ALGÈBRE GÉNÉRALE

1. Groupes

1.1. Groupes $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.1.1. **I**

On note $\mathbb{U}_n$ le groupe des racines n-ièmes de l'unité dans $\mathbb{C}^*$.

(1) Montrer que $\mathbb{U}_n$ est le seul groupe à n éléments de $\mathbb{C}^*$ (utiliser le théorème de Lagrange qui dit que $x^{\operatorname{Card} G} = e$ pour tout élément x du groupe G).
(2) Montrer l'équivalence $n|m \Leftrightarrow \mathbb{U}_n \subset \mathbb{U}_m$.
(3) Montrer que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_d$ où $d = n \wedge m$.
Montrer que $\mathbb{U}_n.\mathbb{U}_m = \{zz' \mid z \in \mathbb{U}_n,\ z' \in \mathbb{U}_m\} = \mathbb{U}_p$ où $p = n \vee m$.

Exercice 1.1.2. **I**

Montrer que le sous-groupe $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ est cyclique ssi $a \wedge b = 1$.

1.2. Groupes.

Exercice 1.2.1. **F**

Soit $n \geqslant 3$, peut-on trouver un ensemble de $n-2$ transpositions qui engendrent $\mathfrak{S}_n$?

Exercice 1.2.2. **F**

Soit G un groupe abélien tel qu'il existe n dans $\mathbb{N}^*$ vérifiant $x^n = e$, e élément neutre, pour tout x de G. On suppose de plus que $n = ab$ avec a et b premiers entre eux. On pose alors $H_a = \{x^a \mid x \in G\}$ et $H_b = \{x^b \mid x \in G\}$.

(1) Montrer que H_a et H_b sont des sous-groupes de G.
(2) Montrer que, pour tout x de G, il existe un et un seul couple (r, s) de $H_a\times H_b$ tel que $x = rs$.
(3) On suppose que n est impair.
   a) Montrer que $x \mapsto x^2$ est un automorphisme de G. Quelle est son application réciproque ?
   b) Même question pour $x \mapsto x^k$ avec k entier premier avec n.

Exercice 1.2.3. **I**

Soit G un groupe commutatif et x, y deux éléments de G d'ordres respectifs a et b.

(1) Montrer que l'ordre de xy divise $m = a \vee b$. A-t-on égalité ?
(2) Étudier le cas où a et b sont premiers entre eux.
(3) Que dire si G n'est pas commutatif.

Exercice 1.2.4. **I**
Soit $\mathbb{K}$ un sous corps de $\mathbb{C}$, G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{K})$ de cardinal p.

(1) Montrer que $P = \dfrac{1}{p}\sum_{M\in G} M$ est un projecteur.
(2) Que dire de P si $\sum_{M\in G} M$ est de trace nulle.

Exercice 1.2.5. **I**
Soit G un groupe où tout élément vérifie $a^2 = e$ où e est l'élément neutre.

(1) Montrer que G est commutatif.
(2) Soit H un sous-groupe de G, $H \neq G$ et a un élément de $G\setminus H$. Montrer que $H \cap aH = \emptyset$ et que $H \cup aH$ est un sous-groupe de G.
(3) Montrer enfin que, si G est fini, alors $\operatorname{Card} G = 2^n$.

Exercice 1.2.6. **D**
Soit G un groupe fini, on pose $G_p = \{x \in G \mid x^p = e\}$. Si $\operatorname{Card} G_p \leqslant p$ pour tout p, montrer que G est cyclique (on utilisera et démontrera la formule $n = \sum_{d|n} \varphi(d)$ où φ désigne la fonction d'Euler).
En déduire que dans tout corps fini $\mathbb{K}$, $(\mathbb{K}\setminus\{0\}, \times)$ est cyclique.

---

2. Anneaux et corps

2.1. **Idéaux d'un anneau commutatif.**

Exercice 2.1.1. **I**
Soit A un anneau commutatif, pour tout x de A, on note (x) l'idéal engendré par x. Soient a et b deux éléments de A. On dit qu'un idéal est principal ssi il est engendré par un élément. Montrer que si $(a) + (b)$ est principal alors $(a) \cap (b)$ est également principal.

Exercice 2.1.2. **I**
Soit A un anneau commutatif, on dit que $a \in A$ est nilpotent ssi il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

(1) Montrer que l'ensemble des éléments nilpotents de A est un idéal.
(2) Déterminer les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ où n est un entier $\geqslant 2$.
(3) Donner un exemple d'anneau non commutatif pour lequel cette propriété est mise en défaut (penser à un anneau de matrices).

2.2. **Idéaux de $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$.**

EXERCICE 2.2.1. **I**

Soit n un élément de $\mathbb{N}^*$ et a dans $\mathbb{Z}/n\mathbb{Z}$, on définit une application de $\mathbb{Z}/n\mathbb{Z}$ dans lui même par $\gamma_a(x) = ax$.

(1) Montrer qu'il existe des valeurs de a telles que $\gamma_a(x+y) = \gamma_a(x) + \gamma_a(y)$ et $\gamma_a(xy) = \gamma_a(x)\gamma_a(y)$ pour tout (x, y) de A^2.
Discuter en fonction de n des valeurs de a qui conviennent ?
Dans ce cas γ_a est-elle un morphisme d'anneaux ?

(2) On suppose que $a \wedge n = 1$ et que n ne divise pas $a^n - a$. Chercher le noyau de γ_a en tant que morphisme de groupe. Montrer que n n'est pas premier.

EXERCICE 2.2.2. **F**

Montrer les congruences suivantes (pour $n \geqslant 1$) :

1. $9^{2n-1} + 8^{n+1} \equiv 0[73]$ 2. $16^n - 15n - 1 \equiv 0[225]$ c) $10^{6n} + 10^{3n} - 2 \equiv 0[111]$.

EXERCICE 2.2.3. **F**

Trouver tous les triplets $(x, y, z) \in (\mathbb{N}^*)^3$ vérifiant l'une des conditions suivantes :

1. $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = 1$.
2. $xyz = 1 + x + y + z$.

EXERCICE 2.2.4. **D**

(1) Montrer que $r_n = \dfrac{5^{n+1} + 6^{n+1}}{5^n + 6^n}$ est irréductible.

(2) Plus généralement, donner une condition nécessaire et suffisante pour que $t_n = \dfrac{\lambda\alpha^{n+1} + \mu\beta^{n+1}}{\lambda\alpha^n + \mu\beta^n}$ soit irréductible pour tout n (où on a supposé que $(\lambda, \mu, \alpha, \beta) \in \mathbb{N}^{*4}$.

2.3. **Application à la cryptographie.**

EXERCICE 2.3.1. **F**

Soit n un entier $\geqslant 1$, montrer qu'il existe n entiers consécutifs non premiers.

EXERCICE 2.3.2. **I**

On pose $n = 2^m + 1$ dans tout cet exercice avec $m \geqslant 2$.

(1) Montrer que si m est impair alors n n'est pas premier.

(2) On suppose m pair et on écrit $m = 2^k(2q+1)$. Montrer que si $q \geqslant 1$ alors n n'est pas premier.

(3) Soit q un facteur premier du nombre de Fermat $F_n = 2^{2^n} + 1$. On note $< 2 >$ le groupe multiplicatif engendré par la classe d'équivalence de 2 dans $\mathbb{Z}/q\mathbb{Z} \setminus \{0\}$. Montrer que $\omega(2) = 2^{n+1}$ où $\omega(2)$ désigne l'ordre de 2 (on utilisera le théorème de Lagrange qui dit que $\omega(2)$ divise $\operatorname{Card} \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$).
En déduire que tout facteur premier de F_n est de la forme $k2^{n+1} + 1$.

Exercice 2.3.3. **I**

Pour quelles valeurs entières de (m, n) avec $n \geqslant m$ a-t-on $\sum_{i=m}^{n} \frac{1}{i} \in \mathbb{N}$? (On pourra poser $v_2(j)$ puissance de 2 dans la décomposition en produit de facteurs premiers de j.)

Exercice 2.3.4. **I**

Montrer qu'il existe une infinité de points de $\mathbb{Q}^2$ sur le cercle $\Gamma = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$.

Exercice 2.3.5. **I**

Montrer que 21 divise $2^{4^n} + 5$ pour tout entier de $\mathbb{N}^*$.

Exercice 2.3.6. **I**

Déterminer les deux derniers chiffres de l'écriture décimale de 3^{2018}.

Exercice 2.3.7. **I**

Soient N_1, N_2, ..., N_q q éléments de $\mathbb{Z}^*$ distincts. On pose $p_k = \prod_{i=1}^{q}(N_i + k)$ et on suppose que pour tout k de $\mathbb{Z}$, p_0 divise p_k.

(1) Montrer qu'il existe i tel que $|N_i| = 1$.
(2) On suppose de plus que, pour tout i, $N_i \geqslant 1$, montrer que $\{N_1, N_2, \ldots, N_q\} = [1, q]$.

2.4. **Idéaux de $\mathbb{K}[X]$.**

Exercice 2.4.1. **I**

Montrer que toute suite croissante d'idéaux de $\mathbb{K}[X]$ est stationnaire. Un anneau A est factoriel si et seulement si il est commutatif unitaire intègre et
On dit qu'un anneau A est factoriel si, pour tout a de A non nul, il existe u élément inversible, p_1, p_2,..., p_n, n éléments irréductibles tels que $a = u.p_1p_2 \ldots p_n$. La décomposition est unique aux inversibles près et à l'ordre près.
On montre alors que tout anneau principal est factoriel en construisant une suite croissante d'idéaux (cf. par exemple
http://pagesperso-orange.fr/christian.squarcini/AgregInterne/Anneauxcorps/3_3.pdf).

Indication 1.1.1

(1) On a $z^n = 1$ pour tout élément d'un sous-groupe de cardinal n.
(2) Immédiat, utiliser la caractérisation de $\mathbb{U}_n$.
(3) Procéder par double inclusion, utiliser Bézout pour la première égalité, pour la deuxième, utiliser les cardinaux.

Indication 1.1.2 Pour l'implication directe, raisonner par contraposée et utiliser le fait que $m = a \wedge b < ab$. Pour la réciproque, montrer que $(1, 1) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est d'ordre ab.

Indication 1.2.1 Penser à chaîner les transpositions.

Indication 1.2.2

(1) Immédiat.
(2) Utiliser Bézout pour l'existence, pour l'unicité, si $rs = r's'$, poser $t = r^{-1}r' = s'^{-1}s$.
(3) Faire intervenir l'identité de Bézout $\alpha k + \beta n = 1$ ($k = 2$ pour le a) et poser $\psi(x) = x^\alpha$.

Indication 1.2.3

(1) Calculer $(xy)^m$ puis donner un contre-exemple où on n'a pas égalité (prendre $G = \mathbb{Z}/n\mathbb{Z}$ avec n bien choisi.
(2) On a égalité dans ce cas (montrer que l'ordre de xy est ab).
(3) Prendre $G = \mathfrak{S}_3$ pour avoir un contre-exemple.

Indication 1.2.4

(1) Utiliser le fait que dans un groupe fini, la multiplication à gauche réalise une permutation des éléments de ce groupe.
(2) Utiliser la relation $\mathrm{Tr}(P) = \mathrm{Rg}(P)$.

Indication 1.2.5

(1) Calculer $(xy)^2$ de 2 façons différentes.
(2) $H \cap aH = \emptyset$ par l'absurde, pour montrer que $H \cup aH$ est un sous-groupe, montrer la stabilité par produit en distinguant les cas x, y dans H, dans aH, l'un dans H, l'autre dans aH.
(3) Construire par récurrence des sous-groupes H_i de G tels que $H_i = H_{i-1} \cup a_i H_{i-1}$.

Indication 1.2.6 Pour prouver la formule, faire une partition de $\mathbb{U}_n$ selon les diviseurs de n. Utiliser ensuite un corollaire du théorème de Lagrange : l'ordre d'un élément divise l'ordre du groupe et écrire que $G = \bigcup_{d|n} \Omega(d)$ (réunion disjointe) où $\Omega(d)$ désigne l'ensemble des éléments de G d'ordre d. Montrer ensuite que $\mathrm{Card}\,\Omega(d) = 0$ ou $\varphi(d)$ et conclure.
On applique le résultat à $G = (\mathbb{K} \setminus \{0\}, \times)$.

Indication 2.1.1 Faire le même genre de raisonnement que sur $\mathbb{Z}$, si x est un générateur de $(a) + (b)$, poser $y = \alpha\beta x$ où $a = \alpha x$ et $b = \beta x$ et montrer que y est générateur de $(a) \cap (b)$.

Indication 2.1.2

(1) Pas de problème pour montrer que $\mathcal{N}$, l'ensemble des éléments nilpotents de A est absorbant. Pour la stabilité par $+$, élever $a + b$ à une puissance convenable et utiliser la formule de Newton.
(2) Montrer qu'un élément de $\mathbb{Z}/n\mathbb{Z}$ est nilpotent ssi il est multiple du produit de tous les diviseurs de n.
(3) Prendre $\mathcal{M}_2(\mathbb{R})$.

Indication 2.2.1

(1) a convient ssi $a = a^2$. Si n est premier alors $a = 0$ ou $a = 1$, sinon on peut trouver d'autres valeurs (prendre des exemples). Seule γ_1 est un morphisme d'anneaux.
(2) $\mathrm{Ker}\,\gamma_a = \{0\}$, raisonner par contraposée en démontrant le petit théorème de Fermat i.e. si n est premier alors n divise $a^n - a$.

Indication 2.2.2 1. Faire une récurrence, 2. utiliser $a^n - b^n = (a - b)(a^{n-1} + \cdots)$, 3. écrire $10^{6n} + 10^{3n} - 2 = (10^{3n} + 2)(10^{3n} - 1)$.

Indication 2.2.3

(1) Étudier les différents cas en supposant $x \leqslant y \leqslant z$ (3 triplets solutions).
(2) Étudier les différents cas en supposant $x \leqslant y \leqslant z$ (une seule solution).

Indication 2.2.4 Poser $u_n = \lambda\alpha^n + \mu\beta^n$ ($\lambda = \mu = 1$ pour le 1) et trouver des relations entre u_n et u_{n+1}.
Pour le 2) on trouve $\lambda \wedge \mu = \lambda \wedge \beta = \mu \wedge \alpha = (\beta - \alpha) \wedge (\lambda + \mu) = 1$.

Indication 2.3.1 Utiliser $n!$...

Indication 2.3.2

(1) Utiliser l'égalité $a^m + b^m = (a+b)(a^{m-1} - \cdots + b^{m-1}$ (m impair) ou raisonner dans $\mathbb{Z}/3\mathbb{Z}$.
(2) Utiliser la même égalité que ci-dessus ou raisonner dans $\mathbb{Z}/2^{2^k}\mathbb{Z}$.
(3) Vu que $\omega(2) = 2^{n+1}$ en déduire que $q = 2^{2^{n+1}}k + 1$.

Indication 2.3.3 Montrer qu'il existe un unique $j \in [\![m, n]\!]$ tel que $j = 2^r k$ avec r maximal puis, en réduisant les termes de la somme au même dénominateur, prouver que cette somme est de la forme $\frac{2K+1}{2^r L}$ et ne peut être un entier que si $n = m = 1$.

Indication 2.3.4 le problème est équivalent à chercher les entiers (a, b, c) premiers entre-eux et tels que $a^2 + b^2 = c^2$ et à prouver que cet ensemble est infini.

Indication 2.3.5 Se placer dans $\mathbb{Z}/3\mathbb{Z}$ et dans $\mathbb{Z}/7\mathbb{Z}$.

Indication 2.3.6 Chercher à quoi est congru 3^{2018} modulo 100.

Indication 2.3.7

(1) Utiliser le fait que $r = \frac{p_1 p_{-1}}{p_0^2}$ est un entier.
(2) Prendre $N_1 = 1$ et (toujours après renumérotation) prouver par récurrence que $N_i = i$ pour $i \leqslant k$.

Indication 2.4.1 Montrer que I réunion des idéaux est un idéal.

1. Solutions :

Solution 1.1.1

(1) Soit G un sous-groupe de cardinal n de $\mathbb{C}^*$, on a $z^n = 1$ pour tout élément de G donc $G \subset \mathbb{U}_n$ et, en comparant les cardinaux, on en déduit que $G = \mathbb{U}_n$.

(2) $\Rightarrow$ on utilise la remarque $z \in \mathbb{U}_n \Leftrightarrow z^n = 1$ donc si $n|m$ alors $z^m = 1$ ce qui donne l'inclusion.
$\Leftarrow$ On a $\omega_n = e^{i\frac{2\pi}{n}} \in \mathbb{U}_m$ donc $\omega_n^m = e^{i\frac{2\pi m}{n}} = 1$ donc $\dfrac{m}{n}$ est un entier i.e. $n|m$.

(3) $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_d$: $d|n$ et $d|m$ donc $\mathbb{U}_d \subset \mathbb{U}_n \cap \mathbb{U}_m$.
Réciproquement, on utilise Bézout : si $z^n = 1$ et $z^m = 1$ alors on sait qu'il existe (u, v) tels que $un + vm = d$ donc $z^{un+vm} = z^d = 1$ soit $\mathbb{U}_n \cap \mathbb{U}_m \subset \mathbb{U}_d$ ce qui donne l'égalité.
$\mathbb{U}_n.\mathbb{U}_m = \mathbb{U}_p$: p est un multiple de m et n donc, si $Z = zz'$ alors $Z^p = z^p z'^p = 1$ donc $\mathbb{U}_n.\mathbb{U}_m \subset \mathbb{U}_p$.
Pour l'inclusion dans l'autre sens, comme il n'est pas immédiat d'écrire $Z = zz'$, on utilise un argument sur les cardinaux : $\mathbb{U}_n.\mathbb{U}_m$ est un sous-groupe de $\mathbb{C}^*$ et il contient moins de nm éléments (en effet $(k, l) \in [\![0, n-1]\!] \times [\![0, m-1]\!] \mapsto e^{i2k\pi/n}.e^{i2l\pi/m} \in \mathbb{U}_n \times \mathbb{U}_m$ est surjective). $\mathbb{U}_n \times \mathbb{U}_m$ est un sous-groupe de cardinal s de $\mathbb{C}^*$ donc égal à $\mathbb{U}_s$. Or $\mathbb{U}_n \subset \mathbb{U}_s$ et $\mathbb{U}_m \subset \mathbb{U}_s$ donne $n|s$ et $m|s$ d'où $\mathbb{U}_p \subset \mathbb{U}_s = \mathbb{U}_n \times \mathbb{U}_m$ d'où l'inclusion annoncée.

Solution 1.1.2

$\Rightarrow$ On raisonne par contraposée, comme $md = ab$ où $m = a \wedge b$ et $d = a \wedge b$, $d > 1 \Rightarrow m < ab$. Si $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ alors $m(x, y) = (0, 0)$ et par conséquent aucun élément de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ne peut être d'ordre ab. Vu que $\operatorname{Card} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = ab$, on en déduit que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ n'est pas cyclique.

$\Leftarrow$ Si $a \wedge b = 1$ alors $k(1, 1) = (0, 0)$ entraîne $a|k$ et $b|k$ soit $ab|k$ donc $(1, 1)$ est un élément d'ordre ab. Il engendre un sous-groupe de cardinal ab de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ donc c'est un générateur de ce groupe i.e. $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique.

Solution 1.2.1 Non, en effet :

- Si toutes les transpositions sont chaînées, il y aura un élément invariant car si p transpositions sont chaînées alors elles n'opèrent que sur un maximum de $p + 1$ éléments. Si $p = n - 2$ alors il y a au moins un élément qui n'est pas concerné par ces transpositions.
- Si elles ne sont pas toutes chaînées, il y aura une transposition (i, j) qui n'aura aucun élément commun avec les autres. On ne pourra donc pas obtenir les transpositions de la forme (i, k) avec $k \neq j$.

Solution 1.2.2

(1) H_a contient e, il est donc non vide, la stabilité est immédiate et si $x \in H_a$ alors $(x^{-1})^a = x^{-a} = e$ donc H_a est un sous-groupe de G (de même pour H_b !)

(2) On utilise Bézout, on a $\alpha a + \beta b = 1$ d'où

$$x = x^{\alpha a + \beta b} = (x^a)^\alpha (x^b)^\beta = rs$$

où $r = (x^a)^\alpha \in H_a$ et $s = (x^b)^\beta \in H_b$ ce qui assure l'existence.
Montrons l'unicité : si $rs = r's'$ alors $r^{-1}r' = s'^{-1}s = t$ où $t \in H_a \cap H_b$.
On a $t^a = e$ car $t = u^b \in H_b$, de même $t^b = e$ alors en reprenant l'identité de Bézout, on a $t = (t^a)^\alpha.(t^b)^\beta = e$ i.e. $r = r'$ et $s = s'$ ce qui prouve l'unicité.

(3) Cas n impair

a) G étant commutatif $\varphi(x) = x^2$ est bien un morphisme. Il est bien évidemment bijectif. $n = 2p+1$ car n est impair, posons $\psi(x) = x^{p+1}$ alors $\psi(\varphi(x)) = (x^2)^{p+1} = x^{2p+2} = x$ et $\varphi(\psi(x)) = (x^{p+1})^2 = x$ donc ψ est bien l'application réciproque de φ.

b) En fait, pour k premier avec n, on va faire intervenir l'identité de Bézout $\alpha k+\beta n = 1$ et, comme à la question précédente, $\psi(x) = x^\alpha$ est bien l'automorphisme inverse de $\varphi(x) = x^k$.

Solution 1.2.3

(1) Comme $(xy)^m = x^m y^m = 1$ (car G est abélien) on en déduit que l'ordre de xy divise $m = a \vee b$. On n'a pas égalité en général comme le prouve l'exemple dans $\mathbb{Z}/24\mathbb{Z}$ avec $x = 2$, $y = 4$. x est d'ordre 12, y est d'ordre 6, le p.p.c.m. vaut 12 or l'ordre de $xy = 8$ est 3.

(2) Si $a \wedge b = 1$ on va prouver que l'ordre de xy est bien m. Supposons pour cela que $(xy)^n = x^n y^n = 1$ avec $x^n \neq 1$ alors $z = x^n = y^{-n} \neq 1$ est dans $(x) \cap (y)$, son ordre divise donc a et b i.e. $z = 1$ ce qui est contradictoire. Par conséquent, $(xy)^n = 1$ entraîne n multiple de a et b donc $m = ab$ est bien ici l'ordre de xy.

(3) Si G n'est pas abélien alors rien ne s'applique. En effet, dans $\mathfrak{S}_3$, la transposition $\tau = (1, 2)$ est d'ordre 2, le cycle $\sigma = (1, 3, 2)$ est d'ordre 3 alors que $\sigma\tau = (2, 3)$ est d'ordre 2. Enfin, si on prend la transposition $\tau' = (2, 3)$ alors $\tau'\tau = \sigma$ qui est d'ordre 3.

Solution 1.2.4

(1) Dans un groupe, la multiplication à gauche est bijective et dans un groupe fini, elle réalise une permutation des éléments de ce groupe. On a donc

$$N \sum_{M \in G} M = \sum_{M \in G} M.$$

On a alors $NP = P$ et donc $\dfrac{1}{p}\left(\sum_{N \in G} N\right) P = P^2 = P$ i.e. P est un projecteur.

(2) Dans le cas particulier où $\mathrm{Tr}(P) = 0$ alors la dimension de l'image de P est nulle ce qui signifie que $P = 0$ (cf *proposition 2.1.8 page 185*).

Solution 1.2.5

(1) On a $e = x^2y^2 = xy.xy$ et, en composant par x à gauche et par y à droite, on obtient $xy = yx$ donc G est commutatif.

(2) Soit $x \in H \cap aH$ alors il existe y dans H tel que $x = ay$ et donc $xy = ay^2 = a$ et donc $a \in H$ ce qui est exclu donc $H \cap aH = \emptyset$.
Posons alors $H_1 = H \cup aH$ et montrons la stabilité ($H_1 \neq \emptyset$).
- Si x et y sont dans H : OK
- Si $x = ax'$ et $y = ay'$ (où x' et y' sont dans H) alors $xy = a^2x'y' = x'y' \in H$.
- Si $x = ax'$ (où $x' \in H$, $y \in H$) alors $xy = ax'y \in aH$.

Conclusion : dans tous les cas, on a prouvé la stabilité. La stabilité par l'inverse est immédiate car dans G, tout élément est égal à son propre inverse.

(3) On peut ainsi, par récurrence construire des sous-groupes H_i de G tels que $H_i = H_{i-1} \cup a_iH_{i-1}$ avec $\mathrm{Card}\, H_i = 2\,\mathrm{Card}\, H_{i-1}$. Partant de $H_0 = \{e\}$, on aura $\mathrm{Card}\, H_i = 2^i$. Comme G est fini, l'ensemble des entiers i tels que la construction ci-dessus soit possible est aussi fini. Si n désigne le plus grand, alors $H_n = G$ (sinon, le processus pourrait se répéter) et donc $\mathrm{Card}\, G = 2^n$.

Remarque : on pouvait directement obtenir ce résultat en considérant G comme espace vectoriel sur $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$. On définit la loi externe par $x * g = \begin{cases} e & \text{si } x = \dot{0} \\ g & \text{si } x = \dot{1} \end{cases}$ (en d'autres termes $x * g = g^x$).

Solution 1.2.6 Commençons par prouver la formule (on pose $n = \operatorname{Card} G$) :

dans $\mathbb{U}_n$ ensemble des racines n-ièmes de l'unité on fait la partition suivante $\mathbb{U}_n = \bigcup_{d|n} \mathbb{P}_d$ où P_d est une racine primitive d-ième de l'unité (i.e. $P_d = \{z \in \mathbb{U} \mid z \text{ engendre } \mathbb{U}_d\}$. Or $\operatorname{Card} P_d = \varphi(d)$ ce qui prouve la formule.

- Soit d un diviseur de n, soit x un élément de G d'ordre d (i.e. le cardinal de l'ensemble engendré par x noté $\omega(x)$). $x^d = e$ donc $(x) \subset G_d$ et $\operatorname{Card}(x) = d \geqslant \operatorname{Card} G_d$ donc $G_d = (x)$. Si y est un autre élément de G tel que $\omega(y) = \omega(x)$ alors $(x) = (y) = G_d$.
- On sait que l'ordre de tout élément est un diviseur de l'ordre du groupe donc, si on note $\Omega(d)$ l'ensemble des éléments de G d'ordre d, on a $G = \bigcup_{d|n} \Omega(d)$ (réunion disjointe) donc $n = \operatorname{Card} G = \sum_{d|n} \operatorname{Card} \Omega(d)$.
- Montrons que $\operatorname{Card} \Omega(d) = 0$ ou $\varphi(d)$. Si $\Omega(d) \neq \emptyset$ alors il existe $x \in G_d$ tel que $G_d = (x)$. Si on considère l'application $\psi : k \in \mathbb{Z}/d\mathbb{Z} \mapsto x^k$ (application bien définie car $x^d = e$) alors ψ est un isomorphisme de groupe et le cardinal de l'ensemble des générateurs de $\mathbb{Z}/d\mathbb{Z}$ vaut $\varphi(d)$, on en déduit que $\operatorname{Card} \Omega(d) = \varphi(d)$.

Conclusion : comme $n = \sum_{d|n} \operatorname{Card} \Omega(d) = \sum_{d|n} \varphi(d)$ et que $\operatorname{Card} \Omega(d) \leqslant \varphi(d)$ c'est que on a égalité pour tout diviseur d de n. Ceci est vrai en particulier pour $d = n$ donc G admet un générateur et finalement G est bien cyclique.
On applique le résultat à $G = (\mathbb{K} \setminus \{0\}, \times)$. En effet, dans un corps, l'équation $x^p - 1 = 0$ a au plus p racines (résultat général sur les polynômes).

Solution 2.1.1 On raisonne comme sur $\mathbb{Z}$. Soit $\mathcal{I}$ l'idéal $(a) + (b)$ supposé principal, on note x un générateur de cet idéal. On a alors $a = \alpha x$ et $b = \beta x$ avec $(\alpha, \beta) \in A^2$. Si on pose $y = \alpha\beta x$ alors $y \in (a) \cap (b)$ (on a supposé A commutatif) et donc $(y) \subset (a) \cap (b)$.
Prouvons l'inclusion dans l'autre sens. Si $z \in (a) \cap (b)$ alors on peut écrire $z = ua = vb$ et en exploitant le fait que $(x) = (a) + (b)$ on a

$$\begin{aligned} x &= ra + sb = r\alpha x + s\beta x = (r\alpha + s\beta)x \\ z &= ua = \alpha ux = \alpha u(r\alpha + s\beta)x \\ &= \alpha ur\alpha x + us(\alpha\beta x) = (\alpha r)(\alpha x u) + (us)y. \end{aligned}$$

Et comme $z = ua = bv = \alpha x u = \beta x v$ on a

$$\begin{aligned} z &= (\alpha r)(\beta x v) + (us)y = (rv)(\alpha\beta x)) + (us)y \\ &= (rv)y + (us)y = (rv + us)y. \end{aligned}$$

et, en conclusion on a l'autre inclusion c.q.f.d.

Solution 2.1.2 (1) Soit $\mathcal{N}$ l'ensemble des éléments nilpotents de A. On vérifie sans peine que si $a \in \mathcal{N}$ et $\alpha \in A$ alors $\alpha a \in \mathcal{N}$. $\mathcal{N} \neq \emptyset$ car $0 \in \mathcal{N}$. Montrons que $\mathcal{N}$ est stable par addition : si a et b sont nilpotents d'ordres respectifs n et p alors

$$(a+b)^{n+p} = \sum_{k=0}^{n+p} C_{n+p}^k a^{n+p-k} b^k = \underbrace{a^n \sum_{k=0}^{p} C_{n+p}^k a^{p-k} b^k}_{=0 \text{ car } a^n=0} + \underbrace{b^p \sum_{k=p+1}^{n+p} C_{n+p}^k a^{n+p-k} b^{k-p}}_{=0 \text{ car } b^p=0} = 0$$

donc $a+b \in \mathcal{N}$ ce qui permet de conclure que $\mathcal{N}$ est un idéal.

(2) Dans $\mathbb{Z}/n\mathbb{Z}$, un élément a est nilpotent ssi son antécédent a' dans $\mathbb{Z}$ est multiple du produit de tous les facteurs premiers qui interviennent dans la décomposition de n.
En effet, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ et si $a' = p_1 \dots p_k \times b$ alors, en posant $\alpha = \max(\alpha_i)$ pour $i \in [1,k]$ on a $a'^{\alpha} = n b^{\alpha} p_1^{\alpha-\alpha_1} \dots p_k^{\alpha-\alpha_k}$ donc $a^{\alpha} = 0$.
Réciproque : s'il existe $\alpha > 0$ tel que $a^{\alpha} = 0$ alors, pour tout i de $[1,k]$ on a $p_i | a'^{\alpha}$ donc $p_i | a'$. Comme les p_i sont premiers entre-eux alors $p_1 \dots p_k$ divise a'.

(3) Si on prend $\mathcal{M}_2(\mathbb{R})$ comme anneau alors les matrices $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$ sont nilpotentes d'ordre 2 mais $A+B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ étant inversible (matrice de rotation d'angle π) ne peut être nilpotente.

Solution 2.2.1

(1) f est bien sûr un morphisme de groupe additif. Ensuite

$$\gamma_a(1.1) = a = \gamma_a(1).\gamma_a(1) = a^2$$

et on vérifie aisément que cette condition entraîne que $\gamma_a(xy) = \gamma_a(x)\gamma_a(y)$.
Si n est premier alors $\mathbb{Z}/n\mathbb{Z}$ est un corps et donc les seules solutions sont $a = 0$ et $a = 1$.
Si n n'est pas premier alors on pourra trouver d'autres valeurs de a convenables. En effet, il suffit que $(a-1)a = 0$ i.e. $(a-1)a = 0 \mod n$ en passant aux antécédents dans $\mathbb{Z}$.
Par exemple pour $n = 2\times 3 = 6$ alors $a = 3$ vérifie $a^2 = a$, $n = 3\times 4 = 12$ avec $a = 4$, $n = 15$ avec $a = 6$...
Si γ_a est un morphisme d'anneau alors $\gamma_a(1) = a = 1$ donc il n'y a que l'application identique qui convient...

(2) Si $x \in \operatorname{Ker} \gamma_a$ alors $ax = 0$ et comme $a \wedge n = 1$ alors a est inversible (cf. *proposition 1.2.9 page 176*) donc $x = 0$. γ_a est injective et comme $\mathbb{Z}/n\mathbb{Z}$ est fini, γ_a est bijective donc γ_a est un automorphisme de groupe.
Si n est premier alors n divise $a^n - a$ (qu'on appelle de P.T.F., petit théorème de Fermat par opposition au grand) (raisonner par récurrence sur a en écrivant $(a+1)^n - (a+1) = a^n - a + \sum_{p=1}^{n-1} \binom{n}{p} a^p$, chacun des termes de cette somme étant divisible par n).
Par contraposée, on peut conclure.

Solution 2.2.2

(1) On le vérifie pour $n = 1$, $n = 2$ et pour $n \geqslant 3$, on a (par récurrence) :

$$9^{2n+1} + 8^{n+2} = (9^{2n-1} + 8^{n+1})(9^2 + 8) - 8.9^2(9^{2n-3} + 8^n) \equiv 0[73]$$

(2) $16^n - 15n - 1 = 15(16^{n-1} + \dots + 1 - n)$ (on utilise ici l'identité $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$ cf *proposition 7.3.10 page 126* avec $a = 16$ et $b = 1$). Or, comme $16^k - 1 \equiv 0[15]$ on a $16^{n-1} + \dots + 1 - n \equiv 0[15]$ et en conclusion $16^n - 15n - 1 \equiv 0[15^2]$

$(15^2 = 225)$.
(On pouvait aussi écrire que $16 = 15 + 1$ et utiliser le binôme de Newton.)

(3) On vérifie que : $10^{6n} + 10^{3n} - 2 = (10^{3n} + 2)(10^{3n} - 1)$ et que $10^{3n} - 1 \equiv 1[999] \equiv 1[111]$.

Solution 2.2.3

(1) On a nécessairement $x \geqslant 2$, $y \geqslant 2$, $z \geqslant 2$. Supposons $x \leqslant y \leqslant z$.
- Si $x = 2$ alors $\dfrac{1}{y} + \dfrac{1}{z} = \dfrac{1}{2}$ donc $y > 2$.
  - Si $y = 3$ alors $z = 6$.
  - Si $y = 4$ alors $z = 4$.
- Si $x = 3$ alors $y = z = 3$.

On obtient finalement les solutions (en supposant $x \leqslant y \leqslant z$) :

$$(x, y, z) = (3, 3, 3),\ (x, y, z) = (2, 3, 6),\ (x, y, z) = (2, 4, 4).$$

(2) Quitte à permuter x, y et z, on peut supposer là aussi que $x \leqslant y \leqslant z$.
- Si $x \geqslant 2$ alors on pose $x = 2 + x_1$, $y = 2 + y_1$, $z = 2 + z_1$ ($x_1 \geqslant 0$, $y_1 \geqslant 0$, $z_1 \geqslant 0$) on trouve une impossibilité car

$$\begin{aligned} xyz = (2 + x_1)(2 + y_1)(2 + z_1) &\geqslant 8 + 2(x_1 + y_1 + z_1) \\ &> 7 + x_1 + y_1 + z_1 = 1 + x + y + z \end{aligned}$$

- Nécessairement $x = 1$ et donc $yz = 2 + y + z$.
  - Si $y \geqslant 3$, on obtient de la même manière une impossibilité, en posant $y = 3 + y_1$, $z = 3 + z_1$

$$yz = (3 + y_1)(3 + z_1) \geqslant 9 + 3(y_1 + z_1) > 8 + y_1 + z_1 = 2 + y + z.$$

  - $y = 1$ est impossible (on aurait $z = 3 + z$).
  - Il ne reste donc que le cas $y = 2$ ce qui donne $z = 4$.

Conclusion : on a $x = 1$, $y = 2$ et $z = 4$ comme seule solution vérifiant $x \leqslant y \leqslant z$.

Solution 2.2.4

(1) Soit $u_n = 5^n + 6^n$ alors $6u_n - u_{n+1} = 5^n$ et $5u_n - u_{n+1} = -6^n$. Or $5 \wedge 6 = 1$ donc $5^n \wedge 6^n = 1$ soit il existe $(x, y) \in \mathbb{Z}^2$ tel que $x5^n + y6^n = 1$ d'où $(6x - 5y)u_n + (y - x)u_{n+1} = 1$ i.e. $u_n \wedge u_{n+1} = 1$.

(2) Une condition nécessaire et suffisante pour que t_n soit irréductible pour tout n est $\lambda \wedge \mu = \alpha \wedge \mu = \beta \wedge \lambda = (\beta - \alpha) \wedge (\lambda + \mu) = 1$.
Montrons l'implication directe par l'absurde.
On suppose qu'il existe $n \in \mathbb{N}^*$ et p premier tel que $p | \lambda\alpha^{n+1} + \mu\beta^{n+1}$ et $p | \lambda\alpha^n + \mu\beta^n$.
On va alors raisonner dans $\mathbb{Z}/p\mathbb{Z}$ qui est un corps et on garde les mêmes écritures pour les éléments de $\mathbb{Z}$ et leur classe dans $\mathbb{Z}/p\mathbb{Z}$.
On a ainsi $\lambda\alpha^n = -\mu\beta^n$ et $\lambda\alpha^{n+1} = -\mu\beta^{n+1}$.
- Si $\alpha = 0$ alors $\mu\beta^n = 0$ donc $\mu = 0$ ou $\beta = 0$ ce qui est impossible car on a supposé que $\alpha \wedge \mu = \alpha \wedge \beta = 1$.
- Il en est alors de même de β, λ, μ.
- On a alors $\lambda = -\mu \left(\dfrac{\beta}{\alpha}\right)^n = -\mu \left(\dfrac{\beta}{\alpha}\right)^{n+1}$ d'où, en simplifiant par $\mu \left(\dfrac{\beta}{\alpha}\right)^n$, on obtient $\dfrac{\beta}{\alpha} = 1$ soit $\beta = \alpha$ et $\lambda = -\mu$.
- On revient à $\mathbb{Z}$, on a prouvé que $p | \beta - \alpha$ et $p | \lambda + \mu$ ce qui est contradictoire et prouve l'implication directe.

Réciproquement : si $(\beta-\alpha)\wedge(\lambda+\mu)\neq 1$, soit p premier qui divise $\beta-\alpha$ et $\lambda+\mu$ alors, dans $\mathbb{Z}/p\mathbb{Z}$, $\lambda\alpha^n=-\mu\beta^n$ pour tout $n\in\mathbb{N}$ donc $p|\lambda\alpha^n+\mu\beta^n$ ce qui prouve la réciproque par contraposée.

Solution 2.3.1 Il suffit de prendre $x_i=i+(n+1)!$ pour $i\in[2,n+1]$ alors chaque x_i est divisible par i.

Solution 2.3.2

(1) Si m est impair, on pose $m=2q+1$, on a alors

$$\begin{aligned}2^{2q+1}+1&=2^{2q+1}+1^{2q+1}\\&=(2+1)(2^{2^{2q}}-2^{2q-1}+\cdots+1)\end{aligned}$$

(cf *proposition 7.3.10 page 126*) donc 2^m+1 n'est pas premier (sauf pour $m=1$ cas écarté).
On peut aussi raisonner dans $\mathbb{Z}/3\mathbb{Z}$, comme $n=2.4^q+1$ alors $4^q\equiv 1[3]$ donc $4^q\equiv 1[3]$ et $2.4^q\equiv -1[3]$ soit $n\equiv 0[3]$.

(2) Si m est pair ($m>0$), on écrit $m=2^k(2q+1)$ avec $k\geqslant 1$. Si $q\geqslant 1$ alors, avec $l=2^{2^k}$ on a

$$2^m+1=l^{2q+1}+1$$

et, avec la même identité que celle utilisée ci-dessus, on en déduit que 2^m+1 n'est pas premier. On peut aussi raisonner dans $\mathbb{Z}/2^{2^k}\mathbb{Z}$ en remarquant que, comme $2^{2^k}\equiv -1\left[2^{2^k}+1\right]$ alors $2^{2^{k+1}}\equiv 1\left[2^{2^k}+1\right]$ puis $n\equiv 0\left[2^{2^k}+1\right]$.
Conclusion : il est nécessaire que m soit de la forme 2^k (ou $m=0$) pour que 2^m+1 soit premier.

(3) Si q est un facteur premier de F_n alors $2^{2^n}\equiv -1[q]$ et donc $2^{2^{n+1}}\equiv 1[q]$. On a donc $2^{n+1}=\omega(2)k$ et comme 2^n n'est pas un multiple de $\omega(2)$ alors k est impair. Or k divise 2 donc $k=1$.
On sait aussi que $\omega(2)$ divise $\operatorname{Card}\mathbb{Z}/q\mathbb{Z}\backslash\{0\}=q-1$, on peut conclure que $q=2^{2^{n+1}}k+1$.
On prouve en fait que si $F_n=2^{2^n}+1$ admet un diviseur, alors celui ci est de la forme $p.2^q+1$ avec p entier premier impair et $q\geqslant n+2$. C'est le théorème d'Euler associé au test de Pépin. Ceci a permis à Euler de factoriser $F_5=(5\times 2^7+1)(52347\times 2^7+1)$.
Il ne faut pas confondre nombres de Fermat et nombres de Mersenne qui sont eux de la forme $M_p=2^p-1$. On vient de voir que les nombres de Fermat premiers sont de la forme $2^{2^k}+1$ ce qui donne des nombres très grand et limite l'intérêt de ces nombres. Par contre les nombres de Mersenne sont plus raisonnables et sont l'objet de recherches actives pour battre des records (le record connu à ce jour—23 août 2008 GIMPS / Smith— est obtenu pour $p=43112609$ et a 12 978 189 chiffres).

Solution 2.3.3 On choisit m et on va chercher s'il existe n tel que $S(n)=\sum_{i=m}^{n}\frac{1}{i}$ soit un entier.

Si $n=m$ alors $S(n)=\dfrac{1}{m}$ et $S(n)\in\mathbb{N}$ ssi $m=1$.
La question que l'on se pose est : peut-on trouver $n>m$ tel que $S(n)$ soit entier ?
Pour tout $j\in\mathbb{N}^*$, on note $v_2(j)$ l'exposant de 2 dans la décomposition de j en produit de facteurs premiers. Soit $r=\sup_{m\leqslant j\leqslant n} v_2(j)$ ($r\geqslant 1$ car on a au moins un nombre pair), montrons que ce sup est atteint en un seul j.
Tout d'abord, il est bien atteint car on n'a qu'un nombre fini d'éléments.

Ensuite, si $v_2(j_1) = v_2(j_2) = r$ avec $m \leqslant j_1 < j_2 \leqslant n$ alors $j_1 = 2^r i_1$ et $j_2 = 2^r i_2$. Comme $i_1 < i_2$ sont impairs, il existe forcément un entier pair compris entre i_1 et i_2, noté $2k$. On a alors $n \leqslant 2^{r+1}k \leqslant m$ ce qui contredit la maximalité de r. On note l l'unique nombre où ce maximum est atteint et α la valeur de ce maximum.
Soit Π le P.P.C.M. de i, pour $i \in [m, n]$ alors $\Pi = 2^\alpha(2q+1)$ et

$$S(n) = \sum_{i \neq l} \frac{1}{i} + \frac{1}{l} = \frac{2A}{\Pi} + \frac{2B+1}{\Pi}$$

car pour tous les $i \neq l$, $\dfrac{1}{i} = \dfrac{2A_i}{\Pi}$ car $v_2(i) \leqslant v_2(\Pi) - 1$ et $\dfrac{1}{l} = \dfrac{2B+1}{\Pi}$ car $v_2(l) = v_2(\Pi)$.
On a donc $S(n) = \dfrac{2(A+B)+1}{\Pi} \notin \mathbb{N}$.
La seule solution au problème est donc $m = n = 1$.

Solution 2.3.4 Soit $x = \dfrac{p}{q}$ et $y = \dfrac{r}{s}$ deux rationnels tels que $(x, y) \in \Gamma$ on a alors $p^2s^2 + r^2q^2 = q^2s^2$. En fait, le problème est équivalent à chercher les entiers (a, b, c) premiers entre-eux et tels que $a^2 + b^2 = c^2$ et à prouver que cet ensemble est infini.
Prenons par exemple b entier non nul et $c = b + 1$ alors $a^2 = 2b + 1$. Si on choisit $a = 2n + 1$ pour n entier naturel, alors $b = 2n^2 + 2n$ et $c = 2n^2 + 2n + 1$. $b \wedge c = 1$ donc les entiers (a, b, c) sont premiers dans leur ensemble. Il reste à prouver qu'on obtient bien ainsi une infinité de points distincts de Γ. Par exemple, comme $x \mapsto \dfrac{2x+1}{2x^2+2x+1}$ est une fonction strictement décroissante sur $[0, +\infty[$ alors les points d'abscisse $\dfrac{2n+1}{2n2+2n+1}$ seront tous distincts.

Solution 2.3.5 Vu que $21 = 3\times7$, il suffit de prouver que $2^{4^n} + 5$ est divisible par 3 et 7.
Dans $\mathbb{Z}/3\mathbb{Z}$, $2^{2p} = 1$ donc $2^{4^n} + 5 = 1 + 5 = 0$ ce qui prouve la première divisibilité.
Montrons maintenant que $2^{4^n} - 2$ est divisible par 7 (ce qui permettra de conclure) :
Comme 2 et 7 sont premiers, cela revient à prouver que $2^{4^n-1} = 1$ dans $\mathbb{Z}/7\mathbb{Z}$. Or $2^3 = 1$ donc, il suffit de prouver que 3 divise $4^n - 1$ ce qui est immédiat dans $\mathbb{Z}/3\mathbb{Z}$.

Solution 2.3.6 En fait, cela revient à chercher à quoi est congru 3^{2018} modulo 100. On remarque que $3^{20} = 1$ dans $\mathbb{Z}/100\mathbb{Z}$. Or $2018 = 20\times100 + 18$ donc $3^{2018} = 3^{18} = 89$ dans $\mathbb{Z}/100\mathbb{Z}$.

Solution 2.3.7

(1) Comme p_0 divise p_1 et p_{-1} alors $r = \dfrac{p_1 p_{-1}}{p_0^2}$ est un entier. Or

$$r = \prod_{i=1}^{q} \frac{(N_i - 1)(N_i + 1)}{N_i^2} = \prod_{i=1}^{q} \left(1 - \frac{1}{N_i^2}\right)$$

donc, si pour tout i, $|N_i| > 1$ alors r serait élément de $]0, 1[$ et ne serait pas un entier. Il existe un entier N_i égal à ±1.

(2) On peut supposer, après renumérotation, que $N_1 = 1$. On fait alors l'hypothèse de récurrence sur k suivante :
il existe k entiers N_i prenant les valeurs $1, \ldots, k$ et après renumérotation, on prend $N_i = i$ pour $i \in [1, k]$.

On a alors p_{-k-1} divisible par p_0 ce qui s'écrit encore :

$$s = \frac{p_{-k-1}}{p_0} = \prod_{i=1}^{k} \frac{(i-k-1)}{i} \prod_{i=k+1}^{q} \frac{N_i - k + 1}{N_i} \text{ qui est entier}$$

$$= \frac{(-k)(-k+1)(\ldots)(-1)}{k!} \prod_{i=k+1}^{q} \left(1 - \frac{k+1}{N_i}\right) = (-1)^k \prod_{i=k+1}^{q} \left(1 - \frac{k+1}{N_i}\right).$$

Si pour chaque $i \geqslant k+1$, on avait $N_i > k+1$, $|s|$ serait dans $]0,1[$ et ne serait pas entier ce qui est écarté. Il existe donc un $j \geqslant k+1$ tel que $N_j \leqslant k+1$. Comme les entiers de 1 à k sont déjà pris, il ne reste pour N_j qu'a prendre la valeur $k+1$ ce qui achève la récurrence.

Solution 2.4.1 Soit (I_n) la suite des idéaux en question, posons $I = \bigcup_{n\in\mathbb{N}} I_n$ et montrons que I est un idéal.

- $I \neq \emptyset$.
- I est absorbant : si $A \in \mathbb{K}[X]$ et $P \in I$ alors il existe $n \in \mathbb{N}$ tel que $P \in I_n$ donc $AP \in I_n \subset I$.
- Si $(P,Q) \in I^2$ alors $P \in I_n$ et $Q \in I_m$ donc $P - Q \in I_p$ où $p = \max(n,m)$.

Il existe donc $R \in \mathbb{K}[X]$ tel que $I = (R)$ or il existe $n \in \mathbb{N}$ tel que $R \in I_n$ d'où $I \subset I_n \subset I$ soit $I = I_n$.