

CORRIGÉ DU T.D. A

Arithmétique, polynômes & structures

25 septembre 2026

Exercice 1. Soit l'intervalle $I =]-1, +1[$. Pour chaque $(x, y) \in I^2$, on définit le réel

$$x * y = \frac{x + y}{1 + xy}.$$

1. Montrer que, pour tout $(x, y) \in I^2$, $x * y \in I$.
2. Montrer que $(I, *)$ est un groupe commutatif.
3. Soit $a \in [0, 1[$. Vérifier que $A = [a, 1[$ est stable par la loi $*$.

L'ensemble $(A, *)$ est-il un sous-groupe de $(I, *)$?

4. Montrer que la fonction $\text{th} : \mathbb{R} \rightarrow I$ est bijective et déterminer l'expression de sa réciproque th^{-1} .
5. Montrer que th est un isomorphisme du groupe $(\mathbb{R}, +)$ vers le groupe $(I, *)$.

1. Soit $(x, y) \in I^2$:

$$\begin{aligned} \frac{x+y}{1+xy} < 1 &\Leftrightarrow x+y < 1+xy \text{ en multipliant par } 1+xy > 0 \\ &\Leftrightarrow 0 < 1-x-y+xy. \end{aligned}$$

Or $1-x-y+xy = (1-x) \cdot (1-y) > 0$. D'où $\frac{x+y}{1+xy} < 1$ et, de même, $-1 \leq \frac{x+y}{1+xy}$. Donc

$*$ est une loi de composition interne

AUTRE MÉTHODE — Soit $x \in I$. On considère la fonction $f : [-1, 1] \rightarrow \mathbb{R}$, $y \mapsto \frac{x+y}{1+xy}$. L'application f est dérivable et $\forall y \in]-1, +1[, f'(y) = \frac{1+xy-x^2-xy}{(1+xy)^2} = \frac{1-x^2}{(1+xy)^2} > 0$. L'application f est continue et strictement croissante, d'où $f(]-1, 1]) = [f(-1), f(1)]$. Or $f(-1) = \frac{x-1}{1-x} = -1$ et $f(1) = \frac{x+1}{1+x} = 1$. Donc $f(I) \subset I$ pour tout $x \in I$.

2. 0 est l'élément neutre de $*$ car, pour tout $x \in I$, $x * 0 = \frac{x+0}{1+x \cdot 0} = x$.

Tout élément x de I possède un inverse car $-x \in I$ et $x * (-x) = \frac{x-x}{1+x(-x)} = 0$. D'où $-x$ est l'inverse de x .

Enfin la loi $*$ est associative car, pour tout $(x, y, z) \in I^3$:

$$\begin{aligned} (x * y) * z &= \frac{x * y + z}{1 + (x * y)z} \\ &= \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy}z} \\ &= \frac{x+y+z+xyz}{1+xy+xz+yz} \\ &= \frac{x(1+yz)+y+z}{1+yz} \\ &= \frac{x + \frac{y+z}{1+yz}}{1 + x \frac{y+z}{1+yz}} \\ &= \frac{x + y * z}{1 + x(y * z)} \\ (x * y) * z &= x * (y * z) \end{aligned}$$

Donc $(I, *)$ est un groupe commutatif

3. Nous avons vu que l'application $f : y \mapsto x * y$ est croissante sur $[-1, 1]$.

D'où $\forall (x, y) \in A^2, \frac{x+y}{1+xy} \geq \frac{x+0}{1+0x} \geq x \geq a$. Donc

A est stable par $*$

Non, l'ensemble $(A, *)$ n'est pas un sous-groupe de $(I, *)$ car il existe $x \in A$ tel que $-x \notin A$.

4. La fonction th est dérivable car c'est le quotient de deux fonctions dérivables et car son dénominateur ne s'annule pas.

Pour tout $x \in \mathbb{R}$, $\text{th}'(x) = \frac{4}{(e^x + e^{-x})^2} > 0$. Donc

la fonction th est strictement croissante

$\text{th}(x) = \frac{1-e^{-2x}}{1+e^{-2x}} \xrightarrow{x \rightarrow +\infty} +1$ et, parce que la fonction th est impaire, $\text{th}(x) \xrightarrow{x \rightarrow -\infty} -1$

PREMIÈRE MÉTHODE — La fonction $\mathbb{R} \rightarrow I, x \mapsto \text{th}(x)$ est bijective d'après la question 4 : injective car elle est strictement monotone et surjective car $\text{th}(\mathbb{R}) =]\lim_{-\infty} \text{th}, \lim_{+\infty} \text{th}[= I$ d'après le TVI car la fonction th est continue. La deuxième méthode sera meilleure car elle permettra non seulement de montrer que th est bijective mais aussi de déterminer l'expression de th^{-1} .

DEUXIÈME MÉTHODE — Soient $x \in \mathbb{R}$ et $y \in]-1, 1[$:

$$\begin{aligned} y = \text{th}(x) &\iff \frac{e^{2x} - 1}{e^{2x} + 1} = y \\ &\iff e^{2x} - 1 = y \cdot (e^{2x} + 1) \\ &\iff e^{2x} \cdot (1 - y) = 1 + y \\ &\iff e^{2x} = \frac{1 + y}{1 - y} \quad \text{car } y \neq 1 \\ &\iff 2x = \ln \frac{1 + y}{1 - y} \quad \text{car } 1 + y > 0 \text{ et } 1 - y > 0 \\ &\iff x = \frac{1}{2} \ln \frac{1 + y}{1 - y}. \end{aligned}$$

Donc th est bijective et $\text{th}^{-1}(y) = \frac{1}{2} \ln \frac{1+y}{1-y}$ pour tout $y \in]-1, 1[$.

5. Soit $(x, y) \in \mathbb{R}^2$: d'après la question précédente, les réels $\text{th}(x)$ et $\text{th}(y)$ appartiennent à I . De plus

$$\begin{aligned} \text{th}(x) * \text{th}(y) &= \frac{\frac{e^x - e^{-x}}{e^x + e^{-x}} + \frac{e^y - e^{-y}}{e^y + e^{-y}}}{1 + \frac{e^x - e^{-x}}{e^x + e^{-x}} \frac{e^y - e^{-y}}{e^y + e^{-y}}} \\ &= \frac{(e^x - e^{-x})(e^y + e^{-y}) + (e^y - e^{-y})(e^x + e^{-x})}{(e^x + e^{-x})(e^y + e^{-y}) + (e^x - e^{-x})(e^y - e^{-y})} \\ &= \frac{(e^{x+y} - e^{-x+y} + e^{x-y} - e^{-x-y}) + (e^{y+x} - e^{-y+x} + e^{y-x} - e^{-y-x})}{(e^{x+y} + e^{-x+y} + e^{x-y} + e^{-x-y}) + (e^{x+y} - e^{-x+y} - e^{x-y} + e^{-x-y})} \\ &= \frac{2e^{x+y} - 2e^{-x-y}}{2e^{x+y} + 2e^{-x-y}} \\ &= \frac{e^{x+y} - e^{-x-y}}{e^{x+y} + e^{-x-y}} \\ &= \text{th}(x + y) \end{aligned}$$

Donc th est un morphisme du groupe $(\mathbb{R}, +)$ vers le groupe $(I, *)$. Et c'est un isomorphisme car th est bijective.

Exercice 2. Soit A un anneau commutatif non réduit à $\{0_A\}$, soit $x \in A$. On dit que x est *nilpotent* si

$$\exists n \in \mathbb{N}, x^n = 0_A.$$

Montrer que :

- si x est nilpotent, alors x n'est pas inversible mais $1_A - x$ est inversible.
- l'ensemble des éléments nilpotents de A est un idéal de A .

1. Soient $x \in A$ et $n \in \mathbb{N}$ tels que $x^n = 0_A$.

Montrons que x n'est pas inversible. Par l'absurde : si x est inversible, alors $\exists y \in A$, $x \times y = y \times x = 1_A$. D'où, en élevant à la puissance n : $x^n \times y^n = 1_A$ car l'anneau est supposé commutatif. Par suite $0_A y^n = 1_A$. C'est absurde.

Montrons que $1_A - x$ est inversible. Par un télescope : $(1_A - x) \times (1_A + x + x^2 + \dots + x^{n-1}) = 1_A - x^n = 1_A$. Donc $1_A - x$ est inversible et son inverse est $1_A + x + x^2 + \dots + x^{n-1}$.

2. Soit I l'ensemble des éléments nilpotents de A .

D'une part $(I, +)$ est un sous-groupe de $(A, +)$ car $0_A \in I$ et $\forall (x, y) \in I^2$, $x - y \in I$. En effet, si $x^{n_1} = 0_A$ et $y^{n_2} = 0_A$, alors $(x - y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} x^k \times y^{n_1+n_2-k}$ car la loi $\times$ est commutative par hypothèse. Et chaque terme de cette somme est nul car la puissance k est supérieure ou égale à n_1 ou la puissance $n_1 + n_2 - k$ est supérieure ou égale à n_2 .

D'autre part, si $i \in I$, alors il existe n tel que $i^n = 0_A$. Pour tout $a \in A$, $i \times a \in I$ car $0_A = i^n \times a^n = (i \times a)^n$ car la loi $\times$ est commutative par hypothèse.

Exercice 3. Soit A un anneau commutatif. Si I est un idéal de A , alors on note

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}^*, x^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A et que $I \subset \sqrt{I}$.
2. Soient I et J deux idéaux de A . Montrer que :
 - (a) $I \cap J$ est un idéal de A ;
 - (b) $I \subset J \implies \sqrt{I} \subset \sqrt{J}$;
 - (c) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
3. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

1. Soit $i \in I$. Alors $i^1 \in I$, d'où $i \in \sqrt{I}$. Donc $I \subset \sqrt{I}$.

D'une part $(\sqrt{I}, +)$ est un sous-groupe de $(A, +)$. En effet $\sqrt{I}$ n'est pas vide car $0_A \in I \subset \sqrt{I}$. Et $\forall (x, y) \in \sqrt{I}^2$, $x - y \in I$. En effet, si $x^{n_1} \in I$ et $y^{n_2} \in I$, alors $(x - y)^{n_1+n_2} = \sum_{k=0}^{n_1+n_2} (-1)^{n_1+n_2-k} \binom{n_1+n_2}{k} x^k \times y^{n_1+n_2-k}$ car la loi $\times$ est commutative par hypothèse. Et chaque terme de cette somme appartient à I car I est un idéal et la puissance k est supérieure ou égale à n_1 ou la puissance $n_1 + n_2 - k$ est supérieure ou égale à n_2 .

D'autre part, pour tout $(i, a) \in \sqrt{I} \times A$, $i \times a \in \sqrt{I}$ car $\exists n \in \mathbb{N}^*$, $i^n \in I$ et, parce que A est commutatif, $(i \times a)^n = i^n \times a^n \in I$ car $i^n \in I$ et I est un idéal.

Donc $\sqrt{I}$ est un idéal.

2. (a) Voir la preuve dans le cours.
 (b) Soit $i \in \sqrt{I}$. Il existe alors n tel que $i^n \in I$. Or $I \subset J$, d'où $i^n \in J$, d'où $i \in \sqrt{J}$. Donc $\sqrt{I} \subset \sqrt{J}$.
 (c) On utilise la question précédente pour prouver une inclusion : $I \cap J \subset I$, d'où $\sqrt{I \cap J} \subset \sqrt{I}$. De même, $\sqrt{I \cap J} \subset \sqrt{J}$. Donc $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

Et pour l'autre inclusion : soit $x \in \sqrt{I} \cap \sqrt{J}$. Il existe alors $(n, p) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $x^n \in I$ et $x^p \in J$. Par suite $x^{n+p} = x^n \times x^p \in I$ car $x^n \in I$ et I est un idéal. Et, de même, $x^{n+p} \in J$. D'où $x^{n+p} \in I \cap J$. Donc $x \in \sqrt{I \cap J}$.

Par double inclusion, $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

3. D'une part, $I \subset \sqrt{I}$ d'après la question 1. D'où $\sqrt{I} \subset \sqrt{\sqrt{I}}$ d'après la question 2b.

D'autre part, $\sqrt{\sqrt{I}} \subset \sqrt{I}$. En effet : soit $x \in \sqrt{\sqrt{I}}$. Il existe alors n tel que $x^n \in \sqrt{I}$. Et il existe donc p tel que $(x^n)^p \in I$. D'où $x^{np} \in I$. D'où $x \in \sqrt{I}$. Donc $\sqrt{\sqrt{I}} \subset \sqrt{I}$.

Par double inclusion, $\sqrt{\sqrt{I}} = \sqrt{I}$.

Exercice 4 (Nombre de diviseurs d'un entier – oral X ENS PSI 2011).

Soient un entier $n \in \mathbb{N}^*$ et la matrice $A_n = (a_{i,j})_{1 \leq i,j \leq n}$ définie par : $a_{i,j} = 1$ si $i|j$ et zéro sinon.

1. Montrer que $a_{i,1} + a_{i,2} + \dots + a_{i,n}$ est égal à la partie entière de $\frac{n}{i}$.

2. Soit s_n la somme des n^2 éléments de la matrice A_n . Déterminer un équivalent de s_n .
3. Soit d_n le nombre des diviseurs de n . Montrer que $d_1 + \dots + d_n \sim n \ln n$.

1. La somme $k = a_{i,1} + a_{i,2} + \dots + a_{i,n}$ est le nombre d'entiers $j \in \llbracket 1, n \rrbracket$ tels que $i|j$, c'est-à-dire le nombre de multiples de i compris dans $\llbracket 1, n \rrbracket$. On cherche donc l'entier k tel que $i, 2i, \dots, ki$ sont $\leq n$ et $n < (k+1)i$, ou encore $k \leq \frac{n}{i} < n+1$. Par définition de la partie entière, on obtient

$$a_{i,1} + a_{i,2} + \dots + a_{i,n} = \left\lfloor \frac{n}{i} \right\rfloor.$$

2. On note H_n le n -ième nombre harmonique $1 + \frac{1}{2} + \dots + \frac{1}{n}$. En effectuant une somme par lignes, la première question montre que $s_n = \sum_{i=1}^n \left\lfloor \frac{n}{i} \right\rfloor$. Comme $x-1 \leq \lfloor x \rfloor \leq x$ pour tout $x \in \mathbb{R}$, on en déduit que $nH_n - n \leq s_n \leq nH_n$. Or $H_n \sim \ln n$ (il s'agit d'une comparaison série-intégrale appliquée à la fonction continue et décroissante $t \in]0, +\infty[\mapsto \frac{1}{t}$) et on en déduit que

$$s_n \sim n \ln n.$$

3. On peut aussi calculer s_n en effectuant une somme par colonnes. Tout d'abord, la définition des $a_{i,j}$ montre que $a_{1,j} + \dots + a_{n,j}$ est le nombre des diviseurs de j compris entre 1 et n , c'est-à-dire le nombre d_j des diviseurs de j (car $j \leq n$). Alors $s_n = \sum_{j=1}^n d_j$.

Le quotient $\frac{s_n}{n}$ est le nombre moyen de diviseurs d'un entier dans $\llbracket 1, n \rrbracket$.

Le résultat démontré dit que ce nombre moyen est équivalent à $\ln(n)$.

Exercice 5. Montrer que, pour tout entier p premier supérieur ou égal à 5 :

$$24 \mid (p^2 - 1).$$

Soit un entier p premier supérieur ou égal à 5.

D'une part $p-1$ et $p+1$ sont des entiers pairs et l'un des deux est un multiple de 4. Par suite $p^2 - 1 = (p-1)(p+1)$ est un multiple de 8.

D'autre part $p-1$ ou $p+1$ est un multiple de 3 car p ne l'est pas. Par suite $p^2 - 1 = (p-1)(p+1)$ est un multiple de 3.

Or 3 et 8 sont premiers entre eux, donc $p^2 - 1$ est un multiple de $3 \times 8 = 24$.

Exercice 6. Soient (a, b) dans $\mathbb{Z}^2$ et n dans $\mathbb{N}^*$ tel que $\text{pgcd}(a, b) = 1$. Montrer que :

1. $\text{pgcd}(a+b, a-b) \in \{1; 2\}$;
2. $\text{pgcd}(a^2+b^2, a+b) \in \{1; 2\}$.

1. D'après le lemme de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ua + vb = 1$.

Soit d un diviseur commun à $a+b$ et $a-b$. Alors d divise $2a$ et $2b$. D'où d divise aussi $u2a + v2b = 2$.

Donc $\text{pgcd}(a+b, a-b) \in \{1; 2\}$.

REMARQUE — les 2 cas sont possibles car :

- si $(a,b)=(2,3)$, alors $\text{pgcd}(5, -1) = 1$;
- si $(a,b)=(3,5)$, alors $\text{pgcd}(8, -2) = 2$.

2. a^2 et b^2 sont aussi premiers entre eux, il existe donc $(u, v) \in \mathbb{Z}^2$ tel que $ua^2 + vb^2 = 1$ d'après le lemme de Bézout.

Soit d un diviseur commun à a^2+b^2 et $a+b$. Alors d divise $2a^2 = (a^2+b^2) + (a+b)(a-b)$ et $2b^2 = (a^2+b^2) - (a+b)(a-b)$. D'où d divise aussi $u2a^2 + v2b^2 = 2$.

Donc $\text{pgcd}(a^2+b^2, a+b) \in \{1; 2\}$.

REMARQUE — les 2 cas sont possibles car :

- si $(a,b)=(2,3)$, alors $\text{pgcd}(13, -1) = 1$;
- si $(a,b)=(3,5)$, alors $\text{pgcd}(34, -2) = 2$.

Exercice 7. Soit n un entier naturel non nul.

1. Ecrire le cycle $(1, 2, 3, 4)$ comme la composée de transpositions de la forme $(1, i)$, où $i \in \llbracket 2, 4 \rrbracket$. Votre solution est-elle unique ?
2. Soient x et y deux éléments distincts de $\llbracket 1, n \rrbracket$. Soit la permutation $f = (1, x) \circ (1, y) \circ (1, x)$. Calculer $f(z)$ pour chaque $z \in \llbracket 1, n \rrbracket$.
3. Montrer que toute permutation de $\llbracket 1, n \rrbracket$ est la composée de transpositions de la forme $(1, i)$, où $i \in \llbracket 1, n \rrbracket$.

1. $(1, 2, 3, 4) \xrightarrow{(1,2)} (2, 1, 3, 4) \xrightarrow{(1,3)} (2, 3, 1, 4) \xrightarrow{(1,4)} (2, 3, 4, 1)$

d'où le cycle $(1, 2, 3, 4)$ est égal à la composée $(1, 4) \circ (1, 3) \circ (1, 2)$.

Cette solution n'est pas unique car $(1, 2) \circ (1, 2) = \text{id}$, d'où une autre solution :

$(1, 2) \circ (1, 2) \circ (1, 4) \circ (1, 3) \circ (1, 2)$.

2. Si $z \notin \{1, x, y\}$, alors $f(z) = z$.

Si $x \neq 1$ et $y \neq 1$, alors $f(1) = 1$, $f(x) = y$ et $f(y) = x$, d'où $f = (x, y)$.

Si $x = 1$, alors $f = (1, y)$.

Si $y = 1$, alors $f = \text{id}$.

3. Toute permutation est une composée de transpositions (x, y) . Or toute transposition (x, y) est, d'après la question précédente, une composée de transpositions de la forme $(1, i)$. Donc toute permutation est une composée de transpositions $(1, i)$.

Exercice 8. Soit $n \geq 2$ et le cycle $c = (1 \ 2 \ \dots \ n-1 \ n)$. Déterminer toutes les permutations σ de S_n telles que $\sigma \circ c = c \circ \sigma$.

Pour chaque $k \in \mathbb{N}$, la permutation c^k est une solution de l'équation $\sigma \circ c = c \circ \sigma$. Réciproquement, montrons que toute solution σ est de la forme c^k .

Si σ est une solution de $\sigma \circ c = c \circ \sigma$, alors (par récurrence), $\sigma \circ c^i = c^i \circ \sigma$ pour tout $i \in \mathbb{N}$. Le cycle $c = (1 \ 2 \ \dots \ n-1 \ n)$ s'écrit aussi $(c^0(1) \ c^1(1) \ \dots \ c^{n-2}(1) \ c^{n-1}(1))$. D'où $\exists k \in \llbracket 0, n-1 \rrbracket$, $\sigma(1) = c^k(1)$. Par suite, pour tout $i \in \llbracket 1, n \rrbracket$, $\sigma(i) = \sigma \circ c^{i-1}(1) = c^{i-1} \circ \sigma(1) = c^{i-1} \circ c^k(1) = c^k \circ c^{i-1}(1) = c^k(i)$. Donc $\sigma = c^k$.

Exercice 9 (Résultant de deux polynômes). Soient deux polynômes $P = X^2 + aX + b$ et $Q = X^2 + cX + d$ de $\mathbb{C}_2[X]$ et le déterminant

$$\Delta(P, Q) = \begin{vmatrix} b & 0 & d & 0 \\ a & b & c & d \\ 1 & a & 1 & c \\ 0 & 1 & 0 & 1 \end{vmatrix}.$$

1. Montrer que $\Delta(P, Q) = 0$ si, et seulement si, il existe deux polynômes $U \in \mathbb{C}_1[X]$ et $V \in \mathbb{C}_1[X]$ non tous nuls tels que $UP = VQ$.
2. Montrer que P et Q ont au moins une racine commune si, et seulement si, $\Delta(P, Q) = 0$.

- 1.

$$\Delta(P, Q) = \begin{vmatrix} b & 0 & d & 0 \\ a & b & c & d \\ 1 & a & 1 & c \\ 0 & 1 & 0 & 1 \end{vmatrix}$$

est égal au déterminant, dans la base $(1, X, X^2, X^3)$ de $\mathbb{C}_3[X]$, de la famille de vecteurs

$$(P, XP, Q, XQ), \quad \text{où} \quad P = X^2 + aX + b \text{ et } Q = X^2 + cX + d.$$

Il est nul ssi cette famille est liée, ssi il existe $(\alpha, \beta, \gamma, \delta) \neq (0, 0, 0, 0)$ tel que $\alpha P + \beta XP + \gamma Q + \delta XQ = 0$, ssi il existe $(\alpha, \beta, \gamma, \delta) \neq (0, 0, 0, 0)$ tel que $(\alpha + \beta X)P = (-\gamma - \delta X)Q$, ssi il existe deux polynômes $U \in \mathbb{C}_1[X]$ et $V \in \mathbb{C}_1[X]$ non tous nuls tels que $UP = VQ$.

2. Il existe $(p_1, p_2, q_1, q_2) \in \mathbb{C}^4$ tel que $P = (X - p_1)(X - p_2)$ et $Q = (X - q_1)(X - q_2)$.

Si P et Q ont une racine commune, alors (par exemple) $p_1 = q_1$, d'où $(X - q_2)P = (X - p_2)Q$.

Réciproquement : si $UP = VQ$, alors $(\alpha + \beta X)(X - p_1)(X - p_2) = (-\gamma - \delta X)(X - q_1)(X - q_2)$, d'où : $q_1 = p_1$ ou $q_1 = p_2$ ou $q_1 = -\frac{\alpha}{\beta}$ (et alors $q_2 = p_1$ ou $q_2 = p_2$). Dans les trois cas, P et Q ont au moins une racine commune.

Exercice 10. On note $\Gamma = \{0, 1\}$, $\Gamma[X]$ l'ensemble des polynômes dont les coefficients appartiennent à Γ et $\Gamma_n[X]$ l'ensemble des polynômes de $\Gamma[X]$ dont le degré est inférieur ou égal à n .

1. Quel est le cardinal de $\Gamma_n[X]$?
2. Montrer que, pour tout $P \in \Gamma_{2p}[X]$,

$$-2 \frac{4^p - 1}{3} \leq P(-2) \leq \frac{4^{p+1} - 1}{3}.$$

3. Soient $P, Q \in \Gamma[X]$ tels que $P(-2) = Q(-2)$. Montrer que $P = Q$.
4. Montrer que, pour tout $N \in \mathbb{Z}$, il existe $P \in \Gamma[X]$ tel que $N = P(-2)$.

1. Le cardinal de $\Gamma_n[X]$ vaut 2^{n+1} car construire un polynôme de $\Gamma[X]$, c'est choisir ses $n+1$ coefficients dans Γ .
2. Pour tout $P \in \Gamma_{2p}[X]$,

$$-2 \frac{4^p - 1}{3} = \sum_{k=0}^{p-1} (-2)^{2k+1} \leq P(-2) \leq \sum_{k=0}^p (-2)^{2k} = \frac{4^{p+1} - 1}{3}.$$

3. Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes différents appartenant à $\Gamma[X]$. On note n_0 le plus grand entier tel que le coefficient de degré n_0 de P n'est pas égal au coefficient de degré n_0 de Q . On a donc :

$$\begin{aligned} |P(-2) - Q(-2)| &= \left| \sum_{k=0}^{n_0} (a_k - b_k)(-2)^k \right| \\ &\geq |a_{n_0} - b_{n_0}| 2^{n_0} - \sum_{k=0}^{n_0-1} |a_k - b_k| 2^k \\ &\geq 2^{n_0} - \sum_{k=0}^{n_0-1} 2^k \\ &= 2^{n_0} - (2^{n_0} - 1) = 1 \end{aligned}$$

Donc $P(-2)$ ne peut être égal à $Q(-2)$.

4. L'application

$$\begin{array}{ccc} \Gamma_n[X] & \rightarrow & \left[2 \frac{4^p - 1}{3}, \frac{4^{p+1} - 1}{3} \right] \\ P & \mapsto & P(-2) \end{array}$$

est injective, d'après la question précédente. Or il y a $2 \frac{4^p - 1}{3} + \frac{4^{p+1} - 1}{3} + 1 = 2^{2p+1}$ éléments dans $\left[2 \frac{4^p - 1}{3}, \frac{4^{p+1} - 1}{3} \right]$ et il y a 2^{2p+1} polynômes dans $\Gamma_n[X]$. Cette application est donc aussi surjective. On en conclut que pour tout $N \in \mathbb{Z}$, en prenant p suffisamment grand, il existe un polynôme $P \in \Gamma_{2p}[X]$ tel que $P(-2) = N$.