François Liret

Arithmétique

François Liret

Arithmétique

DUNOD

Couverture: underworld 111 © istockphoto.com

2019 pour la nouvelle présentation
11 rue Paul Bert, 92240 Malakoff
ISBN 978-2-10-080631-7
www.dunod.com

TABLE DES MATIÈRES

1

RELATION D'ÉQUIVALENCE ET ENSEMBLE QUOTIENT

PLAN

OBJECTIF

On est souvent amené à partager les éléments d'un ensemble en différentes classes, c'est-à-dire à définir une partition de cet ensemble. Il devient alors possible de raisonner et de calculer sur les classes : c'est un puissant procédé algébrique.

1.1 PARTITION ET RELATION D'ÉQUIVALENCE

Définition

Soit E un ensemble. Une *partition* de E est la donnée de parties C_i de E, non vides, deux à deux disjointes et dont la réunion est E. On dit que les parties C_i sont des *classes*.

Exemple

Notons C_0 l'ensemble des entiers impairs, C_1 l'ensemble des entiers multiples de 2 mais pas de 4 et plus généralement, pour tout entier $n \geqslant 0$, notons

C_n l'ensemble des entiers multiples de 2^n mais pas de 2^{n+1}.

Les parties $(C_n)_{n\in\mathbb{N}}$ forment une partition de $\mathbb{Z}$.

1.1.1 Comment définir une partition d'un ensemble E ?

Il y a essentiellement deux procédés.

1. Au moyen d'une application définie sur E

Soit $f : E \longrightarrow F$ une application surjective.
Rappelons que pour tout élément $b \in F$, la partie de E définie par

$$f^{-1}(b) = \{x \in E \mid f(x) = b\}$$

s'appelle *l'image réciproque de b par f*. Puisque f est surjective, $f^{-1}(b)$ est non vide.

Les parties $C_b = f^{-1}(b)$ sont deux à deux disjointes, car s'il existe x commun à C_b et $C_{b'}$, alors $b = f(x) = b'$; leur réunion est E, car pour tout $x \in E$, on a $x \in f^{-1}\big(f(x)\big)$, donc $x \in C_{f(x)}$. Les parties C_b forment donc une partition de E.

Exemple

Soit $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ l'application définie par $f(x,y) = 2x + 3y$. L'application f est surjective car pour tout entier $k \in \mathbb{Z}$, on a $f(-k,k) = -2k + 3k = k$. Ainsi par exemple, les parties

$$C_0 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 0\} \quad \text{et} \quad C_5 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 5\}$$

sont des classes de la partition de $\mathbb{Z} \times \mathbb{Z}$ définie par f.

2. Au moyen d'une relation d'équivalence sur E

Définition

Une relation $\sim$ sur un ensemble E est une *relation d'équivalence* si elle est
(i) réflexive : $\forall a \in E,\ a \sim a$
(ii) symétrique : $\forall a, b \in E,\ (a \sim b) \Longrightarrow (b \sim a)$
(iii) transitive : $\forall a, b, c \in E,\ (a \sim b \text{ et } b \sim c) \Longrightarrow (a \sim c)$
Pour tout $a \in E$, l'ensemble $\mathrm{cl}(a) = \{x \in E \mid x \sim a\}$ s'appelle *la classe (d'équivalence) de a*.

Proposition

Soit $\sim$ une relation d'équivalence sur E.
➤ Pour tout $a \in E$, $a \in \mathrm{cl}(a)$.
➤ Pour tous $a, b \in E$, on a l'équivalence : $a \sim b \Longleftrightarrow \mathrm{cl}(a) = \mathrm{cl}(b)$.
➤ Pour tous $a, b \in E$, si $\mathrm{cl}(a) \neq \mathrm{cl}(b)$, alors $\mathrm{cl}(a) \cap \mathrm{cl}(b) = \emptyset$.

Démonstration. Soient $a, b \in E$.
Puisque $a \sim a$ d'après **(i)**, on a $a \in \mathrm{cl}(a)$.
Supposons $a \sim b$. Alors pour tout $z \in \mathrm{cl}(a)$, on a $z \sim a$ et puisque $a \sim b$, il s'ensuit (transitivité) $z \sim b$, donc $z \in \mathrm{cl}(b)$. Cela montre que $\mathrm{cl}(a) \subset \mathrm{cl}(b)$; mais

comme on a aussi $b \sim a$ (symétrie), il vient $\mathrm{cl}(b) \subset \mathrm{cl}(a)$, donc $\mathrm{cl}(a) = \mathrm{cl}(b)$.
Réciproquement, si $\mathrm{cl}(a) = \mathrm{cl}(b)$, alors $a \in \mathrm{cl}(b)$, donc $a \sim b$.
Montrons la dernière propriété en raisonnant par contraposée.
Supposons $\mathrm{cl}(a) \cap \mathrm{cl}(b) \neq \emptyset$. Alors il existe $z \in \mathrm{cl}(a) \cap \mathrm{cl}(b)$ et l'on a $a \sim z$ et $z \sim b$, donc $a \sim b$, donc $\mathrm{cl}(a) = \mathrm{cl}(b)$. □

Remarquons que E est la réunion des classes d'équivalence, car tout élément $a \in E$ est dans $\mathrm{cl}(a)$. On en déduit la proposition suivante.

Proposition

Etant donnée une relation d'équivalence sur E, les classes d'équivalence forment une partition de E.

Réciproquement, si l'on se donne une partition $(C_i)_{i \in I}$ de E, alors la relation définie par : $a \sim b \iff (\exists i \in I$ tel que $a, b \in C_i)$ est une relation d'équivalence dont les classes sont les C_i.

Exemple

Soit $\overrightarrow{u} \in \mathbb{R}^2$, $\overrightarrow{u} \neq \overrightarrow{0}$. Dans le plan affine, la relation :

$$(M \sim M') \iff \left(\overrightarrow{MM'} \text{ est colinéaire à } \overrightarrow{u}\right)$$

est une relation d'équivalence. La classe d'un point A est la droite affine passant par A et de vecteur directeur $\overrightarrow{u}$.

1.1.2 Relation d'équivalence définie par une application

Soit $f : E \longrightarrow F$ une application. Définissons une relation $\sim_f$ sur E en posant

$$\forall x, y \in E\,,\ x \sim_f y \iff f(x) = f(y)$$

Cette relation est réflexive, symétrique et transitive.

Définition

Soit $f : E \to F$ une application. La relation d'équivalence $\sim_f$ définie par

$$\forall x, y \in E\,,\ x \sim_f y \iff f(x) = f(y)$$

s'appelle *la relation d'équivalence définie par f*.

Pour tout $a \in E$, la classe de a est $\mathrm{cl}(a) = \{x \in E \mid f(x) = f(a)\} = f^{-1}\big(f(a)\big)$.

Exemple

Soit O un point du plan euclidien E et soit $f : E \longrightarrow \mathbb{R}$ la fonction $M \mapsto OM$. La relation d'équivalence associée à f est

$$\forall M, M' \in E, M \sim_f M' \iff OM = OM'$$

La classe d'équivalence d'un point $A \in E$ est formée des points M qui sont à la même distance de O que A : si $A \neq O$, la classe de A est le cercle de centre O passant par A ; la classe de O est $\{O\}$.

1.2 Ensemble quotient

Définitions

Soit $\sim$ une relation d'équivalence sur un ensemble E.

➤ L'ensemble des classes d'équivalence s'appelle *l'ensemble quotient de E par* $\sim$ et se note $E/\sim$.

➤ L'application $p : E \longrightarrow E/\sim$ définie par $p(x) = \text{cl}(x)$ s'appelle la *projection canonique*.

➤ Etant donnée une classe d'équivalence $\text{cl}(a)$, tout élément $x \in \text{cl}(a)$ s'appelle *un représentant* de cette classe.

Propriétés de la projection canonique

➤ L'application p est surjective : $\forall \alpha \in E/\sim, \exists a \in E, \alpha = p(a)$.

➤ La relation $\sim$ est la relation d'équivalence définie par p :

$$\forall x, y \in E, p(x) = p(y) \iff x \sim y$$

Démonstration. Toute classe $\alpha \in E/\sim$ est la classe d'au moins un élément $a \in E$: $\alpha = \text{cl}(a)$, donc $\alpha = p(a)$.
Pour tous $x, y \in E$, on a $x \sim y \iff \text{cl}(x) = \text{cl}(y) \iff p(x) = p(y)$, donc $\sim$ est la relation d'équivalence définie par l'application p. □

Toute relation d'équivalence sur E est donc définie par une application : la projection canonique $E \longrightarrow E/\sim$.

Exemple

Définissons une relation dans $\mathbb{R}^*$ en posant : $x \sim y \iff xy > 0$.
C'est une relation d'équivalence, car $x \sim y$ si et seulement si x et y ont le même signe.
La relation $\sim$ est la relation d'équivalence définie par l'application $\text{sgn} : \mathbb{R}^* \longrightarrow \{+1, -1\}$ qui à tout $x \in \mathbb{R}^*$ associe son signe.
Il y a deux classes : $\text{cl}(1) = \mathbb{R}^{*+}$ et $\text{cl}(-1) = \mathbb{R}^{*-}$. L'ensemble quotient $\mathbb{R}^*/\sim$ a donc deux éléments.

1.3 Passage au quotient d'une application

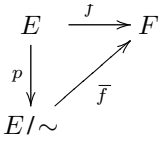
Le théorème suivant permet de définir des applications sur un ensemble quotient. C'est un résultat constamment utilisé en mathématique.

Théorème de passage au quotient

Soit $\sim$ une relation d'équivalence sur un ensemble E et $p : E \longrightarrow E/\sim$ la projection canonique. Soit $f : E \longrightarrow F$.
Pour qu'il existe une application $\bar{f} : E/\sim \longrightarrow F$ telle que $\bar{f} \circ p = f$, il faut et il suffit que $\forall x, y \in E,\ x \sim y \Longrightarrow f(x) = f(y)$.
Dans ce cas,

- $\bar{f}$ est unique et pour toute classe $\alpha \in E/\sim$, on a $\bar{f}(\alpha) = f(a)$ pour tout représentant a de α ;
- $\bar{f}$ est injective si et seulement si $\forall x, y \in E,\ x \sim y \Longleftrightarrow f(x) = f(y)$;
- Les applications f et $\bar{f}$ ont la même image.

Si l'application $\bar{f}$ existe, on dit que *f passe au quotient modulo $\sim$* et $\bar{f}$ s'appelle la *factorisation de f par $E/\sim$*.



passage au quotient de f modulo $\sim$

Démonstration

- Supposons qu'il existe $\bar{f} : E/\sim \longrightarrow F$ telle que $f = \bar{f} \circ p$. Si $x, y \in E$ sont tels que $x \sim y$, alors $p(x) = p(y)$, donc $f(x) = \bar{f}\big(p(x)\big) = \bar{f}\big(p(y)\big) = f(y)$.
  Réciproquement, supposons $\forall x, y \in E,\ x \sim y \Longrightarrow f(x) = f(y)$. Si $\alpha \in E/\sim$, alors pour tous représentants a, a' de α, on a $a' \sim a$ donc $f(a) = f(a')$: l'application f prend la même valeur sur tous les représentants de α. On peut donc poser $\bar{f}(\alpha) = f(a)$, où a est un représentant quelconque de α. On définit ainsi une application $\bar{f} : E/\sim \longrightarrow F$ telle que $\bar{f}\big(p(a)\big) = f(a)$ quel que soit $a \in E$.
- Supposons $\bar{f}$ injective et soient $x, y \in E$ tels que $f(x) = f(y)$. Alors $\bar{f}\big(p(x)\big) = \bar{f}\big(p(y)\big)$, donc $p(x) = p(y)$ et par suite $x \sim y$.
  Réciproquement, supposons $\forall x, y \in E,\ x \sim y \Longleftrightarrow f(x) = f(y)$. Soient $\alpha = p(a)$ et $\beta = p(b)$ des éléments de $E/\sim$ tels que $\bar{f}(\alpha) = \bar{f}(\beta)$. Alors $f(a) = \bar{f}(\alpha) = \bar{f}(\beta) = f(b)$, donc $a \sim b$ et $\alpha = \beta$: l'application $\bar{f}$ est donc injective.
- Puisque $f = \bar{f} \circ p$, on a $f(E) = \bar{f}\big(p(E)\big) = \bar{f}(E/\sim)$ car p est surjective. □

En appliquant le théorème à la relation $\sim_f$ définie par f, on obtient le corollaire très utile suivant.

Corollaire (factorisation canonique d'une application)

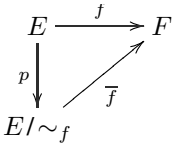
Soit $f : E \longrightarrow F$. Soit $\sim_f$ la relation d'équivalence associée à f et soit $p : E \longrightarrow E/\sim_f$ la projection canonique.

➤ Il existe une unique application $\bar{f} : E/\sim_f \longrightarrow F$ telle que $\bar{f} \circ p = f$.

➤ L'application $\bar{f}$ est injective.

➤ L'application $\bar{f}$ est bijective si et seulement si l'application f est surjective.

DÉMONSTRATION. Dans le théorème, prenons $\sim_f$ comme relation d'équivalence sur E. Pour tous $x, y \in E$, on a alors les deux implications $x \sim_f y \Longrightarrow f(x) = f(y)$ et $f(x) = f(y) \Longrightarrow x \sim_f y$, donc f passe au quotient modulo $\sim_f$ et l'application $\bar{f}$ est injective. Par suite l'application $\bar{f}$ est bijective si et seulement si elle est surjective, c'est-à-dire si et seulement si f est surjective, car f et $\bar{f}$ ont même image. □



Ce diagramme illustre la *factorisation canonique de f*.

Exemple 1

Reprenons l'exemple du paragraphe **1.1.2**. L'ensemble quotient $E/\sim_f$ est l'ensemble des cercles de centre O. L'application $\bar{f} : E/\sim_f \longrightarrow \mathbb{R}$ est définie comme suit : pour tout cercle $C \in E/\sim_f$, $\bar{f}(C) = OM$, où M est un point quelconque de C. Autrement dit, pour tout cercle C de centre O, $\bar{f}(C)$ est le rayon de C. Cette application est bien injective.
Pour qu'une application $g : E \longrightarrow \mathbb{R}$ passe au quotient modulo $\sim_f$, il faut et il suffit que, pour tous M, $M' \in E$, on ait l'implication $OM = OM' \Longrightarrow g(M) = g(M')$: cette propriété signifie que, pour tout $M \in E$, $g(M)$ ne dépend que de la distance OM.

Exemple 2

Dans l'ensemble $E = \mathbb{Z} \times \mathbb{N}^*$, définissons la relation

$$\forall (x, y), (x', y') \in E\ ,\ (x, y) \sim (x', y') \Longleftrightarrow xy' - x'y = 0$$

On vérifie facilement que c'est une relation d'équivalence.
Soit $f : E \longrightarrow \mathbb{Q}$ l'application définie par $f(x, y) = \frac{x}{y}$. Pour tous $(x, y), (x', y') \in E$, on a

$$(x,y) \sim (x', y') \Longleftrightarrow xy' = x'y \Longleftrightarrow \frac{x}{y} = \frac{x'}{y'} \Longleftrightarrow f(x, y) = f(x', y')$$

Ainsi $\sim$ est la relation définie par f.
En appelant $p : E \longrightarrow E/\sim$ la projection canonique, il existe donc une application injective $\bar{f} : E/\sim \longrightarrow \mathbb{Q}$ telle que $\bar{f} \circ p = f$. L'application f est surjective, car tout nombre rationnel s'écrit a/b avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, et l'on a $f(a, b) = a/b$. Par conséquent, l'application $\bar{f}$ est bijective.
L'ensemble quotient $E/\sim$ est une construction de $\mathbb{Q}$ à partir des ensembles $\mathbb{N}$ et $\mathbb{Z}$.

Exercices

1.1 Soit $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ l'application définie par $f(x,y) = y - 2x$.

1. Montrer que chaque classe d'équivalence pour la relation $\sim_f$ est une droite.

2. Montrer que $\mathbb{R}^2/\sim_f$ est l'ensemble des droites parallèles à la droite d'équation $y = 2x$.

3. Montrer que f définit une bijection $\bar{f} : \mathbb{R}^2/\sim_f \longrightarrow \mathbb{R}$.

1.2 Soit $f : \mathbb{C}^* \longrightarrow \mathbb{C}^*$ l'application définie par $f(z) = z^4$.

1. Soit $z \in \mathbb{C}^*$. Déterminer les éléments équivalents à z pour la relation $\sim_f$.

2. Montrer que f définit une bijection $\bar{f} : \mathbb{C}^*/\sim_f \longrightarrow \mathbb{C}^*$.

1.3 Sur l'ensemble $E = \mathbb{N}\backslash\{0\}$, définissons une relation en posant :

$$\forall n, n' \in E\ ,\ n \sim n' \Longleftrightarrow \text{il existe des entiers } u, v \text{ impairs tels que } \frac{n'}{n} = \frac{v}{u}$$

Soit $f : E \longrightarrow \mathbb{N}$ l'application qui à tout entier $n \geqslant 1$ associe l'exposant de 2 dans la décomposition de n en facteurs premiers (voir page 20). Par exemple, $f(8) = f(40) = 3$ et $f(13) = 0$.
Montrer que $\sim$ est une relation d'équivalence et que l'application f définit une bijection $\bar{f} : E/\sim \longrightarrow \mathbb{N}$.

1.4 Soit n un entier au moins égal à 1 et soit $E = \{1,2,\ldots,2n\}$. Le but de l'exercice est de montrer que si l'on choisit $n+1$ nombres de E, il y en a au moins un qui est multiple d'un autre.

1. Soit $\sim$ la relation définie sur E par :

$$\forall x, y \in E\ ,\ x \sim y \Longleftrightarrow \text{il existe un entier } k \in \mathbb{Z} \text{ tel que } y = 2^k x$$

Montrer que $\sim$ est une relation d'équivalence.

2. Montrer que toute classe d'équivalence a un unique représentant impair. En déduire qu'il y a n classes.

3. Soit $A \subset E$ une partie ayant $n+1$ éléments. Montrer qu'il existe $a,b \in A$ tels que $a \neq b$ et $a \sim b$. Conclure.

1.5 Notons $\mathbb{Z}[X]$ l'ensemble des polynômes à coefficients entiers relatifs. Définissons sur $\mathbb{Z}[X]$ la relation $\sim$ en posant

$$\forall P, Q \in \mathbb{Z}[X]\ ,\ P \sim Q \Longleftrightarrow P - Q \text{ est multiple de } X$$

1. Montrer que $\sim$ est une relation d'équivalence sur $\mathbb{Z}[X]$.

2. Soit $P \in \mathbb{Z}[X]$. Montrer que P est équivalent au polynôme constant $P(0)$.

3. Soit $f : \mathbb{Z}[X] \longrightarrow \mathbb{Z}$ l'application définie par $f(P) = P(0)$. Montrer que f définit une bijection $\mathbb{Z}[X]/\sim \longrightarrow \mathbb{Z}$.

Solutions

1.1 **1.** Les classes d'équivalence pour $\sim_f$ sont les parties $(C_m)_{m\in\mathbb{R}}$ de $\mathbb{R}^2$ telles que $C_m = \{(x, y) \in \mathbb{R}^2 \mid y - 2x = m\}$. Pour tout $m \in \mathbb{R}$, la classe C_m est donc une droite de pente 2.

2. Toute droite de pente 2 a une équation de la forme $y - 2x = m$: l'ensemble des C_m est donc l'ensemble des droites de pente 2, c'est-à-dire l'ensemble des droites parallèles à la droite d'équation $y = 2x$.

3. Il suffit de montrer que f est surjective, ce qui est évident puisque, pour tout $m \in \mathbb{R}$, on a $f(0, m) = m$.

1.2 **1.** Pour tout $z, z' \in \mathbb{C}^*$, on a les équivalences

$$z' \sim z \iff z'^4 = z^4 \iff \left(\frac{z'}{z}\right)^4 = 1 \iff \frac{z'}{z} \in \{1,-1,\boldsymbol{i},-\boldsymbol{i}\}$$
$$\iff z' \in \{z,-z,\boldsymbol{i}z,-\boldsymbol{i}z\}$$

La classe de z est donc $\mathrm{cl}(z) = \{z, -z, \boldsymbol{i}z, -\boldsymbol{i}z\}$

2. Il suffit de montrer que f est surjective ; cela résulte de ce que tout nombre complexe non nul possède des racines quatrièmes non nulles.

1.3 Montrons que la relation $\sim$ est égale à la relation $\sim_f$ définie par f. Soit $n,n' \in E$. Si $n \sim n'$, il existe des entiers impairs u et v tels que $nv = n'u$. L'exposant de 2 dans la décomposition de nv est le même que dans n, l'exposant de 2 dans la décomposition de $n'u$ est le même que dans n', donc $f(n) = f(n')$ et l'on a $n \sim_f n'$.

Réciproquement, si n et n' ont le même exposant de 2 dans leur décomposition en facteurs premiers, alors $n = 2^k m$ et $n' = 2^k m'$, où m et m' sont impairs. On a $\dfrac{n'}{n} = \dfrac{m'}{m}$, donc $n \sim n'$. Ainsi $\bar{f}$ existe et est injective. Pour montrer que $\bar{f}$ est surjective, il suffit de montrer que f l'est ; mais c'est évident, car pour tout entier $k \geqslant 0$, on a $f(2^k) = k$.

1.4 **1.** La relation est réflexive, car $x = 2^0 x$. Si $y = 2^k x$, alors $x = 2^{-k} y$, donc la relation est symétrique. Si $z = 2^k y$ et si $y = 2^m x$, avec $k,m \in \mathbb{Z}$, alors $z = 2^{k+m} x$: la relation est donc transitive.

2. Soit $a \in E$ et $\alpha = \mathrm{cl}(a)$. Soit k l'exposant de 2 dans la décomposition en facteurs premiers de a (voir page 20) : alors $k \in \mathbb{N}$ et l'on a $a = 2^k b$, où b est impair et inférieur ou égal à a, donc $b \in E$. Ainsi $a \sim b$ et b est un représentant impair de α. Supposons que α ait un (autre) représentant impair c. Alors on a $b \sim c$, donc il

existe $m \in \mathbb{Z}$ tel que $b = 2^m c$. Comme b et c sont impairs, on a nécessairement $m = 0$, donc $b = c$.
Dans l'ensemble E, il y a n nombres impairs. Il y a donc n classes d'équivalence.

3. On utilise le *principe des tiroirs* :

> *si l'on range plus de n objets dans n tiroirs, alors l'un au moins des tiroirs contient au moins deux objets*

On peut ranger chaque élément de la partie A dans sa classe d'équivalence et comme A possède plus que n éléments et qu'il y a n classes, au moins deux éléments de A sont dans la même classe. Il existe donc $a, b \in A$ tels que $a \neq b$ et $a \sim b$.
Si par exemple $b > a$, alors $b = 2^k a$ avec $k > 0$, donc b est multiple de a.

1.4 **1.** Pour tous polynômes P, Q, $R \in \mathbb{Z}[X]$,
• $P - P = 0$ est multiple de X, donc $P \sim P$.
• Si $P - Q$ est multiple de X, alors $Q - P = -(P - Q)$ aussi : d'où la symétrie de $\sim$.
• si $P - Q$ et $Q - R$ sont multiples de X, leur somme $(P - Q) + (Q - R) = P - R$ est multiple de X : d'où la transitivité de $\sim$.
Cela montre que $\sim$ est une relation d'équivalence sur $\mathbb{Z}[X]$.

2. Le polynôme $P - P(0)$ a pour racine 0, donc est multiple de X.

3. Pour tout $P, Q \in \mathbb{Z}[X]$, on a $P \sim P(0)$ et $Q \sim Q(0)$, donc $P \sim Q \iff P(0) \sim Q(0)$. Mais les polynômes constants $P(0)$ et $Q(0)$ ne sont équivalents que si leur différence $P(0) - Q(0)$ est multiple de X, c'est-à-dire si $P(0) - Q(0) = 0$. Il s'ensuit : $P \sim Q \iff P(0) = Q(0)$. Cela montre que les relations $\sim$ et $\sim_f$ sont les mêmes. La factorisation canonique de f est donc une application injective $\bar{f} : \mathbb{Z}[X]/\sim \longrightarrow \mathbb{Z}$. Pour montrer que $\bar{f}$ est bijective, il suffit de montrer que f est surjective. Or pour tout entier $k \in \mathbb{Z}$, le polynôme constant $P = k$ vérifie $P(0) = k$, c'est-à-dire $f(P) = k$.