

# EXERCICES CORRIGÉS DE MATHÉMATIQUES

Gregorio José

17 août 2006

### Exercice 1

Soit  $\mathbb{K}$  un corps fini (donc commutatif), montrer que  $(\mathbb{K}^*, \cdot)$  est cyclique.

*preuve n°1 :*

On posera  $\wedge$  pour le P.G.C.D. et  $\vee$  pour le P.P.C.M.

$(\mathbb{K}^*, \cdot)$  est un groupe fini (et commutatif) on peut donc montrer facilement grâce au théorème de Lagrange que pour  $x \in \mathbb{K}^*$  et  $y \in \mathbb{K}^*$  avec  $o(x) = m$ ,  $o(y) = n$  et  $m \wedge n = 1$ , on a :  $o(xy) = m.n = m \vee n$ . (\*)

Il s'agit maintenant de montrer que pour tout  $m \in \mathbb{N}^*$  et tout  $n \in \mathbb{N}^*$  on peut trouver  $m'$  et  $n'$  des entiers naturels tels que :  $m'|m$ ,  $n'|n$ ,  $m' \wedge n' = 1$  et  $m'.n' = m \vee n$ . Posons  $a = (m \wedge n) \wedge \frac{m}{m \wedge n}$ , on peut considérer :  $m' = \frac{m.a}{m \wedge n}$  et  $n' = \frac{n}{a}$ .

Comme  $\mathbb{K}$  est fini, il existe un élément  $z \in \mathbb{K}^*$  d'ordre maximal  $M$ . Donc pour tout  $x \in \mathbb{K}^*$  avec  $o(x) = m \in \mathbb{N}$ , il existe  $k \in \mathbb{N}$ ,  $k|m$  et  $l \in \mathbb{N}$ ,  $l|M$  tels que :  $o(x^k) = m'|m$ ,  $o(z^l) = M'|M$ ,  $m' \wedge M' = 1$  et  $o(x^k.z^l) = m'.M' = m \vee M \leq M$  par définition de  $M$  donc  $m \vee M = M$  et  $m|M$  d'où  $x^M = 1$  pour tout  $x \in \mathbb{K}^*$ .

Or comme  $\mathbb{K}$  est un corps, le nombre de racine de l'équation :  $X^M - 1$  dans  $\mathbb{K}$  est inférieur ou égal à  $M$  (cela se montre par récurrence du fait que si  $a$  est une racine de  $P$  alors  $(X - a)$  divise  $P$  (division euclidienne)) mais comme on a montré que :  $x^M = 1$  pour tout  $x \in \mathbb{K}^*$ , on a donc :  $|\mathbb{K}^*| \leq M$  donc :  $|\mathbb{K}^*| = M = |\langle z \rangle|$ . ■

*preuve n°2 :*

On montre plus directement après avoir montré (\*) que pour tout  $x \in \mathbb{K}^*$  d'ordre  $m$ ,  $m|M$  puis on conclut de la même manière que précédemment. Supposons que  $m \nmid M$ , alors il existe  $p$  un nombre premier,  $\alpha, \beta$  des entiers ( $0 \leq \alpha < \beta$ ) tels que  $M = p^\alpha.q$  et  $m = p^\beta.r$  et  $p \wedge q = p \wedge r = 1$ . On a alors :  $o(x^r) = p^\beta$  et  $o(z^{p^\alpha}) = q$  et d'après (\*) comme  $p^\beta \wedge q = 1$ ,  $o(x^r.z^{p^\alpha}) = p^\beta.q > M$  ce qui est absurde par définition de  $M$  donc  $m|M$  ■

*preuve n°3 :*

On pose  $\varphi$  l'indicatrice d'Euler ( $\varphi(n)$  représente le nombre de nombre entiers inférieurs à  $n$  et premier avec  $n$  ou le nombre de générateurs de  $\mathbb{Z}/n\mathbb{Z}$ ) et pour  $d|n = |\mathbb{K}^*|$ ,  $\zeta(d)$  le nombre d'éléments de  $\mathbb{K}^*$  d'ordre  $d$ . On a :

$$n = \sum_{d|n} \varphi(d)$$

Soit  $x \in \mathbb{K}^*$  d'ordre  $d$ , alors : pour tout  $y \in \langle x \rangle$ ,  $y^d = 1$  et comme  $K^*$  est un corps le polynôme  $X^d - 1$  a au plus  $d$  racines qui sont donc les éléments de  $\langle x \rangle$ . A fortiori les éléments d'ordre  $d$  sont tous dans  $\langle x \rangle$  qui est isomorphe à  $\frac{\mathbb{Z}}{d\mathbb{Z}}$  et qui possède exactement  $\varphi(d)$  générateur (éléments d'ordre  $d$ ). Pour conclure, pour tout entier  $d|n$ ,  $\zeta(d) = 0$  ou  $\varphi(d)$  donc  $\zeta(d) \leq \varphi(d)$  et de plus  $n = \sum_{d|n} \zeta(d) = \sum_{d|n} \varphi(d)$  donc nécessairement, pour tout  $d|n$ ,  $\zeta(d) = \varphi(d)$  et en particulier :  $\zeta(n) = \varphi(n) > 0$ . ■

**Exercice 2**

**Pour toute partie non vide  $S \subset \{1, \dots, n\}$ , on pose :**  
 $\omega(S) = \max\{s; s \in S\} - \min\{s; s \in S\}$ . **Calculer la moyenne**  
 $\Omega$  **des  $\omega(S)$  sur toutes les parties non vides de  $\{1, \dots, n\}$ .**

*solution :*

Le nombre de partie non vide de  $P(\{1, \dots, n\})$  est égal à  $2^n - 1$ , le nombre de partie ayant  $k \in \{1, \dots, n\}$  comme *max* est de  $2^{k-1}$  et le nombre de partie ayant  $k$  comme *min* est de  $2^{n-k}$ . On a donc :

$$\begin{aligned}\Omega &= \frac{1}{2^n - 1} \cdot \left( \sum_{k=0}^n k \cdot 2^{k-1} - \sum_{k=0}^n k \cdot 2^{n-k} \right) \\ \Omega &= \frac{1}{2^n - 1} \cdot \left( \sum_{k=0}^n k \cdot 2^{k-1} - \sum_{i=0}^{n-1} (n-i) \cdot 2^i \right) \\ \Omega &= \frac{1}{2^n - 1} \cdot \left( \sum_{k=0}^n k \cdot 2^{k-1} - n \cdot \sum_{i=0}^{n-1} 2^i + 2 \cdot \sum_{i=0}^{n-1} i \cdot 2^{i-1} \right) \\ \Omega &= \frac{1}{2^n - 1} \cdot \left( 3 \cdot \sum_{k=0}^{n-1} k \cdot 2^{k-1} + n \cdot 2^{n-1} - n \cdot \sum_{k=0}^{n-1} 2^k \right)\end{aligned}$$

Il reste à voir maintenant que  $\sum_{k=0}^{n-1} 2^k = 2^n - 1$  (comme somme partiel d'une série géométrique) et  $\sum_{k=0}^{n-1} k \cdot 2^{k-1} = 2^{n-1}(n-2) + 1$  (comme somme "dérivée" de la précédente). Donc :  $\Omega = \frac{1}{2^n - 1} \cdot (3(2^{n-1}(n-2) + 1) + n(1 - 2^{n-1}))$  d'où après simplification :

$$\Omega = \frac{2^n(n-3) + n + 3}{2^n - 1} \quad \blacksquare$$

**Exercice 3**

**Pour tout  $(n, k) \in \mathbb{N}^2$ , on pose  $S_k(n) = \sum_{i=1}^n i^k$ . Montrer que  $S_k(n)$  est un polynôme en  $n$  de degré  $k+1$  et de coefficient dominant  $\frac{1}{k+1}$ .**

*solution :*

Il suffit de remarquer que :  $(n+1)^k - n^k = \sum_{i=0}^{k-1} C_k^i n^i$ . On peut réitérer, et on a :

$$(n+1)^k - n^k = \sum_{i=0}^{k-1} C_k^i n^i$$

$$\begin{array}{ccccccc}
 n^k - (n-1)^k & = & \sum_{i=0}^{k-1} & C_k^i & (n-1)^i & & \\
 \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} \\
 2^k - 1^k & = & \sum_{i=0}^{k-1} & C_k^i & 1^i & & 
 \end{array}$$

En additionnant membre à membre, on remarque que les termes dans le membre de gauche se télescopent et on obtient :

$$(n+1)^k - 1 = \sum_{i=0}^{k-1} C_k^i S_i(n)$$

Il ne reste alors plus qu'à établir le résultat demandé par simple récurrence. ■

#### Exercice 4

Pour tout entier  $n \in \mathbb{N}$ , on pose :

$$A_n = \begin{cases} 2.\mathbb{N} & \text{si } n \text{ est pair} \\ 3.\mathbb{N} & \text{sinon} \end{cases}$$

A-t-on

$$\bigcup_{n=0}^{\infty} \bigcap_{k=0}^{\infty} A_{n+k} = \bigcap_{n=0}^{\infty} \bigcup_{k=0}^{\infty} A_{n+k} \quad ?$$

*solution :*

On peut récrire l'égalité :

$$\bigcup_{n=0}^{\infty} \bigcap_{k=n}^{\infty} A_k = \bigcap_{n=0}^{\infty} \bigcup_{k=n}^{\infty} A_k$$

On reconnaît (ou pas) à gauche la limite Inf des ensembles  $A_n$  (les éléments qui appartiennent à tous les  $A_n$  à partir d'un certain rang) et à droite la limite Sup (les éléments qui appartiennent à une infinité de  $A_n$ ). On a, après vérification :

$$\liminf A_n = 6.\mathbb{N} \subsetneq 2.\mathbb{N} \cup 3.\mathbb{N} = \limsup A_n \quad \blacksquare$$

#### Exercice 5

Soit  $G$  un groupe fini et  $H$  un sous groupe de  $G$ . Montrer que :

$$\bigcup_{x \in G} xHx^{-1} \subsetneq G$$

Donner un contre-exemple dans le cas où  $G$  est infini.

*preuve :*

On remarque que pour  $(x, y) \in G^2$ ,  $xH = yH$  (même classe à gauche modulo  $H$ ) implique  $xHx^{-1} = yHy^{-1}$  en effet, si  $h \in H$ , il existe  $h' \in H$  tel que  $xh = yh'$  on a  $xh^{-1} = yh'h^{-1}h'^{-1}$  et donc :  $xhx^{-1} = yh'x^{-1} = y(xh'^{-1})^{-1} = y(yh'h^{-1}h'^{-1})^{-1} = yh'hh'^{-1}y^{-1} \in yHy^{-1}$ . On a alors égalité par égalité des cardinaux.

On peut poser  $n = |G|$  et  $k = |H|$ . D'après ce que l'on vient de dire, il existe  $(x_1, \dots, x_{\frac{n}{k}})$   $\frac{n}{k}$  représentants des classes à gauche modulo  $H$  tels que  $\bigcup_{x \in G} xHx^{-1} = \bigcup_{1 \leq i \leq \frac{n}{k}} x_i H x_i^{-1}$ . On note au passage que pour tout  $x \in G$ ,  $|xHx^{-1}| = |H| = k$ . Si les ensembles  $x_i H x_i^{-1}$  sont deux à deux totalement disjoints alors on peut majorer le cardinal de leur réunion par  $\frac{n}{k} \cdot k = n$  mais n'étant pas disjoints (ils contiennent tous le neutre du groupe) leur réunion est nécessairement strictement inférieure à  $n = |G|$ . ■

Comme contre-exemple on peut prendre  $G = GL_n(\mathbb{C})$  et  $H$  le sous groupe des matrices triangulaires supérieures de  $G$ . Comme tout polynôme est scindé dans  $\mathbb{C}$ , tout élément de  $G$  est trigonalisable. Donc :  $(\forall y \in G)(\exists x \in G) x^{-1}yx = t \in H$  et on a bien  $y \in \bigcup_{x \in G} xHx^{-1}$ , pour tout  $y \in G$ . ■

### Exercice 6 :

**Montrer que pour tout  $m \in \mathbb{N}$  :**

$$e^{-m} \sum_{k=0}^{\infty} \frac{m^k k^m}{k!}$$

**est un entier.**

*preuve :*

On pose :  $S_m^i = e^{-m} \sum_{k=0}^{\infty} \frac{m^k k^i}{k!}$

On a alors :

$$S_m^{i+1} = e^{-m} \sum_{k=1}^{\infty} \frac{m^k k^{i+1}}{k!}$$

$$S_m^{i+1} = e^{-m} \sum_{k=1}^{\infty} \frac{m^k k^i}{(k-1)!}$$

$$S_m^{i+1} = e^{-m} \sum_{k=0}^{\infty} \frac{m^{k+1} (k+1)^i}{k!}$$

$$S_m^{i+1} = m e^{-m} \sum_{k=0}^{\infty} \frac{m^k (k+1)^i}{k!}$$

$$S_m^{i+1} = m e^{-m} \sum_{k=0}^{\infty} \frac{m^k \sum_{j=0}^i C_i^j k^j}{k!}$$

Tous les termes sont positifs, on peut échanger les deux signes sommes :

$$S_m^{i+1} = m e^{-m} \sum_{j=0}^i C_i^j \sum_{k=0}^{\infty} \frac{m^k k^j}{k!} \quad \text{donc} \quad S_m^{i+1} = m \sum_{j=0}^i C_i^j S_m^j$$

Puisque :  $S_m^0 = 1 \in \mathbb{N}$  on a par une récurrence simple et grâce à la formule précédente :  $S_m^j \in \mathbb{N}$  et ceci pour tout entier  $j \in \mathbb{N}$  donc en particulier :  $S_m^m \in \mathbb{N}$

On peut calculer :  $\blacksquare$

$$S_m^0 = 1; S_m^1 = m; S_m^2 = m(m+1); S_m^3 = m+3m^2+m^3; S_m^4 = m^4+6m^3+7m^2+m$$

Question : peut-on directement avoir en fonction de  $m$  et  $i$  la valeur de  $S_m^i$  ?

### Exercice 7 :

**(Oral des mines)**

Soit  $k \in \mathbb{N}, k \geq 2$  et  $u(n) = n + E((n + n^{\frac{1}{k}})^{\frac{1}{k}})$ , où  $E(x)$  désigne la partie entière de  $x$ . Déterminer  $u(\mathbb{N})$ .

*preuve :*

On peut tout d'abord facilement remarquer que  $(U(n))_n$  est strictement croissante ensuite le développement du binôme de Newton donne l'inégalité suivante :  $n^k + n < (n+1)^k$  et grâce à la croissance de la fonction  $x \rightarrow x^{\frac{1}{k}}$  on a  $n \leq (n^k + n)^{\frac{1}{k}} < n+1$  donc  $U(n^k) = n^k + n$ .

Regardons maintenant l'ensemble  $\{U(i); n^k \leq i \leq (n+1)^k\}$ , comme la suite est strictement croissante il contient  $(n+1)^k - n^k + 1$  éléments. Or entre  $U(n^k) = n^k + n$  et  $U((n+1)^k) = (n+1)^k + (n+1)$  il y a  $(n+1)^k - n^k + 2$  éléments ce qui veut dire que  $U(n)$  prend toutes les valeurs entières de l'intervalle  $[n^k + n; (n+1)^k + (n+1)]$  sauf une. Montrons que  $U(n)$  ne prend pas les valeurs  $n^k$  ( $n \in \mathbb{N}$ ). Si c'est bien le cas nous devrions avoir :

$$U(n^k) = n^k + n$$

$$U(n^k - 1) = n^k + n - 1$$

$$\text{" " "}$$

$$U(n^k - (n-1)) = n^k + 1$$

$$U(n^k - n) = n^k - 1$$

Cette dernière étape est assez simple puisque :

$$n^k - n < n^k \quad \text{donc}$$

$$\begin{aligned}
& (n^k - n)^{\frac{1}{k}} < n \quad \text{et} \\
& n^k - n + (n^k - n)^{\frac{1}{k}} < n^k \\
& E((n^k - n + (n^k - n)^{\frac{1}{k}})^{\frac{1}{k}}) < n \quad \text{ce qui revient} \\
& U(n^k - n) < n^k
\end{aligned}$$

On peut montrer de la même manière que  $U(n^k - (n-1)) > n^k$  ce qui veut bien dire que  $n^k$  est l'unique valeur entière qui n'est pas prise par  $U$  dans l'intervalle  $[(n-1)^k + (n-1); n^k + n]$  et donc pour conclure :  $U(\mathbb{N}) = \mathbb{N} \setminus \{n^k; n \in \mathbb{N}\}$ . ■

**Exercice 8 :**

**Trouver  $D_n$  le cardinal de l'ensemble des permutations de  $S_n$  qui ne fixe aucun des éléments de  $(1, \dots, n)$  puis déterminer  $\lim_{n \rightarrow \infty} \frac{D_n}{n!}$ .**

*Solution 1 :*

Il y a exactement  $C_n^k D_{n-k}$  permutations de  $S_n$  qui fixent  $k$  points. En remarquant que  $D_n$  représente toutes les permutations de  $S_n$  excepté toutes celles qui fixent  $k$  points (avec  $1 \leq k \leq n$ ) et en posant  $D_0 = 1$ , on a la formule (à vérifier) :  $n! = \sum_{k=0}^n C_n^k D_{n-k}$  et puisque  $C_n^k = C_n^{n-k}$  on peut écrire :

$$n! = \sum_{k=0}^n C_n^k D_k \quad (*)$$

Nous allons tout d'abord démontrer que pour :  $0 \leq k < p$   
 $\sum_{i=k}^p (-1)^i C_p^i C_i^k = 0$ . En effet, on a :

$$\begin{aligned}
\sum_{i=k}^p (-1)^i C_p^i C_i^k &= \sum_{i=k}^p (-1)^i \frac{p!}{i!(p-i)!} \frac{i!}{k!(i-k)!} \\
&= \sum_{i=k}^p (-1)^i \frac{p!}{k!(p-i)!(i-k)!} \\
&= \sum_{i=k}^p (-1)^i \frac{p!}{k!(p-k)!(p-i)!(i-k)!} \\
&= \sum_{i=k}^p (-1)^i C_p^k C_{p-k}^{i-k} \\
&= C_p^k \sum_{j=0}^{p-k} (-1)^{j+k} C_{p-k}^j = (-1)^k C_p^k (1-1)^{p-k} = 0
\end{aligned}$$

On en déduit aussi que :

$$\sum_{k=i}^n (-1)^k C_{n+1}^k C_i^k = -(-1)^{n+1} C_{n+1}^i \quad (**)$$

Nous pouvons maintenant montrer par récurrence et grâce à (\*) et (\*\*) la formule suivante :

$$D_n = (-1)^n \sum_{k=0}^n (-1)^k k! C_n^k$$

$$D_{n+1} = (n+1)! - \sum_{k=0}^n C_{n+1}^k D_k \quad (\text{d'après } (*))$$

$$D_{n+1} = (n+1)! - \sum_{k=0}^n C_{n+1}^k (-1)^k \sum_{i=0}^k (-1)^i i! C_k^i \quad (\text{récurrence})$$

$$D_{n+1} = (n+1)! - \sum_{i=0}^n (-1)^i i! \sum_{k=i}^n (-1)^k C_{n+1}^k C_k^i \quad (\text{interversion})$$

$$D_{n+1} = (n+1)! - \sum_{i=0}^n (-1)^i i! (-(-1)^{n+1} C_{n+1}^i) \quad (\text{d'après } (**))$$

$$D_{n+1} = (-1)^{n+1} \sum_{i=0}^{n+1} (-1)^i i! C_{n+1}^i \quad \blacksquare$$

Il est maintenant très simple de vérifier que  $\frac{D_n}{n!} = \sum_{k=0}^n \frac{(-1)^k}{k!} \rightarrow e^{-1}$ .

Remarque 1 : si  $n$  personnes entrent dans une pièce, déposent leur chapeau en entrant et en reprennent un au hasard en sortant alors la probabilité pour qu'aucun ne reprenne son chapeau tend vers  $e^{-1}$ .

Remarque 2 : On peut voir facilement que  $D_n = nD_{n-1} + (-1)^n$  il est curieux qu'une récurrence aussi simple ne soit pas évidente dès le départ.

Remarque 3 :  $D_n$  est l'entier le plus proche de  $\frac{n!}{e}$ . On a même  $D_n = E(\frac{n!}{e} + \frac{1}{2})$ .

Solution 2 :

On utilise la formule du crible de Poincaré (qui se démontre par récurrence), soit  $E$  un ensemble et  $A_{1 \leq i \leq n}$ ,  $n$  parties de  $E$ , alors :

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n \left( (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| \right).$$

Si on pose  $A_i$  l'ensemble des permutations de  $\sigma_n$  qui fixent  $i$  alors :

$$D_n = |A_1^c \cap A_2^c \cap \dots \cap A_n^c| = n! - \left| \bigcup_{i=1}^n A_i \right|$$

Or, avec la formule du crible de Poincaré il ne nous reste plus qu'à calculer :  $\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|$ . Une permutation qui laisse invariant  $i_1, \dots, i_k$  agit sur les  $(n-k)$  autres points comme  $\sigma_{n-k}$ , donc :  $|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = (n-k)!$  et donc :

$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = C_n^k (n-k)!$  et pour finir :  
 $D_n = n! + \sum_{k=1}^n (-1)^k C_n^k (n-k)!$  qui peut aussi s'écrire :  $D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$  ■

*Solution 3 :*

On trouve :  $n! = \sum_{k=0}^n C_n^k D_k$  autrement dit :  $\sum_{k=0}^n \frac{D_k}{k!(n-k)!} = 1$  puis on utilise les séries  $f(z) = \sum_{n \geq 0} \frac{D_n z^n}{n!}$  et  $g(z) = e^z$  dont les rayons de convergences sont  $> 0$ .

Leur produit est égal à :  $\sum_{n \geq 0} a_n z^n$  où  $a_n = \sum_{k=0}^n \frac{D_k}{k!(n-k)!} = 1$ , donc  $f(z)g(z) = \sum_{n \geq 0} z^n = \frac{1}{1-z}$  (pour  $|z| < 1$ ). On trouve alors  $f(z) = \frac{e^{-z}}{1-z}$ , puis en développant

le produit et en identifiant les termes, on a enfin :  $D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$  ■

**Exercice 9 :**

**(Oral Polytechnique)**

**On pose  $A_1 = \emptyset$  et  $B_1 = \{0\}$  et on définit pour  $n \geq 1$  :  
 $A_{n+1} = B_n + 1$  et  $B_{n+1} = A_n \triangle B_n$ . Montrer que si  $n$  est  
une puissance de 2 alors  $B_n = \{0\}$ .**

*Solution 1 :*

On pose  $P_n = \sum_{k \in A_n} X^k$  et  $Q_n = \sum_{k \in B_n} X^k$  et on raisonne modulo 2.

On trouve :

$$Q_{n+1} = \sum_{k \in B_{n+1}} X^k$$

$$Q_{n+1} = \sum_{k \in A_n \triangle B_n} X^k$$

$$Q_{n+1} = \sum_{k \in A_n} X^k + \sum_{k \in B_n} X^k - 2 \cdot \sum_{k \in A_n \cap B_n} X^k$$

$$Q_{n+1} = P_n + Q_n \pmod{2} \quad (*)$$

et :

$$P_{n+1} = \sum_{k \in B_{n+1}} X^k$$

$$P_{n+1} = \sum_{k \in B_n} X^{k+1}$$

$$P_{n+1} = X \cdot Q_n \quad (**)$$

On en déduit, grâce à (\*) et (\*\*) les relations :

$$Q_{n+1} = Q_n + X \cdot Q_{n-1}, \quad \text{avec } Q_1 = Q_2 = 1 \quad (***)$$

$$P_{n+1} = P_n + X.P_{n-1}, \quad \text{avec } P_1 = 0; P_2 = X$$

On cherche ensuite pour tout entier  $k$  des polynômes  $T_k$  et  $S_k$  tels que :

$$Q_{n+k} = T_k.Q_n + S_k.Q_{n-1}.$$

Pour  $k = 1$ , on a  $T_1 = 1 = Q_2$  et  $S_1 = X = P_2$  et ensuite on en déduit grâce à (\*\*\*) que  $T_k$  et  $S_k$  doivent vérifier :  $T_{k+1} = T_k + X.T_{k-1}$  et  $S_{k+1} = S_k + X.S_{k-1}$  et avec les conditions initiales on a :  $T_k = Q_{k+1}$  et  $S_k = P_{k+1}$ .

Donc :  $Q_{n+k} = Q_{k+1}.Q_n + P_{k+1}.Q_{n-1}$  ou encore avec  $k = n$  :

$$Q_{2n} = Q_{n+1}.Q_n + P_{n+1}.Q_{n-1} \text{ et grâce à (**) et (***) : } Q_{2n} = Q_n^2 \text{ et pour finir : } Q_{2^n} = Q_1^{2^n} = 1.$$

Réciproquement on montre par une récurrence simple et grâce à (\*\*\*) que pour tout entier  $n \geq 1$ ,  $Q_n = 1 + n.X + \dots$  et donc  $Q_n = 1$  implique  $2|n$ . Supposons que pour  $k \in \mathbb{N}$ ,  $2^k|n$  et  $2^k \neq n$  (ce qui est vrai pour  $k = 0$  et  $n > 1$ ) et  $Q_n = 1$  alors on a  $p \in \mathbb{N}$  tel que :  $1 = Q_n = Q_{2^k.p} = Q_p^{2^k}$  et donc  $Q_p = 1$  et d'après ce que l'on a dit  $2|p$  et donc  $2^{k+1}|n$ . Finalement,  $n$  est une puissance de 2. ■

*Solution 2 :*

On pouvait aussi considérer un corps contenant  $Z/2Z[X]$  et dans lequel l'équation associée à la suite  $Q_{n+1} = Q_n + X.Q_{n-1}$ ,  $(r^2 - r - X)$  admet deux solutions  $\alpha_1$  et  $\alpha_2$ . On aurait alors avec les conditions initiales et en posant  $Q_0 = 0$  pour que la suite soit indexée dans  $\mathbb{N}$ ,  $Q_n = \alpha_1^n + \alpha_2^n$ . D'autre part  $\alpha_i^2 = \alpha_i + X$  et  $\alpha_i^4 = \alpha_i^2 + X^2$  (car dans  $Z/2Z$  les doubles produits sont nuls). On montre alors très facilement par récurrence que  $\alpha_i^{2^n} = \alpha_i + X + X^2 + \dots + X^{2^{n-1}}$  et donc  $Q_{2^n} = \alpha_1^{2^n} + \alpha_2^{2^n} = \alpha_1 + \alpha_2 = 1$ . ■

(On remarquera qu'on ne montre pas la réciproque avec cette méthode)

**Exercice 10 :**

**(Oral CCP)**

**Trouver toutes les fonctions  $f \in C[0;1]$  dans  $\mathbb{R}^+$  telle que**

$$\text{pour tout } x \in [0;1], f(x) = \sum_{n=1}^{\infty} \frac{f(x^n)}{2^n} (*).$$

*solution :*

Nous allons montrer que les seules fonctions à vérifier cette propriété sont les constantes.  $f$  est continue sur un compact  $[0;1]$  elle atteint donc sa borne inférieure  $m$  et sa borne supérieure  $M$ . Si  $f$  n'est pas constante ( $m \neq M$ ), on peut remplacer  $f$  par  $g = \frac{f-m}{M-m}$  qui vérifie aussi (\*), et de plus  $0 \leq g \leq 1$ . Supposons qu'il existe  $(\alpha, \beta) \in [0;1]^2$  tel que  $g(\alpha) = 0$  et  $g(\beta) = 1$ . Alors  $g(\alpha) = \sum_{n=1}^{\infty} \frac{g(\alpha^n)}{2^n} = 0$  et puisque  $g \geq 0$  on a :  $g(\alpha^n) = 0$  pour tout entier  $n \geq 1$  et donc par continuité  $g(0) = \lim_{n \rightarrow \infty} g(\alpha^n) = 0$ . En appliquant le même raisonnement avec  $\beta$  et en remarquant que  $\sum_{n=1}^{\infty} 2^{-n} = 1$  et que  $g \leq 1$ , on a pour tout entier  $n \geq 1$  :  $g(\beta^n) = 1$  et donc  $g(0) = \lim_{n \rightarrow \infty} g(\beta^n) = 1$ , ce qui est absurde, donc  $m = M$  et  $f$  est constante.

Dans le cas où  $\alpha = 1$  ou  $\beta = 1$ , il suffit de regarder le *min* et le *max* de  $g$  sur  $[0;x]$  avec  $x \in ]0;1[$  et d'en déduire que  $f$  est constante sur  $[0;x]$  pour tout  $x \in ]0;1[$  et par continuité que  $f$  est constante sur  $[0;1]$ . ■

**Exercice 11 :**

Calculer  $\sum_{k=0}^{E(\frac{n}{p})} C_n^{pk}$  où  $n, p$  et  $k$  sont des entiers et  $E$  désigne la fonction partie entière.

*solution :*

L'astuce consiste à calculer une combinaison linéaire de  $(1+x)^n$  où les  $x$  sont des racines  $p^{ieme}$  de l'unité.

$$\sum_{k=0}^{p-1} (1 + e^{\frac{ik2\pi}{p}})^n = \sum_{k=0}^{p-1} \sum_{l=0}^n C_n^l e^{\frac{ik2\pi l}{p}} = \sum_{l=0}^n C_n^l \sum_{k=0}^{p-1} e^{\frac{ik2\pi l}{p}}$$

or la dernière égalité est une somme finie de termes d'une suite géométrique et vaut (après un petit calcul)  $p$  si  $l \equiv 0 \pmod{p}$  et 0 sinon, donc :

$$\sum_{k=0}^{p-1} (1 + e^{\frac{ik2\pi}{p}})^n = p \sum_{k=0}^{E(\frac{n}{p})} C_n^{kp}.$$

Il ne reste plus qu'à calculer :

$$\begin{aligned} \sum_{k=0}^{E(\frac{n}{p})} C_n^{pk} &= \frac{1}{p} \sum_{k=0}^{p-1} (1 + e^{\frac{ik2\pi}{p}})^n \\ &= \frac{1}{p} \sum_{k=0}^{p-1} e^{\frac{ikn\pi}{p}} (e^{-\frac{ik\pi}{p}} + e^{\frac{ik\pi}{p}})^n \\ &= \frac{1}{p} \sum_{k=0}^{p-1} e^{\frac{ikn\pi}{p}} 2^n \cos^n\left(\frac{k\pi}{p}\right) \end{aligned}$$

Et puisque ce nombre est un réel pur, on a :

$$\sum_{k=0}^{E(\frac{n}{p})} C_n^{pk} = \frac{2^n}{p} \sum_{k=0}^{p-1} \cos\left(\frac{kn\pi}{p}\right) \cos^n\left(\frac{k\pi}{p}\right) \quad \blacksquare$$

**Exercice 12 :**

Montrer avec un contre-exemple sur les sous groupes de  $GL(2, \mathbb{R})$  qu'un sous groupe d'un groupe de type fini n'est pas nécessairement de type fini. (Contrairement au cas où le groupe est abélien)

*solution :*

En posant :  $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  et  $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  et  $G$  le groupe engendré par  $A$

et  $B$ . On va montrer que l'ensemble formé par les matrices du type :  $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$

appartenant à  $G$  est un sous groupe  $H$  de  $G$  qui n'est pas de type fini.

Caractérisons tout d'abord  $G$ . Après réflexions, on peut voir où pas que  $G$  est formé par l'ensemble des matrices du type :  $\begin{pmatrix} 2^n & m2^p \\ 0 & 1 \end{pmatrix}$ , où  $(m, n, p) \in \mathbb{Z}^3$ .

Nous allons démontrer que cette ensemble que l'on notera  $F$  est un groupe :

$$\begin{pmatrix} 2^n & m2^p \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2^{-n} & -2^{-n}m2^p \\ 0 & 1 \end{pmatrix} \text{ stabilité par passage à l'inverse.}$$

$$\begin{pmatrix} 2^n & m2^p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^{n'} & m'2^{p'} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2^{n+n'} & m'2^{p'+n} + m2^p \\ 0 & 1 \end{pmatrix} \text{ stabilité par composition.}$$

$F$  est donc un sous groupe de  $GL(2, \mathbb{R})$  qui contient  $G$  puisqu'il contient  $A$  et  $B$ .

De plus en remarquant que pour tout  $(p, m) \in \mathbb{Z}^2$ ,  $A^p = \begin{pmatrix} 2^p & 0 \\ 0 & 1 \end{pmatrix}$  et  $B^m =$

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \text{ on a : } A^p B^m A^{-p} = \begin{pmatrix} 1 & m2^p \\ 0 & 1 \end{pmatrix}, \text{ et donc pour } n \in \mathbb{Z} :$$

$$A^p B^m A^{-p} A^n = \begin{pmatrix} 2^n & m2^p \\ 0 & 1 \end{pmatrix}, \text{ ce qui prouve que } G \text{ contient } F \text{ et donc } F = G.$$

L'ensemble  $H$  formé par les matrices du type :  $\begin{pmatrix} 1 & m2^p \\ 0 & 1 \end{pmatrix}$  est évidemment un sous groupe de  $G$ , il ne reste plus qu'à montrer qu'il n'est pas de type fini. Étant en isomorphe au sous groupe additif de  $\mathbb{R}$  des réels de la forme  $m2^p$ , on peut montrer que ce sous groupe n'est pas de type fini. Si on considère  $(m_1 2^{p_1}, \dots, m_q 2^{p_q})$  une partie fini de ce sous groupe alors il est clair que  $2^{\beta-1}$  ( $\beta = \min_{1 \leq i \leq q} p_i$ ) appartient à ce sous groupe mais pas au groupe engendré par  $(m_1 2^{p_1}, \dots, m_q 2^{p_q})$ . ■

*Autre exemple de tels groupes :*

Dans le groupe de permutations  $\mathfrak{S}(\mathbb{Z})$ , on considère le sous-groupe  $G$  engendré par la transposition  $\tau_{0,1}$  et le décalage  $\sigma : k \mapsto k + 1$ . Par des arguments standards, on voit que  $G$  contient toutes les transpositions de  $\mathbb{Z}$ . Le groupe  $H$  des permutations de  $\mathbb{Z}$  à support fini est donc un sous-groupe de  $G$ . Bien entendu,  $H$  n'est pas de type fini. ■

### Exercice 13 :

**Montrer par récurrence que  $SL(2, \mathbb{Z})$  est engendré par**

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

*solution :*

On va montrer par récurrence sur  $n \in \mathbb{N}$  que que les matrices de  $SL(2, \mathbb{Z})$  du type :  $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$  avec  $|b| \leq n$  sont dans le groupe engendré par  $\{S, T\}$ .

Pour  $n = 0$ , puisque  $\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \in SL(2, \mathbb{Z})$ , il suffit de regarder les matrices qui

s'écrivent comme  $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$  ou  $\begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}$  avec  $c \in \mathbb{Z}$ .

Or il est très facile de remarquer (avec une simple récurrence) que  $T^c = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$

et aussi que  $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$  donc que  $S^2 T^c = \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}$ . La propriété est donc vraie au rang  $n = 0$ , supposons la vraie au rang  $n$  et montrons qu'elle l'est toujours au rang suivant :

Soit  $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in SL(2, \mathbb{Z})$  tel que  $|b| \leq n + 1$ . Le cas  $b = 0$  a déjà été vu, on peut donc supposer  $b \neq 0$ .

Considérons alors  $ST^{-k}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} -b & -d \\ a - kb & c - kd \end{pmatrix}$ .

En choisissant  $k$  comme l'entier le plus proche de  $\frac{a}{b}$  ( $|\frac{a}{b} - k| \leq \frac{1}{2}$ ), on a  $|a - kb| \leq \frac{|b|}{2} < |b| \leq n + 1$  donc  $ST^{-k}M$  appartient au groupe engendré par  $\{S, T\}$  et à fortiori  $M$  aussi. ■

#### Exercice 14 :

**Soit  $G$  un groupe fini d'ordre  $n$  tel que  $n$  et  $\varphi(n)$  sont premiers entre eux (où  $\varphi$  est l'indicatrice d'Euler).  
Montrer que  $G$  est cyclique.**

*solution :*

On peut déjà remarquer que la propriété est connue dans le cas particulier où  $n$  est un nombre premier. D'autre part si  $p_1^{\alpha_1} \dots p_r^{\alpha_r}$  représente la décomposition en facteur premier de  $n$  alors  $\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \dots (p_r - 1)p_r^{\alpha_r - 1}$ . Il est alors aisé de remarquer que si  $n$  et  $\varphi(n)$  sont premiers entre eux alors nécessairement  $\alpha_i = 1$  pour tout  $i$  et  $n = p_1 \dots p_r$  et donc pour tout sous groupe  $H$  strict de  $G$ ,  $|H|$  et  $\varphi(|H|)$  sont aussi premiers entre eux.

*Lemme : Si  $G$  est un groupe fini dont tous les sous groupes stricts sont abéliens alors  $G$  n'est pas simple (possède un sous groupe distingué).*

Supposons le lemme démontré et démontrons la propriété par récurrence. Elle est évidemment vraie pour  $n = 1$ , supposons la vraie au rang  $n$  et soit  $G$  un groupe d'ordre inférieur à  $n + 1$  avec  $\varphi(n + 1)$  premier avec  $n + 1$  (la décomposition en facteur premier de  $n + 1$  ne possède donc que des nombres premiers distincts). Tous les sous groupes stricts de  $G$  sont d'ordre inférieur ou égal à  $n$ , leur cardinal vérifie donc l'hypothèse de récurrence, ils sont donc cycliques et en particulier abéliens donc d'après le lemme  $G$  n'est pas simple. Il existe alors  $H$  un sous groupe distingué strict de  $G$ .  $H$  étant distingué dans  $G$ , il est stable par automorphisme intérieur (pour  $g \in G$  et  $h \in H$ ,  $\sigma_g(h) = ghg^{-1} \in H$ ) et l'application  $\phi : g \mapsto \sigma_g$  est un homomorphisme de  $G$  dans  $Aut(H)$ . Son image  $\phi(G)$  a un cardinal qui divise donc à la fois  $|Aut(H)| = \varphi(|H|)$  et  $|G|$  mais  $|G|$  et  $\varphi(|G|)$  sont premiers entre eux et  $\varphi(|H|)$  divise  $\varphi(|G|)$  donc  $\varphi(|H|)$  et  $|G|$  sont premiers entre eux et  $\phi(G) = Id_H$  donc  $H \subset Z(G)$ . L'hypothèse de récurrence s'applique aussi au groupe quotient  $G/H$  qui est donc cyclique or si  $H \subset Z(G)$  et  $G/H$  est cyclique alors  $G$  est abélien donc cyclique.

**Exercice 15 :**

**Montrer que  $\mathbb{Z}[X]$  n'est pas principal. Soit  $\mathbb{A}$  un anneau commutatif unitaire et intègre, montrer que  $\mathbb{A}[X]$  est principal si et seulement si  $\mathbb{A}$  est un corps.**

*solution :*

On notera que l'on peut aussi utiliser la deuxième question pour répondre à la première.

Considérons  $e_0$  l'homomorphisme évaluation en  $\bar{0}$  de  $\mathbb{Z}[X]$  dans  $\mathbb{Z}/2\mathbb{Z}$  qui à  $P \in \mathbb{Z}[X]$  associe  $e_0(P) = P(\bar{0})$ . D'après le cours  $e_0^{-1}(\bar{0})$  est un idéal de  $\mathbb{Z}[X]$  (c'est en fait l'idéal formé par les polynômes dont le terme constant est pair). Si  $\mathbb{Z}[X]$  était principal  $e_0^{-1}(\bar{0})$  serait engendré par un polynôme  $P$  et puisque le polynôme constant égal à 2 appartient à  $e_0^{-1}(\bar{0})$   $P$  divise 2 donc  $P = (2)$  or on voit clairement que, par exemple,  $X \in e_0^{-1}(\bar{0})$  et  $X \notin (2)$ . ■

Soient  $\mathbb{A}$  un corps,  $I$  un idéal de  $\mathbb{A}[X]$  et  $N = \{d \in \mathbb{N}; (\exists P \in I^*)(\deg(P) = d)\}$ .  $N$  est une partie de  $\mathbb{N}$  et possède donc un plus petit élément  $n$  et il existe  $B \in I^*$  normalisé tel que  $\deg(B) = n$ , autrement dit  $B$  est un polynôme de degré minimum dans  $I^*$ . Soit  $A \in I$ , la division euclidienne dans  $\mathbb{A}[X]$  nous assure l'existence unique d'un couple  $(Q, R)$  avec  $\deg(R) < n$  tels que  $A = BQ + R$ . Donc  $R \in I$  et par définition de  $N$ ,  $R = 0$  d'où  $I = (B)$ .

Réciproquement, si  $\mathbb{A}[X]$  est principal et  $a \in \mathbb{A}^*$  alors il existe  $P \in \mathbb{A}[X]$  tel que  $(P) = (a) + (X)$  donc  $P$  divise le polynôme constant  $a$  et est donc lui-même constant,  $P = p \in \mathbb{A}^*$ , et  $p$  divise  $X$  et donc nécessairement  $p$  est inversible dans  $\mathbb{A}$ . De l'égalité  $(P) = (a) + (X)$ , on peut déduire l'existence de deux polynômes  $Q_1$  et  $Q_2$  tels que  $p = a.Q_1 + X.Q_2$  où l'on a forcément  $Q_2 = 0$  et  $Q_1 = b \in \mathbb{A}$  et donc  $p = ab$  ou encore  $abp^{-1} = 1$  et  $a$  est inversible. ■

**Exercice 16 :**

**On pose  $F_{m,\theta} = X^{2m} - 2\cos(m\theta)X^m + 1$ . Montrer que pour tout  $m \in \mathbb{N}^*$ ,  $F_{1,\theta}$  divise  $F_{m,\theta}$  dans  $\mathbb{C}[X]$ . Trouver le quotient de  $F_{m,\theta}$  par  $F_{1,\theta}$ .**

*solution :*

On rappelle que si  $a \in \mathbb{C}$  est une racine de  $P \in \mathbb{C}[X]$  alors  $(X - a)$  divise  $P$ . On voit facilement que  $F_{1,\theta} = X^2 - 2\cos(\theta)X + 1 = (X - e^{i\theta})(X - e^{-i\theta})$  et  $F_{m,\theta} = (X^m - e^{im\theta})(X^m - e^{-im\theta})$ , on peut donc vérifier que  $e^{i\theta}$  et  $e^{-i\theta}$  sont aussi des racines de  $F_{m,\theta}$  et donc  $F_{1,\theta}$  divise  $F_{m,\theta}$ .

D'autre part, mis sous cette forme, on peut trouver toutes les racines de  $F_{m,\theta}$ , ce sont les racines  $m$  ième de  $e^{im\theta}$  et de  $e^{-im\theta}$  c'est à dire :  $(e^{i(\theta + \frac{k2\pi}{m})})_{0 \leq k \leq m-1}$  et  $(e^{i(-\theta + \frac{k2\pi}{m})})_{0 \leq k \leq m-1}$ . On peut donc écrire :

$$F_{m,\theta} = F_{1,\theta} \prod_{k=1}^{m-1} \left( X - e^{i\left(\theta + \frac{k2\pi}{m}\right)} \right) \prod_{k'=1}^{m-1} \left( X - e^{i\left(-\theta + \frac{k'2\pi}{m}\right)} \right)$$

En regroupant les facteurs de manière à avoir  $k' = m - k$ , on obtient :

$$F_{m,\theta} = F_{1,\theta} \prod_{k=1}^{m-1} \left( X^2 - 2 \cos \left( \theta + \frac{k2\pi}{m} \right) X + 1 \right) \quad \blacksquare$$

### Exercice 17 :

**Montrer que  $(\sin(n))_{n \in \mathbb{N}}$  est dense dans  $[-1; 1]$ .  
La suite  $n|\sin(n)|$  tend-elle vers  $+\infty$  quand  $n \rightarrow +\infty$  ?**

*solution :*

Soient  $x \in [-1; 1]$  et  $\varepsilon > 0$ , puisque  $t \mapsto \sin(t)$  est surjective de  $\mathbb{R}$  dans  $[-1; 1]$ , il existe  $y \in \mathbb{R}$  tel que  $\sin(y) = x$ . Par ailleurs la fonction sinus est continue, il existe  $\alpha > 0$  tel que si  $|z - y| < \alpha$  alors  $|x - \sin(z)| < \varepsilon$ .

D'autre part,  $2\pi$  étant irrationnel, le sous groupe de  $\mathbb{R}$  engendré par 1 et  $2\pi$  est dense dans  $\mathbb{R}$ . Il existe donc deux entiers  $n \in \mathbb{N}$  et  $k \in \mathbb{Z}$  tels que  $|(n + k2\pi) - y| < \alpha$  et donc  $|\sin(n) - x| = |\sin(n + k2\pi) - \sin(y)| < \varepsilon$ .  $\blacksquare$

*Lemme de Kronecker :* Si  $x$  est irrationnel alors il existe une infinité d'éléments  $\frac{p}{q}$  de  $\mathbb{Q}$  tels que  $|x - \frac{p}{q}| < \frac{1}{q^2}$ .

*preuve :*

En notant  $\varepsilon : \mathbb{R} \rightarrow [0; 1[$  la fonction partie fractionnaire, on peut vérifier que la condition  $x$  est irrationnel est équivalente à la fonction  $n \mapsto \varepsilon(nx)$  de  $\mathbb{N}$  dans  $[0; 1[$  est injective et donc l'ensemble  $\{0, \varepsilon(x), \varepsilon(2x), \dots, \varepsilon(Nx)\}$  compte  $N + 1$  nombres distincts de  $[0; 1[$ . Mais cet intervalle ne contient que  $N$  intervalles du type  $[\frac{i}{N}; \frac{i+1}{N}[$  avec  $(0 \leq i \leq N - 1)$ . Il existe donc deux entiers  $i < j$  éléments de  $[0; N - 1]$  tels que  $|\varepsilon(ix) - \varepsilon(jx)| < \frac{1}{N}$ . En notant  $E$  la fonction partie entière, et  $p' = E(ix) - E(jx)$  et  $q' = j - i$ , on a  $|q'x - p'| < \frac{1}{N}$  (\*) puis avec  $p = \frac{p'}{\text{pgcd}(p', q')}$  et  $q = \frac{q'}{\text{pgcd}(p', q')}$ , on a  $|x - \frac{p}{q}| < \frac{1}{qN} < \frac{1}{q^2}$ . Il est alors facile de montrer qu'il existe une infinité de tels entiers  $p$  et  $q$  car sinon en prenant le *min* sur  $p$  et  $q$  dans la relation (\*) vrai pour tout  $N$  on montrerait alors que  $x$  est rationnel.

D'après le théorème de Kronecker puisque  $\pi$  est irrationnel il existe une infinité de rationnels  $\frac{p}{q}$  tels que  $|\pi - \frac{p}{q}| < \frac{1}{q^2}$  donc une infinité de nombres (premiers entre eux) tels que  $|q\pi - p| < \frac{1}{q}$  ou encore  $p = q\pi + \varepsilon$  avec  $|\varepsilon| < \frac{1}{q}$ . On a donc  $|\sin(p)| = |\sin(q\pi + \varepsilon)| = |\sin(\varepsilon)| \leq \frac{1}{q}$  d'où

$0 < p|\sin(p)| \leq \frac{p}{q} \leq \pi + \frac{1}{q^2} \leq 4$  ceci pour une infinité de  $p \in \mathbb{N}$ .  $\blacksquare$

### Exercice 18 :

**Montrer que le groupe  $\mathbb{H}_8 = \{\pm 1; \pm i; \pm j; \pm k\}$  des quaternions n'est pas un produit semi direct de groupes  $N \rtimes_{\varphi} H$ .**

*solution :*

Si c'était possible, il faudrait alors que le produit des ordres de  $N$  et  $H$  soit égal à 8 d'où l'on déduit que  $N$  ou  $H$  est d'ordre 2 i.e. est le centre  $Z(\mathbb{H}_8) = \{\pm 1\}$  de  $\mathbb{H}_8$ . Par ailleurs dans un produit semi direct  $N \rtimes_{\varphi} H$ , l'intersection de  $N$  avec  $H$  doit être trivial mais tous les sous groupes de  $\mathbb{H}_8$  contiennent son centre  $\{\pm 1\}$  c'est donc impossible. ■