# Sommaire

# 1 Algèbre linéaire

## 1.1 Endomorphisme indécomposable (HP prépa)

Soient $u$ un endomorphisme d'un $K$-ev $E$ de dimension finie $> 0$ . On dit de $F$, un sev de $E$ stable par $u$, qu'il est indécomposable sous $u$ s'il vérifie la propriété suivante : si $F_1$ et $F_2$ sont des sev de $F$, supplémentaires dans $F$ et tous deux stables par $u$, alors $F_1 = F$ ou $F_2 = F$.

1- On suppose que $E$ est indécomposable sous $u$. Montrer que $u$ est cyclique et que son polynôme caractéristique est une puissance d'un polynôme irréductible.

2- Réciproquement, on suppose que le polynôme caractéristique de $u$ est une puissance d'un polynôme irréductible et que $u$ est cyclique. Montrer que E est indécomposable sous $u$.

3- En déduire une caractérisation des sev indécomposables.

## 1.2 1000 et 1 vaches (oral ENS)

Un fermier prétend qu'avec son troupeau de 1001 vaches, peu importe la vache qu'il enlève de ce dernier, il est capable de diviser les 1000 vaches restantes en 2 troupeau de 500 de sorte que les 2 troupeaux aient la même masse totale. Que dire de la masse de chaque vache ?

***Indication:*** On pourra traduire ce que le fermier dit en introduisant une matrice.

***Correction:*** Si l'on note $m_i$ la masse de la vache numéro $i$, le fermier dit que pour tout $i$, il existe des indices un ensemble $J \subset [\![1, 1001]\!] \setminus \{i\}$ tel que $\sum_{j \in J} m_j = \sum_{\substack{j \notin J \\ j \neq i}} m_j$.

En faisant tout passer d'un côté, on constate que c'est équivalent à dire qu'il existe une matrice $M \in \mathcal{M}_{1001}$ de diagonale nulle et constituée d'exactement 500 "1" et 500 "-1" sur chaque ligne pour laquelle le vecteur $(m_1, ..., m_{1001})$ est dans $Ker(M)$. On peut se douter que chaque vache a en fait la même masse. Ainsi, on cherche à montrer que $M$ a un noyau de dimension 1.

$1^{ere}$ *méthode*

On peut montrer que la matrice extraite de $M$ par les 1000 premières lignes et colonnes est inversible pour avoir $dim(Ker(M)) \leq 1$ et conclure car le vecteur constitué uniquement de 1 est dans $Ker(M)$. Pour cela, montrons que le noyau de la matrice extraite $N$ mentionnée précédemment a un déterminant impair. On passe dans $\mathbb{Z}/2\mathbb{Z}$ et on note $\tilde{N}$ la matrice associée (i.e celle avec des 0 sur la diagonale et des 1 partout ailleurs). On a :

$$det(\tilde{N}) = \begin{vmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{vmatrix}_{L_1 \leftarrow L_1 + L_2} = \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 1 \\ 1 & \cdots & & 1 & 0 \end{vmatrix}$$

$$= \begin{vmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{vmatrix}_{1000 \times 1000} + \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{vmatrix}_{1000 \times 1000}$$

en développant selon la $1^{ere}$ ligne. A gauche, on voit la même matrice apparaître mais de taille "$n-1$" et à droite on peut montrer que le déterminant vaut 1 : on ajoute $L_2$ à $L_1$, on développe selon la $1^{ere}$ ligne et on constate que l'on retombe sur le même déterminant à un rang plus bas. On conclut donc par récurrence que $det(\tilde{N}) = 1$ et donc que $det(N) = 1$ mod 2.

$2^{eme}$ *méthode*

On note $m$ la masse totale du troupeau de 1001 vaches. On constate que l'on a $\sum_{i=1}^{1001} m_i = m$. Ainsi, on voit que le vecteur $(m_1, ..., m_{1001})$ est solution de $Ax = {}^t(m, ..., m)$ d'une matrice constituée de 1 sur la diagonale, de 500 "2" et 500 "0" sur chaque ligne. La matrice $A$ est inversible car son déterminant est impair (il suffit d'utiliser la formule éclatée du déterminant pour constater que le seul terme impair qui apparaît dans la somme est celui associé à la permutation identité). Ainsi, il y a une unique solution au problème et on constante que $(m/1001, ..., m/1001)$ est solution.

## 1.3 Famille positivement génératrice (oral ENS)

Soit $E$ un $\mathbb{R}$ -ev de dimension finie $n$. On dit que $(e_1, ..., e_p)$ est positivement génératrice si

$$\forall x \in E, \exists \lambda_1, ..., \lambda_p \in \mathbb{R}_+^* x = \lambda_1 e_1 + ... + \lambda_p e_p.$$

1- Montrer qu'il y a équivalence entre :

*i*) $(e_1, ..., e_p)$ est positivement génératrice

*ii*) il existe $\lambda_1, ..., \lambda_p \in \mathbb{R}_+^*$ tels que $0 = \lambda_1 e_1 + ... + \lambda_p e_p$.

On se donne maintenant une telle famille.

2- Justifier que l'on a $p \geq n+1$. Donner un exemple de famille positivement génératrice telle que $p = n+1$.

3- On suppose que l'on a $p \geq 2n+1$.

a) Montrer qu'il existe $I$ tel que $(e_i)_{i \in I}$ soit une base de $E$.

c) Montrer qu'il existe une sous-famille stricte de $(e_1, ..., e_p)$ qui reste positivement génératrice.

***Indication:*** Montrer que $(e_j)_{j\in I^c}$ est liée.

4- Donner un exemple de famille positivement génératrice de cardinal $2n$ dont aucune sous-famille stricte ne l'est.

## 1.4 Caractérisation des homothéties

Soient $E$ un $\mathbb{K}$-ev et $u \in \mathcal{L}(E)$ tel que, pour tout $x \in E$, la famille $(x, u(x))$ soit liée. Montrer que $u$ est une homothétie.

***Correction:*** $1^{ere}$ *méthode*

$(x, u(x))$ étant de taille 2 et liée, on sait que pour tout $x$, il existe $\lambda_x \in \mathbb{K}$ tel que $u(x) = \lambda_x x$. On va maintenant montrer que $\lambda_x = \lambda_y$ pour tout $x, y$ non nuls en distinguant les cas selon que $(x, y)$ soit liée ou libre.

Si elle est liée, on a $\lambda \in \mathbb{K}$ tel que $y = \lambda x$ et en appliquant, on obtient $\lambda\lambda_y x = \lambda\lambda_x x$ d'où le résultat annoncé.

Si elle libre, on regarde $x + y$ :

$$\begin{aligned} u(x+y) &= \lambda_{x+y}(x+y) \\ u(x) + u(y) &= \lambda_{x+y}x + \lambda_{x+y}y \\ \lambda_x x + \lambda_y y &= \lambda_{x+y}x + \lambda_{x+y}y \end{aligned}$$

et on obtient $\lambda_x = \lambda_{x+y} = \lambda_y$ puisque la famille $(x, y)$ est libre.

$2^{eme}$ *méthode, en dimension finie*

On aurait pu prendre une base de $E$ $(e_1, ..., e_n)$ et procéder de même que dans le cas précédent en regardant $e_1 + ... + e_n$.

## 1.5 Stabilité et endomorphisme

Soient $E$ un $\mathbb{K}$-ev de dimension finie $n$, $1 < k < n$ et $u \in \mathcal{L}(E)$ stabilisant tous les sev de $E$ de dimension $k$. Montrer que $u$ est une homothétie (i.e qu'il existe $\lambda \in \mathbb{K}$ tel que $u = \lambda id$).

Que se passe-t-il en dimension infinie ?

***Indication:*** On pourra montrer que les sev de dimensions $k-1$ sont également stables par $u$.

## 1.6 Egalité du parallélogramme

Soit $E$ un evn réel ou complexe. On suppose que l'on a l'égalité du parallélogramme :

$$\forall x, y \in E ||x - y||^2 + ||x + y||^2 = 2(||x||^2 + ||y||^2).$$

Montrer que la norme découle d'un produit scalaire i.e que $E$ est préhilbertien.

## 1.7 Espace vectoriel et dual

Donnez un exemple d'espace vectoriel normé réel de dimension finie non isométrique à son dual pour la norme subordonnée.

**Remarque:** Un espace préhilbertien de dimension finie est toujours isométrique à son dual : il suffit de regarder le morphisme qui envoie $e_i$ sur $e_i*$ si $(e_i)$ est une base orthonormée.

## 1.8 Espace vectoriel non isomorphe à son dual

Soit $\mathbb{K}$ un corps. Montrer que $\mathbb{K}[X]$ n'est pas isomorphe à son dual $\mathbb{K}[X]^*$.

***Indication:*** On pourra montrer que $\mathbb{K}[X]^*$ est isomorphe à $\mathbb{K}^{\mathbb{N}}$ via

$$(u_n) \in \mathbb{K}^{\mathbb{N}} \mapsto (\sum p_i X^i \in \mathbb{K}[X] \mapsto \sum p_i u_i) \in \mathbb{K}[X]^*.$$

On distinguera ensuite les cas selon que $\mathbb{K}$ soit dénombrable ou non.

***Correction:*** - Si $\mathbb{K}$ est indénombrable, alors $\mathbb{K}^{\mathbb{N}}$ n'est pas de dimension dénombrable car les suites $(\lambda^n)_{n\in\mathbb{N}}$, $\lambda \in \mathbb{K}$ forment une famille libre indénombrable (on utilise un déterminant de vandermonde). Ainsi, il ne saurait être isomorphes puisque $\mathbb{K}[X]$ est de dimension dénombrable.

-Sinon, $\mathbb{K}[X] = \bigcup_{n\in\mathbb{N}} \mathbb{K}_n[X]$ est au plus dénombrable en temps qu'union dénombrable d'ensembles au plus dénombrables ($\mathbb{K}_n[X]$ est isomorphe à $\mathbb{K}^n$ et est donc au plus dénombrable). Or, ce n'est pas le cas de $\mathbb{K}^{\mathbb{N}}$ puisqu'il contient $\{0;1\}$ qui est en bijection avec $\mathbb{R}$.

## 1.9 (Facile, sup) Autour de l'indice de nilpotence

Soit $f$ un endomorphisme nilpotent d'un $\mathbb{K}$-espace vectoriel $E$. On note $p$ l'indice de nilpotence de $f$, i.e le plus petit entier $p > 0$ tel que $f^p = 0$.

1- Montrer qu'il existe $x_0$ tel que $(x_0, f(x_0), ..., f^{p-1}(x_0))$ soit libre.

2- En déduire que $f^n = 0$.

## 1.10 Famille libre de formes linéaires

Soient $E$ un $\mathbb{K}$-ev de dimension finie et $(g_1, ..., g_n)$ une famille libre de formes linéaires. Montrer qu'il existe $(x_1, ..., x_n) \in E^n$ tels que la matrice de terme général $g_i(x_j)$ soit inversible.

***Indication:*** Traduire en terme de base de $\mathbb{K}^n$.

***Correction:*** On cherche donc $(x_1, ..., x_n) \in E^n$ tels que les $(g_1(x_i), ..., g_n(x_i))$ forment une base de $\mathbb{K}^n$. On pense alors à poser $f : x \mapsto (g_1(x), ..., g_n(x))$. On souhaite alors montrer que $rg(f) = n$. Pour cela, on utilise le théorème du rang et on montre que $dim(\bigcap_i Ker(g_i)) = dim(E) - n$ (par récurrence).

**Remarque:** En fait, on n'a pas besoin de l'hypothèse de dimension finie sur $E$ : il suffit de dire que $Im(f)$ ne peut pas être contenu dans un hyperplan.

## 1.11 Caractérisation de la liberté d'une famille de formes linéaires

Soient $f_1, ..., f_n, f$ des formes linéaires sur un espace vectoriel. Montrer que l'on a $f \in Vect(f_i)$ si et seulement si $\bigcap_{i=1}^{n} Ker(f_i) \subset Ker(f)$.

***Indication:*** On pourra traiter le cas où les $f_i$ forment une famille libre et se servir (de la remarque) de l'exercice précédent.

## 1.12 SEV stables

Soit $E$ un espace vectoriel de dimension finie dont $(e_1, ..., e_n)$ est une base. Pour $\sigma \in S_n$, on pose $u_\sigma$ l'endomorphisme vérifiant, pour tout $i$, $u_\sigma(e_i) = e_{\sigma(i)}$. Trouver tous les sous-espaces vectoriels de $E$ stables par tous les $u_\sigma$.

***Correction:*** On se donne $F$ sev stable par tous les $u_\sigma$. On suppose $F$ non nul. Il existe une famille de scalaires $(\lambda_i)$ non nulle telle que $\sum_{k=1}^{n} \lambda_i e_i \in F$. Si les $\lambda_i$ ne sont pas tous égaux, on peut toujours supposer $\lambda_1 \neq \lambda_2$. En prenant $\sigma = (1\ 2)$, on obtient $\lambda_1 e_2 + \lambda_2 e1 + \sum_{k=3}^{n} \lambda_i e_i \in F$. En soustrayant cela à notre premier élément, on en déduit $(\lambda_1 - \lambda_2)(e_1 - e_2) \in F$. On applique $u_\sigma$ pour $\sigma = (1\ i)$ et on a alors $(e_1 - e_i) \in F$ pour tout $i$. On vérifie facilement que la famille $(e_1 - e_i)_{i \geq 2}$ est libre. Ainsi, on a finalement $F = E$ ou $F = Vect(e_1 - e_i)$.

S'il n'existe pas d'élément tel que l'on en est donné, cela signifie que $F = Vect(e_1 + ... + e_n)$.

## 1.13 Polynôme minimal et endomorphisme cyclique

Soient $E$ un espace vectoriel et $u$ un endomorphisme de $E$ admettant $\pi_u$ pour polynôme minimal.

On introduit rapidement la notion de polynôme minimal de $f$ en $x \in E$ quand $f$ est un endomorphisme de $E$ : c'est le polynôme $P$ non nul unitaire de degré minimal tel que $P(f)(x) = 0$. On le note $\pi_{f,x}$. Cette définition n'est valable que lorsqu'il existe un polynôme non nul $P$ tel que $P(f)(x) = 0$. $\pi_{f,x}$ est le polynôme unitaire non nul vérifiant $\{P \in \mathbb{K}[X] : P(f)(x)\} = \pi_{f,x}\mathbb{K}[X]$.

On va montrer qu'il existe $x \in E$ tel que $\pi_u = \pi_{u,x}$. Pour rendre l'exercice plus intéressant, on peut chercher à conclure après avoir fait la q.2.

1- Justifier que pour tout $x \in E$, $\pi_{u,x}$ existe .

2- On décompose $\pi_u$ en produit d'irréductibles : $\pi_u = \prod_{i=1}^{n} P_i^{\alpha_i}$.

Justifier que, pour tout $i$, il existe $x_i \in E$ tel que $\pi_{u,x_i} = P_i^{\alpha_i}$.

3- Soient $x, y \in E$ tels que $\pi_{u,x} \wedge \pi_{u,y} = 1$. Montrer que l'on a $\pi_{u,x+y} = \pi_{u,x}\pi_{u,y}$.

4- Conclure.

***Correction:*** 1- $\pi_u$ vérifie $\pi_u(x) = 0$ et $\pi_u \neq 0$.

2- On sait qu'il existe $x \in E$ tel que $P_i^{\alpha_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j^{\alpha_j}(u)(x) \neq 0$ (sans quoi on aurait $P_i^{\alpha_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j^{\alpha_j}(u) = 0$, ce qui contredirait la définition de $\pi_u$).

On prend un tel $x$ et on constate que $x_i = P_i^{\alpha_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j^{\alpha_j}(u)(x)$ convient.

3- On voit facilement que l'on a

$$\pi_{u,x}\pi_{u,y}(u)(x+y) = \pi_{u,x}(\pi_{u,y}(u)(y)) + \pi_{u,y}(\pi_{u,x}(u)(x)) = 0 + 0 \ .$$

On a donc $\pi_{u,x+y}$ divise $\pi_{u,x}\pi_{u,y}$.

De plus, si $P(u)(x+y) = 0$, on a $\pi_{u,x}\pi_{u,y}$ divise $P$. (Il suffira d'appliquer cela à $P = \pi_{u,x+y}$ pour conclure.) En effet, on a alors $P(u)(x) = -P(u)(y)$ et donc $\pi_{u,x}P(u)(y) = 0$ i.e $\pi_{u,y}$ divise $\pi_{u,x}P$.

Or, on a supposé avoir $\pi_{u,x} \wedge \pi_{u,y} = 1$. On en déduit que $\pi_{u,y}$ divise $P$. De même, on peut montrer que l'on a $\pi_{u,x}$ divise $P$. Puisque $\pi_{u,x} \wedge \pi_{u,y} = 1$, on a $\pi_{u,x}\pi_{u,y}$ divise $P$.

4- On prend $x = x_1 + ... + x_n$.

# 2 Réduction des endomorphismes

## 2.1 Sous-groupe de $GL_n(\mathbb{C})$

Soit $G$ un sous-groupe de $GL_n(\mathbb{C})$. On note $||.||$ la norme 2 sur $\mathbb{C}^n$. On suppose qu'il existe $k \in [0; 2[$ tel que :

$$\forall M \in G, \quad ||MX - X|| \leq k||X||.$$

Montrer qu'il existe un entier $m$ tel que pour tout $M \in G$, on a $M^m = I_n$.

***Correction:*** On note $S_p(G) = \bigcup_{M \in G} S_p(M)$ où $S_p(M)$ désigne le spectre de $M$. Dire qu'il existe $m$ tel qu'énoncé signifie exactement que toutes les valeurs propres de n'importe quelle matrice de $G$ (i.e tous les éléments de $S_p(G)$) sont des racines $m^{eme}$ de l'unité et que ces matrices sont diagonalisables. En effet, si ce $m$ existe, alors $X^m - 1$ annule tout $M \in G$. Puisque $X^m - 1$ est scindé à racine simple dans $\mathbb{C}$, tout $M \in G$ est diagonalisable et ses valeurs propres sont des racines $m^{eme}$ de l'unité. Réciproquement, c'est clair.

Soit $\lambda \in S_p(G)$. On a $\lambda^j \in S_p(G)$ pour tout $j \in \mathbb{Z}$ (et même $\lambda^j$ valeur propre de $M^j$ dont $X$ est un vecteur propre si $MX = \lambda X$, où $M \in G$).

L'inégalité de l'énoncé dit pour tout $\lambda \in S_p(G)$, on a $|\lambda - 1| \leq k$. Si $|\lambda| \neq 1$ et $\lambda \in S_p(G)$, on peut toujours supposer $|\lambda| > 1$ quitte à considérer $\lambda^{-1}$, qui est bien dans $S_p(G)$. Or, on a $\lambda^j \in S_p(G)$ pour tout $j > 0$ donc on a $|\lambda^j - 1| \leq k$ mais la quantité de gauche tend vers $+\infty$ quand $j \to +\infty$ par l'inégalité triangulaire, absurde.

Ainsi, on a $|\lambda| = 1$ pour tout $\lambda \in S_p(G)$. L'énoncé dit donc que l'on a, pour tout $e^{2i\pi\theta} \in S_p(G)$, $|e^{2i\pi\theta} - 1| \leq k < 2$. Supposons par l'absurde qu'il existe $\theta$ irrationnel tel que $e^{2i\pi\theta} \in S_p(G)$. Par un exercice classique, on aurait $2\pi\theta\mathbb{Z} + 2\pi\mathbb{Z}$ dense dans $\mathbb{R}$. Or, on a, pour tout $j, l \in \mathbb{Z} e^{2i\pi\theta j + 2i\pi l} = e^{2i\pi\theta j} \in S_p(G)$ par ce qui précède. Ainsi, $S_p(G)$ est dense dans $\mathbf{S}^1$ (le cercle unité) et il existe donc $(\theta_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ tel que $e^{2i\pi\theta_n} \xrightarrow[n\to\infty]{} -1$, si bien que l'on a $|e^{2i\pi\theta} - 1| \xrightarrow[n\to\infty]{} 2$ et que l'inégalité $|e^{2i\pi\theta_n} - 1| \leq k$ ne tient plus à partir d'un certain rang.

Ainsi, tout $\lambda \in S_p(G)$ s'écrit de façon unique comme $e^{\frac{2i\pi j}{l}}$ avec $0 \leq j < l$ et $j \wedge l = 1$. Si, par l'absurde, l'ensemble de ces $l$ n'est pas borné, alors il existe une extractrice $\phi$ et une fonction $f$ telles que $e^{\frac{2i\pi f(j)}{\varphi(j)}} \in S_p(G)$, $0 \leq f(j) < \varphi(j)$ et $f(j) \wedge \varphi(j) = 1$ pour tout $j \in \mathbb{N}$. Puisque $S_p(G)$ est stable par passage à la puissance et que $f(j) \wedge \varphi(j) = 1$, on a $U_{\varphi(j)} \in S_p(G)$ pour tout $j$. Ainsi, l'ensemble des racines de l'unité, qui n'est autre que $\bigcup_{j\in\mathbb{N}} U_{\varphi(j)}$ est inclus dans $S_p$ et on retrouve que $S_p$ est dense dans $U$, absurde.

Soit $M \in G$. Par Jordan-Chevalley, il existe $D, N$ avec $D$ diagonalisable, $N$ nilpotente, $DN = ND$ et $M = D + N$. Remarquons que l'on a $M^j \in G$ pour tout $j$ donc $||M^j - I|| \leq k$ pour tout $j$ et donc $(||M^j||)$ est bornée.

Supposons, par l'absurde, que $r$ - l'indice de nilpotence de $N$ - n'est pas 1 (i.e que $N$ n'est pas nulle). Remarquons que $r$ est également l'indice de nilpotence de $ND^{-1}$. Aussi, on peut compléter $(I, ..., (ND^{-1})^{r-1})$ en une base de de $M_n(\mathbb{C})$ et définir la norme infini associée à cette base, norme que l'on notera $||.||_\infty$. On a $(MD^{-1})^j = \sum_{l=0}^{j} \binom{j}{l} (ND^{-1})^l = \sum_{l=0}^{r-1} \binom{j}{l} (ND^{-1})^l$. Aussi, $(||D^{-j}||)$ est bornée puisque $D$ est diagonalisable et que toutes ses valeurs propres (sont celles de $M$ et donc) sont de module 1. Alors, $(||MD^{-1}||^j)$ est également bornée mais ce n'est pas le cas de $(||(MD^{-1})^j||_\infty)$ puisque $||(MD^{-1})^j||_\infty \geq \binom{j}{1} = j$ n'est pas bornée. On obtient donc une contradiction puisque, $M_n(\mathbb{C})$ étant de dimension finie, les normes subordonnée et infini sont équivalentes.

# 3 Espace vectoriel normé

## 3.1 Réciproque à l'équivalence des normes

Soit $E$ un espace vectoriel normé réel tel que toutes les normes soient équivalentes. On va montrer que $E$ est de dimension finie.

1- Soit $f$ une forme linéaire sur $E$. Montrer que $f$ est continue.

2- Si $E$ est de dimension infinie, construire une forme linéaire non continue.

3- Autre méthode : en comparant la norme infinie et la norme 1 sur $E$.

### 3.2 Noyau d'une forme linéaire

Soit $E$ un espace vectoriel normé.

Montrer qu'une forme linéaire sur $E$ est continue si et seulement si son noyau est fermé.

### 3.3 Existence de supplémentaires et de bases

1- Soit $E$ un espace vectoriel. En utilisant le lemme de Zorn, montrer que tout sous-espace vectoriel de $E$ admet un supplémentaire dans $E$.

***Indication:*** Etant donné $F$ un sev, on regardera $\{G \text{ sev de } E : F \cap G = \{0\}\}$.

2- Faire de même pour montrer que tout espace vectoriel admet une base.

## 4 Matrice

### 4.1 Autour du théorème spectral (Agreg Nancy)

1- Une matrice symétrique à coefficient dans un corps fini est-elle forcément diagonalisable ?

2- Soit $\mathbb{K}$ un corps tel que toute matrice symétrique à coefficient dans ce corps soit diagonalisable.

*i*) Montrer que $-1$ n'est pas un carré.

*ii*) Montrer que la somme de deux carrés est encore un carré.

*iii*) En déduire que l'on peut munir $\mathbb{K}$ d'une structure de corps ordonné.

***Correction:*** 1- Non : la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ est symétrique non diagonalisable dans $\mathbb{Z}/2\mathbb{Z}$ car son polynôme caractéristique $X^2 + X + 1$ n'a pas de racine.

2-*i*) Par l'absurde, si on pouvait trouver $x \in \mathbb{K}$ tel que $x^2 = -1$, on aurait $\begin{pmatrix} 1 & x \\ x & -1 \end{pmatrix}$ diagonalisable. Or, son polynôme caractéristique est $X^2$ donc sa seule valeur propre est 0. Ainsi, cette matrice serait nulle, absurde.

*ii*) La matrice $\begin{pmatrix} \sqrt{a} & \sqrt{b} \\ \sqrt{b} & -\sqrt{a} \end{pmatrix}$ a pour polynôme caractéristique $X^2 - (a + b)$ est scindé puisque, par hypothèse, la matrice est diagonalisable.

*iii*) Il suffit de dire que l'on a $x \leq y$ ssi $y - x$ est un carré.

## 4.2 Le déterminant n'est pas linéaire

Soit $B \in M_n(\mathbb{K})$ telle que $det(A+B) = det(A) + det(B)$ pour tout $A \in M_n(\mathbb{K})$ avec $\mathbb{K}$ un corps de caractéristique différente de 2. Montrer que $B = 0$ ou $n = 1$.

***Correction:*** En particulier pour $A = B$, on obtient $det(2B) = 2det(B)$ et par $n$-linéarité du déterminant, on a $2^n det(B) = 2det(B)$. Si $det(B) \neq 0$, on obtient directement $n = 1$. Sinon, la première égalité se réécrit $det(A+B) = det(A)$. Supposons $B \neq 0$. Par conséquent, on peut trouver une base $(f1, ..., f_k)$ de $Ker(B)$ avec $k < n$ et la compléter en base $(f_1, ..., f_k, e_1, ..., e_{n-k})$ de $\mathbb{K}^n$. En regardant $A$ telle que $Af_i = f_i$, $Ae_1 = -Be1$ et $Ae_i = Be_1$. On a $A$ inversible i.e $det(A) \neq 0$ et pourtant, on a $e1 \in Ker(A+B)$ .

## 4.3 Matrice à diagonale strictement dominante

On dit que $M \in M_n(\mathbb{C})$ est à diagonale strictement dominante lorsque

$$\forall i \in [\![1, n]\!],\ |m_{i,i}| > \sum_{\substack{j=1 \\ j \neq i}}^{n} m_{i,j}.$$

Montrer qu'une telle matrice est inversible.

## 4.4 Matrice compagnon

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ unitaire.

1-Montrer que le polynôme caractéristique de $\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$ est $P$.

***Indication:*** Faire une récurrence en utilisant un développement du déterminant selon une ligne ou une colonne.

2- Donner une CNS pour que la matrice compagnon soit inversible.

3- En déduire des inégalités sur les racines de $P$. (On pourra se servir de l'exercice précédent.)

## 4.5 Existence d'un morphisme à valeurs dans $M_n(\mathbb{K})$ (Tosel)

Soient $\mathbb{K}$ un corps et $x$ un élément algébrique sur $\mathbb{K}$. Sous quelle condition existe-t-il un morphisme de $\mathbb{K}$-algèbre entre $\mathbb{K}(x)$ dans $M_n(\mathbb{K})$ ?

***Indication:*** On pourra penser à se servir de l'exercice précèdent.

***Correction:*** S'il existe un tel morphisme $f$, il est forcément injectif : si $z \in \mathbb{K}[x]$ est non nul, alors $f(z) \neq 0$ puisque $f(z)f(z^{-1}) = f(1) = 1$.

En notant $\pi_a$ le polynôme minimal de $a$ (s'il existe, $a$ étant un élément de $\mathbb{K}[x]$ ou de $M_n(\mathbb{K})$) et $d$ le degré de $x$, on a, par le caractère injectif de $f$, $\pi_x = \pi_{f(x)}$ d'où $n \geq d$ (toute matrice de $M_n(\mathbb{K})$ a un degré plus petit que $n$ par le théorème de Cayley-Hamilton).

Réciproquement, on peut construire une matrice $M$ qui vérifie $\pi_x = \pi_M$ : il suffit de la construire par blocs, en mettant la matrice compagnon de $\pi_x$ en haut à gauche et des matrices nulles autour. Il est alors facilement de vérifier que $\pi_x(M) = 0$ et par l'irréductibilité de $\pi_x$ on conclut que $\pi_x = \pi_M$. Maintenant, il suffit de poser $f(P(x)) = P(M)$ pour tout $P \in \mathbb{K}[X]$ et de vérifier que $f$ est bien définie (i.e que si $P(x) = Q(x)$ alors $P(M) = Q(M)$).

## 4.6 Autour de $GL_n(\mathbb{Z})$

1- On note $GL_n(\mathbb{Z}) = \left\{M \in M_n(\mathbb{Z}) : M \in GL_n(\mathbb{Q}) \text{ et } M^{-1} \in M_n(\mathbb{Z})\right\}$. Montrer que l'on a $GL_n(\mathbb{Z}) = \{M \in M_n(\mathbb{Z}) : |det(M)| = 1\}$.

***Indication:*** Utiliser la formule de la comatrice pour l'inclusion droite-gauche.

2- Montrer que, si $A \in GL_n(\mathbb{Z})$, alors soit on a qu'une des valeurs propres complexes de $A$ est de module strictement plus grand que 1, soit il existe $k \in \mathbb{N}$ tel que $A^k - I_n$ soit nilpotente.

***Indication:*** On pourra remarquer qu'il n'existe qu'un nombre fini de polynômes de $\mathbb{Z}_n[X]$ possédant uniquement des racines exponentielles complexes.

***Correction:*** 2- Supposons la première condition non vérifiée. Notons $\lambda_1, ..., \lambda_n$ les valeurs propres de $A$. On a donc $|\lambda_i| \leq 1$ pour tout $i$. En notant $\chi_M$ le polynôme caractéristique de $M$, on a donc $|\chi_A(0)| = \prod_{i=1}^{n} |\lambda_i| \in \mathbb{Z}$ et ce dernier est dans $]0; 1]$ (0 est exclu car $A$ est inversible). Ainsi, on a forcément $|\chi_A(0)| = 1$ et $|\lambda_i| = 1$ pour tout $i$.

Autrement dit, toutes les valeurs propres de $A$ sont des exponentielles complexes. La condition "$A^k - I_n$ nilpotente" revient donc à montrer que les valeurs propres de $A$ sont en fait des racines de l'unité (on pouvait s'en rendre compte plus tôt en triangularisant $A$). Pour faire apparaître les $\lambda_i^k$, il peut être intéressant de regarder les $A^k$. On note que, par les relations coefficients-racines, il n'existe qu'un nombre fini de polynômes de $\mathbb{Z}_n[X]$ possédant uniquement des racines exponentielles complexes (car ses coefficients sont bornés). Ainsi, il existe $1 < k_1 < k_2$ tel que $\chi_{A^{k_1}} = \chi_{A^{k_2}}$ et alors on a $\left\{\lambda_i^{k_1} : 1 \leq i \leq n\right\} = \left\{\lambda_i^{k_2} : 1 \leq i \leq n\right\}$.

Par conséquent, on dispose d'une application $f : [\![1, N]\!] \to [\![1, N]\!]$ telle que $\lambda_i^{k_1} = \lambda_{f(i)}^{k_2}$. On voit facilement que pour tout $i$, il existe $a < b$ tels que $f^a(i) =$

$f^b(i)$ (on note la composition itérée en puissance). On en déduit $\lambda_{f^a(i)}^{k_1} = \lambda_{f^a(i)}^{k_2(b-a)}$ et donc $\lambda_{f^a(i)}$ est d'ordre fini et il en va alors de même de $\lambda_i$ puisque $\lambda_i^{k_1} = \lambda_{f^a(i)}^{ak_2}$.

Moins prise de tête : on aurait pu construire $f$ de façon à ce qu'elle soit injective (en se basant sur $\chi_{A^{k_1}} = \chi_{A^{k_2}}$) et ensuite utiliser le fait qu'une permutation est d'ordre fini.

## 4.7 Encore autour de $GL_n(\mathbb{Z})$

Donner une CNS pour que $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ soit la première colonne d'une matrice de $GL_n(\mathbb{Z})$.

## 4.8 Diagonalisabilité et carré

Si $M \in GL_n(\mathbb{K})$, montrer que $M$ est diagonalisable ssi $M^2$ l'est.

## 4.9 Endomorphismes semi-simples sur $\mathbb{C}$

Un endomorphisme $f$ est dit semi-simple quand tout sev stable par $f$ admet un supplémentaire stable par $f$.

Soient $E$ un $\mathbb{C}$-ev et $f$ un endomorphisme de $E$. Montrer que $f$ est semi-simple ssi $f$ est diagonalisable.

***Correction:*** Pour le sens réciproque, on suppose $f$ diagonalisable. On note $\lambda_1, ..., \lambda_r$ ses valeurs propres (deux à deux distinctes). Soit $G$ stable par $f$. Puisque $f$ est diagonalisable, il en est de même de $\widetilde{f}$ (la restriction de $f$ à $G$ au départ et à l'arrivée). De plus, $\chi_{\widetilde{f}}$ divise $\chi_f$ donc les valeurs propres de $\widetilde{f}$ sont des valeurs propres de $f$. Ainsi, si $(e_{1,i_1}, ..., e_{j_{i_1},i_1}, e_{1,i_2}, ..., e_{j_{i_k},i_k})$ est une base de $G$ telle que $\widetilde{f}(e_{j,i_k}) = \lambda_{i_k} e_{j,i_k}$ pour tout $k, 1 \leq j \leq j_{i_k}$ (c'est juste une base propre et on a regroupé les vecteurs de la base selon la valeur propre à laquelle ils sont associées), on procède de la façon suivante : on prend $H_r$ un supplémentaire de $Vect(e_{1,i_k}, ..., e_{j_{i_r},i_r})$ dans $E_{\lambda_{i_r}}$. Alors, il est facile de voir que $\bigoplus_{r=1}^{k} H_r$ est un supplémentaire de $G$ dans $E$ ( car $E = \bigoplus_{r=1}^{k} E_{\lambda_{i_r}}$) et qu'il est lui aussi stable par $f$.

## 4.10 Endomorphismes semi-simples sur $\mathbb{R}$

Soit $E$ un $\mathbb{R}$-ev de dimension finie.

1- Montrer que tout endomorphisme $f$ sur $E$ admet une droite un ou un plan stable par $f$.

2- Montrer que $f$ est semi-simple ssi s'écrit, dans une certaine base, comme une matrice diagonale pas blocs de la forme $(\lambda)$ ou $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

## 4.11 Endomorphismes semi-simples sur corps quelconque

Soient $E$ un $\mathbb{K}$-ev de dimension finie et $f$ un endomorphisme de $E$. Montrer que $f$ est semi-simple ssi son polynôme minimal est sans facteur carré i.e si $Q$ divise $\pi_f$ alors $Q^2$ ne le divise pas.

## 4.12 Caractérisation de la diagonalisabilité

Soient $E$ un $\mathbb{C}$-ev et $f$ endomorphisme de $E$. Montrer que $f$ est diagonalisable ssi pour tout $\lambda \in \mathbb{C}$ on a $rg(f - \lambda id) = rg((f - \lambda id)^2)$.

## 4.13 Comatrice de la comatrice

Soient $n \geq 2$, $\mathbb{K}$ un corps infini. Que vaut la transposée de la comatrice de la traponsée de la comatrice d'une matrice $A$ de taille $n$ ?

***Correction:*** On note $f(A) = {}^tCom(A)$. En jouant avec $A{}^tCom(A) = det(A)I_n$, on montre que l'on a $f(f(A)) = det(A)^{n-2}A$ pour toute matrice $A$ inversible. On conclut maintenant en fixant $A$ quelconque. Elle n'a qu'un nombre fini de valeurs propres dans $\mathbb{K}$ et donc on a $f(f(A+\lambda I_n)) = det(A+\lambda I_n)^{n-2}(A+\lambda I_n)$ pour une infinité de $\lambda$. A droite, chaque coefficient de la matrice s'exprime de façon polynomiale en $\lambda$. Il en est de même à gauche puisque la comatrice d'une matrice est composé de déterminants extraits de cette dernière matrice. On en tire finalement une égalité polynomiale qui nous permet d'évaluer la relation en $\lambda = 0$, ce qui conclut.

## 4.14 Morphisme multiplicatif

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Soit $f : M_n(\mathbb{K}) \to \mathbb{K}$ non constante telle que $f(AB) = f(A)f(B)$. Montrer que l'on a $f(M) \neq 0 \Leftrightarrow M \in GL_n(\mathbb{K})$.

***Correction:*** Il existe $A$ telle que $f(A) \neq 0$. Or, on a $f(A) = f(A)f(I)$, d'où $f(I) = 1$. Soit $M \in GL_n(\mathbb{K})$. Alors, on a $f(M)f(M^{-1}) = 1$, d'où $f(M) \neq 1$.

Réciproquement, si $M$ est non inversible, on sait écrire $M = PNQ$ avec $P, Q$ inversibles et $N$ nilpotente. On peut aussi travailler avec $N = J_r$ ou la décomposition $PLU$.

## 4.15 Réduction et transposée

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{R})$. On suppose qu'il existe $k \geqslant 2$ tel que $A^k = {}^tA$.

1. Montrer que ${}^tAA$ est la matrice d'un projecteur orthogonal.
2. Montrer que $A$ est diagonalisable dans $\mathbb{C}$.

***Correction:*** 1- On remarque que ${}^tA$ est symétrique réelle positive donc par le théorème spectral on sait que c'est une matrice diagonalisable dans $\mathbb{R}$, de valeurs propres positives et que ses sous-espaces propres sont en somme orthogonale. Il s'agit donc en fait de montrer que l'on a $\mathrm{Spec}({}^tA) \subset \{0;1\}$. Or, on a

$$\mathrm{Spec}({}^tA) = \mathrm{Spec}(A) = \mathrm{Spec}(A^k).$$

On en déduit que l'on a $\mathrm{Spec}(A)$ inclus dans un ensemble constitué de 0 et de racines de l'unité. On en déduit la même chose sur ${}^tAA = A^{k+1}$ et le fait que ses racines soient réelles positives donne le résultat attendu.

# 5 Réseaux

## 5.1 Sous-groupes discrets de $\mathbb{R}^n$

Soit $V$ un sous-groupe discret de $\mathbb{R}^n$. Montrer que $V$ est un groupe abélien libre.

***Correction:*** Soit $(v_1, ..., v_r) \in V^r$ une base du sous-espace vectoriel engendré par $V$. Posons

$$K = \left\{ \sum_{i=1}^{r} \lambda_i v_i : \lambda_i \in [0;1] \right\}.$$

C'est un compact de $\mathbb{R}^n$ donc $V \cap K$ est fini ; notons $x_1, ..., x_k$ ses points. Montrons maintenant que $V$ est de type fini, ce qui conclura par le théorème de classification des groupes abéliens de type fini. Soit $v \in V$. Il existe des réels $\lambda_i$ tels que

$$v = \sum_{i=1}^{r} \lambda_i v_i.$$

On a donc

$$v - \sum_{i=1}^{r} \lfloor \lambda_i \rfloor v_i \in K \cap V$$

de sorte que $v$ est combinaison entière des $v_i$ et des $x_i$.

# 6 Polynôme / Extension de corps

## 6.1 Alternative à la formule de Bernouilli

Montrer que l'on a $P^n - Q^n = \prod_{k=0}^{n-1} (P - e^{\frac{2ik\pi}{n}} Q)$ pour tout $n > 0$ et tous polynômes de $\mathbb{C}[X]$.

***Indication:*** On peut s'aider de $X^n - 1$.

***Correction:*** On a, en développant :

$$\prod_{k=0}^{n-1} P - e^{\frac{2ik\pi}{n}} Q = \sum_{j=0}^{n} P^j (-Q)^{n-j} \sum_{|I|=n-j} e^{\frac{2i\pi}{n} \sum_{k\in I} k}.$$

Il s'agit donc de montrer que l'on a $\sum_{|I|=j} e^{\frac{2ipi}{n} \sum_{k\in I} k} = 0$ pour tout $0 < j < n$. On applique cela à $P = X$ et $Q = 1$ et on obtient :

$$X^n - 1 = \sum_{j=0}^{n} X^{n-j} (-1)^j \sum_{|I|=j} e^{\frac{2i\pi}{n} \sum_{k\in I} k}.$$

On en déduit ce que l'on voulait en identifiant les coefficients des deux polynômes qui apparaissent.

## 6.2 Nombre de racines

Soit $A$ un anneau commutatif tel que tout polynôme unitaire de degré 2 à coefficients dans $A$ admette au plus 2 racines. Montrer que soit $A$ est intègre, soit $A$ est nul soit $A$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou bien à $\mathbb{F}_2[X]/ < X^2 >$.

***Correction:*** Supposons exclus les deux premiers cas. On a alors $x, y \in A \setminus \{0\}$ tels que $xy = 0$. On considère alors le polynôme $P = X^2 - (x + y)X \in A[X]$. Il admet $0, x, y$ pour racines. Ainsi, on a $y = x$, de sorte que l'on a $x^2 = 0$. Il s'en suit que l'on $(ax)^2 = 0$ pour tout $a \in A$ puisque $A$ est commutatif. Autrement dit, pour tout $a \in A$, $ax$ est racine de $X^2$, qui a également pour racines 0 et $x$. On en déduit que l'on a pour tout $a \in A$, $ax \in \{0, x\}$, i.e. $xa = 0$ ou $x(a-1) = 0$. En utilisant des polynômes analogues à $P$, il vient maintenant que l'on a :

$$\forall a \in A \quad a - 1 \in \{0, x\} \ \ ou\ a \in \{0, x\}\,.$$

En particulier, puisque les deux premiers cas sont exclus, on a $2 = x$ ou $2 = 0$ dans $A$. Selon ces cas, on obtient finalement l'isomorphisme souhaité.

## 6.3 Divisibilité dans $\mathbb{Z}$

Soient $P, Q \in \mathbb{Z}[X]$ tels que $\{n : P(n)|Q(n)\}$ soit infini. Montrer que $P$ divise $Q$ dans $\mathbb{Q}[X]$.

***Indication:*** Montrer que $deg(P) \leq deg(Q)$ si $Q$ n'est pas nul.

***Correction:*** Par l'absurde, on aurait alors que $\frac{Q}{P} \underset{\infty}{\longrightarrow} 0$. Par suite, il existe une infinité d'entiers qui annulent $\frac{Q}{P}$ et, par conséquent, $Q$ est nul.

On effectue ensuite la division euclidienne de $Q$ par $P$ et on rapplique l'indication au reste par l'absurde.

## 6.4 Polynômes positifs (1)

Soit $P \in \mathbb{R}[X]$. Montrer que l'on a :

$$\forall x \in \mathbb{R} \quad P(x) \geq 0 \quad \iff \quad \exists A, B \in \mathbb{R}[X] : P = A^2 + B^2$$

## 6.5 Polynômes positifs (2)

Soit $P \in \mathbb{R}[X]$. Montrer que l'on a :

$$\forall x \in \mathbb{R}_+^* \quad P(x) > 0 \quad \iff \quad \exists A, B \in \mathcal{P} : P = A/B$$

où $\mathcal{P}$ est l'ensemble des polynômes non nuls à coefficients positifs.

***Correction:*** Il suffit de traiter le cas des polynômes irréductibles de degré 2 pour le sens direct. Si $P = X^2 - aX + b$ avec $a, b > 0$, on distingue 2 cas :

-si $a^2 \leq b$ alors on $P.(X + c) = X^3 + (c - a)X^2 + (b - ac)X + bc$. On constate que $c = a$ convient : $P = \frac{P\ (X+a)}{X+a}$.

-Sinon, on cherche $Q = \sum_{i=0}^{n} q_i X^i \in \mathcal{P}$ tel que $PQ \in \mathcal{P}$. En développant le produit, on voit que l'on veut avoir :

$$p_{n-1} - ap_n \geq 0, \quad \forall i \in [\![2; n]\!]\ p_{i-2} - ap_{i-1} + bp_i \geq 0, \quad bp_1 - ap_0$$

et on constate que $n = 0, p_3 = 1, p_2 = a, p_1 = (a^2 - b), p_0 =$.

## 6.6 Contenu d'un polynôme

Si $P \in \mathbb{Z}[X]$, on note $c(P)$ le pgcd de ses coefficients. On dit que $P$ est primitif si son contenu vaut 1.

1- Montrer que le produit de deux polynômes primitifs est primitif.

2- En déduire $c(PQ) = c(P)c(Q)$ et que si $P \in \mathbb{Z}[X]$ n'est pas irréductible dans $\mathbb{Q}[X]$ alors il ne l'est pas non plus dans $\mathbb{Z}[X]$

## 6.7 Irréductibilité (1) (Tosel)

Soient $n \in \mathbb{N}^*$ et $a_1, ..., a_n$ des entiers 2 à 2 distincts. Montrer l'irréductibilité de $P = \prod_{k=1}^{n} (X - a_i) - 1$ dans $\mathbb{Q}[X]$.

***Indication:*** Cela revient à montrer son irréductibilité dans $\mathbb{Z}[X]$.

## 6.8 Irréductibilité (2) (Tosel)

1- Montrer qu'un polynôme de $\mathbb{Z}[X]$ prenant 4 fois la valeur 1 sur $\mathbb{Z}$ ne peut pas prendre la valeur $-1$ sur $\mathbb{Z}$

2- En déduire que pour tout $n \geq 12$ et $P \in \mathbb{Z}[X]$ de degré $n$ prenant les valeurs $\pm 1$ en au moins $\lfloor \frac{n}{2} \rfloor + 1$ entiers est irréductible.

***Correction:*** 1- On a donc $P-1=(X-a_1)...(X-a_4)Q$ où les $a_i$ sont des entiers 2 à 2 distincts et $Q$ un polynôme entier. S'il existe $a\in\mathbb{Z}$ tel que $P(a)=-1$ alors on a $-2=(a-a_1)...(a-a_4)Q(a)$ et par conséquent $a$ serait à distance 1 d'au moins 3 entiers distincts, ce qui est impossible.

2- $P$ prend donc les valeurs $\pm1$ au moins 7 fois. Ainsi, par Dirichlet, au aurait que $P$ prend au moins 4 fois la valeur $-1$ ou au moins 4 fois la valeur 1. Quitte à considérer $-P$, on peut toujours supposer que $P$ prend au moins 4 fois la valeur $-1$. Par la question précédente, on a que $P$ prend la valeur $-1$ au moins $\lfloor\frac{n}{2}\rfloor+1$ fois. Si $P=QR$ avec $Q,R\in\mathbb{Z}[X]$ on a $deg(P)\leq\lfloor\frac{n}{2}\rfloor$ ou $deg(Q)\leq\lfloor\frac{n}{2}\rfloor$. Sans perte de généralité, supposons que ce soit $Q$. On a $QR$ prend la valeur -1 $\lfloor\frac{n}{2}\rfloor+1$ fois donc en ces points on a [$Q$ prend la valeur 1 et $R$ la valeur -1] ou l'inverse. Par Dirichlet, $Q$ prend au moins 4 fois la valeur 1 ou 4 fois la valeur -1. On peut supposer que c'est -1 quitte à considérer $-Q$ et $-R$. Par la q.1, on a que $Q$ prend la valeur -1 $\lfloor\frac{n}{2}\rfloor+1$ fois et est donc constant égal à -1.

## 6.9 Une suite périodique (oral ULM)

Soient $P,Q\in\mathbb{Z}[X]$ n'ayant aucune racine commune dans $\mathbb{C}$. Montrer que $(P(n)\wedge Q(n))_{n\in\mathbb{N}}$ est périodique.

***Correction:*** On a, par hypothèse, $P\wedge Q=1$ dans $\mathbb{C}$. Ainsi, il en est de même dans $\mathbb{Q}$. Par Bezout, il existe $A,B\in\mathbb{Q}[X]$ tels que $PA+QB=1$. Ainsi, il existe $a\in\mathbb{N}^*$ et $U,V\in\mathbb{Z}[X]$ tels que $PU+QV=a$. On a donc, pour tout $n\in\mathbb{N}$, $P(n)\wedge Q(n)\mid a$. On constate que $a$ convient pour période :

$$P(n+a)=\sum_{k=0}^{r}p_k(n+a)^k=P(n)+ab_n$$
$$Q(n+a)=Q(n)+ac_n$$

où $b_n,c_n$ sont des entiers (il suffit de développer). Par une remarque précédente, on a $P(n)\wedge Q(n)\mid P(n+a)\wedge Q(n+a)$ et si $d\mid P(n+a)\wedge Q(n+a)\mid a$, on a, par combinaison, $d\mid P(n),Q(n)$ i.e $d\mid P(n)\wedge Q(n)$.

## 6.10 Stabilité du cercle (Oral X, Mines 2015)

Trouver les polynômes $P\in\mathbb{C}[X]$ tels que $P(\mathbb{U})\subset\mathbb{U}$.

***Correction:*** (d'après Zak)

On a donc :

$$\forall x\in\mathbb{R}\qquad |P(e^{ix})|^2=1=P(e^{ix})\overline{P(e^{ix})}\ .$$

En dérivant, il vient donc :

$$\forall x\in\mathbb{R}\qquad ie^{ix}P'(e^{ix})\overline{P(e^{ix})}+P(e^{ix})\overline{ie^{ix}P'(e^{ix})}=0\ .$$

i.e

$$\forall x\in\mathbb{R}\qquad e^{2ix}\frac{P'(e^{ix})}{P(e^{ix})}=\overline{[\frac{P'(e^{ix})}{P(e^{ix})}]}\ .$$

Or, si $P = \lambda \prod_{k=1}^{n} X - z_i$, on a $\frac{P'(X)}{P(X)} = \sum_{k=1}^{n} \frac{1}{X - z_i}$. Ce qui précède se réécrit donc :

$$\forall x \in \mathbb{R} \qquad e^{2ix} \frac{P'(^{ix})}{P(e^{ix})} = \sum_{k=1} \frac{1}{e^{-ix} - \overline{z_i}} \ .$$

On en déduit :

$$X^2 \frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{\frac{1}{X} - \overline{z_i}}$$

soit

$$XP' \prod_{k=1}^{n} 1 - X\overline{z_i} = P \sum_{k=1}^{n} \prod_{j \neq i} 1 - X\overline{z_i} \ .$$

Ainsi, 0 est racine de $P$ : il existe $Q \in \mathbb{C}[X]$ tel que $P = XQ$. De plus, $Q$ vérifie aussi $Q(\mathbb{U}) \subset \mathbb{U}$. On conclut par récurrence sur le degré que $P = e^{i\theta} X^n$.

## 6.11 Algèbre monogène (Tosel)

Soient $\mathbb{A}_1, ...\mathbb{A}_r$ des $\mathbb{K}$-algèbres monogènes et de dimension finie. On suppose que $\mathbb{K}$ est infini. Montrer que $\mathbb{A}_1 \times ... \times \mathbb{A}_r$ est également monogène.

***Correction:*** Remarquons que, étant donnée $\mathbb{A}$ est une $\mathbb{K}$-algèbre de dimension finie, on a $\mathbb{A}$ monogène ss'il existe $x \in \mathbb{A}$ tel que $(1, x, ..., x^{dim(\mathbb{A}-1)})$ est une base (ce qui n'est le cas que si elle est libre) et cela arrive ss'il n'existe pas de polynôme de degré $< n$ annulant $x$ autre que le polynôme nul.

Aussi, si $(1, ..., x^n)$ est une base d'une algèbre alors il en est de même de $(1, \lambda x, ..., (\lambda x)^n)$ pour tout $\lambda \neq 0$.

On remarque également que, si $\mathbb{A} = \mathbb{K}[x]$ est de dimension finie non nulle, on peut toujours trouver $y$ tel que $\mathbb{A} = \mathbb{K}[y]$ et tel que le polynôme minimal de $y$ n'ait pas 0 pour racine. En effet, quitte à passer dans une extension de $\mathbb{K}$ qui scinde le polynome minimal $P(X) = \prod_{i=1}^{n} X - x_i$ de $x$, il suffit de prendre $x + t$ où $t \in \mathbb{K}$ vérifie $x_i + t \neq 0$ pour tout $i$ (existe car $\mathbb{K}$ est infini et qu'il n'y a qu'un nombre fini de $t \in \mathbb{K}$ tel qu'il existe $i$ vérifient $x_i + t = 0$).

Soient $x_1, ..., x_r$ tels que $\mathbb{A}_i = \mathbb{K}[x_i]$. On pose $dim(\mathbb{A}_1) = n_i$. Par ce qui précède, on sait qu'il existe des scalaires tels que

$$x_i^{n_i} = \sum_{k=0}^{n_i - 1} p_{k,i} x_i^k.$$

On pose $P_i = X^n - \sum_{k=0}^{n-1} p_{k,i} X^k$ . On a $(\lambda x_i)^{n_i} = \lambda^{n_i} P_i(\frac{1}{\lambda}(\lambda x_i))$ et on peut même supposer $p_{0,i} \neq 0$, chose que l'on fait par la suite.

De plus, il existe $\lambda$ tel que les $P_i(\frac{1}{\lambda} X)$ soient deux à deux premier entre eux : quitte à passer sans un surcorps de $\mathbb{K}$ dans lequel les $P_i$ sont scindés,

on est amenés à montrer que les $P_i(\frac{1}{\lambda}X)$ n'ont pas de racine en commun pour un certain $\lambda$ ($pgcd_{\mathbb{K}}(A,B) = pgcd_{\mathbb{L}}(A,B)$ si $\mathbb{L}$ est un surcorps de $\mathbb{K}$ et que $A, B \in \mathbb{K}[X]$). Ce $\lambda$ existe car, en notant $z_{1,i}...z_{n_i,i}$ les racines de $P_i$, pour tout $i$ il n'y a qu'un nombre fini de $\lambda$ qui envoient un $\lambda z_{l,i}$ sur un des $z_{k,j}$ puisque aucune des racines n'est nulle par hypothèse sur les $p_{0,i}$

On se donne un tel $\lambda$. On pose $R_i = \lambda^{n_i} P_i(\frac{1}{\lambda}X)$ et $y_i = \lambda x_i$. On vérifie que l'on a $\mathbb{A}_1 \times ... \times \mathbb{A}_r = \mathbb{K}[(y_1, ..., y_r)]$ : si $M \in \mathbb{K}[X]$ vérifie $M((y_1, ..., y_r)) = 0$ alors on a $M(y_i) = 0$ pour tout $i$ donc $R_i \mid M$ i.e $\prod_{i=1}^{r} R_i = ppcm(R_1, ..., R_r) \mid M$ d'où $deg(M) \geq \sum_{i=1}^{r} n_i$. Il s'ensuit que $(1, ..., (y_1^{n-1}, ..., y_r^{n-1}))$ est libre avec $n = \sum_{i=1}^{r} n_i$.

## 6.12 Polynômes divisibles par leur dérivée

1- Trouver les $P \in \mathbb{C}[X]$ tels que $P'$ divise $P$.

2- (Oral ENS) Déterminer les $P \in \mathbb{C}[X]$ tels qu'il existe $p, q \in \mathbb{N}^*$ tels que $(P')^q$ divise $P^p$.

## 6.13 Polynômes à coefficients dans $\{-1; 0; 1\}$

On souhaite décrire l'ensemble des polynômes scindés sur $\mathbb{R}$ et à coefficients dans $\{-1; 0; 1\}$. On note $E$ cet ensemble.

1- Montrer que l'on a, pour tout $x_1, ..., x_n \in \mathbb{R}^*$ $\sum_{1 \leq i,j \leq n} \frac{x_i^2}{x_j^2} \geq n^2$.

2- Conclure en remarquant que l'on peut étudier les polynômes de $E$ non-divisible par $X$.

## 6.14 Autour de l'indicatrice d'Euler (moi)

Montrer que l'on a $\sum_{\substack{k \in [\![1,n]\!] \\ k \wedge n = 1}} k/n \in \mathbb{Z}$.

***Indication:*** On pourra regarder le terme constant que $n^{eme}$ polynôme cyclotomique.

## 6.15 Groupe de torsion (Tosel)

1- Montrer que $\varphi(n) \xrightarrow[n \to \infty]{} \infty$ où $\varphi$ désigne l'indicatrice d'Euler.

2-Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}$. Déduire de la question précédente que $Tor(\mathbb{K}^*)$ est fini.

***Correction:*** 1- Il est bien connu que si $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^{N} p_i^{\alpha_i - 1}(p_i - 1)$. On suppose, sans perte de généralité, la famille $(p_i)$ croissante. Pour tout $i > 1$, on a $p_i - 1 \geq p_{i-1}$, d'où $\varphi(n) \geq \frac{n}{p_N}$. Alors, si l'on fixe $M > 0$, pour tout $n \geq M^2$, on a $\varphi(n) \geq M$. En effet (on reprend les notations précédentes), soit

on a $p_N \leq M$, dans quel cas l'inégalité donnée précédemment conclut, soit on a $p_N > M$ d'où $\varphi(n) \geq p_N - 1 \geq M$.

*Autre démonstration :*

On pose $d = \lfloor M \rfloor$. Soient $q_1 < ... < q_{d+1}$ les $d+1$ premiers nombres premiers strictement plus grands que $d+1$. Soit $n > q_{d+1}$.

Si $n$ est premier avec tous les $q_i$, alors on a $\varphi(n) >= d+1 > M$ par définition de $\varphi$.

Sinon, il existe $i$ tel que $q_i$ divise $n$ et on a donc $\varphi(n) \geq \varphi(q_i) \geq q_i - 1 > M$.

2- On note $\mathbb{K}_n = \{x \in \mathbb{K}^* : o(x) = n\}$, où $o(x)$ est l'ordre de $x$. Remarquons que $\mathbb{K}_n$ est fini car ses éléments sont racines de $X^n - 1$. Si $Tor(\mathbb{K}^*)$ était infini, il existerait une extractrice $f$ telle qu'il existe $x_{f(n)} \in \mathbb{K}_{f(n)}$ pour tout $n$ (sinon, il n'y aurait qu'une quantité finie de $K_n$ non vide et $Tor(\mathbb{K}^*)$ serait fini en tant qu'union finie d'ensembles finis). Un travail classique sur les polynômes cyclotomiques montre que $x_{f(n)}$ est de degré $\varphi(f(n))$. Par la question 1, on peut donc trouver un élément $x_{f(n_0)}$ de degré strictement plus grand que $[\mathbb{K} : \mathbb{Q}]$, absurde.

## 6.16 Généralisation d'un résultat d'irréductibilité (moi)

Il est bien connu que si l'on se donne un corps $\mathbb{K}$ de caractéristique $p$ et $x \in \mathbb{K}$ tel que $x$ n'ait pas de racine $p^{eme}$ dans $\mathbb{K}$ alors $X^p - x$ est irréductible sur $\mathbb{K}$.

Soit $\mathbb{L}/\mathbb{K}$ une extension, les deux corps étant de caractéristique quelconque et soit $p$ premier. On se donne $Q \in \mathbb{L}[X]$ tel que $Q$ soit unitaire, irréductible sur $\mathbb{L}[X]$, $Q \notin \mathbb{K}[X]$ et $Q^p \in \mathbb{K}[X]$. Montrer que $Q^p$ est irréductible sur $\mathbb{K}[X]$. Expliquer en quoi cela est une généralisation du résultat mentionné plus haut.

***Correction:*** Commençons par montrer qu'il n'existe pas $0 < k < p$ tel que $Q^k \in \mathbb{K}[X]$. Si on pouvait se donner un tel $k$, par Bezout, on pourrait trouver $u, v$ entiers tels que $ku + pv = 1$. Ainsi, on aurait $Q = (Q^k)^u (Q^p)^v \in \mathbb{K}(X)$. Or, si $Q = A/B$ avec $A, B \in \mathbb{K}[X]$, alors on a $BQ = A$ et $Q$ serait donc dans $\mathbb{K}[X]$ en tant que quotient dans la division euclidienne de $A$ par $B$.

Montrons ce qui nous intéressait initialement. Si $Q^p = R_1 R_2$ de façon non triviale dans $\mathbb{K}[X]$ avec $R_1$ et $R_2$ unitaires, on aurait, en remarquant que $Q...Q$ est la décomposition en produit d'irréductibles de $Q^p$ dans $\mathbb{L}[X]$, $R_1 = Q^k$ pour un certain $0 < k < p$, absurde par la discussion qui précède.

Pour la généralisation, il suffit de se donner un surcorps dans lequel $x$ admet une racine $p^{eme}$ disons $z$ et de regarder $Q = X - z$ (il suffit de scinder, et même de simplement trouver un corps de rupture, ce qui est faisable à la main, de $X^p - x = (X - z)^p$).

## 6.17 Nombres de Salem (Tosel)

Un nombre de Salem est un entier algébrique $x$ (irrationnel) vérifiant $x \in ]1; +\infty[$ et tel que toutes les racines de $\pi_x$ autres que $x$ ($\pi_x \in \mathbb{Z}[X]$ désigne le

polynôme minimal de $x$ sur $\mathbb{Q}$) soient de module plus petit que 1 mais qu'il en existe au moins une de module exactement 1.

1- Pour un tel $x$, montrer que $\pi_x$ est un polynôme réciproque et que toutes les racines différentes de $x$ et $\frac{1}{x}$ sont de module 1.

2- Montrer que le degré de $x$ est un entier pair plus grand que 4.

***Correction:*** 1- On note $n$ le degré de $x$ et $P = X^n \pi_x(\frac{1}{X})$. On a bien sûr $n > 1$, sans quoi les conditions de l'énoncé ne sauraient être vérifiées. Ainsi, "la" racine de module 1 dont il est question dans l'énoncé est forcément complexe non réelle (puisque ni 1 ni $-1$ n'est racine de $\pi_x$ par l'irréductibilité de ce dernier). En notant $z$ cette racine, on a $\overline{z} = \frac{1}{z}$ puisque $z$ est de module 1 et donc on a également

$$\pi_x(\frac{1}{z}) = \pi_x(\overline{z}) = \overline{\pi_x(z)} = 0.$$

Puisque $\pi_x = \pi_z$, on a $\pi_x \mid P$ i.e il existe $\lambda \in \mathbb{Z}$ tel que $P = \lambda \pi_x$. On en déduit que si $u$ est racine de $\pi_x$ alors $\frac{1}{u}$ aussi. En identifiant respectivement les dernier et premier coefficients dans la relation $P = \lambda \pi_x$, on obtient $\pi_x(0) = \lambda$ et $1 = \lambda \pi_x(0)$. Ainsi, on a $|\pi_x(0)| = 1$ et en écrivant $\pi_x = (X - x)(X - \frac{1}{x}) \prod_{i=0}^{n-2} X - x_i$, on a donc $\prod_{i=0}^{n-2} |x_i| = 1$, d'où $|x_i| = 1$ (car $|x_i| \leq 1$).

2- D'après ce qui précède, les racines différentes de $x$ et $\frac{1}{x}$ ne sont pas réelles. En les regroupant par pair de conjugués, on voit donc que $n$ est pair. Il est facile de voir qu'il n'y aucun nombre de Salem de degré 2, ce qui conclut.

## 6.18 Nombres de Pisot

Montrer que tout corps de nombre réel $\mathbb{K}$ est engendré par un nombre de Pisot.

***Indication:*** On se servira du théorème de Minkowski avec la matrice $M = (\sigma(\alpha^j))_{\sigma,j}$ où $\sigma$ parcourt l'ensemble des $\mathbb{K} \to \overline{\mathbb{Q}}$ et $\alpha$ est un entier algébrique engendrant $\mathbb{K}$.

***Correction:*** On suit l'indication. Soit $D = |det(M)| \neq 0$. Soit $M$ tel que $M \frac{1}{2^{n-1}} > D$. On note $(e_i)$ la base canonique de $\mathbb{R}$. Par le théorème de Minkowski, le convexe $[-M, M] \times \prod_{i=1}^{n-1} [-1/2, 1/2]$ rencontre le réseau engendré par les $M(ei)$ ailleurs qu'en l'origine. Autrement dit, il existe $(u_i) \in \mathbb{Z}^n$ tel que pour tout $\sigma : \mathbb{K} \to \mathbb{C}$ qui n'est pas l'identité sur $\mathbb{K}$ on a $|\sum_{i=1}^{n} u_i \sigma(\alpha^i)| \leq 1/2$ et $\sum_{i=1}^{n} u_i \alpha^i \leq M$

## 6.19 Dénombrement des irréductibles dans $\mathbb{F}_q[X]$

Soient $p \in \mathbb{P}$, $n > 0$, $q = p^n$, $A(m,q)$ l'ensembles des irréductibles de degré $m$ de $\mathbb{F}_q[X]$ et $I(m,q)$ sont cardinal.

1- Montrer que l'on a $X^{q^m} - X = \prod_{d|m} \prod_{P \in A(d,q)} P(X)$.

***Indication:*** Raisonner avec les nombres algébriques.

2- Montrer que l'on a $I(m,q) = \frac{1}{m} \sum_{d|m} \mu(\frac{m}{d}) q^d$.

***Indication:*** On pourra se servir de l'exercice "Fonction de Möbius" de la section arithmétique.

3- En déduire $I(m,q) \underset{m \to \infty}{\sim} \frac{q^m}{m}$.

**Remarque:** En particulier, pour $m$ assez grand, on sait qu'il existe un irréductible de degré $m$ dans $\mathbb{F}_q[X]$. En fait, on peut montrer que pour tout $m$, $I(m,q) > 0$ en utilisant que les extensions de degré $m$ de $\mathbb{F}_q$ sont données par quotient de $\mathbb{F}_q[X]$ par un irréductibles de degré $m$.

## 6.20 Caractérisation des extensions finies séparables

Soit $\mathbb{L}/\mathbb{K}$ une extension algébrique séparable telle qu'il existe $M$ vérifiant $[\mathbb{K}[x] : \mathbb{K}] < M$ pour tout $x \in \mathbb{L}$. Montrer que $\mathbb{L}$ est une extension finie.

***Correction:*** Si, par l'absurde, $\mathbb{L}$ est une extension infinie, on sait construire $x_1, ..., x_n \in \mathbb{L}$ tels que $[\mathbb{K}[x_1, ..., x_n] : \mathbb{K}] > M$. Or, le théorème de l'élément primitif (qui s'applique bien ici) nous donne $x \in \mathbb{L}$ tel que $\mathbb{K}[x_1, ..., x_n] = \mathbb{K}[x]$ et on devrait donc avoir $[\mathbb{K}[x_1, ..., x_n] : \mathbb{K}] < M$, absurde.

## 6.21 Passage à un surcorps

Soient $\mathbb{L}/\mathbb{K}$ une extension normale et $P \in \mathbb{K}[X]$ un irréductible. Montrer que les facteurs irréductibles dans $\mathbb{L}[X]$ de $P$ ont tous même degré.

***Correction:*** On écrit $P = \prod_{i=1}^{r} P_i^{\alpha_i}$. On va montrer que $deg(P_1) = deg(P_2)$ et c'est pareil pour les autres. Remarquons que dans un surcorps algébriquement clos, les $P_i$ n'ont pas de racine commune (puisqu'ils sont des polynômes minimaux distincts).

Soient $x_1, x_2$ des racines de $P_1$ et $P_2$ respectivement, dans un surcorps de $\mathbb{L}$ $\Omega$ algébriquement clos. Puisque $P$ est le polynôme minimal sur $\mathbb{K}$ de $x_1$ et $x_2$, on peut trouver $\sigma$ un morphisme de corps qui laisse $\mathbb{K}$ inchangé et qui envoie $x_1$ sur $x_2$. On étend $\sigma$ à $\Omega$. On a alors $\sigma.P = P$ car $\mathbb{K}$ est inchangé par $\sigma$ et donc on a $\prod_{i=1}^{r} \sigma.P_i^{\alpha_i} = \prod_{i=1}^{r} P_i^{\alpha_i}$. Or, les $\sigma.P_i$ appartiennent à $\mathbb{L}[X]$ car $\mathbb{L}/\mathbb{K}$ est normale et ils sont irréductibles car les $P_i$ le sont. Par unicité de la décomposition en facteurs irréductibles, on a qu'il existe $k$ tel que $\sigma.P_1 = P_k$ (et $\alpha_1 = \alpha_k$). Forcément, on a $k = 2$ puisque $x_2$ est racine de $\sigma.P_1$, ce qui conclut.

# 7 Spectre d'un anneau

## 7.1 Le spectre de $\mathbb{Z}[X]$

Décrire les idéaux premiers de $\mathbb{Z}[X]$.

***Correction:*** Soit I un tel idéal. On considère $J = I\mathbb{Q}$ l'idéal engendré par $I$ dans $\mathbb{Q}[X]$. Remarquons d'abord que $J$ est également un idéal premier. On distingue maintenant plusieurs cas : soit $J = 0$ i.e. $I = 0$, soit $J =< P >$ avec $P \in \mathbb{Q}[X]$ irréductible, dans quel cas on peut toujours supposer $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Z}[X]$. Alors, on peut montrer que $I$ est l'idéal de $\mathbb{Z}[X]$ engendré par $P$. Dernier cas possible : $J = \mathbb{Q}[X]$, ce qui implique que $I$ contient un entier et comme $I$ est premier, ceci implique que $I$ contient un nombre premier $p$. Maintenant, soit on a $I =< p >$, soit il existe $Q \in I$ irréductible tel que $Q \notin< p >$. Considérons un tel $Q$ de degré minimal. Alors, $Q$ est irréductible modulo $p$, sans quoi on pourrait écrire $Q = pS + R_1R_2$ avec $S, R_1, R_2 \in \mathbb{Z}[X]$, $deg(R_1), deg(R_2) < deg(Q)$, si bien que l'on aurait $R_1R_2 \in I$ et le caractère premier donne qu'un $R_i$ appartient à $I$, ce qui vient contredire la définition de $Q$. Maintenant, on peut montrer que $< p, Q >$ est maximal dans $\mathbb{Z}[X]$, ce qui force $I =< p, Q >$ ou $I = \mathbb{Z}[X]$. En effet, on a $\mathbb{Z}[\mathbb{X}]/ < p, Q >\simeq \mathbb{F}_p[X]/ < \overline{Q} >$ qui est un corps puisque $\overline{Q}$ est irréductible.

## 7.2 Les idéaux maximaux de $\mathbb{K}[X_1, ..., X_n]$

Montrer que les idéaux maximaux de $\mathbb{K}[X_1, ..., X_n]$ sont de la forme $< f_1, ..., f_n >$ où les $f_i$ sont des polynômes irréductibles.

***Correction:*** Soit $I$ un idéal maximal. Par le théorème faible des zéros de Hilbert, $\mathbb{K}[X_1, ..., X_n]/I$ est une extension finie de $\mathbb{K}$. Ainsi, pour tout $i$, $\overline{X_i}$ est algébrique sur $\mathbb{K}$, c'est-à-dire qu'il existe $P_i \in \mathbb{K}[T] \setminus \{0\}$ tel que $P_i(X_i) \in I$. Comme $I$ est premier, on peut toujours supposer $P_i$ irréductible sur $\mathbb{K}[\overline{X_1}, ..., \overline{X_{i-1}}]$ (la barre signifie que l'on considère la classe modulo $I$), de sorte que par le théorème d'isomorphisme (comme dans l'exercice précédent), on montre que $< P_1(X_1), ..., P_n(X_n) >$ est maximal.

## 7.3 Les idéaux premiers filtrent

Lorsque $\mathbf{A}$ est un anneau intègre et $p$ un idéal premier de $\mathbf{A}$, $\mathbf{A}_p$ peut être vu comme un sous-anneau du corps des fractions de $\mathbf{A}$.

1- Montrer que, avec ce point de vue, on a

$$\mathbf{A} = \bigcap_{p \ premier} \mathbf{A}_p.$$

2- Soient $I, J$ deux idéaux de $\mathbf{A}$ tels que $I\mathbf{A}_p = J\mathbf{A}_p$ pour tout idéal premier $p$. Montrer que l'on a $I = J$.

***Correction:*** 1- On a déjà l'inclusion gauche-droite. Supposons par l'absurde qu'il existe $x \in \bigcap_{p \text{ premier}} \mathbf{A}_p \setminus \{\mathbf{A}\}$. Posons $m = \{a \in \mathbf{A} : ax \in \mathbf{A}\}$. Puisque l'on a $x \notin \mathbf{A}$, on constate que $m$ est un idéal propre de $\mathbf{A}$, de sorte qu'il existe un idéal premier propre $p$ tel que $m \subset p$. En particulier, on a $x \in \mathbf{A}_p$ donc il existe $y \in \mathbf{A}, z \notin p$ tels que $x = \frac{y}{z}$. Il s'ensuit que l'on a $zx = y \in \mathbf{A}$, donc, par définition de $m$, on a $z \in m \subset p$, absurde.

2- Par l'absurde, supposons qu'il existe $x \in I \setminus J$. Considérons $m = \{a \in \mathbf{A} : ax \in J\}$. On constate que $m$ est un idéal propre, de sorte qu'il existe un idéal premier propre $p$ tel que $m \subset p$. En particulier, on a $x \in J\mathbf{A}_p$ donc il existe $y \in J, z \notin p$ tels que $zx = y \in J$. Par définition de $m$, on a donc $z \in m \subset p$, absurde.

## 7.4 Finitude du spectre et dimension

1- Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre de dimension finie. Montrer que $Spec(\mathbb{A})$ est fini, de cardinal majoré par la dimension de $\mathbb{A}$.

2- Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre de type finie. Montrer que $Spec(\mathbb{A})$ est fini si et seulement si $\mathbb{A}$ est de dimension finie sur $\mathbb{K}$.

***Correction:*** 1- Commençons par remarquer que tout idéal premier propre de $\mathbb{A}$ est en fait maximal. Soit $p$ un idéal premier propre de $\mathbb{A}$. On constate que, puisque $\mathbb{A}$ est de dimension finie, tout élément de $\mathbb{A}$ est entier sur $\mathbb{K}$, si bien que $\mathbb{A}/p$ est une extension entière de $\mathbb{K}$. De plus, cette extension est intègre. Alors, $\mathbb{A}/p$ est un corps.

Notons $n = dim_{\mathbb{K}}(\mathbb{A})$. Par l'absurde, supposons que l'on a $p_1, ..., p_{n+1}$ des idéaux premiers deux à deux distincts. Alors, le théorème chinois s'applique et donne pour tout $1 \leq i \leq n+1$ un élément $x_i \in \mathbb{A}$ tel que $x_i \notin p_i$ et $x_i \in p_j$ pour tout $j \neq i$. Ensuite, par la théorie de la dimension, il existe $i$ tel que $x_i \in Vect(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$, ce qui est absurde puisqu'on a alors $x_i \in p_i$ (puisque $p_i$ est stable par combinaison linéaire).

On peut remarquer qu'on aurait pu conclure directement en prenant la dimension à l'arrivée et au départ de l'isomorphisme donné par le théorème chinois.

2- Par le lemme de normalisation de Noether, on a $y_1, ..., y_n \in \mathbb{A}$ transcendants (éventuellement, $n = 0$) tels que $\mathbb{A}$ soit une extension entière de $\mathbb{K}[y_1, ..., y_n]$. Avec le going up theorem, on montre alors que $Spec(\mathbb{K}[y_1, ..., y_n])$ est fini, ce qui implique $n = 0$ (sinon il y a une infinite de polynômes irréductibles et donc une infinité d'idéaux premiers) et $\mathbb{A}$ est une extension algébrique de $\mathbb{K}$. Cela conclut puisque $\mathbb{A}$ est de type fini (chaque générateur est algébrique sur $\mathbb{K}$ donc $\mathbb{A}$ est de dimension finie).

## 7.5 Autour des idéaux premiers

Soient $\mathbb{A}$ un anneau, $p_1, ..., p_n$ des idéaux premiers et soit $I$ un idéal vérifiant de $\mathbb{A}$ vérifiant

$$I \subset \bigcup_{i=1}^{n} p_i.$$

Montrer qu'il existe $i \in [\![1; n]\!]$ tel que $I \subset p_i$.

***Correction:*** On raisonne par l'absurde. Quitte à prendre moins de $p_i$, on peut toujours supposer que l'on a

$$\forall K \subsetneq I, \quad I \not\subset \bigcup_{i \in K} p_i.$$

En particulier, on peut supposer que pour tout $j$, il existe $x_j \in p_j$ tel que $x_j \notin p_i$ pour tout $j \neq i$. Alors, il ne peut y avoir de $y \in I$ tel que $y \in p_i$ pour tout $i \neq n$ et $y \notin p_n$, sans quoi il existerait $i$ tel que $y + x_n \in p_i$ ; si $i \neq n$, on a, par différence, $x_n \in p_i$ et si $i = n$ on a $y \in p_n$ mais ces deux cas sont exclus. Autrement dit, on a

$$I \subset \bigcup_{i=1}^{n-1} p_i^c \cup p_n.$$

Ceci est absurde car on a $y := \prod_{j=1}^{n-1} x_j \in p_i \cap I$ pour tout $i \neq n$ de sorte que l'on a $y \in p_n$ et le caractère premier de $p_n$ donne alors un $i$ tel que $x_i \in p_n$, ce qui est exclu.

# 8 Théorie de Galois

## 8.1 Caractérisation de la normalité (stage)

Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Montrer qu'elle est normale si et seulement si pour tout $x \in \mathbb{L} \setminus \mathbb{K}$, il existe $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\sigma(x) \neq x$.

***Correction:*** Le sens direct est évident. Supposons la dernière propriété vérifiée et montrons que l'extension est normale. Supposons le contraire. On a alors $x \in \mathbb{L} \setminus \mathbb{K}$ ayant un de ses $\mathbb{K}$-conjugué qui n'appartient pas à $\mathbb{L}$. On note $x_1 = x, x_2, ..., x_r$ tous les $\mathbb{K}$-conjugués de $x$ qui appartiennent à $\mathbb{L}$. On a donc $\prod_{i=1}^{r} X - x_i \notin \mathbb{K}[X]$ puisque ce dernier polynôme s'annule en $x$ sans s'annuler en tous les $\mathbb{K}$-conjugués de $x$. Ainsi, il existe un polynôme symétrique élémentaire $E$ tel que $E(x_1, ..., x_r) \notin \mathbb{K}$. On a bien sûr $E(x_1, ..., x_r) \in \mathbb{L}$. Par hypothèse, il existe donc $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\sigma(E(x_1, ..., x_r)) \neq E(x_1, ..., x_r)$. Or, on a forcément $\sigma(E(x_1, ..., x_r)) = E(x_1, ..., x_r)$ puisque $E$ est symétrique et que $\sigma(\{x_1, ..., x_r\}) = \{x_1, ..., x_r\}$ car $\sigma$ est injective et parce que les $\sigma(x_i)$ sont des $\mathbb{K}$-conjugués de $x$ qui appartiennent à $\mathbb{L}$ puisque $\sigma$ est à valeurs dans $\mathbb{L}$.

**Remarque:** En fait, cela sert de définition pour la notion d'extension normale dans un cadre plus large qu'est celui de la théorie de Galois différentielle.

## 8.2 Nombre de corps de rupture

Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ un polynôme séparable irréductible. Soit $\Omega$ une clotûre algébrique de $\mathbb{K}$. Montrer que le nombre $N$ de corps de rupture de $P$ inclus dans $\Omega$ divise le degré de $P$.

***Correction:*** Soit $x$ une racine de $P$. On note $X$ l'ensemble des $\mathbb{K}$-conjugués de $x$. Comme le groupe de Galois absolu agit transitivement sur $X$, on montre que l'on a, pour tout $y \in X$, $|\operatorname{Gal}(\mathbb{K}(y)/\mathbb{K})| = |\operatorname{Gal}(\mathbb{K}(x)/\mathbb{K})|$. De plus, pour tout $y \in X$, le nombre de corps de rupture égaux à $\mathbb{K}(y)$ est $|\operatorname{Gal}(\mathbb{K}(y)/\mathbb{K})|$. En effet, si l'on a $y, z \in X$ tels que $\mathbb{K}(y) = \mathbb{K}(z)$ alors on a un $\sigma \in \operatorname{Gal}(P/\mathbb{K})$ (le groupe de Galois du corps de décomposition de $P$) tel que $\sigma(y) = z$ par la théorie. En fait, ce morphisme $\sigma$, restreint à $\mathbb{K}(y)$ définit alors un élément de $\operatorname{Gal}(\mathbb{K}(y)/\mathbb{K})$ et à $z$ on peut associer cet élément de $\operatorname{Gal}(\mathbb{K}(y)/\mathbb{K})$ de façon unique. Réciproquement, si à $\sigma \in \operatorname{Gal}(\mathbb{K}(y)/\mathbb{K})$ on associe également un tel $z$ par $\sigma(y) = z$.

Le lemme du berger appliqué à $y \in X \mapsto K(y)$ (qui a pour image l'ensemble des corps de rupture de $P$) donne $|X| = N|\operatorname{Gal}(\mathbb{K}(x)/\mathbb{K})|$, ce qui conclut puisque l'on a $|X| = \deg(P)$ car $P$ est irréductible et séparable.

## 8.3 Le groupe de Galois absolu

Montrer que $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est équipotent à $\mathbb{R}$.

***Correction:*** On sait injecter $\mathbb{R}$ dedans car on a $\mathbb{R} \simeq \{0;1\}^{\mathbb{N}} \simeq \{-1;1\}^{\mathbb{P}}$. En effet, on peut définir un automorphisme de corps $\mathbb{Q}(\sqrt{\mathbb{P}})$ de qui envoie $\sqrt{p}$ sur $\varepsilon_p\sqrt{p}$ pour toute suite $(\varepsilon_p)_{p\in\mathbb{P}} \in \{-1;1\}^{\mathbb{P}}$ et comme ces morphismes s'étendent à $\overline{\mathbb{Q}}$, on a ce qui a été annoncé.

Aussi, on peut injecter le groupe de Galois absolu dans $\mathbb{R} \simeq \mathbb{N}^{\mathbb{N}}$ (cf remarque qui suit la correction) puisque l'on a $\overline{\mathbb{Q}} \simeq \mathbb{N}$ et

$$\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \subset \overline{\mathbb{Q}}^{\overline{\mathbb{Q}}} \simeq \mathbb{N}^{\mathbb{N}} \simeq \mathbb{R}.$$

**Remarque:** Montrons que l'on a $\mathbb{R} \simeq \mathbb{N}^{\mathbb{N}}$. On a $\mathbb{R} \simeq \{0;1\}^{\mathbb{N}}$ et donc $\mathbb{R}$ s'injecte dans $\mathbb{N}^{\mathbb{N}}$. Ensuite, on a $\mathbb{R}^{\mathbb{N}} \simeq \{0;1\}^{\mathbb{N}\times\mathbb{N}} \simeq \{0;1\}^{\mathbb{N}} \simeq \mathbb{R}$. En particulier, $\mathbb{N}^{\mathbb{N}} \subset \mathbb{R}^{\mathbb{N}}$ s'injecte dans $\mathbb{R}$.

## 8.4 Encore autour du groupe de Galois absolu

Que dire de l'image d'un morphisme continu $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(\mathbb{C})$ ?

***Indication:*** Montrer que son image est finie.

***Correction:*** Notons $\varphi$ le morphisme dont il est question. Son noyau est un sous-groupe normal de $\operatorname{Gal}(\overline{Q}/Q)$. Aussi, le noyau est fermé comme image réciproque de $\{I_n\}$. En fait, le noyau est ouvert parce qu'il existe $r > 0$ tel que le groupe trivial soit le seul sous-groupe $H$ de $GL_n(\mathbb{C})$ tel que $H$ soit inclus dans $B(I_n, r)$ ; on prend alors un tel $r$ et on a $Ker(\varphi) = \varphi^{-1}(Im(\varphi) \cap B(I_n, r))$ ouvert. Finalement, par la correspondance galoisienne, $Ker(\varphi)$ s'écrit $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{K})$ où $\mathbb{K}$ est une extension galoisienne finie de $\mathbb{Q}$. Le théorème d'isomorphisme conclut.

**Remarque:** On peut faire quelque chose de similaire en remplaçant $GL_n(\mathbb{C})$ par un groupe de Lie.

## 8.5 Générateurs d'extensions (Tosel)

Soient $\mathbb{K}$ un corps, $\mathbb{L}_1/\mathbb{K}$, $\mathbb{L}_2/\mathbb{K}$ deux extensions galoisiennes finies.

1- On suppose que $\mathbb{K}$ est de caractéristique nulle et que l'on a $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$. Montrer que si $x$ (resp. $y$) est un élément primitif de $\mathbb{L}_1$ (resp. $\mathbb{L}_2$) alors $x+y$ est un élément primitif de $\mathbb{L}_1\mathbb{L}_2$.

***Indication:*** On pourra montrer que si $\sigma \in \mathrm{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ fixe $x+y$ alors $\sigma$ est l'identité.

2- On suppose que $[\mathbb{L}_1 : \mathbb{K}]$ est premier avec $[\mathbb{L}_2 : \mathbb{K}]$. Monter que si $x$ (resp. $y$) est un élément primitif de $\mathbb{L}_1$ (resp. $\mathbb{L}_2$) alors $xy$ est un élément primitif de $\mathbb{L}_1\mathbb{L}_2$.

## 8.6 Racines de l'unité sur un corps fini

Soit $q$ une puissance d'un nombre premier. Montrer que chaque facteur irréductible du $n^{eme}$ polynôme cyclotomique $\Phi_n$, vu comme un polynôme à coefficients dans $\mathbb{F}_q$, est de degré $r$, où $r$ désigne l'ordre de $q$ dans $\mathbb{Z}/n\mathbb{Z}^*$.

***Correction:*** Les conjugués de n'importe quel racine primitive $\omega$ sont donnés par le frobenius sur $\mathbb{F}_q$.

# 9 Corps complets

## 9.1 Les automorphismes de $\mathbb{Q}_p$

1- Soit $u \in \mathbb{Q}_p^*$. Montrer que l'on a :

$$u \in \mathbb{Z}_p^\times \Leftrightarrow \forall n \in \mathbb{N} : u \wedge p = 1, \quad u^{p-1} \in \mathbb{Q}_p^{*n}.$$

2- En déduire que si $\varphi$ est un endomorphisme de corps de $\mathbb{Q}_p$, alors on a :

$$\forall x \in \mathbb{Q}_p \quad v_p(\varphi(x)) = v_p(x).$$

3- En déduire $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$.

***Correction:*** 1- Supposons $u \in \mathbb{Z}_p$. Alors, on a $u^{p-1} = 1[p]$ de sorte qu'en appliquant le lemme de Hensel au polynôme $X^n - u^{p-1}$, on obtient ce que l'on voulait.

Réciproquement, écrivons $u = p^r v$ avec $r \in \mathbb{Z}$ et $v \in \mathbb{Z}_p^*$. Alors, par ce qui précède, $v$ admet aussi des racines $n^e$ lorsque $n \wedge p = 1$, si bien que $p^r$ admet à son tour des racines $n^e$. Si $r \neq 0$, en passant à la norme (ou à la valuation), on constate que $r \in \mathbb{Z}$ est un point d'accumulation, absurde.

2- On écrit $x = p^r u \in \mathbb{Q}_p^*$ avec les mêmes notations qu'avant. On a alors par la caractérisation de la q.1 $\varphi(u) \in \mathbb{Z}_p^\times$. Comme $\varphi$ fixe $\mathbb{Q}$, en particulier $p$ est fixe, ce qui conclut

3- Soit $\varphi \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$. On a $\varphi$ continue par ce qui précède (et même isométrique) et on a $\varphi_{|\mathbb{Q}} = id_{\mathbb{Q}}$. On en déduit $\varphi = id$ par densité de $\mathbb{Q}$ dans $\mathbb{Q}_p$.

## 9.2 Racines $n^e$ et Hensel

Soit $\mathbb{K}$ un corps $p$-adique. Montrer que, pour tout $n \wedge p = 1$, toutes les racines $n^e$ de $\mathbb{K}$ proviennent de relèvements de racines $n^e$ dans le corps résiduel $k_{\mathbb{K}}$ donnés par le lemme de Hensel.

En déduire que $\mathbb{K}$ a un nombre fini de racines de l'unité d'ordre non divisible par $p$.

***Correction:*** Soit $M = Card(k_{\mathbb{K}}) - 1$. Par le lemme de Hensel, on sait que $\mathbb{K}$ a une racine primitive $M^e$ de l'unité, de sorte que $\mathbb{K}$ a $M$ racines de l'unité (qui sont données par le lemme de Hensel). Supposons par l'absurde que $\mathbb{K}$ ait d'autres racines de l'unité d'ordre non divisible par $p$ que celles-ci. Soit $x$ une telle racine ; notons $n$ son ordre. On constate que, par le lemme de Hensel, il existe $y \in \mathbb{K}$ racine de l'unité d'ordre $r \in \mathbb{N}$, $r \wedge p = 1$ telle que $y = x$ dans $k_{\mathbb{K}}$. Comme on a $x \neq y$ par hypothèse, on peut écrire $X^{nr} - 1 = (X - x)(X - y)Q$ avec $Q \in R[X]$ où $R$ désigne l'anneau de valuation de $\mathbb{K}$. En réduisant, on trouve que $X^{nr} - 1$ n'est pas séparable dans $k_{\mathbb{K}}$, absurde (car $p$ ne divise pas $nr$).

## 9.3 Racines de l'unité

Soit $n$ une puissance d'un nombre premier $p$. Soit $\zeta_n$ une racine $n^e$ de l'unité. Montrer que $\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

***Indication:*** On pourra que le polynôme minimal de $\zeta_n$ est le même sur $\mathbb{Q}_p$ que sur $\mathbb{Q}$. Pour cela, on pourra appliquer le critère d'Eisenstein au polynôme en question composé avec $X + 1$.

## 9.4 Extension non ramifiée

Montrer qu'une extension $\mathbb{L}/\mathbb{K}$ est non-ramifiée si et seulement si les complétés sont non-ramifiés en tout idéal premier $p$ de $\mathcal{O}_{\mathbb{K}}$.

# 10 Théorie des groupes - Algèbre

## 10.1 2 classes de conjugaison

Trouver tous les groupes qui sont tels que :
-il existe exactement deux classes de conjugaison
-il existe un élément non trivial d'ordre fini .

***Correction:*** Notons $G$ un tel groupe. Remarquons que l'on a alors $G = \{1\} \cup G.x$ où $G.x$ désigne la classe de $x$ (puisque 1 est seul dans sa classe) et $x$ un élément non trivial d'ordre fini (car les conjugués ont tous mêmes ordre).

On peut remarquer que si l'on suppose $G$ fini, on a $|G| = |G.x||G_x| = 1+|G.x|$ où $G_x$ est le stabilisateur de $x$. On en déduit $|G.x| = 1$ et donc $G = \mathbb{Z}/2\mathbb{Z}$.

De façon générale, on sait quand même que tous les éléments non nuls de $G$ ont même ordre (car ils sont tous conjugués à $x$) et que cet ordre est premier :

si $o(x) = pq = n$ alors $x^p$ est d'ordre $\frac{n}{p}$ donc $p = 1$ ou $n$ par ce qui précède. Notons le $p$. On a donc $x^{p-1} = gxg^{-1}$ pour un certain $g \in G$. On en déduit $x = g^p x g^{-p} = x^{(p-1)^p}$ et donc $p|(p-1)^p - 1$. Ainsi, par le petit théorème de Fermat, on a $p = 2$ donc $G$ est commutatif (exercice classique) et finalement $G = \mathbb{Z}/2\mathbb{Z}$.

## 10.2 Un sous-groupe distingué

Soient $G$ un groupe fini, $H$ un sous-groupe distingué de $G$ et de cardinal $p$, ce dernier étant le plus petit diviseur premier de $Card(G)$. Montrer que l'on a $H \subset Z(G)$.

***Correction:*** On regarde l'action par conjugaison de $G$ sur $H$ (qui est bien définie puisque $H$ est normal) et on écrit $H =< h >$ (légitime car d'ordre premier). Par l'absurde, supposons $h \notin Z(G)$ (i.e pour tout $1 \leq k < p$, $Stab(h^k) \neq G$). On écrit l'équation aux classes et on se rend compte qu'il n'y a alors qu'une classe car, si $|Stab(h)| \neq |G|/p$ alors $|Stab(h)| < |G|/p$ (car $p$ est le plus petit diviseur premier de $Card(G)$) puis
$|H| = p = \sum_i [G : Stab(x_i)] > p$. Ainsi, on a $H = Orb(h)$. En particulier, puisque $1 \in H$, il existe $g \in G$ tel que $1 = ghg^{-1}$, absurde.

## 10.3 Nombre fini de sous-groupe

Caractériser les groupes n'ayant qu'un nombre fini de sous-groupes.

***Indication:*** On commencera par montrer que tous éléments sont d'ordre fini.

***Correction:*** On note $n$ le nombre de sous-groupes. Pour voir l'indication, on regarde $< x >, < x^2 >, ....$ On conclut par l'absurde : si $G$ infini, on peut construire une suite $(x_i)$ telle que $x_{i+1} \in G \setminus \bigcup_{j<i} < x_j >$. Principe des tiroirs donne $< x_i >=< x_j >$ pour $i \neq j$, absurde.

## 10.4 Groupes non isomorphes

Soit $(K, +, \times)$ un corps. Montrer que les groupes $(K, +)$ et $(K^*, \times)$ ne sont pas isomorphes.

## 10.5 Un peu sur le même thème

Si $\mathbb{K}$ est un corps fini ou $\mathbb{Q}$ et $f$ un morphisme de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \times)$, montrer que l'on a forcément $f(x) = 1$ pour tout $x$.

## 10.6 Ordre dans le groupe quotient (Josette Calais, Elements de théorie des groupes)

Soit $G$ un groupe. On suppose qu'il existe un sous-groupe $H$ normal dans $G$ et d'ordre fini $m$. Si $pgcd(n,m)=1$, montrer que l'on a l'implication :

$$o(\bar{x})=n \implies \exists y \in \bar{x} : o(y)=n.$$

Ceci montre, qu'a priori, $o(x)=n \implies o(\bar{x})=n$ n'est pas toujours une équivalence.

***Indication:*** On pourra chercher à montrer que $x^n$ admet une racine $n^{eme}$ dans $H$.

***Correction:*** Par hypothèse, on $x^n \in H$. Notons $h=x^n$ et $p=o(h)$. Puisque $p|m$ (par Lagrange), on a également $pgcd(p,n)=1$. Ainsi, par Bezout, il existe $u,v$ tels que $nu+pv=1$. On en déduit $h=h^{nu+pv}=(h^u)^n$.

On pose $s=h^u \in H$ qui est donc une racine $n^{eme}$ de $x^n$. Puisque $h=x^n$, $h$ et $x$ commutent et il en est alors de même pour $s$. Par conséquent,$xs^{-1}$ est un élément qui prouve ce que l'on voulait.

## 10.7 Sous-groupes de $S_n$

Soit $n \geq 5$. 1- Soit $H$ un sous-groupe de $S_n$ d'indice $n$. Montrer que l'on a $H \simeq S_{n-1}$.

2- Montrer qu'il n'existe pas de sous groupe de $S_n$ d'indice $2<k<n$.

***Indication:*** Pour ces deux questions, on pourra considérer une action de $S_n$ sur $S_n/H$.

3- Montrer que $\mathcal{A}_n$ est le seul groupe d'indice 2.

***Correction:*** 1- On considère l'action de groupe donnée par $g.\overline{x}=\overline{gx}$ pour tout $g,x \in S_n$. On note $\phi : S_n \to S_{S_n/H}$ le morphisme associé. Puisque $n>4$, on a $Ker(\phi)=S_n$ ou $A_n$ ou $\{id\}$. Or, on a $Ker(\phi) \subset H$ (prendre $x=id$) donc on a $|Ker(\phi)| \leq |H|=(n-1)!$. Ainsi, on a forcément $Ker(\phi)=\{id\}$.

Ainsi, via $\phi$, $H$ est isomorphe à un sous groupe de $S_{S_n/H} =\simeq S_n$ qui laisse stable un même élément (il s'agit de $x=id$) ce qui conclut.

2- Même chose ?

3- Si $H$ est d'indice 2, on a un morphisme de projection (non trivial) $\mathcal{S}_n \to \mathbb{Z}/2\mathbb{Z}$ de noyau $H$. Les transpositions ont même image car elles sont conjuguées et puisqu'elles engendrent $\mathcal{S}_n$, leur image est non triviale. Autrement dit, le morphisme que l'on s'est donné correspond à la signature et donc $H$ est bien le noyau de la signature.

## 10.8 Sous-groupes de $(\mathbb{R},+)$

Soit $G$ un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$. On pose $\alpha=\inf G \cap \mathbb{R}_+^*$.

1- Si $\alpha>0$, montrer que l'on a $G=\alpha\mathbb{Z}$.

2- Sinon, montrer que $G$ est dense dans $\mathbb{R}$.

## 10.9 Partie stable pour l'addition

Soit $P \subset \mathbb{N}$ stable pour l'addition, non vide.

1- On suppose que le *pgcd* des éléments de $P$ vaut 1. Justifier qu'il existe $p_1, ..., p_n \in P$ tels que $p_1 \wedge ... \wedge p_n = 1$.

2- Dans le cas général, montrer qu'il existe $n_0, d$ tel que $P \cap [\![n_0, \infty[\![ = d\mathbb{N} \cap [\![n_0, \infty[\![$.

***Indication:*** Pour la question 2, on se ramènera au cas de la q.1 avant de montrer qu'il existe $m \in P$ tel que $m + 1 \in P$.

***Correction:*** 1- Supposons, par l'absurde, que ce ne soit pas le cas. On pose $P = \{p_i : i \leq 1\}$ et $u_n = p_1 \wedge ... \wedge p_n \geq 2$ par hypothèse. De plus, on remarque de $u_n$ est décroissante. Ainsi, elle converge vers $d \geq 2$ et est donc stationnaire. Ainsi, $d$ divise tous les éléments de $P$, absurde.

2- On se ramène au cas de la q.1 en divisant par le *pgcd* des éléments de $P$. Dans ce cas, soient $p_1, ..., p_n \in P$ et $a_1, ..., a_n \in \mathbb{Z}$ tels que $p_1 a_1 + ... + p_n a_n = 1$. On a $m = (\max_{1 \leq i \leq n} |a_i| + 1)(p_1 + ... + p_n) \in P$ et $m + 1 \in P$.

$d$ est en fait le *pgcd* de $P$ qui, ici, vaut 1. Ainsi, on veut que tous les entiers appartiennent à $P$ à partir d'un certain rang. Soit $n \in \mathbb{N}$. Par division euclidienne, on peut écrire $n = mk + r = m(k - r) + r(m + 1)$ et on conclut que $n \in P$ dès que $k \geq m - 1$ i.e $\leq m(m - 1) = n_0$.

## 10.10 Groupes des automorphismes trivial

Que dire d'un groupe $(G, .)$ dont le groupe des automorphismes est réduit à $id$ ?

***Indication:*** Le seul groupe à vérifier cette propriété est $\mathbb{Z}/2\mathbb{Z}$ si l'on oublie le groupe trivial.

## 10.11 Les sous-groupes finis de $\mathbb{SL}_n(\mathbb{Z})$ (Oral ENS Rennes magistère)

1- Soit $p \in \mathbb{P}$, $p \geqslant 3$. On pose $\pi_p : \ SL_2(\mathbb{Z}) \ \rightarrow \ SL_2(Z/p\mathbb{Z})$ le morphisme de réduction canonique. Montrer que tous les éléments de $Ker(\pi_p) - \{I_2\}$ sont d'ordre infini.

***Indication:*** Le cas $p \geq 5$ est plus facile à traiter.

2- Soit $G$ un sous-groupe fini de $SL_2(Z)$. Montrer que $|G| \leq 24$.

3- Plus généralement, montrer qu'il existe $c(n)$ vérifiant $|G| \leq c(n)$ pour tout sous-groupe fini de $SL_n(Z)$.

***Correction:*** 1- Soit $M \in Ker(\pi_p)$ d'ordre fini. Montrons que l'on a $M = I_2$. Par définition, il existe $n \in \mathbb{N}^*$ tel que $M^n = I_2$. Puisque $X^n - 1$ est scindé à racine simple sur $\mathbb{C}$ (racines de l'unité), on peut diagonaliser $M$ : il existe $P \in GL_2(\mathbb{C})$ telle que $M = P \begin{pmatrix} e^{2ik\pi/n} & 0 \\ 0 & e^{2iq\pi/n} \end{pmatrix} P^{-1}$. Puisque $det(M) = 1$, on

peut écrire $M = P\begin{pmatrix} e^{2ik\pi/n} & 0 \\ 0 & e^{-2ik\pi/n} \end{pmatrix} P^{-1}$. De plus, on a $M = I_2\ [p]$ donc $tr(M) = 2[p]$ et $tr(M) = e^{2ik\pi/n} + e^{-2ik\pi/n} = 2cos(2ik\pi/n) \in \mathbb{Z} \cap [-2; 2]$. Ainsi, on a $cos(2ik\pi/n) \in \left\{\pm\frac{1}{2}; \pm 1; 0\right\}$.

Suivons l'indication : on suppose $p \geq 5$. Alors, on vérifie que l'on a forcément $cos(2ik\pi/n) = 1$ donc $e^{2ik\pi/n} = 1$ donc $M$ est semblable $I_2$ et lui est ainsi égal.

Pour ce qui est du cas $p = 3$, deux choses sont a priori possibles : soit il se passe la même chose que précédemment, soit $cos(2ik\pi/n) = \frac{-1}{2}$. En notant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a donc $tr(M) = a+d = -1$ et $det(M) = ad-bc = 1$. On trouve donc, en injectant la première équation dans la seconde, $a^2 + a + bc + 1 = 0$ c'est à dire que $a$ est solution réelle d'un polynôme de degré 2. Par le discriminant, on obtient que $1 - 4(bc + 1) \geq 0$ et $a = \frac{-1 \pm \sqrt{1 - 4(bc+1)}}{2}$. Ainsi, il existe $z \in \mathbb{Z}$ tel que $1 - 4(bc + 1) = z^2$. En passant modulo $p = 3$ et en remarquant que 1 est le seul carré dans $\mathbb{Z}/3\mathbb{Z}$, on obtient $1 - 4 = 1[3]$, absurde (3 divise $b$ et $c$ puisque $M = I_2\ [p]$).

2- Il suffit d'utiliser ce qui précède : un sous-groupe fini de $SL_2(\mathbb{Z})$ s'injecte dans $SL2(\mathbb{Z}/3\mathbb{Z})$ par le morphisme précédent ($p = 3$). En effet, puisque $G$ est fini, tous ses éléments sont d'ordre fini. Il nous reste à démontrer que $Card(SL2(\mathbb{Z}/3\mathbb{Z})) = 24$. Se reporter à l'exercice "cardinal de $Gl_n(\mathbb{F}_q)$ et $SL_n(\mathbb{F}_q)$ de la section "ensemble / dénombrement".

3- On procède comme en q.1. En diagonalisant, on remarque que $|tr(M)| \leq n$. Or, on a $tr(M) = n[p]$. Il nous suffit donc de prendre $p > 2n$ pour conclure facilement que $M = I_n$.

**Remarque:** La question 1 se généralise en fait à $n$ quelconque. Si $M \in Ker(\pi_p)$ alors $M = I_n + pA$ avec $A$ entière. On a alors $\chi_M = p^n \chi_A((X-1)/p)$. Si l'on note $\lambda_i$ les vp de $M$ (qui sont forcément des racines de l'unité), on a $p^n|\chi_A(0)| = |\chi_M(1)| = |\prod_{k=1}^{n} 1 - \lambda_i| \leq 2^n$. Comme on a $p \geq 3$ et que l'on travaille avec des entiers, on a forcément $\chi_A(0) = 0$. On a donc aussi $\chi_M(1) = 0$. On conclut par récurrence parce que l'on se retrouve maintenant avec une equation de la forme $P(X) = p^{n-1}Q(X - 1/p)$ avec des polynomes entiers de degré $n - 1$.

## 10.12 Les sous-groupes finis de $\mathbb{GL}_n(\mathbb{Z})$

1- Déduire de ce qui précède qu'un sous groupe fini de $GL_n(\mathbb{Z})$ a un cardinal inférieur ou égal à 48.

2- On peut montrer que le cas =48 n'arrive jamais, cf sujet agreg https ://agreg.org/data/uploads/sujets/MG

## 10.13 Produit cartésien et générateur

Soient $G$, $H$ deux groupes tels que $G \times H$ soit monogène. Montrer que soit $G$ ou $H$ est réduit à $\{0\}$ (et l'autre est monogène), soit $G$ et $H$ sont cycliques.

***Correction:*** Supposons que la 1ère situation ne soit pas réalisée. Notons $\alpha = (\alpha_1, \alpha_2)$ un générateur de $G \times H$ et notons les groupes multiplicativement. Soient $h_1 \neq h_2$ deux éléments de $H$. Il existe $k_1, k_2$ tels que $\alpha^{k_1} = (1, h_1)$ et $\alpha^{k_2} = (1, h_2)$. Puisque $(1, h_1) \neq (1, h_2)$, on a $k_1 \neq k_2$. On a également $1 = \alpha_1^{k_1} = \alpha_1^{k_2}$. Ainsi, $\alpha_1$ est d'ordre fini et donc $G$ est cyclique car engendré par $\alpha_1$.

De même pour $H$ en inversant les rôles.

## 10.14 $G$ isomorphe $H \times G/H$ (DM Troesch)

Soient $G$ un groupe abélien fini, $h \in G$ un élément d'ordre maximal. On note $H =< h >$.

1- Montrer que l'ordre de tout élément de $G$ divise $o(h)$.

2- Montrer que $G$ est isomorphe à $H \times G/H$.

***Indication:*** On pourra considérer un élément maximal de l'ensemble des couples $(f, K)$ où $f : K \to H$ est un morphisme prolongeant $id_H$ et $K$ un sous-groupe de $G$ (pour l'ordre de prolongement et d'inclusion).

***Correction:*** 2- Déjà, on peut bien appliquer le lemme de Zorn et trouver un élément maximal comme indiqué.

Ensuite, donnons-nous un élément maximal $(f, K)$ et supposons par l'absurde $K \neq G$. Soit $x \notin K$. On va prolonger $f$ au sous-groupe engendré par $x$ et $K$. Pour cela, il suffit de déterminer $g(x)$ si $g$ est un tel prolongement. On note $n > 0$ le plus petit entier qui vérifie $x^n \in K$ (qui existe puisque $x^{o(x)} = 1 \in K$).

On a forcément $g(x)^n = f(x^n) = h^k$ pour un certain $k$. Ainsi, $g(x)$ est une racine $n^{eme}$ de $h^k$. On peut maintenant construire $g(x)$. On note toujours $f(x^n) = h^k$. Remarquons que l'on a facilement $n|o(x)|Card(H)$. La première division vient de la définition de $n$ et que du fait que l'on a $x^{o(x)} \in K$. La deuxième vient de la q.1. Aussi, en passant $f(x^n) = h^k$ à la puissance $o(x)/n$, on obtient que $Card(H)$ divise $\frac{ko(x)}{n}$. Ce dernier est donc divisible par $o(x)$ i.e $\frac{k}{n}$ est entier. Il nous suffit de poser $g(x) = h^{k/n}$ pour prolonger naturellement $f$.

## 10.15 Autour de $Aut(G)$ (Eloan)

Soit $p \geq 3$ un nombre premier. Montrer qu'il n'existe pas de trouve $G$ tel que $Aut(G) \simeq \mathbb{Z}/p\mathbb{Z}$.

***Correction:*** On a $G$ abélien puisque $G/Z(G) \simeq Int(G) \leqslant Aut(G) \simeq \mathbb{Z}/p\mathbb{Z}$. Alors, $x \mapsto x^{-1}$ est soit un élément d'ordre 2, soit l'identité. Ca ne peut pas être un élément d'ordre 2 sans quoi on aurait $2|p$. C'est donc l'identité i.e. on a $x^2 = 1$ pour tout $x \in G$. Alors, $G$ est un $\mathbb{Z}/2\mathbb{Z}$-ev et on vérifie facilement que $Aut(G) = GL_{dim(G)}(\mathbb{F}_2)$ qui n'est jamais premier.

## 10.16 Contre-exemple à $G \times H \simeq G \times K$

Soient $G, H, K$ des groupes tels que $G \times H \simeq G \times K$. A-t-on forcément $H \simeq K$ ? ?

***Correction:*** Non ! Si l'on regarde $\mathbb{F}_p(X)$, il est connu que c'est un $\mathbb{F}_p(X^p)$-ev de dimension $p$. Ainsi, on a un morphisme de $\mathbb{F}_p(X^p)$-ev (et donc un morphisme de groupe) entre $\mathbb{F}_p(X)$ et $\mathbb{F}_p(X^p)^p$. Or, $A/B \in \mathbb{F}_p(X) \mapsto A(X^p)/B(X^p) \in F_p(X^p)$ est clairement un isomorphisme. On peut donc prendre $G = \mathbb{F}_p(X^p), H = \mathbb{F}_p(X^p)^{p-1}$ et $K = \{1\}$.

Moins bizarre : $G = \mathbb{Z}^{\mathbb{N}}, H = 1, K = \mathbb{Z}$.

## 10.17 Conjugaison et ordre (Eloan)

Soient $H$ un groupe, $a, b \in H$ de même ordre (potentiellement infini). Montrer qu'il existe un groupe $G$ tel que $H \leq G$ et tel que $a$ et $b$ soient conjugués dans $G$ dans chacun de ces cas :

1- $H$ fini

2- $H, G$ dénombrables, $H$ sans torsion.

***Correction:*** 1- Il suffit d'utiliser le plongement de Cayley qui permet de voir $H$ comme un sous-groupe de $S_{|H|}$. On pose $G = S_{|H|}$ et on utilise le fait que deux permutations sont conjuguées si et seulement si elles ont même nombre de $k$-cycles pour tout $k$, ce qui est effectivement vérifié ici puisque leur nombre est donné par l'ordre de $a$ et $b$.

## 10.18 Divers caractérisations du groupe de Prüfer (Eloan)

1- Décrire les groupes infini $G$ dont l'ensemble des sous-groupes est totalement ordonné (pour l'inclusion). Que dire si $G$ est fini ?

2- Décrire les groupes abéliens infinis $G$ dont l'intersection de tous les sous-groupes non nuls soit non triviale.

3- Décrire les groupes abéliens infinis $G$ dont les sous-groupes stricts sont tous finis.

***Correction:*** 1- Déjà, on peut remarquer qu'étant donné $a, b \in G$, on a par hypothèse $< a > \subset < b >$ ou l'inverse, i.e. $a$ est une puissance de $b$ ou l'inverse, ce à quoi on fera référence par "le fait clé".

Ensuite, tout $g \in G$ est d'ordre fini puisque $< g^2 > \subset < g^3 >$ donne un $k \in \mathbb{Z}$ tel que $g^{2-3k} = 1$ et on a $2 - 3k! = 0$ (on a quelque chose de similaire si l'on suppose $< g^3 > \subset < g^2 >$).

De plus, cet ordre est la puissance d'un nombre premier, sans quoi, en notant $p^a q^b m$ sont ordre (sous les hypothèses évidentes $a, b > 0$, $p, q \in \mathbb{P}$, $p \neq q$, $p, q \not| m$), les sous-groupes $< g^{p^a} >$ et $< g^{q^b} >$ (à cause du fait clé et du fait que $g^{p^a}$ a un ordre premier avec $p$, $g^{q^b}$ premier avec $q$).

En fait, on peut (maintenant) même dire qu'il existe $p \in \mathbb{P}$ tel que tout $g \in G$ soit d'ordre une puissance de $p$ à cause de ce qui précède et du fait clé.

Aussi, pour tout $k \in \mathbb{N}$, il existe au plus un sous-groupe de $G$ d'ordre $p^k$ car, si $H_1$ et $H_2$ sont deux tels sous-groupes, on a, par hypothèse, $H_1 \subset H_2$ ou l'inverse, puis égalité par cardinalité.

Alors, il y a une infinité de tel $k$, sans quoi $G$ serait fini puisque tout $g \in G$ appartient à $< g >$, qui est un sous-groupe d'ordre $p^{o(g)}$. En fait, à cause du théorème de structure, on peut même dire que tout sous-groupe d'ordre $p^k$ est engendré par un seul élément (sinon, toute pseudo-base de ce sous-groupe est de cardinal supérieur à 2 et donc on a en particulier deux éléments distincts qui constituent cette pseudo base engendrent des groupes qui sont incomparables).

Par conséquent, cette infinité de $k$ est en fait $\mathbb{N}$ tout entier. On peut donc écrire $G = \bigcup_{k\in\mathbb{N}} G_{p^k}$ où $G_{p^k}$ est le sous-groupe de $G$ d'ordre $p^k$.

Finalement, on constate qu'à isomorphisme près, les seuls groupes possibles sont les $\bigcup_{k\in\mathbb{N}} \mathbb{U}_{p^k}$ où $p \in \mathbb{P}$. On peut expliciter un isomorphisme entre $G = \bigcup_{k\in\mathbb{N}} G_{p^k}$ et $\bigcup_{k\in\mathbb{N}} \mathbb{U}_{p^k}$ où $p \in \mathbb{P}$ en notant $a_1 \in G$ un élément d'ordre $p$ et en construisant par récurrence $a_k$ comme racine $p^e$ de $a_{k-1}$ dans $G$. Il suffit maintenant de constater que

$$g \in G \mapsto exp(\frac{2i\pi k}{p^n}) \text{ si } g = a_n^k$$

est bien définie et définit effectivement un isomorphisme comme celui recherché.

Si $G$ est fini, on montre que $G$ est cyclique d'ordre une puissance d'un nombre premier et que cela est une condition suffisante.

2- Tout d'abord, tout $g \in G$ est d'ordre fini puisque $\bigcap_{n\in\mathbb{N}^*} n\mathbb{Z} = 0$.

Ensuite, puisque les $p$-Sylow de $G$, notés $S_p$, sont d'intersection triviale, il existe $p \in \mathbb{P}$ tel que $G = S_p$ (un $p$-Sylow est non-trivial à partir du moment où il existe un élément dont l'ordre est divisible par $p$).

Aussi, il n'existe qu'un seul sous-groupe d'ordre $p$ puisque si l'on se donne deux tels sous-groupes $H_1, H_2$, ils sont forcément cycliques, engendrés respectivement par des certains $a_1, a_2$. Alors, l'hypothèse $H_1 \cap H_2 \neq \{1\}$ donne $0 < j, k < p$ tels que $a_1^k = a_2^j$. Puisque l'on a $0 < k < p$, on a $k \wedge p = 1$, si bien qu'un couple de Bézout $(u, v)$ associé $(k, p)$ donne $a_1 = a_1^{ku} = a_2^{ju}$. On en déduit $H_1 =< a_1 > \subset < a_2 > = H_2$, puis l'égalité cherchée par cardinalité.

Remarquons également que tout sous-groupe fini est forcément cyclique à cause du théorème de structure.

Tâchons maintenant de montrer que tout élément admet une racine $p^e$. On note $f$ le morphisme "puissance $p$" (qui est bien un morphisme car $G$ est abélien). On veut donc montrer que l'on a $Im(f) = G$. Par l'absurde, supposons qu'il existe $a \notin Im(f)$. Soit $b \in G$. Par ce qui précède, il existe $c \in G$ tel que $< a, b >=< c >$. Il s'ensuit qu'il existe $k \in \mathbb{Z}$ tel que $a = c^k$ et on a $p \wedge k = 1$ puisque $a \notin Im(f)$. Ainsi, en utilisant l'astuce précédent avec le couple de Bézout, on trouve que l'on a $c \in < a >$ et de l'égalité $< a, b >=< c >$ on tire maintenant $b \in < a >$. On obtient finalement $G =< a >$, ce qui est absurde puisque $G$ est infini et que $a$ est d'ordre fini.

On peut donc construire une suite $(a_n) \in G^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $a_n$ est d'ordre $p^n$ et $a_{n+1}^p = a_n$. Montrons que l'on a $G =< a_n >_{n\in\mathbb{N}}$. Soit $b \in G$. On considère le plus petit $j \in \mathbb{N}^*$ tel que $b^j \in < a_n >_{n\in\mathbb{N}}$ (qui n'est rien d'autre que l'ordre de $b$ dans le groupe quotient). Remarquons que l'on a $< a_n >_{n\in\mathbb{N}} = \bigcup_{n\in\mathbb{N}} < a_n >$. Distinguons deux cas : soit $j \wedge p = 1$, dans quel cas l'astuce avec le couple de Bézout donne $b \in < a_n >_{n\in\mathbb{N}}$, soit $p \mid j$, si bien que l'on peut écrire $b^{pj'} = a_n^k = a_{n+1}^{pk}$ pour des certains $n, k$ (on pose $j = pj'$). Ainsi, on a $(b^{j'}a_{n+1}^{-k})^p = 1$ si bien que $b^{j'}a_{n+1}^{-k}$ est d'ordre 1 ou $p$, i.e. cet élément appartient à l'unique sous-groupe d'ordre $p$, qui n'est autre que $< a_1 >$. Ainsi, on a $b^{j'} \in < a_{n+1}$ et le fait que $j' < j$ viennent contredire la définition de $j$. Autrement dit, le deuxième cas traité ici n'arrive jamais.

Finalement, on a bien l'égalité annoncé et on conclut comme en q.1.

3- Tout d'abord, tout $g \in G$ est d'ordre fini sinon deux cas se dessinent : soit $< g >$ est un sous-groupe strict (infini) - ce qui contredit l'hypothèse faite sur $G$ - soit $< g >= G$, si bien que $< g^2 >$ est un sous-groupe strict infini - ce qui contredit de nouveau l'hypothèse faite sur $G$.

De plus, il existe au plus un $p \in \mathbb{P}$ tel que le $p$-Sylow $S_p$ (il n'en existe qu'un seul car $G$ est abélien, il s'agit du sous-groupe formé par l'ensemble des éléments d'ordre $p^?$) de $G$ soit de cardinal infini puisque l'on aurait $G = S_p$ (pousser le raisonnement un cheveux plus loin n'est pas compliqué).

Tâchons de montrer qu'il en existe bien un en raisonnant par l'absurde. Supposons donc que $S_p$ soit fini pour tout $p \in \mathbb{P}$. Alors, puisque $G$ est produit de ses $p$-Sylow, on peut affirmer que $A = \{p \in \mathbb{P} : |S_p| \neq 1\}$ est infini, sans quoi $G$ serait fini. Ainsi, en fixant $p_0 \in A$ quelconque, on aboutit à l'absurdité que le produit des $S_p$ pour tout $p \neq p_0$ est un sous-groupe strict infini de $G$.

Ainsi, on a un (unique) $p \in \mathbb{P}$ tel que $G = S_p$.

Montrons maintenant que tout élément de $G$ admet une racine $p^e$. Pour cela, remarquons d'abord qu'il n'y a qu'un nombre fini d'éléments d'ordre $p$. Par l'absurde, si ce n'était pas le cas, on pourrait construire une suite $(g_n) \in G^{\mathbb{N}}$ telle que, pour tout $n \geq 0$, $g_n$ est d'ordre $p$ et $g_n \notin < g_0, ..., g_{n-1} >$. On aurait alors $G =< g_n >_{n\in\mathbb{N}} =< g_1, ... >$ d'où $g_0 = g_1^{i_1} \cdots g_m^{i_m}$ avec $0 < i_m < p$, si bien que l'on aurait $i_m \wedge p = 1$ puis en choisissant un couple de Bézout $(u, v)$ associé, on aurait $g_0^u g_1^{-i_1 u} \cdots g_{m-1}^{-i_{m-1} u} = g_m$, ce qui contredit la construction de $(g_n)$.

On peut maintenant démontrer ce que l'on a annoncé plus haut. Pour cela, on considère $X = \{g \in G : \exists x \in G \quad x^p = g\} = Im(f)$ où $f$ est le morphisme "puissance $p$". On constate que $X$ est un sous-groupe de $G$. Par l'absurde, supposons $X \neq G$. On a donc $X$ fini, si bien que, par le théorème d'isomorphisme (on pourrait aussi justifier ça à la main avec le lemme des tiroirs), $Ker(f)$ serait infini. L'hypothèse faite sur $G$ impose donc que l'on a $G = Ker(f)$ donc tout les éléments de $G$ sont d'ordre 1 ou $p$. Or, il n'y a qu'un nombre fini d'éléments d'ordre $p$, absurde puisque $G$ est infini.

On peut donc construire une suite $(a_n) \in G^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $a_n$ est d'ordre $p^n$ et $a_{n+1}^p = a_n$. Comme $< a_n >_{n\in\mathbb{N}}$ est infini, on a $G =< a_n >_{n\in\mathbb{N}}$ et on peut conclure comme en q.1.

## 10.19 Nombre d'endomorphisme d'un groupe

Soit $G$ un groupe fini de cardinal $N$. Montrer que l'on a $|\operatorname{End}(G)| \leq N^{\log_2 N}$.

***Correction:*** On construit par récurrence $(H_n)$ une famille de sous-groupes de $G$. On met de côté de le cas où $G$ est trivial.

On se donne d'abord $x_1 \in G \setminus \{0\}$ et on pose $H_1 =< x_1 >$.

Soit un entier $n \geq 1$ tel que $H_1, ..., H_n$ soient construits. Si $H_n = G$, on s'arrête. Sinon, on prend $x_{n+1} \in G \setminus H_n$ et on pose $H_{n+1} =< H_n, x_{n+1} >$. En notant $a_{n+1}$ le plus petit entier naturel non nul tel que $x_{n+1}^{a_{n+1}} \in H_n$, on constate que $H_{n+1}$ contient $\left\{hx_{n+1}^a : h \in H_n, 0 \leq a < a_{n+1}\right\}$ qui est de cardinal $|H_n|a_{n+1}$.

En remarquant que l'on a $a_n \geq 2$ (car $a_n \neq 1$), on montre que l'on a $Card(H_n) \geq 2^n$, ce qui permet de conclure.

## 10.20 Autour de l'indicatrice d'Euler

Montrer que, pour tout $n, q \in \mathbb{N}^*$, on a $n|\varphi(q^n - 1)$.

***Indication:*** On pourra remarquer que $\mathbb{Z}/n\mathbb{Z}$ agit sur l'ensemble des générateurs de $\mathbb{Z}/\varphi(q^n - 1)\mathbb{Z}$ via $k.x = x^{q^k}$.

***Correction:*** Il reste à remarquer que les orbites sont de longueur $n$.

## 10.21 Sylow et groupes d'ordre $pqr$

Soient $p < q < r$ trois nombres premiers. Soit $G$ un groupe d'ordre $pqr$.

1- Montrer qu'il y a un sous-groupe d'ordre $qr$ et que ce sous-groupe est normal.

***Correction:*** On note $n_r$ le nombre de $r$-Sylow de $G$. Par l'absurde, supposons $n_r \neq 1$. Par le théorème de Sylow, on sait que l'on a $n_r|pq$ et $n_r = 1[r]$. On ne ne peut pas avoir $n_r = p$ ni $n_r = q$, sans quoi $r$ diviserait $p - 1$ ou $q - 1$, ce qui exclu puisque $r > p, q > 1$. On a donc $n_r = pq$, chaque $r$-Sylow contient $r$ éléments et l'intersection de deux $r$-Sylow distincts donne le groupe trivial. Ces $r$-Sylow donnent donc $1 + pq(r - 1)$ éléments.

Considérons maintenant $n_q$. On ne peut pas $n_q = p$ car cela donnerait $p-1 = 0[q]$, ce qui est exclu car $q > p > 1$. Par l'absurde, supposons que l'on a également $n_q \neq 1$. On a donc $n_q \geq r$ comme $n_q|pr$ et que $n_q|p$ est exclu. Les éléments de chaque $q$-Sylow et chaque $r$-Sylow donnent donc au moins $1+pq(r-1)+r(q-1)$ éléments, ce qui est absurde car on a $1 + pq(r - 1) + r(q - 1) > pqr$ (ceci est équivalent à $r(q - 1) \geq pq$).

En fait, on vient de montrer que soit $n_r \neq 1$, dans quel cas on a $n_q = 1$, soit $n_r = 1$.

Supposons donc dans un premier temps $n_q = 1$. Soit $H_q$ l'unique $q$-Sylow de $G$ (qui est donc distingué d'après le théorème de Sylow) et $H_r$ un $r$-Sylow. On constate $H_r \cap H_q$ est trivial car $H_r$ et $H_q$ sont d'ordres premiers entre eux et on peut donc considérer le produit semi-direct interne $H_qH_r$ qui est un sous-groupe

de $G$ d'ordre $qr$. Ce sous-groupe est normal car d'indice $p$ qui est le plus petit diviseur de $|G|$ (lemme de Ore).

Supposons maintenant $n_r = 1$. On peut faire de même et considérer le produit semi-direct $H_r H_q$.

2- Montrer que $G$ n'a qu'un seul $r$-Sylow.

Par Sylow, $H$ a un unique $r$-Sylow : si l'on note $m_r$ le nombre de $r$-Sylow de $H$, on ne peut pas avoir $m_r = q$ car on aurait $r|q-1$ alors que l'on a $r > q-1 > 0$ ; on a forcément $m_r = 1$ puisque $m_r|q$. Notons $H_r$ ce $r$-Sylow de $H$. Alors, $H_r$ est également un $r$-Sylow de $G$ et en fait $H_r$ est normal dans $G$ : pour tout $g \in G$, on a $gH_rg^{-1} \subset H$ car $H$ est distingué et $gH_rg^{-1}$ est encore un $r$-Sylow de $H_r$, ce qui force $gH_rg^{-1} = H_r$. Par le théorème de Sylow, $H_r$ est en fait l'unique $r$-Sylow de $G$.

# 11 Analyse

## 11.1 Un taux d'accroissement

Trouver les triplets $(f, g, h)$ de fonctions de $\mathbb{R} \to \mathbb{C}$ tels que :

$$\forall x \neq y \quad \frac{f(x) - f(y)}{x - y} = g(x)h(y).$$

***Indication:*** On pourra distinguer les cas selon que $f$ soit injective ou non.

***Correction:*** On remarque que, pour un tel triplet, le taux d'accroissement s'annule ssi $f$ n'est pas injective ssi $g$ ou $h$ s'annule. Dans ce cas, on montre facilement que $f$ est forcément constante et que $g$ ou $h$ est nulle.

Sinon, on raisonne par analyse-synthèse. On voit que le taux d'accroissement est symétrique en $x, y$ donc on a, pour tout $x \neq y$ $g(x)h(y) = g(y)h(x)$ et cette égalité est encore vraie si $x = y$. On a donc $g(x)/h(x) = g(y)/h(y)$ pour tout $x, y$. Ainsi, $\frac{g}{h}$ est constante, disons égale à $\lambda$.

On est donc amenés à trouver les $f, h$ telles que $\frac{f(x)-f(y)}{x-y} = h(x)h(y)$ (quitte à poser $h_2 = \mu h$ où $\mu$ est une racine carrée de $\lambda$ que l'on se fixe et qui existe puisque l'on travaille dans $\mathbb{C}$ ).

Pour $x \neq y$ on aurait donc $h(x) = \frac{f(x)-f(y)}{h(y)(x-y)}$ et de la bonne définition de $h$ il découle $(x - y_1)h(y_1)(f(x) - f(y_2)) = (x - y_2)h(y_2)(f(x) - f(y_1))$ i.e $f(x)[x(h(y_1) - h(y_2)) + y_2h(y_2) - y_1h(y_1)] = x[h(y_1)f(y_2) - h(y_2)f(y_1)]$ $+y_2h(y_2)f(y_1) - y_1h(y_1)f(y_2)$ pour tout $x, y_1, y_2$.

Ainsi, $f$ est une fraction rationnelle (en prenant $y_1 = 1$ et $y_2 = 0$ par exemple). De plus, le polynôme de gauche ne peut pas s'annuler en un réel sinon ce serait aussi le cas pour celui de droite pour le même réel et ainsi $f$ serait constante partout sauf éventuellement en ce réel et donc $h$ s'annulerait, chose que l'on a exclue.Aussi, on a

$$\frac{\frac{ax+b}{cx+d} - \frac{ay+b}{cy+d}}{x - y} = \frac{ad - bc}{(cx + d)(cy + d)} = h(x)h(y).$$

De même que plus haut, on en déduit $h(y)(cy+d)$ est constante i.e il existe $\gamma$ non nul (car $h$ ne s'annule jamais d'après notre disjonction de cas) tel que $h(x) = \frac{\gamma}{cx+d}$ et $\gamma^2 = ad - bc$.

Conclusion, les solutions du problème initial sont les $(cste, 0, h), (cste, g, 0)$ et $(\frac{ax+b}{cx+d}, \frac{\gamma}{cx+d}, \frac{\gamma}{cx+d})$ avec $\gamma^2 = ad - bc \neq 0$ et $\frac{d}{c} \notin \mathbb{R}$ si $c \neq 0$ pour ne pas avoir de problème de définition comme mentionné plus haut.

## 11.2 Fonction surjective

Soit $f : \mathbb{R}_+ \to \mathbb{R}$ continue surjective. Montrer que $f$ a une infinité de zéros.

## 11.3 La fonction $id$ (oral X)

Montrer que la fonction $id$ est la seule fonction $f : \mathbb{N} \to \mathbb{N}$ vérifiant :

$$\forall n \in \mathbb{N} \quad f(f(n)) < f(n+1).$$

***Indication:*** Quel effet a $f$ sur les $[\![n; +\infty[\![$ ?

## 11.4 Autour de Fourier (TD ENS Rennes)

Donner une condition nécessaire et suffisante sur $\varphi \in \mathbf{L}^2(0, 2\pi)$ $2\pi$-périodique pour avoir $Vect\{x \mapsto \varphi(x-a) : a \in [0, 2\pi[\}$ dense dans cet espace

***Indication:*** Par corollaire du théorème de projection, ceci équivaut à demander $\int_0^{2\pi} \varphi(x-a)\overline{f(x)}dx = 0$ pour tout $a \in \mathbb{R}$ implique que $f = 0$ dans $\mathbf{L}^2(0, 2\pi)$.

***Correction:*** Ceci n'est vérifié que si le $n^{eme}$ coefficient de Fourrier de $\varphi$ est non nul pour tout $n \in \mathbb{Z}$ (forcer l'apparition de coefficients de fourier d'une convolée

## 11.5 Convergence au sens de Cesàro (oral X)

Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite positive bornée.. Montrez que l'on a équivalence entre :

$i) \frac{1}{n}\sum_{k=1}^{n} u_k \xrightarrow[n\to\infty]{} 0$

$ii)$ il existe $A \subset \mathbb{N}$ vérifiant $\lim_{n\to\infty} \frac{|A \cap [\![1, n]\!]|}{n} = 0$ et $u_n \xrightarrow[\substack{n\to\infty \\ n\notin A}]{} 0$.

On dit que $A$ est de densité nulle lorsque $\lim_{n\to\infty} \frac{|A \cap [\![1, n]\!]|}{n} = 0$ (densité de Schnirelmann).

***Correction:*** Pour $i) \implies ii)$, expliquons d'abord notre démarche. En première approche, on peut regarder ce qui se passe lorsque $u_n$ ne tend pas vers 0. On est alors amener à regarder un certain $A_\epsilon = \{n \in \mathbb{N}^* : u_n > \epsilon\}$ qui contiendrait une infinité de terme. On aimerait bien réitérer l'opération aux termes restant

de la suite mais pour traiter tous les cas, on est amené à considérer une suite $\epsilon_n$ tendant vers 0 de façon décroissante. On aurait abouti à cette même réflexion en supposant qu'un tel $A$ existe.

On peut alors se demander s'il existe $\epsilon_n$ tendant vers 0 de façon décroissante telle que $A = \{n \in \mathbb{N}^* : u_n \geq \epsilon_n\}$ convienne. Il facile de voir qu'on aura bien $u_n \xrightarrow[\substack{n\to\infty \\ n\notin A}]{} 0$. Aussi, on remarque que l'on a, avec $c_n = \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} u_k$ :

$$c_n \geq \frac{1}{n} \sum_{k\in A\cap[\![1,n]\!]} u_k \geq \epsilon_n \frac{|A \cap [\![1,n]\!]|}{n}.$$

Ainsi, pour que $A$ soit de densité nulle, il suffit que $\dfrac{c_n}{\epsilon_n}$ tende vers 0. On constate que $\epsilon_n = \sup_{k\geq n} \sqrt(c_k)$ convient pour tout.

## 11.6 Equation fonctionnelle (oral X)

Déterminer les fonctions $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ telles que $f(x) \xrightarrow[x\to\infty]{} 0$ et $f(xf(y)) = yf(x)$ pour tout $x, y \in \mathbb{R}_+^*$.

## 11.7 Une fonction polynomiale

Soit $f : \mathbb{C}^2 \mapsto \mathbb{C}$ telle que, pour tout $x$, $y \mapsto f(x, y)$ soit polynomiale et de même de $x \mapsto f(x, y)$ à $y$ fixé. Montrer que $f$ est polynomiale.

## 11.8 Monotonie et injectivité

Soit $I$ un intervalle réel et $f : I \to \mathbb{R}$ une fonction continue. Montrer que $f$ est strictement monotone si et seulement si $f$ est injective.

## 11.9 Autour de la composition

Soit $f : [0; 1] \to [0; 1]$ continue.

1-On suppose que l'on a $f(0) = 0, f(1) = 1$ et $f^{\circ n} = \mathrm{Id}$. Montrer que l'on a $f = \mathrm{Id}$.

2- (Oral ENS Lyon 2014) On suppose que tout $x \in [0; 1]$, il existe $n_x \in \mathbb{N}^*$ tel que $f^{\circ n_x}(x) = x$. Montrer que l'on a $f \circ f = \mathrm{Id}$.

***Indication:*** On pourra montrer que $f$ est injective.

***Correction:*** 1- On a $f$ injective donc $f$ est strictement monotone par l'exercice précédent et puisque l'on a $f(0) < f(1)$, on en déduit que $f$ est strictement croissante. Par l'absurde, supposons qu'il existe $x \in [0; 1]$ tel que $f(x) \neq x$. Supposons même que l'on a $f(x) < x$. En appliquant $f$, on a donc $f^{\circ 2}(x) < f(x) < x$ et en itérant on obtient $x = f^{\circ n}(x) < f^{\circ n-1}(x) < ... < f(x) < x$, absurde. On peut procéder de façon similaire si l'on a $f(x) > x$.

2- Montrons que $f$ est injective. Soient $x, y \in [0;1]$ tels que $f(x) = f(y)$. On a alors $f^{\circ n_x n_y}(x) = f^{\circ n_x} \circ ... \circ f^{\circ n_x}(x) = x$ et

$$f^{\circ n_x n_y}(x) = f^{\circ n_x n_y - 1}(f(x)) = f^{\circ n_x n_y - 1}(f(y)) = f^{\circ n_x n_y}(y) = y.$$

On sait donc que $f$ est strictement monotone par l'exercice précédent. Ainsi, $f \circ f$ est strictement monotone et vérifie encore l'hypothèse de l'énoncé. En appliquant la méthode de la question précédente, on retrouve donc $f \circ f = \mathrm{Id}$

## 11.10 Nombre d'antécédents (Oral X)

Soit $f : \mathbb{R} \to \mathbb{R}$ continue telle que tout réel a au plus deux antécédents par $f$. Montrer qu'il existe un réel qui admet exactement un antécédent par $f$.

***Indication:*** S'appuyer sur un dessin et essayer de le simplifier pour clarifier sa pensée.

***Correction:*** Raisonnons par l'absurde et supposons donc que tout point de l'image de $f$ a deux antécédents. En particulier, $f$ n'est pas injective : on peut se donner $x < y$ tels que $f(x) = f(y)$. Quitte à translater $f$ (cela préserve les hypothèses faites), on peut supposer $f(x) = 0 = f(y)$. Quitte à considérer $-f$, on peut supposer $f \geq 0$ sur l'intervalle $[x, y]$.

Commençons par remarquer, puisque $f$ ne s'annule que deux fois, on obtient comme conséquence du théorème des valeurs intermédiaires (TVI) que $f$ est de signe constant sur $]-\infty, x], [x, y], [y, +\infty[$. De plus, $f$ ne peut pas être positive sur $[y, +\infty[$. Par l'absurde, supposons qu'elle le soit. Considérons $n$ assez grand de sorte que $x < x + 1/n < y - 1/n < y$. Par le TVI, on sait que tous les réels de l'intervalle $[0, \min(f(x+1/n), f(y-1/n), f(y+1/n)]$ ont un antécédent dans chacun des intervalles suivants : $[x, x+1/n], [y-1/n, y]$ et $[y, y+/n]$ ce qui donne en particulier que $\min(f(x+1/n), f(y-1/n), f(y+1/n)$ a trois antécédents par $f$, absurde. De même, on montre que $f$ est négative sur $]-\infty, x]$. Ainsi, la quantité $\max_{t \in [x,y]} f(t)$ n'est atteinte par $f$ que sur l'intervalle $[x, y]$. Par l'absurde, supposons qu'il existe $a < b \in [x, y]$ tels que $f(a) = \max_{t \in [x,y]} f(t) = f(b)$. En particulier, on a $f(\frac{a+b}{2}) < f(a)$. Par le TVI, il vient que $f(\frac{a+b}{2})$ a un antécédent dans chacun des intervalles suivants : $[x, a]$ et $[b, y]$. Ainsi, $f(\frac{a+b}{2})$ a trois antécédents par $f$, ce qui est exclu.

## 11.11 Caractérisation des fonctions affines (X PC 2022)

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction continue. Supposons que l'on a

$$\forall x \in \mathbb{R}, \quad f(x+h) - 2f(x) + f(x-h) \xrightarrow[h \to +\infty]{} 0.$$

Montrer que $f$ est affine.

***Correction:*** Posons $g(h) = f(h) + f(-h)$. L'hypothèse faite dans l'énoncé (prendre $x = 0$) implique que $g$ tend vers $2f(0) = g(0)$ en $+\infty$ et $-\infty$. Soit $x \in \mathbb{R}$. Remarquons que l'on a

$$\begin{aligned} g(x+h) &= f(x+h) + f(-x-h) \\ &= f(x+h) + f(x-h) \\ &+ f(-x+h) + f(-x-h) \\ &- \underbrace{\left(f(x-h) + f(-x+h)\right)}_{=g(-x+h)}. \end{aligned}$$

Laissant tendre $h$ vers l'infini, on obtient $g(0) = 2f(x) + 2f(-x) - g(0)$, ou encore $2g(0) = 2g(x)$. Autrement dit, $g$ est constante.

Remarquons maintenant que les translatés de $f$ (c'est-à-dire les fonctions de la forme $x \mapsto f(x+a)$) vérifient encore les hypothèses de l'énoncé, de sorte que ce qui précède s'applique également à ces fonctions. On obtient que l'hypothèse de l'énoncé implique en réalité que l'on a

$$\forall x, h \in \mathbb{R}, \quad f(x+h) + f(x-h) = 2f(x).$$

On peut lire cette égalité en observant que $x$ est le milieu de $x+h$ et de $x-h$. Constatons maintenant que l'on a

$$\begin{aligned} f(h) - f(0) &= f(h) + f(2-h) - (f(2-h) - f(0)) \\ &= 2f(1) - 2f(1 - h/2) \end{aligned} \tag{1}$$

pour tout $h \in \mathbb{R}$. On voit que $h = 2$ donne

$$f(2) - f(0) = 2(f(1) - f(0)). \tag{2}$$

En appliquant cela à $x \mapsto f(2x)$ et $x \mapsto f(\frac{x}{2})$ (qui vérifiant aussi les hypothèses de l'énoncé), on obtient, en itérant, $f(2^n) - f(0) = 2^n(f(1) - f(0))$ pour tout $n \in \mathbb{Z}$.

On montre également par récurrence forte sur $k \in \mathbb{N}$ que l'on a $f(k) - f(0) = k(f(1) - f(0))$. Les cas $k \in \{0; 1\}$ sont trivialement vérifiés. Si $k \geq 2$, par l'équation 2 appliquée à $x \mapsto f(x + k - 2)$, on a

$$f(k) - f(k-2) = 2(f(k-1) - f(k-2))$$

et injecter l'hypothèse de récurrence montre facilement que la propriété est encore valable au rang $k$ si elle l'est au rang $k-1$ et $k-2$, ce qui conclut la récurrence.

On voit maintenant que $h = -1$ dans l'équation 1 donne

$$f(-1) - f(0) = -(f(1) - f(0)) \tag{3}$$

puis en appliquant ce qui précède à $x \mapsto f(-x)$ (qui vérifie encore les hypothèses de l'énoncé), on obtient $f(k) - f(0) = k(f(1) - f(0))$ pour tout $k \in \mathbb{Z}$.

On peut maintenant conclure en utilisant l'approximation par des nombres diadiques. Soit $x \in \mathbb{R}$. Posons $x_n = \frac{1}{2^n}\lfloor 2^n x \rfloor = 2^n y_n$. Par ce qui précède, on a $f(x_n) - f(0) = 2^n(f(y_n) - f(0)) = 2^n y_n(f(1) - f(0)) = x_n(f(1) - f(0))$. Laissant tendre $n$ vers l'infini, par la continuité de $f$, on obtient $f(x) - f(0) = x(f(1) - f(0))$, ce qui conclut.

# 12 Développement limité et asymptotique

## 12.1 Autour de $0^0$

Calculer $\lim_{x\to 0} x^{x^x}$ et $\lim_{x\to 0}(x^x)^x$. Commenter.

***Correction:*** Normalement, on en déduit que $(x, y) \mapsto x^y$ n'est pas prolongeable par continuité en $(0, 0)$ (pour les spé, pour les sup on peut juste parler de la "règle" $x^0 = 1$).

## 12.2 Une racine légèrement modifiée

On pose $f(x) = x^5 + x$. Justifier que $f$ est inversible et en donner un équivalent en $+\infty$. En donner le DL à l'ordre 1.

# 13 Suite

## 13.1 Opérateur shift (Oral ENS Rennes Magistère, professeur Hassler)

1- Soient $(u_n)_{n\in\mathbb{N}}$ une suite complexe, $\alpha \in \mathbb{C}$ tel que $|\alpha| < 1$. On suppose que l'on a $u_{n+1} - \alpha u_n \xrightarrow[n\to\infty]{} 0$. Montrons que l'on a $u_n \xrightarrow[n\to\infty]{} 0$.

2- On note $\sigma \in \mathcal{L}(\mathbb{C}^{\mathbb{N}})$ l'opérateur de décalage défini par $\sigma(u) = v$ où $v$ est définie par $v_n = u_{n+1}$ pour tout $n$.

Si $P$ est un polynôme complexe, exprimer $P(\sigma)(u)$ en fonction de $u$.

3- Montrer que l'on a

$$\forall u [P(\sigma)(u)]_n \xrightarrow[n\to\infty]{} 0 \implies u_n \xrightarrow[n\to\infty]{} 0$$

si et seulement si toutes les racines de $P$ sont de module $< 1$.

***Correction:*** 1- Soient $\varepsilon > 0$ et $n_0$ tel que $|u_{n+1} - \alpha u_n| \leq \varepsilon$ pour tout $n \geq n_0$. On montre alors par récurrence sur $k$ que l'on a, pour tout $k > 0$, $|u_{n_0+k}| \leq |\alpha|^k u_{n_0} + \sum_{j=0}^{k-1} |\alpha|^j \varepsilon$.

Le premier terme tend vers 0 car $|\alpha| < 1$ et le deuxième est plus petit qu'une constante (la somme infinie des $|\alpha|^j$, qui ne dépend que de $\alpha$) fois $\varepsilon$. Ainsi, $(u_n)$ tend bien vers 0.

2- Si l'on écrit $P = \sum_{k=0}^{d} a_k X^k$, on a $P(\sigma) = \sum_{k=0}^{d} a_k \sigma^k$.

Ainsi, on a $[P(\sigma)(u)]_n = \sum_{k=0}^{d} a_k u_{n+k}$.

3- Supposons que toutes les racines de $P$ sont de modules $< 1$. On peut toujours supposer $P$ unitaire et écrire $P = \prod_{k=0}^{d} X - \alpha_k$.

On a alors $P(\sigma) = \prod_{k=0}^{d} \sigma - \alpha_k i_d$ (où le produit désigne ici la composition). Si l'on a $[P(\sigma)(u)]_n \xrightarrow[n\to\infty]{} 0$, alors on a $[(\sigma - \alpha_1)(v)]_n \xrightarrow[n\to\infty]{} 0$ où $v = (\prod_{k=1}^{d} \sigma - \alpha_k i_d\ )\ (u)$. Par la q.1, on en déduit $v_n \xrightarrow[n\to\infty]{} 0$. On réitère le même procédé avec $v$ ...

Si l'on a $\forall u [P(\sigma)(u)]_n \xrightarrow[n\to\infty]{} 0 \implies u_n \xrightarrow[n\to\infty]{} 0$ mais qu'une racine de $P$ est de module $\geq 1$, on écrit $P = \prod_{k=0}^{d} X - \alpha_k$ avec $|\alpha_d| \geq 1$. On pose $u_n = \alpha_d^n$. Alors $(\sigma - \alpha_d i_d)(u)$ est la suite nulle donc $P(\sigma)(u) = 0$. On constante que l'on a $[P(\sigma)(u)]_n \xrightarrow[n\to\infty]{} 0$ sans avoir $u_n \xrightarrow[n\to\infty]{} 0$.

### 13.2 Suite sous-additive

Si $(u_n)$ est une suite de réels vérifiant $u_{n+m} \leq u_n + u_m$, montrer que $(\frac{u_n}{n})$ converge ou tend vers $-\infty$

## 14 Série

### 14.1 Un produit divergeant

Montrer que $\prod_{p\in\mathbb{P}} 1 - \frac{1}{p}$ et $\prod_{p\in\mathbb{P}} 1 + \frac{1}{p}$ divergent.

***Indication:*** On pourra montrer que $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge en regardant $\prod_{p\in\mathbb{P}} (1 - \frac{1}{p})^{-1}$.

### 14.2 Fonction complètement multiplicative (ENS Maths D 2019)

Soit $f : \mathbb{N}^* \to \mathbb{C}$ telle que $f(mn) = f(m)f(n)$ pour tout $(m, n) \in (\mathbb{N}^*)^2$. Montrer que si $s > 1$ et $\sum_{n\geq 1} \frac{|f(n)|}{n^s} < \infty$ alors on a $\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} (1 - \frac{f(p)}{p^s})^{-1}$.

***Indication:*** Utiliser une sommation par paquet en posant
$A_n = \{k : k = p_1^{\alpha_1} ... p_n^{\alpha_n}, \alpha_i \geq 0\}$ en écrivant $\mathbb{P} = (p_i)_{i\in\mathbb{N}^*}$ strictement croissante.
Les $A_{n+1} \setminus A_n$ forment une partition de $\mathbb{N}$.

## 14.3 La 5/2

On donne $\sum \frac{1}{n^2} = \pi^2/6$ et $\sum \frac{1}{n^4} = \pi^4/90$.

Calculer $\sum_{p,q\in\mathbb{N}^*} \frac{1}{p^2q^2}$ et en déduire $\sum_{\substack{p,q\in\mathbb{N}^* \\ p\wedge q=1}} \frac{1}{p^2q^2}$.

***Indication:*** Partionner selon le pgcd.

## 14.4 Etude d'une suite

Soient $u_0 > 0$ et $(u_n)$ la suite définie par $u_{n+1} = \sqrt{\sum_{k=0}^{n} u_k}$. Montrer que $(u_n)$ diverge vers $+\infty$ et en déduire que $u_n \sim n/2$.

***Indication:*** Remarquer que l'on a $u_{n+1} = \sqrt{u_n + u_n^2}$.

## 14.5 Comparaison de deux suites

Soient $(u_n) > 0$ , $w_n = \frac{u_n}{u_1 + ... + u_n}$. Montrer que $(w_n)$ et $(u_n)$ sont de même nature.

***Correction:*** Les deux suites sont à termes positifs. Si $\sum u_n$ est convergente, on a $w_n \sim cu_n$ avec $c = (\sum_{n=1}^{\infty} u_n)^{-1}$ et par théorème de comparaison, on a donc $\sum w_n$ convergente.

Si $\sum w_n$ est convergente, on note que l'on a, en notant $S_n = \sum_{k=1}^{n} u_k$,

$$w_n S_n = u_n \ (1)$$

i.e $w_n S_{n-1} = u_n(1-w_n)$ et en utilisant (1) au rang $n-1$, on a donc $\frac{w_n}{w_{n-1}} u_{n-1} = u_n(1-w_n)$ soit $\frac{w_n}{w_{n-1}(1-w_n)} = \frac{u_n}{u_{n-1}}$.

Finalement, en prenant le produit, on remarque un télescopage et on obtient $\frac{w_n}{w_0} \prod_{k=1}^{n} \frac{1}{1-w_k} = \frac{u_n}{u_0}$. On remarque le produit converge en passant au *log*.

Remarquez que l'on n'a jamais divisé par 0.

## 14.6 Fonction génératrice du nombre de partitions

On note $T_n$ le nombre de partitions d'un ensemble a $n$ élément ( on pose $T_0 = 1$).

1- Montrer que l'on a $T_{n+1} = \sum_{k=0}^{n} \binom{n}{k} T_k$.

***Indication:*** On fera un dénombrement en partitionnant selon le nombre d'éléments qui appartiennent à l'ensemble qui contient l'élément "$n+1$".

2- Montrer que l'on a $T(x) := \sum_{n=0}^{\infty} \frac{T_n x^n}{n!} = e^{e^x - 1}$.

***Indication:*** Pour montrer que le rayon est non nul, on pourra remarquer que $T_n \leq n!$ parce que l'on peut injecter une partition dans $S_n$ en lui associant une permutation dont les cycles représentent les ensembles de la partition (ou en le démontrant par récurrence). Il est important de le montrer, sans quoi la dérivée n'a pas de sens.

3- En déduire une expression des $T_n$.

***Correction:*** 1-Une première remarque à faire est que $T_n$ est en fait le nombre de partition de n'importe quel ensemble à $n$ éléments. On suit maintenant l'indication. Soit $n \in \mathbb{N}$. Soit $\{I_1, ..., I_r\}$ une partition de $[\![1; n+1]\!]$. Alors, il existe un unique $i$ tel que $I_i$ contienne $n+1$. Puisque l'on ne tient pas compte de l'ordre des $I_j$, on peut supposer que l'on a $i = 1$. On constate que $I_1$ consiste alors en un ensemble contenant $n+1$ et un certain nombre $k \in [\![0; n]\!]$ d'autres éléments de $[\![1; n+1]\!]$. Alors, $\{I_2, ..., I_r\}$ constitue une partition d'un ensemble à $n+1-|I_1| = n-k$ éléments. Réciproquement, la donnée de tels objets constitue une partition. Cette correspondance est bijective et on en déduit le dénombrement $T_{n+1} = \sum_{k=0}^{n} \binom{n}{k} T_{n-k}$ ( le coefficient binomial représente le choix des $k$ "autres" éléments de $I_1$ et $T_{n-k}$ le choix de la partition $\{I_2, ..., I_r\}$). En posant $k' = n-k$ et en utilisant la symétrie du coefficient binomial, on obtient alors la formule attendue.

2- On cherche à utiliser la formule de récurrence :

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{T_n x^n}{n!} &= 1 + \sum_{n=1}^{\infty} \frac{T_n x^n}{n!} \\
&= 1 + \sum_{n=0}^{\infty} \frac{T_{n+1} x^{n+1}}{(n+1)!} \\
&= 1 + \sum_{n=0}^{\infty} \frac{1}{n+1} \sum_{k=0}^{n} \frac{T_k}{k!} \frac{1}{(n-k)!} x^{n+1}.
\end{aligned}$$

La somme sur $k$ qui apparaît au milieu fait penser à un produit de Cauchy et le $\frac{1}{n+1}$ nous rappelle le lien entre série entière et ses primitives. On se rend compte que l'on a en fait écrit $T(x) = 1 + \int_0^x T(t) e^t dt$. L'indication nous permet de dire que le rayon est strictement positif. En dérivant cette dernière égalité, on trouve $T'(x) = T(x) e^x$ pour tout $x$ dans le disque de convergence. On en déduit qu'il existe $\lambda \in \mathbb{R}$ tel que $T(x) = \lambda e^{e^x}$ pour tout $x$ dans le disque de convergence. En évaluant en $x = 0$, on trouve alors l'expression attendue.

3- On écrit $T(x) = \frac{1}{e}e^{e^x}$ ; le développement en série entière de l'exponentielle nous donne alors

$$T(x) = \frac{1}{e}\sum_{k=0}^{\infty}\frac{e^{kx}}{k!} = \frac{1}{e}\sum_{k=0}^{\infty}\frac{1}{k!}\sum_{n=0}^{\infty}\frac{(kx)^n}{n!}.$$

On a le droit d'inverser les sommes puisque la famille que l'on voit apparaître est sommable (il s'agit en fait de reprendre ce même calcul en remplaçant $x$ par $|x|$) et on en déduit $T_n = \frac{1}{e}\sum\limits_{k=0}^{\infty}\frac{k^n}{k!}$.

# 15 Topologie

## 15.1 Fonction presque contractante et théorème de point fixe

Soit $A$ une partie compacte d'un evn $E$. Soient $f : E \to E$ continue telle que $f(A) \subset A$ et $a \in A$ vérifiant :

$$\forall x \in A, \quad x \neq a \Longrightarrow 0 < ||f(x) - a|| < ||x - a||.$$

Montrer que pour toute suite définie par $x_0 \in A$ et $x_{n+1} = f(x_n)$, on a $x_n \xrightarrow[n\to\infty]{} a$. En déduire que a est l'unique point fixe de f.

***Indication:*** Considérer l'ensemble des valeurs d'adhérence de $x_n$.

***Correction:*** On distingue deux cas. Soit $A$ est réduit à $a$, dans quel cas l'énoncé est trivial. Soit c'est pas le cas et on fait comme suit en supposant $x_0 \neq a$ (la conclusion sous cette hypothèse donne alors la conclusion sans cette hypothèse comme corollaire).

On note $D$ cet ensemble. On remarque que l'on a $D \subset A$ car $A$ est fermée, que $D$ est fermée donc compacte (en tant que partie fermée d'un compact) et que la convergence d'une sous suite de $(x_n)$ vers $a$ implique la convergence de $(x_n)$ par l'inégalité qu'on s'est donnée ( la suite ( $||x_k - a||)_{k\in\mathbb{N}}$ est décroissante). On pose $d = \inf_{l\in D}||l - a||$ . On remarque que $d$ est en fait un min car $D$ est compacte. On a forcément $d = 0$ sinon, en pose $d = ||l - a||$, on aurait $l \neq a$ donc $||f(l) - a|| < d$. Or, on a $f(l) \in D$ car si $x_{\phi(n)}$ tend vers l, alors $x_{\phi(n)+1} \in A$ tend vers $f(l)$.

Ainsi, on a que $(x_n)$ tend vers $a$ donc on a $a \in D$ et comme expliqué précédemment, $D$ est stable par $f$. Par conséquent, on a $f(a) \in D$. Comme $(x_n)$ converge, elle n'a qu'une seule valeur d'adhérence, d'où $f(a) = a$. Ce point fixe est unique sinon l'inégalité du haut donne une absurdité directement.

Preuve que $D$ est fermée : si $l_n \in D$, que $(x_{\phi_n(k)})_{k\in\mathbb{N}}$ tend vers $l_n$ et que $l_n$ tend vers $l \in E$ alors on a $l \in D$ car $x_{\phi(k)}$ tend vers $l$ où $\phi(n)$ est tel que $||l_n - x_{\phi(n)}|| < \frac{1}{n}$ avec $\phi$ strictement croissante (existe par les hypothèses, on peut la construire par récurrence et une inégalité triangulaire montre que $l \in D$).

## 15.2 Fonction presque contractante et théorème de point fixe (2)

Soient $K$ un compact d'un espace métrique et $f : K \to K$ vérifiant :

$$\forall x \neq y, \quad d(f(x), f(y)) < d(x, y).$$

Montrer que $f$ admet un unique point fixe.

***Correction:*** L'unicité est triviale et classique. Pour l'existence, on regarde $x \mapsto d(f(x), x)$. Elle atteint son min en un certain $x_0$ car c'est une fonction continue sur un compact. Si $f(x_0) \neq x_0$, alors on a $d(f(f(x_0)), f(x_0)) < d(f(x_0), x_0)$ donc $f(x_0)$ admet une image strictement plus petite que celle de $x_0$, absurde.

## 15.3 Une fonction de $\mathbb{R}^2 \mapsto \mathbb{R}$ (un peu HP prépa)

Soit $f : \mathbb{R}^2 \mapsto \mathbb{R}$ surjective et continue. Montrer que, pour tout $x \in \mathbb{R}$, $f^{-1}(\{x\})$ n'est pas borné.

***Correction:*** Par l'absurde, on se donne $x, r$ tels que $f^{-1}(\{x\}) \subset B(0, r)$. On a $B(0, r)^c$ connexe car connexe par arcs (faire un dessin). Ainsi, on doit avoir $f(B(0, r)^c)$ connexe également. Or les connexes de $\mathbb{R}$ sont les intervalles. Puisque $f(B(0, r))$ est borné (car $f$ est continue et la boule fermée est compacte) et que $f$ est continue, on a donc $f(B(0, r)^c) = \mathbb{R}$ ce qui est absurde $x \notin f(B(0, r)^c)$.

## 15.4 Partie réversible (pareil)

On dit que $A \subset \mathbb{R}$ est réversible s'il existe $f : \mathbb{R} \to \mathbb{R}$ continue telle que $f(A) \subset \mathbb{R} \setminus A$ et $f(\mathbb{R} \setminus A) \subset A$.

1- Donnez un exemple de partie réversible pour la fonction $x \mapsto x + 1$

2- Est-ce qu'un ouvert ou un fermé de $\mathbb{R}$ peut être réversible ?

3- $\mathbb{Q}$ est réversible ?

4-Est-ce qu'une partie réversible peut être bornée ?

## 15.5 Ensembles homéomorphes

Soient $D, D'$ deux droites distinctes du plan. Montrer que $\mathbb{R}$ n'est pas homéomorphe à $D \cup D'$.

***Indication:*** On pourra distinguer les cas selon que les droites soient parallèles ou non.

***Correction:*** On suit l'indication. Par l'absurde, supposons qu'il existe un homéomorphisme $f : \mathbb{R} \to D \cup D'$. Si les droites sont parallèles, on a que $D \cup D' = f(\mathbb{R})$ est connexe, ce qui n'est pas le cas.

Si les droites ne sont pas parallèles, on note $a$ le point d'intersection. On note toujours $f : \mathbb{R} \setminus f^{-1}(a) \to (D \cup D') \setminus \{a\}$ qui reste un homéomorphisme. Ainsi, $\mathbb{R} \setminus f^{-1}(a)$ et $(D \cup D') \setminus \{a\}$ devraient avoir le même nombre de composantes

connexes. En effet, il est facile de voir que si $g : X \to Y$ est un homéomorphisme, alors $g$ induit une bijection de l'ensemble des composantes connexes de $X$ dans l'ensemble des composantes connexes de $Y$ ($X$ et $Y$ sont des espaces topologiques). Or, ce n'est pas le cas puisque l'un en a 4 et l'autre 2.

## 15.6 Ouvert connexe

Soient $E$ un espace vectoriel normé et $U \subset E$ un ouvert. Montrer que $U$ est connexe si et seulement s'il est connexe par arc.

***Correction:*** La réciproque fait parti du cours et ne fait pas appel au caractère ouvert de $U$. Pour le sens direct, posons $A$ l'ensemble des points reliés à 0. Il est non vide car contient 0. C'est un ouvert car si $b \in A$, alors il existe $r > 0$ tel que $B(b, r) \subset U$ puisque $U$ est ouvert et on peut relier tous les points $c$ de cette boule en reliant 0 à $b$ puis $b$ à $c$ par le segment qui les lie. C'est également un fermé : si $(b_n) \in A$ tend vers $b \in E$ alors $b \in A$ car il existe $r > 0$ tel que $B(b, r) \subset U$ et il existe $n_0$ tel que $b_{n_0} \in B(b, r)$. Il suffit donc de relier 0 à $b_{n_0}$ puis à $b$.

## 15.7 Ensembles connexes par arcs

Soit $D$ une partie au plus dénombrable de $\mathbb{C}$. Montrer que $\mathbb{C} \setminus D$ est connexe par arcs. En déduire que $GL_n(\mathbb{C})$ est connexe par arcs.

***Indication:*** Pour la deuxième partie, on pourra essayer de relier une matrice quelconque à $I_n$.

***Correction:*** Soit $x \in \mathbb{C} \setminus D$. Il existe une infinité de $\theta$ tel que la droite passant par $x$ et d'angle $\theta$ par rapport à l'axe des abscisses n'intersecte jamais $D$. En effet, $[0; 2\pi[$ est indénombrable et l'ensemble des $\theta$ tel que la droite mentionnée avant intersecte $D$ est au plus dénombrable : on écrit $D = \{d_i : i \in I\}$ avec $I = [\![1; n]\!]$ ou égal à $\mathbb{N}$. Il suffit alors d'associer à un tel $\theta$ le plus petit $i$ tel que $d_i$ appartiennent à la droite (la droite est entièrement donnée par la connaissance de ce $d_i$ puisque c'est exactement la droite reliant $x$ à $d_i$).

On conclut, si $y \in \mathbb{C} \setminus D$, qu'il y a un chemin entre $x$ et $y$ en prenant deux $\theta_1, \theta_2$ distincts tel que la droite d'angle $\theta_1$ (resp. $\theta_2$) passant par $x$ (resp. $y$) ne rencontre pas $D$ : il suffit de relier $x$ à l'intersection des deux droites puis à $y$, en suivant le chemin dessiné par les droites.

$1^{ere}$ *méthode*

Il suffit de trigonaliser : si $M \in GL_n(\mathbb{C})$, puisque son polynôme caractéristique est scindé, elle est trigonalisable et on peut écrire $M = PTP^{-1}$ avec $T$ triangulaire supérieure inversible, et $P$ inversible. Maintenant, on applique ce qui précède à $D = \{0\}$, on relie les coefficients diagonaux de $T$ à 1 sans passer par 0 et les sur-diagonaux à 0 de façon quelconque.

$2^{eme}$ *méthode (Kaoo)*

Soient $M_1, M_2 \in GL_n(\mathbb{C})$. Puisque $t \mapsto det(tM_1 + (1-t)M_2)$ est polynomiale, il n'y a qu'un nombre fini de racines. On note $D$ cet ensemble. Par ce qui précède,

on peut trouver un chemin $\gamma$ reliant 0 à 1 dans $\mathbb{C} \setminus D$ et il suffit alors de regarder $t \mapsto \gamma(t)M_1 + (1 - \gamma(t))M_2$ pour conclure.

## 15.8 Compact en dimension infinie (hors prépa à cause de Riesz)

Soient $E$ un espace vectoriel normé de dimension infinie et $K$ un compact de $E$. Montrer que $E \setminus K$ est connexe par arcs.

***Indication:*** Etant donné $x \notin K$, on pourra trouver une droite affine passant par $x$ et ne rencontrant jamais $K$.

**Remarque:** On a vraiment besoin d'être en dimension infinie : penser à un donut dans le plan.

## 15.9 Touche à tout

Soient $(X, d)$ un espace topologique compact, $f : X \to X$ continue et une suite $(u_n)$ définie par $u_0 \in X$, $u_{n+1} = f(u_n)$ n'admettant qu'un nombre fini de valeurs d'adhérences, que l'on note $v_1, ..., v_p$.

Montrer qu'il existe $i$ une permutation de $\{1, ..., p\}$ telle que :

$$\forall 0 \leq k < p \quad u_{pn+k} \xrightarrow[n\to\infty]{} v_{i(k)}.$$

## 15.10 Recouvrement pas des boules disjointes

Est-il vraiment possible de recouvrir un carré (incluant ses bords ou non) avec des boules disjointes ?

***Correction:*** La réponse est non : si le carré s'écrit $\bigcup_{i\in I} O_i$, on a en particulier une partition du carré en 2 ouverts non-vides et disjoints, chose impossible puisque le carré est connexe (par arcs).

## 15.11 Ouvert fermé

Soient $X$ un espace topologique, $O$ un ouvert fermé de $X$ et $x \in O$. Montrer que la composante connexe $C$ de $x$ est incluse dans $O$.

***Indication:*** On pourra considérer l'indicatrice de $O$.

***Correction:*** Cette indicatrice est continue et donc constante sur $C$. Or, elle vaut 1 en $x \in C$.

# 16 Logique / divers

## 16.1 Problèmes de pesée

1 - On dispose de neuf billes visuellement identiques, huit d'entre elles ont même masse mais la neuvième est plus lourde. Comment, en deux pesées sur une balance à deux plateaux, peut-on démasquer l'intruse ?

2 (plus dure) - On dispose de neuf billes visuellement identiques, elles ont toutes la même masse sauf une. Comment, à l'aide d'une balance à deux plateaux, démasquer l'intruse en trois pesées ?

***Correction:*** 2- On procède un peu de la même façon. On regroupe les billes par trois. On dispose alors de trois tas, chacun composé de trois billes. On compare le tas 1 et le tas 2 disons en mettant chaque tas sur un plateau de la balance. On distingue maintenant deux cas.

Si la balance est à l'équilibre, cela signifie que l'intruse est parmi les billes du tas 3. On compare alors deux billes du tas 3, disons les billes $a$ et $b$. Si la balance est encore à l'équilibre, l'intruse est forcément la troisième bille. Sinon, disons que la balance penche du côté de la bille $b$, à droite. On remplace alors la bille $b$ par la troisième bille $c$ du tas 3 et on a de nouveau deux situations possibles : soit la balance penche encore du côté droit, dans quel cas l'intruse est forcément la bille de gauche $a$ (sans quoi la bille de gauche aurait forcément même poids que l'une des deux billes que l'on a testée à droite puisqu'il n'y a qu'une intruse), soit la balance est à l'équilibre et l'intruse est donc la bille $b$.

Si lors de notre première pesée la balance n'est pas à l'équilibre, disons qu'elle penche du côté du tas 2, à droite. On remplace alors le tas 2 par le tas 3. Deux situations se présentent à nous ; première situation : la balance est à l'équilibre, dans quel cas on sait que l'intruse est parmi les billes du tas 2 et que l'intruse est plus lourde que les autres billes. Il suffit alors de comparer deux billes du tas 2 pour conclure. Deuxième situation : la balance penche encore du côté droit. Alors, l'intruse est forcément dans le tas 1 (sans quoi le tas 1 aurait même poids que l'un des deux autres tas puisqu'il n'y a qu'une intruse) et l'intruse est plus légère que les autres billes. Il suffit alors de comparer deux billes du tas 1 pour conclure.

## 16.2 Partage en deux parties (oral ENS Cachan 2014)

On se donne 100 points dans le plan. Montrez qu'il existe une droite séparant cet ensemble de points en deux parties de 50 points.

## 16.3 Partie de $\mathbb{R}$

Soit $A$ une partie finie de $\mathbb{R}$. On pose $A - A = \{a - a' : a, a' \in A\}$. Montrez que l'on a $|A - A| \geq 2|A| - 1$. Généralisez à une partie de $\mathbb{R}^d$.

## 16.4 66 Points (Rallye d'Alsace, 2012)

Dans un plan sont placés 66 points distincts. On trace toutes les droites déterminées par deux de ces points et on en compte 2012 distinctes. Justifiez que parmi ces 66 points, 4 au moins sont alignés.

## 16.5 Réunions égales

Soient $n \in \mathbb{N}^*$ et $X_1 ... X_{n+1}$ des parties non vides de $[\![1; n]\!]$. Montrer qu'il existe $I, J \subset [\![1; n]\!]$ disjointes telles que $\bigcup_{i \in I} X_i = \bigcup_{j \in J} X_j$.

***Indication:*** On pourra penser à utiliser de l'algèbre linéaire.

## 16.6 Optimisation

Trouver le max de $ab + bc + cd$ lorsque $a, b, c, d \in \mathbb{N}$ et $a + b + c + d = 63$.

***Correction:*** Une première intuition serait de mettre un maximum de poids sur $b$ et $c$ puisqu'ils apparaissent plus souvent que $a$ et $d$. On voudrait donc que le max soit donné par $(0, 31, 32, 0)$ et que ce soit donc 992.

Pour commencer, il peut être intéressant de voir que $a, b$ et $c, d$ jouent des rôles "miroirs" dans le sens où si $a, b, c, d$ est une solution alors $d, c, b, a$ l'est aussi. Ainsi, on peut se donner un couple qui donne la valeur maximale tel que $b \leq c$.

Supposons $b < c$. Alors, on a forcément $a = 0$ sinon le couple $(a-1, b+1, c, d)$ donne une valeur strictement plus grande que le couple $(a, b, c, d)$. En isolant $d$ dans $a + b + c + d = 63$, on a $ab + bc + cd = 63c - c^2$ et le max de ce polynôme est atteint en $63/2$. Puisque $c$ doit être entier, le max est atteint pour $c = 31$ ou $c = 32$ et $b, d$ quelconques vérifiant $b + c + d = 63$. Ainsi, sous la condition $b < c$, on obtiendrait 992 comme valeur maximale.

Sinon, on a $b = c$ et, en isolant $d$ comme plus haut, on a $ab+bc+cd = 63c-c^2$ donc $c = 31 = b$ et de même on trouve que le max vaut 992 qui est donc effectivement la valeur maximale.

## 16.7 Nombres de Liouville

On dit que $x \in \mathbb{R}$ est un nombre de Liouville si pour tout $n \geq 1$ il existe $(p_n, q_n) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0; 1\})$ tel que

$$0 < |x - \frac{p_n}{q_n}| < (\frac{1}{q_n})^n$$

.

1 - Montrer que les nombres de Liouville sont irrationnels.

2- Soient $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ et $P \in \mathbb{Z}[X]$ de degré $d \geq 2$ irréductible dans $\mathbb{Q}[X]$ tels que $P(\alpha) = 0$. Montrer qu'il existe $c > 0$ tel que pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$

$$|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}.$$

3- En déduire que les nombres algébriques sur $\mathbb{Q}$ ne sont pas de Liouville.

4- En déduire que

$$\sum_{k=1}^{\infty} \frac{1}{10^{n!}}$$

n'est pas algébrique.

***Indication:*** Pour la q.2, on pourra s'aider de l'inégalité des accroissements finis.

***Correction:*** 1- Par l'absurde, supposons $\alpha = \frac{p}{q}$. On a alors $|q_n p - q p_n| \longrightarrow 0$. Puisque notre quantité est entière, elle est nulle à partir d'un certain rang ( il n'y a que 0 comme entier entre $-\frac{1}{2}$ et $\frac{1}{2}$). Autrement dit, on a $\frac{p_n}{q_n} = \frac{p}{q}$ à partir d'un certain rang, absurde car on demandait $0 < |x - \frac{p_n}{q_n}|$.

2- On pose $M = \max_{x \in [\alpha-1;\alpha+1]} |P'(x)| > 0$ (qui est bien défini car $|P'|$ est continue et que l'intervalle est compact et est non nul sinon $P'$ serait nul car aurait une infinité de racine et donc $P$ serait constant). Pour tout $\frac{p}{q}$ dans cet intervalle, on a $|P(p/q)| \leq M|\alpha - \frac{p}{q}|$ par théorème des accroissements finis. De plus, on $q^d P(p/q) \in \mathbb{Z}$ et ce nombre n'est pas nul sinon $P$ est divisible par $X - \frac{p}{q}$ et par irréductibilité de $P$, on aurait alors $P$ de degré 1. Ainsi, pour tous ces $\frac{p}{q}$, on a $|x - \frac{p}{q}| \geq \frac{1}{Mq^d}$. Il suffit donc de poser $c = \min(1, \frac{1}{M})$.

3- Un $P$ tel que l'on se l'est donné existe et on montre facilement que $c = 0$ si $\alpha$ était de Liouville.

4-Il suffit de vérifier que ce nombre est de Liouville en considérant la somme partielle.

## 16.8 Autour des irrationnels

1- Soit $\alpha > 0$ un irrationnel. Montrer que pour tout $\epsilon > 0$ il existe $p, q \in \mathbb{Z}$ tels que $0 < p\alpha - q \leq \epsilon$.

2- Montrer que l'on peut se restreindre à $p, q \in \mathbb{N}$.

3- Soient $a, b \in \mathbb{R}_+^*$ tels que $\frac{a}{b} \notin \mathbb{Q}$. Montrer que $a\mathbb{N} - b\mathbb{N}$ est dense dans $\mathbb{R}$.

## 16.9 Points entiers sur un disque

On note $N(r)$ le nombre de point à coordonnées entières appartenant au disque de rayon $r$. Montrez que l'on a $N(r) \underset{n\to\infty}{\sim} \pi r^2$.

***Correction:*** On découpe le cercle à l'aide du quadrillage donnée par les droites $x = n$ et $y = n$ où $n$ est un entier de $[-r, r]$. L'aire du disque de rayon $r$ vaut exactement $\pi r^2$. On a donc $\pi r^2 = A(r) + B(r)$ où $A(r)$ est la somme des aires des carrés obtenus par le quadrillage et $B(r)$ le reste.

La partie du disque correspondant au reste est

$$\{(x, y) : \exists n \in \mathbb{N}, n \in [-r, r], (n, y_n) \leq (|x|, |y|)\}$$

pour l'ordre lexicographique, où $y_n = \lfloor \sqrt{r^2 - n^2} \rfloor$. On remarque que l'on a, pour tout $n$ entier de $[-r, r]$,

$$n^2 + y_n^2 \geq n^2 + (\sqrt{r^2 - n^2} - 1)^2 \geq 1 + r^2 - 2\sqrt{r^2 - n^2} \geq (r-1)^2.$$

Ainsi, cette partie du disque se trouve entre le cercle de rayon $r-1$ et celui de rayon $r$ donc son aire est majorée par $\pi(r^2 - (r-1^2) = \pi(2r-1) = \underset{n\to\infty}{o}(r^2)$.

Intéressons-nous maintenant à $A(r)$. Tous les carrés le constituant sont d'aire égale à 1. De plus, (en comptant les carrés de gauche à droite et de haut en bas et) en attribuant à chaque carré le point qui se trouve dans le coin supérieur gauche, on constate qu'il y a $N(r) - C(r)$ carrés, où $C(r)$ est le nombre de points entiers appartenant à la dernière droite horizontale et au disque de rayon $r$. On a $C(r) \leq 2\lfloor r \rfloor = \underset{n\to\infty}{o}(r^2)$, d'où le résultat annoncé.

## 16.10 Le tueur fou

Safik n'a pas été admissible aux ENS. Fou de rage, il prend le fusil à pompe de son père - qui est chasseur - et va en ville. Une fois arrivé, il tombe nez à nez avec les membres d'une secte satanique, tous fana de stats. Ces $n$ personnes étaient toutes disposées selon un cercle ; elles portaient toutes un maillot de foot, tous numérotés de 1 à $n$ et les numéros apparaissent dans l'ordre strictement croissant quand on part du numéro un et que l'on marche dans le sens trigonométrique. Dans sa colère, Safik décida de tous les tuer, à l'exception d'une personne, en suivant ces règles :

-Safik tue d'abord le numéro 1

-Il marche dans le sens trigonométrique et tue une personne sur 2 : il tue le numéro 1, puis le 3, puis le 5 (si $n > 4$) ...

-Le dernier en vie est le seul à pouvoir repartir en vie.

Quel est le numéro du dernier en vie ?

***Indication:*** On tâchera d'intuiter une formule avant de la montrer par récurrence.

***Correction:*** On montre par récurrence forte que le numéro $2n - 2^{\lceil \log_2(n) \rceil}$ est le survivant. On laisse au lecteur le soin de vérifier l'initialisation sur quelques $n$. Il suffit de constater qu'après le premier tour, tous les numéros impairs sont morts et d'effectuer une nouvelle numérotation tout en conservant l'ordre des éliminations :

-si $n$ est pair, alors la dernière victime du premier tour est $n-1$ et la suivante est 2. Ainsi, on se retrouve dans le cas où il y a $n/2$ personnes, que le numéro 2 du cercle à $n$ personnes jouent le role du numéro 1 dans le cercle à $n/2$, ..., le numéro $2k$ celui du numéro $k$. On applique la formule de récurrence et conclut.

-Si $n$ est impair, alors la dernière victime du premier tour est $n$, la suivante est le numéro 4. En fait, on se retrouve dans le cas du cercle à $\frac{n-1}{2}$ personnes, 4 joue le rôle de 1, ..., $2k$ celui de $k-1$ si $1 < k$ et 2 celui de $\frac{n-1}{2}$. Si, avec cette nouvelle numérotation, $i$ est le numéro du survivant, alors, quand $i \neq \frac{n-1}{2}$, alors

dans l'ancienne numérotation, le survivant est le numéro $2(i+1)$ et on conclut lorsque $n$ n'est pas de la forme $2^k+1$. Pour ce dernier cas, on montre par récurrence (de façon indépendante) que $n$ est une puissance de 2 si et seulement si $n$ est le survivant.

## 16.11 L'absurde

On suppose que $1=2$. Montrer que je suis le pape.

***Correction:*** L'ensemble $\{moi, pape\}$ est non vide donc de cardinal plus grand que 1 mais est aussi de cardinal plus petit que $2=1$ donc est de cardinal 1.

## 16.12 Le jus et la bière

Sofia va au bar rencontrer un ami mais elle est forcée d'amener son frère Dylan. Sofia se commande une bière et prend un verre de jus pour son frère. Les deux verres contiennent la même quantitée de bière et de jus respectivement. Pendant que Sofia a le dos tourné, Dylan prend une cuillière de bière, la met dans son verre de jus et homogénise le tout avant de mettre une cuillière de son verre de "jus-bière" dans le verre de Sofia.

Y a-t-il plus de jus dans le verre de bière que de bière dans le verre de jus ? Le contraire ? Y en a-t-il autant ?

***Correction:*** Autant !

## 16.13 Caractérisation de la suite nulle

Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite de complexes vérifiant, pour tout $j\in\mathbb{N}^*$ $\sum_{n=1}^{\infty} a_{nj}=0$. Montrer que $(a_n)$ est nulle !

***Correction:*** Disons que l'on veut montrer que $a_j$ est nulle. On a $\sum_{n=1}^{\infty} a_{nj}=0$. On enlève la somme des $a_{2nj}$ puis on enlève la somme des $a_{3nj}$ qui sont pas de la forme $a_{2nj}$ (cette somme est tj nulle pcq c'est la somme des $a_{3nj}$ moins celle des $a_{6nj}$) etc etc.

## 16.14 Pavage de carrés ...

Quels sont les nombres de carrés avec lesquels on peut paver un carré ?

***Correction:*** Tous sauf $2, 3$ et $5$ !

On traitera ces cas plus tard. Montrons d'abord que si l'on a $n$ alors on a $n+3$. En effet, il nous suffit de couper le carré en quatre parts égales et de paver un de ces sous-carrés avec $n$ carrés.

On peut paver un carré avec 6 carrés : si notre carré initiale est de taille $1\times 1$, il nous suffit de placer un carré $\frac{2}{3}\times\frac{2}{3}$ en haut à gauche puis de combler le reste avec des carrés de taille $\frac{1}{3}\times\frac{1}{3}$.

On peut paver un carré avec 7 carrés : on sait faire 4 et donc on sait faire $4+3$.

On peut paver un carré avec 8 carrés : si notre carré initiale est de taille $1 \times 1$, il nous suffit de placer un carré $\frac{3}{4} \times \frac{3}{4}$ en haut à gauche puis de combler le reste avec des carrés de taille $\frac{1}{4} \times \frac{1}{4}$.

Par conséquent, on sait faire tous les nombres plus grand que 6 et on sait également faire 4. On sait aussi faire 1. Les seuls cas qui nous restent à traiter sont donc $2, 3$ et 5.

On ne peut pas paver un carré avec 2 carrés : disons que le premier sous-carré est en haut à gauche (quitte à retourner la figure) et de taille $x \times x$. Alors, le deuxième carré recouvre forcément le bord supérieur droit et on a donc qu'il est de taille $1-x \times 1-x$. On voit bien que l'aire totale n'est pas recouverte puisque $x^2 + (1-x)^2 < x + 1 - x = 1$.

On ne peut pas paver un carré avec 3 carrés : disons que le premier sous-carré est en haut à gauche et de taille $x \times x$. Deux cas se présentent : soit le bord supérieur droit est recouvert par les 2 autres carrés, dans quel cas on a de même un soucis d'aire. Sinon, le bord supérieur droite à recouvert par un seul carré, de taille $1-x \times 1-x$. Forcément, le bord inférieur gauche est lui aussi recouvert par un seul carré de taille $1-x \times 1-x$ et de même on a un soucis d'aire si $x \geq \frac{1}{2}$ ou ce n'est pas un pavage si $x \leq \frac{1}{2}$.

Pour 5 ça commence à devenir embêtant.

### 16.15 Potion mortelle

On a 1000 potions dont exactement une est mortelle et on veut savoir laquelle. Pour ce faire, on dispose de rats pour les tester : si un rat boit la potion empoisonnée, il meurt le lendemain. Il est tout a fait possible de donner plusieurs potions à un même rats et il est également possible de donner une même potion à plusieurs rats. Montrer qu'avec 10 rats on peut savoir quelle est la potion empoisonnée dès le lendemain.

***Correction:*** Remarquons que l'on a $2^10 = 1024 > 1000$. On numérote les potions de 1 à 1000 et on appelle les rats $R_1, ..., R_{10}$. Pour tout $k \in [\![1; 1000]\!]$, on donne la potion numéro $k$ aux rats $R_j$ avec $j$ qui est tel que le $j$-ème chiffre de $k$ en base 2 soit 1.

Notons $i$ le numéro de la potion mortelle. Le lendemain, les numéros des rats morts indiquent où sont les 1 dans l'écriture binaire de $i$ (il y a donc des 0 ailleurs) et on retrouve ainsi $i$.

## 17 Ensemble / Dénombrement

### 17.1 Fonction 1-Lipschitzienne et point fixe (Oral ENS Lyon)

Soit $f : \mathbb{R} \to \mathbb{R}$ telle que :

$$\forall x, y \in \mathbb{R} \quad |f(x) - f(y)| \leq |x - y|.$$

Montrer que l'ensemble des points fixes de $f$ est un intervalle de $\mathbb{R}$.

***Correction:*** Si $a, b$ sont 2 éléments de cet ensemble et que $x \in [a, b]$, on a $b - a = |b - a| = |f(b) - f(x) + f(x) - f(a)| \leq |b - x| + |x - a| = b - a$ donc il y a égalité dans les inégalités utilisées, d'où $f(x) = x$.

## 17.2 Caractérisation de l'égalité ensembliste

Soient $A, B, X$ 3 parties (d'un même ensemble) telles que $A \cap X = B \cap X$ et $A \cup X = B \cup X$. Montrer que $A = B$.

***Correction:*** On a

$$\begin{aligned} A &= [A \cap X] \cup [A \cap X^c] \\ &= [B \cap X] \cup [(A \cup X) \cap X^c] \\ &= [B \cap X] \cup [(B \cup X) \cap X^c] \\ &= B. \end{aligned}$$

## 17.3 Cardinal de $GL_n(\mathbb{F}_q)$ et $Sl_n(\mathbb{F}_q)$

Dénombrer ces deux ensembles.

***Indication:*** Pour le premier, on pourra compter le nombre de famille libre à $0 < k \leq n$ éléments de $(\mathbb{F}_q)^n$. Pour le second, on pourra utiliser ce qui précède et la fonction $M \mapsto M/det(M)$.

***Correction:*** On suit les indications. Pour le premier vecteur, on a $q^n - 1$ choix (il faut simplement qu'il ne soit pas nul). Pour le second, il ne faut pas qu'il soit dans l'espace vectoriel engendré par le 1er : on a donc $q^n - q$ choix, pour le troisième $q^n - q^2$ choix etc. On peut formaliser avec une récurrence en remarquant que $(e_1, ..., e_k)$ est libre si et seulement si $(e_1, ..., e_{k-1})$ est libre et $e_k \notin Vect(e1, ..., e_{k-1})$. En bref, il y a $(q^n - 1)(q^n - q)...(q^n - q^{k-1})$ familles libres composées d'exactement $k$ vecteurs. Le cas particulier $k = n$ donne le cardinal de $GL(\mathbb{F}_q)$ puisqu'une matrice est inversible si et seulement si ses colonnes forment une base de $(\mathbb{F}_q)^n$ si et seulement si cette famille est libre (car de taille de maximale).

Pour ce qui est de $Sl_n(\mathbb{F}_q)$, il suffit d'utiliser le morphisme mentionné en regardant que son noyau contient $q - 1$ éléments qui sont les $kI_n$ avec $k$ non nul. On conclut en utilisant le théorème d'isomorphisme.

Sinon, on aurait aussi pu utiliser le morphisme *det* et procéder de même. On trouve donc $Card(Sl_n(\mathbb{F}_q)) = \dfrac{(q^n - 1)(q^n - q)...(q^n - q^{n-1})}{(q - 1)}$.

### 17.4 Densité de certains sous-groupes de $\mathbb{R}_+$

Soient $a, b \in \mathbb{R}^*$. Montrer que l'on a $a\mathbb{Z} + b\mathbb{Z}$ dense dans $\mathbb{R}$ si et seulement si $\frac{a}{b}$ est irrationnel.

***Correction:*** Supposons $a\mathbb{Z} + b\mathbb{Z}$ dense. Si, par l'absurde, on pouvait écrire $\frac{a}{b} = \frac{p}{q}$ avec $p, q$ deux entiers premiers entre eux alors on aurait $a\mathbb{Z} + b\mathbb{Z} = \frac{b}{q}\mathbb{Z}$ puisque $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$ par Bezout. Ainsi, $a\mathbb{Z} + b\mathbb{Z}$ ne saurait être dense.

L'autre sens se fait également par l'absurde/contraposée. En effet, si $a\mathbb{Z}+b\mathbb{Z}$ n'est pas dense alors (exercice classique, se référer à l'exercice "Sous-groupes de $(\mathbb{R}, +)$ de la section théorie des groupes) alors il existe un certain réel $c > 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$ et donc il existe des entiers $p, q$ tels que $a = cp$, $b = cq$ et donc $\frac{a}{b}$ est rationnel.

## 18 Arithmétique

### 18.1 Un produit

Trouver les $a > 0$ tels qu'il existe des entiers $n, s, m_1...m_n, k_1...k_s$ tous strictement positifs, que les $m_i$ soient 2 à 2 distincts, les $k_i$ aussi et :

$$(a^{m_1} - 1)...(a^{m_n} - 1) = (a^{k_1} + 1)...(a^{k_s} + 1)$$

***Correction:*** On se donne de tels objets et on distingue 2 cas (qui viennent naturellement en se demandant ce que deviennent les 1) :

-si $n$ est impair, on a, $-1 = 1[a]$ d'où $a = 2$ ou $a = 1$. On voit que $a = 1$ n'est pas possible car le produit de gauche est toujours nul tandis que celui de droite ne l'est pas. De plus, $a = 2$ est possible car on a $2^2 - 1 = 2^1 - 1$.

-sinon, on peut supposer $n$ pair et $a > 2$. Soit $p$ un diviseur premier de $a-1$ (il en existe car $a - 1 > 1$). L'égalité donnée implique qu'il existe $j > 0$ tel que $p \mid a^j + 1$. Il s'ensuit que $a^j = 1 = -1[p]$ d'où $p = 2$ et ainsi $a$ s'écrit sous la forme $a = 2^k + 1$.

### 18.2 Lifting the exponent

Si $p \geq 3$ est premier, que $p|(x - y)$ , $p \nmid x$ , $p \nmid y$ et que $n > 0$ alors $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$.

***Correction:*** Dans un premier temps, montrons que la formule annoncé est valable lorsque $n = p^N$. Pour ce faire, on va travailler par récurrence sur $N$. On commence avec $N = 1$ ($N = 0$ est vraie mais le cas $N = 1$ nous sera utile).

On a, par la formule de factorisation de Bernouilli :

$$x^p - y^p = (x - y)\sum_{k=0}^{p-1} x^{p-1-k}y^k$$

d'où il vient

$$v_p(x^p - y^p) = v_p(x-y) + v_p(\sum_{k=0}^{p-1} x^{p-1-k}y^k).$$

Montrons que le dernier $v_p$ vaut 1.

On a bien $p|\sum_{k=0}^{p-1} x^{p-1-k}y^k$ puisque l'on a

$$\sum_{k=0}^{p-1} x^{p-1-k}y^k = \sum_{k=0}^{p-1} x^{p-1-k}x^k = px^{p-1}[p]$$

(on a supposé $x = y[p]$ dans l'énoncé).

De plus, on ne peut pas avoir $p^2|\sum_{k=0}^{p-1} x^{p-1-k}y^k$. En effet, on peut écrire $y = x + pu$ pour un certain entier $u$. Notons $1/x$ un inverse de $x$ modulo $p^2$. Puisque $p \geq 3$, on a

$$\begin{aligned}
\sum_{k=0}^{p-1} x^{p-1-k}y^k &= x^{p-1}\sum_{k=0}^{p-1}(1+pu/x)^k \ [p^2] \\
&= x^{p-1}\sum_{k=0}^{p-1} 1 + kpu/x \ [p^2] \\
&= x^{p-1}(p + \frac{p(p-1)}{2}pu/x) \ [p^2] \\
&= px^{p-1} \ [p^2]
\end{aligned}$$

qui ne peut être nul modulo $p^2$, sans quoi le lemme de Gauss donnerait $p|x$.

Procédons à l'hérédité. Soit $N > 1$. Supposons que l'énoncé est vrai pour tout $x, y$ vérifiant les hypothèses de l'énoncé et lorsque $n = p^{N-1}$. On a alors

$$v_p(x^{p^N} - y^{p^N}) = v_p((x^{p^{N-1}})^p - (y^{p^{N-1}})^p) = v_p(x^{p^{N-1}} - y^{p^{N-1}}) + 1$$

par le cas $N = 1$ ($x^{p^{N-1}}$ et $y^{p^{N-1}}$ vérifient bien les hypothèses de l'énoncé) et on conclut simplement en faisant appel à l'hypothèse de récurrence.

Pour (presque) finir, montrons que la formule tient lorsque $p$ ne divise pas $n$. Comme précédemment, on a

$$v_p(x^m - y^m) = v_p(x-y) + v_p(\sum_{k=0}^{m-1} x^{m-1-k}y^k).$$

De plus, on a $v_p(\sum_{k=0}^{m-1} x^{m-1-k}y^k) = 0$ puisque l'on a

$$\sum_{k=0}^{m-1} x^{m-1-k}y^k = mx^{m-1} \neq 0 \ [p].$$

On conclut maintenant dans le cas général en écrivant $n = p^N m$. Par ce qui précède, on a $v_p(x^n - y^n) = v_p(X^m - Y^m) = v_p(x^{p^N} - y^{p^N})$ où $X = x^{p^N}, Y = y^{p^N}$ et le résultat prouvé par récurrence nous permet de conclure.

## 18.3 Un carré (Oral ENS Lyon 2015)

Trouver les $n > 0$ tels que $n^2 \mid 2^n + 1$.

***Correction:*** Le cas $n = 1$ convient. Supposons maintenant que $n$ est solution et que l'on a $n > 1$. Alors, $n$ admet des diviseurs premiers. Remarquons également que $n$ est nécessairement impair (sans quoi on aurait $2|n^2|2^n + 1$). Soit $p$ le plus petit diviseur non trivial de $n$ (qui sera naturellement premier et impair). On a $p|2^n + 1$, si bien que l'on a $2^{2n} = 1$ dans $\mathbb{F}_p$. Ainsi, on a que l'ordre de 2 dans $\mathbb{F}_p^*$ divise $2n \wedge p - 1$. De plus, on a $2|p - 1$ puisque $p$ est impair et on a aussi $n \wedge p - 1 = 1$ car $p$ est le plus petit diviseur non trivial de $n$ et que tout diviseur de $p - 1$ est strictement inférieur à $p$. On en déduit que l'ordre de 2 divise 2, c'est-à-dire que l'on a $2^2 = 1$ dans $\mathbb{F}_p$, i.e. $p|3$ puis $p = 3$ (ou encore $v_3(n) \geq 1$).

On a aussi $v_3(n^2) \leq v_3(2^n - (-1)^n)$ et l'exercice précédent donne alors

$$2v_3(n) \leq v_3(2 - (-1)) + v_3(n)$$

d'où $v_3(n) = 1$ (les hypothèses de l'exercice précédent sont bien vérifiées).

Maintenant, supposons par l'absurde que l'on a $n > 3$. Soit $p$ le plus petit diviseur de $n$ strictement supérieur à 3 (on a naturellement $p$ premier de nouveau puisque $v_3(n) = 1$ et que $n$ est impair). Comme précédent, l'ordre de 2 dans $\mathbb{F}_p^*$ divise $2n \wedge p - 1$. On distingue deux cas : soit $n \wedge p - 1 = 1$, dans quel cas l'ordre de 2 divise 2 et comme précédemment, on obtient $p = 3$, absurde. Soit on a $n \wedge p - 1 \neq 1$ mais puisque tout diviseur de $p - 1$ est strictement inférieur à $p - 1$, on a nécessairement $n \wedge p - 1 = 3$, donc l'ordre de 2 divise 6. Si l'ordre de 2 est 2, on se retrouve dans le cas précédent et on aboutit à la même absurdité. Si c'est 6, on a $2^6 = 1$ dans $\mathbb{F}_p$ puis $2^3 = -1$ et donc $p|2^3 + 1$, d'où $p = 3$, absurde de nouveau. Si c'est 3, on a $2^3 = 1$ dans $\mathbb{F}_p$ puis $p|2^3 - 1$ et donc $p = 7$, ce qui conduit à $7|n^2|2^n + 1$ mais $2^n + 1 = 2^{3*q} + 1 = 2$ dans $\mathbb{F}_7$ (où $q = \frac{n}{3}$), absurde.

## 18.4 (Facile,sup) Racine dans $\mathbb{Q}$

Trouver une cns sur $p, q \in \mathbb{N}^*$ pour que $\sqrt{\frac{p}{q}} \in \mathbb{Q}$. Etendre ce résultat.

## 18.5 Fonction de Möbius

On définit $\mu : \mathbb{N}^* \to \{-1; 0; 1\}$ par $\mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \text{ a un facteur carré} \\ (-1)^r \text{ si } n = p_1 ... p_r \end{cases}$.

1- Montrer que $\mu$ est multiplicative (i.e $\mu(nm) = \mu(n)\mu(m)$ si $n \wedge m = 1$).

2- Montrer que $\sum_{d|n} \mu(d)$ vaut 1 ou 0 selon que $n$ vaille 1 ou non.

3- Soient $f, g : \mathbb{N}^* \to G$ où $(G, +)$ est un groupe abélien. Démontrer la formule d'inversion :

si pour tout $n$, on a $g(n) = \sum_{d|n} f(d)$ alors on a $f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$.

### 18.6 Nombres premiers et polynômes

1- Soit $P$ tel que pour tout $n \in \mathbb{N}$, l'entier $P(n)$ soit premier. Montrer que $P$ est constant.

2- Ce résultat tient-il toujours si l'on suppose plutôt que $P(n)$ soit premier pour une infinité de $n$ ?

***Correction:*** Non, penser à Dirichlet faible : considérer $1 + 2X$.

## 19 Probabilités

### 19.1 Suite équirépartie modulo 1 (Oral ENS ULCR 2019)

On dit que $(x_n) \in \mathbb{R}^{\mathbb{N}}$ est équirépartie modulo 1 si pour tout $a < b$, $a, b \in [0; 1]$, on a

$$\frac{1}{n} Card \{k \in [\![0; n]\!] : x_k - \lfloor x_k \rfloor \in [a, b]\} \longrightarrow b - a.$$

On admet le critère de Weyl : $(x_n)$ est équirépartie modulo 1 ssi

$$\forall p \in \mathbb{Z} \quad \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi p x_k} \longrightarrow 0.$$

1- Montrer que $(n log_{10}(2))$ est équirépartie modulo 1.

2- Pour tout $n \geq 1$, on se donne une variable aléatoire $X_n$ à valeur dans $[\![1; n]\!]$ équiprobable. Etudier, quand $n \to \infty$, le comportement de la probabilité que le premier chiffre (celui de poids maximal) de $2^{X_n}$ soit j.

***Indication:*** Une question faisait remarquer que $log_{10}(2)$ est irrationnel.

## 20 Intégration de Lebesgue

### 20.1 Une mesure particulière

Caractériser les mesures $\mu$ sur $\mathcal{B}(\mathbb{R})$ vérifiant :

$$\forall X \in \mathcal{B}(\mathbb{R}), \quad \mu(X) < \infty \quad ou \quad \mu(\mathbb{R} \setminus X) < \infty.$$

***Correction:*** Ce sont les mesures finies et celles pour lesquelles il existe $x \in \mathbb{R}$ tel que $\mu(\{x\}) = \infty$ et $\mu(\mathbb{R} \setminus \{x\}) < \infty$.

Il est facile de voir que ces mesures vérifient la propriété.

Supposons donnée une mesure $\mu$ non-finie vérifiant cette propriété. Ainsi, le "ou" apparaissant dans la propriété est strict. De plus, on a, par continuité de

la mesure, $\mu(\mathbb{R} \setminus [-n,n]) \xrightarrow[n\to\infty]{} 0$. Alors, il existe $n$ vérifiant $\mu(\mathbb{R} \setminus [-n,n]) < \infty$ i.e $\mu([-n,n]) = \infty$.

En faisant une dichotomie, on montre alors l'existence d'un $x$ tel que

$\mu(\{x\}) = \infty$ : on a $\mu([-n,0]) = \infty$ ou $\mu([0,n])$ puis on répète indéfiniment l'opération en coupant en 2 (au milieu) le segment de mesure infinie et on utilise la continuité de la mesure. Par hytpohèse, on a également $\mu(\mathbb{R} \setminus \{x\}) < \infty$.

### 20.2 Les non-boréliens

Si $A \subset \mathbb{R}$ n'est pas un borélien, montrer que $A \times \{0\}$ n'est pas borélien.

***Correction:*** $x \mapsto (x,0)$ est continue sur $\mathbb{R}$ donc c'est une fonction borélienne. Par l'absurde, supposons qu'il existe $A$ contredisant l'énoncé. Alors, on aurait $A = f^{-1}(A \times \{0\})$ borélien, ce qui est exclu.

## 21 Analyse complexe

### 21.1 Fonction holomorphe sur le disque unité

Soit $f : \overline{D(0,1)} \to \mathbb{C}$ une fonction holomorphe.

1- Montrer que si $f$ est nulle sur le cercle unité alors $f$ est identiquement nulle.

2- En déduire que si $f$ est nulle sur un arc de cercle (de longueur non nulle) alors $f$ est nulle.

**Remarque:** On veillera à ne pas utiliser le théorème des zéros isolés.

***Indication:*** Pour la q.2, on pourra remarquer que l'ensemble des fonctions holomorphes sur le disque unité est un anneau intègre.

### 21.2 Fonction entière

Soit $f : \mathbb{C} \to \mathbb{C}$ holomorphe et non constante. Montrer que son image est dense.

***Correction:*** Par l'absurde, supposons qu'il existe $b \in \mathbb{C}, \epsilon > 0$ tels que, pour tout $z \in \mathbb{C}$, $|f(z) - b| > \epsilon$. Alors, la fonction $z \mapsto \frac{1}{f(z)-b}$ est bien définie, entière et bornée. Ainsi, elle est constante donc $f$ l'est aussi.

**Remarque:** En fait, le théorème de Picard dit que son image est soit tout $\mathbb{C}$, soit $\mathbb{C}$ privé d'un point.

### 21.3 Caractérisation des polynômes

Montrer que si $f$ est une fonction entière vérifiant $|f(z)| \leq A + B|z|^k$ pour tout $z$ de module assez grand ($A, B$ et $k$ ne dépendent pas de $z$) alors $f$ est un polynôme.

## 21.4 Singularité, série entière et bijection (Tauvel)

1- Soit $f$ une fonction entière. On pose $g(z) = f(\frac{1}{z})$. Montrer que $f$ est un polynôme si et seulement si $g$ admet 0 pour singularité non-essentielle.

2- Dans cette question, on se donne $U$ un ouvert de $\mathbb{C}$, $A$ une partie localement finie de $U$, $f$ une fonction injective et holomorphe sur $U \setminus A$.

a) Montrer que si $a \in A$ alors $f$ n'a pas de singularité essentielle en $a$.

b) De plus, montrer que si $a \in A$ est un pôle de $f$, alors $a$ est un pôle d'ordre 1.

c) Montrer que si tout point de $A$ est une singularité illusoire, alors le prolongement holomorphe de $f$ à $U$ est injectif.

3- a) Déterminer les polynômes de $\mathbb{C}[X]$ bijectifs de $\mathbb{C}$ dans lui-même.

b) Déduire de ce qui précède les séries entières sur $\mathbb{C}$ réalisant une bijection de $\mathbb{C}$ dans lui-même.

***Correction:*** 1- Si $f$ est un polynôme, on a $\frac{f(z)}{z^{deg(f)+1}} \xrightarrow[|z|\to\infty]{} 0$. En particulier, on a $g(z)z^{deg(f)+1} \xrightarrow[|z|\to 0]{} 0$ donc 0 est soit un pôle soit une singularité illusoire de $g$.

Réciproquement, on a un $m$ tel que $\frac{f(z)}{z^m} \xrightarrow[|z|\to\infty]{} 0$ et on peut utiliser l'exercice précédent pour en déduire que $f$ est un polynôme : il existe $B(0,r)$ tel que $|f(z)| \leq |z|^m$ hors de cette boule.

2-a) Sans perdre en généralité, on suppose $U = B(a,R)$ et $A = \{a\}$. Soit $0 < r < R$. Raisonnons par l'absurde. On aurait alors $f(B(a,r))$ dense dans $\mathbb{C}$ mais on a $f(B(a,r)) \cap f(B(a,R) \setminus B_f(a,r)) = \emptyset$ par injectivité de $f$ et $f(B(a,R) \setminus B_f(a,r))$ ouvert (puisque $f$ est holomorphe, c'est une application ouverte), asburde.

b) S'il est d'ordre $k$, on sait que c'est un zéro d'ordre $k$ de $1/f$ (qui est aussi injective) et qu'il existe un voisinage $U$ de $a$ et $V$ de $1/f(a)$ tels que tout élément de $V \setminus \{1/f(a)\}$ admette exactement $k$ antécédents dans $V \setminus \{a\}$. Ainsi, on l'injectivité de $1/f$ force $k = 1$.

c) Il faut utiliser le théorème d'inversion locale.

3-a) En fait, il est facile de voir que les polynômes non-constants sont tous surjectifs : il suffit d'appliquer le théorème de d'Alembert à $P - \lambda$ pour avoir qu'il existe $z$ tel que $P(z) = \lambda$.

Pour l'injectivité, en particulier, on a que notre polynôme $P$ ne s'annule qu'au plus en un point. Ainsi, puisque $P$ n'est pas constant, on peut écrire $P = \lambda(X-a)^n$. On constante que $P$ prend les mêmes valeurs en les $a+\epsilon$ avec $\epsilon$ racine $n^{eme}$ de l'unité. Finalement, on a donc que $P$ est de degré 1 (pour n'avoir qu'une racine $n^{eme}$ de l'unité) et réciproquement, on vérifie que tout polynôme de degré 1 convient.

b) Si $f$ est une telle série entière, on a par les questions $2-a$ (appliquée à $U = \mathbb{C}$, $A = \{0\}$ et $g$ à la place de $f$, en reprenant les notations de la q.1) et 1, on on obtient que $f$ est un polynôme. La question précédente conclut.

# 22 Banach et topologie faible

## 22.1 Base de Schauder (exo 13 TD 1)

1- c) On travaille par réc sur $n$. On a $y_{n+1} \in Vect(e_0, ..., e_{n+1})$ parce que ce dernier ev est fermé. De plus, on a $S_{n+1}(x_j) = S_n(x_j) + a_{n+1}(x_j)e_{n+1}$. En passant à la limite quand $j \to \infty$, on obtient le résultat attendu ($a_{n+1}(x_j)$ converge parce que les normes sont équivalentes en dim finie).

d)

2- Pour le sens indirect, on commence par montrer l'uncicité.

Si $(a_k(x))$ et $(b_k(x))$ vérifie ce à quoi on pense, alors on a $||(a_0(x)-b_0(x))e_0|| \leq C||\sum_{k=0}^{n}(a_k(x) - b_k(x))e_k||$ pour tout $n$. En faisant tendre $n \to \infty$, on obtient $||(a_0(x) - b_0(x))e_0|| = 0$ et puisque $e_0 \neq 0$, on a forcément $a_0(x) = b_0(x)$. On procède de même pour les suivants (réc sur $k$ pour formaliser).

On montre maintenant l'existence. Soit $x \in E$.

Par densité, on sait qu'il existe $(a_{k,n})$ tel que $\sum_{k=0}^{n} a_{k,n}e_k \to x$. Montrer que, pour tout $k$, la suite $(a_{k,n})_{n\geq 0}$ converge en montrant qu'elle est de Cauchy.

On a $||(a_{0,p} - a_{0,q})e_0|| \leq C||\sum_{k=0}^{p} a_{k,p}e_k - \sum_{k=0}^{q} a_{k,q}e_k||$ donc $(a_{0,n})$ est de Cauchy. On procède par récurrence sur $k$ pour démontrer le résultat attendu de la même façon. On note $a_{k,\infty}$ la limite de $(a_{k,n})$.

Montrons finalement que $\sum_{k=0}^{n} a_{k,\infty}e_k$ converge vers $x$. Remarquons que l'on a, pour tout $p, q > N$, $||\sum_{k=0}^{N}(a_{k,p} - a_{k,q})e_k|| \leq C||\sum_{k=0}^{p} a_{k,p}e_k - \sum_{k=0}^{q} a_{k,q}e_k||$. En faisant tendre $p$ vers l'infini, on obtient $||\sum_{k=0}^{N}(a_{k,p}-a_{k,q})e_k|| \leq C||x-\sum_{k=0}^{q} a_{k,q}e_k||$, ce qui conclut.

## 22.2 Fonction (presque) surjective

Soient $E, F$ deux Banach et $T \in \mathcal{L}(E, F)$ une application linéaire continue presque surjective i.e :

$$\exists\ 0 < \alpha < 1\ \exists r > 0\ :\ \forall y \in \overline{B_F(0,1)}\ \exists x \in \overline{B_E(0,r)} \quad ||y - T(x)|| \leq \alpha.$$

1- Soit $y \in \overline{B_F(0,1)}$. Montrer qu'il existe $(x_n) \in \overline{B_E(0,r)}$ telle que :

$$||y - T(x_1) - \alpha T(x_2) - ... - \alpha^{n-1}T(x_n)|| \leq \alpha^n.$$

2- Montrer que pour tout $y \in \overline{B_F(0,1)}$, il existe $x \in \overline{B_E(0, \frac{r}{1-\alpha})}$ tel que $y = T(x)$.

3- En déduire que $T$ est surjective.

4- Soit $S$ l'ensembles des applications linéaires continues surjectives de $E$ dans $F$. Montrer que $S$ est un ouvert.

5- Suite dans le poly, flemme.

***Correction:*** 1- On crée $x_n$ par rec en disant que $x_{n+1}$ est donné par l'hypothèse appliquée à $\frac{1}{\alpha^n}(y - T(x_1) - \alpha T(x_2) - ... - \alpha^{n-1}T(x_n))$ à la place de $y$.

2- $\sum \alpha^{n-1}T(x_n)$ converge car $F$ est un Banach et conv abs. De la plus, sa somme vaut $y$ (en faisant tendre $n$ vers l'infini dans l'inégalité de la q. précédente).

3- Oui.

4- Par le théorème de l'application ouverte, si $T_0$ est surjective, alors $T$ est presque surjective (on peut prendre $\alpha = 0$). On note $r$ le $r$ de la définition de presque surjective pour $T_0$

Ensuite, on montre que si $T \in B(T_0, \frac{1}{2r})$, on a $T$ presque surjective : si $||y|| \leq 1$, on sait que $T_0$ est presque surjective, on prend $||x|| \leq r$ tel que $T_0(x) = y$ et on a $||y - T(x)|| <= \frac{1}{2}$.

## 22.3 Théorème de Eberlein-Smuli

On veut montrer que si $E$ est un evn et $A$ une partie faiblement compacte de $E$, alors $A$ est séquentiellement faiblement compacte.

Soit $E$ un evn.

1- Montrer que si $E$ est séparable alors $E$ admet une famille dénombrable $(l_j)_{j\in\mathbb{N}} \subset E^{'}$ séparant les points et toutes de norme 1.

2- Montrer que si $E$ admet une famille dénombrable de formes linéaires continues séparant les points alors les compacts faibles sont métrisables.

3- Conclure en montrant $A \cap F$ est séquentiellement faiblement compacte dans $F = \overline{Vect(a_n)_{n\in\mathbb{N}}}$.

1- Soit $D = \{d_n : n \in \mathbb{N}\}$ dense dans $E$. On sait qu'il existe $f_n \in E^{'}$ telle que $||f_n|| = 1$ et $|f_n(d_n)| = ||d_n||$. Cette famille convient : si $x$ est tel que $f_n(x) = 0$ pour tout $n$, alors on a, en prenant $d_{\varphi(n)} \xrightarrow[n\to\infty]{} x$ :

$$||x|| \leq ||x - d_{\varphi(n)}|| + \underbrace{||d_{\varphi(n)}||}_{\substack{=|f_{\varphi(n)}(d_{\varphi(n)})| \\ =|f_{\varphi(n)}(d_{\varphi(n)} - x)|}} \leq 2||x - d_{\varphi(n)}||.$$

2- On prend $A$ un compact faible, $(f_n)$ séparant les points et on pose $d(x,y) = \sum_{n\geq 1} \frac{|fn(x) - fn(y)| \wedge 1}{2^n}$. C'est bien une distance. On va montrer qu'elle convient.

On veut d'abord montrer qu'un ouvert de $A$ pour cette distance est un ouvert de la topologie faible sur $A$. Il suffit de montrer que c'est bien le cas pour les boules.

Soit $x_0 \in A, r > 0$, $x \in B_d(x_0, r)$ et $N$ tel que $\sum_{n\geq N_0} \frac{1}{2^n} < \varepsilon$ avec $\varepsilon$ tel que $2\varepsilon + d(x, x_0) < r$. Montrons que $B_d(x_0, r)$ contient un voisinage ouvert faible de $x$. Pour tout $y \in V(x, f_1, ..., f_{N-1}, \varepsilon) := \{z \in A : \forall 1 \leq i < N | f_i(z) - f_i(x)| < \varepsilon\}$, on a :

$$\begin{aligned} d(y, x_0) &\leq d(y, x) + d(x, x_0) \\ &\leq \varepsilon \sum_{i=1}^{N-1} \frac{1}{2^n} + \sum_{i\geq N} \frac{1}{2^n} + d(x, x_0) \\ &\leq 2\varepsilon + d(x, x_0) < r. \end{aligned}$$

Ainsi, $B_d(x_0, r)$ est bien un ouvert faible de $A$.

Réciproquement, soit $O$ un ouvert faible de $A$. Supposons, par l'absurde, que $O$ ne soit pas un ouvert pour la topologie liée à $d$. On a donc $x \in O$ et $x_n \in B_d(x, \frac{1}{n})$ tel que $x_n \notin O$. Or, les $B_d(x, \frac{1}{n}) \cap O^c$ sont des compacts faibles de $A$ pour la topologie faible (car fermés dans un compact et la topologie faible est séparée). Par le théorème des compacts emboîtés, on a un certain $z$ dans l'intersection des $B_d(x, \frac{1}{n}) \cap O^c$. Forcément, à cause de la distance qui tend vers 0, on a $z = x$, ce qui est absurde.

3- $F$ est séparable ($Vect_{\mathbb{Q}}(an)$ est dense dans $F$) donc $F$ admet une famille dénombrable séparant les points par la q.1. $A \cap F$ est un compact faible de $F$ et ce dernier est métrisable par la q.2. Ainsi, il est séquentiellement (faiblement) compacte puisque cette notion coïncide avec la notion de compacité dans un espace métrique.

## 22.4 Fonction presque continue

Soient $(E, ||.||_E)$ Banach réflexif, $F$ Banach et $T$ un opérateur compact de $E$ dans $F$. On considère $||.||'_E$ une autre norme sur $E$, moins fine que l'autre. Montrer que l'on a :

$$\forall \varepsilon > 0 \ \exists C > 0 \ \forall x \in E \quad ||T(x)|| \leq \varepsilon ||x||_E + C||x||'_E.$$

***Correction:*** On raisonne par l'absurde. On a $\varepsilon > 0$, $x_n \in E$ tels que

$$||T(x_n)|| \geq \varepsilon ||x_n||_E + n||x_n||_E^{'}.$$

On a évidemment $x_n \neq 0$ pour tout $n$ (sans quoi cette inégalité ne serait pas possible) donc on peut, quitte à diviser par $||x_n||_E$, supposer que l'on a, pour tout $n$, $||x_n||_E = 1$.

Puisque $E$ est un Banach réflexif, on peut alors extraire une sous-suite faiblement convergente de $(x_n)$ : $x_{\varphi(n)} \xrightarrow[n\to\infty]{w} x$.

Remarquons que l'on a $x \neq 0$ puisque $||T(x_n)|| \geq \varepsilon$ donc $||T(x)|| \geq \varepsilon$ en passant à la limite (légitime car $T$ étant compact, on a $T(x_{\varphi(n)}) \xrightarrow[n\to\infty]{} T(x)$) .

Avec l'inégalité obtenue via le raisonnement par l'absurde, on obtient facilement que $||x_n||_E^{'}$ tend vers 0. Ainsi, au sens de la $2^{eme}$ norme, $x_n$ tend fortement, et a fortiori faiblement, vers 0.

De plus, puisque la $2^{eme}$ topologie est moins fine que la $1^{ere}$, on a $x \in (E, ||.||_E) \mapsto x \in (E, ||.||_E^{'})$ continue fort-fort donc continue faible-faible.

Ainsi, puisque $x_n \xrightarrow[n\to\infty]{w} x$ dans $(E, ||.||_E)$, on a également $x_n \xrightarrow[n\to\infty]{w} x$ dans $(E, ||.||_E^{'})$. Absurde puisque dans le premier evn on a $x \neq 0$ et $x = 0$ dans le second.

# 23 Vecteurs de Witt

## 23.1 Propriétés de $A$ et de $W(A)$

Soit $p$ un nombre premier et $A$ un anneau commutatif de caractéristique $p$.

1- Montrer que $A$ est un anneau intègre si et seulement si $W(A)$ l'est.

2- Montrer que $A$ est réduit si et seulement si $W(A)$ l'est.

3- Montrer que $A$ est parfait si et seulement si $W(A)/pW(A)$ est réduit.

***Correction:*** 1 et 2- Il suffit (à peu près) d'utiliser l'application $A \to W(A)$.

3- Supposons $A$ parfait. Alors, on sait que $pW(A) = V_1(A)$ est l'idéal maximal de $W(A)$ et que l'on a $W(A)/pW(A) \simeq A$ qui est donc réduit. En effet, si $x \in A$ est tel qu'il existe $n > 0$ vérifiant $x^n = 0$, alors, quitte à multiplier par une bonne puissance de $x$, on peut supposer que $n$ est une puissance de $p$. Comme $A$ est parfait, le frobenius est un automorphisme et cela donne $x = 0$.

Réciproquement supposons $W(A)/pW(A)$ réduit. Montrons que le frobenius est injectif. Soit $x \in A$ tel que $x^p = 0$. En notant $[.] : A \to W(A)$ (notée $\tau$ dans le Bourbaki chap.8 et 9), on obtient $[x]^p = 0$ puis, puisque $W(A)/pW(A)$ est réduit, on en déduit $[x] \in pW(A)$. On a donc $[x] = p.(y_n)_{n\in\mathbb{N}}$ et en identifiant les premières coordonnées, on trouve $x = py_0 = 0$ (car l'addition dans $W(A)$ modifie la première coordonnée en sommant de façon habituelle). Montrons maintenant que le frobenius est surjectif. Dans un premier temps, montrons que l'on a $pW(A) = V_1(A)$. En effet, on a déjà $pW(A) \subset V_1(A)$ (par la formule (52) du Bourabaki). Soit $x \in V_1(A)$. Comme on a $V_1(A)^2 = pV_1(A) \subset pW(A)$, on a $x^2 = 0$ dans $W(A)/pW(A)$ et comme ce dernier est réduit, on a bien $x \in pW(A)$.

On a, pour tout $a \in W(A)$, $p.a = V(F(a))$ et comme $pW(A) = V_1(A)$, cela donne $F$ surjectif i.e. le frobenius est surjectif.

# 24 Théorie du corps de classe

## 24.1 Nombre de classe de certains corps cylotomique

Soit $\mathbb{K} = \mathbb{Q}(\zeta_p)$ où $p$ est un nombre premier impair, $\zeta_p$ une racine primitive $p$-ème de l'unité. Soit $\mathbf{k}$ un corps intermédiaire. Montrer que l'on a $h_{\mathbf{k}} | h_{\mathbb{K}}$.

***Correction:*** On cherche à appliquer le théorème 5 de l'annexe de [Was97]. On doit donc montrer qu'il n'y a pas d'extension intermédiaire de $\mathbb{K}/\mathbf{k}$ qui soit non ramifiée à part $\mathbf{k}$. Cela découle de la relation "degré $= edf$" et du fait qu'il n'y a qu'un seul idéal premier au dessus de $p$. En effet, soit $\mathbb{F}$ un corps intermédiaire. On sait que $p$ est totalement ramifié dans $\mathbb{K}$, d'où $f(\mathbb{F}/\mathbf{k}) = 1$ et si l'on suppose $e(\mathbb{F}/\mathbf{k}) = 1$ on obtient finalement que le degré de $\mathbb{F}/\mathbf{k}$ est 1.

# Références

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields.*, volume 83 of *Grad. Texts Math.* New York, NY : Springer, 2nd ed. edition, 1997.