2.7 Théorème chinois

Théorème 49. *Soit n et m des entiers positifs. Soit $\pi_n \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ et $\pi_m \colon \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ les morphismes d'anneaux quotient. Soit $\pi_n \times \pi_m \colon \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ le morphisme d'anneaux produit.*

Alors :

- *On a $\mathrm{Ker}(\pi_n \times \pi_m) = n\mathbf{Z} \cap m\mathbf{Z} = \mathrm{ppcm}(n,m)\mathbf{Z}$.*
- *Supposons en outre n et m premiers entre eux ; alors $\pi_n \times \pi_m$ est surjectif. En particulier le morphisme $\pi_n \times \pi_m$ induit un isomorphisme d'anneaux*

$$\mathbf{Z}/nm\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

Démonstration. Par définition du quotient, le noyau de π_n (respectivement π_m) est $n\mathbf{Z}$ (respectivement $m\mathbf{Z}$). Par ailleurs, par définition du morphisme produit, on a $\mathrm{Ker}(\pi_n \times \pi_m) = \mathrm{Ker}(\pi_n) \cap \mathrm{Ker}(\pi_m)$.

Montrons, pour mémoire, l'égalité $n\mathbf{Z} \cap m\mathbf{Z} = \mathrm{ppcm}(n,m)\mathbf{Z}$. Soit $d \in \mathbf{N}$ tel que $n\mathbf{Z} \cap m\mathbf{Z} = d\mathbf{Z}$. En particulier $d \in n\mathbf{Z}$ et $d \in m\mathbf{Z}$, donc d est un multiple de n et de m. Par ailleurs, si e est un multiple de n et de m, on a $e \in n\mathbf{Z} \cap m\mathbf{Z}$, donc $e \in d\mathbf{Z}$, donc e est un multiple de d. Ceci montre bien que $d = \mathrm{ppcm}(m,n)$.

Pour la seconde partie, notons que comme n et m sont premiers entre eux, on a $\mathrm{ppcm}(m,n) = mn$. Ainsi le théorème de factorisation et la première partie donneront le résultat une fois montrée la surjectivité de $\pi_n \times \pi_m$.

Soit $(x,y) \in \mathbf{Z}^2$. Il s'agit de montrer qu'il existe $z \in \mathbf{Z}$ tel que

$$z = x \pmod{n}, \quad z = y \pmod{m}.$$

Comme n et m sont premiers entre eux, il existe $(u,v) \in \mathbf{Z}^2$ tel que $un + vm = 1$ (théorème de Bezout dans $\mathbf{Z}$). L'entier $z = yun + xvm$ convient. □

Théorème 50. *Soit A un anneau et $\mathcal{I}$, $\mathcal{J}$ deux idéaux de A.*

Soit $\pi_{\mathcal{I}} \colon A \to A/\mathcal{I}$ et $\pi_{\mathcal{J}} \colon A \to A/\mathcal{J}$ les morphismes d'anneaux quotient. Soit $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}} \colon A \to A/\mathcal{I} \times A/\mathcal{J}$ le morphisme d'anneaux produit.

- *On a $\mathrm{Ker}(\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}) = \mathcal{I} \cap \mathcal{J}$.*
- *Supposons en outre $\mathcal{I} + \mathcal{J} = A$. Alors $\mathcal{I} \cap \mathcal{J} = \mathcal{I} \cdot \mathcal{J}$ et le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ est surjectif. En particulier le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ induit un isomorphisme d'anneaux*

$$A/(\mathcal{I} \cdot \mathcal{J}) \cong (A/\mathcal{I}) \times (A/\mathcal{J}).$$

Démonstration. On raisonne similairement au cas $A = \mathbf{Z}$ (théorème précédent). Ce qui ne s'obtient pas directement par extension de la démonstration du théorème précédent : si $\mathcal{I} + \mathcal{J} = A$, alors $\mathcal{I} \cap \mathcal{J} = \mathcal{I} \cdot \mathcal{J}$ et le morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$ est surjectif.

Montrons le. Par définition du produit d'idéaux, l'inclusion $\mathcal{I} \cdot \mathcal{J} \subset \mathcal{I} \cap \mathcal{J}$ est toujours vraie. Montrons l'inclusion réciproque. Par hypothèse, il existe $(a, b) \in \mathcal{I} \times \mathcal{J}$ tel que $a+b = 1$ Soit alors $z \in \mathcal{I} \cap \mathcal{J}$. Alors $z = za + zb$. Comme $z \in \mathcal{J}$ et $a \in \mathcal{I}$, on a $za \in \mathcal{I} \cdot \mathcal{J}$. Comme $z \in \mathcal{I}$ et $b \in \mathcal{J}$, on a $zb \in \mathcal{I} \cdot \mathcal{J}$. Ainsi $z = za + zb \in \mathcal{I} \cdot \mathcal{J}$.

Passons à la surjectivité du morphisme $\pi_{\mathcal{I}} \times \pi_{\mathcal{J}}$. Il faut montrer : soit $(x, y) \in A^2$; alors il existe $z \in A$ tel que $z = x \pmod{\mathcal{I}}$ et $z = y \pmod{\mathcal{J}}$. Soit $(a, b) \in \mathcal{I} \times \mathcal{J}$ tel que $a + b = 1$. Alors $z := ay + bx$ convient. En effet comme $a + b = 1$ et $b \in \mathcal{J}$, on a $a = 1 \pmod{\mathcal{J}}$ donc $ay = y \pmod{\mathcal{J}}$. Comme $b \in \mathcal{J}$, on a par ailleurs $bx = 0 \pmod{\mathcal{J}}$. Donc $z = ay + bx = y + 0 \pmod{\mathcal{J}}$. De même, on montre $z = x \pmod{\mathcal{I}}$. □

Remarque. Si $\mathcal{I} + \mathcal{J} = A$, on dit que les idéaux $\mathcal{I}$ et $\mathcal{J}$ sont étrangers (ou comaximaux, ou premiers entre eux). Dans le cas où A est principal (intègre, tout idéal est engendré par un élément), l'hypothèse que les idéaux sont étrangers est équivalente à l'hypothèse que les générateurs des idéaux sont premiers entre eux.

Pour mémoire, si $\mathbf{K}$ est un corps, les éléments X et Y de $A = \mathbf{K}[X, Y]$ sont premiers entre eux, mais les idéaux $\mathcal{I} = \langle X \rangle$ et $\mathcal{J} = \langle Y \rangle$, dont la somme est $\langle X, Y \rangle$, ne sont pas étrangers. Exercice : montrer que dans ce cas ni $A/\mathcal{I} \cdot \mathcal{J}$ ni $A/\mathcal{I} \cap \mathcal{J}$ ne sont isomorphes à $(A/\mathcal{I}) \times (A/\mathcal{J})$ (on pourra consulter l'indication de la correction de l'exercice 1.8 du CC1 de 2018-2019).

On peut généraliser le théorème chinois à un nombre fini d'idéaux.

Théorème 51. *Soit A un anneau. Soit $n \geqslant 1$ un entier. Soit $(\mathcal{I}_i)_{i=1,\dots,n}$ un ensemble fini d'idéaux de A.*

Pour $i = 1, \dots, n$, soit $\pi_i \colon A \to A/\mathcal{I}_i$ le morphisme d'anneaux quotient. Soit

$$\prod_{i=1}^{n} \pi_i \colon A \to \prod_{i=1}^{n} A/\mathcal{I}_i$$

le morphisme d'anneaux produit.

- *On a $\operatorname{Ker}(\prod_{i=1}^{n} \pi_i) = \cap_{i=1}^{n} \mathcal{I}_i$.*
- *On suppose en outre que si $i \neq j$, on a $\mathcal{I}_i + \mathcal{I}_j = A$. Alors $\cap_{i=1}^{n} \mathcal{I}_i = \prod_{i=1}^{n} \mathcal{I}_i$ et le morphisme $\prod \pi_i$ est surjectif. En particulier $\prod \pi_i$ induit un isomorphisme d'anneaux*

$$A/\prod_{i=1}^{n} \mathcal{I}_i \cong \prod_{i=1}^{n} A/\mathcal{I}_i.$$

Le démonstration de ce dernier résultat peut se faire par récurrence à partir du résultat pour deux idéaux. Il est utile de noter à ce sujet qu'on vérifie facilement que le « produit d'idéaux est associatif ». Par exemple si $\mathcal{I}_1$, $\mathcal{I}_2$ et $\mathcal{I}_3$ sont des idéaux d'un anneau A, on a

$$(\mathcal{I}_1 \cdot \mathcal{I}_2) \cdot \mathcal{I}_3 = \mathcal{I}_1 \cdot (\mathcal{I}_2 \cdot \mathcal{I}_3) = \mathcal{I}_1 \cdot \mathcal{I}_2 \cdot \mathcal{I}_3.$$

Remarque. L'hypothèse que les idéaux $\mathcal{I}_i$ de l'énoncé sont *deux à deux* étrangers est importante ; on ne peut pas se contenter de l'hypothèse $\sum_{i=1}^{n} \mathcal{I}_i = A$. On se penchera par exemple sur le cas de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/r\mathbf{Z}$ pour $(n, m, r) = (6, 10, 15)$ et on montrera que ce produit n'est pas isomorphe à $\mathbf{Z}/nmr\mathbf{Z}$.

2.8 Diviseurs de zéros, anneaux intègres, corps

Définition 52. Soit A un anneau. Un *diviseur de zéro* dans A est un élément a de A tel qu'il existe un élément b *non nul* de A vérifiant $a \times b = 0_A$.

Un diviseur de zéro nul est appelé diviseur de zéro trivial.

Remarque. Attention, cette terminologie, bien qu'usuelle, peut être source de confusion. Par exemple, dans $\mathbf{Z}$, n'importe quel entier divise 0, mais seul 0 est un diviseur de zéro...

Exemple. Un élément de $A^\times$ n'est jamais diviseur de zéro (y compris si A est l'anneau nul ; dans ce cas 0_A est inversible mais n'est pas diviseur de zéro).

Les anneaux $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}[X]$, $\mathbf{C}[X]$... n'ont pas de diviseurs de zéros non triviaux.

Soit p et q deux nombres premiers et $N := p.q$. Alors $[p]_N$ et $[q]_N$ sont des diviseurs de zéro non triviaux de $\mathbf{Z}/N\mathbf{Z}$.

L'anneau nul n'a pas de diviseur de zéro. C'est d'ailleurs le seul anneau vérifiant cette propriété.

Remarque. Attention, on peut trouver dans d'autres références une définition de « diviseur de zéro » qui correspond à ce que nous appelons « diviseur de zéro non trivial » dans ce texte. Certains des énoncés s'adaptent en conséquence. Il faut bien penser à vérifier la définition employée dans la référence consultée.

Définition 53. Un anneau est dit *intègre* s'il est *non nul* et ne possède pas de diviseurs de zéro non triviaux.

Remarque. Ainsi un anneau A est intègre si et seulement si A est non nul et on a la propriété

$$\forall (x, y) \in A^2, \quad x \times y = 0_A \Rightarrow (x = 0_A \text{ ou } y = 0_A).$$

C'est souvent sous cette dernière forme qu'on exploite l'intégrité d'un anneau ; la généralisation à un produit de plus de deux éléments est immédiate (ritournelle : « Un produit est nul si et seulement si l'un des facteurs est nul »).

Proposition 54. *Soiut A un anneau. Alors A est intègre si et seulement si l'idéal nul $\{0_A\}$ est un idéal premier.*

Démonstration. L'anneau A est non nul si et seulement si l'idéal nul est un idéal propre. Ainsi vu la définition d'un idéal premier, cette proposition n'est qu'une reformulation de la remarque précédente. □

Proposition 55. *Un sous-anneau d'un anneau intègre est encore intègre.*

Démonstration. Soit A un anneau. La propriété

$$\forall (x, y) \in A^2, \quad x \times y = 0_A \Rightarrow (x = 0_A \text{ ou } y = 0_A).$$

est évidemment encore vraie sur tout sous-anneau de A.

Il suffit donc de montrer qu'un sous-anneau d'un anneau non nul est non nul. Ceci vient du fait qu'un anneau et ses sous-anneaux ont les mêmes 0 et 1, et qu'un anneau nul est caractérisé par l'égalité $1 = 0$. □

Définition 56. Un *corps* est un anneau A non nul et tel que tout élément non nul est inversible. De manière équivalente, un corps est un anneau A tel que $A^\times = A \setminus \{0_A\}$.

Un *sous-corps* d'un corps est un sous-anneau de ce corps qui est également un corps.

Un *morphisme de corps* entre deux corps est un morphisme d'anneaux entre ces deux corps ; un morphisme de corps est aussi appelé une *extension de corps*.

Exemple. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}/n\mathbf{Z}$ si n est premier, $\mathbf{K}[X]/P\mathbf{K}[X]$ si $\mathbf{K}$ est un corps et si $P \in \mathbf{K}[X]$ est un polynôme irréductible. $\mathbf{Q}$ est un sous-corps de $\mathbf{R}$; $\mathbf{Z}$ est un sous-anneau de $\mathbf{C}$ mais ce n'est pas un sous-corps de $\mathbf{C}$

Remarque. Un corps est un anneau intègre.

Proposition 57. *Soit A un anneau. Les propriétés suivantes sont équivalentes :*

- *A est un corps ;*
- *A possède exactement deux idéaux ;*
- *$\{0_A\} \neq A$ et A et $\{0_A\}$ sont les seuls idéaux de A ;*
- *$\{0_A\}$ est un idéal maximal de A.*

En particulier si A est un corps, B est un anneau non nul, et $\varphi\colon A \to B$ est un morphisme d'anneaux, φ est injectif et B possède un sous-anneau isomorphe au corps A.

Démonstration. Exercice □

Théorème 58. *Soit A un anneau et $\mathcal{I}$ un idéal de A.*
L'idéal $\mathcal{I}$ est premier si et seulement si le quotient $A/\mathcal{I}$ est intègre.
L'idéal $\mathcal{I}$ est maximal si et seulement si le quotient $A/\mathcal{I}$ est un corps.

Démonstration. Soit $\pi\colon A \to A/\mathcal{I}$ le morphisme quotient.

Supposons l'idéal $\mathcal{I}$ premier. En particulier il est propre et le quotient $A/\mathcal{I}$ est distinct de l'anneau nul. Soit $x, y \in A/\mathcal{I}$ tel que $xy = 0$. Soit $x', y' \in A$ tels que $x = \pi(x')$ et $y = \pi(y')$. Alors $xy = \pi(x')\pi(y') = \pi(x'y')$ car π est un morphisme d'anneaux. Comme $xy = 0$, on en déduit $x'y' \in \mathrm{Ker}(\pi) = \mathcal{I}$. Comme $\mathcal{I}$ est premier, soit $x' \in \mathcal{I}$, soit $y' \in \mathcal{I}$. Donc soit $x = \pi(x') = 0$, soit $y = \pi(y') = 0$. Donc $A/\mathcal{I}$ est intègre.

Supposons le quotient $A/\mathcal{I}$ intègre. En particulier, il est distinct de l'anneau nul et l'idéal $\mathcal{I}$ est propre. Soit $x, y \in A$ tels que $xy \in \mathcal{I}$. Donc $\pi(xy) = 0$ et comme π est un morphisme d'anneaux, on a $\pi(x)\pi(y) = 0$. Comme $A/\mathcal{I}$ est intègre, on a soit $\pi(x) = 0$, soit $\pi(y) = 0$, donc soit $x \in \mathcal{I}$, soit $y \in \mathcal{I}$. Donc $\mathcal{I}$ est un idéal premier.

Supposons l'idéal $\mathcal{I}$ maximal. En particulier il est propre et le quotient $A/\mathcal{I}$ est distinct de l'anneau nul. Soit $x \in A/\mathcal{I}$ tel que $x \neq 0$. Soit $x' \in A$ tel que $x = \pi(x')$. Comme x est non nul, on a $x' \notin \mathcal{I}$. Comme $\mathcal{I}$ est maximal, l'idéal engendré par $\mathcal{I}$ et x' est A, donc il existe $y \in \mathcal{I}$ et $u \in A$ tel que $y + ux' = 1$. Ainsi, comme π est un morphisme d'anneaux, on a $1 = \pi(y + ux') = \pi(y) + \pi(u)\pi(x')$ or $\pi(y) = 0$ donc $\pi(u)\pi(x') = 1$. Donc x est inversible. Ainsi $A/\mathcal{I}$ est un corps.

Supposons que $A/\mathcal{I}$ est un corps. En particulier, $A/\mathcal{I}$ n'est pas l'anneau nul donc $\mathcal{I}$ est un idéal propre. Soit $\mathcal{J}$ un idéal de A tel que $\mathcal{I} \subset \mathcal{J}$. Alors, comme π est surjectif, $\pi(\mathcal{J})$ est un idéal de $A/\mathcal{I}$. Comme $A/\mathcal{I}$ est un corps, d'après la proposition 57, on a $\pi(\mathcal{J}) = A/\mathcal{I}$ ou $\pi(\mathcal{J}) = \{0\}$. Comme $\mathcal{J}$ contient $\mathcal{I} = \mathrm{Ker}(\pi)$, on a $\pi^{-1}(\pi(\mathcal{J})) = \mathcal{J}$ (*cf.* proposition 20). Ainsi $\mathcal{J} = \mathcal{I}$ ou $\mathcal{J} = A$. □

Remarque. On retrouve en particulier qu'un anneau est intègre si et seulement si son idéal nul est premier et est un corps si et seulement si son idéal nul est maximal.

Remarque. Version condensée de l'argument pour un corps : d'après la proposition 20), l'ensemble des idéaux de $A/\mathcal{I}$ est en bijection avec l'ensemble des idéaux de A contenant $\mathcal{I}$. Ainsi, d'après la proposition 57, $A/\mathcal{I}$ est un corps si et seulement si $\mathcal{I}$ est contenu dans exactement deux idéaux de A. Cette dernière propriété caractérise les idéaux maximaux de A.

Théorème 59. *Soit n un entier* strictement *positif. Alors $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier*

Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme non nul. *Alors $\mathbf{K}[X]/P\mathbf{K}[X]$ est un corps si et seulement si $\mathbf{K}[X]/P\mathbf{K}[X]$ est intègre si et seulement si P est irréductible.*

Remarque. L'anneau $\mathbf{Z}/0\mathbf{Z}$ est isomorphe à $\mathbf{Z}$, c'est donc un anneau intègre qui n'est pas un corps.

Démonstration. Au vu du théorème 58, cela découle aussitôt des propositions 28 et 30. □

Corollaire 60. *La caractéristique d'un corps est zéro ou un nombre premier.*

Remarque. Un anneau de caractéristique un nombre premier p n'est pas nécessairement un corps. Considérer par exemple $\mathbf{Z}/p\mathbf{Z}[X]$.

2.9 Éléments irréductibles d'un anneau intègre

On va généraliser, dans le cadre des anneaux intègres, la notion de nombre premier d'une part, de polynôme irréductible d'autre part. Dans tout ce qui suit, A est un anneau *intègre* fixé.

Définition 61. Soit a et b des éléments de A. On dit que a divise b, ou encore que b est un multiple de a, et on note $a|b$, s'il existe $c \in A$ tel que $b = c\,a$.

Remarque. Encore une fois, attention à la terminologie ! Tout élément de A divise 0_A, mais comme A est intègre le seul diviseur de zéro dans A (au sens de la définition 52) est 0_A.

Remarque. Soit $a \in A^\times$. Alors a divise n'importe quel élément de A.

Lemme 62. *Soit $a, b \in A$.*

Alors a divise b si et seulement si on a l'inclusion $b\,A \subset a\,A$.

Par ailleurs les propriétés suivantes sont équivalentes :

1. *a divise b et b divise a ;*
2. *on a $b\,A = a\,A$;*
3. *il existe $c \in A^\times$ tel que $b = c\,a$;*
4. *il existe $c \in A^\times$ tel que $a = c\,b$.*

Démonstration. La première propriété se démontre exactement comme dans le cas particulier $A = \mathbf{Z}$. L'équivalence 1. $\Leftrightarrow$ 2. en découle aussitôt. L'équivalence 3. $\Leftrightarrow$ 4. est facile et laissée au lecteur. Compte tenu de cette dernière équivalence, on en déduit alors 3. $\Rightarrow$ 1..

Il reste à montrer 1. $\Rightarrow$ 3.. Si $b = 0$, on a $a = 0$ et 3. est vraie avec $c = 1$. Supposons $b \neq 0$. Par hypothèse, il existe $c \in A$ tel que $b = c\,a$ et $d \in A$ tel que $a = d\,b$. En particulier on a $b = c\,d\,b$ soit $b\,(1 - c\,d) = 0$. Comme A est supposé intègre et b est non nul, on en déduit $c\,d = 1$. En particulier $c \in A^\times$. □

Définition 63. Soit $a, b \in A$. On dit que a et b sont des éléments *associés* si l'une des quatre conditions équivalentes de la proposition précédente est vérifiée.

Slogan. Les propriétés des éléments d'un anneau intègre liées à la notion de divisibilité sont « invariantes par association ».

Remarque. Il est à noter que si a, a' et b sont des éléments de A, avec a et a' d'une part, b, b' d'autre part, associés, alors a divise b si et seulement a' divise b'.

Définition 64. Un élément a de A est dit *irréductible* s'il est *non inversible* et pour tous élément $b, c \in A$ tels que $a = bc$, on a $b \in A^\times$ *ou* $c \in A^\times$.

Remarque. Un élément irréductible est nécessairement non nul.

Exemple. Les éléments irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés.

Les éléments irréductibles de $\mathbf{K}[X]$ sont... les polynômes irréductibles (ouf !).

Remarque. Soit $a \in A$. Alors a est irréductible si et seulement s'il est non nul, non inversible, et tout élément qui divise a est soit inversible soit associé à a.

Par ailleurs a est irréductible si et seulement si tout élément associé à a est irréductible.

Définition 65. Deux éléments a et b de A sont dit *premiers entre eux* si les seuls éléments de A qui divisent à la fois a et b sont les inversibles de A.

Proposition 66. *Soit a un élément irréductible de A et $b \in A$. Alors a et b ne sont* pas *premiers entre eux si et seulement si a divise b. En d'autres termes, a et b sont premiers entre eux si et seulement si a ne divise pas b.*

Démonstration. Si a divise b, a est un diviseur commun de a et b qui est non inversible (car a est irréductible), donc a et b ne sont pas premiers entre eux.

Si a et b ne sont pas premier entre eux, il existe un diviseur commun c de a et b qui n'est pas inversible. Comme a est irréductible, c et a sont associés. Donc, comme c divise b, a divise également b. □

Théorème 67. *Soit a un élément de A. Supposons l'idéal $a \cdot A$ premier et non nul. Alors a est irréductible.*

Démonstration. Comme l'idéal $a \cdot A$ est premier, il est propre, donc a est non inversible.

Soit $b, c \in A$ tels que $a = bc$. En particulier $bc \in a \cdot A$. Comme $a \cdot A$ est premier, on a $b \in a \cdot A$ ou $c \in a \cdot A$. Supposons par exemple $b \in a \cdot A$. Donc a divise b. Par ailleurs b divise a, donc a et b sont associés. Ainsi il existe $\alpha \in A^\times$ tel que $a = a\alpha c$. Comme $a \cdot A$ est non nul, a est non nul, et comme A est intègre, on a donc $\alpha c = 1$. Donc c est inversible. De même, si $c \in a \cdot A$, on trouve par symétrie $b \in A^\times$.

Ainsi a est bien un élément irréductible de A. □

La réciproque est *fausse* (un élément irréductible n'engendre pas toujours un idéal premier), mais les contre-exemples ne sont pas immédiats. On verra en particulier en TD que dans $\mathbf{Z}[i\sqrt{3}]$, 2 est irréductible mais n'engendre pas un idéal premier.

Nous terminons par quelques considérations spécifiques aux polynômes en une indéterminée sur un corps. Soit $\mathbf{K}$ un corps. On note $\mathrm{Irr}(\mathbf{K}[X])$ l'ensemble des polynômes unitaires irréductibles de $\mathbf{K}[X]$.

Théorème 68. *Soit $\mathbf{K}$ un corps. Soit $Q \in \mathbf{K}[X]$ non nul. Il existe une unique famille presque nulle $(\nu_P(Q))_{P \in \mathrm{Irr}(\mathbf{K}[X])}$ d'entiers positifs et un unique $\alpha \in \mathbf{K}^\times$ tel que*

$$Q = \alpha \prod_{P \in \mathrm{Irr}(\mathbf{K}[X])} P^{\nu_P(Q)}.$$

Nous donnerons plus tard une démonstration générale de ce théorème pour tous les anneaux dits principaux. En fait en anticipant sur les notions introduites ultérieurement, on montrera que tout anneau principal est factoriel.

Définition 69. Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X] \setminus \{0\}$. On dit que P est *sans facteur multiple* si pour tout $Q \in \mathrm{Irr}(\mathbf{K}[X])$ on a $\nu_Q(P) \leqslant 1$.

On vérifie qu'il est équivalent de demander que si $Q \in \mathbf{K}[X]$ est non constant alors Q^2 ne divise pas P.

Proposition 70. *Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$. Si $\mathrm{pgcd}(P, P') = 1$ alors P est sans facteur multiple.*

Démonstration. Montrons la contraposée. Supposons qu'il existe $Q \in \mathbf{K}[X]$ irréductible et $R \in \mathbf{K}[X]$ tels que $P = Q^2 R$. En dérivant, on trouve $P' = 2QQ'R + Q^2R' = Q\,(2Q'R + QR')$. Ainsi Q est un facteur irréductible commun à P et P', et P et P' ne sont pas premiers entre eux. □

Attention, la réciproque est fausse en général ! Elle est vraie si $\mathbf{K}$ est de caractéristique zéro, ou plus généralement est un corps dit *parfait* (*cf.* exercices de TD ; un corps fini est parfait ; le corps des fractions rationnelles en une indéterminée sur un corps fini ne l'est pas).

Définition 71. Un corps $\mathbf{K}$ est dit *algébriquement clos* si tout élément de $\mathbf{K}[X]$ non constant a au moins une racine dans $\mathbf{K}$.

Proposition 72. *Soit $\mathbf{K}$ un corps algébriquement clos et $P \in \mathbf{K}[X] \setminus \{0\}$ sans facteur multiple. Alors P a exactement $\deg(P)$ racines dans $\mathbf{K}$.*

2.10 Notion d'algèbre

Définition 73. Soit A un anneau. Une *algèbre sur A* est un couple (B, φ) où B est un anneau et $\varphi\colon A \to B$ un morphisme d'anneaux.

Si $\varphi\colon A \to B$ est une A-algèbre, on a une loi de composition externe naturelle (« multiplication par un scalaire ») :

$$\begin{array}{rcl} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b := \varphi(a) b \end{array}$$

Elle vérifie les propriétés suivantes :

$$\forall b \in B, \quad 0_A \cdot b = 0_B \ ;$$

$$\forall b \in B, \quad 1_A \cdot b = b \ ;$$

$$\forall a \in A, \quad \forall (b_1, b_2) \in B^2, \quad a \cdot (b_1 + b_2) = a \cdot b_1 + a \cdot b_2 \ ;$$

$$\forall (a_1, a_2) \in A^2, \quad \forall b \in B, \quad a_1 \cdot (a_2 \cdot b) = (a_1 a_2) \cdot b.$$

En particulier, on a la remarque importante suivante : si A est un corps, *toute A-algèbre B est naturellement munie d'une structure de A-espace vectoriel*. Rappelons qu'en outre si B n'est pas l'anneau nul alors B possède un sous-anneau isomorphe au corps A.

Le produit par un scalaire vérifie aussi des propriétés de compatibilités vis à vis de la multiplication dans A

$$\forall (a_1, a_2) \in A^2, \quad \forall (b_1, b_2) \in B^2, \quad (a_1 \cdot b_1)(a_2 \cdot b_2) = (a_1 a_2) \cdot (b_1 b_2).$$

Réciproquement, si B est un anneau muni d'une loi de composition externe

$$\begin{array}{rcl} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

vérifiant les propriétés ci-dessus, B est naturellement muni d'une structure de A-algèbre : le morphisme φ correspondant est $a \mapsto a \cdot 1_B$

Exemple. Tout anneau est muni d'une unique structure de $\mathbf{Z}$-algèbre.

Si A est un sous-anneau de B, B est naturellement muni d'une structure de A-algèbre.

En particulier, si A est un anneau, $A[X]$ et $A[[X]]$ sont naturellement munis de structures de A-algèbres.

Si A est un anneau et B une A-algèbre, tout quotient de B par un idéal est naturellement muni d'une structure de A-algèbre.

Si A est un anneau, l'anneau nul est naturellement muni d'une structure de A-algèbre. A^E est naturellement muni d'une structure de A-algèbre (morphisme diagonal)

Un anneau de caractéristique n possède une unique structure de $\mathbf{Z}/n\mathbf{Z}$-algèbre (et plus généralement une unique structure de $\mathbf{Z}/m\mathbf{Z}$-algèbre pour tout multiple m de n).

Définition 74. Soit $\varphi_B \colon A \to B$ une A-algèbre. Une sous-A-algèbre de B est un sous-anneau B' de B tel que le morphisme d'anneaux $\iota \colon B' \to B$ se factorise par φ_B, en d'autres termes il existe une structure de A-algèbre $\varphi_{B'} \colon A \to B'$ telle que $\varphi_B = \iota \circ \varphi_{B'}$.

Soit $\varphi_C \colon A \to C$ une autre A-algèbre. Un morphisme de A-algèbres de B vers C est un morphisme d'anneaux $\psi \colon B \to C$ qui vérifie $\psi \circ \varphi_B = \varphi_C$.

La plupart des propriétés et notions relatives aux anneaux, sous-anneaux et morphismes d'anneaux, correctement adaptés, s'étendent facilement aux A-algèbres et à leur morphismes et sous-algèbres.. Par exemple la composée de deux morphismes de A-algèbres est un morphisme de A-algèbres ; on définit de manière évidente la notion d'isomorphisme de A-algèbres, et un morphisme de A-algèbres est un isomorphisme si et seulement si c'est une application bijective.

Nous détaillons ci-dessous la situation pour l'algèbre $A[X]$ et pour les quotients de A-algèbres, d'une importance fondamentale dans la pratique.

Théorème 75. Propriété universelle de l'algèbre des polynômes en une indéterminée

Soit A un anneau. Soit $\iota \colon A \to A[X]$ le morphisme d'anneaux injectif naturel (qui munit A d'une structure de A-algèbres). L'application

$$\begin{array}{rcl} \mathrm{Hom}_{A-alg}(A[X], B) & \longrightarrow & B \\ \varphi & \longmapsto & \varphi(X) \end{array}$$

est bijective.

Démonstration. Ceci découle de la propriété universelle de l'anneau des polynômes en une indéterminée (théorème 44). En reprenant les notations de ce théorème, pour tout $(\psi, b) \in \mathrm{Hom}_{\mathrm{anneaux}}(A, B) \times B$, le morphisme $\varphi \in \mathrm{Hom}_{\mathrm{anneaux}}(A[X], B)$ correspondant est par définition un morphisme de A-algèbres si et seulement si le morphisme ψ coïncide avec la structure de A-algèbres $A \to B$ sur B. □

Slogan. Se donner un morphisme de A-algèbres de la A-algèbre $A[X]$ vers une A-algèbre B, c'est se donner un élément de B.

Définition 76. Soit A un anneau et B une A-algèbre. Soit $b \in B$. L'unique élément de $\mathrm{Hom}_{A-\mathrm{alg}}(A[X], B)$ qui envoie X sur b est appelé morphisme d'évaluation en b, et noté $\mathrm{ev}_b \colon P \mapsto P(b)$. On note $A[b]$ l'image de $A[X]$ par ev_b.

Si $P \in A[X]$, une racine (ou zéro) de P dans B est un élément $b \in B$ tel que $P(b) = 0$.

Le résultat suivant peut de manière savante s'exprimer ainsi : « le quotient d'une A-algèbre par un idéal est un quotient dans la catégories des A-algèbres ».

Théorème 77. *Soit A un anneau.*

Soit $\iota \colon A \to B$ une A-algèbre, $\mathcal{I}$ un idéal de B, $\pi \colon B \to B/\mathcal{I}$ le morphisme d'anneaux quotient. On considère sur $B/\mathcal{I}$ la structure de A-algèbre donnée par $\pi \circ \iota$. En particulier π est un morphisme de A-algèbres.

Soit C une A-algèbre et $\varphi \colon B \to C$ un morphisme de A-algèbres dont le noyau contient $\mathcal{I}$.

Alors l'unique morphisme d'anneaux $\psi \colon B/\mathcal{I} \to C$ tel que $\psi \circ \pi = \varphi$ est un morphisme de A-algèbres.

En particulier, les théorèmes 47, 48 et 46 restent vrais en remplaçant partout dans les énoncés « anneau » (y compris dans « morphisme d'anneaux ») par « algèbre » (sur un anneau de base fixé).

Démonstration. On pourra s'aider d'un petit diagramme pour appréhender la démonstration.

Notons $\theta \colon A \to C$ la structure de A-algèbre sur C. Le fait que φ soit un morphisme de A-algèbres se traduit par l'égalité de morphismes $\varphi \circ \iota = \theta$.

Par ailleurs, montrer que ψ est un morphisme de A-algèbres revient à montrer l'égalité $\psi \circ \pi \circ \iota = \theta$. Comme $\psi \circ \pi = \varphi$, c'est immédiat. □