Anneaux, idéaux.

1 Premières définitions et premier panorama.

Anneaux

Définition 1 (*Anneau*)

Un anneau est un triplet $(A,+,\times)$ où A est un ensemble, muni de deux lois de composition internes, $+$ et $\times$, telles que

- *$(A,+)$ est un anneau commutatif*
- *$\times$ est associative sur A, et distributive par rapport à l'addition:*

$$\forall (x,y,z)\in A^3,\quad x\times(y+z)=x\times y+x\times z \quad et \quad (y+z)\times x=y\times x+z\times x.$$

Notations: On note 0_A l'élément neutre du groupe $(A,+)$, et $-a$ l'élément inverse de $a\in A$ pour la loi $+$. Lorsque l'anneau possède un élément neutre (noté 1_A) pour la loi $\times$ (i.e. $\exists 1_A\in A$ tel que $\forall a\in A$, $1_A\times a=a$), on dira que l'anneau est *unitaire*. Sauf mention contraire, nous supposerons dans la suite que les anneaux que nous considérerons seront toujours unitaire, et que $1_A\neq 0_A$. Un anneau est dit *commutatif* si la loi $\times$ l'est.

Exemples:
$(\mathbb{Z};+;\times)$ est un anneau unitaire et commutatif. Pour un exemple d'anneau non unitaire, on peut considérer $(2\mathbb{Z};+;\times)$ l'ensemble des entiers pairs.
$(\mathcal{M}_n(\mathbb{R}),+,\times)$ est un anneau unitaire mais non commutatif. Il en est de même de l'anneau $(\mathcal{L}(E);+;\circ)$ où E est un espace vectoriel de dimension finie (ces deux derniers anneaux sont forts semblables: si l'on choisit une base $\mathfrak{B}$ de E, nous avons un isomorphisme naturel de l'un sur l'autre).
Enfin, les précédents anneaux sont de cardinal infini: si l'on souhaite un exemple d'anneau unitaire commutatif mais de cardinal fini, on pourra considérer $(\mathbb{Z}/n\mathbb{Z},+,\times)$.

Exercice: Règle de calcul

1. Montrer que pour tout élément $a\in A$, $0_A\times x=x\times 0_A=0_A$ (un tel élément est dit *absorbant*.
2. Montrer que $(-1_A)\times a=-a$ (on désigne par $-x$ l'opposé de x pour la loi $+$)
3. Montrer que si $|A|\geqslant 2$, alors $1_A\neq 0_A$.

Solution

1. Utilisons la distributivité du produit sur l'addition. Nous avons: $x=(1_A+0_A)\times x=1_A\times x+0_A\times x$ soit en additionnant dans les deux membres par $-x$: $0_A\times x=0_A$.
2. Nous souhaitons montrer que $(-1_A)\times a$ est l'opposé de a: pour ce faire, considérons:

$$(-1_A)\times a+a=(-1_A)\times a+1_A\times a=(-1_A+1_A)\times a=0_A\times a=0_A.$$

3. Supposons que $1_A=0_A$. Alors $\forall a\in A$, $a=1_A\times a=O_A\times a=0_A$, d'où $A=\{0_A\}$. On montre ainsi que si les éléments neutres 0_A et 1_A sont confondus, alors l'anneau A n'a qu'un seul élément.

Proposition 1 (*Formule du binôme de Newton*)

Soit $(A,+,\times)$ un anneau commutatif. Alors, pour tout entier naturel n et tout couple d'élément (x,y) de A^2, nous avons:

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

Démonstration On procède par récurrence sur l'entier n: pour $n=1$, c'est évident. A présent, considérons

la formule vraie au rang $n \geqslant 1$ donné et démontrons-là au rang $n+1$. Nous avons:

$$\begin{array}{ll}(x+y)^{n+1} & = (x+y)\times(x+y)^n = (x+y)\times\left(\sum_{k=0}^n \binom{n}{k}x^k y^{n-k}\right)\\ & = \sum_{k=0}^n \binom{n}{k}x^{k+1}y^{n-k} \ + \ \sum_{k=0}^n \binom{n}{k}x^k y^{n+1-k}\\ & = \sum_{k=1}^{n+1} \binom{n}{k-1}x^k y^{n+1-k} \ + \ \sum_{k=0}^n \binom{n}{k}x^k y^{n+1-k}\\ & = x^{n+1} + \sum_{k=1}^n \left(\binom{n}{k-1}+\binom{n}{k}\right)x^k y^{n+1-k} \ + \ y^{n+1}\\ & = \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}.\end{array}.$$

La formule du binôme de Newton n'est pas vraie dans un anneau non commutatif, comme par exemple l'anneau des matrices $\mathcal{M}_n(\mathbb{R})$, sauf lorsque les matrices A et B commutent.

Eléments inversibles d'un anneau

Dans la suite, nous considérons un anneau $(A,+,\times)$ (sous-entendu un anneau unitaire). On notera 1_A son élément neutre pour la multiplication.

Définition 2 (*Elément inversible*)

On dit que $a \in A$ est inversible (ou encore est une unité de A) si et seulement s'il existe $a' \in A$ tel que $a \times a' = a' \times a = 1_A$.
L'élément a' est dit l'inverse de a dans A. On note $A^\times$ l'ensemble des inversibles de A.

Remarques:

- Puisque $0_A \neq 1_A$ et que 0_A est un élément absorbant, il s'ensuit que 0_A n'est jamais inversible.
- Il ne faut pas confondre $A^\times$ (l'ensemble des éléments inversibles de A) et $A^* = A\setminus\{0_A\}$. Pour certains anneaux, comme $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, ces deux ensembles sont égaux. Dans d'autres cas, par exemple $\mathcal{M}_n(\mathbb{R})$, $\mathbb{R}[X]$, $\mathcal{F}(\mathbb{R};\mathbb{R})$, ces ensembles sont différents!

Exercice: Unicité de l'inverse

Montrer que l'inverse de $a \in A$ est unique.

Solution

Soit $a \in A^\times$, et supposons qu'il existe deux éléments, a' et b vérifiants $aa' = a'a = 1_A$ et $ab = ba = 1_A$. Alors $b = (aa')b = (a'a)b = a'ab = a'$ (on utilise l'associativité du produit dans A), d'où $a' = b$ ce qui implique que l'inverse de a est unique.

Proposition 2 (*Structure de l'ensemble des inversibles d'un anneau*)

L'ensemble $A^\times$, muni du produit $\times$ de l'anneau A est un groupe.

Démonstration Attention: ici on ne peux pas se contenter de montrer que $A^\times$ est un sous-groupe de $(A,\times)$ puisque $(A,\times)$ n'a pas, a priori, de structure de groupes. Il faut donc revenir à la définition d'un groupe. Comme $(A,+,\times)$ est un anneau, la loi $\times$ est associative sur A, donc sur $A^\times$. L'élément $1_A \in A$ est un inversible de A, donc l'ensemble $A^\times$ n'est pas vide. Il nous faut montrer que le produit $\times$ est une loi de composition interne sur $A^\times$. Raisonnons par l'absurde: supposons l'existence de deux éléments $(a,b) \in (A^\times)^2$ tels que $ab = 0$. Alors il existe a' et b' tels que $aa' = a'a = 1_A$ et $bb' = b'b = 1_A$. Alors, $(ab)\times(b'a') = a(bb')a' = aa' = 1$. Or, $(ab)\times(b'a') = 0_A \times (b'a') = 0_A$, d'où $1_A = 0_A$ ce qui apporte la contradiction voulue.
Soit a un élément de $A^\times$. Alors, il existe $a' \in A$ tel que $a \times a' = a' \times a = 1_A$. Il s'ensuit donc que $a' \in A^\times$ et a' est l'inverse de a dans $(A^\times;\times)$. Aussi, tout élément de $A^\times$ admet un inverse (au sens de la loi produit $\times$) dans $A^\times$.
Soient a et b deux éléments de $A^\times$: il existe donc a', b' dans $A^\times$ tels que $aa' = a'a = 1_A$ et $bb' = b'b = 1_A$. Le produit $a \times b$ admet donc pour inverse $b' \times a'$, donc le produit de deux éléments de $A^\times$ est bien un élément de A.

Exercice: Inverse de $\mathbb{R}[X]$

On désigne par $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels et d'inconnu X. On désigne par A un polynôme inversible de $\mathbb{R}[X]$.

1. Rappeler la formule des degrés $deg(P \times Q)$ en fonction de $deg(P)$ et $deg(Q)$.
2. Précisez l'élément neutre pour le produit de $\mathbb{R}[X]$. En déduire que $deg(A) = 0$.
3. Précisez alors $\mathbb{R}[X]^\times$

Solution

1. Nous avons la formule $deg(P \times Q) = deg(P) + deg(Q)$. *Note: Par convention, $deg(0) = -\infty$ (cette convention pour le polynôme nul vient justement du fait de la formule précédente)*
2. L'élément neutre de $\mathbb{R}[X]$ pour le produit est le polynôme constant 1.
   Soit donc A un polynôme inversible de $\mathbb{R}[X]$: aussi, il existe un polynôme B tel que $A \times B = 1$, d'où d'après la formule du degré, nous avons $deg(A \times B) = deg(A) + deg(B) = deg(1) = 0$. Comme le degré de polynôme non nul est toujours à valeurs dans $\mathbb{N}$, nous en déduisons que $deg(A) = deg(B) = 0$ et donc A est un polynôme constant.
3. Nous avons montré dans la question précédente que si A était inversible, alors A était un polynôme constant. Réciproquement, supposons A polynôme constant non nul. Alors $A = k$ admet pour inverse le polynôme constant $B = \frac{1}{k}$ et donc nous en déduisons que les inversibles de $\mathbb{R}[X]$ sont les polynômes constants non nuls, d'où $\mathbb{R}[X]^\times = \mathbb{R}^*$. Aussi, il existe un polynôme B tel que $A \times B = 1_A$.

Définition 3 (*Corps*)

Un anneau $(A, +, \times)$ dont tous les éléments non nul sont inversibles est appelé un corps .

Exemples: $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des exemples de corps (tous unitaire et commutatifs). $(\mathbb{Z}, +, \times)$ lui n'en est pas un (par exemple 2 n'admet pas d'inverse dans $\mathbb{Z}$). De même, $(\mathcal{M}_n(\mathbb{R}), +, \times)$ n'est pas un corps car il existe des matrices non inversibles. Attention, $(\mathcal{G}l_n(\mathbb{R}), +, times)$ n'est pas non plus un corps ($\mathcal{G}l_n(\mathbb{R})$ désigne l'ensemble des matrices carrées $n \times n$ inversibles) en effet, bien que $(\mathcal{G}l_n(\mathbb{R}), \times)$ soit un groupe, $(\mathcal{G}l_n(\mathbb{R}), +)$ n'en est pas un. Par exemple, si 1_n désigne la matrice de l'identité (matrice avec des 1 sur la diagonale et des 0 ailleurs), alors $1_n + (-1_n) = 0_n$: aussi, la somme de deux matrices inversibles n'est pas nécessairement inversible.

Proposition 3 (*Caractérisation des corps par la structure de A)**

Un anneau $(A, +, \times)$ est un corps si et seulement si $(A \setminus \{0\}, \times)$ est un groupe.

Démonstration Si $(A, +, \times)$ est un corps, alors par définition $A^\times = A^* = A \setminus \{0\}$. Or, nous avons prouvé dans une précédente proposition que l'ensemble $A^\times$ des inversibles d'un anneau est un groupe pour le produit: aussi, nous en déduisons que si $(A, +, \times)$ est un corps, alors A^* est un groupe.
Réciproquement, si $(A^*, \times)$ est un groupe, alors tout élément non nul est inversible, donc $A^\times = A^*$ ce qui caractérise donc un corps.

Remarques sur les notations: Dans le cas d'un corps, nous avons $A^\times = A^*$ où A^* désigne l'ensemble $A \setminus \{0\}$. Il faut faire attention à la proximité de ces notations. Nous avons tendance à les employer l'une pour l'autre car nous revenons trop rapidement au cas de $\mathbb{R}$, pour lequel $\mathbb{R}^* = \mathbb{R}^\times$.

Une autre notation délicate: les éléments inversibles d'un anneaux sont aussi appelés ses *unités*. Evidemment, cela ne se réfère pas uniquement à l'élément unité (pour le produit).

Exemples: $\mathbb{Z}^\times = \{-1, 1\}$ donc $(\mathbb{Z}, +, \times)$ n'est pas un corps. A contrario, $\mathbb{R}^\times = \mathbb{R}^*$ donc $(\mathbb{R}, +, \times)$ est un corps. Il en va de même de $\mathbb{Q}$ et de $\mathbb{C}$ par exemple.

Exercice: Caractérisation des $\mathbb{Z}/n\mathbb{Z}$ corps

Dans la suite, n désigne un entier naturel supérieur ou égal à 2. On admet que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau, et on note $\{\overline{0}; \overline{1}; \cdots, \overline{n-1}\}$ les classes de congruence modulo n.
1. Montrer que $(Z/n\mathbb{Z})^\times = \{\overline{k};\ k \wedge n = 1\}$.
2. Montrer que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Solution

1. Pour montrer l'égalité de ces deux ensembles, procédons par double inclusion: La classe de congruence $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il existe une classe $\overline{u}$ de congruence de $\mathbb{Z}/n\mathbb{Z}$ telle que $\overline{k} \times \overline{u} = \overline{1}$. En passant aux congruence, cela implique l'existence d'un entier relatif $v \in \mathbb{Z}$ tel que $k \times u + 1 = v \times n$ soit encore $k \times (-u) + v \times n = 1$. D'après l'identité de Bezout, nous en déduisons alors que k et n sont premiers entre eux.
Montrons à présent l'inclusion réciproque: si $k \wedge n = 1$ alors d'après l'identité de Bezout, il existe deux entiers relatifs u et v tels que $uk + vn = 1$. En considérant alors les classes d'équivalences de cette relation, nous obtenons: $\overline{uk + vn} = \overline{1}$, soit $\overline{u} \times \overline{k} + \overline{v} \times \overline{n} = \overline{1}$. Nous avons donc bien l'égalité de ces deux ensembles.
2. $\mathbb{Z}/n\mathbb{Z}$ est corps si et seulement si tout classe de congruence $\overline{k}$ vérifie $k \wedge n = 1$, donc que n est premier avec tout entier naturel qui lui est strictement inférieur, ce qui implique que n est premier. La réciproque est immédiate.

Notion de diviseurs dans un anneau et anneaux produits

Définition 4 (*Diviseur*)

Soient a et b deux éléments d'un anneau $(A, +, \times)$, avec $b \neq 0_A$. On dit que a est un diviseur de b *s'il existe $c \in A$ tel que $b = a \times c$. On note alors $a|b$.*

De la précédente définition, mettons en évidence que b doit être non nul. Pour la notion de *diviseur de zéro*, nous ajoutons la condition que a et b doivent être non nul; plus précisément:

Définition 5 (*Diviseur de zéro*)

On dit que $a \in A \setminus \{0_A\}$ est un diviseur de zéro *s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = 0_A$.*

Exemple: Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ et $\overline{3}$ sont des diviseurs de zéro. Il est aussi aisé d'en rencontrer dans les anneaux de matrices $\mathcal{M}_n(\mathbb{R})$. A l'inverse, $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$ ou $(\mathbb{C}, +, \times)$ ainsi que l'anneau des polynômes $(\mathbb{K}[X], +, \times)$ sont des anneaux intègres, donc sans diviseurs de zéro.

Exercice: Inversible et diviseur de zéro

Montrer que tout élément inversible de l'anneau A n'est pas un diviseur de zéro.

Solution

Raisonnons par l'absurde: supposons que $a \in A^\times$, $a \neq 0_A$ et a est un diviseur de zéro: il existe donc $b \in A^*$ tel que $a \times b = 0_A$. En multipliant cette égalité par a^{-1} par la gauche, nous obtenons que $(a'a) \times b = 1_A \times b = b = 0_A$, ce qui contredit le fait que $b \in A^* = A \setminus \{0_A\}$.

Définition 6 (*Anneau intègre*)

Un anneau est dit intègre *(ou un* domaine d'intégrité*) s'il n'admet pas de diviseur de zéro.*

Exemple: L'anneau $(\mathbb{Z}; +; \times)$ est un anneau intègre. On peut remarquer que l'exercice montrant que tout inversible n'est pas un diviseur de zéro implique que tout corps est un anneau intègre.

Remarque: Il faut ici se méfier de nos habitudes dans $\mathbb{R}$: nous avons souvent tenu le raisonnement suivant: si le produit $a \times b$ est nul, alors l'un des deux termes est nul. La structure *intègre* était donc sous-jaçente. Pourtant, il existe de nombreux anneaux usuels non intègres: matrices, fonctions, classes de congruences ...

Structure d'anneau produit

Etant donné n ensembles, nous savons construire le produit cartésien $\prod_{i=1}^n A_i = A_1 \times A_2 \times \cdots \times A_n$, formé par tous les n-uplets d'éléments de $(A_i)_{1 \leqslant i \leqslant n}$. Nous avons vu la structure de groupe produit de deux groupes $G_1 \times G_2$. Nous définissons de même, lorsque les A_i sont des anneaux, le structure d'anneaux produit sur le produit cartésien $\prod_{i=1}^n A_i$.

Définition 7 (*Structure produit d'anneaux*)

Soient $A_1, A_2, \cdots, A_n$ des anneaux. On définit les loi $+$ et $\times$ sur $A_1 \times A_2 \times \cdots \times A_n$ par $(x_1, x_2, \cdots, x_n) + (x'_1, x'_2, \cdots, x'_n) = (x_1 + x'_1, x_2 + x'_2, x_3 + x'_3, \cdots, x_n + x'_n)$ et $(x_1, x_2, \cdots, x_n) \times (x'_1, x'_2, \cdots, x'_n) = (x_1 \times x'_1, x_2 \times$

$x'_2, \cdots, x_n \times x'_n)$. *Muni de ces deux lois,* $\prod_{i=1}^n A_i$ *est un anneau unitaire.*

Dans la précédente construction, on peut voir que l'élément neutre pour l'addition ainsi définie est l'élément $(0_{A_1}, 0_{A_2}, \cdots, 0_{A_n})$, et que l'élément neutre pour la multiplication est l'élément $(1_{A_1}, 1_{A_2}, \cdots, 1_{A_n})$.

Proposition 4 (*Attention!*)

Le produit de deux anneaux intègres n'est pas un anneau intègre.

Démonstration Il suffit de remarquer que $(0_{A_1}; 1_{A_2}) \times (1_{A_1}; 0_{A_2}) = (0_{A_1}; 0_{A_2})$, donc le produit de deux anneaux admet nécessairement des diviseurs de zéros.

Sous et sur-structures d'un anneau

Définition 8 (*Sous-anneau*)

Soit $(A, +, \times)$ *un anneau. Une partie* $B \subset A$ *de* A *est un sous-anneau de* $(A, +, \times)$ *si* $(B, +, \times)$ *est un sous-anneau.*

Proposition 5 (*Caractérisation pratique d'un sous-anneau*)

B est un sous-anneau de A si $1_A \in B$, $(B, +)$ *est un sous-groupe de* $(A, +)$ *et* $\forall (x, y) \in B^2$, $x \times y \in B^2$.

Exemples: $(\mathbb{Z}; +; \times)$ est un sous anneau de $(\mathbb{Q}, +, \times)$, qui est lui-même un sous-anneau de $(\mathbb{R}, +, \times)$ qui est lui-même un sous-anneau de $(\mathbb{C}, +, \times)$.

Définition 9 (*Homomorphisme*)

Soient $(A, +, \times)$ *et* $(A', +, \times)$ *deux anneaux, et* $\varphi : A \to A'$. *On dit que* φ *est un* morphisme d'anneaux *(ou* homomorphisme d'anneaux*) si* φ *est une application à la fois additive et multiplicative, c'est-à-dire si elle vérifie:*

$$\forall (x, y) \in A^2, \quad \varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{et} \quad \varphi(x \times y) = \varphi(x) \times \varphi(y).$$

Nous devons aussi avoir: $\varphi(1_A) = A_{A'}$.

Exercice: Propriété d'un morphisme d'anneaux

Montrer que si $\varphi : A \to A'$ est un morphisme d'anneaux, alors nécessairement $\varphi(0_A) = 0_{A'}$.
Pourquoi n'a-t'on pas la même propriété pour 1_A?

Solution

Si φ est un morphisme d'anneaux de $(A, +, \times)$ dans $(A', +,)$, alors $\forall (x, y) \in A^2$, $\varphi(x + y) = \varphi(x) + \varphi(y)$. Aussi, en considérant $y = 0_A$, nous obtenons que $\varphi(\underbrace{x + 0_A}_{=x}) = \varphi(x) + \varphi(0_A)$. Il s'ensuit alors, par unicité de l'élément neutre du groupe $(A', +)$, que $\varphi(0_A) = 0_{A'}$.
On ne peut pas faire de même avec l'unité 1_A. En effet, nous avons $\forall x \in A$, $\varphi(\underbrace{1_A \times x}_{=x}) = \varphi(1_A) \times \varphi(x)$. A ce niveau, on ne peut rien dire! En effet, pour simplifier, il faudrait multiplier par l'inverse de $\varphi(x)$, mais celui-ci n'existe pas nécessairement dans $(A, +, \times)$.

Proposition 6 (*Structure de l'image d'un morphisme*)

Soit $\varphi : A \to A'$ *un morphisme d'anneau. Alors* $\mathfrak{Im}(\varphi)$ *est un sous-anneau de* $(A', +, \times)$.

Démonstration Comme A et A' sont des anneaux unitaires et φ morphisme d'anneaux, il s'ensuit que $\varphi(1_A) = 1_{A'}$. $(A, +)$ et $(A', +)$ étant deux groupes et φ étant a fortiori un morphisme de groupe, nous en déduisons que $\mathfrak{Im}(\varphi)$ est un sous-groupe de A'. Reste à montrer que $\mathfrak{Im}(\varphi)$ est stable par produit: soient donc $z, z' \in \mathfrak{Im}(\varphi)$. Ainsi, il existe $x, x' \in A$ tel que $z = \varphi(x)$ et $z' = \varphi(x')$. Alors comme φ est multiplicative, nous avons $\varphi(x \times x') = \varphi(x) \times \varphi(x')$ d'où le produit $z \times z' \in \mathfrak{Im}(\varphi)$. Il s'ensuit donc que $\mathfrak{Im}(\varphi)$ est un sous-anneau de $(A', +, \times)$.

Théorème 1 (*Sur-structure d'un anneau*)

Soit $(A,+,\times)$ un anneau commutatif intègre. Alors, il existe $(\mathbb{K},+,\times)$ un corps tel que A soit un sous-anneau de $(\mathbb{K},+,\times)$ et $\forall x\in\mathbb{K}$, $\exists u\in A$ tel que $u\times x\in A$.

La démonstration de ce théorème est constructiviste et est calquée sur la construction du corps $\mathbb{Q}$ en partant de l'anneau $\mathbb{Z}$. Donnons le plan de la démonstration: déjà, on définit une relation d'équivalence $\mathcal{R}$ sur $A\times A^\times$. Ensuite, on définit deux lois internes associatives, $+$ et $\times$ compatibles avec la relation d'équivalence $\mathcal{R}$. On vérifie alors que $\times$ est distributives sur $+$. On peut alors définir une structure d'anneau sur $\mathbb{K}=A\times A^\times/\mathcal{R}$, et on montre que cet anneau est un corps. Enfin, on identifie les éléments de A aux éléments de $\mathbb{K}$ de la forme $(a,1)$.

Démonstration Définissons $A\times A^\times$ la relation $\mathcal{R}$ par $(x,y)\mathcal{R}(u,v)$ si $a\times v=b\times u$. Il est aisé de vérifier que $\mathcal{R}$ est une relation d'équivalence.
Définissons alors sur $A\times A^\times$ les lois internes suivantes:

$$\forall (a,b),(u,v)\in A\times A^\times,\quad (a,b)+(u,v)=(av+bu;bv),\quad (a,b)\times(u,v)=(au;bv).$$

On vérifie que se sont bien des lois internes sur $A\times A^\times$ car puisque b et v sont non nuls, il s'ensuit que $bv\neq 0$ (puisque A est intègre).
On vérifie alors que ces deux opérations sont compatibles avec la relation d'équivalence $\mathcal{R}$, c'est-à-dire que si $(a,b)\mathcal{R}(a',b')$ alors $\forall (u,v)\in A\times A^\times$, $(a,b)+(u,v)=(a',b')+(u,v)$ et $(a,b)\times(u,v)=(a',b')\times(u,v)$. Aussi, la somme et le produit de deux classes d'équivalences pour la relation $\mathcal{R}$ ne dépendent pas du représentant choisi dans sa classe.
On vérifie aussi que ces deux opérations admettent pour élément neutre $(0,1)$ et $(1,1)$ respectivement pour l'addition et la multiplication. Enfin, l'addition et la multiplication sont des lois commutatives et la multiplication est distributive sur l'addition. Aussi, peut-on munir le quotient $\mathbb{K}=A\times A^\times/\mathcal{R}$ d'une structure d'anneaux.
Il reste donc à montrer que $\mathbb{K}$ est un corps: on remarque alors que l'inverse de l'élément (a,b) est l'élément (b,a), d'où tout élément non nul est inversible.
Enfin, pour montrer que A s'injecte naturellement dans $\mathbb{K}$, considérons l'application $A\to\mathbb{K}$ définie par $a\mapsto(a,1)$. Il s'ensuit donc que A s'identifie bien à un sous-anneau de $(\mathbb{K},+,\times)$.

2 Ideaux et anneaux quotients

Introduction informelle Dans les groupes, nous avons vu que l'image directe et l'image réciproque de sous groupes par des morphismes de groupes sont des sous-groupes. Dans le cadre des anneaux, nous allons voir qu'une autre notion semble pertinente pour l'étude du Ker de morphisme d'anneaux: il s'agit de la notion d'idéal.

Proposition 7 (*Noyau d'un morphisme d'anneaux*)

Soit $\varphi:A\to A'$ un morphisme d'anneau, et $\mathfrak{K}$ son noyau. Alors, $\mathfrak{K}$ est un sous-groupe de A vérifiant: $\forall a\in A$ et $\forall k\in\mathfrak{K}$, $ak\in\mathfrak{K}$ et $ka\in\mathfrak{K}$.

Démonstration En effet, si $k\in\mathfrak{K}$ et $a\in A$, alors $\varphi(ak)=\varphi(a)\varphi(k)=0$ et de même pour $\varphi(ka)=0$. Aussi, il s'ensuit que $ak\in\mathfrak{K}$ et $ka\in\mathfrak{K}$.

Fort de cette remarque, définissons donc cette nouvelle structure et étudions-là:

Définition 10 (*Idéal*)

Soit $(A,+,\times)$. Une partie $\mathfrak{I}\subset A$ de A est un idéal à gauche de l'anneau $(A,+,\times)$ si $(\mathfrak{I},+)$ est un sous-groupe de $(A,+)$ et si $\forall x\in\mathfrak{I}$ et $\forall a\in A$, $a\times x\in\mathfrak{I}$.
On dit que $\mathfrak{I}$ est un idéal de droite de A si $(\mathfrak{I};+)$ est un sous-groupe de $(A,+)$, et si $\forall a\in A$, $\forall x\in\mathfrak{I}$, $x\times a\in\mathfrak{I}$.
Enfin, $\mathfrak{I}$ est un idéal bilatère de A si c'est à la fois un idéal à gauche et à droite de $(A,+,\times)$.

Sauf mention explicite, dans la suite, nous ne considérerons que des idéaux bilatères: aussi, lorsque l'on ne précisera rien sur l'idéal, il devra être considéré comme bilatère par défaut.
Exemples: Comme usuellement, $\{0_A\}$ et A lui-même sont toujours des idéaux de l'anneau $(A,+,\times)$, appelés *idéaux triviaux de A*.

Exercice: Caractérisation des idéaux de $(\mathbb{Z};+;\times)$

On admet dans cet exercice que $(\mathbb{Z};+;\times;\leqslant)$ est un anneau ordonné et qu'il est muni d'une division euclidienne.
1. Montrer que les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$ où $n\in\mathbb{N}$ (on pourra considérer le plus petit élément strictement positif, s'il existe, d'un tel sous-groupe).
2. Montrer que les idéaux de $(\mathbb{Z},+,\times)$ sont aussi les $n\mathbb{Z}$, $n\in\mathbb{N}$.

Solution

Considérons donc H un sous-groupe de $(\mathbb{Z},+)$. Soit $H=\{0\}$ (et alors $n=0$), soit il existe $\alpha\in H$ avec $\alpha\neq 0$. Comme H est un sous-groupe, $-\alpha\in H$, donc quitte à échanger les rôles de α et de son opposé, on peut toujours considéré que $\alpha>0$. Considérons alors n le plus petit entier naturel de l'ensemble $H\cap\mathbb{N}^*$ (cet ensemble est non vide car il contient α et tout ensemble non vide de $\mathbb{N}$ admet un plus petit élément). Montrons que $H=n\mathbb{Z}$. Comme H est un sous-groupe contenant n, nous en déduisons que $nZ\subset H$. Montrons l'inclusion réciproque: soit $h\in H$. Effectuons la division euclidienne de h par n: $\exists!(q,r)\in\mathbb{Z}^2$ tel que $h=nq+r$ et $0\leqslant r<n$, donc $0\leqslant \underbrace{r=h-nq}_{\in H}<n$, ce qui implique que $r=0$ puisque n est le plus petit élément de $H\cap\mathbb{N}^*$. On a bien démontré notre affirmation.
2. Les idéaux de $\mathbb{Z}$ sont à chercher parmis les sous-groupes de $\mathbb{Z}$: ici, on veut montrer que tout sous-groupe de $\mathbb{Z}$ est un idéal. Pour ce faire, il suffit de remarquer que le produit d'un multiple de n par un entier naturel est un multiple de n.

Exercice: Opérations ensemblistes conservant la notion d'idéal

Soient $\mathfrak{I}_1$ et $\mathfrak{I}_2$ deux idéaux de $(A,+,\times)$.
Montrer que $\mathfrak{I}_1+\mathfrak{I}_2$ et $\mathfrak{I}_1\cap\mathfrak{I}_2$ sont des idéaux de $(A,+,\times)$.

Solution

On vérifie déjà que $\mathcal{I}_1+\mathcal{I}_2=\{i_1+i_2|i_1\in\mathcal{I}_1,i_2\in\mathcal{I}_2\}$ est un sous-groupe de $(A,+)$. Ensuite, reste à montrer que le produit de tout élément a de A par un élément de $\mathcal{I}_1+\mathcal{I}_2$ est un élément de $\mathcal{I}_1+\mathcal{I}_2$, ce qui résulte de la définition d'un idéal: en effet, si $a\in A$ et $x_1+x_2\in\mathcal{I}_1+\mathcal{I}_2$, nous avons $a\times(x_1+x_2)=\underbrace{a\times x_1}_{\in\mathcal{I}_1}+\underbrace{a\times x_2}_{\in\mathcal{I}_2}\in\mathcal{I}_1+\mathcal{I}_2$.
Pour $\mathcal{I}_1\cap\mathcal{I}_2$, nous savons déjà qu'il s'agit d'un sous-groupe de $(A,+)$ comme intersection de deux sous-groupes de $(A,+)$. La stabilité de $\mathcal{I}_1\cap\mathcal{I}_2$ par produit avec un élément de A résulte de là encore de la définition des idéaux: si $a\in A$ et $x\in\mathcal{I}_1\cap\mathcal{I}_2$ alors de $x\in\mathcal{I}_1$ nous déduisons que $ax\in\mathcal{I}_1$ et de $x\in\mathcal{I}_2$ nous déduisons que $ax\in\mathcal{I}_2$. Il s'ensuit alors que $ax\in\mathcal{I}_1\cap\mathcal{I}_2$.

Définition 11 (*Idéal engendré par une partie*)

Soit P une partie de A. On appelle idéal de $(A,+,\times)$ engendré par la partie P le plus petit idéal (au sens de l'inclusion) contenant P. On ne note (P).

Comme usuellement, on montre que l'idéal engendré par une partie est l'intersection de tous les idéaux contenant cette partie. On peut la caractériser différemment: c'est aussi l'ensemble des combinaisons linéaires à coefficients dans A d'éléments de P, c'est-à-dire que si $P=\{x_1,\cdots,x_n\}$, alors $(P)=\{\lambda_1x_1+\cdots+\lambda_nx_n;\ (\lambda_1;\cdots,\lambda_n)\in A^n\}$.

Proposition 8 (*Etude du cas d'égalité $(x)=A$*)

L'idéal engendré par l'élément $x\in A$ est égal à A si et seulement si $x\in A^\times$.

Démonstration Déjà, remarquons que si $\mathcal{I}$ est un idéal de A contenant 1_A, alors $\mathcal{I}=A$ (cela résulte de la stabilité par produit par un élément de A). Aussi, l'idéal (x) est égal à A si et seulement si $1\in(x)$, ce qui implique qu'il existe $y\in A$ tel que $xy=1$, ce qui est équivalent à $x\in A^\times$.

Remarque: C'est à retenir: pour montrer qu'un idéal $\mathcal{J}$ est égal à l'anneau A tout entier, il suffit de prouver que $\mathcal{J}$ contient un élément inversible de A (souvent, on montre que $1_A\in\mathcal{J}$).

3 Anneau quotient $A/\mathcal{I}$

Puisque $\mathcal{I}$ est un idéal de A, c'est en particulier un sous-groupe du groupe commutatif $(A,+)$, donc il est nécessairement distingué (car tout sous-groupe d'un groupe commutatif est distingué). Il s'ensuit donc, d'après ce que nous avons vu dans la partie groupe, que $A/\mathcal{I}$ admet une structure de groupe (héritée de celle de $(A,+)$). A présent, nous allons munir le groupe $(A/\mathcal{I};+)$ d'une loi multiplicative.

Les éléments de $A/\mathcal{I}$ sont les classe $a+\mathcal{I}$. On définit donc $(a+\mathcal{I})\times(b+\mathcal{I}) = \{ab+ay+xb+xy; x,y\in\mathcal{I}\} \subset ab+\mathcal{I}$. On définit donc $(a+\mathcal{I})\times(b+\mathcal{I}) = ab+\mathcal{I}$ (on vérifie que cette définition de dépend pas du représentant choisit dans la classe mais seulement de la classe elle-même).

Proposition 9 (*Image directe et image réciproque d'un idéal par un morphisme*)

Soit $\varphi : A \to A'$ un morphisme d'anneaux, et soient $\mathcal{I}$ et $\mathcal{I}'$ deux idéaux respectivement de $(A,+,\times)$ et $(A',+,\times)$. Alors:
$\varphi^{-1}(\mathcal{I}')$ est un idéal de $(A,+,\times)$.
Si φ est **surjectif**, *$\varphi(\mathcal{I})$ est un idéal de $(A',+,\times)$.*

Démonstration Si $\mathcal{I}'$ est un idéal de A', alors $\varphi^{-1}(A')$ est un sous-groupe de A comme image réciproque d'un sous-groupe par un morphisme de groupe (un morphisme d'anneaux étant en particulier un morphisme de groupes). Reste donc à montrer que $\varphi^{-1}(\mathcal{I})$ est stable par produit par un élément de A: soit donc $a\in A$ et $x\in\varphi^{-1}(\mathcal{I})$. On a donc $\varphi(ax)=\varphi(a)\varphi(x)\in\mathcal{I}'$ d'où $ax\in\varphi^{-1}(\mathcal{I}')$.
Soit $\mathcal{I}$ un idéal de A et φ un morphisme **surjectif** d'anneaux de A dans A'. Alors nous savons déjà que $\varphi(\mathcal{I})$ est un sous-groupe de A' comme image directe d'un sous-groupe de A par un morphisme de groupes. Reste donc à montrer que $\varphi(\mathcal{I})$ est stable par le produit par un élément de A'. Soit donc $y\in A'$ et $x\in\mathcal{I}$. Comme φ est surjectif, on en déduit l'existence de $x'\in A$ tel que $y=\varphi(x')$. Aussi: $y\varphi(x)=\varphi(x')\varphi(x)=\varphi(\underbrace{x'x}_{\in\mathcal{I}})\in\varphi(\mathcal{I})$.

Proposition 10

Soit $\varphi : A\to A'$ un morphisme d'anneaux et soit $\mathcal{I}$ un idéal de $(A,+,\times)$ qui soit contenu dans $Ker(\varphi)$. Alors il existe un unique morphisme $\psi : A/\mathcal{I}\to A'$ tel que $\varphi=\psi\circ p$ où p est l'homomorphisme canonique de A dans $A/\mathcal{I}$. Aussi, nous avons le diagramme commutatif:

$$\begin{array}{ccc} A & \overset{\varphi}{\to} & A' \\ \downarrow & \nearrow & \\ A/\mathcal{I} & & \end{array} .$$

Démonstration Définissons ψ par $\psi(x+\mathcal{I})=\varphi(x)$. Montrons que cette formule de dépend pas du représentant choisit: si $x+\mathcal{I}=x'+\mathcal{I}$ on a, par hypothèse, $\varphi(x)=\varphi(x')$ puisque $x=x'+\alpha$ avec $\alpha\in\mathcal{I}\subset Ker(\varphi)$. Reste à présent à vérifier que ψ est un homomorphisme.

$$\psi(x+\mathcal{I}+x'+\mathcal{I})=\psi(x+x'+\mathcal{I})=\varphi(x)+\varphi(x')=\psi(x+\mathcal{I})+\psi(x'+\mathcal{I})$$

De même pour le produit:

$$\psi((x+\mathcal{I})\times(x'+\mathcal{I}))=\psi(xx'+\mathcal{I})=\varphi(xx')=\varphi(x)\varphi(x')=\psi(x+\mathcal{I})\psi(x'+\mathcal{I}).$$

Enfin, l'unicité de l'application ψ provient de la surjectivité de p.

On déduit en particulier du précédent théorème le théorème de factorisation pour les morphismes d'anneaux (en prenant $\mathcal{I}=Ker(\varphi)$).

Dans la suite, nous noterons $\overline{x}$ la classe modulo l'idéal $\mathcal{I}$ de l'élément $x+\mathcal{I}$. Ainsi, $\overline{x}$ désignement la classe $x+\mathcal{I}$ de l'anneau quotient $A/\mathcal{I}$. On remarquera que $\overline{0}$ désigne alors l'idéal $\mathcal{I}$ lui-même.

Caractérisation des propriétés des idéaux en terme d'anneau quotient

Définition 12 (*Idéal premier*)

Un idéal $\mathcal{I}$ de l'anneau $(A,+,\times)$ est un idéal premier *si pour tout $x,y\in A$, la condition $xy\in\mathcal{I}$ implique $x\in\mathcal{I}$ ou $y\in\mathcal{I}$.*

Proposition 11 (*Caractérisation des anneaux principaux à l'aide des anneaux quotients*)

Un idéal $\mathcal{I}$ de l'anneau $(A,+,\times)$ est un idéal premier de $(A,+,\times)$ si et seulement si l'anneau quotient $A/\mathcal{I}$ est intègre.

Démonstration Supposons déjà le quotient $A/\mathcal{I}$ intègre, et soient x, y deux éléments de A tels que $\overline{x}\times\overline{y}=\overline{0}$. Alors $xy\in\mathcal{I}$. Or, l'anneau quotient $A/\mathcal{I}$ étant intègre, nous avons donc $\overline{x}=\overline{0}$ (i.e. $x\in\mathcal{I}$) ou $\overline{y}=\overline{0}$ (i.e. $y\in\mathcal{I}$). On en déduit donc que $\mathcal{I}$ est premier.

Réciproquement, supposons $\mathcal{I}$ premier. Alors soient $\overline{x}$ et $\overline{y}$ deux éléments de $A/\mathcal{I}$ tel que le produit $\overline{x}\times\overline{y}$ soit nul. On a donc $xy\in\mathcal{I}$ et comme $\mathcal{I}$ est premier, on en déduit que soit $x\in\mathcal{I}$ (et alors $\overline{x}=\overline{0}$) ou $y\in\mathcal{I}$ (et alors $\overline{y}=\overline{0}$). Il s'ensuit donc que $\mathcal{I}$ est un anneau intègre.

Définition 13 (*Idéal maximal*)

Un idéal $\mathcal{I}$ de l'anneau $(A,+,\times)$ distinct de A. L'idéal $\mathcal{I}$ est dit maximal *s'il n'existe pas d'idéal $\mathcal{J}$ différent de $\mathcal{I}$ et de A tel que l'on ai l'inclusion $\mathcal{I}\subset\mathcal{J}$.*

Les idéaux maximaux d'un anneau sont des les idéaux stricts de A (i.e. non égaux à A) maximaux au sens de l'inclusion.

■■■ Exercice: Idéaux maximaux d'un ensemble de fonctions

On considère l'ensemble $\mathcal{C}([0;1],\mathbb{R})$ des fonctions continues sur $[0;1]$ et à valeurs réelles et x un réel fixé de l'intervalle $[0;1]$.
Soit $I_x=\{f\in\mathcal{C}([0;1];\mathbb{R})|f(x)=0\}$.

1. Montrer que I_x est un idéal maximal de $\mathcal{C}([0;1],\mathbb{R})$.
2. Soit $\mathfrak{I}$ un idéal maximal de $\mathcal{C}([0;1],\mathbb{R})$. Montrer qu'il existe $x\in[0;1]$ tel que $\mathfrak{I}=I_x$.

Solution

1. Montrons déjà que I_x est un idéal de l'anneau $(\mathcal{C}([0;1],\mathbb{R});+;\times)$. Pour ce faire, montrons déjà que I_x est un sous-groupe de $(\mathcal{C}([0;1],\mathbb{R})+)$. I_x est non vide puisqu'il contient la fonction nulle (élément neutre du groupe additif $(\mathcal{C}([0;1],\mathbb{R});+;\times)$). Si f est une fonction s'annulant en x alors la fonction opposée $-f$ s'annule aussi en x. Enfin, si f et g sont deux fonctions continues s'annulant en x, alors la fonction somme $f+g$ est aussi continue et s'annule en x, d'où I_x est bien un sous groupe du groupe additif $(\mathcal{C}([0;1],\mathbb{R});+)$.
   A présent, montrons que c'est un idéal: considérons donc $f\in I_x$ et $g\in\mathcal{C}([0;1],\mathbb{R})$. Alors la fonction produit $f\times g$ est aussi continue et s'annule en x donc $g\times g\in I_x$. Aussi, I_x est bien un idéal de $(\mathcal{C}([0;1],\mathbb{R});+;\times)$.
   Montrons que I_x est un idéal maximal de cet anneau: pour ce faire, considérons $\mathfrak{F}$ un idéal contenant strictement I_x. Aussi, il existe $f\in\mathfrak{I}\setminus I_x$, donc la fonction f ne s'annule pas en x. Aussi, la fonction $\frac{f}{f(x)}$ est dans $\mathfrak{I}$ (comme produit de la fonction $f\in\mathfrak{I}$ avec la fonction constante $\frac{1}{f(x)}$). Or, la fonction $1-\frac{f}{f(x)}$ s'annule en x, donc est un élément de I_x. Il s'ensuit que la fonction constante 1 appartient à $\mathfrak{I}$ comme somme de deux fonctions de $\mathfrak{I}$: la fonction $\frac{f}{f(x)}\in\mathfrak{I}$ et la fonction $1-\frac{f}{f(x)}\in I_x\subset\mathfrak{I}$. Aussi, puisque $1\in\mathfrak{I}$, nous en déduisons que $\mathfrak{I}=\mathcal{C}([0;1],\mathbb{R})$ ce qui implique que l'idéal I_x est maximal.
2. Raisonnons par l'absurde en supposant que $\forall x\in[0;1]$, $\mathfrak{I}\neq I_x$ c'est-à-dire qu'il existe une fonction $f_x\in\mathfrak{I}$ tel que $f_x(x)\neq 0$. Par continuité des fonctions f_x sur $[0,1]$, il existe un voisinage $\mathcal{V}_x$ ouvert de x sur lequel la fonction f ne s'annule pas. Ainsi, nous obtenons $\{\mathcal{V}_x, x\in[0,1]\}$ un recouvrement de l'intervalle $[0;1]$ par des ouverts. Or, $[0;1]$ étant compact, on peut extraire un sous-recouvrement fini: soit $x_1,\cdots,x_n\in[0;1]$ tel que $\{\mathcal{V}_{x_i}, 1\leqslant i\leqslant n\}$ soit un recouvrement fini de $[0;1]$. Les fonctions f_{x_i} étant dans $\mathfrak{I}$, les fonction $f_{x_i}^2$ le sont aussi, et la fonction $\sum_{i=1}^n f_{x_i}^2$ aussi, puisque $\mathfrak{I}$ est un idéal (dont sous-groupe). Il reste à remarquer que cette fonction ne s'annule pas sur $[0;1]$, donc qu'elle admet un inverse dans $\mathcal{C}([0;1],\mathbb{R})$. Aussi, la fonction constante 1 appartient à $\mathfrak{I}$, et donc $\mathfrak{I}=\mathcal{C}([0;1],\mathbb{R})$ ce qui contredit la maximalité de l'idéal $\mathfrak{I}$.

Proposition 12 (*Caractérisation des idéaux à l'aide des anneaux quotients*)

Un idéal $\mathcal{I}$ de $(A,+,\times)$ est dit maximal si et seulement si l'anneau quotient $A/\mathcal{I}$ est un corps.

Démonstration Supposons déjà que l'anneau quotient $A/\mathcal{I}$ est un corps, et considérons un idéal $\mathcal{J}$ contenant strictement $\mathcal{I}$. Montrons alors que $\mathcal{J}=A$. Puisque $\mathcal{I}\subsetneq\mathcal{J}$, il existe $x\in\mathcal{J}\setminus\mathcal{I}$. Aussi, $\overline{x}\neq\overline{0}$, donc est un inversible du corps $A/\mathcal{I}$: il existe donc $\overline{y}\in A/\mathcal{I}$ tel que $\overline{xy}=\overline{1}$ d'où $\exists u\in\mathcal{I}$ tel que $xy=1+u$. Par suite, $xy-u\in\mathcal{J}$ et donc $1\in\mathcal{J}$ et donc $\mathcal{J}=A$.

Réciproquement, supposons $\mathcal{I}$ idéal maximal de A. Soit alors $\overline{x}\neq\overline{0}$, c'est-à dire que $x\notin\mathcal{I}$. Le plus petit idéal contenant à la fois l'idéal $\mathcal{I}$ et l'élément x est donc A puisque $\mathcal{I}$ est maximal. Aussi, puisque cet idéal est constitué des éléments de la forme $ax+u$ avec $a\in A$ et $u\in\mathcal{I}$, nous en déduisons qu'il existe $a\in A$ et $u\in\mathcal{I}$ tel que $ax+u=1$, d'où en passant à la classe modulo l'idéal $\mathcal{I}$ nous obtenons que $\overline{ax}=\overline{1}$ (car $u\in\mathcal{I}$ donc $\overline{u}=\overline{0}$). Il s'ensuit alors que $\overline{a}\times\overline{x}=\overline{1}$ et donc la classe de tout élément non nul est inversible, d'où $A/\mathcal{I}$ est un corps.

Exemple: Les idéaux maximaux de $\mathbb{Z}$ sont des idéaux (p) où p est un nombre premier.

Remarquons qu'un corps est nécessairement un anneau intègre: aussi, nous en déduisons par les théorèmes précédents que si $\mathcal{I}$ est maximal, alors $\mathcal{I}$ est premier.
La réciproque n'est pas vraie. Par exemple, $(\mathbb{Z};+;\times)$ est un anneau intègre qui n'est pas un corps.

4 Anneaux principaux.

Rappel sur les polynômes

On désigne dans la suite par $\mathbb{K}$ un corps commutatif. **Ensemble des polynômes en une indéterminée**

Une suite $(a_k)_{n\in\mathbb{K}}$ est dite *presque nulle* si il n'existe qu'un nombre fini d'indice $k\in\mathbb{N}$ tel que $a_k\neq 0$. Soit $(a_k)_{k\in\mathbb{N}}$ une telle suite: si d est le plus grand indice de la suite $(a_k)_{k\in\mathbb{N}}$ dont le terme est non nul, on note alors $P(X)=\sum_{k=0}^{d}a_kX^k$. On désigne donc par $\mathbb{K}[X]$ l'ensemble des suites presques nulles d'éléments de $\mathbb{K}$, et on appelle ses éléments les *polynômes à une indéterminée et à coefficients dans* $\mathbb{K}$.
On peut munir $\mathbb{K}[X]$ d'une somme (héritée de la structure des suites) $\mathbb{K}^n$ de sorte que $(\mathbb{K}[X],+)$ soit un groupe commutatif. On définit alors le produit de deux polynômes, appelé produit de Cauchy, de la manière suivante: si $P(X)=\sum_{k=0}^{n}a_kX^k$ et $Q(X)=\sum_{k=0}^{m}b_kX^k$, nous avons alors $PQ(X)=\sum_{k=0}^{n+m}c_kX^k$ où $c_k=\sum_{j=0}^{k}a_jb_{k-j}$.
Muni de ces deux lois, on montre que $(\mathbb{K}[X],+,\times)$ est un anneau unitaire commutatif intègre.

Degré d'un polynôme

On appelle *degrè* du polynôme P le plus grand indice $k\in\mathbb{N}$ tel que $a_k\neq 0$. On pose par convention $deg(0)=-\infty$.
Nous avons les formules:
$deg(P+Q)\leqslant Max(deg(P);deg(Q))$ et $deg(P\times Q)=deg(P)\times deg(Q)$.

Division euclidienne dans $\mathbb{K}[X]$

Théorème 2 (*Division euclidienne dans* $\mathbb{K}[X]$)

L'application degré permet de munir l'anneau $(\mathbb{K}[X],+,\cdot)$ d'une division euclidienne.

Démonstration Déjà, l'anneau $\mathbb{K}[X]$ est nécessairement intègre puisque si $PQ=0$, alors $deg(PQ)=-\infty$ ce qui implique que $deg(P)=-\infty$ ou $deg(Q)-\infty$ et donc que $P=0$ ou $Q=0$.
A présent, montrons que l'application deg permet de munir $\mathbb{K}[X]$ d'une structure d'anneau euclidien. Soient A,B deux polynômes avec $B\neq 0$. Si $deg(A)<deg(B)$ alors $Q=0$ et $R=A$ convient. Sinon, on procède par récurrence sur $deg(A)\geqslant deg(B)$ en remarquant que le polynôme $A-\frac{coef(A)}{coef(B)}B$ est un polynôme de degré $deg(A)-1$. Ainsi, par hypothèse de récurrence, il existe un unique couple $(\tilde{Q},\tilde{R})$ de $\mathbb{R}[X]$ tel que $A-\frac{coef(A)}{coef(B)}B=\tilde{Q}B+\tilde{R}$ d'où $A=\left(\frac{coef(A)}{coef(B)}+\tilde{Q}\right)B+\tilde{R}$. On démontre ainsi que $\mathbb{K}[X]$ est muni d'une division euclidienne.

Exercice: Reste de la division euclidienne d'un polynôme par un polynôme de degré 1.

Soit $P\in\mathbb{K}[X]$ et $\alpha\in\mathbb{K}$. Quel est le reste de la division euclidienne de P par $(X-\alpha)$?

Solution

Effectuons donc la division euclidienne de P par $(X-\alpha)$. Il exsite donc un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que $P(X)=Q(X)\times(X-\alpha)+R(X)$ avec $deg(R)<deg(X-a)=1$. Aussi, R est un polynôme constant:

pour en connaitre la valeur, evaluons l'expression précédente en α: nous obtenons alors $R(\alpha) = P(\alpha)$. Aussi, le reste de la division euclidienne de P par $(X-\alpha)$ est $P(\alpha)$.

Racine d'un polynôme

Dans ces rappels, nous redonnons les deux définitions équivalentes de ce qu'est une racine: cela est plus glissant qu'il n'y parait, car on passe ici de la notion (algébrique) de *polynôme* à celle (analytique) de *fonction polynômiale*. Lorsque $\mathbb{K}$ est un corps infini, cela ne pose pas de problème, mais lorsque $\mathbb{K}$ est un corps fini (par exemple $\mathbb{Z}/5\mathbb{Z}$), ces deux notions ne peuvent être confondues. Aussi dans ce petit paragraphe, nous considérerons que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 14 (*Racine d'un polynôme*)

Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine *de P si $P(\alpha) = 0$, ou de manière équivalente si $(X-\alpha)|P$.*

Théorème 3 (*Lien nombre de racines / degré d'un polynôme*)

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \geqslant 1$. Alors P admet au plus n racines.

Démonstration Raisonnons par récurrence sur l'entier naturel n.
Initialisation: Pour $n = 1$ alors $P(X)$ est un polynôme de degré 1, donc admettant au plus une racine.
Hérédité: Supposons que pour $n \geqslant 1$ fixé, tout polynôme de degré n admet au plus n racines et démontrons cette propriété pour les polynômes de degré $n+1$. Soit donc A un polynôme de degré $n+1$. Alors soit A n'admet aucune racine, auquel cas la propriété est vérifiée, soit A admet au moins une racine α. Alors, d'après la précédente proposition, $(X-\alpha)|P$ et donc il existe $Q \in \mathbb{K}[X]$, tel que $P(X) = (X-\alpha) \times Q(X)$ avec $deg(Q) \leqslant deg(P) - 1 = n$. Aussi, nous pouvons appliquer l'hypothèse de récurrence au polynôme Q: il admet au plus n racines, d'où P admet au plus $n+1$ racines (on ajoute aux racines de Q la racine α). L'hypothèse de récurrence est donc vraie au rang $n+1$. On démontre donc ainsi par récurrence cette propriété.

Anneaux principaux

Introduction informelle

Nous allons ici voir une catégorie d'anneaux généralisant certaines propriétés de l'anneau $\mathbb{Z}$: ces propriétés sont celles permettant de pratiquer l'arithmétique dans $\mathbb{Z}$. On appliquera ensuite les définitions et conséquence au cas de l'anneau $(\mathbb{K}[X]; +; \times)$ que nous montrerons aussi principal.

On considère à présent que tous les anneaux sont unitaires et commutatifs.

Définition 15 (*Anneaux principaux*)

Un anneau $(A; +; \times)$ est dit principal *s'il est intègre et que tout idéal de A est engendré par un élément (c'est-à-dire est de la forme $(x) = \{ax; a \in A\}$).*

Exemple: Nous avons vu précédemment que les idéaux de l'anneau $(\mathbb{Z}; +; \times)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}^*$. Aussi, ces idéaux sont tous principaux (c'est-à dire engendré par un élément puisque $(n) = n\mathbb{Z}$), donc $(\mathbb{Z}, +, \times)$ est un anneau principal.

■■ **Exercice: Propriétés des idéaux de $(\mathbb{Z}, +, \times)$**

Soient n et m deux entiers. Que pouvez-vous dire de $(n) + (m)$ et $(n) \cap (m)$?

Solution

Remarque sur les notations: La notation usuelle de l'idéal engendré par un élément n es (n); dans le cas de $\mathbb{Z}$, on a $(n) = n\mathbb{Z}$. Il faut donc faire le lien entre les deux notations.

Nous avons déjà montré que les idéaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$ (ie. les multiples d'un même entier naturel) : aussi, (n) et (m) sont deux idéeaux de $(\mathbb{Z}, +, \times)$. Or, nous avions aussi montré que la somme et l'intersection de deux idéaux étaient aussi des idéaux: aussi $\mathcal{I} = (n) + (m)$ et $\mathcal{J} = (n) \cap (m)$ sont deux idéaux de $(\mathbb{Z}, +, \times)$. Or, les idéaux de $(\mathbb{Z}, +, \times)$ sont engendré par un unique élément: aussi, il existe deux entiers naturels a et b tels que $(n) + (m) = (a)$ et $(n) \cap (m) = (b)$.
Montrons que $b = ppcm(n, m)$ et $a = pgcd(n, m)$:
Déjà, tout élément de $(n) \cap (m)$ est à la fois un multiple de n et de m, donc est un multiple de $ppcm(n, m)$. Aussi, nous avons l'inclusion $(n) \cap (m) \subset (ppcm(n, m))$. Réciproquement, par définition du $ppcm(n, m)$,

on a $ppcm(n,m) \in (n)$ et $ppcm(n,m) \in (m)$ d'où $ppcm(n,m) \in (n) \cap (m)$. Il s'ensuit alors que $(ppcm(n,m)) \subset (n) \cap (m)$ et donc on a l'égalité $(n) \cap (m) = (ppcm(n,m))$.
On peut remarquer que tout élément de $(n)+(m)$ s'écrit $un+vm$ avec $(u,v) \in \mathbb{Z}^2$, donc est un multiple de $pgcd(n,m)$ (puisque $pgcd(n,m)|n$ et $pgcd(n,m)|m$). Il s'ensuit donc que $(n)+(m) \subset (pgcd(n,m))$. Montrons alors l'inclusion réciproque: d'après le théorème de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tels que $un+vm = pgcd(n,m)$ d'où $pgcd(n,m) \in (n)+(m)$ d'où $(pgcd(n,m)) \subset (n)+(m)$. On a donc $(n)+(m) = (pgcd(n,m))$.

Théorème 4 (*L'anneau $\mathbb{K}[X]$ est principal*)

Soit $\mathbb{K}$ un corps. Alors l'anneau $(\mathbb{K}[X],+,\times)$ est principal.

Démonstration: Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$. Si $\mathcal{I} = \{0\}$, alors $\mathcal{I} = (0)$. Sinon, $\mathcal{I} \neq \{0\}$ et donc il existe des éléments dans $\mathcal{I}$ non nul. Considérons alors P un polynôme non nul de $\mathcal{I}$ de degré minimal. Montrons alors que $\mathcal{I} = (P)$. Pour ce faire, considérons $B \in \mathcal{I}$, et effectuons la division euclidienne de B par P: il existe un unique couple (Q,R) tels que $B = QP + R$ et $deg(R) < deg(P)$. Donc $R = B - QP \in \mathcal{I}$ (puisque $P \in \mathcal{I}$ idéal donc $PQ \in \mathcal{I}$ et $B \in \mathcal{I}$ d'où $R \in \mathcal{I}$). Or, comme $deg(R) < deg(P)$, nous avons $R = 0$ (sinon, cela contredit la minimalité du degré de P). Il s'ensuit donc que B est un multiple de P, donc $B \in (P)$ et donc $\mathcal{I} \subset (P)$. Comme l'inclusion réciproque est évidente (puisque $P \in \mathcal{I}$), nous en déduisons que $\mathcal{I} = (P)$ et donc l'anneau $(\mathbb{K}[X],+,\times)$ est bien principal. □

Définition 16 (*Elément irréductible*)

Un élément $x \in A \setminus \{0_A\}$ est dit irréductible *si l'égalité $x = uv$ implique qu'exactement l'un des deux éléments u ou v est un inversible de A.*

Cette définition généralise la notion de nombre premier dans $\mathbb{Z}$: si dès que l'on écrit l'égalit $p = uv$ alors u ou v est un inversible de $\mathbb{Z}$ (rappelons que $\mathbb{Z}^\times = \{-1;1\}$) alors p est un nombre premier.

Etude de quelques exemples:

• Dans $(\mathbb{Z},+,\times)$: Les inversibles de $\mathbb{Z}$ sont $\mathbb{Z}^\times = \{-1;1\}$. Aussi, les irréductibles de $(\mathbb{Z},+,\times)$ sont $\pm$ les nombres premiers.
Exemples: $6 = 2 \times 3$ n'est pas irréductible puisqu'il s'écrit comme produit de deux éléments non inversibles.
$5 = 1 \times 5 = (-1) \times (-5)$ est irréductible puisqu'à chaque fois qu'on l'écrit comme produit de deux termes de $\mathbb{Z}$, l'un d'eux est un inversibles de $\mathbb{Z}$.

• Dans $(\mathbb{R}[X],+,\times)$. Les inversibles de $(\mathbb{R}[X],+,\times)$ sont les polynômes de degré 1 (i.e. les constantes non nulle), donc $\mathbb{R}[X]^\times = \mathbb{R}^*$.
Les irréductibles de $(\mathbb{R}[X],+,\times)$ sont les polynômes de degré 1 ou les polynômes de degré 2 à discriminant strictement négatif.
Quelques exemples: $(X-1)(X+3) = X^2+2X-3$ n'est pas irréductible puisqu'il s'écrit comme produit de deux polynômes non inversibles. Par contre, $(X-1) = \frac{1}{2} \times (2X-2) = \frac{\pi}{4} \times \frac{4}{\pi}(X-1) = \cdots$ est irréductibles car à chaque fois qu'on l'écrit comme produit de deux polynômes de $\mathbb{R}[X]$, l'un deux est un inversible de $\mathbb{R}[X]$ (i.e. une constante non nulle).

• Dans $\mathbb{C}[X]$: les inversibles de $\mathbb{C}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls. Comme tout polynôme de degré au moins 1 admet une racine dans $\mathbb{C}$ (théorème de d'Alembert-Gauss), alors les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré 1.
• Dans $\mathbb{Z}/5\mathbb{Z}[X]$ (rappelons que $\mathbb{Z}/p\mathbb{Z}$ est un corps lorsque p est premier). Les inversibles de $\mathbb{Z}/5\mathbb{Z}[X]$ sont les polynômes constants non nuls (i.e. $\{1;2;3;4\}$).
Pour savoir si les polynômes $P(X) = X^2 - X + 3$ et $Q(X) = X^2 - X + 1$ sont irréductibles dans $\mathbb{Z}/5\mathbb{Z}[X]$, il faut voir s'ils admettent ou non des racines dans $\mathbb{Z}/5\mathbb{Z}$. Aussi, nous avons:

	X^2	X	X^2-X+3	X^2-X+1
0	0	0	3	1
1	1	1	3	1
2	4	2	0	3
3	4	3	4	2
4	1	4	0	3

On constate alors que $P(X) = X^2 - X + 3$ n'est pas irrédictible puisqu'il admet deux racines (aussi, ce polynôme se factorise en $P(X) = (X-5)(X-4)$ dans $\mathbb{Z}/5\mathbb{Z}[X]$). Par contre, le polynôme $Q(X) = X^2 - X + 1$ n'admet par de racines dans $\mathbb{Z}/5\mathbb{Z}$, donc est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$.

■■■ Exercice: Lien x irréductible, (x) premier et (x) maximal dans un anneau maximal

1. Montrer que $\mathcal{I} = \{P \in \mathbb{R}[X]; P(2) = 0\}$ est un idéal de $(\mathbb{R}[X], +, \times)$. Précisez en la forme.
2. Montrer que $\mathbb{K}[X]/(X-2)$ est isomorphe (en tant qu'anneaux) à $\mathbb{R}$.
3. L'idéal $(X-2)$ est-il premier ? maximal ?
4. Faire de même avec $\mathcal{J} = \{P \in \mathbb{R}[X]; P(2) = P(3) = 0\}$.

Solution

1. Vérifions déjà que $\mathcal{I}$ est un sous-groupe de $(\mathbb{R}[X], +)$.
Déjà, $\mathcal{I}$ non vide car le polynôme nul appartient clairement à $\mathcal{I}$ (il s'annule en 2).
Soient P et Q deux polynômes de $\mathcal{I}$. Alors $P+Q$ vérifie $(P+Q)(2) = P(2) + Q(2) = 0$ d'où $P+Q \in \mathcal{I}$.
Enfin, si $P \in \mathbb{R}[X]$, alors $(-P)(2) = -P(2) = 0$ et donc $-P \in \mathcal{I}$ d'où nous en déduisons que $\mathcal{I}$ est un sous-groupe de $(\mathbb{R}[X], +, \times)$.
Vérifions alors que $\mathcal{I}$ est un idéal: soit $P \in \mathcal{I}$ et $Q \in \mathbb{R}[X]$. Alors $(PQ)(2) = P(2) \times Q(2) = 0$ d'où $PQ \in \mathcal{I}$ et donc $\mathcal{I}$ est bien un idéal de $\mathbb{R}[X]$.
Remarquons que $P \in \mathcal{I} \Leftrightarrow P(2) = 0$, c'est-à dire si et seulement si 2 est racine de P, ce qui est équivalent à $(X-2)|P$, soit encore $P \in (X-2)$. On en déduit alors que $\mathcal{I} = (X-2)$.
2. Considérons l'application $\Phi : \mathbb{R}[X] \to \mathbb{R}$ définie par $\Phi(P) = P(2)$. Montrons que Φ est un morphisme d'anneaux: nous avons $\Phi(P+Q) = \Phi(P) + \Phi(Q)$ et $\Phi(PQ) = \Phi(P) \times \Phi(Q)$. Enfin, $\Phi(1) = 1$, d'où Φ est bien un morphisme d'anneaux de $\mathbb{R}[X]$ dans $\mathbb{R}$. Son noyau est (exactement) $\mathcal{I}$ d'où, par le théorème de factorisation il existe une application injective $\tilde{\Phi} : \mathbb{R}/(X-2) \to \mathbb{R}$ telle que $\tilde{\Phi} \circ \pi = \Phi$ (où π désigne la surjection canonique de $\mathbb{K}[X]$ dans $\mathbb{K}[X]/(X-2)$). Reste alors à montrer que Φ est surjective: comme $\forall k \in \mathbb{R}$, $\Phi(k) = k$, nous en déduisons que Φ est surjective et donc $\tilde{\Phi}$ réalise un isomorphisme d'anneaux entre $\mathbb{R}[X]/(X-2)$ et $\mathbb{R}$.
2. Nous allons montrer que $\mathcal{I} = (X-2)$ est premier par deux méthodes.
Première méthode: retour à la définition: Supposons que $PQ \in \mathcal{I}$, c'est-à-dire que $(X-2)|PQ$. Alors $(X-2)|P$ ou $(X-2)|Q$ ce qui implique que soit $P \in \mathcal{I}$ soit $Q \in \mathcal{I}$. On obtient bien que $\mathcal{I}$ est un idéal premier.
Seconde méthode: on utilise la caractérisation des idéaux par passage à l'anneau quotient: nous savons que $\mathbb{R}[X]/\mathcal{I}$ est isomorphe (en tant qu'anneaux) à $\mathbb{R}$ qui est intègre donc $\mathbb{R}[X]/\mathcal{I}$ l'est aussi. Il s'ensuit que $\mathcal{I}$ est un idéal premier.
Nous allons de même montrer que $\mathcal{I} = (X-2)$ est maximal selon les deux mêmes méthodes:
Première méthode: retour à la définition. Soit $\mathcal{J}$ un idéal de $\mathbb{R}[X]$ contenant strictement $\mathcal{I}$. Comme l'inclusion est stricte, il existe $P \in \mathcal{J}$ tel que $P \notin \mathcal{I}$. Effectuons alors la division euclidienne de P par $X-2$: il existe un unique couple $(Q;R)$ de polynômes tels que $P(X) = (X-2)Q(X) + R(X)$ avec $deg(R) < deg(X-2) = 1$. Donc R est une constante, éventuellement nulle: or, si $R = 0$ alors nous aurions $P \in \mathcal{I}$ ce qui est absurde, donc R est une constante non nulle, c'est-à-dire un élément inversible de $\mathbb{R}[X]$. Il s'ensuit donc que $R = P(X) - (X-2)Q(X) \in \mathcal{J}$ et donc $\mathcal{J} = \mathbb{R}[X]$ d'où l'idéal $\mathcal{I}$ est maximal dans $\mathbb{R}[X]$.
Seconde méthode: par la caractérisation avec l'anneau quotient: nous savons que $\mathbb{R}[X]/(X-2)$ est isomorphe, en tant qu'anneaux, à $\mathbb{R}$. Or, $\mathbb{R}$ est un corps, donc tous ses éléments non nul sont inversibles: aussi il en est de même de $\mathbb{R}[X]/(X-2)$ qui est donc aussi un corps, et donc $\mathcal{I} = (X-2)$ est un idéal maximal.
4. Il est aisé de montrer que $\mathcal{J} = \{P \in \mathbb{R}[X]; P(2) = P(3) = 0\}$ est un idéal de $\mathbb{R}[X]$ et que $\mathcal{J} = (P)$ avec $P(X) = (X-2)(X-3)$. Or, cet idéal n'est pas premier puisque $X-2 \notin \mathcal{J}$ et $X-3 \notin \mathcal{J}$ et pourtant $(X-2)(X-3) \in \mathcal{J}$. De plus, il n'est pas maximal puisque maximal $\Rightarrow$ premier.

Conclusions: On voit que $X-2$ est irréductible dans $\mathbb{R}[X]$ et que l'idéal engendré par $X-2$ est à la fois premier et maximal. A l'inverse, le polynôme $(X-2)(X-3)$ n'est pas irréductible et l'idéal qu'il engendre n'est ni premier, ni maximal. Cet exemple ce généralise dans le théorème suivant:

Proposition 13

Soit $(A, +, \times)$ un anneau principal et x un élément non nul. Alors les conditions suivantes sont équivalentes:

i x est un élément irréductible.

ii L'idéal (x) est premier.

iii L'idéal (x) est maximal.

Démonstration *iii* $\Rightarrow$ *ii*: Si (x) est maximal alors $A/(x)$ est un corps donc est intègre, donc (x) est premier.
ii $\Rightarrow$ *i*: Supposons que $x = uv$. Donc $uv \in (x)$. Or, (x) étant un idéal premier, donc soit $u \in (x)$ soit $v \in (x)$. Sans perte de généralité (l'anneau étant supposé commutatif), on peut supposer que $u \in (x)$. Aussi, $\exists a \in A$ tel que $u = ax$ et donc $x = axv$. Comme l'anneau A est principal donc intègre, de $x(1 - av) = 0$ nous déduisons que $1 - av = 0$ ce qui implique que $av = 1$ et donc que v est inversible.
i $\Rightarrow$ *iii*: Supposons x irréductible, et montrons alors que l'idéal (x) est maximal. Pour ce faire, considérons un idéal $\mathcal{I}$ contenant strictement l'idéal (x) et soit $y \in \mathcal{I} \setminus (x)$. L'anneau $(A, +, \times)$ étant principal, il existe $z \in A$ tel que $(z) = \mathcal{I}$. Comme $x \in (z)$ il existe $a \in A$ tel que $x = az$. x est irréductible, donc soit $z \in A^\times$ et alors $(z) = A$, soit $a \in A^\times$; dans cette dernière éventualiténous auriosn $(z) = (x)$ ce qui est absurde puisque $\mathcal{I} = (z) \neq (x)$.
Il s'ensuit donc que l'idéal (x) est maximal.

Théorème 5 (*Décomposition d'un élément de A en produit d'irréductibles*)

Soit x un élément non nul d'un anneau principal $(A, +, \times)$. Alors il existe un élément u inversible $u \in A^\times$, $x_1, \cdots, x_n$ n éléments irréductibles de A et $\alpha_1, \cdots, \alpha_n$ des entiers naturels non nuls tels que

$$x = u \times \prod_{i=1}^{n} x_i^{\alpha_i}.$$

La précédente décomposition est unique à l'ordre près des facteurs.

La démonstration de ce théorème utilise le lemme suivant:

Lemme 1 (*Suite croissande d'idéaux*)

Toute suite croissante (au sens de l'inclusion) dans un anneau principal est stationnaire à partir d'un certain rang.

Démonstration Soit donc $\mathcal{I}_1 \subset \mathcal{I}_2 \subset \cdots \mathcal{I}_k \subset \mathcal{I}_{k+1} \subset \cdots$ une suite croissante d'idéaux de $(A, +, \times)$. Considérons alors $\mathcal{J} = \bigcup_{k\in\mathbb{N}} \mathcal{I}_k$ l'union de tous les idéaux de cette suite et montrons que c'est un idéal de $(A, +, \times)$. Motrons donc que c'est déjà un sous-groupe de $(A, +)$: il est clairement non vide puisque les $\mathcal{I}_k$ le sont, et si $x \in \mathcal{J}$ alors $\exists k \in \mathbb{N}$ tel que $x \in \mathcal{I}_k$ donc $-x \in \mathcal{I}_k \subset \mathcal{J}$. Il reste donc à démontrer la stabilité par la loi interne: supposons $x, y \in \mathcal{J}$ alors $\exists (n, m) \in \mathbb{N}^2$ tel que $x \in \mathcal{I}_n$ et $y \in \mathcal{I}_m$. Si $n \leqslant m$ alors de l'inclusion $\mathcal{I}_n \subset \mathcal{I}_m$ nous déduisons que $x + y \in \mathcal{I}_m \subset \mathcal{J}$. Pour montrer que c'est un idéal, reste à montrer que pour tout $x \in \mathcal{J}$ et tout $a \in A$, $ax \in \mathcal{J}$. Si $x \in \mathcal{J}$, il existe $k \in \mathbb{N}$ tel que $x \in \mathcal{I}_k$ ce qui implique que $\forall a \in A$, $ax \in \mathcal{I}_k \subset J$.
Aussi, comme l'anneau $(A, +, \times)$ est principal, il existe $x \in A$ tel que $(x) = \mathcal{J}$, donc $\exists k \in \mathbb{N}$ tel que $x \in \mathcal{I}_k$ ce qui implique que $\forall n \geqslant k$, $\mathcal{I}_n = \mathcal{J}$.

Passons donc à la démonstration du théorème:

Démonstration Raisonnons par l'absurde en supposant que l'ensemble S est éléments non nul et non inversible et ne pouvant pas s'écrire comme produit d'un inversible par des éléments irréductibles ne soit pas vide. Soit alors $x \in S$. Aussi, puisque x n'est pas irréductible, nous pouvons l'écrire $x = x_1 y_1$ où ni x_1 ni y_1 ne sont inversibles. On voit que $x_1 \in S$ ou $y_1 \in S$ puisque sinon, nous aurions $x_1 \notin S$ et $y_1 \notin S$ donc $x = x_1 y_1 \notin S$; sans perte de généralité, on suppose $x_1 \in S$. L'inclusion $(x) \subset (x_1)$ est alors stricte puisque $y_1 \notin A^\times$.
On procède alors de même à partir de x_1: il existe (x_2, y_2) dont au moins l'un est dans S tel que $x_1 = x_2 y_2$ (on suppose $x_2 \in S$ et l'inclusion $(x_1) \subset (x_2)$ est alors stricte puisque $y_2 \notin A^\times$).
On construit ainsi une suite $(x) \subset (x_1) \subset (x_2) \subset \cdots \subset (x_n) \subset$ strictement croissante d'idéaux, ce qui contredit le lemme 1. Aussi, l'ensemble S est-il vide et donc l'existence de l'écriture est prouvée.

On admet ici l'unicité d'une telle écriture (la démonstration repose sur une récurrence).

Théorème 6 (*Lemme d'Euclide*)

Soit $(A, +, \times)$ un anneau principal et x un élément irréductible de A. Si x divise le produit ab (avec $a \in A$ et $b \in A$) alors x divise a ou x divise b.

Démonstration Raisonnons par l'absurde en supposant que x ne divise ni a ni b. Donc, par le précédent théorème, nous avons que $A/(x)$ est un corps puisque x est irréductible: aussi les classes $\overline{a}$ et $\overline{b}$ sont inversibles dans $A/(x)$. Aussi, il existe u, v, u', v' dans A tels que $ux + va = 1$ et $u'x + v'b = 1$. En effectuant le produit de ces deux égalités, nous obtenons que

$$uu'x^2 + uv'xb + vu'ax + vv'ab = 1.$$

Comme x divise le membre de gauche, on en déduit que x divise 1 donc est inversible, ce qui est absurde car x est irréductible donc non inversible.

Définition 17 (*Pgcd de deux éléments de l'anneau* $(A, +, \times)$)

Soit x et y deux éléments différents de 0 de l'anneau principal $(A, +, \times)$. On appelle Pgcd de x et y un élément z tel que (z) est égal à l'idéal (x, y) engendré par x et y.

Notons déjà que la précédente définition a bien toujours un sens puisque l'idéal (x, y) engendré par x et y est un idéal d'un anneau principal, donc est engendré par un élément z. Ensuite, cette définition n'est pas unique, mais à un inversible près: en effet, $\forall u \in A^\times$, $(z) = (uz)$.

Proposition 14 (*Lien pgcd(x, y) et décomposition en éléments irréductibles de x et y*)

Soient x et y deux éléments non nuls de l'anneau principal $(A, +, \times)$ et $x_1, x_2, \cdots x_n$ les éléments irréductibles de A apparaissants dans la décomposition de x et y en produit d'éléments irréductibles. Ainsi, il existe deux inversibles, u et v, et des entiers naturels (non nécessairement non nul) $\alpha_1, \cdots, \alpha_n$ et $\beta_1, \cdots, \beta_n$ tels que $x = u \times x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ et $y = v \times x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$. Alors $Pgcd(x, y) = \prod_{k=1}^{n} x_i^{Inf(\alpha_k;\beta_k)}$.

Théorème 7 (*Identité de Bezout*)

Soient x et y deux éléments différents de zéro d'un anneau principal $(A, +, \times)$ et soit v leur pgcd.
Alors il existe $(a, b) \in A^2$ tel que $ax + by = v$.
Les éléments non nuls x et y sont premiers entre eux si et seulement s'il existe $a, b \in A$ tels que $ax + by = 1$.

Théorème 8 (*Lemme de Gauss*)

Soit A un anneau principal et $x \in A$ tel que x divise le produit ab d'éléments de A tel que le pgcd de x et a est égal à 1. Alors x divise b.