y]/(Y-X^2)$ est isomorphe à $\mathbb{C}[X]$. En effet, introduisons le morhisme d'anneaux : $\varphi : \mathbb{C}[X,Y] \to \mathbb{C}[X]$ défini par $\varphi(P) = P(X,X^2)$. Il est clair que φ est surjectif. On a $\varphi(Y-X^2) = X^2 - X^2 = 0$ donc $Y - X^2 \in \ker\varphi$. Par ailleurs, si $P \in \ker\varphi$ on peut effectuer la division euclidienne de P par $Y - X^2$ car le coefficient dominant de $Y - X^2$ dans $\mathbb{C}[X][Y]$ est égal à 1 donc inversible. On a ainsi $P(X,Y) = (Y-X^2)Q(X,Y) + R(X,Y)$ où $R(X,Y)$ est un polynôme de $\mathbb{C}[X][Y]$ de degré en Y strictement inférieur à celui de $Y - X^2$, c'est-à-dire de degré nul. Donc $R(X,Y)$ est un polynôme en X uniquement. On a donc

$$0 = \varphi(P) = \varphi(Y-X^2)\varphi(Q) + \varphi(R) = \varphi(R).$$

Mais $\varphi(R) = R(X,X^2) = R(X)$ donc $R = 0$ et $P \in (Y-X^2)$. On a donc $\ker\varphi = (Y-X^2)$ ce qui nous donne un isomorphisme

$$\overline{\varphi} : \mathbb{C}[X,Y]/(Y-X^2) \to \mathbb{C}[X].$$

Comme $\mathbb{C}[X]$ est principal, $\mathbb{C}[X,Y]/(Y-X^2)$ l'est aussi.

Exercice 29. "Soit $A = \dfrac{\mathbb{C}[X,Y]}{(XY-1)}$; on pose " $x = Cl(X)$.

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) Si $y = Cl(Y)$, on a $xy = 1$ donc x est inversible d'inverse y (en particulier $y = x^{-1}$. Soit $a \in A$, on peut écrire

$$a = \sum_{i,j} \alpha_{i,j} x^i y^j = \sum_{i,j} \alpha_{i,j} x^i x^{-j} = \sum_{i,j} \alpha_{i,j} x^{i-j} = \sum_k \beta_k x^k,$$

où $\beta_k = \sum_j \alpha_{j+k,j}$. Soit m le plus petit entier tel que $\beta_m \neq 0$ (il existe car il n'y a qu'un nombre fini de $\alpha_{i,j}$ non nuls) et soit $P(X) = \sum_{k\geq 0} \beta_{k+m} X^k$. On a bien $a = x^m P(x)$ et $P(0) = \beta_m \neq 0$. Il reste à voir que cette écriture est unique. Si on a deux telles écriture $x^m P(x) = a = x^n Q(x)$ avec disons $m \leq n$, alors on a $x^m(P(x) - x^{n-m}Q(x)) = 0$ et comme x est inversible on a $P(x) - x^{n-m}Q(x) = 0$. Ceci signifie que $XY - 1$ divise $P(X) - X^{n-m}Q(X)$ et comme ce dernier polynôme est de degré 0 en Y ceci impose que $P(X) - X^{n-m}Q(X) = 0$. On a donc $P(X) = X^{n-m}Q(X)$ et $P(0) \neq 0$. Ceci impose que $n = m$ et on a alors $P = Q$.

b) Si $a = 0$, on choisit $q = r = 0$. Sinon, écrivons $a = x^m A(x)$ et $b = x^n B(x)$ où A et B sont des polynômes tels que $A(0) \neq 0$ et $B(0) \neq 0$. Effectuons la division euclidienne de A par B : il existe Q et R deux polynômes tels que $R = 0$ ou $\deg R < \deg B$ tels que $A = BQ + R$. Mais alors on a

$$a = x^m A(x) = x^m B(x)Q(x) + x^m R(x) = x^n B(x) x^{n-m} Q(x) + x^m R(x).$$

On pose alors $q = x^{n-m}Q(x)$ et $r = x^m R(x)$ et on a $a = bq + r$. Si $R = 0$, on a $r = 0$ ce qui convient. Si $R(0) \neq 0$, alors $e(r) = \deg R < \deg B = e(b)$. Si enfin $R(0) = 0$, alors il existe $k > 0$ tel que $R(X) = X^k U(X)$ avec $U(0) \neq 0$. On a alors $r = x^{m+k}U(x)$ et

$$e(r) = \deg U = \deg R - k < \deg R < \deg B = e(b).$$

c) Soit I un idéal, si $I = (0)$, alors I est principal, sinon soit $b \in I$ tel que $e(b)$ soit minimal. Soit maintenant $a \in I$, on a $a = bq + r$ avec $r = 0$ ou $e(r) < e(b)$. Comme a et b sont dans I, on a $r \in I$. Comme $e(b)$ est minimal, on a nécessairement $r = 0$ donc $a = bq \in (b)$ donc $I = (b)$.

Exercice 30. Soit k un corps et $A = k[X,Y]/(X^2, XY, Y^2)$.
(ı) Déterminer les éléments inversibles de A.
(ıı) Déterminer tous les idéaux principaux de A.
(ıı) Déterminer tous les idéaux de A.

Solution. (i) Soient x et y les images de X et Y dans A. On a $x^2 = xy = y^2$, ainsi tou élément de A s'écrit sous la forme $a + bx + cy$ avec a, b et c dans k. Cet élément est inversible si et seulement s'il existe a', b' et c' dans k tels que

$$(a + bx + cy)(a' + b'x + c'y) = 1$$

c'est-à-dire

$$aa' + (ab' + a'b)x + (ac' + a'c)y = 1.$$

Ceci impose que l'on ait $aa' = 1$, $ab' + a'b = 0$ et $ac' + a'c = 0$. Ce système a une solution si et seulement si $a \neq 0$, la solution est alors $a' = \frac{1}{a}$, $b' = -\frac{b}{a^2}$ et $c' = -\frac{c}{a^2}$. Ainsi $a+bx+cy$ est inversible si et seulement si $a \neq 0$.
(ii) Soit I un idéal principal de A. Si $I = A$, alors I est engendré par un élément inversible quelconque. Supposons $I \neq A$, alors I est engendré par un élément non inversible donc de la forme $bx + cy$. Il reste à déterminer à quelle condition deux éléments $bx + cy$ et $b'x + c'y$ définissent le même idéal c'est-à-dire à quelle condition ils diffèrent par multiplication par un inversible.
On cherche donc $\alpha + \beta x + \gamma y$ tel que $\alpha \neq 0$ et $(\alpha + \beta x + \gamma y)(bx + cy) = b'x + c'y$. Ceci nous donne $\alpha b = b'$ et $\alpha c = c'$, c'est-à-dire les couple (b, c) et (b', c') sont proportionnels. Ainsi, on voit que si $b \neq 0$, on peut supposer $b = 1$ et on a $c \in k$ quelconque. Si par contre $b = 0$ et $c \neq 0$, on peut supposer $c = 1$ et on a le couple $(0, 1)$, enfin il y a le couple $(0, 0)$. Les idéaux principaux de A sont donc A, $(x + cy)$, (y) et (0).
(iii) Soit I un idéal non principal de A. Alors I est engendré par deux éléments qui sont de la forme $ax + by$ et $cx + dy$ (ils ne peuvent être inversibles sinon $I = A$ est principal) et non proportionnels. Ainsi les vecteurs (a, b) et (c, d) engendrent tout k^2 c'est-à-dire que $ax + by$ et $cx + dy$ engendrent tous les termes de la forme $\alpha x + \beta y$. L'idéal I contient donc l'idéal (x, y). Or $A/(x, y) \simeq k$ donc (x, y) est maximal. Comme $I \neq A$, on a $I = (x, y)$ qui est le seul idéal non principal de A.

Exercice 31. *Soit A un anneau intègre et $\mathfrak{p}$ un idéal premier principal non nul. Soit I un idéal principal de A contenant $\mathfrak{p}$. Montrer que $I = \mathfrak{p}$ ou $I = A$.*

Solution. On écrit $\mathfrak{p} = (a)$ avec $a \neq 0$ et $I = (b)$. Comme $I \supset \mathfrak{p}$, alors b divise a, c'est-à-dire $a = ub$. Comme $\mathfrak{p}$ est premier ceci impose que $b \in (a)$ ou $u \in (a)$. Dans le premier cas on a $I = \mathfrak{p}$. Dans le second cas $u = ax$ donc $a = axb$ et comme $a \neq 0$ et A intègre on a $1 = xb$ donc b est inversible et $I = A$. Cet exercice est une autre forme du premier exercice du paragraphe.

Exercice 32. Montrer qu'il n'existe pas d'homomorphisme d'anneaux de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{3}]$.

Solution. Tout élément de $\mathbb{Z}[\sqrt{2}]$ s'écrit de manière unique sous la forme $a + b\sqrt{2}$ avec a et b dans $\mathbb{Z}$ (l'unicité résulte du fait que $\sqrt{2} \notin \mathbb{Q}$).
De même tout élément de $\mathbb{Z}[\sqrt{3}]$ s'écrit de manière unique sous la forme $a + b\sqrt{3}$ avec a et b dans $\mathbb{Z}$ (l'unicité résulte du fait que $\sqrt{3} \notin \mathbb{Q}$).
Soit maintenant $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ un morphisme d'anneaux, alors $\varphi'\sqrt{2}) = a + b\sqrt{3}$ avec a et b dans $\mathbb{Z}$. Mais alors on a

$$\varphi(2) = \varphi(\sqrt{2}^{\,2}) = \varphi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Par ailleurs, on a $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$. Ainsi on doit avoir l'égalité

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2.$$

Ceci impose $a^2 + 3b^2 = 2$ et $2ab = 0$. On a donc $a = 0$ ou $b = 0$. Si $a = 0$, alors $3b^2 = 2$ ce qui est impossible (on a pas $b = 0$ et si $b \geq 1$, alors $3b^2 > 2$). Si $b = 0$, alors $a^2 = 2$ qui n'a pas de solution dans $\mathbb{Z}$ car $\sqrt{2} \notin \mathbb{Q}$.

Exercice 33. Soit $f : A \to B$ un homomorphisme d'anneaux. Pour tout idéal I de A on note $f_*(I)$ l'idéal de B engendré par $f(I)$ et on l'appelle extension de I dans B. Pour tout idéal J de B on appelle contraction de J l'idéal $f^{-1}(J)$. Soit I un idéal de A et J un idéal de B. Montrer que :

a) $I \subset f^{-1}\big(f_*(I)\big)$ et $J \supset f_*\big(f^{-1}(J)\big)$,
b) $f^{-1}(J) = f^{-1}\big[f_*\big(f^{-1}(J)\big)\big]$ et $f_*(I) = f_*\big[f^{-1}\big(f_*(I)\big)\big]$.
c) Soit $\mathcal{C}$ l'ensemble des idéaux de A qui sont des contractions d'idéaux de B et $\mathcal{E}$ l'ensemble des idéaux de B qui sont des extensions d'idéaux de A. Montrer que :
d) $\mathcal{C} = \big\{I : I = f^{-1}\big(f_*(I)\big)\big\}$ et $\mathcal{E} = \big\{J : J = f_*\big(f^{-1}(J)\big)\big\}$,
e) f_* définit une bijection de $\mathcal{C}$ sur $\mathcal{E}$; quel est son inverse ?
Soient I_1 et I_2 deux idéaux de A et J_1 et J_2 deux idéaux de B. Montrer que :
f) $f_*(I_1 + I_2) = f_*(I_1) + f_*(I_2)$ et $f^{-1}(J_1 + J_2) \supset f^{-1}(J_1) + f^{-1}(J_2)$,
g) $f_*(I_1 \cap I_2) \subset f_*(I_1) \cap f_*(I_2)$ et $f^{-1}(J_1 \cap J_2) = f^{-1}(J_1) \cap f^{-1}(J_2)$,

h) $f_*(I_1 \cdot I_2) = f_*(I_1) \cdot f_*(I_2)$ et $f^{-1}(J_1 \cdot J_2) \supset f^{-1}(J_1) \cdot f^{-1}(J_2)$,

i) $f_*(I_1 : I_2) \subset (f_*(I_1) : f_*(I_2))$ et $f^{-1}(J_1 : J_2) \subset (f^{-1}(J_1) : f^{-1}(J_2))$,

j) $f_*\big(\sqrt{I}\big) \subset \sqrt{f_*(I)}$ et $f^{-1}\big(\sqrt{J}\big) = \sqrt{f^{-1}(J)}$.

Solution. a) Soit $x \in I$, alors $f(x) \in f(I) \subset f_*(I)$ et donc $x \in f^{-1}(f_*(I))$. Soit maintenant $y \in f_*(f^{-1}(J))$, alors on peut écrire $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(f^{-1}(J)) \subset J$. Mais alors $y \in J$.

b) Si on applique (ı) à $f^{-1}(J)$, on a $f^{-1}(J) \subset f^{-1}(f_*(f^{-1}(J)))$. Mais par (ı), on a aussi $f_*(f^{-1}(J)) \subset J$ donc $f^{-1}(f_*(f^{-1}(J))) \subset f^{-1}(J)$.

De même, on applique (ı) à $f_*(I)$, on a $f_*(f^{-1}(f_*(I))) \subset f_*(I)$. Mais par (ı), on a aussi $I \subset f^{-1}(f_*(I))$ donc $f_*(I) \subset f_*(f^{-1}(f_*I))$.

c) Si $I \in \mathcal{C}$, alors $I = f^{-1}(J)$, ainsi par (ıı) on a bien $I = f^{-1}(f_*I)$. Réciproquement si $I = f^{-1}(f_*I)$, alors I est la contraction de f_*I idéal de B.

Si $J \in \mathcal{E}$, alors $J = f_*I$ et par (ıı) on a bien $J = f_*(f^{-1}(J))$. Réciproquement, si on a $J = f_*(f^{-1}(J))$, alors J est l'extension de $f^{-1}(J)$ idéal de A.

d) Considérons les applications $f_* : \mathcal{C} \to \mathcal{E}$ et $f^{-1} : \mathcal{E} \to \mathcal{C}$ définies par $I \mapsto f_*I$ et $J \mapsto f^{-1}(J)$. On a alors par (ıı) : si $I \in \mathcal{C}$, alors $f^{-1}(f_*I) = I$ et si $J \in \mathcal{E}$, alors $f_*(f^{-1}(J)) = J$. Ainsi f^{-1} est la bijection réciproque de f_*.

e) Soit $y \in f_*(I_1 + I_2)$, alors $y = \sum_i b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 + I_2)$. Ainsi, on a $y_i = f(x_{i,1} + x_{i,2})$ avec $x_{i,1} \in I_1$ et $x_{i,2} \in I_2$. Mais alors on a $y = \sum b_i f(x_{i,1}) + \sum b_i f(x_{i,2})$ et donc $y \in f_*(I_1) + f_*(I_2)$.
Réciproquement, si $y \in f_*(I_1) + f_*(I_2)$, alors $y = \sum b_i f(x_{i,1}) + \sum b_i f(x_{i,2})$ avec $x_{i,1} \in I_1$ et $x_{i,2} \in I_2$. Mais alors on a $y = \sum b_i f(x_{i,1} + x_{i,2}) \in f_*(I_1 + I_2)$.
Soit $x \in f^{-1}(J_1) + f^{-1}(J_2)$, alors $x = x_1 + x_2$ avec $f(x_1) \in J_1$ et $f(x_2) \in J_2$. On a donc $f(x) = f(x_1) + f(x_2) \in J_1 + J_2$ et donc $x \in f^{-1}(J_1 + J_2)$.

f) Soit $y \in f_*(I_1 \cap I_2)$, alors $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 \cap I_2)$. On a donc $y_i \in f(I_1)$ et donc $y \in f_*(I_1)$ et de même $y_i \in f(I_2)$ et donc $y \in f_*(I_2)$.
Soit $x \in f^{-1}(J_1 \cap J_2)$, alors $f(x) \in J_1 \cap J_2$. On a donc $f(x) \in J_1$ c'est-à-dire $x \in f^{-1}(J_1)$ et de même $f(x) \in J_2$ c'est-à-dire $x \in f^{-1}(J_2)$.
Réciproquement soit $x \in f^{-1}(J_1) \cap f^{-1}(J_2)$, alors on a $f(x) \in J_1$ et $f(x) \in J_2$. On a donc $f(x) \in J_1 \cap J_2$, ainsi $x \in f^{-1}(J_1 \cap J_2)$.

g) Soit $y \in f_*(I_1 \cdot I_2)$, alors $y = \sum b_i y_i$ avec $b_i \in B$ et $y_i \in f(I_1 \cdot I_2)$ donc $y_i = f(\sum a_{i,j} c_{i,j})$ avec $a_{i,j} \in I_1$ et $c_{i,j} \in I_2$. On a donc $y = \sum_i \sum_j b_i f(a_{i,j}) f(c_{i,j})$. Mais $b_i f(a_{i,j}) \in f_*I_1$ et $f(c_{i,j}) \in f_*I_2$ donc $\sum_j b_i f(a_{i,j}) f(c_{i,j}) \in f_*I_1 \cdot f_*I_2$ et donc $y = \sum_i \sum_j b_i f(a_{i,j}) f(c_{i,j}) \in f_*I_1 \cdot f_*I_2$.
Soit $x \in f^{-1}(J_1) \cdot f^{-1}(J_2)$, alors $x = \sum a_i b_i$ avec $a_i \in f^{-1}(J_1)$ et $c_i \in f^{-1}(J_2)$. On a donc $f(x) = \sum f(a_i) f(c_i) \in J_1 \cdot J_2$.

h) Soit $y \in f_*(I_1 : I_2)$, alors $y = \sum_i b_i f(x_i)$ avec $b_i \in B$ et $x_i \in (I_1 : I_2)$ et soit $z \in f_*I_2$, on a $z = \sum_j c_j f(z_j)$ avec $c_j \in B$ et $z_j \in I_2$, on calcule alors $yz = \sum_i \sum_j b_i c_j f(x_i z_j)$ mais comme $x_i \in (I_1 : I_2)$ et $z_j \in I_2$, on a $x_i z_j \in I_1$ et donc $yz \in f_*I_1$. On a donc $y \in (f_*I_1 : f_*I_2)$.
Soit $x \in f^{-1}(J_1 : J_2)$, alors $f(x) \in (J_1 : J_2)$. Soit maintenant $z \in f^{-1}(J_2)$ c'est-à-dire $f(z) \in J_2$, on calcule $f(yz) = f(y)f(z) \in J_1$ donc $yz \in f^{-1}(J_1)$ et ainsi $y \in (f^{-1}(J_1) : f^{-1}(J_2))$.

i) Soit $y \in f_*(\sqrt{I})$, alors $y = \sum b_i f(x_i)$ avec $x_i \in \sqrt{I}$ c'est-à-dire qu'il existe $n_i \in \mathbb{N}$ tel que $x_i^{n_i} \in I$.

Exercice 34. Considérons l'homomorphisme d'anneau $\varphi : k[U,V] \longrightarrow k[X]$ défini par $\varphi(U) = X^3$ et $\varphi(V) = -X^2$ et tel que $\varphi(a) = a$ pour tout $a \in k$?

a) Quel est le noyau de φ ?

b) Quelle est l'image de φ ?

c) Montrer que A est intègre et que son corps des fractions est isomorphe à $k(X)$.

Solution. a) Remarquons que $\varphi(U^2 + V^3) = (X^3)^2 + (X^2)^3 = X^6 - X^6 = 0$ donc on a $U^2 + V^3 \in \ker\varphi$. Soit $P \in \ker\varphi$, on effectue la division euclidienne de P par $U^2 + V^3$ ce qui est possible car le coefficient dominant en U de $U^2 + V^3$ est 1 donc inversible. On a donc $P(U,V) = (U^2 + V^3)Q(U,V) + R(U,V)$ avec R de degré 1 en U donc $R(U,V) = A(V)U + B(V)$ où A et B sont des polynômes en une variable. On a $0 = \varphi(P) = \varphi(R)$ donc $A(-X^2) + X^3 B(-X^2) = 0$ ce qui impose $2\deg A = 2\deg B + 3$. Ce n'est possible que si $\deg A = \deg B = -\infty$ et donc $A = B = 0$. On a donc $R = 0$ et $P \in (U^2 + V^3)$. On a $\ker\varphi = (U^2 + V^3)$.

b) Soit $k \geq 2$, montrons que $X^k \in \mathrm{Im}\varphi$. Si $k = 2p$ est par, on a

$$\varphi((-1)^p V^p) = (-1)^p(-X^2)^p = X^{2p}.$$

Si $k = 2p + 3$ est impair avec $p \geq 0$, on a

$$\varphi((-1)^p UV^p) = (-1)^p X^3(-X^2)^p = X^{2p+3}.$$

Ainsi par combinaison linéaire, tout polynôme $P(X) = a_0 + \sum_{k=2}^{n} a_k X^k$ est dans $\mathrm{Im}\varphi$. Par ailleurs si $Q(U, V) \in k[U, V]$, on écrit $Q(U, V) = \sum_{i\geq 0, j\geq 0} \alpha_{i,j} U^i V^j$, on a alors

$$\varphi(Q) = \sum_{i\geq 0, j\geq 0} \alpha_{i,j}(-1)^j X^{3i+2j}.$$

On ne peut avoir $3i + 2j = 1$ avec $i \geq 0$ et $j \geq 0$ donc

$$\mathrm{Im}\varphi = \left\{ P(X) = a_0 + \sum_{k=2}^{n} a_k X^k \ / \ a_i \in k \right\}.$$

C'est un sous-anneau de $k[X]$ et est donc intègre.

c) Soit K le corps des fractions de A. Il est contenu dans $k(X)$ le corps des fractions de $k[X]$. Comme $k(X)$ est le plus petit corps contenant $k[X]$, il suffit de montrer que $k[X] \subset K$ et donc que $X \in K$. Cependant

$$X = \frac{X^3}{X^2} = -\frac{\varphi(U)}{\varphi(V)} \in K.$$

Exercice 35. Montrer que l'algèbre quotient $\mathbb{R}[X]/(X^2+X+1)$ est isomorphe à $\mathbb{C}$ et que l'algèbre $\mathbb{R}[X]/(X(X+1))$ est isomorphe à $\mathbb{R}^2$.

Solution. Considérons le morphisme de $\mathbb{R}$-algèbre $f : \mathbb{R}[X] \to \mathbb{C}$ défini par $f(1) = 1$ et $f(X) = j$ ($\mathbb{R}[X]$ est une $\mathbb{R}$-algèbre libre engendrée par 1 et X). Comme $\mathbb{C}$ est engendré comme $\mathbb{R}$ espace vectoriel (et donc comme $\mathbb{R}$-algèbre) par 1 et j, le morphisme f est surjectif. Il reste à déterminer son noyau. On a $\ker f = \{P \in \mathbb{R}[X] \ / \ P(j) = 0\}$. Remarquons que $1 + j + j^2 = 0$ donc $(1 + X + X^2) \subset \ker f$. Soit $P \in \ker f$, on effectue la division euclidienne de P par $1 + X + X^2$. On a $P = (1 + X + X^2)Q + R$ où R est un polynôme de degré 1. On écrit $R(X) = aX + b$ avec a et b des réels. Comme $P(j) = 0$, on a $R(j) = 0$. On a donc $aj + b = \frac{a}{2} + b + \frac{a}{2}i = 0$. Ceci impose que $a = b = 0$ donc $R = 0$. Ainsi si $\ker f \subset (1 + X + X^2)$ et donc $\ker f = (1 + X + X^2)$ d'où l'isomorphisme recherché.
Considérons le morphisme de $\mathbb{R}$-algèbre $f : \mathbb{R}[X] \to \mathbb{R}^2$ défini par $f(1) = (1, 1)$ et $f(X) = (-1, 0)$ ($\mathbb{R}[X]$ est une $\mathbb{R}$-algèbre libre engendrée par 1 et X). Comme $\mathbb{R}$ est engendré comme $\mathbb{R}$ espace vectoriel (et donc comme $\mathbb{R}$-algèbre) par $(1, 1)$ et $(-1, 0)$, le morphisme f est surjectif. Il reste à déterminer son noyau. On a $\ker f = \{P = \sum_i a_i X^i \in \mathbb{R}[X] \ / \ \sum_i a_i(-1, 0)^i = 0\}$ (par convention $(a, b)^0 = (1, 1)$. On commence par remarquer que $X(X + 1) \in \ker f$. En effet, on a $f(X(X + 1)) = (-1, 0)((-1, 0) + (1, 1)) = (-1, 0)(0, 1) = (0, 0)$. Soit maintenant $P \in \ker f$, on effectue la division euclidienne de P par $X(X + 1)$. On a $P = X(X + 1)Q + R$ où R est un polynôme de degré 1. On écrit $R(X) = aX + b$ avec a et b des réels. Comme $P((-1, 0)) = 0$, on a $R((-1, 0)) = 0$. On a donc $a(-1, 0) + b(1, 1) = (b - a, b) = (0, 0)$. Ceci impose que $a = b = 0$ donc $R = 0$. Ainsi si $\ker f \subset (X(X + 1))$ et donc $\ker f = (X(X + 1))$ d'où l'isomorphisme recherché.

Exercice 36. Soit k un corps de caractéristique $p > 0$ et A une k-algèbre. Montrer que le morphisme

$$F : A \to A$$

$$x \mapsto x^p$$

appelé morphisme de Frobenius est un morphisme d'anneaux.

Solution. Il s'agit de montrer que pour tout $x \in A$ et $y \in A$, on a

$$F(x + y) = F(x) + F(y) \quad \text{et} \quad F(xy) = F(x)F(y).$$

La seconde est évidente car $(xy)^p = x^p y^p$. Pour la première, on doit montrer que

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

Comme la caractéristique est $p > 0$, il suffit de montrer que $\binom{p}{k}$ est divisible par p si $0 < k < p$. On écrit

$$p! = k!(p-k)!\binom{p}{k},$$

de sorte que p divise le terme de droite. Cependant comme $k < p$ et $p - k < p$ et que p est premier, p ne divise pas $k!(p-k)!$. Il divise donc $\binom{p}{k}$.

Exercice 37. Soit k un corps et A une k-algèbre de dimension finie comme k-espace vectoriel.

a) Montrer qu'une algèbre *intègre* de dimension finie sur un corps est un corps [Montrer que l'application de multiplication par a non nul est injective puis surjective].

b) Soit $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
Montrer que $A/\mathfrak{p}$ est de dimension finie sur k.

c) Montrer que $\mathfrak{p}$ est un idéal maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.

d) Montrer que la flèche

$$A \to \bigoplus_{i=1}^{n} A/\mathfrak{p}_i$$

est surjective. En déduire l'inégalité $n \leq \dim_k(A)$.
On suppose dorénavant A réduite (c'est-à-dire $\mathrm{nil(A)} = 0$).

e) Montrer que la flèche

$$A \to \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}$$

est un isomorphisme d'anneaux.

f) Considérons l'algèbre $A = \mathbb{R}[X]/((X^2 + a)X(X + 1))$ avec $a \in \mathbb{R}$.
À quelle condition sur $a \in \mathbb{R}$, l'algèbre A est elle réduite ?

g) Dans le cas où A est réduite, expliciter l'isomorphisme précédent.

Solution. a) Soit $a \in A$ un élément non nul. Il faut montrer que a est inversible. Considérons alors l'application A-linéaire (et donc k-linéaire) :

$$\mu_a : A \to A$$
$$x \mapsto ax.$$

Son noyau est formé des $x \in A$ tels que $ax = 0$ mais comme A est intègre et $a \neq 0$, on a $x = 0$. Ainsi μ_a est injective et comme A est un k-espace vectoriel de dimension finie, elle est aussi surjective. Il existe donc $b \in A$ tel que $\mu_a(b) = 1_A$ c'est-à-dire $ab = 1_A$ et donc a est inversible d'inverse b.

b) Soit $\mathfrak{p} \in \mathrm{Spec}(A) = \{\mathfrak{p} \ / \ \mathfrak{p} \text{ est un idéal premier}\}$.
On a une application A-linéaire (et donc k-linéaire) surjective $A \to A/\mathfrak{p}$. Ainsi comme A est de dimension finie sur k, c'est aussi le cas de $A/\mathfrak{p}$.

c) La k-algèbre $A/\mathfrak{p}$ est de dimension finie et intègre (car $\mathfrak{p}$ est un idéal premier). On peut donc appliquer le **1.** pour dire que $A/\mathfrak{p}$ est un corps. Ainsi $\mathfrak{p}$ est maximal.
Soient $\mathfrak{p}_i \in \mathrm{Spec}(A), i = 1, \cdots, n$ des idéaux distincts.

d) On a vu au (ıı).b que les $\mathfrak{p}_i$ sont maximaux, ainsi si $\mathfrak{p}_i \neq \mathfrak{p}_j$, alors $\mathfrak{p}_i + \mathfrak{p}_j$ est un idéal contenant strictement $\mathfrak{p}_i$ et par maximalité, on a $\mathfrak{p}_i + \mathfrak{p}_j = A$. On peut donc appliquer le lemme chinois aux $\mathfrak{p}_i$. Et on a

$$A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n) \simeq \bigoplus_{i=1}^{n} A/\mathfrak{p}_i.$$

Ainsi l'application

$$A \to \bigoplus_{i=1}^{n} A/\mathfrak{p}_i$$

s'identifie à

$$A \to A/(\mathfrak{p}_1 \cdots \mathfrak{p}_n)$$

qui est évidement surjective.

Comme les $\mathfrak{p}_i$ sont premiers, on a $A/\mathfrak{p}_i \neq 0$ donc $\dim_k(A/\mathfrak{p}_i) \geq 1$. On voit alors que

$$\dim_k(A) \geq \dim_k\left(\bigoplus_{i=1}^{n} A/\mathfrak{p}_i\right) \geq n.$$

e) D'après ce qui précède, on a nécessairement $\mathrm{card}(\mathrm{Spec}(A)) \leq \dim_k(A)$, c'est-à-dire qu'on a un nombre fini d'idéaux premiers. On peut donc reprendre le raisonnement précedent avec tous les idéaux premiers et on a

$$A/(\prod_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}) \simeq \bigoplus_{\mathfrak{p}\in\mathrm{Spec}(A)} A/\mathfrak{p}.$$

Cependant, on a évidement que

$$\prod_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} \subset \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$$

et ce dernier idéal est nul car A est réduite. Ainsi, on a l'isomorphisme

$$A \simeq \bigoplus_{\mathfrak{p}\in\mathrm{Spec}(A)} A/\mathfrak{p}.$$

f) Considérons l'algèbre $A = \mathbb{R}[X]/((X^2+a)X(X+1))$ avec $a \in \mathbb{R}$.
On a ici un anneau factoriel $\mathbb{R}[X]$, ainsi le quotient $A = \mathbb{R}[X]/((X^2+a)X(X+1))$ est réduit si et seulement si l'élément $(X^2+a)X(X+1)$ n'a pas de facteur carré. Il y a alors quatre cas à distinguer :
1. Si $a > 0$, alors X^2+a est irréductible sur $\mathbb{R}$, il n'y a pas de facteur carré et A est réduite.
2. Si $a = 0$, alors il y a un facteur carré (et même cube) : X^3 et A n'est pas réduite.
3. Si $a = -1$, alors $X^2+a = (X-1)(X+1)$ et $(X+1)^2$ est un facteur carré, A n'est pas réduite.
4. Si $a < 0$ et $a \neq -1$, alors $X^2+a = (X+\sqrt{-a})(X-\sqrt{-a})$ et il n'y a pas de facteur carré, A est réduite.

g) Notons $\overline{P}$ la classe d'un polynôme $P \in \mathbb{R}[X]$ dans A. L'isomorphisme précedent est alors donné dans le cas 4. par

$$A \simeq \mathbb{R}[X]/(X-a) \oplus \mathbb{R}[X]/(X+a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X+1) \simeq \mathbb{R}^4$$

$$\overline{P} \mapsto (P(a), P(-a), P(0), P(1)).$$

Dans le cas 1. il est donné par

$$A \simeq \mathbb{R}[X]/(X^2+a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X+1) \simeq \mathbb{C} \oplus \mathbb{R}^2$$

$$\overline{P} \mapsto (\alpha X+\beta, P(0), P(1)) \mapsto (P(\sqrt{-a}), P(0), P(1))$$

avec

$$\sqrt{-a} = i\sqrt{a}, \quad \alpha = \frac{P(\sqrt{-a}) - P(-\sqrt{-a})}{2\sqrt{-a}} \quad \text{et} \quad \beta = \frac{P(\sqrt{-a}) + P(-\sqrt{-a})}{2}.$$

Dans le cas 4, le morphisme se factorise par $\mathbb{R}[X]/(X^2+a) \oplus \mathbb{R}[X]/(X) \oplus \mathbb{R}[X]/(X+1)$ et la seconde formule est encore valable ce qui donne une formule valable dans tous les cas.

3 Anneaux locaux et localisation

Exercice 38. Un anneau est dit local s'il contient un unique idéal maximal.

a) Montrer qu'un anneau A est local si et seulement si $A\backslash A^*$ est un idéal.

b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est il local ?

c) Soient A un anneau local, I, J deux idéaux de A et $a \in A$ un élément non diviseur de 0 tels que $IJ = (a)$. Montrer qu'il existe $x \in I$ et $y \in J$ tels que $a = xy$. En déduire que $I = (x)$ et $J = (y)$.

Solution. a) Si A est un anneau local d'idéal maximal $\mathfrak{m}$, alors $\mathfrak{m} \subset A\backslash A^*$. Si $x \in A\backslash A^*$, alors (x) est un idéal propre, et donc contenu dans un idéal maximal, nécessairement $\mathfrak{m}$. Donc $A\backslash A^*$ est bien un idéal.
Réciproquement, si $A\backslash A^*$ est un idéal, comme tout idéal propre est inclus dans $A\backslash A^*$, $A\backslash A^*$ est l'unique idéal maximal de A.

b) Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ correspondent aux nombre premiers divisant n. Donc $\mathbb{Z}/n\mathbb{Z}$ est local si et seulement si n est une puissance d'un nombre premier.

c) Par hypothèse, pour tout $(x,y) \in IJ$, il existe $f_{x,y} \in A$ tel que $xy = f_{x,y}a$. Si $f_{x,y}$ est inversible, on obtient le résultat voulu en remplaçant x par $f_{x,y}^{\vee 1}x$. On peut donc supposer par l'absurde que $f_{x,y} \in \mathfrak{m}$ pour tout (x,y). Mais alors $IJ \subset \mathfrak{m}(a)$. Or $\mathfrak{m}(a) \neq (a)$, car sinon, on aurait $a = am$ avec $m \in \mathfrak{m}$, et donc $a(1-m) = 0$ et donc $a = 0$ puisque $1-m$ est inversible. Et donc $IJ \neq (a)$.
Si $x' \in I$, $x'y \in IJ = (a)$ donc $x'y = af = xyf$ avec $f \in A$. Donc $y(x' - xf) = 0$. Or y n'est pas diviseur de 0 car sinon a le serait aussi. Donc $x' = xf \in (x)$. Donc $I = (x)$. De même pour J.

Exercice 39. Soit A un anneau et S une partie multiplicative de A (c'est-à-dire $1 \in S$ et si $r, s \in S$ alors $rs \in S$.

a) Montrer que $S^{-1}A = A \times S/\sim$, où $(a,r) \sim (b,s)$ si et seulement si il existe $t \in S$ tel que $t(as - br) = 0$, est un anneau pour l'addition $(a,r) + (b,s) = (as + br, rs)$ et la multiplication $(a,r) \cdot (b,s) = (ab, rs)$. On note a/s la classe de (a,s).

b) Montrer que $f : A \to S^{-1}A$, défini par $f(a) = a/1$ est un morphisme d'anneau et que les éléments de $f(S)$ sont inversibles. Montrer que $S^{-1}A$ et f sont caractérisés (à isomorphisme près) par la propriété universelle suivante : pour tout morphisme d'anneau $\varphi : A \to B$ tel que les éléments de $\varphi(S)$ sont inversibles, il existe un unique morphisme d'anneau $\bar{\varphi} : S^{-1}A \to B$ tel que $\varphi = \bar{\varphi}f$.

c) Montrer que si S ne contient pas de diviseur de 0, alors $A \to S^{-1}A$ est injective.

d) Montrer que si A est intègre et $S = A\backslash\{0\}$, $S^{-1}A$ est un corps (appelé corps des fractions de A).

e) Montrer que $S^{-1}A$ est nul si et seulement si $0 \in S$. Montrer en particulier que $A[\frac{1}{f}]$ (c'est-à-dire $S^{-1}A$, avec $S = \{f^n, n \in \mathbb{N}\}$) est non nul si et seulement si f n'est pas nilpotent.

f) Soit $\mathfrak{p}$ un idéal premier de A ne rencontrant pas S, montrer que $S^{-1}\mathfrak{p}$ est l'idéal de $S^{-1}A$ engendré par $\pi(\mathfrak{p})$ et qu'il est premier. Montrer que $\mathfrak{p} = \pi^{-1}(S^{-1}\mathfrak{p})$.

g) Montrer que les idéaux premiers de $S^{-1}A$ s'identifient aux idéaux premiers de A ne rencontrant pas S.

h) Montrer que tout idéal I de $S^{-1}A$ est de la forme $S^{-1}J$ pour J un idéal de A.

i) Supposons $0 \notin S$. Montrer que si A est :
   i) intègre,
   ii) principal,
   iii) factoriel,
   iv) réduit,
   alors $S^{-1}A$ l'est aussi.

Exercice 40. Soit A un anneau non nul et $\mathfrak{p}$ un idéal premier.

a) Montrer que $S = A - \mathfrak{p}$ est une partie multiplicative.

b) Montrer que $A_{\mathfrak{p}} := S^{-1}A$ est un anneau local.

Solution. a) Si $rs \in \mathfrak{p}$,r ou $s \in \mathfrak{p}$. La contraposée donne la multiplicativité de $A - \mathfrak{p}$.

b) Soit $(a,r) \in A_{\mathfrak{p}}$ est inversible si et seulement si $a \notin \mathfrak{p}$ (l'inverse est alors (r,a)). Il suffit donc de vérifier que $\mathfrak{p}A_{\mathfrak{p}} = \{(a,r), a \in \mathfrak{p}\}$ est un idéal, ce qui est immédiat.

Exercice 41. Soit A un anneau. Montrer que $A \to \bigoplus_{\mathfrak{m} \in \mathrm{Specmax}(A)} A_{\mathfrak{m}}$ est injective.

Solution. Soit $f \neq 0 \in A$. Alors $\mathrm{Ann}(f)$ est un idéal propre de A, puisqu'il ne contient pas 1. Donc $\mathrm{Ann}(f)$ est contenu dans un idéal maximal $\mathfrak{m}$. Comme $rf \neq 0$ pour tout r dans $A - \mathfrak{m}$, l'image de f dans $A_{\mathfrak{m}}$ est non nulle.

Exercice 42. a) Soit n un entier, calculer les localisés $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$ où $\mathfrak{p} = p\mathbb{Z}$ est un idéal premier.

b) En déduire que l'application

$$\mathbb{Z}/n\mathbb{Z} \to \bigoplus_{\mathfrak{p}} (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$$

est un isomorphisme de groupes.

Solution. a) Ecrivons $n = p^a m$ avec m premier à p. Si $x \in p^a\mathbb{Z}$ alors $\bar{m}\bar{x} = 0$ et $\bar{m} \notin \mathfrak{p}$, donc l'image de x dans $(\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$ est nulle : le morphisme $\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$ se factorise à travers $\mathbb{Z}/p^a\mathbb{Z}$. Récirpoquement, si x est tel que $\bar{m}\bar{x} = 0$ pour un $\bar{m}$ premier à p, alors x est divisible par p^r. Cela prouve que $\mathbb{Z}/p^a\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$ est injectif. Si $\bar{r}/\bar{s} \in (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$, comme s est premier à p^a, il existe $u, v \in \mathbb{Z}$ tels que $us + vp^a = 1$. Alors $m(sur - r) = rn \equiv 0$ donc, comme $m \notin \mathfrak{p}$, $\bar{r}/bars = \overline{(ur)}/1$, ce qui prouve la surjectivité de $\mathbb{Z}/p^a\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})_{\mathfrak{p}}$.

4 Modules

Exercice 43. Soit M un A-module, montrer que la somme directe $M^{\mathbb{N}}$ est isomorphe au module des polynômes $M[X]$.

Solution. Considérons le morphisme de A-modules

$$f : M^{\mathbb{N}} \to M[X]$$

$$(m_i)_{i\in\mathbb{N}} \mapsto \sum_{i=0}^{+\infty} m_i X^i.$$

La somme de droite est finie car le terme$(m_i)_{i\in\mathbb{N}}$ est dans une somme directe donc seul un nombre fini de termes est non nul. On montre que f est un isomorphisme. En effet, si $f((m_i)_{i\in\mathbb{N}}) = 0$, alors pour tout $i \in \mathbb{N}$, on a $m_i = 0$, donc f est injective. Par ailleurs si $P = \sum_{i=0}^{N} n_i X^i$ avec $n_i \in M$, alors posons $m_i = n_i$ pour $1 \leq i \leq N$ et $m_i = 0$ pour $i > N$, on a $f((m_i)_{i\in\mathbb{N}}) = P$ et f est surjective.

Exercice 44. Soit A et B deux anneaux et $f : A \longrightarrow B$ un homomorphisme d'anneaux.
(i) Montrer que la loi $a.b = f(a).b$ (où $a \in A$ et $b \in B$) munit B d'une structure de A-module. B muni de sa structure d'anneau et de cette structure de A-module est appelé une A-algèbre.
(ii) Montrer que si A est un corps k alors f est injectif (c'est-à-dire : une k-algèbre contient un corps isomorphe à k).
(iii) Montrer que tout B-module N est muni naturellement d'une structure de A-module. Quel est l'annulateur $\mathrm{Ann}(N) = (0_A : N)$ de ce module ?

Solution. (i) On a les égalités

$$1 \cdot b = f(1)b = b$$

$$(a + a') \cdot b = f(a + a')b = (f(a) + f(a'))b = f(a)b + f(a')b = a \cdot b + a' \cdot b$$
$$(aa') \cdot b = f(aa')b = (f(a)f(a'))b = f(a)(a' \cdot b) = a \cdot (a' \cdot b)$$

qui prouvent que cette loi muni B d'une structure de A-module.
(ii) Le noyau de f est un idéal de A. Comme A est un corps, les seuls idéaux de A sont (0) ou A. Mais comme $f(1_A) = 1_B \neq 0$, on a $1_A \notin \ker f$ et donc $\ker f = (0)$.
(iii) Soit N un B-module, la loi $a \cdot n = f(a)n$ munit N d'une structure de A-module(on garde la même addition). Soit maintenant $x \in (0_A : N) = \mathrm{Ann}_A(N)$. On a

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ \forall n \in N,\ x \cdot n = 0$$

$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ \forall n \in N,\ f(x)n = 0$$
$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ f(x) \in \mathrm{Ann}_B(N)$$
$$x \in \mathrm{Ann}_A(N) \Leftrightarrow \ x \in f^{-1}(\mathrm{Ann}_B(N)).$$

L'annulateur de N vu comme A-moduleest l'image réciproque par f de l'annulateur de N vu comme B-module : $\mathrm{Ann}_A(N) = f^{-1}(\mathrm{Ann}_B(N))$.

Exercice 45. Soit M un A-module, on définit $M^\vee = \hom_A(M, A)$. On dit que M est réflexif si le morphisme naturel $\theta : M \to M^{\vee\vee}$ défini par $m \mapsto \theta(m) = (\varphi \mapsto \varphi(m))$ avec $\varphi \in M^\vee = \hom_A(M, A)$ est un isomorphisme. Soit $f \in \mathrm{End}_A M$, on définit sa transposée ${}^t f \in \mathrm{End}_A M^\vee$ par ${}^t f(\varphi) = \varphi \circ f$ pour tout $\varphi \in M^\vee = \hom_A(M, A)$.

a) Montrer que l'ensemble des polynômes P de $A[X]$ tels que $P(f) = 0$ est un idéal que l'on notera $I(f)$.

b) Montrer que $I(f) \subset I({}^t f)$.

c) Montrer que ${}^t({}^t f) \circ \theta = \theta \circ f$.

d) Montrer que si M est réflexif, on a $I(f) = I({}^t f)$.

Solution. (i) Considérons le morphisme de A-modules $\psi : A[X] \to \mathrm{End}_A M$ défini par $\psi(P) = P(f)$. On a $I(f) = \ker \psi$ donc c'est un idéal.
(ii) Soit $P \in I(f)$ On a alors $P(f) = 0$. On calcule alors $P({}^t f)(\varphi)$ pour $\varphi \in M^\vee$. On a $P({}^t f)(\varphi) = \varphi \circ P(f) = 0$ car $P \in I(f)$. On a donc $P({}^t f) = 0$ donc $P \in I({}^t f)$. On a bien $I(f) \subset I({}^t f)$.
(iii) On a

$$\big({}^t({}^t f) \circ \theta\big)(m) = {}^t({}^t f)(\theta(m)) = \theta(m) \circ {}^t f$$

et pour $\varphi \in M^\vee$, on a

$$\Big(\big({}^t({}^t f) \circ \theta\big)(m)\Big)(\varphi) = (\theta(m) \circ {}^t f)(\varphi) = (\theta(m))(\varphi \circ f) = \varphi(f(m)).$$

Par ailleurs, on a

$$(\theta \circ f)(m) = \theta(f(m))$$

et pour $\varphi \in M^\vee$, on a

$$\big((\theta \circ f)(m)\big)(\varphi) = \big(\theta(f(m))\big)(\varphi) = \varphi(f(m)),$$

ce qui prouve l'égalité ${}^t({}^t f) \circ \theta = \theta \circ f$.
(iv) Si M est réflexif on a donc ${}^t({}^t f) = \theta \circ f \circ \theta^{-1}$. Soit $P \in I({}^t f)$. On a alors $P \in I({}^t({}^t f))$, ainsi $P(\theta \circ f \circ \theta^{-1}) = P({}^t({}^t f)) = 0$ c'est-à-dire $\theta \circ P(f) \circ \theta^{-1} = 0$. Comme θ est inversible, ceci impose que $P(f) = 0$ donc $P \in I(f)$.

Exercice 46. Soit M un A-module
(i) On suppose que M est monogène, montrer qu'il existe un idéal I de A tel que $M \simeq A/I$.
(ii) On suppose que $M \neq (0)$ est simple (c'est-à-dire que ses seuls sous-modules sont (0) et M). Montrer que M est monogène, engendré par tout élément non nul de M. Montrer que M est isomorphe à $A/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal de A.
(iii) Quels sont les $\mathbb{Z}$-modules simples ?

Solution. (i) Soit m un générateur de M et considérons le morphisme de A-modules $f : A \to M,\ a \mapsto am$. Il est surjectif (car m engendre M) et son noyau est un idéal I de A. Le morphisme $\overline{f} : A/I \to M$ est donc un isomorphisme.
(ii) Soit $m \in M$ un élément non nul et soit N le sous-module de M engendré par m. Comme $0 \neq m \in N$, le sous-module N est non nul, c'est donc M tout entier. L'élément m engendre donc M.
D'après la question précédente, on sait qu'il existe un idéal $\mathfrak{m}$ tel que $M \simeq A/\mathfrak{m}$. Il reste à vérifier que cet idéal est maximal. Soit donc I un idéal contenant strictement $\mathfrak{m}$, alors on a la suite exacte

$$0 \to I/\mathfrak{m} \to M \simeq A/\mathfrak{m} \to A/I \to 0.$$

Le module $I/\mathfrak{m}$ est donc un sous-module strict de M, il doit être nul c'est-à-dire $I = \mathfrak{m}$ donc $\mathfrak{m}$ est maximal.
(iii) D'après la question précédente, les modules simples de $\mathbb{Z}$ sont de la forme $\mathbb{Z}/\mathfrak{m}$ où $\mathfrak{m}$ est un idéal maximal. Il reste à déterminer les idéaux maximaux de $\mathbb{Z}$. Comme $\mathbb{Z}$ est principal, on a $\mathfrak{m} = (n)$ avec $n \in \mathbb{Z}$. L'idéal, (n) est maximal si et seulement si $\mathbb{Z}/(n)$ est un corps, c'est le cas si et seulement si n est premier. Les $\mathbb{Z}$ modules simples sont les $\mathbb{Z}/(p)$ avec p un nombre premier.

Exercice 47. Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si $(0 : x) \neq 0$. On note $T(M)$ l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

a) Montrer que l'ensemble des éléments de torsion de M est un sous-module de M.
b) Montrer que $M/T(M)$ est sans torsion.
c) Montrer que si $f : M \to N$ est un morphisme de A-modules alors $f(T(M)) \subset T(N)$.

Solution. (i) Il faut montrer que $T(M)$ est non vide et stable par addition et multiplication par un scalaire.
Il est clair que $0 \in T(M)$ car $(0 : 0) = \mathrm{Ann}(0) = M$.
Soit maintenant m et m' dans TM), a et a' dans A et x et x' dans $M - \{0\}$ tels que $xm = 0$ et $x'm' = 0$. Alors on a $(xx')(ax + a'm') = ax'(xm) + ax(x'm') = 0$ et $xx' \neq 0$ car A est intègre. Ainsi $T(M)$ est stable par addition et multiplication par un scalaire.
$T(M)$ est donc un sous-module de M.
(ii) Soient $Cl(m) \in M/T(M)$ et $a \in A - \{0\}$ tels que $a \cdot Cl(m) = 0$. Ceci signifie que $am \in T(M)$. Il existe donc $x \in A - \{0\}$ tel que $x(am) = 0$ et donc $(xa)m = 0$. Comme $a \in A - \{0\}$ et $x \in A - \{0\}$ on a $xa \in A - \{0\}$ (A intègre) et donc $m \in T(M)$. On a donc $Cl(m) = 0$ ce qui signifie que le seul élément de torsion de $M/T(M)$ est 0, le module $M/T(M)$ est donc sans torsion.
(iii) Soit $m \in T(M)$ et $x \in A - \{0\}$ tels que $xm = 0$. On considère alors $f(m)$ et on a $af(m) = f(am) = f(0) = 0$. L'élément $f(m)$ est donc de torsion d'où l'inclusion $f(T(M)) \subset T(N)$.

Exercice 48. Soit M un A-moduleet $m \in M$ un élément dont l'annulateur $\mathrm{Ann}(m)$ est réduit à (0). Montrer que Am est facteur direct de M si et seulement si il existe $f \in M^\vee = \hom_A(M, A)$ tel que $f(m) = 1$. Montrer qu'alors on a $M = Am \oplus \ker f$.

Solution. Soit N un facteur direct de Am de sorte que $M = Am \oplus N$. Comme $\mathrm{Ann}(m) = (0)$, l'homomorphisme $A \to Am,\ a \mapsto am$ est un isomorphisme. On peut alors définir une forme linéaire f sur M par $f(am, n) = a$. On a bien $f(m) = 1$.
Réciproquement, s'il existe un tel f, le noyau de f est un sous-module N de M. De plus, si $am \in Am \cap N$, alors $f(am) = a = 0$ donc $Am \cap N = 0$. Enfin, si $m' \in M$, on écrit $m' = f(m')m + (m' - f(m')m)$. On a $f(m')m \in Am$ et $f(m' - f(m')m) = 0$ donc $m' - f(m')m \in N$ ce qui prouve que $Am \oplus N = M$.

Exercice 49. Soient $M_1, \ldots, M_r$ des A-modules et $I_1 = \mathrm{Ann}(M_1), \cdots, I_r = \mathrm{Ann}(M_r)$ leurs annulateurs. On suppose que les I_α sont deux à deux comaximaux (c'est-à-dire que l'on a $I_\alpha + I_\beta = A$ pour $\alpha \neq \beta$).
On pose : $M = \bigoplus_{\alpha=1}^r M_\alpha$, $I = \bigcap_{\alpha=1}^r I_\alpha$, $N_\alpha = \bigoplus_{\beta\neq\alpha} M_\beta$ et $J_\alpha = \bigcap_{\beta\neq\alpha} I_\beta$. Si J est un idéal de A on notera $(0 : J)$ le sous-A-module de M égal à $\{m \in M, J.m = 0\}$. Montrer les formules suivantes :
(i) Montrer que pour tout α, I_α et J_α sont comaximaux.
(ii) $J_\alpha = (0 : N_\alpha)$,
(iii) $N_\alpha = (0 : J_\alpha) = I_\alpha \cdot M$.
(iv) $M_\alpha = (0 : I_\alpha) = J_\alpha \cdot M = \bigcap_{\beta\neq\alpha} N_\beta$.

Solution. (i) Fixons α, si $\beta \neq \alpha$, les idéaux I_α et I_β sont comaximaux. On peut donc écrire $1 = x_\beta + y_\beta$ avec $x_b \in I_\alpha$ et $y_\beta \in I_\beta$. On a alors

$$1 = \prod_{\beta\neq\alpha} (x_\beta + y_\beta).$$

On voit alors que 1 est somme d'éléments de I_α (touts les termes multiples d'un x_β) et de $\prod_{\beta\neq\alpha} y_\beta \in \prod_{\beta\neq\alpha} I_\beta \subset J_\alpha$.
(ii) Un élément $a \in A$ est dans $(0 : N_\alpha)$ si pour tout $n \in N_\alpha$ on a $an = 0$ c'est-à-dire pour tout $\beta \neq \alpha$ et pour tout $m \in M_\beta$, on a $am = 0$. Ainsi $(0 : N_\alpha)$ est l'intersection des $\mathrm{Ann}(M_\beta)$ pour $\beta \neq \alpha$ et donc $J_\alpha = (0 : N_\alpha)$.
(iii) Un élément $\sum m_\beta \in M$ avec $m_\beta \in M_\beta$ est dans $(0 : J_\alpha)$ si et seulement si $J_\alpha \cdot (\sum m_\beta) = 0$ c'est-à-dire pour tout β, on a $J_\alpha \cdot m_\beta = 0$. Si $\alpha \neq \beta$, l'inclusion $J_\alpha \subset I_\beta$ montre que tout $m_\beta \in M_\beta$ convient. Pour $\beta = \alpha$, l'égalité $I_\alpha + J_\alpha = A$ implique $I_\alpha m_\alpha + 0 = Am_\alpha$ et comme I_α annule M_α ceci impose $Am_\alpha = 0$ donc $m_\alpha = 0$. Ainsi $(0 : J_\alpha) = \oplus_{\beta\neq\alpha} M_\beta = N_\alpha$.
Pour $\beta \neq \alpha$, on a $A = I_\alpha + I_\beta$ donc $M_\beta = (I_\alpha + I_\beta)M_\beta = I_\alpha M_\beta$ et pour $\beta = \alpha$, on a $I_\alpha M_\alpha = 0$. Ainsi

$$I_\alpha M = \bigoplus_\beta I_\alpha M_\beta = \bigoplus_{\beta\neq\alpha} M_\beta = N_\alpha.$$

(iv) Un élément $\sum m_\beta \in M$ avec $m_\beta \in M_\beta$ est dans $(0 : I_\alpha)$ si et seulement si $I_\alpha \cdot (\sum m_\beta) = 0$ c'est-à-dire pour tout β, on a $I_\alpha \cdot m_\beta = 0$. Si $\alpha = \beta$, on a $I_\alpha = \mathrm{Ann}(M_\alpha)$ donc tout $m_\alpha \in M_\alpha$ convient. Pour $\beta \neq \alpha$, l'égalité $I_\alpha + I_\beta = A$ implique $0 + I_\beta m_\beta = Am_\beta$ et comme I_β annule M_β ceci impose $Am_\beta = 0$ donc $m_\beta = 0$. Ainsi $(0 : I_\alpha) = M_\alpha$.
On a $J_\alpha M = \oplus_\beta J_\alpha M_\beta = J_\alpha M_\alpha$ car $J_\alpha \subset I_\beta$ pour $\beta \neq \alpha$. On a par ailleurs $J_\alpha + I_\alpha = A$ donc $M_\alpha = J_\alpha M_\alpha + I_\alpha M_\alpha = J_\alpha M_\alpha$. On a donc $J_\alpha M = M_\alpha = \bigcap_{\beta\neq\alpha} N_\beta$.