Anneaux : énoncés

Exercices CCP

1) Calculer $\displaystyle\sum_{0\leq 3k\leq n} \binom{n}{3k}$ (on utilisera la formule du binome de Newton).

2) Soit p un nombre premier. Montrer que l'ensemble

$$\mathbb{Z}_p = \{x \in \mathbb{Q},\ \exists\,(a,b) \in \mathbb{Z}\times\mathbb{Z}^*,\ x = \frac{a}{b} \text{ et } b \wedge p = 1\}$$

est un sous-anneau de $\mathbb{Q}$. Montrer que si un sous-anneau A de $\mathbb{Q}$ contient $\mathbb{Z}_p$, on a soit $A = \mathbb{Z}_p$, soit $A = \mathbb{Q}$.

3) Déterminer le groupe des inversibles de l'anneau $\mathbb{Z}/9\mathbb{Z}$ et trouver un groupe simple qui lui est isomorphe.

4) Résoudre dans $\mathbb{Z}$ les systèmes $\begin{cases} x \equiv 7\,[16] \\ x \equiv 21\,[55] \end{cases}$ et $\begin{cases} x \equiv 7\,[16] \\ x \equiv 21\,[68] \end{cases}$.

5) Quel est le reste de la division euclidienne de $P = X^{15} + 3X^{12} - 5X^{10} + 8X^7 + 5X^6 + 5X^4 - 3X^2 + 2$ par $(X-2)^2$?

6) Soit $n \in \mathbb{N}$. Montrer qu'il existe un unique couple $(a_n, b_n) \in \mathbb{Z}^2$ tel que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$. Montrer que $a_n \wedge b_n = 1$.

Exercices Mines-Centrale : anneaux

7) Soit A un anneau commutatif et I un idéal de A. Le radical de I est la partie :

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

a) Montrer que $\sqrt{I}$ est un idéal de A contenant I. Que vaut $\sqrt{\sqrt{I}}$?

b) Si J est un second idéal de A, montrer que $\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$ et $\sqrt{I\cap J} = \sqrt{\sqrt{I}\cap\sqrt{J}}$.

c) Déterminer les idéaux de $\mathbb{Z}$ et leurs radicaux.

8) Soit A un anneau et $a, b \in A$. Montrer que si $1-ab$ est inversible, $1-ba$ l'est également.

Exercices Mines-Centrale : l'anneau $\mathbb{Z}$

9) Soit p un nombre premier impair et soit q un diviseur de $2^p - 1$. Montrer que $q \equiv 1 \bmod 2p$.

10) a) Si p est premier, montrer que $(p-1)! \equiv -1 \bmod p$.

b) Calculer, si $n \in \mathbb{N}^*$, le reste de la division de $(n-1)!$ par n.

11) La fonction indicatrice d'Euler

a) Soient n et m deux entiers strictement positifs. Montrer que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ si et seulement si $n \wedge m = 1$.

Pour n entier ≥ 2, on note A_n l'ensemble des éléments x de $\mathbb{Z}/n\mathbb{Z}$ tels que x engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et $\varphi(n)$ le cardinal de A_n. On pose $\varphi(1) = 1$.

b) Montrer que $x = \overline{k} \in A_n \iff k \wedge n = 1$. En déduire que A_n est le groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

b) Calculer $\varphi(n)$ pour $n \in [\![2, 10]\!]$.

d) Calculer $\varphi(p^v)$ pour p premier et $v \in \mathbb{N}^*$.

e) Montrer que $\varphi(nm) = \varphi(n)\varphi(m)$ quand n et m sont premiers entre eux.

f) En déduire une expression de $\varphi(n)$ en fonction de la décomposition de n en produit de facteurs premiers.

g) Démontrer l'identité : $\forall n \in \mathbb{N}^*,\ n = \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d)$.

12) (Mines 2019) Soit p un nombre premier impair. On note C l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$, i.e.

$$C = \{x \in \mathbb{Z}/p\mathbb{Z},\ \exists y \in \mathbb{Z}/p\mathbb{Z},\ x = y^2\}.$$

a) Calculer le cardinal de C.

b) Calculer la classe de $(p-1)!$ modulo p et en déduire que si $p \equiv 1\ [4]$, -1 est un carré modulo p.

c) On suppose que -1 est un carré modulo p. Montrer que $p \equiv 1[4]$.

13) a) Soient $p, q \in \mathbb{N} \setminus \{0, 1\}$. Montrer que si $q^p - 1$ est premier, $q = 2$ et p est premier.

b) Montrer que si p est premier impair et si k est un diviseur de $2^p - 1$, k est congru à 1 modulo $2p$. On pourra commencer par étudier le cas où k est premier.

14) (Mines 22) Résoudre l'équation $2^n - 3^m = 1$ avec $n, m \in \mathbb{N}$.

15) (Mines 23) Résoudre $3^m = 8 + n^2$ dans $\mathbb{N}^2$.

16) Quelle est la nature de la série de terme général $\dfrac{\cos(\ln\, n)}{\ln\, n}$?

Exercices Mines-Centrale : l'anneau des polynômes

17) Résoudre dans $\mathbb{R}$ le système $\begin{cases} x + y + z = 1 \\ xy + yz + zx = -5 \\ x^3 + y^3 + z^3 = -2 \end{cases}$.

18) Trouvez un polynôme réel de degré minimal égal à $X^2 + X + 1$ modulo $P = X^4 - 2X^3 - 2X^2 + 10X - 7$ et à $2X^2 - 3$ modulo $Q = X^4 - 2X^3 - 3X^2 + 13X - 10$.

19) Trouvez P et Q dans $\mathbb{R}_{n-1}[X]$ tels que $(1 - X)^n P + X^n Q = 1$.

20) Déterminer les polynômes P non nuls tels que $P(X^2) = P(X)P(X + 1)$.

21) Soient $a_1, a_2, \ldots, a_n$ entiers relatifs distincts. Montrez que les polynômes

$$P = 1 + \prod_{i=1}^{n}(X - a_i)^2 \text{ et } Q = -1 + \prod_{i=1}^{n}(X - a_i)$$

sont irréductible dans $\mathbb{Z}[X]$, puis dans $\mathbb{Q}[X]$.

Indication : on remarquera que si $P = UV$ avec $U, V \in \mathbb{Z}[X]$, U et V gardent un signe constant sur $\mathbb{R}$.

22) Soit $P \in \mathbb{R}[X]$ tel que $P(x) \geq 0$ pour tout $x \in \mathbb{R}$. On pose $Q = \sum_{k\geq 0} P^{(k)}$. Montrer que $\forall x \in \mathbb{R},\ Q(x) \geq 0$.

23) Soient $n \geq 1$ et $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$ avec $a_n a_0 \neq 0$. On pose $M_0 = \max_{0\leq k\leq n-1} |a_k|$ et $M_1 = \max_{1\leq k\leq n} |a_k|$. Montrer que, pour toute racine z de P, on a $\left(1 + \dfrac{M_1}{|a_0|}\right)^{-1} \leq |z| \leq 1 + \dfrac{M_0}{|a_n|}$.

24) Soient $P \in \mathbb{Q}[X]$ non nul et $k \in \mathbb{N}^*$. Montrer que si P est de degré au plus $2k-1$ et si α est une racine de P d'ordre k, alors $\alpha \in \mathbb{Q}$.

25) Soit $P = X^3 - 2X^2 + 7X + k$ un polynôme complexe. Trouver k, sachant que l'une des racines de P a pour carré la somme des carrés des deux autres racines de P.

26) Soient $(a_i)_{1\leq i\leq n}$ et $(b_i)_{1\leq i\leq n}$ deux familles de complexes deux à deux distincts. Démontrer :

$$\left(\exists \lambda \in \mathbb{C},\ \forall i \in [\![1,n]\!], \prod_{j=1}^{n}(a_i + b_j) = \lambda\right) \iff \left(\exists \mu \in \mathbb{C},\ \forall j \in [\![1,n]\!], \prod_{i=1}^{n}(a_i + b_j) = \mu\right).$$

27) (Mines 2017) a) Déterminer les $P \in \mathbb{R}[X]$ tels que $P(\mathbb{Q}) \subset \mathbb{Q}$.

b) Montrer que les polynômes réels tels que $P(\mathbb{Q}) = \mathbb{Q}$ sont les polynôme $P = aX + b$ avec $a \in \mathbb{Q}^*$ et $b \in \mathbb{Q}$. On pourra considérer un polynôme solution et utiliser que $1/p$ est l'image par P d'un rationnel, avec p nombre premier quelconque.

28) (Mines 2017) Soit $P \in \mathbb{C}[X]$ de degré $d \geq 1$. Pour $a \in \mathbb{C}$, on note $n(a)$ le nombre de racines de l'équation $P(z) = a$, sans tenir compte des multiplicités. Ainsi, si $P = (X-2)^2$, $n(0) = 1$ car 2 est l'unique solution de l'équation. Calculer $\sum_{a\in\mathbb{C}}(d - n(a))$.

29) (Centrale 2019) Soit $P \in \mathbb{R}[X]$ de degré $n \geq 2$.

a) On suppose P scindé sur $\mathbb{R}$ et on considère x tel que $P'(x) = 0$ et $P(x) \neq 0$. En utilisant $\dfrac{P'}{P}$, montrer que $P''(x)P(x) < 0$.

b) Soient $a < b$ tels que $P - a$ et $P - b$ sont scindés. Montrer que P' est scindé à racines simples.

30) (Centrale 2019) Pour $P \in \mathbb{C}[X]$ non constant, on note $Z(P)$ l'ensemble des racines de P dans $\mathbb{C}$.

a) Exprimer le cardinal de $Z(P)$ en fonction de P et $P \wedge P'$.

b) Soient P et Q dans $\mathbb{C}[X]$ non constants tels que $Z(P) = Z(Q)$ et $Z(P-1) = Z(Q-1)$. Montrer que $P = Q$. En supposant que $n = \deg(P) \geq \deg(Q)$, on montrera que le polynôme $P - Q$ possède au moins $n+1$ racines.

31) Si P est un polynôme complexe normalisé de degré $n \geq 1$, de racines (non nécessairement distinctes) $\lambda_1, \ldots, \lambda_n$, on définit les *sommes de Newton* de P :

$$\forall k \in \mathbb{N},\ S_k(P) = \sum_{i=1}^{n} \lambda_i^k.$$

Montrer que pour P, Q normalisés de degré $n \geq 1$, on a :

$$\Big(\forall k \geq 1, S_k(P) = S_k(Q)\Big) \Longrightarrow P = Q.$$

32) On se donne P et Q dans $\mathbb{Z}[X]$ premiers entre eux dans $\mathbb{Q}[X]$ et on pose, pour tout $n \in \mathbb{N}$, $u_n = P(n) \wedge Q(n)$. Le but de l'exercice est de montrer que $(u_n)_{n\in\mathbb{N}}$ est périodique.

a) En utilisant le théorème de Bézout, montrer qu'il existe $d \in \mathbb{N}^*$ tel que pour tout $n \in \mathbb{N}$, u_n divise d.

b) Montrer, pour tous $R \in \mathbb{Z}[X]$ et $n \in \mathbb{N}$, que $R(n+d) - R(n)$ est divisible par d.

c) Conclure.

33) Soit $P = \displaystyle\sum_{k=1}^{n}(X - a_i)$ un polynôme normalisé scindé simple. Décomposer $\dfrac{P''}{P}$ en éléments simples. En déduire la valeur de $S = \displaystyle\sum_{k=1}^{n} \frac{P''(a_k)}{P'(a_k)}$.

34) Soit P une polynôme complexe de degré n possédant n racines distinctes non nulles $a_1, \ldots, a_n$. Calculer $\displaystyle\sum_{k=1}^{n} \frac{1}{P'(a_k)}$ et $\displaystyle\sum_{k=1}^{n} \frac{1}{a_k P'(a_k)}$.

Exercices X-ENS

35) Formules de Newton.

Soit $P = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_n = \displaystyle\prod_{k=1}^{n}(X - \lambda_k) \in \mathbb{K}[X]$, où K est un corps commutatif Pour tout entier naturel k, la k-ème somme de Newton de P est :

$$S_k = \sum_{i=1}^{n} \lambda_i^k$$

Pour tout $i \in [\![1, n]\!]$, nous noterons $\sigma_1^{(i)}, \ldots, \sigma_{n-1}^{(i)}$ les fonctions symétriques élémentaires du polynôme $P_i = \dfrac{P}{X - \lambda_i}$:

$$\frac{P}{X - \lambda_i} = X^{n-1} - \sigma_1^{(i)} X^{n-2} + \cdots + (-1)^k \sigma_k^{(i)} X^{n-1-k} + \cdots + (-1)^{n-1} \sigma_{n-1}^{(i)}.$$

a) Montrez que pour $m \geq n$, $S_m - \sigma_1 S_{m-1} + \cdots + (-1)^n \sigma_n S_{m-n} = 0$.

b) En utilisant un développement asymptotique au voisinage de $+\infty$, montrer que pour $i \in [\![1, n]\!]$:

$$P_i = X^{n-1} + (\lambda_i - \sigma_1)X^{n-2} + (\lambda_i^2 - \lambda_i\sigma_1 + \sigma_2)X^{n-3} + \cdots + (\lambda_i^{n-1} - \lambda_i^{n-2}\sigma_1 + \cdots + (-1)^{n-1}\sigma_{n-1})$$

c) Que vaut $\displaystyle\sum_{i=1}^{n} P_i$? En déduire :

$$\forall\, k \in [\![1, n]\!], \qquad S_k - \sigma_1 S_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1} S_1 + (-1)^k k\, \sigma_k = 0.$$

Nous avons ainsi mis en évidence que l'application $(\sigma_1, \dots, \sigma_n) \longmapsto (S_1, \dots, S_n)$ était bijective. En particulier, une famille $(\lambda_1, \dots, \lambda_n)$ est entièrement déterminée, à l'ordre près, par ses sommes de Newton $(S_1, \dots, S_n)$.

d) Autre méthode pour le b) et c) quand $K = \mathbb{C}$: montrer que la série $f(z) = \sum_{p \geq 0} S_p \, z^p$ converge pour z de module assez petit, puis que, pour z non nul de module assez petit :

$$f(z) \left(z^n P\left(\frac{1}{z}\right)\right) = z^{n-1} P'\left(\frac{1}{z}\right).$$

Conclure en utilisant un produit de Cauchy. On montrera que si $g(z) = \sum_{n=0}^{+\infty} a_n z^n$ est définie au voisinage de 0, alors g admet le DL $g(z) = \sum_{i=0}^{n} a_k z^k + O(z^{n+1})$ au voisinage de 0.

36) Polynômes irréductibles dans $\mathbb{Q}[X]$.

a) Soit p un nombre premier. Montrez que p est irréductible dans $\mathbb{Z}[X]$ mais pas dans $\mathbb{Q}[X]$. Montrez que pX est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

b) Pour tout polynôme non nul F à coefficients entiers, on note $c(F)$ le p.g.c.d. des coefficients de F. C'est le *contenu de* F. Montrez que pour $P, Q \in \mathbb{Z}[X] \setminus \{0\}$, $c(PQ) = c(P)c(Q)$. On montrera d'abord le résultat pour deux polynômes de contenus égaux à 1.

c) Soit $F \in \mathbb{Z}[X]$ non constant. Montrez que F est irréductible dans $\mathbb{Z}[X]$ si et seulement si $c(F) = 1$ et si F est irréductible dans $\mathbb{Q}[X]$.

d) Soient $a_1, \dots, a_n$ des entiers distincts. Montrer que $P = (X - a_1) \dots (X - a_n) - 1$ est irréductible sur $\mathbb{Q}$.

e) **Critère d'Eisenstein.**

Soit p un nombre premier et soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. On suppose que p divise $a_0, a_1, \dots, a_{n-1}$, que p ne divise pas a_n et que p^2 ne divise pas a_0. Montrez que P est irréductible dans $\mathbb{Q}[X]$.

37) (P) Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{R}[X]$. On suppose qu'il existe $k \in \{1, \dots, n-1\}$ tel que : $a_{k-1} a_{k+1} > 0$ et $a_k = 0$. Montrer que P n'est pas scindé sur $\mathbb{R}$.

38) (X) Soit p un nombre premier ≥ 5. On écrit $1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{a}{(p-1)!}$. Montrer que p^2 divise a.

39) (X) Pour $n \in \mathbb{N}$, on note $\mathcal{P}_n$ l'ensemble des nombres premiers inférieurs ou égaux à n et a_n son cardinal.

a) Soit $p \in \mathcal{P}_{2n} \setminus \mathcal{P}_n$. Montrer que p divise $\binom{2n}{n}$.

b) Montrer que $n^{a_{2n} - a_n} \leq 2^{2n}$.

c) Montrer qu'il existe $C > 0$ tel que $a_n \leq C \, \frac{n}{\ln n}$ pour tout $n \geq 2$.

40) (X) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, avec $a_n \geq 1$, $a_{n-1} \geq 0$. On pose $h = \max(|a_0|, \dots, |a_{n-2}|)$.

a) Soit z une racine de P. Montrer que $\mathrm{Re}(z) \leq 0$ ou $|z| < \frac{1 + \sqrt{1 + 4h}}{2}$. b) Soit p un premier s'écrivant $p = a_n \dots a_0$ en base 10. Montrer que $P = \sum_{k=0}^{n} a_k X^k$ est irréductible dans $\mathbb{Z}[X]$.

41) (X 2019) On fixe un nombre premier p et on note F_p le corps $\mathbb{Z}/p\mathbb{Z}$, $\mathcal{P}$ l'ensemble des polynômes unitaires de $F_p[X]$, $\mathcal{D}$ l'ensemble des éléments de $\mathcal{P}$ qui sont sans facteurs carrés (c'est-à-dire sans facteurs multiples dans leur décomposition en produit de facteurs irréductibles) et $H = \{z \in \mathbb{C},\ \Re(z) > 1\}$. On note $d(P)$ le degré d'un polynôme P.

a) Soit $s \in H$. Montrer que la famille $\left(p^{-s\,d(P)}\right)_{P\in\mathcal{P}}$ est sommable. On note :

$$\xi(s) = \sum_{P\in\mathcal{P}} p^{-s\,d(P)} \text{ et } \chi(s) = \sum_{P\in\mathcal{D}} p^{-s\,d(P)}.$$

b) Montrer que $\xi(2s)\chi(s) = \xi(s)$ pour tout $s \in H$.

c) Soit un entier $n \geq 2$. Montrer qu'il y a exactement $p^n - p^{n-1}$ polynômes unitaires de $F_p[X]$ de degré n et sans facteur carré.

42) (X 2020) Soit n un entier naturel non nul et k le nombre de 1 dans son écriture en base 2. Montrer que le polynôme $P(X) = (X-1)^n \in \mathbb{Z}[X]$ a exactement 2^k coefficients impairs.

43) Pour $n \in \mathbb{N}^*$, on note δ_n le nombre de diviseurs de n et on définit, pour $x \geq 1$, $F(x) = \sum_{\substack{n\in N^* \\ n\leq x}} \delta_n$.

a) Trouver un équivalent simple de $F(x)$ au voisinage de $+\infty$.

b) Démontrer que $F(x) = x\ln x + (2\gamma - 1)x + O(\sqrt{x})$ au voisinage de $+\infty$.

Anneaux : corrigés

Exercices CCP

1) Pour $i \in \{0,1,2\}$, notons $S_i = \sum_{\substack{0\leq k\leq n\\ k\equiv i \bmod n}} \binom{n}{k}$. Nous avons alors :

$$\begin{aligned}(1+1)^n &= \sum_{k=0}^{n}\binom{n}{k} = S_0+S_1+S_2\\ (1+j)^n &= \sum_{k=0}^{n}\binom{n}{k}j^k = S_0+jS_1+j^2S_2\\ (1+j^2)^n &= \sum_{k=0}^{n}\binom{n}{k}j^{2k} = S_0+j^2S_1+jS_2\end{aligned}$$

et on obtient S_0 en sommant ces trois égalités :

$$S_0 = \frac{1}{3}\left(2^n+(1+j)^n+(1+j^2)^n\right) = \frac{1}{3}\left(2^n+(-j^2)^n+(-j)^n\right)$$

Comme $(-j^2)^n+(-j)^n = (-1)^n\left(j^{2n}+j^n\right) = \begin{cases}(-1)^n\times 2 & \text{si } n\equiv 0 \bmod 3\\ (-1)^{n+1} & \text{sinon}\end{cases}$, on obtient :

$$S_0 = \begin{cases}\dfrac{2^n+2\times(-1)^n}{3} & \text{si } n\equiv 0 \bmod 3\\ \dfrac{2^n+(-1)^{n+1}}{3} & \text{sinon}\end{cases}$$

2) Si x, y sont deux éléments de $\mathbb{Z}_p$, avec $x=\dfrac{a}{b}$, $y=\dfrac{c}{d}$ où a,b,c,d sont des entiers tels que $b\wedge p = d\wedge p = 1$, on a :

$$x-y = \frac{ad-bc}{bd} \text{ et } xy = \frac{ac}{bd}$$

avec $ad-bc\in\mathbb{Z}$, $ac\in\mathbb{Z}$, $bd\in\mathbb{Z}^*$ et $bd\wedge p = 1$ (car p est premier). On en déduit que $\mathbb{Z}_p$ est stable par différence et par produit. Comme il contient l'élément unité ($1=\frac{1}{1}$ avec $1\wedge p = 1$), $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$.

Supposons que A soit un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}_p$. Si A est différent de $\mathbb{Z}_p$, il existe $x\in\mathbb{A}\setminus\mathbb{Z}_p$. On peut écrire $x=\dfrac{a}{b}$ avec $a\in\mathbb{Z}$, $b\in\mathbb{Z}^*$ et $a\wedge b = 1$. Comme x n'est pas élément de $\mathbb{Z}_p$, b n'est pas premier avec p, p divise b : il existe c tel que $b=pc$. Ainsi, p ne divise pas a (car 1 est le seul diviseur commun à a et b), donc $a\wedge p = 1$. On en déduit que $\dfrac{c}{a}$ est élément de $\mathbb{Z}_p$, donc de A. Comme A est un anneau, $\dfrac{c}{a}\,x = \dfrac{1}{p}$ est élément de a.

Tout rationnel q s'écrit alors sous la forme $\dfrac{\alpha}{p^i\beta}$ avec $\alpha\in\mathbb{Z}$, $i\in\mathbb{N}$, $\beta\in\mathbb{Z}^*$ et $\beta\wedge p = 1$. Comme $\dfrac{1}{p}$ et $\dfrac{\alpha}{\beta}$ sont éléments de A, q est le produit d'éléments de A : c'est un élément de A, qui est donc égal à $\mathbb{Q}$. Ainsi, un sous-anneau contenant $\mathbb{Z}_p$ est soit égal à $\mathbb{Z}_p$, soit égal à $\mathbb{Q}$. On dit que $\mathbb{Z}_p$ est un sous-anneau maximal de $\mathbb{Q}$.s

3) Dans $\mathbb{Z}/9\mathbb{Z}$, les éléments inversibles sont $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$ et $\overline{8}$. Le groupe des inversibles de $\mathbb{Z}/9\mathbb{Z}$ est donc de cardinal 6. Comme il est commutatif, il est isomorphe à $(\mathbb{Z}/6\mathbb{Z},+)$ (on sait qu'il n'existe que deux groupes de cardinal 6 : $(\mathbb{Z}/,\mathbb{Z}+)$ qui est commutatif et $(\mathfrak{S}_3,\circ)$ qui ne l'est pas.

On peut aussi montrer que $(\mathbb{Z}/9\mathbb{Z})^*$ est cyclique en exhibant un élément d'ordre 6 : en posant $x=\overline{2}$, on a

$$x^0=\overline{1},\ x^1=\overline{2},\ x^2=\overline{4},\ x^3=\overline{8},\ x^4=\overline{7},\ x^5=\overline{5} \text{ et } x^6=\overline{1}$$

donc x engendre le groupe multiplicatif $(\mathbb{Z}/9\mathbb{Z})^*$, qui est ainsi isomorphe à $(\mathbb{Z}/6\mathbb{Z},+)$.

4) 55 et 16 sont premiers entre eux, et on obtient facilement la relation de Bézout :

$$7\times 55 - 24\times 16 = 1.$$

On cherche x tel que $x = 7+16a = 21+55b$, avec $a,b\in\mathbb{Z}$. Cela donne $55b-16a=-14$. En multipliant la relation de Bézout par -14, on obtient :

$$-98\times 55 + 336\times 24 = -14$$

On choisit donc $b_0=-98$ et $x_0 = 21+55b = -5369$. Cette valeur x_0 est solution particulière et la solution générale du premier système est :

$$x \equiv x_0 \pmod{55\times 16},$$

soit encore :

$$x \equiv 791 \pmod{880}.$$

On a par contre $16\wedge 68 = 4$. On cherche x tel que $x = 7+16a = 21+68b$, avec $a,b\in\mathbb{Z}$. Cela donne $68a-16a=-14$ et il n'y a pas de solution, car $-14\notin 4\mathbb{Z} = 16\mathbb{Z}+68\mathbb{Z}$).

5) On peut écrire $P = Q(X-2)^2 + aX + b$ avec $a,b\in\mathbb{R}$. On utilise que 2 est une racine d'ordre 2 de $(X-2)^2$, donc $P(2) = 2a+b$ et $P'(2) = a$. On obtient ainsi $a = 298580$ et $b = -555810$.

6) On a $(1+\sqrt{2})^n = \sum k=0^n \binom{n}{k}\sqrt{2}^k = \sum_{0\le 2p\le n}\binom{n}{2p}2^p + \sqrt{2}\sum_{0\le 2p+1\le n}\binom{n}{2p+1}2^p$ donc les entiers :

$$a_n = \sum_{0\le 2p\le n}\binom{n}{2p}2^p \text{ et } b_n = \sum_{0\le 2p+1\le n}\binom{n}{2p+1}2^p$$

sont solutions du problème.

Si (a'_n,b'_n) est une autre solution, on a $a_n - a'_n + \sqrt{2}\,(b_n-b'_n) = 0$, ce qui impose $a_n = a'_n$ et $b_n = b'_n$ car $\sqrt{2}\notin\mathbb{Q}$.

On a d'autre part $(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$, puis :

$$(-1)^n = (1+\sqrt{2})^n(1-\sqrt{2})^n = (a_n+b_n\sqrt{2})(a_n-b_n\sqrt{2}) = a_n^2 - 2b_n^2$$

ce qui est une relation de Bézout entre a_n et b_n, qui sont donc premiers entre eux.

Exercices Mines-Centrale : anneaux

7) a) $0\in\sqrt{I}$ car $0^1 = 0\in I$: I est donc non vide.

Soient $x,y\in\sqrt{I}$. Il existe $n,m\in\mathbb{N}$ tels que $x^n, y^m\in I$. On en déduit :

$$\begin{aligned}(x-y)^{n+m} &= \sum_{k=0} x^{n+m}\binom{k}{n+m}x^k(-1)^{n+m-k}y^{n+m-k}\\ &= \underbrace{y^m}_{\in I}\underbrace{\left(\sum_{k=0}^{n}\binom{k}{n+m}x^k(-1)^{n+m-k}y^{n-k}\right)}_{\in A} + \underbrace{x^n}_{\in I}\underbrace{\left(\sum_{k=n+1}^{n+m}\binom{k}{n+m}x^{k-n}(-1)^{n+m-k}y^{n+m-k}\right)}_{\in A}\in I\end{aligned}$$

donc $x+y\in\sqrt{I}$, qui est ainsi stable par différence.

Si $x\in\sqrt{I}$ et $y\in A$, on choisit $n\in\mathbb{N}$ tel que $x^n\in I$ et $(xy)^n = x^ny^n\in I$, donc $xy\in\sqrt{I}$, qui est un idéal de A.

On a $I \subset \sqrt{I}$ (car $six \in I$, $x^1 \in I$ et $x \in \sqrt{I}$. On a en particulier $\sqrt{I} \subset \sqrt{\sqrt{I}}$. L'inclusion réciproque est évidente : si $x \in \sqrt{\sqrt{I}}$, il existe $n \in \mathbb{N}$ tel que $x^n \in \sqrt{I}$, puis il existe $m \in \mathbb{N}$ tel que $(x^n)^m \in I$, d'où $x^{nm} \in I$ et $x \in \sqrt{I}$.

b) Remarque : la somme de deux idéaux est un idéal, donc les ensembles manipulés sont bien définis.

Si I_1 et I_2 sont deux idéaux, on a facilement $I_1 \subset I_2 \Longrightarrow \sqrt{I_1} \subset \sqrt{I_2}$. Ainsi, comme $I + J \subset \sqrt{I} + \sqrt{J}$, on a $\sqrt{I+J} \subset \sqrt{\sqrt{I} + \sqrt{J}}$. L'inclusion réciproque se montre avec la même idée que pour le a) : si $x \in \sqrt{\sqrt{I} + \sqrt{J}}$, il existe $n \in \mathbb{N}$ tel que $x^n \in \sqrt{I} + \sqrt{J}$. On peut alors écrire $x^n = y + z$ avec $y \in \sqrt{I}$ et $z \in \sqrt{J}$. Il existe ensuite $p, q \in \mathbb{N}$ tels que $y^p \in I$ et $z^q \in J$. On en déduit :

$$x^{n(p+q)} = (y+z)^{p+q} = \underbrace{y^p}_{\in I} \underbrace{\sum_{k=p}^{p+q} \binom{k}{p+q} y^{k-p} z^{p+q-k}}_{\in A} + \underbrace{z^q}_{\in J} \underbrace{\sum_{k=0}^{p-1} \binom{k}{p+q} y^k z^{p-k}}_{\in A} \in I + J$$

et $x \in \sqrt{I+J}$.

Nous avons également $I \cap J \subset \sqrt{I} \cap \sqrt{J}$, donc $\sqrt{I \cap J} \subset \sqrt{\sqrt{I} \cap \sqrt{J}}$. Inversement, si $x \in \sqrt{\sqrt{I} \cap \sqrt{J}}$, il existe $n \in \mathbb{N}$ tel que $x^n \in \sqrt{I} \cap \sqrt{J}$. Il existe alors p et q tels que $x^{np} \in I$ et $x^{nq} \in J$. On en déduit que $x^{nk} \in I \cap J$, avec $k = \max(p, q)$ ($x^{nk} = x^{np} x^{n(k-p)} \in I$ et $x^{nk} = x^{nq} x^{n(k-q)} \in J$ car I et J sont des idéaux), soit que $x \in \sqrt{I \cap J}$.

c) Les idéaux de $\mathbb{Z}$ sont les parties $m\mathbb{Z}$ pour $m \in \mathbb{N}$. On a $\sqrt{0\mathbb{Z}} = \sqrt{\{0\}} = \{0\} = 0\mathbb{Z}$ et $\sqrt{\mathbb{Z}} = \mathbb{Z}$. Pour $m \geq 2$, on peut décomposer m en produit facteur irréductibles : $m = \prod_{i=1}^{k} p_i^{n_i}$ avec $k \geq 1$, $p_1, \ldots, p_k$ nombres premiers et $n_1, \ldots, n_k \geq 1$. On a alors :

$$\forall x \in \mathbb{Z},\ x \in \sqrt{m\mathbb{Z}} \Longleftrightarrow \exists n \geq 1,\ \prod_{i=1}^{k} p_i^{n_i} \text{ divise } x^n \Longleftrightarrow \forall i,\ p_i \text{ divise } x$$

donc $\sqrt{m\mathbb{Z}} = p_1 \ldots p_k \mathbb{Z}$.

On peut chercher à retrouver ce résultat en appliquant les formules précédentes :

$$\sqrt{m\mathbb{Z}} = \sqrt{p_1^{n_1}\mathbb{Z} \cap \cdots \cap p_k^{n_k}\mathbb{Z}} = \sqrt{\sqrt{p_1^{n_1}\mathbb{Z}} \cap \cdots \cap \sqrt{p_k^{n_k}\mathbb{Z}}} = \sqrt{p_1\mathbb{Z} \cap \cdots \cap p_k\mathbb{Z}} = \sqrt{p_1 \ldots p_k \mathbb{Z}} = p_1 \ldots p_k \mathbb{Z}$$

8) Pour trouver l'inverse de $1 - ba$, on peut penser à ce développement formel :

$$(1-ba)^{-1} = \sum_{n \geq 0} (ba)^n = 1 + b \left(\sum_{n \geq 0} (ab)^n \right) a = 1 + b(1-ab)^{-1} a.$$

Ce calcul, qui n'a aucun sens dans un anneau A quelconque, donne pourtant la bonne expression de l'inverse ; on pose $c = 1 + b(1-ab)^{-1}a$ et on n'a plus qu'à vérifier :

$$\begin{cases} (1-ba)c = (1-ba)(1+b(1-ab)^{-1}a) = 1 - ba + \underbrace{(b - bab)}_{=b(1-ab)}(1-ab)^{-1}a = 1 \\ c(1-ba) = (1+b(1-ab)^{-1}a)(1-ba) = 1 - ba + b(1-ab)^{-1} \underbrace{(a - aba)}_{=(1-ab)a} = 1 \end{cases}$$

donc $1 - ba$ est inversible., d'inverse $1 + b(1-ab)^{-1}a$.

Exercices Mines-Centrale : l'anneau $\mathbb{Z}$

9) Soit d un diviseur premier de q : d est donc un diviseur premier de $2^p - 1$ et 2^p est congru à 1 modulo d. Dans le groupe multiplicatif $G = (\mathbb{Z}/d\mathbb{Z})^*$, l'élément $x = \overline{2}$ vérifie $x^p = \overline{1}$: son ordre divise donc p ; comme $x \neq \overline{1}$ et que p est premier, x

est d'ordre p, ce qui impose que p divise $\mathrm{Card}(G) = d-1$: d est donc congru à 1 modulo p. Comme d est impair (il divise $2^p - 1$ qui est impair), on a $d \equiv 1\ [p]$ et $d \equiv 1\ [2]$: 2 et p étant premier entre eux, $d \equiv 1\ [2p]$ (lemme chinois).

En écrivant $q = d_1 \dots d_k$ où les d_i sont premiers (avec $k \geq 0$, la cas $k = 0$ correspondant au cas trivial $q = 1$), on a $d_i \equiv 1\ [2p]$ pour tout i, puis $q \equiv 1\ [2p]$.

10) a) Travaillons dans le corps $\mathbb{Z}/p\mathbb{Z}$, en notant $\bar{n}$ la classe modulo p d'un entier n. Comme $(\mathbb{Z}/p\mathbb{Z})^*$ est de cardinal $p-1$, on a $x^{p-1} = \bar{1}$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$. On en déduit que le polynôme $X^{p-1} - 1$ a pour racines les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, ce qui s'écrit :

$$X^{p-1} - \bar{1} = \prod_{k=1}^{p-1} (X - \bar{k}).$$

On obtient en évaluant en $\bar{0}$ (car pour $p = 2$, $(-\bar{1})^{p-1} = -\bar{1} = \bar{1}$ et sinon, $p-1$ est pair et $(-\bar{1})^{p-1} = \bar{1}$) :

$$-\bar{1} = (-\bar{1})^{p-1} \prod_{k=1}^{p-1} \bar{k} = (-\bar{1})^{p-1} \overline{(p-1)!} = \overline{(p-1)!}$$

ce qui donne le résultat demandé.

b) Si n est premier, on a donc $(n-1)! \equiv n-1 \bmod n$. On peut ensuite deviner le résultat en regardant les premières valeurs de n :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$(n-1)! \bmod n$	0	1	2	2	4	0	6	0	0	0	10	0	12	0	0	0	16	0	18	0

On a donc $(n-1)! \equiv 2 \bmod n$ quand $n = 4$ et on peut conjecturer que $(n-1)! \equiv 0 \bmod n$ pour tout entier n non premier différent de 4.

Soit donc $n > 4$ non premier. Il existe une factorisation non triviale de la forme $n = ab$ avec $2 \leq a \leq b \leq n-1$. Si $a < b$, on a $n = ab \,|\, (n-1)!$ car a et b sont deux des $n-1$ facteurs de $(n-1)!$; si $a = b$, on a $a \geq 3$ donc $1 \leq a < 2a < a^2 = n$ donc $2n$ divise $(n-1)!$ puisque que a et $2a$ sont deux des $n-1$ facteurs de $(n-1)!$; dans les deux cas, n divise $(n-1)!$.

11) a) Nous noterons $\overline{a}$, $\dot{a}$ et $\hat{a}$ les classes d'un entier relatif a respectivement modulo nm, n et m.

Remarquons pour commencer que si f est un morphisme d'anneau de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, on a $f(\overline{1}) = (\dot{1}, \hat{1})$ (l'image de l'unité est l'unité), puis l'additivité de f donne par récurrence immédiate $f(\overline{k}) = (\dot{k}, \hat{k})$ pour tout $k \in \mathbb{N}$ et cette propriété se prolonge à $k \in \mathbb{Z}$ car $f(-x) = -f(x)$ pour tout x.

Réciproquement, l'application $f : \overline{k} \longmapsto (\dot{k}, \hat{k})$ est bien définie (car si deux entiers sont égaux modulo nm, ils le sont modulo n et modulo m) et est un morphisme d'anneau.

On calcule facilement le noyau de f :

$$\hat{k} \in \mathrm{Ker}(f) \iff \dot{k} = \dot{0} \text{ et } \hat{k} = \hat{0} \iff n \,|\, k \text{ et } m \,|\, k \iff n \vee m \,|\, k.$$

f est donc injective si et seulement si $n \vee m = nm$, soit si et seulement n et m sont premiers entre eux. Comme $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont finis de même cardinal, f est un isomorphisme si et seulement si $n \wedge m = 1$.

b) Soit $x = \overline{k}$. Notons q l'entier tel que $k \vee n = kq$. Les éléments x, $2x$, …, $(q-1)x$ sont non nuls et $qx = \overline{0}$: x est donc d'ordre q et le groupe engendré par x est de cardinal q. On en déduit :

$$x \in A_n \iff q = n \iff k \vee n = kn \iff k \wedge n = 1.$$

On retrouve la caractérisation des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$: on a donc $A_n = (\mathbb{Z}/n\mathbb{Z})^*$.

c) On trouve facilement $A_2 = \{\overline{1}\}$, $A_3 = \{\overline{1}, \overline{2}\}$, $A_4 = \{\overline{1}, \overline{3}\}$, $A_5 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, … et on obtient :

$$\varphi(2) = 1,\ \varphi(3) = \varphi(4) = 2,\ \varphi(5) = 4,\ \varphi(6) = 2,\ \varphi(7) = 6,\ \varphi(8) = 4,\ \varphi(9) = 6,\ \varphi(10) = 4.$$

d) Les entiers non premiers avec p^v sont les multiples de p. Dans $[\![1, p^d]\!]$, ce sont donc les p^{v-1} entiers $p, 2p, 3p, \ldots, p^{v-1}p$. On en déduit que $(\mathbb{Z}/p^v\mathbb{Z}) \setminus A_{p^v}$ est de cardinal p^{v-1}, d'où $\varphi(p^v) = p^v - p^{v-1} = p^v\left(1 - \dfrac{1}{p}\right)$.

e) Si n et m sont premiers entre eux, l'anneau $\mathbb{Z}/nm\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Nous avons donc un isomorphisme (de groupe) entre leurs groupes multiplicatifs :

$$\varphi(nm) = \mathrm{Card}\,(\mathbb{Z}/nm\mathbb{Z})^* = \mathrm{Card}\,(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* = \mathrm{Card}\,(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* = \varphi(n)\varphi(m)$$

en remarquant que dans un anneau produit $A \times B$, un couple (a, b) est inversible si et seulement a et b le sont.

f) En écrivant $n = \prod_{i=1}^{k} p_i^{v_i}$ la décomposition de n en produit de facteurs premiers, nous avons en utilisant e) (et par récurrence) :

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{v_i}) = \prod_{i=1}^{k} \left[p_i^{v_i}\left(1 - \frac{1}{p_i}\right)\right] = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

g) Pour $n \geq 1$, notons D_n l'ensemble des diviseurs positifs de n. Le résultat se prouve par récurrence sur le nombre de facteur premiers dans la décomposition de n.

- Si $n = p^v$ avec p premier et $v \geq 1$, on a :

  $$\sum_{d \in D_n} \varphi(d) = \sum_{k=0}^{v} \varphi(p^k) = \varphi(1) + \sum_{k=1}^{v}\left(p^k - p^{k-1}\right) = p^v = n$$

  donc la récurrence est initialisée.

- Soit $k \geq 2$ et supposons la propriété vérifiée pour tout tout entier n possédant $k-1$ facteurs premiers distincts. Si $n = \prod_{i=1}^{k} p_i^{v_i}$ où les p_i sont des nombres premiers distincts et les v_i des entiers naturels non nuls, on a alors $n = ab$ avec $a = p_1^{v_1}$ et $b = \prod_{i=2}^{k} p_i^{v_i}$. a et b sont premiers entre eux et l'hypothèse de récurrence au rang $p-1$ et au rang 1 donne :

  $$n = ab = \left(\sum_{d \in D_a} \varphi(d)\right)\left(\sum_{d \in D_b} \varphi(d')\right) = \sum_{(d_1, d_2) \in D_a \times D_b} \varphi(d_1)\varphi(d_2)$$

  Quand $(d_1, d_2) \in D_a \times D_b$, $d_1 \wedge d_2 = 1$ donc $\varphi(d_1)\varphi(d_2) = \varphi(d_1 d_2)$. D'autre part, l'application $(d_1, d_2) \longmapsto d_1 d_2$ est une bijection de $D_a \times D_b$ sur D_{ab}. Nous obtenons donc :

  $$n = \sum_{(d_1, d_2) \in D_a \times D_b} \varphi(d_1 d_2) = \sum_{d \in D_{ab}} \varphi(d)$$

  et la propriété est démontrée au rang k.

12) a) L'application $f :\ x \longmapsto x^2$ est est surjective de $\mathbb{Z}/p\mathbb{Z}$ sur C. Si $y \in C$, avec $y = a^2$, nous avons :

$$\forall x \in \mathbb{Z}/p\mathbb{Z},\ f(x) = a \Longleftrightarrow (x+a)(x-a) = 0 \Longleftrightarrow x = a \text{ ou } x = -a.$$

Si $y = 0$, $a = 0$ est le seul antécédent de y ; sinon, y possède deux antécédents (on a $a \neq -a$ car p est impair). Comme $\mathbb{Z}/p\mathbb{Z}$ est de cardinal p, C est de cardinal $1 + \dfrac{p-1}{p}$.

b) Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est de cardinal $p-1$ donc $a^{p-1} = 1$ pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^*$. On en déduit que le polynôme $X^{p-1} - 1$ est scindé et que ses racines sont les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. En notant $\overline{k}$ la classe modulo p d'un entier k, nous avons donc :

$$X^{p-1} - \overline{1} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^*} (X - a) = \prod_{1 \leq k \leq p-1} (X - \overline{k})$$

Les relations entre racines et coefficients donnent en particulier (produit des racines) :

$$\overline{(p-1)!} = \prod_{1 \leq k \leq p-1} \overline{k} = (-1)^{p-1}(-\overline{1}) = -\overline{1}$$

car $p-1$ est pair.

Supposons que p est congru à 1 modulo 4 ; on peut donc écrire $p = 1 + 4q$ avec $q \in \mathbb{N}^*$, puis :

$$(p-1)! = 1 \times 2 \times \cdots \times (2q-1) \times 2q \times \underbrace{(2q+1)}_{\equiv -2q \ [p]} \times \underbrace{(2q+2)}_{\equiv -(2q-1) \ [p]} \cdots \times \underbrace{(4q-1)}_{\equiv -2 \ [p]} \times \underbrace{(4q)}_{\equiv -1 \ [p]}$$

On en déduit que $-\overline{1} = (-1)^{2q}\,\overline{1}^2\,\overline{2}^2 \ldots \overline{2q}^2 = \overline{(2q)!}^2$: -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

c) Supposons maintenant que p est congru à 3 modulo 4 et montrons que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. Nous avons cette fois $p = 3 + 4q$ avec $q \in \mathbb{N}$. Notons $D = C \setminus \{0\}$, partie de cardinal $1 + 2q$. L'application $g : \ a \longmapsto a^{-1}$ est une bijection involutive de $(\mathbb{Z}/p\mathbb{Z})^*$ sur lui-même et $g(D) \subset D$, donc $g(D) = D$. Comme 1 et -1 sont les seuls points fixes de g, nous pouvons choisir des éléments $a_1, \ldots, a_q$ de $(\mathbb{Z}/p\mathbb{Z})^*$ tels que les parties $\{1\}$, $\{-1\}$, $\{a_1, a_1^{-1}\}$, $\ldots, \{a_q, a_q^{-1}\}$ forment une partition de $(\mathbb{Z}/p\mathbb{Z})^*$. Comme D est stable par g, il est réunion de certaines de ces parties : le cardinal de D étant impair, il contient une seule partie de cardinal 1. Enfin, $1 \in D$, donc $-1 \notin D$ et -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. Ceci prouve par contraposée que si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier impair, alors p est congru à 1 modulo 4 (un entier impair est congru soit à 1, soit à 3 modulo 4).

13) a) On a $q^p - 1 = (q-1)(q^{p-1} + \cdots + q + 1)$, donc $(q-1) = 1$ (car $q^{p-1} + \cdots + q + 1 \geq 2$ et $q^p - 1$ est premier).

Supposons que a est un diviseur de p et posons $p = ab$; on a $2^p - 1 = (2^a)^b - 1 = (2^a - 1)(2^{b-1} + 2^{b-2} + \cdots + 1)$ donc $2^a - 1 = 1$ ou $2^a - 1 = 2^p - 1$, i.e. $a = 1$ ou $a = p$: p est donc premier.

b) Comme k divise $2^p - 1$ qui est impair, k est impair : il est donc congru à 1 modulo 2.

On peut ensuite écrire $k = \prod_{i=1}^{N} q_i$ où $N \in \mathbb{N}$ et où les q_i sont premiers. Pour tout i, q_i divise $2^p - 1$, donc 2^p est congru à 1 modulo q_i. Dans le groupe multiplicatif $(\mathbb{Z}/q_i\mathbb{Z})^*$, l'ordre de $\overline{2}$ est donc un diviseur de p ; comme $\overline{2} \neq \overline{1}$ (car $q_i \neq 2$) et que p est premier, $\overline{2}$ est d'ordre p ; enfin, l'ordre d'un élément d'un groupe fini est un diviseur de l'ordre du groupe, donc p divise $q_i - 1$, ce qui traduit que q_i est congru à 1 modulo p.

Nous avons donc, par produit de congruences, que k est congru à 1 modulo p ; on en déduit que $k - 1$ est divisible par p et par 2, donc par $2p$ (2 et p sont premiers entrée eux) : c'est le résultat souhaité.

14) Pour chaque valeur de n, il existe au plus une valeur de m telle que (n, m) soit solution. Les premières valeurs de n donnent facilement :

- si $n = 0$, aucune valeur de m ne convient ;
- $(1, 0)$ et $(2, 1)$ sont solutions.

Soit $(n, m) \in \mathbb{N}^2$ avec $n \geq 3$. On a $2^n \equiv 0 \bmod 8$ et $1 + 3^m$ est congru à 2 ou à 4 modulo 8 : (n, m) n'est pas solution.

Les seules solutions sont donc $(1, 0)$ et $(2, 1)$.

15) Soit (n, m) une solution. Remarquons tout d'abord que 3^m est impair, donc n l'est également : on peut donc écrire $n = 2a + 1$ avec $a \in \mathbb{N}$. On a ensuite :

$$3^m = 8 + (2a+1)^2 = 8 + 4a^2 + 4a + 1 \equiv 1 \bmod 4.$$

Comme 3 est d'ordre 2 dans le groupe multiplicatif $(\mathbb{Z}/4\mathbb{Z})^*$, ceci impose à m d'être pair : on peut donc écrire $m = 2b$ avec $b \in \mathbb{N}$.

L'égalité s'écrit donc $(3^b - n)(3^b + n) = 3^{2b} - n^2 = 8$. Les entiers $3^b - n$ et $3^b + n$ étant pairs, avec $3^b - n < 3b + n$ et $3b + n > 0$, nous avons nécessairement $3b - n = 2$ et $3b + n = 4$, soit $n = 1$ et $b = 1$.

Réciproquement, $(n, m) = (1, 2)$ est bien solution de l'équation.

16) L'idée est que la croissance très lente de $\ln n$ va nous permettre de définir de longs paliers $[\![a_k, b_k]\!]$ sur lesquels le cosinus sera assez grand (par exemple supérieur à 1/2), ce qui permettra d'écrire :

$$\sum_{n=a_k}^{b_k} \frac{\cos(\ln\, n)}{\ln\, n} \geq \frac{1}{2} \sum_{n=a_k}^{b_k} \frac{1}{\ln\, n}.$$

Pour $k \in \mathbb{N}^*$, nous avons $\cos(\ln\, x) \geq \frac{1}{2}$ pour $x \in \left[e^{-\frac{\pi}{3}+2k\pi}, e^{\frac{\pi}{3}+2k\pi}\right]$.

En posant $a_k = \lceil e^{-\frac{\pi}{3}+2k\pi} \rceil$ et $b_k = \lfloor e^{\frac{\pi}{3}+2k\pi} \rfloor$, une comparaison série-intégrale permet d'écrire :

$$S_k \overset{\text{def}}{=} \sum_{n=a_k}^{b_k} \frac{\cos(\ln\, n)}{\ln\, n} \geq \frac{1}{2} \sum_{n=a_k}^{b_k} \frac{1}{\ln\, n} \geq \int_{a_k}^{b_k+1} \frac{1}{\ln\, x}\, \mathrm{d}x$$

La dernière idée consiste à remplacer $\frac{1}{\ln x}$ par une fonction dont on connaît une primitive, en gardant le même ordre de grandeur au voisinage de $+\infty$. Ici, nous pouvons remarquer que

$$\frac{\mathrm{d}}{\mathrm{d}\, x}\left(\frac{x}{\ln\, x}\right) = \frac{1}{\ln\, x} - \frac{1}{\ln^2 x} \leq \frac{1}{\ln\, x}$$

ce qui donne :

$$S_k \geq \int_{a_k}^{b_k+1} \left(\frac{1}{\ln\, x} - \frac{1}{\ln^2 x}\right) \mathrm{d}x = \left[\frac{x}{\ln\, x}\right]_{a_k}^{b_k+1} \geq \frac{e^{\frac{\pi}{3}+2k\pi}}{\ln\left(e^{\frac{\pi}{3}+2k\pi}+1\right)} - \frac{e^{-\frac{\pi}{3}+2k\pi}+1}{\ln\left(e^{-\frac{\pi}{3}+2k\pi}\right)}$$

en utilisant les inégalités :

$$e^{-\frac{\pi}{3}+2k\pi} \leq a_k \leq e^{-\frac{\pi}{3}+2k\pi}+1 \text{ et } e^{\frac{\pi}{3}+2k\pi} \leq b_k+1 \leq e^{\frac{\pi}{3}+2k\pi}+1.$$

Nous avons, pour terminer :

$$\frac{e^{\frac{\pi}{3}+2k\pi}}{\ln\left(e^{\frac{\pi}{3}+2k\pi}+1\right)} \sim_{+\infty} \frac{e^{\frac{\pi}{3}}}{2\pi}\,\frac{e^{2k\pi}}{k} \text{ et } \frac{e^{-\frac{\pi}{3}+2k\pi}+1}{\ln\left(e^{-\frac{\pi}{3}+2k\pi}\right)} \sim_{+\infty} \frac{e^{-\frac{\pi}{3}}}{2\pi}\,\frac{e^{2k\pi}}{k}$$

d'où

$$S_k \sim_{+\infty} \frac{\mathrm{sh}\left(\frac{\pi}{3}\right)}{\pi}\,\frac{e^{2k\pi}}{k} \xrightarrow[k\to+\infty]{} +\infty.$$

Ceci prouve que la série est divergente (comme a_k et b_k tendent vers l'infini, S_k tendrait vers 0 en cas de convergence de la série).

Exercices Mines-Centrale : l'anneau des polynômes

17) x, y, z seront, s'ils existent, les racines du polynôme $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ avec :

$$\sigma_1 = x+y+z = 1,\ \sigma_2 = xy+yz+zx = -5 \text{ et } \sigma_3 = xyz.$$

Il suffit donc de retrouver la valeur de σ_3 qui est imposée par la condition $x^3+y^3+z^3 = -2$. Nous avons :

$$x^2+y^2+z^2 = (x+y+z)^2 - 2(xy+yz+zx) = \sigma_1^2 - 2\sigma_2 = 11$$

puis

$$11 = (x+y+z)(x^2+y^2+z^2) = x^3+y^3+z^3+xy^2+xz^2+yz^2+yx^2+zx^2+zy^2$$

donc

$$xy^2+xz^2+yz^2+yx^2+zx^2+zy^2 = 13.$$

On a enfin :

$$-5 = (x+y+z)(xy+yz+zx) = xy^2+xz^2+yz^2+yx^2+zx^2+zy^2+3xyz$$

d'où $\sigma_3 = -6$. On en déduit que x, y, z sont les racines du polynômes $X^3 - X^2 - 5X^2 + 6 = (X-2)(X^2+X-3)$; on obtient donc :

$$\{x, y, z\} = \left\{2, \frac{-1+\sqrt{13}}{2}, \frac{-1-\sqrt{13}}{2}\right\}.$$

18) On commence par calculer une relation de Bézout entre P et Q :

$$\begin{cases} P = Q + R_1 & \text{avec } R_1 = X^2 - 3X + 3 \\ Q = (X^2+X-3)R_1 + R_2 & \text{avec } R_2 = X - 1 \\ R_1 = (X-2)R_2 + 1 \end{cases}$$

donc P et Q sont premier entre eux et on a :

$$\begin{aligned} 1 &= R_1 - (X-2)R_2 \\ &= R_1 - (X-2)(Q - (X^2+X-3)R_1) \\ &= (X^3 - X^2 - 5X + 7)R_1 - (X-2)Q \\ &= (X^3 - X^2 - 5X + 7)(P-Q) - (X-2)Q \\ &= (X^3 - X^2 - 5X + 7)P - (X^3 - X^2 - 4X + 5)Q \end{aligned}$$

On cherche $A, B \in \mathbb{R}[X]$ tels que $X^2 + X + 1 + AP = 2X^2 - 3 + BQ$, i.e.

$$AP - BQ = X^2 - X - 4.$$

On peut choisir comme solution particulière $\begin{cases} A_0 = (X^2 - X - 4)(X^3 - X^2 - 5X + 7) \\ B_0 = (X^2 - X - 4)(X^3 - X^2 - 4X + 5) \end{cases}$, ce qui donne la solution particulière :

$$S_0 = X^2 + X + 1 + A_0 P = X^9 - 4X^8 - 6X^7 + 46X^6 - 30X^5 - 152X^4 + 246X^3 + 75X^2 - 370X + 197$$

La solution générale est $S = S_0 + C(P \vee Q) = S_0 + CPQ$ avec $C \in \mathbb{R}[X]$: la solution de degré minimal est donc le reste de S_0 dans la division euclidienne par PQ, soit $S_0 - XPQ$. La solution de degré minimal est donc :

$$S = -5X^7 + 13X^6 + 27X^5 - 130X^4 + 75X^3 + 266X^2 - 440X + 197$$

19) On peut déjà remarquer que les polynômes $(1-X)^n$ et X^n étant premiers entre eux et de degrés n, le problème possède une unique solution (l'algorithme étendu d'Euclide donne une solution avec les bons degrés et si (P_1, Q_1) est une autre solution, on a $(1-X)^n(P - P_1) = X^n(Q_1 - Q)$, donc X^n divise $P - P_1$ (lemme d'Euclide) : comme $P - P_1$ est de degré au plus $n-1$, il est nul, donc $P = P_1$ puis $Q = Q_1$).

On souhaite obtenir $(1-X)^n P = 1 - X^n Q$. On peut utiliser ici le DL de la fonction $x \longmapsto \dfrac{1}{(1-x)^n}$:

$$\frac{1}{(1-x)^n} = \underbrace{\sum_{k=0}^{n-1} \binom{n+k-1}{k} x^k}_{=P(x)} + O(x^n)$$

car par produit de DL, nous avons :

$$1 = (1-x)^n \frac{1}{(1-x)^n} = (1-x)^n P(x) + O(x^n)$$

Par unicité du DL, cela traduit que le polynôme $(1-X)^n P(X)$ s'écrit $1 + X^n Q(X)$ avec $Q \in \mathbb{R}_{n-1}[X]$.

On obtient, en posant $P_1(X) = P(1-X)$ et $Q_1(X) = Q(1-X)$:

$$X^n P_1(X) + (1-X)^n Q_1(X)$$

et donc $Q(X) = Q_1(1-X) = \sum_{k=0}^{n-1} \binom{n+k-1}{k} (1-X)^k$.

La solution est donc :

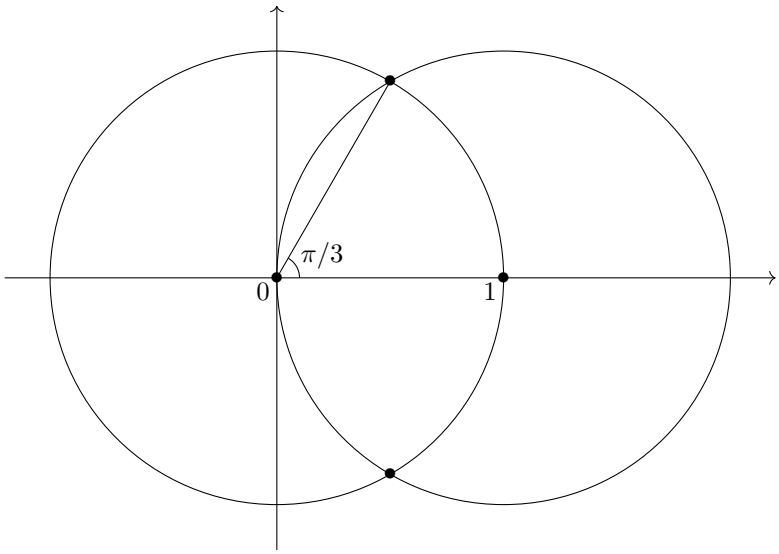
$$P = \sum_{k=0}^{n-1} \binom{n+k-1}{k} X^k \text{ et } Q = \sum_{k=0}^{n-1} \binom{n+k-1}{k} (1-X)^k$$

20) Si P est constant, l'équation donne directement les deux solutions $P = 0$ et $P = 1$.

Supposons que P est un polynôme non constant solution du problème. Si z est une racine de P, on a $P(z^2) = P(z)P(z+1) = 0$, donc z^2 est également une racine de P. Par récurrence, tous les z^{2^n} sont racines de P : comme l'ensemble des racines de P est fini, il existe deux entiers n, m tels que $0 \leq n < m$ et $z^{2^n} = z^{2^m}$: on en déduit que soit z est nul, soit $|z| = 1$.

Si z est non nulle, on peut ensuite écrire $P((z-1)^2) = P(z-1)P(z) = 0$, donc $(z-1)^2$ est racine de P : on a donc soit $z - 1 = 0$, soit $|z-1| = 1$.

Nous avons donc démonté que soit $z = 0$, soit $z = 1$, soit $|z| = |z-1| = 1$, i.e. que $z \in \{0, 1, e^{i\pi/3}, e^{-i\pi/3}\}$, puisque les deux dernières valeurs possibles sont les intersections de deux cercles de rayon 1 :



On ne peut cependant pas avoir $z = e^{\pm i\pi/3}$, car z^2 ne serait pas racine de P : on en déduit que les seules racines possibles de P sont 0 ou 1, ce qui permet d'écrire $P = \alpha X^a (X-1)^b$ avec $\alpha \in \mathbb{C}$ et $a, b \in \mathbb{N}$. En revenant à l'équation, nous obtenons :

$$\alpha X^{2a}(X^2-1)^b = \alpha^2 X^a (X-1)^b (X+1)^a X^b$$

ce qui impose $\alpha = 1$ (α est non nul car $P \neq 0$) et $a = b$.

Réciproquement, les polynômes $X^a(X-1)^a$ sont des solutions non constantes pour tout $a \in \mathbb{N}^*$. L'ensemble des solutions est donc $\{0\} \cup \{X^a(X-1)^a,\ a \in \mathbb{N}\}$.

21) Supposons que $P = UV$ avec $U, V \in \mathbb{Z}[X]$. Comme P ne s'annule pas sur $\mathbb{R}$, il en est de même de U et V. D'après le théorème des valeurs intermédiaires, U et V sont de signes constants sur $\mathbb{R}$. Quitte à remplacer (U, V) par $(-U, -V)$, nous supposerons que $U(x) > 0$ et $V(x) > 0$ pour tout $x \in \mathbb{R}$.

Nous avons, pour $i \in [\![1,n]\!]$, $U(a_i)V(a_i) = 1$; comme $U(a_i)$ et $V(a_i)$ sont des entiers positifs, on a $U(a_i) = V(a_i) = 1$. Si U est de degré strictement inférieur à n, on a $U = 1$ (car $U - 1$ a n racines distinctes et est de degré au plus $n-1$) ; si V est de degré au plus $n-1$, on a de même $V = 1$; sinon, U et V sont de degré n. En notant u_n et v_n les coefficients dominants de U et V, on a $u_n v_n = 1$ et $u_n, v_n \in \mathbb{Z}$. On a donc $u_n = v_n = 1$ (car U et V sont positifs sur $\mathbb{R}$). On en déduit que $U - V$ est de degré au plus $n-1$ et a au moins n racines : on a donc $U = V$ et $P = U^2$, ce qui donne l'absurdité

$$1 = U^2 - W^2 = (U - W)(U + W) \text{ avec } W = \prod_{i=1}^{n}(X - a_i).$$

Nous avons donc démontré que les seuls factorisations de P dans $\mathbb{Z}[X]$ sont $P = 1 \times P$ et $P = (-1) \times (-P)$: P est irréductible dans $\mathbb{Z}[X]$.

La preuve est presque identique pour Q : supposons que $Q = UV$ avec $U, V \in \mathbb{Z}[X]$. On a cette fois, pour tout $i \in [\![1,n]\!]$, $U(a_i)V(a_i) = -1$ avec $U(a_i), V(a_i) \in \mathbb{Z}$: on en déduit que soit $U(a_i) = 1$ et $V(a_i) = -1$, soit $U(a_i) = -1$ et $V(a_i) = 1$; dans tous les cas, $(U + V)(a_i) = 0$. Ainsi, $U + V$ a n racines distinctes. Si U et V sont non constants, U et V sont de degré au plus $n-1$, donc $U+V$ également ; on en déduit que $U + V = 0$, ce qui donne l'absurdité $Q = -U^2$ (le coefficient dominant de $-U^2$ est négatif alors que celui de Q vaut 1). On a donc montré que soit U est constant, soit V est constant. Comme U et V valent ± 1 en a_1, nous avons démontré que les seules factorisations de Q dans $\mathbb{Z}[X]$ sont $Q = 1 \times Q$ et $Q = (-1) \times (-Q)$.

Pour démontrer que P et Q sont irréductibles dans $\mathbb{Q}[X]$, nous aurons besoin d'une définition : pour $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$ (la somme est évidemment finie), le *contenu* de P, noté $\mathcal{C}(P)$, est le P.G.C.D. des coefficients a_k. Nous pouvons montrer la propriété :

$$\forall P, Q \in \mathbb{Z}[X] \setminus \{0\},\ \mathcal{C}(PQ) = (P)\mathcal{C}(Q).$$

La preuve se fait en commençant par le cas où $\mathcal{C}(P) = \mathcal{C}(Q) = 1$. Si on note $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$, on a $PQ = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$. Si p est un nombre premier, il existe $i_0 \geq 0$ tel que $p \,|\, a_i$ pour tout $i < i_0$ et $p \not| a_{i_0}$ (les a_i sont premiers entre eux) ; de même, il existe j_0 tel que $p \,|\, b_j$ pour tout $j < j_0$ et $p \not| b_{j_0}$. On a alors

$$c_{i_0+j_0} = \sum_{i=0}^{i_0+j_0} a_i b_{i_0+j_0-i} = \underbrace{\sum_{i=0}^{i_0-1} a_i b_{i_0+j_0-i}}_{\text{divisible par } p} + a_{i_0} b_{j_0} + \underbrace{\sum_{j=0}^{j_0-1} a_{i_0+j_0-j} b_j}_{\text{divisible par } p}$$

Comme $a_{i_0} b_{j_0}$ est non nul modulo p (p est premier), nous avons démontré que les coefficients de PQ n'avaient pas de facteur premier commun : ils sont donc premiers entre eux, soit $\mathcal{C}(PQ) = 1$.

Supposons maintenant que P et Q sont quelconques dans $\mathbb{Z}[X] \setminus \{0\}$. On peut factoriser par les contenus et écrire $P = aP_1$ et $Q = bQ_1$ avec $a = \mathcal{C}(P)$, $b = \mathcal{C}(Q)$, $P_1, Q_1 \in \mathbb{Z}[X]$ et $\mathcal{C}(P_1) = \mathcal{C}(Q_1) = 1$. On a alors :

$$\mathcal{C}(PQ) = \mathcal{C}(abP_1Q_1) = abC(P_1Q_1) = ab = \mathcal{C}(P)\mathcal{C}(Q)$$

en remarquant que pour $P \in \mathbb{Z}[X]$ non nul et $a \in \mathbb{Z}$ non nul, on a trivialement $\mathcal{C}(aP) = a\mathcal{C}(P)$.

Nous pouvons maintenant démontrer que P (la preuve serait identique pour Q) est irréductible dans $\mathbb{Z}[X]$: si $P = UV$ avec $U, V \in \mathbb{Q}[X]$, il existe deux entiers $a_1, b_1 \geq 1$ tels que $U_1 = a_1 U \in \mathbb{Z}[X]$ et $V_1 = b_1 V \in \mathbb{Z}[X]$ (il suffit de prendre le P.P.C.M. des dénominateurs des coefficients de U ou de V). On a donc $a_1 b_1 P = U_1 V_1$. On peut ensuite écrire $U_1 = a_2 U_2$ et $V_1 = b_2 V_2$ avec $a_2 = \mathcal{C}(U_1)$, $b_2 = \mathcal{C}(V_1)$, $U_2, V_2 \in \mathbb{Z}[X]$ et $\mathcal{C}(U_2) = \mathcal{C}(V_2) = 1$. On a ensuite $a_1 b_1 P = a_2 b_2 U_2 V_2$; en prenant le contenu, on obtient $a_1 b_1 \mathcal{C}(P) = a_2 b_2$, soit $a_1 b_1 = a_2 b_2$ car $\mathcal{C}(P) = 1$ (son coefficient dominant est égal à 1) ; il reste à simplifier par $a_1 b_1$ pour obtenir $P = U_2 V_2$ avec $U_2, V_2 \in \mathbb{Z}[X]$: on a donc $U_2 = \pm 1$ ou $V_2 = \pm 1$, ce qui montre que U ou V est un polynôme constant$= P$ est bien irréductible dans $\mathbb{Q}[X]$.

22) Si P est constant, le résultat est évident. Sinon, $P(x)$ tend vers $+\infty$ quand x tend vers $-\infty$ ou vers $+\infty$. On en déduit donc que P est de degré pair et a un coefficient dominant strictement positif. Il en est donc de même pour Q (Q a même terme dominant que P). Ainsi, $Q(x)$ tend vers $+\infty$ quand x tend vers $\pm\infty$. On en déduit que Q est minoré sur $\mathbb{R}$ et atteint sa borne inférieure. La preuve est classique : il existe $A > 0$ tel que

$$\forall x \in]-\infty, -A] \cup [A, +\infty[,\ Q(x) \geq Q(0)$$

puis Q est continue sur le compact $[-A, A]$, donc il existe $a \in [-A, A]$ tel que

$$\forall x \in [-A, A],\ Q(x) \geq Q(a).$$

En particulier, $Q(0) \geq Q(a)$, ce qui donne :

$$\forall x \in]-\infty, -A] \cup [A, +\infty[,\ Q(x) \geq Q(0) \geq Q(a).$$

Ainsi, Q atteint un minimum en a et $Q'(a) = 0$. On a ensuite $Q = P + Q'$, donc $Q(a) = P(a) \geq 0$: ceci prouve que $Q \geq 0$.

23) Soit z une racine de P. On a :

$$|a_n z^n| = \left| -\sum_{k=0}^{n-1} a_k z^k \right| \leq \sum_{k=0}^{n-1} |a_k| |z|^k \leq M_0 \sum_{k=0}^{n-1} |z|^k.$$

Si $|z| \leq 1$, on a bien $|z| \leq 1 + \frac{M_0}{|a_n|}$; sinon, on a :

$$|a_n|\,|z|^n \leq M_0\, \frac{|z|^n - 1}{|z| - 1} \leq M_0\, \frac{|z|^n}{|z| - 1}$$

ce qui donne $|z| \leq 1 + \frac{M_0}{|a_n|}$.

On obtient la minoration de $|z|$ en appliquant cette première inégalité au polynôme $Q(X) = \sum_{k=0}^{n} a_{n-k} X^k$ et à sa racine $1/z$.

24) L'ensemble $\mathcal{I} = \{Q \in \mathbb{Q}[X],\ Q(\alpha) = 0\}$ est un idéal de $\mathbb{Q}[X]$ non réduit à $\{0\}$ (il contient P) ; il est donc engendré par un polynôme normalisé $P_0 \in \mathbb{Q}[X]$, α est alors racine simple de P_0 puisque dans le cas contraire, on aurait $P_0' \in \mathcal{I}$ et P_0 diviserait P_0', ce qui est absurde car P_0' est non nul de degré strictement plus petit que celui de P_0.

On peut alors écrire $P = P_0 Q_1$ avec $Q_1 \in \mathbb{Q}[X]$ et α est racine de Q_1 d'ordre $k - 1$; une récurrence immédiate montre que $P = P_0^k Q_k$ avec $Q_k \in \mathbb{Q}[X]$; on a donc $2k - 1 \geq \deg(P) \geq k\deg(P_0)$, ce qui impose $\deg(P_0) = 1$, i.e. $\alpha \in \mathbb{Q}$.

25) Notons a, b, c les trois racines de P, avec $a^2 = b^2 + c^2$. Nous avons $a + b + c = 2$, $ab + bc + ca = 7$ et $abc = -k$. On en déduit :

$$\begin{cases} b + c = 2 - a \\ bc = 7 - a(b + c) = 7 - 2a + a^2 \end{cases}$$

puis $(2 - a)^2 = (b + c)^2 = b^2 + 2bc + c^2 = a^2 + 2(7 - 2a + a^2) = 14 - 4a + 3a^2$, ce qui donne $a^2 = -5$. Il existe donc $\varepsilon \in \{-1, 1\}$ tel que $a = \varepsilon\sqrt{5}\, i$ et $k = -abc = -7a + 2a^2 - a^3 = -2a - 10 = -10(1 + \varepsilon\sqrt{5}\, i)$.

Nous avons trouvé deux valeurs possibles pour k, il reste à démontrer que ces valeurs conduisent bien à une solution. Pour $\varepsilon \in \{-1, 1\}$, on peut poser $a = \varepsilon\sqrt{5}\, i$ et définir $b, c \in \mathbb{C}$ tels que $b + c = 2 - a$ et $bc = 7 - 2a + a^2$ (b et c sont les racines du polynôme $X^2 - (2 - a)X + 7 - 2a + a^2$). On a ensuite :

$$(X - a)(X - b)(X - c) = X^3 - 2X^2 + 7X - 10(1 + \varepsilon\sqrt{5}\, i)$$

et on a bien $b^2 + c^2 = (b + c)^2 - 2bc = (2 - a)^2 - 2(7 - 2a + a^2) = -10 - a^2 = -5 = a^2$.

26) Notons $A(X) = \prod_{i=1}^{n} (X - a_i)$ et $B(X) = \prod_{j=1}^{n} (X - b_j)$ et supposons qu'il existe $\lambda \in \mathbb{C}$ tel que $\prod_{j=1}^{n} (a_i + b_j) = \lambda$ pour tout i. Le polynôme $P = \prod_{j=1}^{n} (X + b_j) - \lambda$ est de degré n, unitaire et admet les a_i pour racines : comme les a_i sont deux à deux distincts, on en déduit que $P = A$, ce qui donne après développement :

$$X^n + \sum_{k=1}^{n-1} \sigma_{n-k}(b) X^k + \sigma_n(b) - \lambda = X^n + \sum_{k=0}^{n-1} (-1)^{n-k} \sigma_{n-k}(a) X^k$$

en notant, pour $x=(x_1,\dots,x_n)\in\mathbb{C}^n$ et $1\leq k\leq n$, $\sigma_k(x)=\displaystyle\prod_{1\leq i_1<i_2<\dots<i_k\leq n} x_{i_1}\dots x_{i_k}$. Par identification, nous obtenons donc :

$$\sigma_n(b)-\lambda=(-1)^n\sigma_n(a) \text{ et } \forall k\in[\![1,n-1]\!],\ \sigma_{n-k}(b)=(-1)^{n-k}\sigma_{n-k}(a).$$

Symétriquement, nous pouvons écrire :

$$B=X^n+\sum_{k=0}^{n-1}(-1)^{n-k}\sigma_{n-k}(b)X^k=X^n+\sum_{k=1}^{n-1}\sigma_{n-k}(a)X^k+\sigma_n(a)+(-1)^n\lambda=\prod_{i=1}^{n}(X+a_i)-(-1)^n\lambda.$$

Comme $B(b_j)=0$ pour tout j, nous obtenons

$$\forall j\in[\![1,n]\!],\ \prod_{i=1}^{n}(a_i+b_j)=(-1)^n\lambda$$

d'où l'existence de μ.

Par symétrie, l'équivalence est démontrée.

27) a) Soit $P\in\mathbb{R}[X]$ tel que $P(\mathbb{Q})\subset\mathbb{Q}$. Si P est non nul, notons d son degré et fixons $a_0,\dots,a_d$, rationnels distincts. Le polynôme P est alors le polynôme d'interpolation de Lagrange de la famille de points $(a_i,P(a_i))_{0\leq i\leq d}$, ce qui donne :

$$P=\sum_{i=0}^{d}\underbrace{P(a_i)}_{\in\mathbb{Q}}\prod_{\substack{0\leq j\leq d\\ j\neq i}}\underbrace{\frac{X-a_j}{a_i-a_j}}_{\in\mathbb{Q}[X]}$$

et on en déduit que $P\in\mathbb{Q}[X]$. Comme $0\in\mathbb{Q}[X]$, on a $P\in\mathbb{Q}[X]$ dans tous les cas.

Réciproquement, si $P\in\mathbb{Q}[X]$, on a trivialement $P(\mathbb{Q})\subset\mathbb{Q}$.

b) Il est évident que les polynômes $aX+b$ avec $a\in\mathbb{Q}^*$ et $b\in\mathbb{Q}$ sont solutions. Réciproquement, supposons maintenant que $P(\mathbb{Q})=\mathbb{Q}$ avec $P\in\mathbb{R}[X]$. On sait donc que $P\in\mathbb{Q}[X]$ et on peut ensuite écrire $P=\dfrac{1}{q}\underbrace{\displaystyle\sum_{k=0}^{d}a_kX^k}_{=Q}$ avec $d\geq 1$, $q\in\mathbb{N}^*$, $a_0,\dots,a_d\in\mathbb{Z}$ et $a_d\neq 0$. On a $Q(\mathbb{Q})=qP(\mathbb{Q})=\mathbb{Q}$. Pour tout p entier premier, il existe donc $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$ tel que $a\wedge b=1$ et $Q(a/b)=1/p$. On en déduit, en multipliant par pb^d :

$$p\sum_{k=0}^{d}a_ka^kb^{d-k}=b^d.$$

Ainsi, p divise b^d, donc p divise b (car p est premier). Supposons que $d\geq 2$; b^d est alors divisible par p^2, ce qui prouve que p divise $\sum_{k=0}^{d}a_ka^kb^{d-k}$. Comme p divise tous les b^{d-k} pour $0\leq k<d$, on en déduit que p divise a_da^d. Enfin, p divise b et $a\wedge b=1$, donc $p\wedge a=1$: le lemme de Gauss prouve que p divise a_d, ce qui est absurde : un entier non nul ne peut pas être divisible par tous les nombres premiers. Ainsi, l'hypothèse $d\geq 2$ est absurde : P est de degré 1 et P est bien de la forme voulue.

Les polynômes réels P vérifiant $P(\mathbb{Q})=\mathbb{Q}$ sont donc les polynômes de la forme $P=aX+b$ avec $a\in\mathbb{Q}^*$ et $b\in\mathbb{Q}$.

28) Pour $a\in\mathbb{C}$, notons $P_a=P-a$. Comme $P_a'=P$, un complexe z est racine multiple d'ordre $1+k$ de P_a si et seulement si z est racine de P_a et racine d'ordre k de P_a. On en déduit que si $a\in\mathbb{C}$ n'est pas de la forme $P(z)$ avec z racine de P', P_a aura d racines simples et $d-n(a)$ sera nul. On peut donc restreindre la somme aux a de la forme $P(z)$ avec z racine de P'. Notons donc $z_1,\dots,z_k$ les racines de P', d'ordres respectifs $n_1,\dots,n_k\in\mathbb{N}^*$. Notons alors $\{a_1,\dots,a_q\}=\{P(z_1),\dots,P(z_k)\}$ (les a_i étant deux à deux distincts). On peut alors écrire $\{1,\dots,k\}=I_1\bigsqcup I_2\bigsqcup\dots\bigsqcup I_q$ avec :

$$\forall j,\ i\in I_j\iff P(z_i)=a_j.$$

On a alors $\sum_{a\in\mathbb{C}} d-n(a) = \sum_{j=1}^{q} d-n(a_j)$ et pour tout j, P_{a_j} a pour racines multiples les z_i pour $i\in I_j$. Comme chacun de ces z_i est racines de P_{a_i} d'ordre n_i+1 et que les autres racines sont simples, nous pouvons écrire :

$$\begin{cases} d = \deg(P_a) = m_j + \sum_{i\in I_j}(1+n_i) \\ n(a_j) = m_j + \sum_{i\in I_j} 1 \end{cases}$$

où m_j est le nombre de racines simple de P_{a_j}. On obtient donc :

$$\sum_{a\in\mathbb{C}} d-n(a) = \sum_{j=1}^{d}\sum_{i\in I_j} n_i = \sum_{i=1}^{k} n_i = \deg(P') = d-1.$$

29) a) On peut écrire $P = \alpha\prod_{i=1}^{k}(X-a_i)^{n_i}$ avec $\alpha\neq 0$, $k\geq 1$, $a_1<\cdots<a_k$ et $n_1,\ldots,n_k\in\mathbb{N}^*$. On a alors $\dfrac{P'}{P} = \sum_{i=1}^{k}\dfrac{n_i}{X-a_i}$. Par dérivation, on obtient :

$$\forall x\in\mathbb{R}\setminus\{a_1,\ldots,a_k\},\ \frac{P''(x)P(x)-(P'(x))^2}{P^2(x)} = -\sum_{i=1}^{k}\frac{n_i}{(x-a_i)^2}$$

Ainsi, si $P'(x)=0$ et $x\notin\{a_1,\ldots,a_k\}$, on obtient $P''(x)P(x) = -P^2(x)\sum_{i=1}^{k}\dfrac{n_i}{(x-a_i)^2} < 0$.

b) Remarquons tout d'abord que si un polynôme $P\in\mathbb{R}[X]$ est scindé sur $\mathbb{R}$, P' l'est également : en notant comme précédemment $P=\alpha\prod_{i=1}^{k}(X-a_i)^{n_i}$, le théorème de Rolle assure l'existence de racines $b_1,\ldots,b_{k-1}$ de P' avec :

$$\forall i\in\{1,\ldots,k-1\},\ a_i<b_i<a_{i+1}.$$

Comme chaque a_i est racine de P' d'ordre n_i-1, nous avons mis en évidence $n-1$ racines réelles de P' (comptées avec leur multiplicité), puisque $\sum_{i=1}^{k}(n_i-1)+\sum_{i=1}^{k-1}1 = n-k+(k-1) = n-1$. Ceci prouve que P' est scindé sur $\mathbb{R}$ et que les $b_1,\ldots,b_{k-1}$ sont des racines simples de P' (c'est aussi une conséquence de la question a, appliquée à P, $x_1=a_i$, $x_2=a_{i+1}$ et $x=b_i$: $P''(b_i)P(b_i)<0$ implique que $P''(b_i)$ est non nul).

Supposons maintenant que $P-a$ et $P-b$ sont scindés sur $\mathbb{R}$; $(P-a)'$ est donc scindé sur $\mathbb{R}$ et ses racines multiples ne peuvent être que des racines de $P-a$; de même, $(P-b)'$ est scindé et ses racines multiples ne peuvent être que des racines de $P-b$. On en déduit que P' est scindé sur $\mathbb{R}$ et que ses éventuelles racines multiples appartiennent à $\{x\in\mathbb{R},\ P(x)=a\}\cap\{x\in\mathbb{R},\ P(x)=b\}$: comme cette intersection est vide, P' n'a que des racines simples.

30) a) En écrivant $P=\alpha\prod_{i=1}^{k}(X-a_i)^{n_i}$, avec $\alpha\in\mathbb{C}^*$, a_i complexes distincts et $n_i\in\mathbb{N}^*$, nous avons $P\wedge P' = \prod_{i=1}^{k}(X-a_i)^{n_i-1}$. Nous en déduisons :

$$\deg(P)-\deg(P\wedge P') = \sum_{i=1}^{k} n_i - \sum_{i=1}^{k}(n_i-1) = k = \mathrm{Card}(Z(P)).$$

b) On a $Z(R)\subset Z(P)\cup Z(P-1)$ et $Z(P)\cap Z(P-1)=0$, donc $\mathrm{Card}(Z(R))\geq \mathrm{Card}(Z(P))+\mathrm{Card}(Z(P-1))$. Nous obtenons donc :

$$\mathrm{Card}(Z(R))\geq \deg(P)-\deg(P\wedge P')+\deg(P-1)-\deg((P-1)\wedge(P-1)') = 2n-\deg(P\wedge P')-\deg((P-1)\wedge P')$$

Les polynômes $Q_1 = P\wedge P'$ et $Q_2=(P-1)\wedge P'$ sont premiers entre eux (car P et $P-1$ le sont) et divisent P', donc Q_1Q_2 divise P'. On en déduit que $\deg(Q_1)+\deg(Q_2)\leq\deg(P')=n-1$, ce qui donne :

$$\mathrm{Card}(Z(R))\geq 2n-(n-1) = n+1.$$

Ainsi, R est de degré au plus n et a au moins $n+1$ racines : on en déduit que $R=0$, i.e. que $P=Q$.

Remarque : plus généralement, nous avons démontré que si a et b sont deux complexes distincts, un polynôme non constant P est caractérisé par les ensembles $P^{-1}(\{a\})$ et $P^{-1}(\{b\})$, i.e. :

$$\forall P,Q\in\mathbb{C}[X]\setminus\mathbb{C},\ \left(P^{-1}(\{a\})=Q^{-1}(\{a\}) \text{ et } P^{-1}(\{b\})=Q^{-1}(\{b\})\right)\Longrightarrow P=Q.$$

31) Notons E la réunion des ensembles de racines de P et de Q. Nous pouvons donc écrire $E=\{\lambda_1,\dots,\lambda_m\}$ où les λ_i sont deux à deux distincts et noter, pour tout i, p_i (resp. q_i) l'ordre de multiplicité de λ_i comme racine de P (resp. de Q). Nous avons donc :

$$\forall k\in\mathbb{N}^*,\ S_k(P)=\sum_{i=1}^m p_i\lambda_i^k \text{ et } \forall k\in\mathbb{N}^*,\ S_k(Q)=\sum_{i=1}^m q_i\lambda_i^k.$$

En supposant que P et Q ont les mêmes sommes de Newton, nous avons :

$$\forall k\in[\![0,m-1]\!],\ \sum_{i=1}^m(p_i-q_i)\lambda_i^k=0$$

(la formule est également vérifiée pour $k=0$ car $\sum_{i=1}^k p_i=\sum_{i=1}^k q_i=n$). Comme les λ_i sont distincts deux à deux, on peut voir ces équations comme un système linéaire homogène d'inconnues p_i-q_i dont le déterminant (Vandermonde) est non nul. On en déduit que $p_i=q_i$ pour tout i, ce qui traduit que P et Q ont les mêmes racines associées aux mêmes ordres de multiplicité ; comme P et Q sont normalisés, ils sont égaux.

32) a) Comme P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, il existe $U,V\in\mathbb{Q}[X]$ tels que $UP+VQ=1$. En notant d le P.P.C.M des dénominateurs des coefficients des polynômes U et V, nous avons $dUP+dVQ=d$ avec $U_1=dU\in\mathbb{Z}[X]$ et $V_1=dV\in\mathbb{Z}[X]$: on a alors, pour tout $n\in\mathbb{N}$, $u_n\,|\,U_1(n)P(n)+V_1(n)Q(n)=d$, puisque u_n divise $P(n)$ et $Q(n)$ et que $U_1(n)$ et $V_1(n)$ sont entiers.

b) En posant $R=\sum_{k=0}^n a_kX^k$ avec $a_k\in\mathbb{Z}$ pour tout k, nous avons :

$$\begin{aligned}\forall n\in\mathbb{N},\ R(n+d)-R(n) &= \sum_{k=0}^n a_k((n+d)^k-n^k)\\ &= \sum_{k=0}^n a_k\,(n+d-n)((n+d)^{k-1}+(n-d)^{k-2}n+\cdots+(n-d)n^{k-2}+n^{k-1})\\ &= d\underbrace{\sum_{k=0}^n a_k\,((n+d)^{k-1}+(n-d)^{k-2}n+\cdots+(n-d)n^{k-2}+n^{k-1})}_{\in\mathbb{Z}}\in d\mathbb{Z}\end{aligned}$$

c) Pour $n\in\mathbb{N}$, u_n divise d, qui divise $P(n+d)-P(n)$: comme u_n divise $P(n)$, il divise $P(n+d)$; de même, u_n divise $Q(n+d)$, donc u_n divise $u_{n+d}=P(n+d)\wedge Q(n+d)$. Une preuve symétrique prouve que u_{n+d} divise u_n : u est donc d périodique.

33) Comme les a_k sont des racines simples, on a :

$$\frac{P''}{P}=\sum_{k=1}^n\frac{P''(a_k)}{P'(a_k)}\,\frac{1}{X-a_k}.$$

On en déduit la décomposition en éléments simples :

$$\frac{XP''}{P}=\sum_{k=1}^n\frac{P''(a_k)}{P'(a_k)}+\sum_{k=1}^n\frac{P''(a_k)}{P'(a_k)}\frac{a_k}{X-a_k}$$

Comme XP'' est de degré $n-1$ et P de degré n, la partie entière de cette décomposition est nulle : $S=0$.

34) On a $P=\prod_{k=1}^{n}(X-a_k)$, puis $P'=\sum_{i=1}^{n}\prod_{\substack{k=1\\k\neq i}}^{n}(X-a_k)$. cela donne :

$$S_1=\sum_{i=1}^{n}\frac{1}{\prod_{\substack{k=1\\k\neq i}}(a_i-a_k)}.$$

On peut alors penser à l'expression des polynômes interpolateurs de Lagrange : pour $b_1,\dots b_n$ complexes quelconques, l'unique polynôme $Q\in\mathbb{C}_{n-1}[X]$ tel que $Q(a_i)=b_i$ pour tout i est le polynôme :

$$Q=\sum_{i=1}^{n}b_i\,\frac{\prod_{k\neq i}(X-a_k)}{\prod_{k\neq i}(a_i-a_k)}.$$

En choisissant tous les b_i égaux à 1, Q est le polynôme constant égal à 1, ce qui donne :

$$1=\sum_{i=1}^{n}\frac{\prod_{k\neq i}(X-a_k)}{\prod_{k\neq i}(a_i-a_k)}.$$

S_1 est alors le coefficient de degré $n-1$ de ce polynôme : on a donc $S_1=0$ puisque $n\geq 2$.

Pour la seconde somme, on peut penser à décomposer en éléments simples la fraction $\frac{1}{P}$:

$$\frac{1}{P}=\sum_{i=1}^{n}\frac{1}{\prod_{k\neq i}(a_i-a_k)}\,\frac{1}{X-a_i}.$$

En évaluant en $X=0$, nous obtenons $S_2=-\dfrac{1}{P(0)}=\dfrac{(-1)^{n+1}}{a_1\dots a_n}$.

Exercices X-ENS

35) a) Soit $m\in\mathbb{N}$. Nous avons $\lambda_i^{m-n}P(\lambda_i)=0$ pour tout i, ce qui donne la relation demandée en sommant pour i variant de 1 à n.

b) L'idée est de faire un développement asymptotique du polynôme $P_i=\dfrac{P}{X-\lambda_i}$ au voisinage de l'infini :

$$\begin{aligned}P_i &= \left(X^n-\sigma_1X^{n-1}+\dots+(-1)^n\sigma_n\right)\left(\frac{1}{X}+\frac{\lambda_i}{X^2}+\dots+\frac{\lambda_i^{n-1}}{X^n}+o\left(\frac{1}{X^n}\right)\right)\\ &= \sum_{k=0}^{n-1}\left(\lambda_i^k+\sum_{j=1}^{k}(-1)^j\sigma_j\lambda_i^{k-j}\right)X^{n-1-k}+o(1)\end{aligned}$$

Le terme $o(1)$ est un polynôme qui tend vers 0 à l'infini, c'est donc le polynôme nul, d'où l'égalité :

$$P_i=\sum_{k=0}^{n-1}\left(\lambda_i^k+\sum_{j=1}^{k}(-1)^j\sigma_j\lambda_i^{k-j}\right)X^{n-1-k}$$

c) Nous avons classiquement $\dfrac{P'}{P}=\sum_{i=1}^{n}\dfrac{1}{X-\lambda_i}$, d'où $\sum_{i=1}^{n}P_i=P'$.

Nous obtenons donc :

$$\begin{aligned} P' = \sum_{i=1}^{n} P_i &= nX^{n-1} + \sum_{k=1}^{n-1} \left[\sum_{i=1}^{n} \left(\lambda_i^k + \sum_{j=1}^{k} (-1)^j \sigma_j \lambda_i^{k-j} \right) \right] X^{n-1-k} \\ &= nX^{n-1} + \sum_{k=1}^{n-1} \left[S_k + \left(\sum_{j=1}^{k-1} (-1)^j \sigma_j S_{k-j} \right) + (-1)^k n \sigma_k \right] X^{n-1-k} \end{aligned}$$

qui nous donne

$$nX^{n-1} + \sum_{k=1}^{n-1} (-1)^k (n-k) \sigma_k X^{n-k-1} = nX^{n-1} + \sum_{k=1}^{n-1} \left[S_k + \left(\sum_{j=1}^{k-1} (-1)^j \sigma_j S_{k-j} \right) + (-1)^k n \sigma_k \right] X^{n-1-k}$$

Il suffit ensuite d'identifier ces deux polynômes pour obtenir :

$$\forall k \in [\![1, n-1]\!],\ S_k + \left(\sum_{j=1}^{k-1} (-1)^j \sigma_j S_{k-j} \right) + (-1)^k k \sigma_k = 0$$

et la relation pour $k = n$ a été obtenue à la question a).

d) Soit $M = \max\limits_{1 \leq i \leq n} |\lambda_i|$. Pour z tel que $|z| < M$ et $i \in \{1, 2, \ldots, n\}$, $(\lambda_i z)^k$ est le terme général d'une série géométrique absolument convergente (car $|\lambda_i z| < 1$). La somme $f(z)$ est donc bien définie, comme somme de n séries absolument convergente et, pour z non nul et de module $< M$:

$$\begin{aligned} f(z)\, z^n P\left(\frac{1}{z}\right) &= \left(\sum_{i=1}^{n} \sum_{k=0}^{\infty} \lambda_i^k z^k \right) z^n \prod_{i=1}^{n} \left(\frac{1}{z} - \lambda_i \right) \\ &= \left(\sum_{i=1}^{n} \frac{1}{1 - \lambda_i z} \right) \prod_{i=1}^{n} (1 - \lambda_i z) \\ &= \sum_{i=1}^{n} \left(\frac{1}{1 - \lambda_i z} \prod_{j=1}^{n} (1 - \lambda_j z) \right) \\ &= \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} (1 - \lambda_j z) \\ &= z^{n-1} P'\left(\frac{1}{z}\right) \end{aligned}$$

Commençons par démontrer le lemme : si $\sum\limits_{k \geq 0} a_k z^k$ converge absolument pour $|z|$ assez petit, alors pour tout $n \in \mathbb{N}$, $\sum\limits_{k=0}^{+\infty} a_k z^k = \sum\limits_{k=0}^{n} a_k z^k + O(z^{n+1})$.

Ceci revient à démontrer que $\sum\limits_{k=n+1}^{+\infty} a_k z^k = O(z^{n+1})$: fixons donc $\rho > 0$ tel que $\sum_{k \geq 0} a_k \rho^k$ converge absolument. Nous avons, pour tout z de module inférieur à ρ (en remarquant que $|a_k \rho^{k-n-1}|$ est le terme général d'une série convergente, puisque c'est un O de $|a_k \rho^k|$) :

$$\left| \sum_{k=n+1}^{+\infty} a_k z^k \right| \leq |z^{n+1}| \underbrace{\sum_{k=n+1}^{+\infty} \left| a_k \rho^{k-n-1} \right|}_{\text{constante}}$$

Les deux séries étant absolument convergentes, nous pouvons écrire par produit de Cauchy :

$$\begin{aligned} f(z)\, z^n P\left(\frac{1}{z}\right) &= \left(\sum_{p=0}^{+\infty} S_p z^p\right)\left(1-\sigma_1 z+\sigma_2 z^2+\cdots+(-1)^n\sigma_n z^n\right) \\ &= \sum_{p=0}^{+\infty}\left(\sum_{k=0}^{p} S_k(-1)^{p-k}\sigma_{p-k}\right) z^p \\ &= \sum_{p=0}^{n}\left(\sum_{k=0}^{p} S_k(-1)^{p-k}\sigma_{p-k}\right) z^p + O(z^{n+1}) \end{aligned}$$

en posant $\sigma_0 = 1$ et $\sigma_k = 0$ pour $k > n$.

Comme $z^{n-1}\, P'\left(\frac{1}{z}\right) = n-(n-1)\sigma_1 z+\cdots+(-1)^k(n-k)\sigma_k z^k+\cdots+(-1)^{n-1}\sigma_{n-1}z^{n-1}$, nous pouvons identifier ces deux DL (il y a unicité du DL au voisinage de 0), ce qui donne :

$$\forall p \in \{0,\ldots,n\},\ \sum_{k=0}^{p} S_k(-1)^{p-k}\sigma_{p-k} = (-1)^p(n-p)\sigma_p$$

ce qui donne les relations demandées, en remarquant que $S_0 = n$ et $\sigma_0 = 1$.

36) a) On rappelle qu'un élément a d'un anneau commutatif A est dit irréductible s'il est non inversible et si les seules décompositions de la forme $a = bc$ sont triviales (i.e. telles que b ou c est inversible).

Dans $Z[X]$, les seuls éléments inversibles sont les polynômes 1 et -1 : p est donc irréductible dans $\mathbb{Z}[X]$, car p n'est pas inversible et si $B, C \in \mathbb{Z}[X]$ vérifient $BC = p$, B et C sont des entiers dont le produit est égal à p : l'un des deux est donc égal à 1 ou -1.

p n'est par contre pas irréductible dans $\mathbb{Q}[X]$, car il y est inversible.

pX est irréductible dans $\mathbb{Q}[X]$ (comme tout polynôme de degré 1), mais il ne l'est pas dans $\mathbb{Z}[X]$ car p et X ne sont pas inversibles dans $\mathbb{Z}[X]$.

b) Supposons pour commencer que $c(P) = c(Q) = 1$ et notons $P = \sum_{n=0}^{+\infty} a_n X^n$ et $Q = \sum_{n=0}^{+\infty} b_n X^n$ (sommes finies). Nous devons montrer que les entiers $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ sont premiers entre-eux dans leur ensemble, i.e. qu'ils n'ont pas de diviseur premier. Or si p est un nombre premier, il existe k_a et k_b tels que :

$$\begin{cases} p \not| a_{k_a} \text{ et } \forall i < k_a,\ p \,|\, a_i \\ p \not| b_{k_b} \text{ et } \forall i < k_b,\ p \,|\, b_i p \not| b_{k_b} \end{cases}$$

Nous avons alors :

$$c_{k_a+k_b} = \left(\sum_{i=0}^{k_a-1} a_i b_{k_a+k_b-i}\right) + a_{k_a} b_{k_b} + \left(\sum_{i=k_a+1}^{k_a+k_b} a_i b_{k_a+k_b-i}\right) \equiv a_{k_a} b_{k_b} \pmod{p}$$

donc p ne divise pas $c_{k_a+k_b}$.

Dans le cas général, il existe deux polynômes P_1 et Q_1 tels que $P = c(P)P_1$ et $Q = c(Q)Q_1$. COmme les coefficients de P_1 (resp.de Q_1) sont ceux de P (resp. de Q) divisés par leur p.g.c.d., on a $c(P_1) = c(Q_1) = 1$. On en déduit que $c(PQ) = c(c(P)c(Q)P_1Q_1) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$.

c) Supposons que P est irréductible sur $\mathbb{Z}$ et non constant.

(i) Comme $P = c(P)P_1$ avec $P_1 \in \mathbb{Z}[X] \setminus \{-1, 1\}$, $c(P) = \pm 1$, i.e. $c(P) = 1$ (car P est irréductible sur $\mathbb{Z}$).

(ii) Comme P n'est pas constant, il n'est pas inversible dans $\mathbb{Q}[X]$.

(iii) Supposons que $P = QR$ avec $Q, R \in \mathbb{Q}[X]$. Il existe deux entiers non nuls u et v et deux polynômes entiers Q_1 et R_1 tels que $uQ = Q_1$ et $vR = R_1$ (u et v sont par exemple les p.p.c.m. des dénominateurs des coefficients de Q et R). On peut ensuite écrire $Q_1 = c(Q_1)Q_2$ et $R_1 = c(R_1)R_2$ avec $Q_2, R_2 \in \mathbb{Z}[X]$ de contenus 1, ce qui nous donne $uvP = c(Q_1)c(R_1)Q_2R_2$. On a ensuite :

$$uv = c(uvP) = c\left(c(Q_1)c(R_1)Q_2R_2\right) = c(Q_1)c(R_1)$$

et on peut simplifier par l'entier non nul uv pour obtenir $P = Q_2R_2$. Comme P est irréductible sur $\mathbb{Z}$ et que $Q_2, R_2 \in \mathbb{Z}[X]$, soit $Q_2 = \pm 1$, soit $R_2 = \pm 1$, ce qui prouve que Q ou R est constant : P n'a pas de factorisation non triviale dans $\mathbb{Q}[X]$.

Réciproquement, supposons que $c(P) = 1$ et que P est irréductible sur $\mathbb{Q}$. P n'est pas inversible dans $\mathbb{Z}[X]$ (il est différent de ± 1) et si $P = QR$ avec $Q, R \in \mathbb{Z}[X]$, on peut supposer par symétrie que Q est constant (car P est irréductible sur $\mathbb{Q}$). Comme $1 = c(P) = c(Q)c(R)$ avec $c(Q), c(R) \in \mathbb{Z}$, Q est égal à ± 1 : P est irréductible dans $\mathbb{Z}[X]$.

d) D'après la question précédente, comme P est de contenu 1 (son coefficient dominant est égal à 1), il suffit de montrer u'il est irréductible sur $\mathbb{Z}$. Supposons donc que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$. Pour tout i, on a $Q(a_i)R(a_i) = -1$ et donc $\{Q(a_i), R(a_i)\} = \{-1, 1\}$ (car $Q(a_i)$ et $R(a_i)$ sont entiers). L'astuce consiste à remarquer que dans les deux cas possibles, $Q(a_i) + R(a_i) = 0$. Si Q et R étaient de degré non nuls, $Q + R$ serait de degré au plus $n - 1$ et aurait n racines distinctes : on aurait alors $Q + R = 0$, puis $P = -Q^2$, ce qui est absurde car le coefficient dominant de P est égal à 1, alors que celui de $-Q^2$ est négatif. Ainsi, Q ou R est constant et donc égal à ± 1 (puisque $\{Q(a_1), R(a_1)\} = \{-1, 1\}$) et P est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.

e) Comme le polynôme $\dfrac{P}{c(P)}$ vérifie exactement les mêmes hypothèses que P (car p n'est pas facteur de $c(P)$, puisque p ne divise pas le coefficient dominant de P), on peut supposer que $c(P) = 1$. D'après le c), P est irréductible sur $\mathbb{Q}$ si et seulement s'il l'est sur $\mathbb{Z}$: supposons que P ne soit pas irréductible ; on peut alors écrire $P = QR$ avec $Q, R \in \mathbb{Z}_{n-1}[X]$. Posons $Q = \sum_{k=0}^{q} b_k X^k$ et $R = \sum_{k=0}^{r} c_k X^k$. Pour $A \in \mathbb{Z}[X]$, notons $\overline{A}$ le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ dont les coefficients sont les classes modulo p des coefficients de A. On a alors $\overline{Q}\,\overline{R} = \overline{P}$, soit $\overline{Q}\,\overline{R} = \overline{a_n}X^n$. Comme a_n est non nul modulo p, il existe m tel que $m \leq q$, $n - m \leq r$ et $\overline{Q} = \overline{b_m}X^m$ et $\overline{R} = \overline{c_{n-m}}X^{n-m}$. Ceci signifie que tous les b_i (resp. tous les c_i) sont divisibles par p, sauf pour $i = m$ (resp. sauf pour $i = n - m$). Comme m et $n - m$ sont différentes de 0 (car $n - m \leq r \leq n - 1$ et $m \leq q \leq n - 1$), $\overline{b_0} = \overline{c_0} = 0$. On en déduit que $a_0 = b_0c_0$ est divisible par p^2 : c'est absurde.

Le critère d'Eisenstein permet de démontrer par exemple que le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$, qui est donc le polynôme minimal du nombre algébrique $\sqrt[n]{2}$.

37) Nous allons utiliser deux résultats classiques :

lemme 1 : si P est un polynôme réel scindé, P' est également scindé.

lemme 2 : si P est un polynôme réel scindé, $P(x)P''(x) - P'(x)^2 \leq 0$ pour tout $x \in \mathbb{R}$.

Le premier lemme se montre à l'aide du théorème de Rolle : en supposant P non constant (sinon le résultat est évident), on peut écrire $P = \alpha \prod_{i=1}^{k} (X - a_i)^{n_i}$ avec $\alpha \neq 0$, $k \in \mathbb{N}^*$, $a_1 < \cdots < a_k$ et $n_1, \ldots n_k \in \mathbb{N}^*$. D'après le théorème de Rolle (quand $k \geq 2$), P' possède une racine b_i dans chaque intervalle $]a_i, a_{i+1}[$. Nous pouvons donc écrire :

$$P' = \left(\prod_{i=1}^{k} (X - a_i)^{n_i - 1}\right) \times \left(\prod_{i=1}^{k-1} (X - b_i)\right) \times Q$$

avec $Q \in \mathbb{R}[X]$. Comme P' est de degré $n_1 + n_2 + \cdots + n_k - 1 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) + k - 1$, Q est constant et P' est scindé.

Pour le second point, toujours avec $P = \alpha \prod_{i=1}^{k} (X - a_i)^{n_i}$, on peut penser à utiliser la fraction rationnelle $\dfrac{P'}{P}$, qui se décompose éléments simples sous la forme $\sum_{i=1}^{k} \dfrac{n_i}{X - a_i}$. En dérivant, on obtient :

$$\forall x \in \mathbb{R} \setminus \{a_1, \ldots, a_k\},\ \frac{P(x)P''(x) - P'(x)^2}{P(x)^2} = -\sum_{i=1}^{k} \frac{n_i}{(x - a_i)^2} < 0,$$

ce qui donne l'inégalité demandée (en prolongeant par continuité l'inégalité stricte en une inégalité large).

Nous pouvons maintenant résoudre l'exercice : supposons que $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{R}[X]$ et qu'il existe $k \in \{1, \dots, n-1\}$ tel que $a_{k-1}a_{k+1} > 0$ et $a_k = 0$. Le polynôme $Q = P^{(k-1)}$ vérifie alors :

$$Q(0) = P^{(k-1)}(0) = (k-1)!\, a_{k-1},\ Q'(0) = P^{(k)}(0) = k!\, a_k \text{ et } Q''(0) = P^{(k+1)}(0) = (k+1)!\, a_{k+1}.$$

On a donc $Q(0)Q''(0) - Q'(0)^2 = (k-1)!\,(k+1)!a_{k-1}a_{k+1} > 0$, ce qui prouve que Q n'est pas scindé (contraposée du lemme 2), puis P ne l'est pas non plus (contraposée du lemme 1).

38) Pour tous entiers k, k', nous noterons $\overline{k}$ la classe de k modulo p et nous écrirons $k \equiv k'$ pour traduire que k et k' sont congrus modulo p. Nous pouvons démontrer que p divise a en considérant le polynôme $P = X^{p-1} - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[X]$. Comme le groupe multiplicatif du corps $\mathbb{Z}/p\mathbb{Z}$ est de cardinal $p-1$, on a $\overline{k}^{p-1} = \overline{1}$ pour tout $k \in [\![1, p-1]\!]$. On en déduit que P a $p-1$ racines distinctes, qui sont les $p-1$ éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$. Les relations entre racines et coefficients donnent :

$$\sigma_{p-1} = \prod_{k=1}^{p-1} \overline{k} = (-\overline{1})^p = -\overline{1} \text{ et } \sigma_{p-2} = \sum_{k=1}^{p-1} \left(\prod_{\substack{1 \le q \le p-1 \\ q \ne k}} \overline{q} \right) = \overline{0}.$$

La première égalité donne la formule de Wilson : $(p-1)! \equiv -1$; la seconde donne :

$$a = \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = \sum_{k=1}^{p-1} \left(\prod_{\substack{1 \le q \le p-1 \\ q \ne k}} q \right) \equiv 0.$$

Pour montrer que p^2 divise a, nous allons utiliser une autre méthode qui va permettre de commencer par factoriser a par p. L'astuce consiste à écrire :

$$2a = (p-1)! \left(\sum_{k=1}^{p-1} \frac{1}{k} + \sum_{k=1}^{p-1} \frac{1}{p-k} \right) = (p-1)! \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) = p \sum_{k=1}^{p-1} \underbrace{\frac{(p-1)!}{k(p-k)}}_{=b_k}.$$

Comme $k \ne p-k$ (p est impair), b_k est entier. Nous avons ensuite :

$$\forall k \in [\![1, p-1]\!],\ b_k k(p-k) = (p-1)! \equiv -1$$

soit encore, puisque $p - k \equiv -k$:

$$\forall k \in [\![1, p-1]\!],\ b_k k^2 \equiv 1$$

Pour tout $k \in [\![1, p-1]\!]$, il existe un unique entier $q(k) \in [\![1, p-1]\!]$ tel que $kq(k) \equiv 1$ ($\overline{q(k)}$ est l'inverse de $\overline{k}$). Nous pouvons alors écrire :

$$\sum_{k=1}^{p-1} b_k \equiv \sum_{k=1}^{p-1} b_k k^2 q_k^2 \equiv \sum_{k=1}^{p-1} q_k^2$$

Comme $k \longmapsto q_k$ est une permutation de $[\![1, p-1]\!]$, nous avons :

$$\sum_{k=1}^{p-1} b_k \equiv \sum_{q=1}^{p-1} q^2 = \frac{(p-1)p(2p-1)}{6}.$$

Nous avons ainsi prouvé que $12a$ est divisible par p^2. Comme p est premier et différent de 3, p est premier avec 6 et p^2 divise a d'après le lemme de Gauss.

Remarque : on peut aussi dire que $\sum_{q=1}^{p-1} \overline{q}^2 = \sigma_1^2 - 2\sigma_2$ où les σ sont les fonctions symétriques élémentaires associées au polynôme P. Comme les coefficients de degré $p-2$ et $p-3$ de P sont nuls (car $p > 3$), $\sigma_1 = \sigma_2 = 0$ et p divise $\sum_{k=1}^{p-1} b_k$, puis p^2 divise $2a$ et p^2 divise a car $p \wedge 2 = 1$.

39) a) p divise $(2n)!$, i.e. $(n!)^2 \binom{2n}{n}$; comme p est premier avec $n!$ (les diviseurs premiers de $n!$ sont tous élément de $\mathcal{P}_n$), le théorème de Gauss prouve que p divise $\binom{2n}{n}$.

b) Notons $k = a_{2n} - a_n$ et $\mathcal{P}_{2n} \setminus \mathcal{P}_n = \{p_1, p_2, \ldots, p_k\}$. D'après la question précédente, chaque p_i divise $\binom{2n}{n}$, donc leur produit le divise également (les p_i sont des nombres premiers deux à deux distincts). Comme les p_i sont minorés par n, on en déduit :

$$n^k \leq p_1 p_2 \ldots p_k \leq \binom{2n}{n} \leq \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}.$$

c) Nous avons donc :

$$\forall n \geq 2,\ a_{2n} - a_n \leq \frac{2n \ln 2}{\ln n}$$

soit, en posant $\alpha_k = a_{2^k}$:

$$\forall k \geq 1,\ \alpha_{k+1} - \alpha_k \leq \frac{2^{k+1} \ln 2}{\ln 2^k} = 2\,\frac{2^{k+1}}{k}.$$

En sommant, nous obtenons :

$$\forall k \geq 3,\ \alpha_k \leq \alpha_3 + 2\sum_{i=2}^{k-1} \frac{2^i}{i} \leq \alpha_3 + 2\int_2^k \frac{2^t}{t}\,\mathrm{d}t$$

car la fonction $f :\ t \longmapsto \dfrac{2^t}{t}$ est croissante sur $\left[\frac{1}{\ln 2}, +\infty\right[$, donc sur $[2, +\infty[$. Comme f est positive et non sommable sur $[2, +\infty[$, on sait que $\displaystyle\int_2^x \frac{2^t}{t}\,\mathrm{d}t$ est équivalent à $\displaystyle\int_2^x g(t)\,\mathrm{d}t$ quand x tend vers $+\infty$, quand $f(t) \sim_{+\infty} g(t)$. On a :

$$f(t) = \frac{2^t}{t} \underset{+\infty}{\sim} \frac{2^t}{t} - \frac{2^t}{(\ln 2)\,t^2} = \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{2^t}{(\ln 2)\,t}\right) = g(t)$$

donc

$$\int_2^k \frac{2^t}{t}\,\mathrm{d}t \underset{+\infty}{\sim} \int_2^k g(t)\,\mathrm{d}t = \left[\frac{2^t}{\ln 2\, t}\right] \underset{+\infty}{\sim} \frac{2^k}{(\ln 2)\,k}.$$

On a donc en particulier $\alpha_k = O\left(\frac{2^k}{k}\right)$ au voisinage de $+\infty$: il existe K telle que :

$$\forall k \in \mathbb{N},\ \alpha_k \leq M\frac{2^k}{k}.$$

Pour $n \geq 2$, il existe un unique $k \in \mathbb{N}^*$ tel que $2^{k-1} < n \leq 2^k$. On a donc alors $2^k \leq 2n$ et $k \geq \dfrac{\ln n}{\ln 2}$, d'où

$$a_n \leq \alpha_k \leq M\frac{2^k}{k} \leq 2M \ln 2\,\frac{n}{\ln n}$$

et $C = 2M \ln 2$ convient.

40) a) Si $n = 1$, P a pour unique racine $-\dfrac{a_1}{a_0}$, qui est de partie réelle négative. Supposons que $n \geq 2$ et montrons le résultat par contraposée. Soit $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 0$ et $|z| \geq \dfrac{1 + \sqrt{1+4h}}{2}$. Nous avons :

$$|P(z)| \geq \left|a_n z^n + a_{n-1} z^{n-1}\right| - h\sum_{k=0}^{n-2} |z|^k$$

L'idée consiste à se débarrasser de la somme en la majorant. Comme $|z| \geq \dfrac{1+\sqrt{1+4h}}{2} > 1$ (en traitant séparément le cas trivial $h = 0$), nous allons remplacer la somme divergente par une somme convergente en divisant par $|z|^n$. Nous obtenons :

$$\frac{|P(z)|}{|z|^n} \geq \left|a_n + \frac{a_{n-1}}{z}\right| - h\sum_{k=2}^{n} \frac{1}{|z|^k} > \left|a_n + \frac{a_{n-1}}{z}\right| - h\sum_{k=2}^{+\infty} \frac{1}{|z|^k} = \left|a_n + \frac{a_{n-1}}{z}\right| - \frac{h}{|z|^2 - |z|}$$

C'est le moment d'utiliser la seconde hypothèse : $\mathrm{Re}(z) > 0$. L'astuce consiste à remarquer que le complexe $Z = a_n + \dfrac{a_{n-1}}{z}$ a une partie réelle positive, ce qui donne l'inégalité intéressante :

$$|Z| \geq \mathrm{Re}(Z) = \underbrace{a_n}_{\geq 1} + \underbrace{\frac{a_{n-1}}{|z|^2}\,\mathrm{Re}(z)}_{\geq 0} \geq 1$$

ce qui donne :

$$\frac{|P(z)|}{|z|^n} > 1 - \frac{h}{|z|^2 - |z|} = \frac{|z|^2 - |z| - h}{|z|^2 - |z|} \geq 0$$

car les racines de $X^2 - X - h$ sont $\dfrac{1-\sqrt{1+4h}}{2}$ et $\dfrac{1+\sqrt{1+4h}}{2}$, avec $|z| \geq \dfrac{1+\sqrt{1+4h}}{2}$. Nous avons ainsi montré que $|P(z)| > 0$: z n'est pas racine de P.

b) Soient $Q, R \in \mathbb{Z}[X]$ tels que $P = QR$. Le but est de démontrer que cette décomposition est triviale, i.e. que $Q = \pm 1$ ou $R = \pm 1$ (les éléments inversibles dans $\mathbb{Z}[X]$ sont les polynômes 1 et -1). Nous avons

$$Q(10)R(10) = P(10) = p$$

Comme p est premier et $Q(10), R(10) \in \mathbb{Z}$, nous avons soit $Q(10) = \pm 1$, soit $R(10) = \pm 1$. Par symétrie, supposons que $Q(10) = \pm 1$. Le polynôme Q se factorise sur $\mathbb{C}$:

$$Q = a\prod_{i=1}^{d}(X - \alpha_i)$$

avec $a \in \mathbb{Z}^*$, $d \in \mathbb{N}$ et $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$. Pour $i \in \{1, \ldots, d\}$, α_i est racine de Q, donc également de P. D'après la question a), deux cas sont possibles :

- $\mathrm{Re}(\alpha_i) \leq 0$ et $|10 - \alpha_i| \geq 10$;
- $|\alpha_i| < \dfrac{1+\sqrt{1+4h}}{2} \leq \dfrac{1+\sqrt{37}}{2}$ (car $h \leq 9$).

Dans le premier cas, $|10 - \alpha_i| > 1$ et cette inégalité est également vérifiée dans le second cas :

$$|10 - \alpha_i| \geq 10 - |\alpha_i| > 10 - \frac{1+\sqrt{37}}{2} = \frac{19-\sqrt{37}}{2} > 1.$$

Si r était non nul, nous aurions l'absurdité $1 = |Q(10)| > |a| \geq 1$. On en déduit que $r = 0$, puis $Q = a = \pm 1$ puisque $Q(10) = \pm 1$.

Remarque 1 : la preuve de la question b) se généralise sans problème à la décomposition de p dans une base quelconque.

Remarque 2 : le polynôme est irréductible sur $\mathbb{Z}$ mais aussi sur $\mathbb{Q}$. La preuve est une conséquence élémentaire du résultat :

Pour tout polynôme non nul P à coefficients entiers, on note $c(P)$ le p.g.c.d. des coefficients de P. C'est le contenu de P. Montrez que pour $P, Q \in \mathbb{Z}[X] \setminus \{0\}$, $c(PQ) = c(P)c(Q)$. On montrera d'abord le résultat pour deux polynômes de contenus égaux à 1.

41) a) Pour $n \geq 0$, il existe p^n éléments $P \in \mathcal{P}$ de degré n (on a p choix pour chaque coefficient $a_0, \ldots, a_{n-1}$ et $a_n = 1$ est imposé). En posant $\mathcal{P}_n = \{P \in \mathcal{P},\ d(P) = n\}$, nous avons :

- pour tout n, $\left(|p^{-s\,d(P)}|\right)_{P\in\mathcal{P}_n}$ est finie donc sommable, de somme $p^{(1-\Re(s))\,n}$;
- la famille $\left(p^{(1-\Re(s))\,n}\right)_{n\in\mathbb{N}}$ est sommable (famille géométrique de raison $q = p^{(1-\Re(s))} \in]0,1[$ car $1 - \Re s < 0$).

Le théorème de sommation par paquets assure donc que la famille est sommable. On peut ensuite calculer $\xi(s)$ (toujours en sommant par paquets) :

$$\forall s \in H,\ \xi(s) = \sum_{n=0}^{+\infty} p^n p^{-sn} = \sum_{n=0}^{+\infty} \left(p^{1-s}\right)^n = \frac{1}{1-p^{1-s}}.$$

b) Nous réserve de sommabilité, nous avons :

$$\chi(s)\xi(2s) = \left(\sum_{P\in\mathcal{P}} p^{-2sd(P)}\right)\left(\sum_{D\in\mathcal{D}} p^{-sd(D)}\right) = \sum_{(P,Q)\in\mathcal{P}\times\mathcal{D}} p^{-2sd(P)}p^{-sd(D)} = \sum_{(P,Q)\in\mathcal{P}\times\mathcal{D}} p^{-sd(P^2D)}$$

On montre facilement que $f :\ (P, D) \longmapsto P^2D$ est une bijection de $\mathcal{P} \times \mathcal{D}$ sur $\mathcal{P}$, sa réciproque étant l'application qui à $R = \prod_{i\in I} P_i^{\alpha_i}$ (les P_i sont unitaires, irréductibles et deux à deux distincts et les α_i sont des entiers ≥ 1) associe le couple $(\prod_{i\in I} P_i^{\beta_i}, \prod_{i\in I} P_i^{\gamma_i})$ où $\alpha_i = 2\beta_i + \gamma_i$ est la division euclidienne de α_i par 2.

Nous pouvons donc une nouvelle fois appliquer le théorème de sommations par paquets : comme $s \in H$, la famille $\left(p^{-sd(P^2Q)}\right)_{(P,Q)\in\mathcal{P}\times\mathcal{D}}$ est sommable et :

$$\xi(s) = \sum_{(P,Q)\in\mathcal{P}\times\mathcal{D}} p^{-sd(P^2Q)} = \sum_{P\in\mathcal{P}} p^{-2sd(P)} \underbrace{\left(\sum_{D\in\mathcal{D}} p^{-sd(Q))}\right)}_{=\chi(s)} = \xi(2s)\chi(s).$$

c) Nous avons, en notant a_n le nombre de polynômes normalisés de degré n sans facteur carré :

$$\forall s \in H,\ \chi(s) = \sum_{n=0}^{+\infty} a_n p^{-sn} = \sum_{n=0}^{+\infty} a_n \left(p^{-s}\right)^n$$

Le calcul des a_n va se faire en utilisant un développement en série entière : quand s décrit $]1, +\infty[$, $x = p^{-s}$ décrit $]0, 1[$. Nous allons donc utiliser la relation de la question b) pour obtenir un autre développement de $\chi(s)$. Pour $s \in]1, +\infty[$, toujours en posant $x = p^{-s}$, nous avons :

$$\begin{aligned}
\sum_{n=0}^{+\infty} a_n x^n &= \frac{\xi(s)}{\xi(2s)} \\
&= (1-p^{1-2s}) \sum_{n=0}^{+\infty} p^n p^{-sn} \\
&= (1-px^2) \sum_{n=0}^{+\infty} p^n x^n \\
&= \sum_{n=0}^{+\infty} p^n x^n - \sum_{n=0}^{+\infty} p^{n+1} x^{n+2} \\
&= 1 + px + \sum_{n=2}^{+\infty} (p^n - p^{n-1}) x^n
\end{aligned}$$

Cette égalité étant valable pour $x \in]0, 1[$, elle l'est sur $[0, 1[$ par continuité en 0, ce qui permet d'identifier les deux développements :

$$\forall n \geq 2,\ a_n = p^n - p^{n-1}.$$

On remarquera que cette relation est fausse quand $n = 1$ ($a_1 = p \neq p - 1$).

42) On peut écrire $n = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_k}$ avec $0 \leq e_1 < e_2 < \cdots < e_k$. En notant $Q(X)$ le polynôme $(X-1)^n$ sur le corps $\mathbb{Z}/2\mathbb{Z}$ (les coefficients de Q sont donc les restes modulo 2 des coefficients de P), nous devons montrer que Q a exactement 2^k coefficients non nuls. Il suffit pour cela de remarquer que pour $e \in \mathbb{N}$, $(X-1)^{2^e} = X^{2^e} - 1 = X^{2^e} + 1$ (dans $\mathbb{Z}/2\mathbb{Z}[X]$) (preuve évidente par récurrence sur e), ce qui donne :

$$Q(X) = \prod_{i=1}^{k} (X-1)^{2^{e_i}} = \prod_{i=1}^{k} (X^{2^{e_i}} + 1) = \sum_{J \subset \{1,2,\ldots,k\}} \prod_{i \in J} X^{2^{e_i}} = \sum_{J \subset \{1,2,\ldots,k\}} X^{\sum_{i \in J} 2^{e_i}}.$$

Comme l'application $J \in \mathcal{P}(\{1, 2, \ldots, k\}) \longmapsto \sum_{i \in J} 2^{e_i} \in \mathbb{N}$ est injective (unicité de la décomposition d'un entier en base 2), Q est bien la somme d'exactement 2^k monômes.

43) a) On a, pour $x \geq 1$:

$$\begin{aligned} F(x) &= \sum_{n \leq x} \sum_{\substack{d \in \mathbb{N}^* \\ d \mid n}} \\ &= \sum_{d \in \mathbb{N}^*} \sum_{\substack{n \in \mathbb{N}^* \\ n \leq x \text{ et } d \mid n}} 1 \\ &= \sum_{d \in \mathbb{N}^*} E\left(\frac{x}{d}\right) \end{aligned}$$

En utilisant l'encadrement $y - 1 \leq E(y) \leq y$, on obtient l'encadrement :

$$x \sum_{d=1}^{E(x)} \frac{1}{d} - E(x) = \sum_{\substack{d \in \mathbb{N}^* \\ d \leq x}} \left(\frac{x}{d} - 1\right) \leq F(x) \leq \sum_{\substack{d \in \mathbb{N}^* \\ d \leq x}} \frac{x}{d} = x \sum_{d=1}^{E(x)} \frac{1}{d}$$

Comme $\displaystyle\sum_{d=1}^{E(x)} \frac{1}{d} \sim_{+\infty} \ln E(x) \sim_{+\infty} \ln x$, on obtient $F(x) \sim_{+\infty} x \ln x$.

b) On peut écrire

$$F(x) = \sum_{\substack{d,q \in \mathbb{N}^* \\ dq \leq x}} 1$$

Dans cette somme, les couples (d, q) intervenant vérifient $d \leq \sqrt{x}$ ou $^q \leq \sqrt{x}$, ce qui permet d'écrire :

$$F(x) = \sum_{\substack{d \leq \sqrt{x} \\ dq \leq x}} 1 + \sum_{\substack{q \leq \sqrt{x} \\ dq \leq x}} 1 - \sum_{d,q \leq \sqrt{x}} 1 = 2 \sum_{\substack{p \leq \sqrt{x} \\ dq \leq x}} 1 - \sum_{d,q \leq \sqrt{x}} 1$$

puisque les termes de la dernière somme sont comptés une fois dans chacune des deux premières sommes. Nous obtenons cette fois :

$$F(x) = 2 \sum_{d \leq \sqrt{x}} E\left(\frac{x}{d}\right) - E(\sqrt{x})^2.$$

La même méthode qu'à la question a) donne :

$$F(x) = 2x \sum_{d \leq \sqrt{x}} \frac{1}{d} - x$$

et on conclut en utilisant le développement $\displaystyle\sum_{d=1}^{N} \frac{1}{d} = \ln N + \gamma + O\left(\frac{1}{N}\right)$.