Fonctions et nombres, en plus du TD

1 Sommes presque géométriques

On veut calculer la somme suivante :

$$S_n(x) = \sum_{k=0}^{n} kx^k.$$

Pour cela, on considére la fonction :

$$T_n(x) = \sum_{k=0}^{n} x^k.$$

Montrer que T_n est dérivable sur $\mathbb{R}$ et que pour tout réel x :

$$xT_n'(x) = S_n(x).$$

En partant de la formule de la somme géométrique pour T_n, en déduire que une formule pour $S_n(x)$ pour $x \neq 1$.
Avec une méthode similaire, calculer :

$$\sum_{k=0}^{n} k^2 \left(\frac{1}{2}\right)^k.$$

2 Lemme des pics

Soit (x_n) une suite de nombre réels. Une suite *extraite* de (x_n), ou *sous-suite* de (x_n) est une suite obtenue en ne gardant que certains termes (toujours une infinité) de la suite (x_n). Concrètement, c'est une suite de la forme $(x_{f(n)})$ avec $f : \mathbb{N} \longrightarrow \mathbb{N}$ une application strictement croissante.

1. Considérons la suite définie par $x_n = (-1)^n$. Exhiber deux sous-suites de (x_n) qui sont constantes.
2. Expliquer pourquoi une sous-suite d'une sous-suite de (x_n) est une sous-suite de (x_n).

Le but de l'exercice est de démontrer le lemme des pics, qui dit la chose suivante :

Lemme 1. *(Lemme des pics)*
Toute suite réelle (x_n) possède une sous-suite monotone (c'est à dire soit croissante soit décroissante).

Soit donc (x_n) une suite réelle. On dit qu'un entier n est un pic de la suite (x_n) si toutes les valeurs qui suivent (x_n) sont inférieures ou égales à (x_n), c'est à dire :

$$\forall k \geq n \;\; x_k \leq x_n.$$

3. Supposons que (x_n) possède une infinité de pics. On extrait alors une sous-suite de (x_n) formée de ces pics. Expliquer pourquoi cette suite est décroissante.
4. Supposons que (x_n) possède, au contraire, un nombre fini de pics. Expliquer alors pourquoi (x_n) possède une sous-suite croissante.
5. Conclure que (x_n) possède toujours une sous-suite monotone.

3 Théorème des bornes

Le théorème des bornes est un énoncé qui semble complétement évident, mais qui n'est pas si immédiat que ça à démontrer (on aura besoin du lemme des pics). L'idée est la suivante : étant donnée une fonction *continue* $f : [a,b] \longrightarrow \mathbb{R}$ définie sur le segment $[a,b]$, il s'agit de voir que f est bornée sur $[a,b]$. Cela semble évident : si on trace un graphe de fonction entre a et b à la main, le graphe ne pourra pas aller indéfiniment haut ni indéfiniment bas. Cependant il faut se méfier de ce genre d'arguments car les fonctions continues sont en générales bien plus subtiles que de simples tracés à la main (il est par exemple possible de construire une fonction de $[a,b]$ vers $\mathbb{R}$ dont le graphe est de longueur infinie).
Démontrons donc ce théorème : soit $f : [a,b] \longrightarrow \mathbb{R}$ une fonction continue et montrons qu'elle est majorée (le raisonnement pour obtenir un minorant est bien sûr complétement similaire).
1. Si f n'est pas majorée, construire une suite (x_n) dans $[a,b]$ telle que $f(x_n)$ tend vers l'infini.
2. Par le lemme des pics appliqué à la suite précédente, construire une suite (y_n) monotone dans $[a,b]$ telle que $f(y_n)$ tend vers l'infini.
3. Montrer que (y_n) converge vers un réel ℓ et utiliser la continuité de f pour obtenir que $f(y_n) \longrightarrow f(\ell)$ quand n tend vers l'infini. Aboutir à une contradiction.
On a montré que f est majorée.
On peut aussi montrer que f a un maximum sur $[a,b]$ mais cela demande la notion de borne supérieure que l'on n'a pas encore vue.

4 Infinité des nombres premiers

1. Supposons par l'absurde qu'il y ait seulement un nombre fini de nombres premiers, et notons les $p_1,\dots,p_n$ dans l'ordre croissant. On pose alors $N = p_1 p_2 \dots p_n + 1$. Montrer que N est un nombre premier et aboutir à une contradiction.
2. Supposons par l'absurde qu'il y ait seulement un nombre fini de nombres premiers qui sont congrus à 3 modulo 4 et notons les $p_1,\dots,p_n$ dans l'ordre croissant. On pose alors $N = 2p_1 \dots p_n + 1$. Observer que $N \equiv 3\ [4]$ et que les diviseurs premiers de N sont tous congrus à 1 modulo 4. Aboutir à une contradiction.
Un théorème bien plus général est vrai, mais sa preuve est bien au delà de ce cours.

Théorème 2. *(Progression arithmétique de Dirichlet) Si a et b sont deux entiers premiers entre eux au moins égaux à* 1*, il existe une infinité de nombres premiers congrus à a modulo b.*

Il est même possible de dire quelle "proportion" de nombres premiers vérifient cette congruence : on peut montrer qu'il y a à peu près autant (en un sens à définir) de nombres premiers pour chaque reste a (premier à b) modulo b.

5 Valuations p-adiques et irrationalité

Dans les deux prochains exercices, on présente des méthodes pour prouver l'irrationalité de certains nombres, et c'est l'occasion d'introduire des concepts phares de théorie des nombres.
Soit $n \in \mathbb{N}^*$. Le théorème de décomposition en facteurs premiers permet d'écrire n de façon unique comme produit de facteurs premiers. Par exemple, $60 = 2^2 \times 3 \times 5$. On définit, pour p un nombre premier, la valuation p-adique de n, notée $v_p(n)$, comme l'exposant qui apparaît sur le nombre premier p dans la décomposition de n. Par exemple, $v_2(60) = 2$, $v_3(60) = 1$, $v_5(60) = 1$ et $v_1 1(60) = 0$ puisque 11 ne divise pas 60.
Par convention, on pose aussi $v_p(0) = \infty$ et si $n < 0$, on pose $v_p(n) = v_p(|n|)$. On peut aussi voir $v_p(n)$ comme le plus grand entier k tel que p^k divise n.
1. Calculer $v_5(148)$, $v_2(148)$ et $v_3(-81)$.
2. Donner un entier n tel que $v_5(n) = 2$ et $v_3(n) = 2$.
3. Montrer que pour tous entiers $m, n \in \mathbb{Z}$ non-nuls, on a $v_p(mn) = v_p(m) + v_p(n)$.

4. Soit $x = \frac{a}{b}$ un nombre rationnel non-nul avec a, b deux entiers non-nuls. On pose $v_p(x) = v_p(a) - v_p(b)$. Expliquer pourquoi cela ne dépend que de x et pas de l'écriture $\frac{a}{b}$.
5. Calculer $v_7(40/21)$ et $v_2(15.2)$.
5. Montrer qu'on a encore $v_p(xy) = v_p(x) + v_p(y)$ pour tous rationnels non-nuls x et y.
6. En remarquant qu'une valuation p-adique est toujours un nombre entier, montrer que $\sqrt{2}$ est irrationnel. Indication : si $\sqrt{2}$ était rationnel, on aurait :

$$v_2(2) = v_2(\sqrt{2} \times \sqrt{2}) = 2v_2(\sqrt{2}).$$

7. Avec une méthode similaire, montrer que $5^{1/4}$ est irrationnel.

6 Entiers algébriques et irrationalité

Un polynôme P est dit *unitaire* si son coefficient de plus haut degré est 1. Par exemple, $X^3 + 2X$ est unitaire mais $5X^2 + 1$ ne l'est pas.
Les entiers algébriques sont les nombres complexes z annulés par un polynôme P *unitaire et à coefficients entiers*. Par exemple, les racines du polynôme $X^2 - 2$ sont des entiers algébriques donc $\sqrt{2}$ et $-\sqrt{2}$ sont des entiers algébriques. De même, grâce au polynôme $X^2 + 1$, le nombre imaginaire i est algébrique. On note $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques.
1. Montrer que $2^{1/3}$, $2^{1/10}$ et le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ sont des entiers algébriques et expliquer pourquoi ce ne sont pas des nombres entiers.
2. Montrer que tous les nombres entiers sont des entiers algébriques (par exemple 1 est algébrique car $X - 1$ est un polynôme à coefficients entiers qui annule 1).
3. On va montrer que les entiers algébriques qui sont rationnels sont toujours des nombres entiers, autrement dit :

$$\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Soit donc $z = \frac{p}{q}$ un entier algébrique rationnel, avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ *premiers entre eux*. Puisque z est un entier algébrique, il existe $P(X) = X^n + a_{n+1}X^{n-1} + \cdots + a_1 X + a_0$ un polynôme unitaire à coefficients entiers qui annule z, autrement dit :

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0.$$

Montrer que :

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0.$$

En déduire que $q \mid p^n$ et que $q = 1$ (on rappelle que p et q sont supposés premiers entre eux). Conclure que $z \in \mathbb{Z}$.
4. En déduire que $\sqrt{2}$, φ, $2^{1/10}$ et $\sqrt{7}$ sont irrationnels.

Il s'agit d'un outil très puissant pour montrer qu'un nombre est irrationnel, malheureusement ça ne marche pas avec tous les nombres (par exemple π).
Il est possible de démontrer que $\overline{\mathbb{Z}}$ est un *anneau*, c'est à dire qu'il est stable par somme, par le fait de prendre l'opposé, par produit et qu'il contient 0 et 1, mais c'est loin d'être évident avec les outils dont on dispose pour le moment.

7 Un théorème de point fixe en analyse

1. Soit $f : [0,1] \longrightarrow [0,1]$ une fonction continue. Montrer que f possède un point fixe, c'est à dire un $a \in [0,1]$ tel que $f(a) = a$. On pourra utiliser le théorème des valeurs intermédiaires appliqué à une fonction bien choisie.
2. Construire une fonction non continue de $[0,1]$ dans $[0,1]$ sans point fixe.

8 Un théorème de point fixe en arithmétique

Soit p un nombre premier, X un ensemble et $f : X \longrightarrow X$ une application telle que :

$$f \circ \cdots \circ f(x) = x$$

pour tout $x \in X$ avec p itérations de f. On note $f^0(x) = x$, $f^1(x) = f(x)$, $f^2(x) = f \circ f(x)$, etc. Ainsi, on peut reformuler cette hypothèse en :

$$f^p(x) = x.$$

1. Montrer que f est une bijection.
Ceci permet de considérer aussi l'application inverse notée f^{-1} et ses itérées f^{-1}, f^{-2}, f^{-3}, etc. On a donc des fonctions f^n pour tout $n \in \mathbb{Z}$.
2. Expliquer pourquoi $f^m \circ f^n = f^{m+n}$ pour tous $m, n \in \mathbb{Z}$. 3. Soit $x \in X$. Supposons qu'il existe un entier k tel que $1 \leq k < p$ et $f^k(x) = x$. Montrer qu'il existe $u, v \in \mathbb{Z}$ tels que $1 = uk + vp$ et en déduire que :

$$f(x) = f^{uk+vp}(x) = x.$$

4. Pour tout $x \in X$, on considère l'orbite de x, notée O_x, qui est l'ensemble formé des images successives de x par f :

$$O_x = \{x, f(x), f(f(x)), f(f(f(x))), \dots\}.$$

Montrer que $|O_x| \leq p$, où $|A|$ désigne le cardinal d'un ensemble A.
5. Montrer qu'en fait $|O_x|$ vaut soit 1 soit p : autrement dit soit x est un point fixe soit son orbite est de taille p (utiliser 3).
6. Expliquer pourquoi, si x est dans l'orbite de y, alors y est dans l'orbite de x. On regroupe alors les éléments de x par orbites. On note F l'ensemble des points fixes de f, c'est à dire des éléments seuls dans leur orbite. En utilisant 5, déduire de cette répartition en orbites la congruence suivante modulo p :

$$|X| \equiv |F| \ [p].$$

7. En déduire que si $|X|$ n'est pas divisible par p, alors f possède au moins un point fixe.