Vous serez à la rentrée prochaine en MP* et toute l'équipe pédagogique sera ravie de vous recevoir.

Le site de la classe est https://neogene3.fr/MPEtoileToursDescartes/

L'accès à certaines choses nécessite une identification.

Via le menu du site, vous pouvez accéder au forum.
Des identifiants pour le site vous seront communiqués. Ceux du forum sont identiques.

Vous aurez quelques devoirs mathématiques de vacances. Les devoirs seront postés sous forme numérique (écrits sur copies, scannés et convertis au format pdf. Diverses applications pour téléphones font cela) sur le forum, pour le dimanche de la semaine correspondante. Ils seront corrigés, et postés corrigés sous la même forme.

Rien de gigantesque, et il ne s'agit pas de gâcher vos vacances évidemment.
Les documents contiennent quelques rappels de cours, et des compléments à connaître qui nous feront gagner un peu de temps, ainsi que des exercices visant à vous entretenir durant les vacances, afin de ne pas arriver en ayant tout oublié...
Certains exercices sont optionnels

Le fait de sécher sur certains exercices ne préjuge en rien de votre future réussite. L'important est de chercher, et le fait de sécher est intrinsèque à toute activité de recherche.

Le programme est le suivant:
Semaine du 11 juillet: Groupes
Semaine du 18 juillet: Polynômes
Semaine du 25 juillet: Suites
Semaine du 8 août: Arithmétique des entiers
Semaine du 15 août: Algèbre linéaire.
Semaine du 22 août: Séries. Ce dernier devoir sera rendu normalement à la rentrée.

Nous commencerons, à la rentrée, par de l'algèbre linéaire.

Les chapitres de probabilités et d'espaces préhilbertiens et euclidiens sont très importants, mais ne feront pas l'objet d'exercices durant l'été. Des révisions du programme de Sup sur ces chapitres seront programmées durant les vacances en cours d'année scolaire.

Respectez le calendrier, et ne faîtes pas les exercices à l'avance. Le but principal est de vous entretenir régulièrement durant les congés.

1 Quelques rappels et compléments

Une remarque préliminaire: moins un ensemble a d'opérations, moins il y a de contraintes, et plus l'étude est compliquée.
Ainsi l'étude des groupes est plus compliquée que celle des anneaux, elle-même plus compliquée que celle des corps.

Le cours d'algèbre générale sera le dernier chapitre. Mais nous aurons besoin de certains résultats bien avant, principalement la notion d'ordre d'un élément, et la propriété 2.

1.1 Itérés d'un éléments

Il y a essentiellement deux types de notations pour un groupe G:
La notation multiplicative, le composé de x et y étant noté $x \cdot y$, $x \times y$, ou plus simplement en général xy (c'est la notation que j'emploierai). Dans ce cas, on note généralement, ce que je ferai, 1 le neutre. (1_G éventuellement), et x^{-1} le symétrique (appelé inverse) de x
La notation additive, exclusivement réservée à des groupes commutatifs (se dit aussi abéliens), le composé de x et y étant noté $x+y$. Dans ce cas, on note généralement, ce que je ferai, 0 le neutre. (0_G éventuellement), et $-x$ le symétrique (appelé opposé) de x

En notation multiplicative, si $x \in G$, G groupe, et $n \in \mathbb{Z}$, on définit l'itéré n-ième de x, noté x^n, par:
$x^0 = 1$.
$x^n = \underbrace{xx...x}_{n\ termes}$ si $n > 0$. $x^n = \underbrace{x^{-1}x^{-1}...x^{-1}}_{-n\ termes}$ si $n < 0$.
On a facilement $(x^n)^{-1} = x^{-n}$, et plus généralement $(x^n)^m = x^{mn}$ ainsi que $x^m x^n = x^{m+n}$.

En notation additive, si $x \in G$, G groupe, et $n \in \mathbb{Z}$, on définit l'itéré n-ième de x, noté nx, par:
$0x = 0$.
$nx = \underbrace{x+x+...+x}_{n\ termes}$ si $n > 0$. $nx = \underbrace{-x-x...-x}_{-n\ termes}$ si $n < 0$.
On a facilement $-(nx) = (-n)x$, et plus généralement $(m+n)x = mx + nx$.
Il est à noter qu'il n'y a pas de produit, et que nx n'est pas $n \times x$.
nx correspond à un produit si $G = \mathbb{Z}$ par exemple.

1.2 Le théorème de Lagrange

Ce théorème n'est plus au programme de Spé, mais fait partie des quelques résultats hors-programme indispensables en MP*.

Propriété 1: Théorème de Lagrange
Soit G un groupe fini, et H un sous-groupe de G. Alors card(H) (notations autres: $\#H$, $|H|$) divise card(G).

Démonstration
On prend une notation multiplicative.
Soit G un groupe fini, et H un sous-groupe de G.
On peut créer une relation d'équivalence, et utiliser le fait que les classes partitionnent G, mais je préfère le présenter de manière plus élémentaire.
Si $x \in G$, on pose $xH = \{xh \mid h \in H\}$.

Un fait simple d'usage constant: Soit $x \in G$. $t_x : \begin{cases} G \to G \\ y \mapsto xy \end{cases}$ est bijective, de réciproque $t_{x^{-1}}$.
En particulier, t_x est injective, et comme $xH = t_x(H)$, $\text{card}(xH) = \text{card}(H)$.

$G = \bigcup_{x \in G} xH$, car $1 \in H$, donc $x = x \times 1 \in xH$.
On va montrer que, si $x, y \in G$, on a soit $xH = yH$, soit $xH \cap yH = \emptyset$.
De ce fait, dans $\bigcup_{x \in G} xH$, en éliminant les répétitions, on se retrouve avec une union de p ensembles disjoints deux à deux, tous de même cardinal que H, et donc $\text{card}(G) = p\,\text{card}(H)$.

Soient donc $x, y \in G$. Supposons que $xH \cap yH \neq \emptyset$. Il s'agit de montrer que $xH = yH$.
Soit $a \in xH \cap yH$. On peut donc se donner $h_1, h_2 \in H$ tels que $a = xh_1 = yh_2$.
Ainsi $x = yh_2h_1^{-1}$. Notons $h_3 = h_2h_1^{-1}$. $h_3 \in H$ car H est un sous-groupe.
Si $b \in xH$: $b = xh$, $h \in H$, donc $b = y\underbrace{h_3h}_{\in H} \in yH$. Ainsi $xH \subset yH$, et comme on a l'inclusion réciproque en échangeant les rôles de x et y, $xH = yH$. ♣

1.3 Ordre d'un élément

Soit G un groupe et $x \in G$. En notation multiplicative, on dit que x est d'ordre fini si et seulement si $\exists n \in \mathbb{N}^*;\ x^n = 1$ (devient $nx = 0$ en notations additives).
Si x est d'ordre fini, on définit son ordre par $ordre(x) = \min\{n \in \mathbb{N}^* \mid x^n = 1\}$. Ainsi, si $n = ordre(x)$, $x \neq 1$, $x^2 \neq 1$,...,$x^{n-1} \neq 1$, et $x^n = 1$.

Par exemple, dans le groupe $(\mathbb{C}^*, .)$, si $n \in \mathbb{N}^*$, $e^{\frac{2i\pi}{n}}$ est d'ordre n.

Le seul élément d'ordre 1 est le neutre.

Propriété 2:
Soient G un groupe, et $x \in G$

1. Si x est d'ordre fini n, alors $\forall k, p \in \mathbb{Z}$, $x^k = x^p \iff k \equiv p[n]$, et donc (cas $p = 0$), $x^k = 1 \iff n|k$.
2. $Gr(x) := \{x^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de G. ($Gr(x)$ est ce qu'on appelle le sous-groupe engendré par x)
   $Gr(x)$ est fini si et seulement si x est d'ordre fini, et, si x est d'ordre fini, $\text{card}(Gr(x)) = ordre(x)$.
3. **Si G est fini de cardinal n, et $x \in G$, alors x est d'ordre fini, $ordre(x)$ divise n, et donc $x^n = 1$.**

Démonstration

1. On suppose x d'ordre fini n. Soient $k, p \in \mathbb{Z}$.
   On écrit la division euclidienne de $k - p$ par n:
   $k - p = qn + r$, $r \in [\![0, n-1]\!]$.
   $x^k = x^p \iff x^{k-p} = 1 \iff (\underbrace{x^n}_{=1})^q x^r = 1 \iff x^r = 1 \iff r = 0$ car $x \neq 1$, $x^2 \neq 1$,...,$x^{n-1} \neq 1$.
2. $Gr(x)$ est facilement un sous-groupe de G.
   Si x est d'ordre fini, n:
   Si $k \in \mathbb{Z}$, on écrit la division euclidienne de k par n: $k = qn + r$, $r \in [\![0, n-1]\!]$.
   $x^k = x^r$.
   Donc $Gr(x) = \{1, x, x^2, ..., x^{n-1}\}$.
   Par le 1, $1, x, ..., x^{n-1}$ sont distincts deux à deux, car si $0 \leq p < k \leq n-1$, $0 < k - p < n$, donc n ne divise pas $k - p$.
   Donc $\text{card}(Gr(x)) = n$.

   Si $Gr(x)$ est fini:

Comme $\mathbb{Z}$ est infini, il existe $k, p \in \mathbb{Z}$, $k < p$ tels que $x^k = x^p$, et alors (on multiplie par x^{-k}), $x^{p-k} = 1$ avec $p - k \in \mathbb{N}^*$, donc x est d'ordre fini.

3. Soit G fini de cardinal n, et $x \in G$.
Comme $Gr(x) \subset G$, $Gr(x)$ est fini de cardinal $p = ordre(x)$.
Par le théorème de Lagrange, p divise n.

Si G est commutatif, on peut donner une preuve sans Lagrange:
On suppose G commutatif. Soit $p = \prod_{g \in G} g$.
p a un sens, car G est commutatif, et l'ordre du produit n'a pas d'importance.
Soit $x \in G$. On a $x^n p = \prod_{g \in G} (gx) = p$ car $h_x \begin{cases} G \to G \\ g \mapsto gx \end{cases}$ est bijective (d'inverse $h_{x^{-1}}$)
$x^n p = p$, donc en multipliant par p^{-1}, $x^n = 1$. ♣

1.4 Sous-groupes finis de $\mathbb{C}^*$

Dans cette partie, on se place dans $\mathbb{C}^*$.
On note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité. C'est facilement un sous-groupe de $\mathbb{C}^*$.
On a:

Propriété 3: Les sous-groupes finis de $\mathbb{C}^*$ sont les $\mathbb{U}_n$.
Démonstration
On sait que les $\mathbb{U}_n$ sont des sous-groupes finis de $\mathbb{C}^*$.
Inversement, soit G un sous-groupe fini de $\mathbb{C}^*$, de cardinal n.
Par la propriété 2, si $x \in G$, $x^n = 1$, donc $G \subset \mathbb{U}_n$. Comme $\text{card}(G) = n = \text{card}(\mathbb{U}_n)$, $G = \mathbb{U}_n$. ♣.

Définition 1: $n \in \mathbb{N}^*$. On appelle racine primitive n-ième de l'unité tout $x \in \mathbb{C}^*$ dont l'ordre est n.
Les racines primitives n-ièmes de l'unité sont les $\exp(2ik\pi/n)$ avec $k \wedge n = 1$ (cf exercice 1)
Notons G_n l'ensemble des racines primitives n-ièmes de l'unité.
Par la propriété 2, tout élément de $\mathbb{U}_n$ a un ordre d divisant n, donc $\mathbb{U}_n = \bigcup_{d|n} G_d$, union disjointe.

1.5 Sous-groupes de $\mathbb{R}$

Il s'agit d'un résultat qui a plutôt une nature analytique.

Propriété 4: Soit G un sous-groupe de $(\mathbb{R}, +)$. Alors soit il existe $d \in \mathbb{R}$ tel que $G = d\mathbb{Z}$, soit G est dense dans $\mathbb{R}$.

Démonstration:
Si $G = \{0\}$, $d = 0$ convient. Supposons donc $G \neq \{0\}$.
Comme $x \in G \Longrightarrow -x \in G$, $G \cap \mathbb{R}_+^* \neq \emptyset$.
On peut donc considérer $d = \inf(G \cap \mathbb{R}_+^*)$.
Nous allons montrer que, si $d = 0$, G est dense dans $\mathbb{R}$, et que si $d > 0$, $G = d\mathbb{Z}$.

Si $d = 0$: d est un inf, pas un min car $0 \notin G \cap \mathbb{R}_+^*$.
Soient $a, b \in \mathbb{R}$, $a < b$. Soit $\varepsilon = \dfrac{b-a}{2} > 0$.
Il existe $g \in G \cap \mathbb{R}_+^*$ tel que $g \leq \varepsilon$. On se fixe un tel g.
Alors G contient les itérés de g, ie contient $g\mathbb{Z}$.
$g\mathbb{Z}$ "recouvre $\mathbb{R}$ avec un pas inférieur à ε", donc rencontre $[a, b]$, et $G \cap [a, b] \neq \emptyset$. (mise en forme laissée au lecteur)
Ainsi G est dense dans $\mathbb{R}$.

Si $d > 0$: Montrons d'abord que d est un minimum.

Supposons que ce ne soit pas le cas: il existe alors $y \in]d, 2d[\cap G$, puis $x \in]d, y[\cap G$. Alors $y - x \in G$, et $y - x \in]0, d[$ ce qui contredit la définition de d.
Ainsi d est un minimum, et $d \in G$. Donc $d\mathbb{Z} \subset G$.
Réciproquement, si $x \in G$, soit $k = E(x/d)$. On a $x = kd + r$ avec $r \in [0, d[$. De plus $r = x - kd \in G$. Du fait de la définition de d, $r = 0$, et $x = kd \in d\mathbb{Z}$.
♣

1.6 Sous-groupes de $\mathbb{Z}$ et application à l'arithmétique

1.6.1 Description des sous-groupes de $\mathbb{Z}$

$\mathbb{Z}$ est un groupe commutatif pour l'addition (c'est aussi un anneau).
Si $a \in \mathbb{Z}$, on pose $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$. C'est facilement un sous-groupe de $\mathbb{Z}$.
Si $A_1, ..., A_n$ sont des parties de $\mathbb{Z}$, on pose $A_1 + ... + A_n = \{a_1 + ... + a_n \mid a_1 \in A_1, ..., a_n \in A_n\}$.
Ainsi $a_1\mathbb{Z} + ... + a_n\mathbb{Z} = \{a_1k_1 + ... + a_nk_n \mid k_1, ..., k_n \in \mathbb{Z}\}$. C'est facilement un sous-groupe de $\mathbb{Z}$.

Propriété 5: Sous-groupes de $\mathbb{Z}$
Les sous-groupes de $\mathbb{Z}$ sont les $a\mathbb{Z}$, $a \in \mathbb{Z}$.
De plus, si G est un sous-groupe de $\mathbb{Z}$ différent de $\{0\}$, il existe un unique $a > 0$ tel que $G = a\mathbb{Z}$.

Démonstration:
On a déjà dit que $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Soit donc G un sous-groupe de $\mathbb{Z}$.
Si $G = \{0\}$, $G = 0\mathbb{Z}$.
Si $G \neq \{0\}$:
Soit $a \in G \backslash \{0\}$. $-a \in G$. Donc $G \cap \mathbb{N}^* \neq \emptyset$ car a ou $-a$ est > 0.
Soit $b = \min(G \cap \mathbb{N}^*)$ (partie de $\mathbb{N}$ non vide).
$b \in G$, et G est un groupe, donc les itérés de b sont dans G ie $b\mathbb{Z} \subset G$.
Inversement, soit $x \in G$. On écrit la division euclidienne de x par b. $x = bq + r$, $r \in [\![0, b-1]\!]$.
Alors $r = x - \underbrace{bq}_{\in G} \in G$. Mais $0 \leq r < b$, donc $r = 0$ du fait de la définition de b.
Ainsi $x \in b\mathbb{Z}$ et on a $G \subset b\mathbb{Z}$, et finalement $G = b\mathbb{Z}$.

Dernier point : Soit $G = a\mathbb{Z} \neq \{0\}$ un sous-groupe de $\mathbb{Z}$. On a aussi $G = (-a)\mathbb{Z}$, donc on peut prend prendre $a > 0$.
Alors $G = \{..., -2a, -a, 0, a, 2a, ...\}$ donc $a = \min(G \cap \mathbb{N}^*)$, et est donc entièrement déterminé par G. ♣

1.6.2 Application à l'arithmétique

Le programme actuel de Sup proscrit l'usage des sous-groupes de $\mathbb{Z}$ en arithmétique, et prescrit une méthode plus pédestre, donc vous avez dû procéder autrement que ce qui suit en cours d'arithmétique.

Le point essentiel est le suivant: Soient $a_1, ..., a_n \in \mathbb{Z}$ non tous nuls. $a_1\mathbb{Z} + ... + a_n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc il existe un unique $\delta > 0$ tel que $a_1\mathbb{Z} + ... + a_n\mathbb{Z} = \delta\mathbb{Z}$.

Ceci permet d'établir facilement les propriétés fondamentales du PGCD.

Propriété 6: PGCD et relation de Bezout

Soient $a_1, ..., a_n \in \mathbb{Z}$ non tous nuls. Soit δ l'unique entier > 0 tel que $a_1\mathbb{Z} + ... + a_n\mathbb{Z} = \delta\mathbb{Z}$. Alors:

1. Il existe $b_1, ..., b_n \in \mathbb{Z}$ tels que $\delta = b_1a_1 + ... + b_na_n$ (relation de Bezout. Il n'y a pas unicité)
2. δ est un diviseur commun des a_i.
3. Si β est un diviseur commun des a_i, alors $\beta | \delta$. Ceci implique $|\beta| \leq \delta$, et donc δ est le plus grand diviseur commun des a_i.

On écrit $\delta = a_1 \wedge a_2 \wedge ... \wedge a_n$, ou $\delta = pgcd(a_1, ..., a_n)$.

Démonstration

1. $\delta = \delta \times 1 \in \delta\mathbb{Z} = a_1\mathbb{Z} + ... + a_n\mathbb{Z}$, d'où le résultat.
2. $\forall i,\ a_i = 0 \times a_1 + ... + 1 \times a_i + ... + 0 \times a_n$, donc $a_i \in a_1\mathbb{Z} + ... + a_n\mathbb{Z} = \delta\mathbb{Z}$, donc δ divise a_i.
3. Soit β un diviseur commun des a_i.
   On se donne une relation de Bezout $\delta = b_1a_1 + ... + b_na_n$.
   β divise les a_i, donc les b_ia_i, donc $\delta = \sum_i b_ia_i$. ♣

Note:
Il y a de l'"arithmétique" dans des anneaux autres que $\mathbb{Z}$. Par exemple, vous en avez parlé dans $K[X]$.
La notion qui intervient, que nous verrons, est celle d'idéal.
Il se trouve que dans $\mathbb{Z}$, il y a coïncidence entre idéaux et sous-groupes.

2 Exercices

Exercice 1:
On se place dans le groupe $(\mathbb{C}^*, .)$.
Soient $k \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$. Montrer que $z := e^{\frac{2ik\pi}{n}}$ est d'ordre $\frac{n}{n \wedge k}$.

Exercice 2:
Soit $(G, .)$ un groupe fini de cardinal p premier. Si $x \in G\backslash\{1\}$, que vaut $Gr(x)$?

Exercice 3:
Soit $(G, .)$ un groupe commutatif, $a, b \in \mathbb{N}^*$ tels que $a \wedge b = 1$, $x \in G$ d'ordre a, et $y \in G$ d'ordre b.
Montrer que xy est d'ordre ab.
On suggère de montrer que $(xy)^n = 1 \iff ab|n$. Un sens de l'équivalence est facile.

Exercice 4: Ordre d'une permutation
Soit $\sigma \in S_n$. On décompose σ en produit (=composée) de cycles à supports disjoints: $\sigma = c_1...c_k$.
l_i est la longueur du cycle c_i.
Montrer que c_i est d'ordre l_i, et σ d'ordre $ppcm(l_1, ..., l_k)$.

Exercice 5: Classes de similitude de S_n, morphismes de S_4
Si $\sigma \in S_n$, notons $C(\sigma) = \{\tau \in S_n \mid \tau\sigma = \sigma\tau\}$.

1. Soit $\sigma = (a_1...a_k) \in S_n$ un cycle, et $\tau \in S_n$. Vérifier que $\tau\sigma\tau^{-1} = (\tau(a_1)...\tau(a_k))$, et généraliser au cas où σ est produit de cycles à supports disjoints.

   suite de l'exercice optionnelle
   Dans la suite, on est dans S_4.

2. Si $\sigma = (ab) \in S_4$ est une transposition, donner le cardinal de $C(\sigma)$.
   Faire de même si σ est produit de deux transpositions à supports disjoints.
   On doit trouver des résultats différents.

   Soit $\phi : S_4 \to S_4$ bijective telle que $\forall \sigma, \tau \in S_4$, $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$ (ie un automorphisme de groupe)

3. Montrer que $\phi(id) = id$, $\phi(\sigma^{-1}) = (\phi(\sigma))^{-1}$, $\phi(C(\sigma)) = C(\phi(\sigma))$.
4. Montrer que $ordre(\phi(\sigma)) = ordre(\sigma)$.
5. Si σ est une transposition, montrer que $\phi(\sigma)$ est également une transposition.

6. On a donc $\phi((12)) = (a_1a_2)$, et $\phi((13)) = (b_1b_2)$.
   Montrer que $\{a_1, a_2\} \cap \{b_1, b_2\} \neq \emptyset$.
   Disons $a_1 = b_1$. Notons $\phi((12)) = (a_1a_2)$, et $\phi((13)) = (a_1a_3)$.
   Montrer que $\phi((14))$ s'écrit (a_1a_4).

7. Montrer qu'il existe $\tau \in S_4$ tel que $\forall \sigma \in S_4$, $\phi(\sigma) = \tau\sigma\tau^{-1}$.
   Remarque: reste vrai pour S_n en général, sauf pour $n = 5$.

Exercice 6:

1. Soient $q_1, ..., q_n \in \mathbb{Q}$ et $G = \{m_1q_1 + ... + m_nq_n \mid m_1, ..., m_n \in \mathbb{Z}\}$.
   Vérifier que G est un sous-groupe de $\mathbb{Q}$. (c'est ce qu'on appelle le sous-groupe engendré par $\{q_1, ..., q_n\}$. C'est le plus petit sous-groupe de $\mathbb{Q}$, au sens de l'inclusion, contenant $\{q_1, ..., q_n\}$)

   Montrer qu'il existe $x \in \mathbb{Q}$ tel que $G = Gr(x) = \{mx \mid m \in \mathbb{Z}\}$. (On dit que G est monogène car engendré par un seul élément)

2. Trouver un sous-groupe G non trivial de $\mathbb{Q}$ ie différent de $\mathbb{Q}$ et $\{0\}$ tel qu'il n'existe pas $x \in \mathbb{Q}$ vérifiant $G = Gr(x)$.

Exercice 7:
Soit G un groupe n'ayant qu'un nombre fini de sous-groupes.
On veut montrer que G est fini.

1. Soit $x \in G$. Supposons que x n'est pas d'ordre fini.
   Montrer que les $Gr(x^n)$, $n \in \mathbb{N}$ sont distincts deux à deux. Conclusion?

2. En notant que $G = \bigcup_{x \in G} Gr(x)$ (justifier), montrer que G est fini.

Exercice 8:

1. Soit G un groupe fini de cardinal pair.
   En associant x à x^{-1}, si $x \in G$, montrer que G possède un élément d'ordre 2.

2. Soit G un groupe fini de cardinal impair $2q + 1$.
   Montrer que $\forall x \in G$, $\exists! y \in G$; $x = y^2$.
   On utilisera la notion d'ordre et la propriété 2.

Exercice 9: On admet que π est irrationnel. Montrer que $\mathbb{Z} + 2\pi\mathbb{Z} = \{a + 2\pi b \mid a, b \in \mathbb{Z}\}$ est un sous groupe dense de $\mathbb{R}$, et que $\{\cos(n) \mid n \in \mathbb{Z}\}$ est dense dans $[0, 1]$.

Exercice 10:
optionnel
Soit p un nombre premier, et $G = \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$.
Vérifier que G est un sous-groupe de $\mathbb{C}^*$, et montrer que tout sous-groupe fini de G est un $\mathbb{U}_{p^n}$, $n \in \mathbb{N}$.

Exercice 11:
optionnel
Soit G un groupe fini non commutatif. On note $Z = \{x \in G \mid \forall y \in G,\ xy = yx\}$ le centre de G, $C = \{(x, y) \in G^2 \mid xy = yx\}$, et, si $x \in G$, $C_x = \{y \in G \mid xy = yx\}$.

1. Vérifier que Z et C_x, $x \in G$, sont des sous-groupes de G.

2. On suppose que $p = \text{card}(G)/\text{card}(Z)$ est un nombre premier.
   Soient $x \in G \backslash Z$, et $H = \{x^n h \mid n \in \mathbb{Z},\ h \in Z\}$.
   Montrer que H est un sous-groupe de G, contenant strictement Z, puis que $H = G$.
   Trouver une contradiction.

3. Justifier que $\text{card}(G)/\text{card}(Z) \geq 4$

4. Montrer que $\text{card}(C) = \sum_{x \in G} \text{card}(C_x) \leq \text{card}(G)\text{card}(Z) + (\text{card}(G) - \text{card}(Z))\frac{\text{card}(G)}{4}$ puis que $\text{card}(C) \leq \frac{5}{8}\text{card}(G)^2$.

Exercice 12:
optionnel
Soit G un groupe fini additif (donc commutatif) et A, B deux parties de G.

1. Montrer que si $\text{card}(A) + \text{card}(B) > \text{card}(G)$, alors $A + B = G$. $(A + B = \{x + y \mid (x, y) \in A \times B\})$
   On montrera que, si $x \in G$, $\{x - a \mid a \in A\} \cap B \neq \emptyset$.

2. Soit $H = \{x \in G \ ; \ A = x + A\}$. Montrer que H est un sous-groupe de G. $(x + A = \{x + y \mid y \in A\})$

3. Montrer que $\text{card}(A + B) = \text{card}(A)$ si et seulement si il existe $b \in G$ tel que $B \subset b + H$.

Partout, K est un corps commutatif, pas nécessairement sous-corps de $\mathbb{C}$. $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$, typiquement $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

1 Rappels

1.1 construction

Vous avez pu construire $K[X]$ en passant par les fonctions associées, pour $K = \mathbb{R}$ ou $\mathbb{C}$.

La manière théorique de construire les polynômes sur K, sans passer par les fonctions associées est de passer par les suites presque nulles :
$(a_n) \in K^{\mathbb{N}}$ est dite presque nulle si et seulement si $\exists N; \forall n \geq N,\ a_n = 0$.
Un polynôme est alors une suite presque nulle.
On donne un nom particulier au polynôme, $(0, 1, 0, 0, ...)$, souvent X, auquel cas on note $K[X]$ l'ensemble des polynômes.
On définit ensuite les opérations, si $A = (a_n), B = (b_n) \in K[X]$:

1. $A + B = (a_n + b_n)$.
2. $AB = (c_n)$ avec $\forall n \in \mathbb{N},\ c_n = \sum_{i+j=n} a_i b_j = \sum_{k=0}^{n} a_k b_{n-k}$.
3. Si $\lambda \in K$, $\lambda A = (\lambda a_n)$.

On vérifie aisément que ces opérations donnent des polynômes, et donnent à $K[X]$ une structure d'anneau commutatif, et de K-ev.
Le neutre additif est $0 = (0)_{n\in\mathbb{N}}$.
Le neutre multiplicatif est $(1, 0, 0, ...)$.
Un polynôme du type $(\lambda, 0, 0, ...)$ est assimilé au scalaire λ.
Un calcul facile donne, si $n, p \in \mathbb{N}$, $X^n = (\underbrace{0, ..., 0}_{n\ termes}, 1, 0, 0, ...)$, $X^n X^p = X^{n+p}$.
Ainsi, si $P = (a_n) \in K[X]$, et se donnant N tel que $\forall n \geq N + 1$, $a_n = 0$, $P = (a_0, ..., a_N, 0, ...) = a_0(1, 0, ...) + ... + a_N(0, 0, ..., 1, 0, ...) = a_0 X^0 + a_1 X + ... + a_N X^N$.
X^0 est noté 1, et omis en général.

On note parfois $P = \sum_{k=0}^{+\infty} a_n X^n$, la somme étant faussement infinie.

On définit ensuite le degré. Si $P = \sum_{k=0}^{+\infty} a_n X^n \neq 0$, $deg(P) = \max\{n;\ a_n \neq 0\}$, et on convient que $deg(0) = -\infty$.

On vérifie aisément $deg(AB) = deg(A) + deg(B)$, ce qui donne au passage l'intégrité de $K[X]$.

Du fait de l'intégrité, $\begin{cases} AB = AC \\ A \neq 0 \end{cases} \Longrightarrow B = C$.

Un polynôme est un objet algébrique, pas une fonction. Sur certains corps finis (nous verrons $\mathbb{Z}/p\mathbb{Z}$, p premier), deux polynômes distincts peuvent avoir la même fonction associée.

En rechanche, si K est infini, il n'y a pas ce problème, car (cf infra) un polynôme ayant une infinité de racines est le polynôme nul.

1.2 Division euclidienne

Propriété 1:
Soient $A, B \in K[X]$, $B \neq 0$. Alors $\exists!(Q, R) \in K[X]^2$ tel que:

1. $A = BQ + R$
2. $deg(R) < deg(B)$

On ne rappelle pas la démonstration, mais, si $B = b_n X^n + ... + b_0$, vous noterez en la reprenant que la seule division qui apparaît est par b_n. Le reste est produits et sommes.

Ainsi, si $A, B \in \mathbb{Z}[X]$, en général, $Q, R \in \mathbb{Q}[X]$ ($\mathbb{Q}$ est le premier corps contenant l'anneau $\mathbb{Z}$), mais, si B est

unitaire (ie $b_n = 1$), $Q, R \in \mathbb{Z}[X]$. C'est un résultat utile.

De la division euclidienne de A par $X-a$ résulte que si a est racine de A, il existe $B \in K[X]$ tel que $A = (X-a)B$, et par itération, que si $a_1, ..., a_n$ sont des racines distinctes deux à deux de A, A est divisible par $(X-a_1)...(X-a_n)$, puis pour raison de degré, que si $deg(A) = n \neq -\infty$, A a au plus n racines.

1.3 Polynômes irréductibles

Définition 1:
Si $A \in K[X]$ et $deg(A) \geq 1$, A est dit irréductible si et seulement si $\forall B, C \in K[X]$, $A = BC \Longrightarrow deg(B) = 0$ *ou* $deg(C) = 0$, ie que les seules factorisations de A sont triviales, ie par un scalaire.

Un polynôme de degré 1 est toujours irréductible.
Dans l'arithmétique des polynômes, les polynômes irréductibles sont le pendant des nombres premiers dans l'arithmétique des entiers.

Dans $\mathbb{Z}$, on convient que les nombres premiers sont > 0 pour avoir unicité d'une décomposition.
Dans $K[X]$, pour avoir l'unicité, on imposera le caractère unitaire.

Vous avez vu que dans $\mathbb{C}[X]$, les irréductibles sont les polynômes de degré 1, à cause du théorème de d'Alembert-Gauss.
Dans $\mathbb{R}[X]$, il y a ceux de degré 1, et les $aX^2 + bX + c$ avec $a \neq 0$, et $b^2 - 4ac < 0$.

1.4 Interpolation

On ne rappellera pas ici l'énoncé, mais ne pas oublier un résultat très important: le théorème d'interpolation de Lagrange.

2 Arithmétique des polynômes

2.1 Idéaux de K[X], PGCD

On a vu la notion de PGCD d'entiers via les sous-groupes de $\mathbb{Z}$.
Dans $K[X]$ (et dans dans d'autres anneaux en général), c'est la notion d'idéal qui intervient.

Définition 2: Un idéal de $K[X]$ est une partie I de $K[X]$ telle que

1. I est un sous-groupe de $(K[X], +)$
2. Si $A \in I$ et $B \in K[X]$, $AB \in I$.

Si $A \in K[X]$, on pose $AK[X] = \{AB \mid B \in K[X]\}$, et plus généralement, si $A_1, ..., A_n \in K[X]$, $A_1K[X] + ... + A_nK[X] = \{A_1B_1 + ... + A_nB_n \mid B_1, ..., B_n \in K[X]\}$.
On vérifie immédiatement que ce sont des idéaux de $K[X]$.

Propriété 2: Description des idéaux de $K[X]$
Les idéaux de $K[X]$ sont les $AK[X]$, $A \in K[X]$.
De plus, si I est un idéal $\neq \{0\}$, il existe un unique $A \in K[X]$ unitaire tel que $I = AK[X]$.

Démonstration:
On a déjà dit que les $AK[X]$ sont des idéaux.
Soit I un idéal de $K[X]$.
Si $I = \{0\}$, $I = 0K[X]$.
Si $I \neq \{0\}$:
$D = \{deg(A) \mid A \in I \backslash \{0\}\}$ est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément d.
On se donne $A \in I$ tel que $deg(A) = d$.
$\forall B \in K[X]$, $AB \in I$ car I idéal, donc $AK[X] \subset I$.
Inversement, Soit $C \in I$. On fait la division euclidienne de C par A, $C = AQ + R$.
$R = C - AQ \in I$, car I est un groupe, et $C, AQ \in I$. Mais $deg(R) < d$, donc $R = 0$, et $C \in AK[X]$.
Finalement, $I = AK[X]$.

Si $\lambda \in K^*$, $\lambda AB = A(\lambda B)$, $AB = (\lambda A)(\lambda^{-1})B$, donc $(\lambda A)K[X] = AK[X]$.
Ainsi, en divisant A par son coefficient dominant, on peut prendre A unitaire tel que $I = AK[X]$.

Enfin, si $I = AK[X] = BK[X]$ avec A, B unitaires: $A = A \times 1 \in AK[X] = BK[X]$, donc B divise A. De même A divise B. Donc, pour des raisons de degré, $A = \lambda B$, $\lambda \in K$. Mais comme A et B sont unitaires, $\lambda = 1$ et $A = B$. ♣

On peut alors fonder la notion de PGCD comme dans $\mathbb{Z}$:
Propriété 3: PGCD et relation de Bezout

Soient $A_1, ..., A_n \in K[X]$ non tous nuls.
Soit Δ l'unique polynôme unitaire tel que $A_1K[X] + ... + A_nK[X] = \Delta K[X]$. Alors:

1. Il existe $B_1, ..., B_n \in K[X]$ tels que $\Delta = B_1A_1 + ... + B_nA_n$ (relation de Bezout. Il n'y a pas unicité)
2. Δ est un diviseur commun des A_i.
3. Si β est un diviseur commun des A_i, alors $\beta|\Delta$. Ceci implique $deg(\beta) \leq \deg(\Delta)$, et donc Δ est le plus grand diviseur commun des A_i unitaire au sens du degré.

On écrit $\Delta = A_1 \wedge A_2 \wedge ... \wedge A_n$, ou $\Delta = pgcd(A_1, ..., A_n)$.

Démonstration

1. $\Delta = \Delta \times 1 \in \Delta K[X] = A_1K[X] + ... + A_nK[X]$, d'où le résultat.
2. $\forall i,\ A_i = 0 \times A_1 + ... + 1 \times A_i + ... + 0 \times A_n$, donc $A_i \in A_1K[X] + ... + A_nK[X] = \Delta K[X]$, donc Δ divise A_i.
3. Soit β un diviseur commun des A_i.
   On se donne une relation de Bezout $\Delta = B_1A_1 + ... + B_nA_n$.
   β divise les A_i, donc les B_iA_i, donc $\Delta = \sum_i B_iA_i$. ♣

On parle parfois d'un PGCD, si on n'adopte pas la normalisation unitaire.

Il en résulte le lemme de Gauss (même démonstration de dans $\mathbb{Z}$):
Propriété 4:
Si $A, B, C \in K[X]$, $A|BC$, et $A \wedge B = 1$, alors $A|C$.
Démonstration
On fait les hypothèses de l'énoncé. On écrit une relation de Bezout $1 = UA + VB$, et on multiplie par C, d'où $C = AUC + \underbrace{VBC}_{A|BC}$, et donc $A|C$.

2.2 Théorème de décomposition

Propriété 5: Soit $A \in K[X]$ de degré ≥ 1. Alors A se décompose de manière unique (à l'ordre des termes près) $A = \lambda A_1...A_k$, où $\lambda \in K^*$, et les A_i sont irréductibles unitaires.

Démonstration:
Existence
On procède par récurrence sur le degré. H_n: "Si $deg(P) = n$, alors P admet une décomposition"
$n = 1$: Si $P = aX + b$, $a \neq 0$, $P = a(X + b/a)$, et $X + b/a$ est irréductible car de degré 1.
Supposons $H_1, ..., H_n$ vraies. Soit P de degré $n + 1$.
Si P est irréductible, on factorise son coefficient dominant, et la décomposition est faite.
Sinon, il existe A, B de degrés ≥ 1 tels que $P = AB$. On se fixe de tels A, B.
Par $H_{deg(A)}$ et $H_{deg(B)}$, A et B se décomposent, et en faisant le produit de leurs décompositions, on obtient une décomposition de P

Unicité

Soit A de dégré ≥ 1 admettant deux décompositions $A = \lambda A_1...A_k = \beta B_1...B_q$.
Déjà, $\lambda = \beta = dom(A)$, donc $A_1...A_k = B_1...B_q$.
A_1 divise $B_1...B_q$.
Si $A_1 = B_1$, on simplifie par intégrité, $A_2...A_k = B_2...B_q$.
Sinon $A_1 \neq B_1$ et alors $A_1 \wedge B_1 = 1$. En effet, soit $\Delta = A_1 \wedge B_1$. Δ divise A_1, A_1 et Δ sont unitaires, et A_1 est irréductible, donc $\Delta = A_1$ ou $\Delta = 1$.
Si $\Delta = A_1$, A_1 divise B_1, $deg(A_1) \geq 1$, B_1 est irréductible, et A_1, B_1 sont unitaires, donc $A_1 = B_1$ ce qui n'est pas.
Ainsi, par le lemme de Gauss, A_1 divise $B_2...B_q$.
On recommence avec $B_2...B_q$

Finalement, on obtient nécessairement qu'il existe i tel que $A_1 = B_i$, sinon on finirait par "A_1 divise 1".
Quitte a renuméroter, disons $A_1 = B_1$, et donc dans tous les cas, on aboutit à $A_2...A_k = B_2...B_q$.
Ensuite, on recommence avec A_2. On peut rédiger une récurrence sur $deg(A)$, évidemment. ♣

A noter : Si $K' \subset K$, les irréductibles de $K[X]$ le sont dans $K'[X]$. $K'[X]$ a plus d'irréductibles que $K[X]$
Alors, si $P \in K'[X]$, sa décomposition dans $K[X]$ a plus de termes que celle dans $K'[X]$. Pensez à la décomposition d'un polynôme réel dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

2.3 Notion de polynôme minimal

Si $x \in K$, notons $Ann(x) = \{P \in K[X] \mid P(x) = 0\}$.
$Ann(x)$ est facilement un idéal de $K[X]$.
Si $Ann(x) \neq \{0\}$, il existe alors un unique polynôme unitaire P tel que $Ann(x) = PK[X]$.
Ce polynôme P est appelé polynôme minimal de x. Nous le noterons μ_x, ou éventuellement $\mu_{K,x}$ s'il y a plusieurs corps à considérer.
Les polynômes ayant x comme racine sont donc les multiples de μ_x.

Un exemple très simple: $\mu_{\mathbb{R},\sqrt{2}} = X - \sqrt{2}$, $\mu_{\mathbb{Q},\sqrt{2}} = X^2 - 2$.

Dans l'année, nous parlerons d'application de polynômes à des matrices et endomorphismes, et verrons la notion de polynôme minimal de matrices et d'endomorphismes.

3 Exercices

Exercice 1:
Justifier que $X^3 - 3$ est irréductible dans $\mathbb{Q}[X]$. (Si on invoque l'irrationalité d'un réel, il faut la montrer)
$\mu_{\mathbb{Q},3^{1/3}} = ?$.

Exercice 2: Théorème de Gauss-Lucas.
$n \in \mathbb{N}^*$. Soit $P = \lambda \prod_{i=1}^{n} (X - a_i)^{d_i} \in \mathbb{C}[X]$ avec $\lambda \in \mathbb{C}^*$, $d_i \in \mathbb{N}^*$, les a_i étant distincts deux à deux.

1. Vérifier que $\dfrac{P'}{P} = \sum_i \dfrac{d_i}{X - a_i}$ (pas de ln!).
2. Soit x une racine de P' qui n'est pas l'un des a_i.
   En partant de $\dfrac{P'(x)}{P(x)} = 0$, et en conjuguant, montrer qu'il existe $\beta_1, ..., \beta_n \in \mathbb{R}^+$ tels que $\sum_{i=1}^{n} \beta_i = 1$ et $x = \sum_{i=1}^{n} \beta_i a_i$.
   Quelle est l'interprétation géométrique?
3. Ici, $P = (X - i)(X - i - 1)(X + 5)(X - 3 - 2i)$. Dessiner dans le plan complexe une zone qui contient toutes les racines de P'.

Exercice 3: Soit $P \in \mathbb{R}[X]$ de degré ≥ 1, scindé dans $\mathbb{R}[X]$.
$P = \lambda \prod_{i=1}^{n} (X - a_i)^{d_i} \in \mathbb{C}[X]$ avec $\lambda \in \mathbb{R}^*$, les a_i étant réels distincts deux à deux.
Montrer que P' est scindé dans $\mathbb{R}[X]$, sans utiliser l'exercice précédent, qui donnerait le résultat. (on pensera aux ordres entre-autre).

Exercice 4: Soit $P \in \mathbb{C}[X]$ tel que $P(\mathbb{Q}) \subset \mathbb{Q}$. Montrer que $P \in \mathbb{Q}[X]$.

Exercice 5: On se demande quels sont les polynômes $P \in \mathbb{C}[X]$ tels que $|z| = 1 \Longrightarrow |P(z)| = 1$.

1. Soient $F, G \in \mathbb{C}(X)$ deux fractions rationnelles telles que $\{z \in \mathbb{C} \mid F(z) = G(z)\}$ soit infini. Montrer que $F = G$.

   Si $P = \sum_k a_k X^k$, on note $\overline{P} = \sum_k \overline{a_k} X^k$.
   Soit $P \in \mathbb{C}[X]$ tel que $|z| = 1 \Longrightarrow |P(z)| = 1$.
2. Montrer que $P(X)\overline{P}\left(\dfrac{1}{X}\right) = 1$.

3. En déduire que la seule racine possible de P est 0, et la forme de P.

Exercice 6:

1. [Polynômes de Chebychev]
   Montrer que pour tout $n \in \mathbb{N}$ il existe un unique polynôme $T_n \in \mathbb{R}[X]$ tel que

   $$\forall \theta \in \mathbb{R},\ T_n(\cos(\theta)) = \cos(n\theta)$$

   ind : pour montrer l'existence d'une suite (T_n) convenable, on vérifiera que
   $\cos((n+1)x) = 2(\cos(nx))\cos(x) - \cos((n-1)x)$, et on définira (T_n) par récurrence. L'unicité se traite à part.

   Montrer que $\deg(T_n) = n$, et que si $n \in \mathbb{N}^*$, le coefficient dominant de T_n est 2^{n-1}.

2. Soit $n \in \mathbb{N}^*$ et $P \in \mathbb{R}[X]$ de degré n unitaire.

   On veut montrer que $\sup_{x\in[-1,1]} |P(x)| \geq \frac{1}{2^{n-1}}$.

   (a) Montrer qu'existent $-1 \leq x_0 < x_1 < ... < x_n \leq 1$ tels que, si $k \in [\![0, n]\!]$, $T_n(x_k) = (-1)^{(n-k)}$.

   (b) Montrer le résultat voulu en considérant $2^{n-1}P - T_n$. (raisonner par l'absurde et montrer que $2^{n-1}P - T_n$ possède au moins n racines distinctes)

3. Soit $P \in \mathbb{R}[X]$ de degré $n \in \mathbb{N}^*$ unitaire, $a < b$ deux réels tels que $\forall x \in [a, b]$, $|P(x)| \leq 2$. Montrer que $b - a \leq 4$.
   On fera un changement de variable affine permettant de se ramener à $[-1, 1]$.

Exercice 7: Contenu d'un polynôme.
Si $P = a_nX^n + ... + a_1X + a_0 \in \mathbb{Z}[X]$, avec $a_n \neq 0$, on appelle contenu de P la quantité $cont(P) := pgcd(a_0, ..., a_n)$.

1. $A, B \in \mathbb{Z}[X]\backslash\{0\}$. On suppose qu'un nombre premier q divise tous les coefficients de AB.
   Montrer que q divise tous les coefficients de A, ou tous les coefficients de B.

2. Montrer, si $A, B \in \mathbb{Z}[X]\backslash\{0\}$, que $cont(AB) = cont(A)cont(B)$.

Exercice 8: Optionnel. Soient $a_1 < a_2 < ... < a_n$ avec $a_i \in \mathbb{Z}$, et $P = 1 + \prod_{i=1}^{n}(X - a_i)^2$.

Montrer que P est irréductible dans $\mathbb{Z}[X]$ ie si $P = AB$ avec $A, B \in \mathbb{Z}[X]$, alors A ou B est de degré 0.

Exercice 9: Optionnel. Démonstration du théorème de d'Alembert-Gauss
Soit $P = a_nX^n + ... + a_1X + a_0 \in \mathbb{C}[X]$ de degré $n \geq 1$.
La fonction associée, de $\mathbb{C}$ dans $\mathbb{C}$ est continue (même définition que dans le cas réel: $\forall a \in \mathbb{C},\ \forall \varepsilon > 0,\ \exists \delta > 0;\ \forall b \in \mathbb{C},\ |b - a| \leq \delta \Longrightarrow |P(a) - P(b)| \leq \varepsilon$). Il en est de même par composition de $z \mapsto |P(z)|$.

Soit $m = \inf\{|P(z)| \mid z \in \mathbb{C}\}$.

1. Montrer que $|P(z)| \underset{|z|\to+\infty}{\longrightarrow} +\infty$ et en déduire qu'il existe $r > 0$ tel que $m = \inf\{|P(z)| \mid z \in \mathbb{C}\ et\ |z| \leq r\}$.

2. Montrer que m est un minimum ie $\exists a \in \mathbb{C}$ tel que $|P(a)| = m$. (reprendre la démonstration du théorème vu en Sup pour une fonction continue sur un segment: utiliser le théorème de Bolzano-Weierstrass dans $\mathbb{C}$)
   On se fixe un tel a. Le but est de voir que $P(a) = 0$.

3. Justifier l'existence d'un DL en a du type $P(a + h) = P(a) + bh^k + h^k\varepsilon(h)$, avec $\varepsilon(h) \underset{h\to0}{\longrightarrow} 0$, $b \in \mathbb{C}^*$, $k \in \mathbb{N}^*$.

4. Si $P(a) \neq 0$, montrer qu'il existe h tel que $|P(a + h)| < |P(a)|$.
   Ind: faire en sorte que bh^k ait un argument décalé de π par rapport à celui de $P(a)$.

   Conclusion?

Exercice 10: Optionnel
On se demande quels sont les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{Z}) \subset (\mathbb{Z})$.
On pose $H_0 = 1$, et, si $k \in \mathbb{N}^*$, on pose $H_k = \frac{1}{k!}X(X - 1)...(X - (k - 1))$. (polynômes de Hilbert)

1. Justifier que $(H_0, ...H_n)$ est une base de $\mathbb{C}_n[X]$.

2. Montrer que, si $n \in \mathbb{Z}$, $H_k(n) \in \mathbb{Z}$. On distinguera $n < 0,\ n \in [\![0, k - 1]\!],\ n \geq k$.

3. Soit $P \in \mathbb{C}_n[X]$. Montrer que $P(\mathbb{Z}) \subset \mathbb{Z}$ si et seulement si il existe $a_0, ..., a_n \in \mathbb{Z}$ tels que $P = \sum_{k=0}^{n} a_k H_k$.

Exercice 11: **Optionnel**. Déterminer $\mu_{\mathbb{Q},(\sqrt{2}+\sqrt{3})}$ (quelque part, il faudra montrer que $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$)

Exercice 12: **Optionnel**. Soit $P \in \mathbb{C}[X]$ non constant tel que $P(X)P(X+1) = P(X^2)$.

1. On note que, si a est racine de P, a^2 et $(a-1)^2$ le sont aussi.
   A partir de là, avec des itérations et utilisant le fait que P n'a qu'un nombre fini de racines, montrer que seuls 1 et 0 peuvent être racines de P.
2. Montrer qu'il existe $n \in \mathbb{N}^*$ tels que $P = \pm(X-1)^n X^n$.

Partout, $K = \mathbb{R}$ ou $\mathbb{C}$.

1 Quelques rappels et compléments

1.1 Négations

Diverses propriétés des suites ont intérêt à être niées, pour des raisonnements par l'absurde par exemple, mais pas seulement.
On peut donner des négations entièrement quantifiées, mais il est souvent plus efficace d'utiliser des sous-suites.

Exemple 1: $(a_n) \in K^{\mathbb{N}}$. Comment exprimer la propriété "(a_n) est non bornée".
(a_n) bornée: "$\exists C \in \mathbb{R}^+ \ ; \ \forall n, \ |a_n| \leq C$".
(a_n) non bornée: "$\forall C \in \mathbb{R}^+ \ ; \ \exists n, \ |a_n| \geq C$". (ou $|a_n| > C$. Indifférent vu les quantifications).

Forme séquentielle: (a_n) non bornée si et seulement si il existe une sous-suite $(a_{\phi(n)})$ telle que $|a_{\phi(n)}| \underset{n\to+\infty}{\longrightarrow} +\infty$. (on parle de sous-suite, donc il est implicite que $\phi : \mathbb{N} \to \mathbb{N}$ est strictement croissante)
Démonstration du sens non trivial ($\Longrightarrow$)
On suppose (a_n) non bornée.
On pose $\phi(0) = 0$.
$\phi(0) < ... < \phi(n)$ ayant été définis, on définit $\phi(n+1)$ de la sorte:
$\exists k \in \mathbb{N}; |a_k| \geq 1 + \max\limits_{0\leq i\leq \phi(n)} |a_i|$. On se donne un tel k, et on pose $\phi(n+1) = k$.
Du fait de la définition, $\phi : \mathbb{N} \to \mathbb{N}$ est strictement croissante, et $\forall n \geq 1, \ |a_{\phi(n)}| \geq n \underset{n\to+\infty}{\longrightarrow} +\infty$. ♣

Autres négations, dont la vérification est laissée au lecteur:

1. (a_n) ne converge pas vers $b \in K$ si et seulement si il existe une sous-suite $(a_{\phi(n)})$, et une constante $\varepsilon > 0$ tels que $\forall n, \ |a_{\phi(n)} - b| \geq \varepsilon$.

2. $(|a_n|)$ ne diverge pas vers $+\infty$ si et seulement si il existe une sous-suite $(a_{\phi(n)})$ bornée (et si par exemple $a_n \in \mathbb{Z}$, on peut même extraire une sous-suite constante)

3. $(a_n) \in \mathbb{R}^n$ ne diverge pas vers $+\infty$ si et seulement si il existe une sous-suite $(a_{\phi(n)})$ majorée.

Vous pourrez créer des négations pour bien d'autres propriétés.

1.2 Sous-suites, valeurs d'adhérence

Vous avez vu le théorème de Bolzano-Weierstrass: De toute suite $(a_n) \in K^{\mathbb{N}}$ bornée, on peut extraire une sous-suite convergente.
Ce résultat apparaît par exemple dans la démonstration du théorème de compacité: Si $f \in \mathcal{C}([a,b],\mathbb{R})$, alors f est bornée et atteint ses bornes. (si f est à valeurs dans $\mathbb{C}$, le résultat s'applique à $|f|$)

Définition 1: Si $(a_n) \in K^{\mathbb{N}}$, $b \in K$ est dit valeur d'adhérence de (a_n) si et seulement si il existe une sous-suite $(a_{\phi(n)})$ convergeant vers b.
On notera $VA((a_n))$ l'ensemble des valeurs d'adhérences de (a_n).
Une suite convergente a donc une seule valeur d'adhérence, sa limite.

Propriété 1: Caractérisation "en ε" d'une valeur d'adhérence:
b est valeur d'adhérence de (a_n) si et seulement si $\forall \varepsilon > 0$, $\forall N \in \mathbb{N}$, $\exists n \geq N$; $|a_n - b| \leq \varepsilon$.

Démonstration
$\Longrightarrow$: Soit ϕ strictement croissante telle que $a_{\phi(n)} \to b$.
Si $\varepsilon > 0$ et $N > 0$, pour n assez grand, $m = \phi(n)$ vérifie $m \geq N$ et $|a_m - b| \leq \varepsilon$.
$\Longleftarrow$: On suppose $\forall \varepsilon > 0$, $\forall N \in \mathbb{N}$, $\exists n \geq N$; $|a_n - b| \leq \varepsilon$.
On construit $\phi(n)$ par récurrence.
Posons $\phi(0) = 0$.
$\phi(0) < ... < \phi(n)$ étant construits, on définit $\phi(n+1)$ de la sorte:
$\exists m \geq \phi(n) + 1$; $|a_m - b| \leq \dfrac{1}{n+1}$. On se donne un tel m, et on pose $\phi(n+1) = m$.
Ainsi ϕ est strictement croissante, et $\forall n > 0$, $|a_{\phi(n)} - b| \leq \dfrac{1}{n}$, donc $a_{\phi(n)} \to b$. ♣

Propriété 2: Extractions successives: Si (a_n), $(b_n) \in K^{\mathbb{N}}$ sont deux suites bornées, alors il existe $\phi : \mathbb{N} \to \mathbb{N}$ telle que $(a_{\phi(n)})$ et $(b_{\phi(n)})$ convergent.
Le résultat s'étend à un nombre fini de suites bornées en augmentant le nombre d'étapes de la démonstration.
Démonstration
Soient (a_n), $(b_n) \in K^{\mathbb{N}}$ deux suites bornées.
Par BW, on se donne $\phi_1 : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(a_{\phi_1(n)})$ converge.
$(b_{\phi_1(n)})$, sous-suite de (b_n), est bornée, donc par BW, on se donne $\phi_2 : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(b_{\phi_1(\phi_2(n))})$ converge.
Soit $\phi = \phi_1 \circ \phi_2$. ϕ est strictement croissante.
$(b_{\phi(n)})$ converge, et $(a_{\phi(n)})$ aussi, puisque c'est une sous-suite de $(a_{\phi_1(n)})$, qui converge. ♣
Notez bien: $\phi = \phi_1 \circ \phi_2$, et non $\phi = \phi_2 \circ \phi_1$.

Propriété 3: Caractérisation de la convergence avec les valeurs d'adhérence
Soit $(a_n) \in K^{\mathbb{N}}$ une suite bornée. (donc, par BW, (a_n) a au moins une valeur d'adhérence)
Alors (a_n) converge si et seulement si elle a une seule valeur d'adhérence.

Note: puisque, par BW, (a_n) a au moins une valeur d'adhérence, en pratique, seule l'unicité est à établir.

Démonstration:
Le sens $\Longrightarrow$ est trivial.
Pour $\Longleftarrow$: Soit (a_n) bornée ayant une seule valeur d'adhérence que l'on note b. Il s'agit de montrer que $a_n \to b$.
Par l'absurde, supposons $a_n \underset{n \to +\infty}{\not\longrightarrow} b$.
Alors il existe $\varepsilon > 0$, et une sous-suite $(a_{\phi(n)})$ tels que $\forall n$, $|a_{\phi(n)} - b| \geq \varepsilon$.
On se fixe de tels ε, ϕ.
$(a_{\phi(n)})$ est bornée, donc par BW, il existe une sous-suite $(a_{\phi(\psi(n))})$ convergeant vers un $c \in K$.
On se fixe une telle sous-suite.
$\forall n$, $|a_{\phi(\psi(n))} - b| \geq \varepsilon$, donc par passage à la limite, $|b - c| \geq \varepsilon$, donc $b \neq c$.
Mais $(a_{\phi(\psi(n))})$ est une sous-suite de (a_n), donc c est une valeur d'adhérence de (a_n).
Ceci contredit l'unicité d'une valeur d'adhérence. ♣

Propriété 4: L'ensemble des valeurs d'adhérence est fermé:
Soit $a = (a_n) \in K^{\mathbb{N}}$. On suppose que $\forall n \in \mathbb{N}$, $b_n \in VA(a)$, et $b_n \underset{n \to +\infty}{\longrightarrow} b \in K$.

Alors $b \in VA(a)$.

Démonstration
On fait les suppositions de l'énoncé.
Soit $\varepsilon > 0$.
On peut alors se donner p tel que $|b_p - b| \leq \varepsilon/2$.
Alors, comme $b_p \in VA(a)$, $\forall N \in \mathbb{N}$, $\exists n \geq N$; $|a_n - b_p| \leq \varepsilon/2$, ce qui implique $|a_n - b| \leq \varepsilon$.

Ainsi, on a établi : $\forall \varepsilon > 0$, $\forall N \in \mathbb{N}$, $\exists n \geq N$; $|a_n - b| \leq \varepsilon$, ce qui est la caractérisation "en ε" de $b \in VA(a)$. ♣

1.3 Limites supérieure et inférieure

Définition 2: Soit $(u_n) \in \mathbb{R}^n$ une suite .
Posons $s_n = \sup\{u_k \ | k \geq n\} \in \mathbb{R} \cup \{+\infty\}$.
(s_n) est décroissante, donc admet une limite $l \in \mathbb{R} \cup \{+\infty, -\infty\}$.
l est appelée limite supérieure de (u_n), et nous la noterons $\limsup_{n\to+\infty} u_n$.
Vous vérifierez que: $\limsup_{n\to+\infty} u_n = +\infty \Longleftrightarrow (u_n)$ non majorée, et $\limsup_{n\to+\infty} u_n = -\infty \Longleftrightarrow u_n \to -\infty$.
Similairement, on pose $m_n = \inf\{u_k \ | k \geq n\} \in \mathbb{R} \cup \{-\infty\}$.
(m_n) est croissante, donc admet une limite dans $\mathbb{R} \cup \{+\infty, -\infty\}$, notée $\liminf_{n\to+\infty} u_n$.
Vous vérifierez que: $\liminf_{n\to+\infty} u_n = -\infty \Longleftrightarrow (u_n)$ non minorée, et $\liminf_{n\to+\infty} u_n = +\infty \Longleftrightarrow u_n \to +\infty$.

L'intérêt de ces deux limites est qu'elles existent toujours, et leur usage peut considérablement simplifier certaines démonstrations. On a parmi d'autres les propriétés fondamentales:
Propriété 5:

1. $\limsup_{n\to+\infty} u_n \geq \liminf_{n\to+\infty} u_n$
2. Si $\forall n$ (APCR suffit évidemment) $u_n \leq w_n$, alors $\limsup_{n\to+\infty} u_n \leq \limsup_{n\to+\infty} w_n$. Idem pour limite inf.
3. $u_n \underset{n\to+\infty}{\longrightarrow} a \in \mathbb{R} \cup \{+\infty, -\infty\} \Longleftrightarrow \limsup_{n\to+\infty} u_n = \liminf_{n\to+\infty} u_n = a$.

Démonstration

1. Avec les notations de la définition, $s_n \geq m_n$ donc $\lim s_n \geq \lim m_n$.
2. On suppose $\forall n$, $u_n \leq w_n$. Alors $s_n = \sup\{u_k \ | k \geq n\} \leq s'_n = \sup\{w_k \ | k \geq n\}$, donc $\lim s_n \leq \lim s'_n$.
3. Le sens $\Longrightarrow$ est simple, car si $u_n \to a$, $s_n \to a$ et $m_n \to a$.
   Pour $\Longleftarrow$: On suppose $\limsup_{n\to+\infty} u_n = \liminf_{n\to+\infty} u_n = a$.
   Toujours en reprenant les notations de la définition : $m_n \leq u_n \leq s_n$. Or $m_n \to a$ et $s_n \to a$, donc par encadrement $u_n \to a$. ♣

1.4 Suites dans K^n, dans $\mathcal{M}_{n,p}(K)$

Nous parlerons dans l'année de suites et de convergence dans divers espaces.

Définition 3: Si $(a_n) = (a_n(1), ..., a_n(k))$ est une suite d'éléments de K^k, on dit que $a_n \underset{n\to+\infty}{\longrightarrow} b = (b_1, ..., b_k) \in K^k$ si et seulement si $\forall i,\ a_n(i) \underset{n\to+\infty}{\longrightarrow} b_i$.

On a facilement l'unicité de la limite, la compatibilité vis-a-vis de la somme et de la multiplication scalaire.
Si $K = \mathbb{R}$ et que l'on munit $\mathbb{R}^k$ de la norme euclidienne standard $||(b_1, ..., b_k)|| = \sqrt{b_1^2 + ... + b_k^2}$, vous vérifierez facilement que $a_n \underset{n\to+\infty}{\longrightarrow} b \iff ||a_n - b|| \underset{n\to+\infty}{\longrightarrow} 0$.

On étend naturellement la définition aux suites de matrices (une matrice $n \times p$ peut être vue comme un élément de $\mathbb{K}^{np}$):

Définition 4: Si $(A_n) = (a_{i,j}(n))_{\substack{1\le i\le p\\1\le j\le q}} \in \mathcal{M}_{p,q}(K)^{\mathbb{N}}$, on dit que $A_n \underset{n\to+\infty}{\longrightarrow} B = (b_{i,j})_{\substack{1\le i\le p\\1\le j\le q}} \in \mathcal{M}_{p,q}(K)$ si et seulement si $\forall i, j,\ a_{i,j}(n) \underset{n\to+\infty}{\longrightarrow} b_{i,j}$.

Là encore, on a facilement l'unicité de la limite, la compatibilité vis-a-vis de la somme de la multiplication scalaire, **et du produit matriciel**, en utilisant la formule des coefficients d'un produit, et les propriétés usuelles des suites scalaires.
On a aussi, si $A_n \to B$, en utilisant la formule de la trace, et la formule générale du déterminant, $\det(A_n) \to \det(B)$, $tr(A_n) \to tr(B)$.

La définition des valeurs d'adhérence dans ces espaces est inchangée.

Propriété 6: Généralisation du théorème de BW à $\mathbb{R}^p$:
[Idem pour $\mathcal{M}_{p,q}(\mathbb{R}) \sim K^{pq}$. On peut prendre $K = \mathbb{C}$, mais vous ne connaissez pas encore la notion de norme sur $\mathbb{C}^n$].
On note $||(a_1, ..., a_p)|| = \sqrt{a_1^2 + ... + a_p^2}$ la norme euclidienne standard de $\mathbb{R}^p$.

Une partie P de $\mathbb{R}^p$ est dite bornée si et seulement si il existe $C \in \mathbb{R}^+$ telle que $\forall a \in P$, $||a|| \le C$.
Une suite (a_n) de $(\mathbb{R}^p)^{\mathbb{N}}$ est dite bornée si et seulement si $\{a_n \mid n \in \mathbb{N}\}$ est bornée.
Si $a_n = (a_n(1), ..., a_n(p))$, ceci revient facilement à $\forall i,\ (a_n(i))_{n\in\mathbb{N}}$ est bornée.

Propriété 7: Si $(a_n) \in (\mathbb{R}^p)^{\mathbb{N}}$, est bornée, alors (a_n) admet une valeur d'adhérence ie admet une sous-suite convergente.

Démonstration
Il suffit d'appliquer la propriété précédente d'extractions successives aux suites $(a_n(i))_{n\in\mathbb{N}}$, $i = 1...p$.

En remplaçant $|\cdot|$ par $\|\cdot\|$, on démontre similairement au cas $\mathbb{R}$ ou $\mathbb{C}$:

Propriété 8: Si $(a_n) \in (\mathbb{R}^p)^{\mathbb{N}}$ est bornée, (a_n) converge si et seulement si (a_n) admet une unique valeur d'adhérence.

2 Exercices

1. Soit $(a_n) = \left(\frac{p_n}{q_n}\right)$ une suite de rationnels convergente, avec $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}^*$, et (q_n) bornée. Montrer que $\lim a_n \in \mathbb{Q}$. (La formalisation est simplifiée en utilisant des sous-suites. On pourra commencer par noter que (q_n) admet une sous-suite d'un type très simple)
2. Définir une suite $(a_n) \in [0,1]^{\mathbb{N}}$ telle que $VA((a_n)) = [0,1]$.

Formule inutile: un schéma / la donnée d'un nombre suffisant de premiers termes expliquant le procédé de construction suffit.

3. Soit $(a_n), (b_n), (c_n) \in \mathbb{C}^n$ telles que $\forall n,\ a_{n+1} = b_n a_n + c_n$, $b_n \to \dfrac{1}{2}$, $c_n \to 3$.

   (a) Si (s_n) vérifie $s_{n+1} = \dfrac{3}{4}s_n + 4$, calculer s_n, et en donner la limite.

   (b) On se donne N tel que $\forall n \geq N$, $|b_n| \leq \dfrac{3}{4}$ et $|c_n| \leq 4$.
   En utilisant une suite comme en (a), définie à partir du rang N (s_N est à définir), et une majoration à établir de $|a_n|$, montrer que (a_n) est bornée.

   (c) **Optionnel**: si x est une valeur d'adhérence de (a_n), établir la valeur (unique) de x. Conclusion?

4. Un théorème de Dirichlet.
   C'est une utilisation du principe des tiroirs: si $n+1$ objets sont rangés dans n tiroirs, au moins un tiroir contient deux objets. C'est tout bête, mais bien appliqué on en déduit des résultats importants.

   (a) Soient $\alpha \in \mathbb{R}$ et $n \in \mathbb{N}^*$. En considérant $k\alpha - E(k\alpha)$, $k = 0, ..., n$, qui sont dans $[0,1[= [0, 1/n[\cup [1/n, 2/n[\cup \ ... \cup [(n-1)/n, 1[$, montrer qu'il existe $p \in \mathbb{Z}$ et $q \in [\![1, n]\!]$ tels que $\left|\alpha - \dfrac{p}{q}\right| \leq \dfrac{1}{nq} \leq \dfrac{1}{q^2}$.

   (b) On suppose $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. En vertu de la question précédente, on peut se donner $(p_n) \in \mathbb{Z}^{\mathbb{N}}$, et $(q_n) \in (\mathbb{N}^*)^{\mathbb{N}}$ tels que $\forall n,\ q_n \in [\![1, n]\!]$ et $\left|\alpha - \dfrac{p_n}{q_n}\right| \leq \dfrac{1}{nq_n} \leq \dfrac{1}{q_n^2}$.
   On a donc $\alpha - \dfrac{p_n}{q_n} \underset{n\to+\infty}{\longrightarrow} 0$ et $\left|\alpha - \dfrac{p_n}{q_n}\right| \leq \dfrac{1}{q_n^2}$
   Montrer, par l'absurde, que $q_n \to +\infty$.

5. Pour $n \geq 2$, on considère le polynôme $P_n = X^n - nX - 1$.

   (a) Montrer que P_n possède une unique racine dans $\mathbb{R}^+$, que l'on note x_n.

   (b) Soit $a \geq 0$. Vérifier que $P_n(a) \underset{n\to+\infty}{\longrightarrow} \begin{cases} -\infty \ si\ a \leq 1 \\ +\infty \ si\ a > 1 \end{cases}$.

   En déduire que $x_n \underset{n\to+\infty}{\longrightarrow} 1$ (On justifiera, si $\varepsilon > 0$, que $x_n \in [1, 1+\varepsilon]$ pour n assez grand).

   (c) On pose $u_n = \ln(x_n)$. Vérifier que $u_n = \dfrac{\ln(n)}{n} + \dfrac{u_n}{n} + \dfrac{1}{n}\ln\left(1 + \dfrac{e^{-u_n}}{n}\right)$.
   Déterminer un équivalent de u_n puis de $1 - x_n$ quand $n \to +\infty$. (quel est le terme prépondérant du membre droite de l'égalité?)
   Déterminer un développement asymptotique à deux termes de $1 - x_n$.

6. On rappelle que, si $A \in \mathcal{M}_n(K)$ est de rang r, il existe $P, Q \in GL_n(K)$ telles que $A = PJ_rQ$, où $J_r = diag(\underbrace{1, ..., 1}_{r\ termes}, 0, ..., 0)$.

   (a) $GL_n(K)$ est dense dans $\mathcal{M}_n(K)$: Si $A \in \mathcal{M}_n(K)$, montrer qu'il existe $(B_k) \in GL_n(K)^{\mathbb{N}}$ telle que $B_k \underset{k\to+\infty}{\longrightarrow} A$.
   Résultat très important que nous utiliserons à bien des reprises.

(b) Un exemple d'application (qui aura son utilité dans le cours):
Si $A \in GL_n(K)$, $B \in \mathcal{M}_n(K)$, et $x \in K$, montrer que $\det(xI_n - AB) = \det(xI_n - BA)$.
Etablir le résultat avec $A, B \in \mathcal{M}_n(K)$.

7. Si $n \in \mathbb{N}^*$ on pose $f_n : x \mapsto \left(1 + \frac{x}{n+1}\right)^n - e^x$.
On admet que pour tout n impair l'équation $f_n(x) = 0$ admet une unique solution dans $\mathbb{R}_-^*$, que l'on note x_n. (simple étude de fonction)

(a) Si $x \in \mathbb{R}$, montrer que $f_n(x) \underset{n\to+\infty}{\longrightarrow} 0$.

(b) Déterminer, si $x \in \mathbb{R}\backslash\{0, -2\}$ est fixé, un équivalent de $f_n(x)$ quand $n \to +\infty$. (on trouvera un équivalent du type $f_n(x) \underset{n\to+\infty}{\sim} \frac{C(x)}{n}$. Faire très attention aux "o", on peut facilement se tromper. $C(x)$ est censé changer de signe en $x = 2$.)

(c) En considérant le signe de $C(x)$, montrer que $x_n \underset{\substack{n\to+\infty \\ n \text{ impair}}}{\longrightarrow} -2$. ("en ε")

8. **Optionnel** Lemme de Feteke
Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$ une suite positive sous-additive : $\forall m, n,\ u_{m+n} \leq u_m + u_n$.
On va montrer que $\left(\frac{u_n}{n}\right)$ converge.
Ce résultat a entre-autre des conséquences en probabilité sur les phénomènes de grandes déviations.

(a) On se fixe $q \in \mathbb{N}^*$. Pour $n \geq q$, on note $n = k_n q + r_n$ avec $r_n \in [\![0, q-1]\!]$ (division euclidienne de n par q)
Montrer que $u_n \leq (k_n - 1)u_q + u_{q+r_n}$ puis que $\frac{u_n}{n} \leq \frac{n - r_n - q}{n}\frac{u_q}{q} + \frac{\max\limits_{0\leq i\leq q-1} u_{q+i}}{n}$.

(b) Passer l'inégalité précédente à la limite supérieure sur n puis le résultat obtenu à la limite inférieure sur q, et conclure.

9. **Optionnel**. Nombre de Liouville.
Un réel x est dit algébrique si et seulement si il existe $P \in \mathbb{Q}[X]\backslash\{0\}$ tel que $P(x) = 0$.
Si $x \in \mathbb{Q}$, x est algébrique car racine de $X - x$.
$\sqrt{2}$ est algébrique, car racine de $X^2 - 2$, et irrationnel.
x est dit transcendant si et seulement si il n'est pas algébrique.

(a) Soit $x \in \mathbb{R}$ un nombre algébrique. On se donne $P \in \mathbb{Q}[X]\backslash\{0\}$ tel que $P(x) = 0$. Soit $N = deg(P)$
Quitte à multiplier P par un certain entier, on peut supposer $P \in \mathbb{Z}[X]$.
Soit $\delta > 0$ tel que P n'ait pas de racine dans $[x - \delta, x + \delta]$ autre que x. (justifier)
Notons $C = \sup\limits_{t\in[x-\delta,x+\delta]} |P'(t)|$ (justifier que $C < \infty$)
Montrer que si $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et $0 < \left|x - \frac{a}{b}\right| \leq \delta$, alors $\frac{1}{b^N} \leq C\left|x - \frac{a}{b}\right|$.
Ceci dit qu'un nombre algébrique ne peut pas s'approcher "trop vite" par des rationnels.

(b) Justifier l'existence de $x = \sum_{n=0}^{+\infty} \frac{1}{10^{n!}}$.
On écrit $S_n = \sum_{k=0}^{n} \frac{1}{10^{k!}}$.
Si $N \in \mathbb{N}$, montrer que $10^{n!N}|S_n - x| \underset{n\to+\infty}{\longrightarrow} 0$ puis que x est transcendant.

10. **Optionnel**.
Soit $(a_n) \in \mathbb{R}^n$ bornée telle que $a_{n+1} - a_n \xrightarrow[n\to+\infty]{} 0$.

Rappel: Ceci n'implique pas que (a_n) converge (cex: $a_n = \ln(n)$. (a_n) cv si et seulement si $\sum_n (a_{n+1} - a_n)$ converge).

On note $I = VA((a_n))$.
Si $c, d \in I$, $c < d$, et $x \in [c, d]$, montrer que $x \in I$. (faire un dessin, comprendre ce qui se passe. La formalisation peut s'avérer un peu pénible).
De quel type est I?

11. **Optionnel**. Critère de Cauchy
Soit $(u_n) \in K^{\mathbb{N}}$. Montrer que (u_n) converge si et seulement si
$\forall \varepsilon > 0,\ \exists N \in \mathbb{N};\ \forall n, p \geq N,\ |u_n - u_p| \leq \varepsilon$.
Pour le sens "$\Leftarrow$" on pourra montrer que (u_n) est bornée, et utiliser la propriété 3.

12. **Optionnel**.
Recouvrement de la sphère unité de $\mathbb{R}^n$.

Ici, K ne désigne pas $\mathbb{R}$ ou $\mathbb{C}$. $\|\cdot\|$ désigne la norme euclienne standard de $\mathbb{R}^n$.

$n \in \mathbb{N}^*$ est fixé.
Si $a \in \mathbb{R}^n$, on note $B_{a,r} = \{x \in \mathbb{R}^n\ ;\ \|x - a\| \leq r\}$ la boule fermée de centre a et de rayon r.
$S = \{a \in \mathbb{R}^n \mid \|a\| = 1\}$ est la sphère unité de $\mathbb{R}^n$.

Soit K une partie bornée non vide de $\mathbb{R}^n$, et soit $\varepsilon > 0$.

(a) Montrer que l'on peut trouver un sous ensemble fini A de K tel que :

$$K \subset \bigcup_{a \in A} B_{a, \frac{\varepsilon}{2}}.$$

On pourra raisonner par l'absurde en construisant une suite de $K^{\mathbb{N}}$ niant le théorème de Bolzano-Weierstrass.

(b) Soit Λ un sous ensemble de K tel que pour tous x, y distincts dans Λ, $\|x - y\| > \varepsilon$. Montrer que Λ est fini et que son cardinal est majoré par celui d'un ensemble A du type considéré à la question précèdente.
Si de plus Λ est de cardinal maximal, montrer que : $K \subset \bigcup_{a \in \Lambda} B_{a,\varepsilon}$

On admet l'existence d'une fonction μ, appelée *volume*, définie sur certaines parties bornées de $\mathbb{R}^n$ (on fera ici comme si μ était définie sur toutes les parties bornées. En fait, μ n'est pas définie sur des parties assez pathologiques) et vérifiant les propriétés suivantes.

(i) Pour tout vecteur a de $\mathbb{R}^n$ et tout nombre réel $r > 0$, $\mu(B_{a,r}) = r^n$.

(ii) Pour toute famille $K_1, \ldots, K_m$ de parties bornées $\mathbb{R}^n$ deux à deux disjointes on a :

$$\mu\left(\bigcup_{1 \leq i \leq m} K_i\right) = \sum_{i=1}^{m} \mu(K_i).$$

(iii) Pour toutes K, K' parties bornées de $\mathbb{R}^n$, $K \subset K'$ implique $\mu(K) \leq \mu(K')$.

Soit Λ une partie finie de S telle que pour tous x, y distincts dans Λ, $\|x - y\| > \varepsilon$.

(c) Vérifier que les boules $B_{a,\frac{\varepsilon}{2}}$ pour $a \in \Lambda$ sont toutes contenues dans $B_{0,1+\frac{\varepsilon}{2}}$.

Montrer alors que le cardinal de Λ est majoré par $\left(\frac{2+\varepsilon}{\varepsilon}\right)^n$.

(d) Justifier l'existence d'une partie finie Λ_n de S, de cardinal majoré par 5^n, et telle que :

$$S \subset \bigcup_{a \in \Lambda_n} B_{a,\frac{1}{2}}.$$

1 Quelques rappels

1.1 Congruences

Deux remarques servent souvent:
Remarque 1: $a, b \in \mathbb{N}^*$. On s'intéresse aux congruences de a^n modulo b.
$\forall n \in \mathbb{N}$, $a^n \equiv c_n[b]$ avec $c_n \in [\![0, b-1]\!]$.
Donc (principe des tiroirs), il existe $n, m \in [\![0, b]\!]$ avec $n < m$ tels que $c_n = c_m$ ie $a^n \equiv a^m[b]$.
Alors en multipliant par a, $a^{n+1} \equiv a^{m+1}[b]$, puis $a^{n+2} \equiv a^{m+2}[b]$, etc...
Donc les puissances de a modulo b cyclent à partir d'un certain rang.
Par exemple, si on regarde $4^n[14]$, $1, 4, 4^2, 4^3, 4^4$ sont congrus à $1, 4, 2, 8, 4$ modulo 14, donc il y a un cycle de longueur 3 commençant pour $n = 1$, $4^{1+3k} \equiv 4^k[14]$, et 4^n ne prend par toutes les congruences possibles modulo 14.

Remarque 2: Cette fois-ci, on fixe n, et on regarde $a^n[b]$ quand a décrit $\mathbb{Z}$.
Il suffit de regarder $a \in [\![0, b-1]\!]$ pour voir toutes les valeurs possibles.
Par exemple, si on calcule $a^3[13]$ pour $a = 0, 1, ..., 12$, on trouve $0, 1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12$.
Donc un cube ne peut être congru qu'à $0, 1, 8, 5, -1$ modulo 13.(cf exercice 6)

1.2 PGCD, lemme de GAUSS

Il est souvent nécessaire de simplifier par le PGCD avant d'utiliser le lemme de Gauss:
Si $a|bc$, et $d = a \wedge b$, on écrit $a = da'$, $b = db'$. $a' \wedge b' = 1$, et $a'|b'c$, donc $a'|c$.

Deux entiers proches ne peuvent avoir un gros PGCD, car $(a \wedge b)|(b - a)$ (et plus généralement $au + bv$).
Ainsi $n \wedge (n+1) = 1$, $n \wedge (n+2) = \begin{cases} 1 \text{ si } n \text{ impair} \\ 2 \text{ sinon} \end{cases}$.

1.3 Théorème de décomposition, valuations

Notons P l'ensemble des nombres premiers.
Si $n \in \mathbb{N}$, $n \geq 2$, $v_p(n)$ (valuation de n en p) est la puissance à laquelle apparaît p dans la décomposition de n.
On convient que $v_p(1) = 0$.
On a $n = \prod_{p \in P} p^{v_p(n)}$ (produit faussement infini. Seul un nombre fini de facteurs ne valent pas 1).

On rappelle:
Propriété: Si $m, n \in \mathbb{N}^*$

1. $\forall p \in P$, $v_p(mn) = v_p(m) + v_p(n)$.
2. $m|n$ si et seulement si $\forall p \in P$, $v_p(m) \leq v_p(n)$, et, si $m|n$, $\forall p \in P$, $v_p(n/m) = v_p(n) - v_p(m)$.
3. $pdcg(m, n) = \prod_{p \in P} p^{\min(v_p(n), v_p(m))}$, $ppcm(m, n) = \prod_{p \in P} p^{\max(v_p(n), v_p(m))}$.
4. Les diviseurs positifs de n sont les $\prod_{p \in P} p^{\alpha_p}$ avec $\alpha_p \in [\![0, v_p(n)]\!]$. Il y en a $\prod_{p \in P} (1 + v_p(n))$.

Beaucoup de choses se voient bien mieux en pensant nombres premiers que lemme de Gauss.

Ayant parlé de diviseurs, parlons de multiples. Un point simple mais d'usage constant:
Si $m, n \in \mathbb{N}^*$, il y a $E(n/m)$ multiples de m dans $[\![1, n]\!]$. En effet ce sont $m, 2m, 3m, ..., km$ avec $km \leq n < (k+1)m$, ie $k \leq n/m < k+1$, ie $k = E(n/m)$.

1.4 Petit théorème de Fermat

Rappelons l'énoncé: si $p \in P$, $a \in \mathbb{N}^*$, et p ne divise pas a, alors $a^{p-1} \equiv 1[p]$.

C'est un cas particulier du théorème d'Euler, que nous verrons en cours.

Il en résulte que $\forall a$, $a^p \equiv a[p]$, ceci étant vrai si $p|a$.

2 Exercices

Exercice 1:

Quel est le dernier chiffre de l'écriture en base 10 de $7^{7^{7^{7^{7^{7}}}}}$?
Attention: $a^{b^{c^{\cdots}}}$ se lit $a^{\left(b^{(c^{\cdots})}\right)}$ et non $\left(\left((a^b)^c\right)^{\cdots}\right) = a^{bc\cdots}$.

Exercice 2:

1. Soient $n \in \mathbb{N}^*$, $a_0, ..., a_{n-1} \in \mathbb{Z}$ et $r \in \mathbb{Q}$ tels que $a_0 + a_1 r + ... + a_{n-1} r^{n-1} + r^n = 0$.
   En écrivant r sous forme irréductible, montrer que $r \in \mathbb{Z}$.
2. Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, montrer que $\cos((n+1)x) = 2\cos(x)\cos(nx) - \cos((n-1)x)$.
3. Montrer que pour tout $n \in \mathbb{N}^*$ il existe P_n, polynôme à coefficients entiers relatifs du type $P_n(X) = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$ tel que $\forall x \in \mathbb{R}$, $P_n(2\cos(x)) = 2\cos(nx)$. [$P_n$ est en relation avec le n-ième polynôme de Tchebychev]
4. Soit $n \in \mathbb{N}^*$. Si $r \in \mathbb{Q}$ vérifie $P_n(r) = 2$ montrer que $r \in \mathbb{Z}$.
5. Si $x \in \mathbb{R}$ est tel que $\cos(x) \in \mathbb{Q}$ et $\dfrac{x}{\pi} \in \mathbb{Q}$, montrer que $\cos(x) \in \{-1, -1/2, 0, 1/2, 1\}$

Exercice 3:
Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs positifs de n.

1. Montrer que si $n = ab$ avec $a \wedge b = 1$, alors $d_n = d_a d_b$.
2. Montrer que n est un carré (d'entier) si et seulement si d_n est impair.
3. Montrer que : $\displaystyle\prod_{d|n} d = \sqrt{n}^{d_n}$ (regroupement de termes par deux, un terme pouvant rester seul).
4. On pose $\theta(i,j) = \begin{cases} 1 \ si \ i|j \\ 0 \ sinon \end{cases}$.
   Si $j \in [\![1, n]\!]$, vérifier que $\displaystyle\sum_{i=1}^{n} \theta(i,j) = d_j$.
   Si $i \in [\![1, n]\!]$, montrer que $\displaystyle\sum_{j=1}^{n} \theta(i,j) = E(n/i)$.
   Montrer que $\displaystyle\sum_{k=1}^{n} d_k = \sum_{k=1}^{n} E(n/k)$.
5. Donner un équivalent de cette somme quand $n \to +\infty$. (encadrement intégral)

Exercice 4:

1. Montrer que tout entier > 6 peut s'écrire $a + b$ où $a, b \geq 2$ et $a \wedge b = 1$. (penser à des choses comme $n \wedge (n+1) = 1$)

2. Soit $(p_n)_{n\in\mathbb{N}^*}$ la suite croissante des nombres premiers. ($p_1 = 2,\ p_2 = 3,\ p_3 = 5, ...$)
Montrer que pour $n \geq 3$, $p_1 p_2 ... p_n \geq p_{n+1} + p_{n+2}$.

Exercice 5:

1. $a, b \in \mathbb{N}^*$ et $a \wedge b = 1$. Justifier que ab est un carré (d'entier) si et seulement si a et b sont des carrés.
Si $a \wedge b = 2$ et ab est un carré, justifier que $a/2$ et $b/2$ sont des carrés.

2. Montrer que, si $n \in \mathbb{N}^*$, $n(n+1)(n+2)$ n'est pas un carré.

Exercice 6:

1. Soient $x, y, z \in \mathbb{Z}$ tels que $5x^3 + 11y^3 + 13z^3 = 0$. Montrer que 13 divise x, y, z.

2. Quelles sont les solutions dans $\mathbb{Z}^3$ de $5x^3 + 11y^3 + 13z^3 = 0$?

Exercice 7: Soit $a \in \mathbb{N}$ premier à 10.

1. Montrer que pour tout entier $k \in \mathbb{N}$, $a^{4\times 10^k} \equiv 1[10^{k+1}]$.

2. En déduire qu'il existe un nombre $x \in \mathbb{N}$ tel que x^3 se termine par 123456789 en base 10. On cherchera x sous la forme 123456789^n

Exercice 8: Théorème chinois (sera revu en cours)
Soient $a_1, ..., a_n \in \mathbb{N}^*$ premiers entre eux deux à deux, et $b_1, ..., b_n \in \mathbb{Z}$.

1. Si $i \in [\![1, n]\!]$, notons $(S_i) : \begin{cases} x \equiv 0[a_1] \\ \vdots \\ x \equiv 1[a_i] \\ \dots \\ x \equiv 0[a_n] \end{cases}$.
A l'aide d'une relation de Bezout, justifier l'existence de $x_i \in \mathbb{Z}$ solution de (S_i).

2. Montrer qu'il existe $x \in \mathbb{Z}$ tel que $\forall i \in [\![1, n]\!],\ x \equiv b_i[a_i]$.

3. Une application: On dit que $n \in \mathbb{N}^*$ a un facteur carré s'il existe p premier tel que $v_p(n) \geq 2$.
Montrer qu'il existe 1000 entiers ≥ 1 consécutifs ayant un facteur carré.

Exercice 9:
Dans la suite, $C_n^p = \dfrac{n!}{p!(n-p)!}$ désigne un coefficient binomial.

p est un nombre premier. Si $n \in \mathbb{N}^*$, $v_p(n)$ désigne la valuation en p de n.

1. On pose $\theta(i, j) = \begin{cases} 1 \text{ si } p^i \text{ divise } j \\ 0 \text{ sinon} \end{cases}$. Que vaut $\displaystyle\sum_{i=1}^{+\infty} \theta(i, j)$?

2. Montrer que $v_p(n!) = \displaystyle\sum_{k=1}^{+\infty} E(n/p^k)$ (formule de Legendre).
Les deux questions suivantes sont optionnelles.

3. q est un entier > 0 non divisible par p, et $k \in \mathbb{N}$. Montrer que $v_p\left(C_{p^k q}^{p^k}\right) = 0$.

4. $n \in \mathbb{N}$, $n \geq 2$. Montrer que p divise tous les C_n^k, $k = 1, ..., n-1$, si et seulement si n est une puissance de p.

Exercice 10: Inégalités de Tchebychev
Optionnel

On utilisera: si p est premier et $n \in \mathbb{N}^*$, $v_p(n!) = \sum_{k\geq 1} E\left(\frac{n}{p^k}\right)$ (voir exercice précédant)

Si $\mathbf{x} \in \mathbb{R}^+$ notons $\pi(\mathbf{x})$ le nombre de nombres premiers inférieurs ou égaux à x.
Un célèbre théorème stipule que $\pi(x) \underset{x\to+\infty}{\sim} \frac{x}{\ln(x)}$.
On établit un résultat plus faible, le premier obtenu par Tchebychev.

1. Montrer que $\forall k \in \mathbb{N}$, $\pi(2^{k+1}) \leq 2^k$.

2. Soit $n \in \mathbb{N}^*$. Si $p \leq 2n$ premier et $r \in \mathbb{N}^*$ est l'unique entier tel que $p^r \leq 2n < p^{r+1}$ (justifier) montrer que $v_p(C_{2n}^n) \leq r$ puis que: $\prod_{\substack{p \text{ premier} \\ \text{dans }]n,2n]}} p \mid C_{2n}^n \mid \prod_{\substack{p \text{ premier} \leq 2n \text{ et } r \\ \text{tel que } p^r \leq 2n < p^{r+1}}} p^r$

   En déduire que $n^{\pi(2n)-\pi(n)} < C_{2n}^n \leq (2n)^{\pi(2n)}$.

3. Montrer que $\forall n \in \mathbb{N}^*$, $2^n \leq C_{2n}^n \leq 2^{2n}$ et en déduire en prenant $n = 2^k$ pour $k \in \mathbb{N}$ que:

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \text{ et } 2^k \leq (k+1)\pi(2^{k+1})$$

4. Montrer que si $k \in \mathbb{N}$: $\frac{2^{k+1}}{2(k+1)} \leq \pi(2^{k+1}) \leq 3\frac{2^{k+1}}{k+1}$

5. Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ tel que $2^k \leq n < 2^{k+1}$. Montrer que: $\frac{n\ln 2}{4\ln(n)} \leq \pi(n) < \frac{(6\ln 2)n}{\ln(n)}$

Exercice 11: Optionnel
Si $n \in \mathbb{N}^*$, soit $a_n = \max\{ordre(\sigma) \mid \sigma \in S_n\}$.
Si $k \in \mathbb{N}$, montrer que $n^k \underset{n\to+\infty}{=\!=} o(a_n)$.
Penser à la relation entre l'ordre et la décomposition en produit de cycles à supports disjoints, et au fait que des entiers proches n'ont pas un gros PGCD.

1 Quelques rappels et compléments

1.1 Introduction et notations

Partout, K est un corps commutatif (au programme, officiellement un sous-corps de $\mathbb{C}$), E, F, G des K-ev non réduits à $\{0\}$.
Je noterai $Mat_{B,B_2}(f)$ la matrice de f avec base de départ B et base d'arrivée B_2, et $Pass_{B,B_2}$ la matrice de passage de la base B à la base B_2.
Il n'y a pas de notation standard pour ces choses, mais toutes se comprennent très bien.
Un rappel : la définition des matrices de passage est illogique. $Pass_{B,B_2} = Mat_{B_2,B}(id)$. On lit sur les colonnes de $Pass_{B,B_2}$ les décompositions des éléments de B_2 dans la base B.

Si B, B_2 sont deux familles de E, je noterai (B, B_2) la famille obtenue en concaténant les deux.

BC_n désigne la base canonique de K^n.
Rapellons qu'on assimile couramment K^n à $\mathcal{M}_{n,1}(K)$ (vecteurs colonne).
Si $A \in \mathcal{M}_{n,p}(K)$, et qu'on écrit AX avec $X \in K^p$, il est sous-entendu que X est écrit "en colonne".

Si $f \in \mathcal{L}(E)$, et $n \in \mathbb{N}$, f^n désigne l'itérée n-ième de f : $f^0 = id$, $f^n = \underbrace{f \circ ... \circ f}_{n \text{ termes}}$ si $n \geq 1$.

Si de plus f est bijective, $f^{-n} = (f^{-1})^n$. On a $f^n \circ f^m = f^{n+m}$.

1.2 Théorème du rang et conséquence

On rappelle:

Propriété 1: Si $f \in \mathcal{L}(E, F)$, et S est un supplémentaire de $Ker(f)$ ($E = Ker(f) \oplus S$), alors $g : \begin{cases} S \to Im(f) \\ x \mapsto f(x) \end{cases}$ est un isomorphisme.

Cette propriété est importante en soit. Vous l'avez démontrée pour établir le théorème du rang:

Propriété 2: Si $f \in \mathcal{L}(E, F)$ et E est de dimension finie, alors $Im(f)$ est de dimension finie et $\dim(E) = \dim(Ker(f)) + rg(f)$.

Rappelons quelques conséquences usuelles du théorème du rang: Soit $f \in \mathcal{L}(E, F)$, E étant de dimension finie. On a

1. $rg(f) \leq \dim(E)$ (une application linéaire n'augmente pas les dimensions) avec égalité si et seulement si $Ker(f) = \{0\}$ ie f injective.
2. Si $\dim(E) < \dim(F)$, f ne peut être surjective, et si $\dim(E) > \dim(F)$, f ne peut être injective.
3. Si f est un isomorphisme, alors $\dim(E) = \dim(F)$.
4. Si $\dim(F) = \dim(E)$, alors (f injective)$\Longleftrightarrow$(f surjective)$\Longleftrightarrow$(f bijective)

1.3 Restriction et induit

Si $f \in \mathcal{L}(E, F)$, et V un sev de E, la restriction de f à V est l'application $f_{|V} : \begin{cases} V \to F \\ x \mapsto f(x) \end{cases}$.
$f_{|V} \in \mathcal{L}(V, F)$.

Les remarques liées au théorème du rang s'appliquent à $f_{|V}$: si V est de dimension finie, $\dim(f(V)) =$

$\dim(Im(f_{|V})) \leq \dim(V)$, avec égalité si et seulement si $Ker(f_{|V}) = \{0\}$, ie $Ker(f) \cap V = \{0\}$.

Si E, F sont de dimension finies, que B_V est une base de V, que l'on complète en $B = (B_V, B_2)$ base de E, que B_F est une base de F, et que, par blocs, on a $Mat_{B,B_F} = \begin{pmatrix} \underbrace{A}_{f(B_V)} & B \end{pmatrix}$, alors $A = Mat_{B_V,B_F}(f_{|V})$.

Si $f \in \mathcal{L}(E)$, et V est un sev de E, on dit que V est stable par f si et seulement si $f(V) \subset V$ ie $\forall x \in V$, $f(x) \in V$.
Si V est stable par f, on appelle induit par f sur V l'application $f_V : \begin{cases} V \to V \\ x \mapsto f(x) \end{cases}$.
$f_V \in \mathcal{L}(V)$.

Si E est de dimension finie, V sev de E, que B_V est une base de V, que l'on complète en $B = (B_V, B_2)$ base de E :
Notons $W = vect(B_2)$. On a donc $V \oplus W = E$.
Notons par bloc $Mat_B(f) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, les blocs étant adaptés à B_V, B_2.
Alors V est stable par f si et seulement si $C = 0$, et, si c'est le cas, $A = M_{B_V}(f_V)$.

Si $C \neq 0$, f_V n'existe pas, et $A = M_{B_V}(p \circ f_{|V})$, où p est la projection sur V parallèlement à W, considérée comme élément de $\mathcal{L}(E, V)$.

Tout ceci se généralise avec plus de découpage, B_V n'étant pas forcément en première position.

1.4 Quelques points sur les composées

$f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$.

On rappelle les inclusions immédiates d'usage constant $Im(g \circ f) \subset Im(g)$, $Ker(f) \subset Ker(g \circ f)$.

Si E, F sont de dimensions finies on a $rg(g \circ f) \leq \min(rg(f), rg(g))$.
L'inégalité $rg(g \circ f) \leq rg(f)$ vient de $Im(g \circ f) = g(Im(f))$.

Il peut être intéressant d'écrire le théorème du rang pour $g_{|Im(f)} \in \mathcal{L}(Im(f), G)$:
$g_{|Im(f)} = g(Im(f)) = Im(g \circ f)$, et $Ker(g_{|Im(f)}) = Ker(g) \cap Im(f)$, donc on a:
$rg(f) = rg(g \circ f) + dim(Ker(g) \cap Im(f))$.

1.5 Théorèmes de factorisation

Complément indispensable à connaître.
E, F sont supposés de dimensions finies.

Propriété 3: Théorèmes de factorisation

1. Si $g \in \mathcal{L}(F, G)$, $h \in \mathcal{L}(E, G)$, alors il existe $f \in \mathcal{L}(E, F)$ tel que $h = g \circ f$ si et seulement si $Im(h) \subset Im(g)$
2. Si $f \in \mathcal{L}(E, F)$, $h \in \mathcal{L}(E, G)$, alors il existe $g \in \mathcal{L}(F, G)$ tel que $h = g \circ f$ si et seulement si $Ker(f) \subset Ker(h)$

Démonstration

1. $\Longrightarrow$: facile
   $\Leftarrow$: On suppose $Im(h) \subset Im(g)$.
   Soit $(e_1, ..., e_n)$ une base de E.
   $\forall i$, $h(e_i) \in Im(h) \subset Im(g)$, donc on peut se fixer $y_i \in F$ tel que $g(y_i) = h(e_i)$.

Soit f l'unique application linéaire telle que $\forall i,\ f(e_i) = y_i$.
$g \circ f(e_i) = g(y_i) = h(e_i)$. h et $g \circ f$, linéaires, coïncident sur une base, donc sont égales.

2. $\Longrightarrow$: facile
   $\Leftarrow$: on suppose $Ker(f) \subset Ker(h)$.
   Soient S un supplémentaire de $Ker(f)$, et V un supplémentaire de $Im(f)$. $E = Ker(f) \oplus S$, $F = Im(f) \oplus V$.
   Soit $q : \begin{cases} S \to V \\ x \mapsto f(x) \end{cases}$. On sait que q est bijective.
   Comme $F = Im(f) \oplus V$, on peut définir g comme l'unique application linéaire telle que:
   $g_{|V} = 0$ (linéaire)
   $g_{|Im(f)} = h \circ q^{-1}$ (linéaire).

   $\forall x \in Ker(f),\ g \circ f(x) = 0 = h(x)$ car $Ker(f) \subset Ker(h)$.
   $\forall x \in S,\ g \circ f(x) = h(q^{-1}(f(x))) = h(x)$ car $x \in S$, donc $q^{-1}(f(x)) = x$.

   Alors, h et $g \circ f$, linéaires, coïncident sur $Ker(f)$ et S, donc sont égales car $E = Ker(f) \oplus S$. ♣

1.6 Application linéaire canoniquement associée

Si $A \in \mathcal{M}_{n,p}(K)$, l'application linéaire canoniquement associée à A est $f_A : \begin{cases} K^p \to K^n \\ X \mapsto AX \end{cases}$. (pas ne notation standard)

Par définition, $rg(A)$, $Im(A)$, $Ker(A)$ sont $rg(f_A)$, $Im(f_A)$, $Ker(f_A)$.

Le théorème du rang pour A est donc: $p = \dim(Ker(A)) + rg(A)$.

On a $A = Mat_{BC_p, BC_n}(f_A)$.

$f_A + f_B = f_{A+B}$, $f_{\lambda A} = \lambda f_A$, $f_A \circ f_B = f_{AB}$.

En passant par les ALCA, le pendant matriciel du premier théorème de factorisation, par exemple, est: si $G \in \mathcal{M}_{q,p}(K)$ et $H \in \mathcal{M}_{q,n}$, alors il existe $F \in \mathcal{M}_{p,n}(K)$ telle que $H = GF$ si et seulement si $Im(H) \subset Im(G)$.

Propriété 4: Invariance du rang par extension de corps
Si $K_1 \subset K_2$ sont des corps commutatifs, (exemple: $K_1 = \mathbb{R},\ K_2 = \mathbb{C}$) et $A \in \mathcal{M}_n(K_1)$, le rang de A en tant que matrice de $\mathcal{M}_n(K_1)$ est le même que celui en tant que matrice de $\mathcal{M}_n(K_2)$.

Démonstration: On peut invoquer la caractérisation du rang avec les matrices extraites inversibles, et l'inversibilité d'une matrice est invariante par extension de corps du fait de la caractérisation avec le déterminant. ♣

1.7 Équivalence de matrices

Définition 1: Si $A, B \in \mathcal{M}_{n,p}(K)$, On dit que A est équivalente à B si et seulement si il existe $P \in GL_n(K)$, $Q \in GL_p(K)$ telles que $A = PBQ$.

C'est facilement une relation d'équivalence, et on rappelle:

Propriété 5: $A, B \in \mathcal{M}_{n,p}(K)$ sont équivalentes si et seulement si $rg(A) = rg(B)$.

1.8 Similitude de matrices

Définition 2: Si $A, B \in \mathcal{M}_n(K)$, on dit que A est semblable à B (on notera $A \sim B$, non standard) si et seulement si il existe $P \in GL_n(K)$ telle que $A = PBP^{-1}$.

La relation de similitude est facilement une relation d'équivalence. Elle ne concerne que les matrices carrées.
C'est une relation plus fine et compliquée de la relation d'équivalence, que nous étudierons en détail dans l'année.

On rappelle la caractérisation géométrique, dont la démonstration repose sur les formules de changement de bases:

Propriété 6: Soient $A, B \in \mathcal{M}_n(K)$.
Sont équivalents:

1. $A \sim B$
2. Il existe une base C de K^n telle que $B = Mat_C(f_A)$.
3. Si E est un K-ev de dimension n, il existe $f \in \mathcal{L}(E)$, et C, C' deux bases de E telle que $A = Mat_C(f)$ et $B = Mat_{C'}(f)$.

On se sert surtout du deuxième point : Inutile d'introduire un espace théorique, K^n est standard.

Un exemple, dans $\mathcal{M}_3(\mathbb{R})$:
Soient $A = \begin{pmatrix} 7 & 2 & -5 \\ 6 & 2 & -4 \\ 6 & 1 & -3 \end{pmatrix}$ et $B = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.
On veut montrer élémentairement que $A \sim B$.

On cherche $C = (e_1, e_2, e_3)$ base de $\mathbb{R}^3$ telle que $B = Mat_C(f_A)$ ie $\begin{cases} f_A(e_1) = 4e_1 \\ f_A(e_2) = e_2 \\ f_A(e_3) = e_2 + e_3 \end{cases}$ ie $\begin{cases} Ae_1 = 4e_1 \\ Ae_2 = e_2 \\ Ae_3 = e_2 + e_3 \end{cases}$.

Trouvez une telle base C (il n'y a pas unicité), et en écrivant $A = Mat_{BC_3}(f_A) = Pass_{BC_3,C} Mat_C(f_A) Pass_{C,BC_3}$, donner $P \in GL_3(\mathbb{R})$ telle que $A = PBP^{-1}$.

Certaines quantités sur des endomorphismes sont définies à partir des matrices, ce qui implique un choix de base, en prenant la même au départ et à l'arrivée. Encore faut-il que la quantité matricielle ne dépende pas du choix de la base. Pensez à la trace.
On en parlera en cours (invariant de similitude)

1.9 Un exemple de récurrence

On sera souvent amené à faire des récurrences sur la dimension / les tailles de matrices avec des calculs par blocs, en naviguant entre arguments "géométriques" (changements de bases, endomorphismes), et calcul matriciel.
Un exemple (classique, ce n'est pas un résultat de cours)

Propriété 7: Soit $A \in \mathcal{M}_n(K)$ de trace nulle. Alors A est semblable à une certaine matrice de diagonale nulle.

On utilisera la propriété:

Propriété 8: Soit $A \in \mathcal{M}_n(K)$, $A \notin vect(I_n)$. Alors il existe $x \in K^n$ tel que (x, Ax) soit libre.

La démonstration de la propriété 8 est laissée au lecteur. Vous l'avez probablement fait en exercice en sup, sous forme matricielle, ou endomorphisme (valable en dimension infinie)

Démonstration de la propriété 7
H_n : "Si $A \in \mathcal{M}_n(K)$ est de trace nulle, alors A est semblable à une certaine matrice de diagonale nulle".
$n = 1$: Soit $A \in \mathcal{M}_1(K)$ de trace nulle. Alors $A = 0$, et donc $A \sim 0$.
Si $n \in \mathbb{N}^*$: supposons $H_1, ..., H_n$ vraies.
Soit $A \in \mathcal{M}_{n+1}(K)$ de trace nulle.
Si $A = \lambda I_n$, $n\lambda = 0$ ie $\lambda = 0$. $A = 0$ et c'est fini.
Sinon : par la propriété 7, on se donne $x \in K^n$ tel que (x, Ax) soit libre.
On complète en $C = (x, Ax, e_3, ..., e_{n+1})$ base de K^{n+1}.
A est semblable à $B = Mat_C(f_A) = \begin{pmatrix} 0 & L \\ 1 & \\ \vdots & T \\ 0 & \end{pmatrix}$ (Sur la première colonne, on lit la décomposition de Ax dans la base $(x, Ax, ..., e_{n+1})$).

$T \in \mathcal{M}_n(K)$. Comme $A \sim B$, $0 = tr(A) = tr(B) = tr(T)$.
Par H_n, il existe $Q \in GL_n(K)$ et $D \in \mathcal{M}_n(K)$ à diagonale nulle telles que $T = QDQ^{-1}$.
On se fixe Q et D ainsi.
Notons $U = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{pmatrix}$. Un produit pas blocs montre que U est inversible d'inverse $U^{-1} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & Q^{-1} & \\ 0 & & & \end{pmatrix}$.
On fait le produit par bloc $U^{-1}BU = \begin{pmatrix} 0 & ? \\ ? & Q^{-1}TQ \end{pmatrix} = \begin{pmatrix} 0 & ? \\ ? & D \end{pmatrix} = W$.
W est donc de diagonale nulle. $A \sim B$ et $B \sim W$, donc $A \sim W$. ♣

1.10 Déterminant

Le déterminant est polynomial en ses coefficients.

On utilise souvent des argument polynomiaux.

Notez, par exemple, (peut se voir avec la formule générale) des choses comme:
Si $A, B \in \mathcal{M}_n(K)$, $\det(A + xB) = \det(A) + \alpha_1 x + ... + \alpha_{n-1}x^{n-1} + \det(B)x^n$.

Hormis les opérations élémentaires, le développement par rapport une rangée, des produits par bloc peuvent être utiles.

Par exemple, si $A, B, C \in \mathcal{M}_n(K)$: $\begin{pmatrix} I_n & 0 \\ -B & I_n \end{pmatrix}\begin{pmatrix} I_n & A \\ B & C \end{pmatrix} = \begin{pmatrix} I_n & A \\ 0 & -BA + C \end{pmatrix}$, donc
$\det \begin{pmatrix} I_n & A \\ B & C \end{pmatrix} = \det(C - BA)$.

La formule $A\ {}^tCom(A) = \det(A)I_n$ est très importante. Elle ne présente pas d'intérêt pour calculer A^{-1}, mais un intérêt théorique.

Par exemple: Soit $A \in \mathcal{M}_n(\mathbb{Z})$ telle que $\det(A) \neq 0$. $\det(A) \in \mathbb{Z}$ par la formule générale du déter-

minant.
$\mathbb{Z}$ n'est pas un corps. Le premier corps contenant $\mathbb{Z}$ est $\mathbb{Q}$, et en général $A^{-1} \in \mathcal{M}_n(\mathbb{Q})$.
En revanche, si $\det(A) = \pm 1$, la formule $A^{-1} = \dfrac{1}{\det(A)}\ {}^tCom(A)$ montre que $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$, car du fait de la formule du déterminant, les cofacteurs sont entiers.

Donnons une propriété importante que nous rencontrerons à diverses reprises:

Propriété 9: $GL_n(\mathbb{Z})$
Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Sont équivalents:

1. $M\mathbb{Z}^n = \mathbb{Z}^n$ $(M\mathbb{Z}^n = \{MX \mid X \in \mathbb{Z}^n\})$
2. M est inversible (dans $\mathcal{M}_n(\mathbb{Q})$ par exemple), et $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$
3. $\det(M) = \pm 1$.

Démonstration:
$1 \Longrightarrow 2$. On suppose 1.
$\mathbb{Z}$ n'est pas un corps. On passe dans $\mathbb{Q}$. Soit $f \in \mathcal{L}(\mathbb{Q}^n)$ l'application linéaire canoniquement associée à f.
Les vecteurs de la base canonique de $\mathbb{Q}^n$ sont dans $\mathbb{Z}^n$, donc dans $f(\mathbb{Z}^n)$, donc dans $Im(f) = f(\mathbb{Q}^n)$.
Donc f est surjective, donc bijective, et M est inversible dans $\mathcal{M}_n(\mathbb{Q})$.
$M\mathbb{Z}^n = \mathbb{Z}^n$ donc $\mathbb{Z}^n = M^{-1}\mathbb{Z}^n$. En particulier si $(e_1, ..., e_n)$ est la base canonique, $M^{-1}e_i \in \mathbb{Z}^n$, et $M^{-1}e_i$ est la colonne i de M^{-1}, donc M^{-1} est à coefficients entiers.
$2 \Longrightarrow 3$. On suppose 2.
$1 = \det(M)\det(M^{-1})$ et les deux déterminants sont entiers, donc $\det(M) = \pm 1$.
$3 \Longrightarrow 1$. On suppose 3.
Comme $M \in \mathcal{M}_n(\mathbb{Z})$, $M\mathbb{Z}^n \subset \mathbb{Z}^n$.
Comme $\det(M) = \pm 1$, par ce qui a été dit avant, $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.
Ainsi, si $Y \in \mathbb{Z}^n$, $Y = M(M^{-1}Y)$, et $M^{-1}Y \in \mathbb{Z}^n$ ce qui donne $\mathbb{Z}^n \subset M\mathbb{Z}^n$. ♣.

2 Exercices

Exercice 1: Très important, et à connaître. Nous en aurons l'usage à diverses reprises.
K est un corps infini, et E un K-ev.
Soient $F_1, ..., F_n$ des sev de E tels que $E = \bigcup_{i=1}^{n} F_i$.
On souhaite montrer qu'il existe i tel que $F_i = E$.

1. Soient $x, y \in E$. En considérant les $n+1$ vecteurs $x, x+y, x+2y, ..., x+ny$, montrer qu'il existe i tel que $x \in F_i$ et $y \in F_i$. (principe des tiroirs).
2. Supposons $F_1 \neq E$. On se fixe $x \in E \backslash F_1$.
   A l'aide de la question précédente, montrer que pour tout $y \in E$, $y \in \bigcup_{i=2}^{n} F_i$.
3. Montrer le résultat annoncé.

Exercice 2: Un rang

1. Soit $J_n \in \mathcal{M}_n(\mathbb{R})$ dont tous les coefficients valent 1, hormis les coefficients diagonaux qui valent 0. Montrer que $\det(J_n) = (-1)^{n-1}(n-1)$ (opérations élémentaires)

2. Soit $M = (m_{i,j}) \in \mathcal{M}_n(\mathbb{R})$ telle que $\forall i \neq j$, $m_{i,j} \in \{-1, 1\}$, et $m_{i,i} = 0$.
   Avec la formule du déterminant, montrer que $\det(M) \equiv \det(J_n)[2]$.
   Montrer que, si n est pair, M est inversible, et que, si n est impair, $rg(M) \geq n - 1$.

Exercice 3: Soit $f \in \mathcal{L}(\mathcal{M}_n(K), K)$ telle que $\forall M, N \in \mathcal{M}_n(K)$, $f(MN) = f(NM)$.
Montrer qu'il existe $\lambda \in K$ tel que $f = \lambda \cdot Tr$ (Utiliser les matrices élémentaires $E_{i,j}$, et rappeler ce que vaut $E_{i,j}E_{k,l}$)

Exercice 4: Très important. A connaître.
Soient $A, B \in \mathcal{M}_n(\mathbb{R})$. On suppose que A et B sont semblables dans $\mathcal{M}_n(\mathbb{C})$.
On souhaite montrer que A et B sont semblables dans $\mathcal{M}_n(\mathbb{R})$.
On se donne $P \in GL_n(\mathbb{C})$ telle que $A = PBP^{-1}$.
On écrit $P = Q + iT$ avec $Q, T \in \mathcal{M}_n(\mathbb{R})$.

1. Vérifier que $QB = AQ$, et $TB = AT$, puis que pour tout $z \in \mathbb{C}$, $(Q + zT)B = A(Q + zT)$.
2. Justifier que $f : z \mapsto \det(Q + zT)$ est polynomiale, et n'est pas une constante non nulle.
3. En déduire qu'il existe $z \in \mathbb{R}$ tel que $f(z) \neq 0$, et conclure.

Exercice 5:
Soit E un K-ev de dimension $n \in \mathbb{N}^*$, $p \in \mathbb{N}^*$ et $E_1, ..., E_p$ des sev de E.
On suppose que $\sum_{i=1}^{p} \dim(E_i) > (p-1)n$.
Soit $\Phi : (x_1, ..., x_p) \in E_1 \times ... \times E_p \to (x_2 - x_1, x_3 - x_2, ..., x_p - x_{p-1}) \in E^{p-1}$.

1. Vérifier que Φ est linéaire.
2. Montrer que $\mathcal{K}er(\Phi) \neq \{0_{E_1 \times ... \times E_p}\}$.
3. En déduire que $\bigcap_{i=1}^{p} E_i \neq \{0_E\}$.

Exercice 6: Soit $f : \mathcal{M}_n(K) \to K$ telle que $f(0) = 0$, $f(I_n) \neq 0$ et $\forall A, B \in \mathcal{M}_n(k)$, $f(AB) = f(A)f(B)$.
Montrer que si $M \in \mathcal{M}_n(K)$, $f(M) \neq 0$ ssi $M \in GL_n(K)$.
ind : On pourra justifier qu'une matrice non inversible est équivalente à une matrice nilpotente.

Exercice 7:
$n \in \mathbb{N}$, $n \geq 3$. Dans toute la suite E désigne un ensemble de n points distincts du plan.

On appelle droite déterminée par E toute droite passant par deux points distincts de E.

1. Quel est le nombre maximal (en fonction de n) de droites déterminées par E?

   Que doit vérifier E pour qu'il détermine ce nombre de droites?
2. Mêmes questions qu'en 1 avec minimal au lieu de maximal.
3. Donner un exemple d'ensemble E non inclus dans une droite déterminant exactement n droites.

4. On suppose maintenant que E n'est pas inclus dans une droite. On veut montrer que E détermine au moins n droites.

   On note $x_1, ..., x_n$ les éléments de E. Notons p le nombre de droites déterminées par E, $D_1, ..., D_p$ ces droites.

   On définit la matrice d'incidence $A = (a_{i,j})_{\substack{1\leq i\leq n\\1\leq j\leq p}} \in \mathcal{M}_{n,p}(\mathbb{R})$ par $a_{i,j} = \begin{cases} 1 \text{ si } x_i \in D_j \\ 0 \text{ si } x_i \notin D_j \end{cases}$.

   (a) Vérifier que $B = A({}^tA)$ est bien définie et donner sa taille.
   Montrer que $B = \begin{pmatrix} d_1 & 1 & \dots & \dots & 1 \\ 1 & d_2 & 1 & \dots & 1 \\ & & \vdots & & \\ 1 & \dots & \dots & 1 & d_n \end{pmatrix}$. ($d_1, ..., d_n$ sur la diagonale et 1 ailleurs) où $\forall i$, $d_i \geq 2$.

   (b) Si $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ et $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$, on définit le produit scalaire de X et Y par $< X, Y >= x_1y_1 + x_2y_2 + ... + x_ny_n$.

   Que vaut $< X, Y >$ si $X = 0_{\mathbb{R}^n}$?

   Montrer que $< BX, X >= (x_1 + ... + x_n)^2 + (d_1 - 1)x_1^2 + ... + (d_n - 1)x_n^2$. En déduire que B est inversible.

   (c) Retrouver que B est inversible en utilisant des opérations élémentaires.

   (d) Montrer que $n \leq p$.

Exercice 8:
Si $n \in \mathbb{N}^*$ on note S_n l'ensemble des permutations de $[\![1, n]\!]$ ie l'ensemble des bijections de $[\![1, n]\!]$ dans lui-même.
Si $f \in S_n$ et $x \in [\![1, n]\!]$, on dira que x est un point fixe de f ssi $f(x) = x$.
On notera u_n le nombre de $f \in S_n$ n'ayant aucun point fixe. On convient que $u_0 = 1$.

1. une formule d'inversion.

   On définit $\Phi : \mathbb{R}_n[X] \to \mathbb{R}_n[X]$ et $\Psi : \mathbb{R}_n[X] \to \mathbb{R}_n[X]$ par: $\Phi(P) = P(X + 1)$ et $\Psi(P) = P(X - 1)$.

   (a) Vérifier que Ψ et Φ sont linéaires.

   (b) Calculer $M_{B_n}(\Psi)$ et $M_{B_n}(\Phi)$, où $B_n = (1, X, X^2, ..., X^n)$.

   (c) Montrer que $\begin{pmatrix} C_0^0 & C_1^0 & C_2^0 & \dots & C_n^0 \\ 0 & C_1^1 & C_2^1 & \dots & C_n^1 \\ 0 & 0 & C_2^2 & & \vdots \\ 0 & \dots & & \ddots & C_n^{n-1} \\ 0 & \dots & \dots & 0 & C_n^n \end{pmatrix} \begin{pmatrix} C_0^0 & -C_1^0 & C_2^0 & \dots & (-1)^n C_n^0 \\ 0 & C_1^1 & -C_2^1 & \dots & (-1)^{n-1} C_n^1 \\ 0 & 0 & C_2^2 & & \vdots \\ 0 & \dots & & \ddots & -C_n^{n-1} \\ 0 & \dots & \dots & 0 & C_n^n \end{pmatrix} = I_{n+1}$.
   (la première matrice a pour coefficient sur la i-ème ligne et la j-ième colonne C_{j-1}^{i-1} si $j \geq i$ et 0 sinon, et la seconde $(-1)^{j-i}C_{j-1}^{i-1}$ si $j \geq i$ et 0 sinon)

2. Quel est le cardinal de S_n?

3. Exprimer le nombre de $f \in S_k$ ayant exactement $i \in [\![0, k]\!]$ points fixes en fonction de $u_0, u_1, u_2, ...$
   Montrer que, si $k \in \mathbb{N}$, on a (E_k) : $k! = C_k^k u_k + C_k^{k-1} u_{k-1} + C_k^{k-2} u_{k-2} + ... + C_k^0 u_0$.

4. Ecrire le système formé par $(E_n), (E_{n-1}), ..., (E_0)$ et en déduire que:

$$u_n = C_n^n n! - C_n^{n-1}(n-1)! + C_n^{n-2}(n-2)! - ... + (-1)^n C_n^0 0!$$

.

5. Soit a_n le nombre de $f \in S_n$ ayant exactement 1 point fixe.
   Montrer que $a_n = C_n^1 u_{n-1} = n! \sum_{i=0}^{n-1} \frac{(-1)^i}{i!}$.

6. Equivalent de a_n quand $n \to +\infty$?

Exercice 9: Formule de Pick (optionnel)

Tous les polygones et triangles sont supposés non plats.
On se place dans $\mathbb{R}^2$. $a = (x, y) \in \mathbb{R}^2$ est dit entier si et seulement si $x, y \in \mathbb{Z}$.
Si P est un polygone "plein", ∂P désigne la frontière de P ie le polygone formé d'une union finie de segments délimitant P, et $\mathring{P}$ désigne l'intérieur de P, ie $\mathring{P} = P \backslash \partial P$
La (célèbre) formule de Pick est le résultat suivant:
Soit P un polygone dont les sommets sont entiers. Alors $aire(P) = \text{card}(\mathring{P} \cap \mathbb{Z}^2) + \frac{1}{2}\text{card}(\partial P \cap \mathbb{Z}^2) - 1$.

1. Triangles "fondamentaux".
   Soient $a = (x_a, y_a), b = (x_b, y_b) \in \mathbb{Z}^2$. T est le triangle plein $((0,0)\ a\ b)$ et P le parallélogramme plein $((0,0)\ a\ a+b\ b)$. (faire un dessin)

   (a) Montrer que si $\mathring{P}$ contient un point entier alors $\mathring{T}$ aussi (utiliser $\frac{a+b}{2}$).
   On suppose désormais que les seuls points entiers de T sont $0, a, b$.

   (b) Justifier que les seuls points entiers de P sont $0, a, b, a+b$.

   (c) Si $(x, y) \in \mathbb{Z}^2$, montrer qu'il existe $m, n \in \mathbb{Z}$ tels que $(x, y) = ma + nb$ (utiliser des divisions euclidiennes).
   En notant $M = \begin{pmatrix} x_a & x_b \\ y_a & y_b \end{pmatrix}$, en déduire que $M\mathbb{Z}^2 = \mathbb{Z}^2$.
   Ainsi $(GL_2(\mathbb{Z}))$, $\det(M) = \pm 1$. De plus $|\det(M)|$ est l'aire de P, donc $aire(P) = 1$.

   (d) Plus généralement, si T est un triangle (plein) à sommets entiers, dont les seuls points entiers sont les sommets, établir que $aire(T) = 1$

2. Soit $T = (abc)$ un triangle à sommets entiers. Si T contient un point entier autre que a, b, c, justifier que T se découpe en deux ou trois triangles à sommets entiers, contenant tous strictement moins de points entiers que T.

3. Établir la formule de Pick dans le cas d'un triangle.

4. Comment procéder dans le cas d'un polygone?

Exercice 10: matrices nilpotentes (optionnel)

Soit $A \in \mathcal{M}_n(K)$ telle qu'il existe $p \in \mathbb{N}$ tel que $A^p = 0$ (on dit que A est nilpotente).
Montrer que A est semblable à une certaine matrice triangulaire supérieure à diagonale nulle.
Conseillé: Récurrence. On commencera par se donner une base $(e_1, ..., e_n)$ de K^n telle que $e_1 \in ker(A)$.

Exercice 11: Idéaux de $\mathcal{M}_n(K)$ (optionnel)

Une partie I de $\mathcal{M}_n(K)$ est dite :

• idéal à gauche de $\mathcal{M}_n(K)$ si et seulement si I est un sev de $\mathcal{M}_n(K)$ et $\forall A \in \mathcal{M}_n(K)$, $\forall B \in I$, $AB \in I$.

• idéal à droite de $\mathcal{M}_n(K)$ si et seulement si I est un sev de $\mathcal{M}_n(K)$ et $\forall A \in \mathcal{M}_n(K)$, $\forall B \in I$, $BA \in I$.

• idéal bilatère de $\mathcal{M}_n(K)$ si et seulement si I est un sev de $\mathcal{M}_n(K)$ et $\forall A \in \mathcal{M}_n(K)$, $\forall B \in I$, $BA \in I$ et $AB \in I$ (ie I idéal à gauche et à droite).

Idéaux bilatères
Soit I un idéal bilatère de $\mathcal{M}_n(K)$. On se propose de montrer que $I = \mathcal{M}_n(K)$ ou $I = \{0\}$.
On suppose $I \neq \{0\}$. On veut donc montrer que $I = \mathcal{M}_n(K)$.

1. Si I contient une matrice inversible, montrer que $I = \mathcal{M}_n(K)$.
2. Soit $A \in I$ de rang r. Montrer que toutes les matrices de rang r sont dans I.
3. Montrer que I contient une matrice de rang 1.
4. Montrer que $I = \mathcal{M}_n(K)$.

Idéaux à gauches
Si V est un sev de K^n, on pose $K_V = \{M \in \mathcal{M}_n(K) \mid V \subset Ker(M)\}$.

5. Montrer que si V est un sev de K^n, K_V est un idéal à gauche de $\mathcal{M}_n(K)$.

On se propose maintenant de montrer qu'en fait tout idéal à gauche est du type K_V pour un certain V. On se donne maintenant I un idéal à gauche de $\mathcal{M}_n(K)$.

6. Justifier l'existence de $d = \min\{\dim(Ker(A)) \mid A \in I\}$.
   On se fixe $A \in I$ tel que $\dim(Ker(A)) = d$, et on pose $V = Ker(A)$.

7. En utilisant le théorème de factorisation, montrer que $K_V \subset I$.
8. Soit $B \in I$. Supposons que V n'est pas inclus dans $Ker(B)$. On pose $W = Ker(B) \cap V$.
   (a) Justifier que $\dim(W) < d$.
   (b) Justifier qu'il existe $T \in \mathcal{M}_n(K)$ telle que $Ker(T) = W$.
   On se fixe T ainsi.
   On définit la matrice par bloc $M = \begin{pmatrix} A \\ B \end{pmatrix} \in \mathcal{M}_{2n,n}(K)$.
   (c) Montrer que $Ker(M) = W$.
   (d) Montrer qu'il existe $U, V \in \mathcal{M}_n(K)$ telles que $UA + VB = T$.
   (e) Trouver une contradiction.
9. Conclure

Idéaux à droite
Si V est un sev de K^n, on pose $J_V = \{M \in \mathcal{M}_n(K) \mid Im(M) \subset V\}$.

10. Montrer que Si V est un sev de K^n, J_V est un idéal à droite de $\mathcal{M}_n(K)$.

On se propose maintenant de montrer qu'en fait tout idéal à droite est du type J_V pour un certain V.

On se donne I un idéal à droite de $\mathcal{M}_n(K)$.

11. Justifier l'existence de $d = \max\{rg(A) \mid A \in I\}$.
    On se fixe $A \in I$ tel que $rg(A) = d$. Soit $V = Im(A)$.

12. Montrer que $J_V \subset I$.

13. Soit $B \in I$. Supposons $Im(B)$ non inclus dans V. On pose $W = Im(B) + V$.

    (a) Justifier que $\dim(W) > d$.

    (b) Justifier qu'il existe $T \in \mathcal{M}_n(K)$ telle que $Im(T) = W$.
    On se fixe une telle matrice T.
    On définit la matrice par bloc $M = (\,A|B\,) \in \mathcal{M}_{n,2n}(K)$.

    (c) Montrer que $Im(M) = W$.

    (d) Montrer qu'il existe $U, V \in \mathcal{M}_n(K)$ telles que $AU + BV = T$.

    (e) Trouver une contradiction

14. Conclure

Exercice 12: Dimension d'un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ formé de matrices de rangs $\leq r$. (optionnel)

On rappelle que si $A \in \mathcal{M}_r(\mathbb{R})$, $B \in \mathcal{M}_{r,n-r}(\mathbb{R})$, $C \in \mathcal{M}_{n-r,r}(\mathbb{R})$, $D \in \mathcal{M}_{n-r}(\mathbb{R})$, $X \in \mathcal{M}_{r,1}(\mathbb{R})$,

et $Y \in \mathcal{M}_{n-r,1}(\mathbb{R})$, alors $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} AX+BY \\ CX+DY \end{pmatrix}$. (produit par blocs)

On fera attention aux tailles des matrices. Partout, ${}^tAA$ est $({}^tA)(A)$ (et non ${}^t(AA)$).

Si $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R})$ et $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{R})$, on définit le produit scalaire de X et Y par $< X, Y >= \sum_{k=1}^{n} x_i y_i$.

On notera qu'en assimilant les matrices 1×1 aux scalaires, $< X, Y >= {}^tXY$. (le vérifier)

On se donne V un sev de $\mathcal{M}_n(\mathbb{R})$ constitué de matrices de rangs $\leq r$ ($r \in [\![1, n]\!]$), et on se propose de montrer que $\dim(V) \leq nr$, l'inégalité étant optimale.

1. Résultats préliminaires.

   (a) i. Si $X \in \mathcal{M}_{n,1}(\mathbb{R})$, vérifier que $< X, X >= 0 \iff X = 0$.
   ii. Si $A, B \in \mathcal{M}_n(\mathbb{R})$ et $X, Y \in \mathcal{M}_{n,1}(\mathbb{R})$, vérifier que $< AX, BY >=< X, {}^tABY >$.
   iii. Soit $M \in \mathcal{M}_n(\mathbb{R})$.
   Montrer que $\mathcal{K}er(M) = \mathcal{K}er({}^tMM)$ et que $rg(M) = rg({}^tMM)$. (pour une inclusion des noyaux utiliser $< MX, MX >$).

   (b) Soient $B \in \mathcal{M}_{r,n-r}(\mathbb{R})$, $C \in \mathcal{M}_{n-r,r}(\mathbb{R})$, $D \in \mathcal{M}_{n-r}(\mathbb{R})$ et $M = \begin{pmatrix} I_r & B \\ C & D \end{pmatrix}$.

   On veut montrer que $rg(M) \geq r$ avec égalité ssi $D = CB$.

   i. Justifier l'inégalité.

ii. Soient $X \in \mathcal{M}_{r,1}(\mathbb{R})$, $Y \in \mathcal{M}_{n-r,1}(\mathbb{R})$ et $Z = \begin{pmatrix} X \\ Y \end{pmatrix}$.

Ecrire les relations entre B, C, D, X, Y caractérisant le fait que Z soit dans le noyau de M.

iii. Vérifier que $f : \begin{cases} \mathcal{K}er(D - CB) \to \mathcal{M}_{n,1}(\mathbb{R}) \\ Y \mapsto \begin{pmatrix} -BY \\ Y \end{pmatrix} \end{cases}$ est une application linéaire injective et que $Im(f) = \mathcal{K}er(M)$.

iv. Regardant $\dim(\mathcal{K}er(D - CB))$, montrer que $rg(M) = r$ ssi $D = CB$.

2. On suppose pour l'instant que V contient $J_{n,n,r} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

(a) Soit $W = \left\{ \begin{pmatrix} 0 & B \\ {}^tB & A \end{pmatrix} \mid A \in \mathcal{M}_{n-r}(\mathbb{R}) \text{ et } B \in \mathcal{M}_{r,n-r}(\mathbb{R}) \right\}$.

Montrer que W est un sev de $\mathcal{M}_n(\mathbb{R})$ de dimension $n(n-r)$.

(b) Si $\begin{pmatrix} 0 & B \\ {}^tB & A \end{pmatrix} \in W \cap V$, montrer que $\forall \lambda \in \mathbb{R}$, $\lambda A = \lambda^2({}^tBB)$ puis que $A = B = 0$.

(c) Que dire de la somme $V + W$? Montrer que $\dim(V) \leq nr$.

3. On ne suppose plus que $J_{n,n,r} \in V$ mais que V contient une matrice M de rang r. On se donne $P, Q \in GL_n(\mathbb{R})$ tels que $M = PJ_{n,n,r}Q$.

Utilisant $\Theta : \begin{cases} V \to \mathcal{M}_n(\mathbb{R}) \\ N \mapsto P^{-1}NQ^{-1} \end{cases}$, montrer que $\dim(V) \leq nr$.

4. Si V ne contient pas de matrice de rang r, montrer que l'on a toujours $\dim(V) \leq nr$.

5. Optimalité de la majoration: trouver un sev (simple) de $\mathcal{M}_n(\mathbb{R})$ formé de matrices de rang $\leq r$ et de dimension nr.

Partout, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1 Quelques rappels et compléments

1.1 Rappel des fondamentaux

1.1.1 Les séries à termes positifs

Le point très fondamental est, que si $(a_n) \in \mathbb{R}_+^{\mathbb{N}}$, $\left(\sum_{k=0}^{n} a_k\right)_n$ est croissante, et donc converge si et seulement si elle est majorée.
Vous avez vu les séries de références:

Propriété 1:

1. Si $a \geq 0$, $\sum_n a^n$ converge si et seulement si $a < 1$
2. Séries de Riemann: $\sum_{n\geq 1} \frac{1}{n^\alpha}$ converge si et seulement si $\alpha > 1$.

Le premier point s'obtient par simple calcul, le second par majorations/minorations par des intégrales, outil essentiel.
On utilise par exemple que si f est réelle décroissante, $f(n+1) \leq \int_n^{n+1} f \leq f(n)$, et on somme les inégalités.

Ces séries sont d'usage constant, le premier cas traitant des cas grossiers (convergence rapide), le second des cas plus fins. Vous avez démontré la propriété cruciale:

Propriété 2:

1. Si $(a_n),\ (b_n) \in \mathbb{R}_+^{\mathbb{N}}$ vérifient $a_n \underset{n\to+\infty}{=\!=} O(b_n)$, et que $\sum_n b_n$ converge, alors $\sum_n a_n$ converge.
   Notez que $a_n \sim b_n$ ou $a_n = o(b_n)$ impliquent $a_n \underset{n\to+\infty}{=\!=} O(b_n)$.
2. Si $a_n \geq b_n$ APCR et $\sum_n b_n$ diverge, alors $\sum_n a_n$ diverge.
3. Si $(a_n),\ (b_n) \in \mathbb{R}_+^{\mathbb{N}}$ vérifient $a_n \underset{n\to+\infty}{\sim} b_n$, alors $\sum_n a_n$ et $\sum_n b_n$ ont même nature.
   Rappel: c'est une conséquence du premier point car $a_n \sim b_n \Longrightarrow (a_n = O(b_n)$ et $b_n = O(a_n))$ (pas de réciproque).

   Note importante: le "O" est une comparaison en module. Dans le cas général, non positif, $|a_n| = O(|b_n|)$, $a_n = O(|b_n|)$, $a_n = O(b_n)$ sont équivalents.

Quand $a_n \geq 0$, $\sum_n a_n$ diverge s'abrège souvent $\sum_{n=0}^{+\infty} a_n = +\infty$, car $\sum_{k=0}^{n} a_k \underset{n\to+\infty}{\longrightarrow} +\infty$.

1.1.2 L'absolue convergence

Le résultat très fondamental, dans le cas général est

Propriété 3: Si $(a_n) \in \mathbb{K}^{\mathbb{N}}$, alors $\sum_n |a_n|$ converge$\Longrightarrow \sum_n a_n$ converge.

Ainsi, par exemple, si $a_n = \dfrac{\cos(n)}{n^2+n+2}$, on écrit $|a_n| \sim \dfrac{|\cos(n)|}{n^2} = O(1/n^2)$, $\dfrac{1}{n^2} > 0$ est tg d'une série convergente, donc $\sum_n |a_n|$ converge, donc $\sum_n a_n$ converge.

On commence toujours par une étude de convergence absolue, en simplifiant au maximum en terme d'équivalent.

1.2 Le résultat principal de semi-convergence

Définition 1: Une série $\sum a_n$ est dite semi-convergente si et seulement si $\sum_n a_n$ converge et $\sum_n |a_n|$ diverge.
On ne peut donc traiter une semi-convergence directement par comparaison (O,o,...), ce qui ne veut pas dire qu'à un certain stade on n'utilise pas de comparaison.

Il y a deux outils essentiels, la transformation d'Abel dont nous parlerons en cours, et le théorème des séries alternées.

Propriété 4: Théorème des séries alternées
Soit $(a_n) \in \mathbb{R}^{\mathbb{N}}$ telle que : $\forall n, a_n a_{n+1} < 0$ (alternance de signes), $(|a_n|)_n$ décroît, et $a_n \underset{n\to+\infty}{\longrightarrow} 0$.
Alors

1. $\sum_n a_n$ converge.
2. $R_n := \sum_{k=n+1}^{+\infty} a_k$ est du signe de son premier terme, à savoir a_{n+1}, et $|R_n| \leq |a_{n+1}|$

Le second point est aussi important que le premier, et nous en aurons l'usage.
Il est à noter que si $n \geq p$, $\sum_{k=n}^{p} a_k$ est du signe de a_n et majoré en module par $|a_n|$, car si on remplace a_k par 0 pour $k \geq p+1$, le théorème s'applique toujours.
Comme toujours, on peut se contenter des propriétés APCR, mais alors le deuxième point ne s'applique qu'à partir d'un tel rang.
Notez que le deuxième point s'applique à $\sum_{n=0}^{+\infty} a_n = R-1$. La somme totale est aussi le premier reste.
Ainsi $\sum_{n=0}^{+\infty} a_n$ est du signe de a_0, et $\left|\sum_{n=0}^{+\infty} a_n\right| \leq |a_0|$.
Un cas typique d'application est : Si $\alpha > 0$, $\sum_{n\geq 1} \dfrac{(-1)^n}{n^\alpha}$ converge.
Dans ce cas, si $\alpha > 1$, le TSA est inutile, on peut procéder par comparaison, et il y a convergence absolue.

1.3 L'usage de DLs

Contentons nous d'un exemple: prenons $a_n = \ln\left(1 + \dfrac{(-1)^n}{\sqrt{n}} + \dfrac{1}{n}\right)$.
$|a_n| \sim \dfrac{1}{\sqrt{n}}$ tg d'une série divergente, donc $\sum_n |a_n|$ diverge.
$a_n \sim \dfrac{(-1)^n}{\sqrt{n}}$, tg d'une série convergente par CSA, mais les résultats de comparaison ne s'appliquent qu'en

comparant à une série à termes positifs, donc cela ne donne rien.
Faisons un DL : $a_n \underset{n\to+\infty}{=} \underbrace{\frac{(-1)^n}{\sqrt{n}}}_{b_n} + \underbrace{\frac{1}{2n}}_{c_n} + \underbrace{O\left(\frac{1}{n^{3/2}}\right)}_{d_n}$.
$\sum b_n$ converge par TSA, $\sum c_n$ diverge, et $\sum d_n$ converge absolument par comparaison, donc $\sum_n a_n$ diverge.

A propos de DLs, si $a_n \sim b_n$, et qu'on a un calcul précis à faire, ceci se réécrit $a_n = b_n + o(b_n)$ (ou $b_n = a_n + o(a_n)$)

1.4 L'art de regrouper les termes

Si (a_n) est une suite notons $Sa_n = \sum_{k=0}^{n} a_k$ ses sommes partielles.

Pour étudier $a_0 + a_1 + a_2 + ...$, on peut songer à étudier $\sum_n b_n$, les b_n étant définis selon le schéma:
$\underbrace{a_0 + ... + a_{n_1}}_{b_0} + \underbrace{a_{n_1+1} + ... + a_{n_2}}_{b_1} + \underbrace{a_{n_2+1} + ... + a_{n_3}}_{b_2} + ...$ avec $n_1 < n_2 < n_3 < ....$

Plus formellement, on considère $\phi : \mathbb{N} \to \mathbb{N}$ strictement croissante, et on pose $b_n = \sum_{k=\phi(n)}^{\phi(n+1)-1} a_k$.

Ainsi $Sb_n = Sa_{\phi(n+1)-1}$.
De ce fait, $\sum_n a_n$ converge $\implies \sum_n b_n$ converge, et donc $\sum_n b_n$ diverge $\implies \sum_n a_n$ diverge.
Mais la réciproque est fausse. Un exemple trivial:
$\sum_n (-1)^n$ diverge grossièrement. Mais $a_0 + a_1 + ... = \underbrace{1-1}_{b_0=0} + \underbrace{1-1}_{b_1=0} + ...$ et $\sum_n b_n$ converge.
Si on montre que $\sum_n b_n$ converge, on a en fait montré que $(Sa_{\phi(n+1)-1})_n$ converge, et il faut regarder ce qui se passe entre $Sa_{\phi(n+1)-1}$ et $Sa_{\phi(n+2)-1}$ (ie les Sa_k, $k = \phi(n+1), ..., \phi(n+2)-2$), quand $n \to +\infty$.

Vous vous convaincrez facilement que, par exemple, si le nombre de termes constituant b_n est fixe, ou simplement majoré, et que $a_n \to 0$, on a bien la réciproque $\sum_n b_n$ converge $\implies \sum a_n$ converge.

$\sum_n \frac{(-1)^n}{n}$ converge par TSA, mais la convergence peut aussi se voir en regroupant les termes par deux car $\frac{1}{2k} - \frac{1}{2k+1} \underset{k\to+\infty}{\sim} \frac{1}{4k^2}$.

1.5 Les permutations de termes

Nous en parlerons (familles sommables), mais dans le cas général, si $\sigma : \mathbb{N} \to \mathbb{N}$ est bijective, il n'y a pas de rapport entre $\sum_k a_k$ et $\sum_k a_{\sigma(k)}$. (Nous verrons que si $a_k \geq 0$, si).
Voir l'exercice 2.

1.6 Les produits infinis

Pour étudier $p_n = \prod_{k=0}^{n} a_k$ quand $n \to +\infty$, on utilise ln.
Mais avant : on se demande s'il existe un k tel que $a_k = 0$, auquel cas (p_n) stationne en 0.
Sinon, on écrit $a_k = (-1)^{s_k} b_k$ avec $b_k > 0$.

Alors $p_n = (-1)^{s_0+\ldots+s_n} \prod_{k=0}^{n} b_k$.

$\prod_{k=0}^{n} b_k$ s'étudie en passant au logarithme, ce qui ramène à une série: $\ln\left(\prod_{k=0}^{n} b_k\right) = \sum_{k=0}^{n} \ln(b_k)$.

1.7 La transformation suite/série

Il s'agit simplement d'écrire $a_n = a_0 + \sum_{k=0}^{n-1}(a_{k+1} - a_k)$, ce qui a pour conséquence que (a_n) converge si et seulement si $\sum_n (a_{n+1} - a_n)$ converge.

A propos des sommes télescopiques, il peut aussi être utile, si (a_n) converge vers x, d'écrire $x - a_n = \sum_{k=n}^{+\infty}(a_{k+1} - a_k)$ afin de préciser le comportement (équivalent notamment) de $x - a_n$ quand $n \to +\infty$ (sera vu en cours).

2 Exercices

Exercice 1: $\alpha > 0$. Étudier l'existence de $\lim_{n\to+\infty} \prod_{k=2}^{n}\left(1 - \frac{1}{k^\alpha}\right)$. (plusieurs cas. la limite est calculable dans certains cas)

Exercice 2:

1. Développement asymptotique des sommes harmoniques.
   On pose et $H_n = \sum_{k=1}^{n} \frac{1}{k}$
   (a) Encadrer H_n par des intégrales, qui se calculent, et en déduire $H_n \underset{n\to+\infty}{\sim} \ln(n)$.
   Ainsi $H_n \underset{n\to+\infty}{=} \ln(n) + o(\ln(n))$.
   On va pousser le développement.
   (b) On pose $a_n = H_n - \ln(n)$. Simplifier $a_{n+1} - a_n$, en calculer un équivalent, et en déduire que (a_n) converge.

   On note $\gamma = \lim_{n\to+\infty} a_n$ (constante d'Euler).
   $a_n \to \gamma$ se réécrit $a_n = \gamma + o(1)$ ($o(1) = 1 \times \varepsilon_n$, avec $\varepsilon_n \to 0$), et donc $H_n \underset{n\to+\infty}{=} \ln(n) + \gamma + o(1)$.
2. Une permutation de termes
   (a) Calcul de $\sum_{n=1}^{+\infty} \frac{(-1)^n}{n}$. (la série converge par TSA)
   On note $S_n = \sum_{k=1}^{n} \frac{(-1)^k}{k}$.
   On remarque que $\sum_{\substack{1\le k\le 2n \\ k \text{ pair}}} \frac{1}{k} = \sum_{k=1}^{n} \frac{1}{2k} = \frac{1}{2} H_n$.
   Exprimer S_{2n} avec des H_k, et montrer que $\sum_{n=1}^{+\infty} \frac{(-1)^n}{n} = -\ln(2)$

(b) Changement de l'ordre de sommation. Au lieu de faire $-1+\frac{1}{2}-\frac{1}{3}+\frac{1}{4}-...$, on considère maintenant: $-1-\frac{1}{3}+\frac{1}{2}-\frac{1}{5}-\frac{1}{7}+\frac{1}{4}-...$ (dans l'ordre, deux négatifs, un positif, répétés)
On note W_n les sommes partielles de cette nouvelle série, n commençant à 1.
Exprimer W_{3n} avec des H_k, et calculer $a=\lim_{n\to+\infty} W_{3n}$. On notera que $a\neq-\ln(2)$.
Justifier que $W_n \xrightarrow[n\to+\infty]{} a$.

Exercice 3: étude asymptotique d'une suite récurrente
On rappelle le théorème de Cesaro:
Si $a_n \xrightarrow[n\to+\infty]{} x$, alors $\frac{a_0+...+a_{n-1}}{n}\to x$.
Notez une certaine souplesse. Ainsi $\frac{a_0+...+a_n}{n}\to x$ également par exemple puisque $\frac{n+1}{n}\to 1$.
C'est un cas particulier d'un résultat que nous verrons sur les séries.

La suite (x_n) vérifie $x_0\in]0,1[$ et $\forall n\in\mathbb{N}$, $x_{n+1}=x_n-x_n^2$.

1. Montrer que $\forall n\in\mathbb{N}$, $x_n\in]0,1[$ et que $x_n \xrightarrow[n\to+\infty]{} 0$.
2. Montrer que $\frac{1}{x_{n+1}}-\frac{1}{x_n} \xrightarrow[n\to+\infty]{}$. En utilisant le théorème de Cesaro, montrer que $x_n \underset{n\to+\infty}{\sim} \frac{1}{n}$.
3. Montrer que $\frac{1}{x_{n+1}}-\frac{1}{x_n}=1+\frac{1}{n}+o\left(\frac{1}{n}\right)$.
4. Montrer que $\frac{1}{x_n}-n \underset{n\to+\infty}{\sim} \ln(n)$. (plus difficile. Aisé avec un résultat que nous verrons en cours. Si vous n'y arrivez pas, pas grave. Utiliser l'exercice 2, partie 1)
5. Montrer que $x_n \underset{n\to+\infty}{=} \frac{1}{n}-\frac{\ln(n)}{n^2}+o\left(\frac{\ln(n)}{n^2}\right)$. (on partira de la question précédente qui se réécrit $\frac{1}{x_n}=n+\ln(n)+o(\ln(n))$).

Exercice 4: Soient $a,b\in\mathbb{R}$ avec $|a|<1$. (u_n) vérifie $u_0\in\mathbb{R}$ et $\forall n,\ u_{n+1}=a\sin(u_n)+b$.
Montrer que $|u_{p+1}-u_p|\leq|a|^p|u_1-u_0|$. En déduire que (u_n) converge.

Exercice 5:

1. Montrer qu'il existe $c>0$ tel que $\forall x\in\mathbb{R}$, $|\sin(x)|+|\sin(x+1)|\geq c$.
2. En regroupant les termes par deux et en minorant, montrer que $\sum_{n\geq1}\frac{|\sin(n)|}{n}$ diverge.

   Nous verrons avec la transformation d'Abel que $\sum_{n\geq1}\frac{\sin(n)}{n}$ converge.

Exercice 6:
On s'intéresse à la convergence de $\sum_{n\geq1}\frac{\cos(\ln n)}{n}$.
Les techniques habituelles ne s'appliquent pas à cette série.
On va procéder par comparaison avec une intégrale, mais pas en encadrant car $t\mapsto\frac{\cos(\ln t)}{t}$ n'a aucune monotonie.

1. Soit $f \in \mathcal{C}^1([1,+\infty[)$ telle que la suite $\left(\int_1^n |f'|\right)_{n\geq 1}$ soit majorée (ce qui revient à convergente car la suite est croissante).
   On note $a_n = \int_n^{n+1} |f'|$.
   (a) Montrer que $\sum_{n\geq 1} a_n$ converge.
   (b) $n \in \mathbb{N}^*$. Si $x \in [n, n+1]$, établir $|f(x) - f(n)| \leq a_n$, puis $\left|f(n) - \int_n^{n+1} f\right| \leq a_n$.
   (c) En déduire que $\sum_n f(n)$ converge si et seulement si la suite $\left(\int_1^n f\right)_{n\geq 1}$ converge. (on utilisera $\int_1^n f - \sum_{k=1}^n f(k)$)
   On pose désormais $f(t) = \dfrac{\cos(\ln t)}{t}$.
2. Vérifier que si $t \geq 1$, $|f'(t)| \leq \dfrac{2}{t^2}$, et en déduire que $\left(\int_1^n |f'|\right)_{n\geq 1}$ est majorée.
3. En déduire la nature de $\sum_{n\geq 1} \dfrac{\cos(\ln n)}{n}$.
   Remarque: avec le même résultat (Q.1), on peut montrer par exemple que $\sum_{n\geq 1} \dfrac{\cos(\sqrt{n})}{n}$ converge.
   Mais la convergence de $\left(\int_1^n \dfrac{\cos(\sqrt{t})}{t} dt\right)_{n\geq 1}$ nécessite des résultats qui seront vus en cours (chapitre "intégrales généralisées")

Exercice 7: Optionnel
On se donne $x \in \mathbb{R}^+$. On définit $(\varepsilon_n) \in \{0,1\}^{\mathbb{N}^*}$ par:
$\varepsilon_1 = 1$ si $x \geq 1$, $\varepsilon_1 = 0$ si $x < 1$.
Si $n \geq 2$, $\varepsilon_n = 1$ si $x \geq \dfrac{1}{n} + \sum_{k=1}^{n-1} \dfrac{\varepsilon_k}{k}$ et $\varepsilon_n = 0$ sinon.

1. Montrer qu'il existe une infinité de n tels que $\varepsilon_n = 0$.
2. Montrer que $\sum_{n\in\mathbb{N}^*} \dfrac{\varepsilon_n}{n}$ converge et que $\sum_{n\in\mathbb{N}^*} \dfrac{\varepsilon_n}{n} = x$
3. Y-a-t-il une unique suite $(\varepsilon_n) \in \{0,1\}^{\mathbb{N}^*}$ telle que $x = \sum_{n\in\mathbb{N}^*} \dfrac{\varepsilon_n}{n}$?

Exercice 8: Optionnel
Une étude de convergence par regroupement de termes.
On s'intéresse à la convergence de $\sum \dfrac{(-1)^{E(\sqrt{n})}}{n}$.
On pose $a_n = \sum_{k=n^2}^{(n+1)^2-1} \dfrac{1}{k}$.

1. A l'aide d'un encadrement intégral de a_n, montrer que (a_n) est décroissante à partir d'un certain rang et que $a_n \to 0$.

2. Montrer que $\sum_{n\geq 1}(-1)^n a_n$ converge, puis que $\sum \frac{(-1)^{E(\sqrt{n})}}{n}$ converge.

Exercice 9: Optionnel

1. Soit $(a_k)_{k\geq 2}$ une suite telle que $a_k \in \{0, 1, ..., k-1\}$ et $S = \sum_{k=2}^{+\infty} \frac{a_k}{k!}$.

   (a) Justifier l'existence de S.

   (b) Calculer $\sum_{k=n}^{+\infty} \frac{k-1}{k!}$. Montrer que $\sum_{k=n}^{+\infty} \frac{a_k}{k!} = O(1/(n-1)!)$.

   (c) Montrer que $2\pi n!S - 2\pi n! \sum_{k=0}^{n+1} \frac{a_k}{k!} \underset{n\to+\infty}{\longrightarrow} 0$ puis que $\sin(2\pi n!S) - \sin\left(2\pi \frac{a_{n+1}}{n+1}\right) \underset{n\to+\infty}{\longrightarrow} 0$.

2. Limite de $\sin(2\pi n!e)$?

3. Etudier la convergence de $\sum_{k\geq 0} \sin(2\pi k!e)$.

4. $x \in [-1, 1]$. Montrer qu'il existe $a \in \mathbb{R}$ tel que $\sin(n!a) \underset{n\to+\infty}{\longrightarrow} x$.