# Super-Math-Quizz
## à l'usage des petits génies

### I. Hyper-méga-triv'...

**I1.** On se donne $n$ points $A_1, \dots, A_n$ d'un espace euclidien. On demande à quelle condition nécessaire et suffisante la composée

$$\sigma_{A_n} \circ \sigma_{A_{n-1}} \circ \cdots \circ \sigma_{A_1}$$

des symétries de centres $A_1, \dots, A_n$, est l'identité.

**I2.** Soient $A$ et $A'$ deux points du plan euclidien. Donné un point $M$, on appelle $P$ et $P'$ les images de $M$ par des rotations de centres respectifs $A$ et $A'$ et d'angles respectifs $\frac{\pi}{2}$ et $-\frac{\pi}{2}$, $I$ le milieu de $[PP']$. Montrer que $I$ ne dépend pas de $M$.

**I3.** Donnée l'écriture en base 3 d'un entier, comment déterminer, de la manière la plus simple possible, s'il est pair ou impair ?

**I4.** Montrer que tout entier $n$ s'écrit d'une infinité de façons comme

$$\pm 1^2 \pm 2^2 \pm 3^2 \pm \cdots \pm k^2$$

pour un certain $k$ et un certain choix des signes.

**I5.** Montrer qu'un polyèdre quelconque a toujours deux faces ayant le même nombre de côtés.

**I6.** Montrer que l'équation $e^x = x + 3$ admet une solution réelle. (Oui, oui, c'est ridicule, mais cet exercice m'a été posé en khôlle !)

### II. Divers...

**II1.** Trouver un polynôme $P \in \mathbb{R}[X, Y]$ à deux variables et à coefficients réels dont la fonction associée a pour image exactement $\mathbb{R}_+^*$.

**II2.** On suppose donnée une famille finie $(x_i)_{i \in I}$ de nombres réels telle que pour tout $i \in I$ il existe une partition de $I \setminus \{i\}$ en deux ensembles, $I_+$ et $I_-$ tels que

$$\sum_{i \in I_+} x_i = \sum_{i \in I_-} x_i$$

Montrer alors que les $x_i$ sont tous égaux.

**II3.** Montrer que la somme

$$S_n = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

n'est un entier pour aucun $n$.

**II4.** Montrer qu'un espace vectoriel $E$ sur un corps $K$ est l'union de $n+1$ sous-espaces propres si et seulement si $K$ a au plus $n$ éléments.

**II5.** Montrer qu'il existe une partie dense de $\mathbb{R}^3$ dont quatre points quelconques ne sont pas coplanaires.

**II6.** Montrer qu'il existe une famille de suites arithmétiques de réels deux-à-deux disjointes et dont les raisons recouvrent $\mathbb{R}$. (Cet exercice vous était proposé par Péter Horvai.)

**II7.** Montrer que le dernier chiffre non nul de $n!$ forme une suite non périodique.

**II8.** Si $\Omega$ est un ouvert connexe de $\mathbb{R}^n$, alors $\Omega$ est connexe par arcs $C^\infty$.

**II9.** Si $(a_n)_{n \in \mathbb{N}}$ est une suite quelconque de réels, alors il existe une application $f : \mathbb{R} \to \mathbb{R}$ de classe $C^\infty$ telle que $f^{(n)}(0) = a_n$ pour tout $n$. Ce théorème est dû à Emile Borel. (Voir aussi l'exercice III2.)

**III. Sommation des séries divergentes.**

**III1.** Soit $(\Sigma a_n)$ une série : on dit que $(\Sigma a_n)$ est sommable de somme $S$ au sens de Mittag-Leffler si et seulement s'il existe une fonction $f: \Omega \to \mathbb{C}$ holomorphe (i.e. dérivable au sens complexe) sur un ouvert $\Omega$ de $\mathbb{C}$ telle que $[0;1] \subseteq \Omega$, que $f(1) = S$ et qu'il existe un voisinage $V$ de 0 dans $\mathbb{C}$ sur lequel la série $\sum_{n=0}^{\infty} a_n z^n$ est absolument convergente et vaut $f(z)$. Par exemple, la série $(\Sigma(-1)^n)$ est sommable de somme $\frac{1}{2}$ au sens de Mittag-Leffler, avec $f: z \mapsto \frac{1}{1+z}$. On pose $\lambda_0 = 0$ et, pour $n > 0$, $\lambda_n = n \log n$. Si $(\Sigma a_n)$ est sommable de somme $S$ au sens de Mittag-Leffler, montrer que

$$\lim_{t \to 0^+} \sum_{n=0}^{\infty} a_n e^{-t\lambda_n}$$

a un sens et vaut $S$. (On pourra d'abord établir le résultat pour la série $(\Sigma x^n)$.) Ce théorème est dû à Ernst Lindelöf.

**III2.** Soit $V$ un secteur ouvert de sommet 0 dans le plan complexe (i.e. un ouvert dont la frontière est la réunion de deux segments d'origine 0 et d'un arc de cercle centré en 0). Soient $f$ une fonction holomorphe sur $V$ et $\hat{f} = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{C}[[X]]$ une série formelle. On dit que $f$ est asymptotique à $\hat{f}$ sur $V$ si et seulement si pour tout sous-secteur compact $W$ de $V \cup \{0\}$ et tout naturel $n$ il existe un réel strictement positif $M$ tel que

$$|x|^{-n} \left| f(x) - \sum_{p=0}^{n-1} a_p x^p \right| < M$$

pour tout $x \in W \setminus \{0\}$. Montrer alors le théorème de Borel-Ritt : pour tout secteur ouvert $V$ de sommet 0 et toute série formelle $\hat{f}$ il existe une fonction holomorphe $f: V \to \mathbb{C}$ asymptotique à $\hat{f}$ sur $V$. Cette fonction n'est pas unique, et cette méthode n'est donc pas adaptée à la sommation des séries divergentes. La méthode suivante permet de remédier à ce problème.

**III3.** Soit $k > 0$ un réel. Soit $V$ un secteur ouvert de sommet 0 dans le plan complexe (i.e. un ouvert dont la frontière est la réunion de deux segments d'origine 0 et d'un arc de cercle centré en 0). Soient $f$ une fonction holomorphe sur $V$ et $\hat{f} = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{C}[[X]]$ une série formelle. On dit que $f$ est asymptotique Gevrey à l'ordre $1/k$ à $\hat{f}$ sur $V$ si et seulement si pour tout sous-secteur compact $W$ de $V \cup \{0\}$ il existe des réels strictement positifs $C$ et $A$ tels que

$$|x|^{-n} \left| f(x) - \sum_{p=0}^{n-1} a_p x^p \right| < C(n!)^{1/k} A^n$$

pour tout naturel $n$ et tout $x \in W \setminus \{0\}$. Montrer alors le théorème de Watson : soit $k > \frac{1}{2}$ un réel et $V$ un secteur ouvert de sommet 0 et d'ouverture (angle au sommet) $> \frac{\pi}{k}$ ; soit $f$ une fonction holomorphe sur $V$ asymptotique Gevrey à l'ordre $1/k$ à la série nulle ; alors $f$ est identiquement nulle. (On pourra utiliser le théorème du maximum sous une forme Phragmèn-Lindelöf).

## IV. Théorie descriptive des ensembles.

**IV1.** On dit qu'une partie $N$ de $\mathbb{R}$ est fortement négligeable si et seulement si pour toute suite $(\varepsilon_n)$ de réels strictement positifs il existe une suite $(I_n)$ d'intervalles ouverts tels que la longueur de chaque $I_n$ soit inférieure à $\varepsilon_n$ et que $N \subseteq \bigcup_{n=0}^{\infty} I_n$. On suppose vérifiée l'hypothèse du continu (i.e. toute partie de $\mathbb{R}$ est soit au plus dénombrable soit équipotente à $\mathbb{R}$). Montrer alors qu'il existe une partie de $\mathbb{R}$ fortement négligeable et équipotente à $\mathbb{R}$. (On pourra considérer l'ensemble des fermés de $\mathbb{R}$ d'intérieur vide et construire une partie $N$ de $\mathbb{R}$ ayant une intersection dénombrable avec tout fermé d'intérieur vide.)

**IV2.** On rappelle qu'une tribu est un ensemble d'ensembles stable par union dénombrable et passage au complémentaire. Toute intersection de tribus est une tribu, et on peut donc définir la tribu engendrée par un ensemble d'ensembles comme la plus petite tribu contenant cet ensemble. On définit alors la tribu borélienne de $\mathbb{R}$ comme la tribu engendrée par les ouverts de $\mathbb{R}$. Ses éléments s'appellent les boréliens. On dit qu'une partie $N$ de $\mathbb{R}$ est négligeable ssi pour tout $\varepsilon > 0$ il existe une suite $(I_n)$ d'intervalles ouverts dont la somme des longueurs converge et est inférieure à $\varepsilon$ et tels que $N \subseteq \bigcup_{n=0}^{\infty} I_n$. Une partie $E$ de $\mathbb{R}$ est dite mesurable ssi elle s'écrit $E = B \Delta N = (B \setminus N) \cup (N \setminus B)$ où $B$ est borélien et $N$ négligeable. Montrer que $[0;1]$ n'est pas négligeable. Montrer que l'image réciproque d'un borélien par une application continue est un borélien, que l'image directe d'un borélien par une application continue est mesurable mais pas nécessairement borélienne. Montrer que l'image réciproque ou directe d'un mesurable par une application continue peut ne pas être mesurable. Montrer que l'image directe d'un borélien par une application localement intégrable au sens de Riemann peut ne pas être mesurable.

**IV3.** Dans cet exercice, on ne suppose pas l'axiome du Choix. On reprend les définitions de l'exercice précédent. On dit de plus qu'une partie de $\mathbb{R}$ est rare ssi son adhérence est d'intérieur vide (autrement dit ssi son complémentaire contient un ouvert dense). On dit qu'une partie de $\mathbb{R}$ est maigre ssi elle est réunion dénombrable d'ensembles rares. On dit qu'une partie $E$ de $\mathbb{R}$ vérifie la propriété de Baire ssi elle s'écrit $E = B \Delta M$ où $B$ est borélien et $M$ maigre. Si $\mathcal{A}$ est une partie de $\mathcal{N} = \mathbb{N}^{\mathbb{N}}$, l'ensemble des suites de naturels, on définit le jeu $G_{\mathcal{A}}$ comme suit : deux joueurs, $A$ et $B$ s'affrontent ; $A$ commence et joue un naturel quelconque, $a_0$ ; puis $B$ joue et choisit un naturel $b_0$ ; puis $A$ choisit $a_1$, et ainsi de suite. Le joueur $A$ gagne ssi la suite $a_0, b_0, a_1, b_1, \ldots$ appartient à $\mathcal{A}$, sinon $B$ gagne. Le jeu $G_{\mathcal{A}}$ (ou la partie $\mathcal{A}$) est dit déterminé ssi un des deux joueurs possède une stratégie gagnante. L'axiome de Détermination affirme que toute partie $\mathcal{A}$ de $\mathcal{N}$ est déterminée. Montrer que cet axiome contredit l'axiome du Choix. Montrer que l'axiome de Détermination implique l'axiome de Solovay : toute partie de $\mathbb{R}$ est mesurable. Montrer que l'axiome de Détermination implique que toute partie de $\mathbb{R}$ vérifie la propriété de Baire. Montrer que l'axiome de Détermination implique que toute partie de $\mathbb{R}$ équipotente à $\mathbb{R}$ possède un sous-ensemble parfait (fermé sans point isolé).

## V. Les nombres réels.

On appelle coefficient d'irrationnalité d'un réel $\theta$ la borne inférieure (éventuellement infinie) de l'ensemble des réels $\alpha$ positifs pour lesquels l'équation

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^\alpha}$$

a une infinité de solutions rationnelles $\frac{p}{q}$ ($p$ entier, $q$ naturel non nul, $p$ et $q$ premiers entre eux). On le note $\deg\theta$.

**V1.** Montrer que l'ensemble $\{\deg\theta : \theta \in \mathbb{R}\}$ des degrés d'irrationnalité possibles est $\{1\} \cup [2; +\infty]$. Montrer que presque tous les réels ont degré 2 (i.e. $\{\theta \in \mathbb{R} : \deg\theta \neq 2\}$ est négligeable, comme défini dans l'exercice IV2). Montrer que quasiment tous les réels ont degré $+\infty$ (i.e. $\{\theta \in \mathbb{R} : \deg\theta < +\infty\}$ est maigre, comme défini dans l'exercice IV3). Montrer que si $P$ est un polynôme non constant de degré $d$ à coefficients entiers, alors pour tout réel $\theta$, $\deg P(\theta) \geq \frac{1}{d}\deg\theta$ (ce dernier résultat est connu sous le nom de théorème de Liouville). Quelle est la dimension de Hausdorff de $\{\theta \in \mathbb{R} : \deg\theta = d\}$ ?

**V2.** On pose $u_n = \frac{1}{n \sin n}$. $u_n$ tend-elle vers 0 ? $\limsup_{n\to+\infty} u_n$ est-elle finie ? (D'accord, cette dernière question est vraiment vicieuse.)

**V3.** Montrer que pour tous réels $\theta_1, \ldots, \theta_n$ et pour tout $\varepsilon > 0$ il existe un naturel non nul $q$ et des entiers $p_1, \ldots, p_n$ tels que

$$\left|\theta_i - \frac{p_i}{q}\right| < \frac{\varepsilon}{q}$$

pour tout $i$.

## VI. Théorie des ensembles.

**VI1.** On suppose qu'il existe une injection $j : A \to B$ et une surjection $s : A \to B$. Montrer qu'il existe une bijection $\theta : A \to B$.

**VI2.** On suppose vérifiée l'hypothèse du continu (i.e. toute partie de $\mathbb{R}$ est soit au plus dénombrable soit équipotente à $\mathbb{R}$). Monter qu'il n'existe pas de mesure non triviale définie sur <u>toutes</u> les parties de $[0;1]$, c'est-à-dire pas d'application $\mu : \mathcal{P}([0;1]) \to \bar{\mathbb{R}}_+$ ($\mathcal{P}([0;1])$ désignant l'ensemble des parties de $[0;1]$) telle que $\mu(\emptyset) = 0$, $\mu([0;1]) = 1$, $\mu(\{a\}) = 0$ pour tout $a \in [0;1]$ et $\mu(\bigcup_{n=0}^{\infty} A_n) = \sum_{n=1}^{\infty} \mu(A_n)$ lorsque les $A_n$ sont des parties deux-à-deux disjointes de $[0;1]$.

## VII. Topologie générale.

**VII1.** Donner un exemple d'espace topologique infini dénombrable séparé et connexe.

**VII2.** Si $(T, \leq)$ est un ensemble totalement ordonné, on le munit d'une topologie de la manière suivante : les ouverts de $T$ sont les réunions d'intervalles ouverts. (Note : les demi-droites ouvertes sont considérées comme des intervalles ouverts, ainsi que $T$ lui-même.) On dit que cette topologie est induite par l'ordre total de $T$. Donner un exemple d'ensemble totalement ordonné dont l'ordre total induise une topologie connexe, mais non connexe par arcs.

**VII3.** On définit une topologie sur l'ensemble $E = \mathbb{R}^{\mathbb{N}}$ des suites de réels de la manière suivante : une partie de $E$ sera dite ouverte ssi elle s'écrit comme une réunion d'ensembles de la forme $\prod_{n\in\mathbb{N}} \Omega_n$ où $\Omega_n$ est ouvert dans $\mathbb{R}$. Montrer alors que $E$ n'est pas connexe. A quelle condition nécessaire et suffisante une suite $(x_n)$ d'éléments de $E$ converge-t-elle vers la suite nulle ?

## VIII. Topologie, suite.

**VIII1.** Montrer que, pour $m \neq n$, $\mathbb{R}^m$ et $\mathbb{R}^n$ ne sont pas homéomorphes. (Cet exercice est virtuellement impossible ; après la lecture de la section XIII, il l'est peut-être un peu moins. Et encore...) Ce résultat, connu sous le nom de théorème d'"invariance du domaine", est dû à Luitzen Egbertus Jan Brouwer.

**VIII2.** On dira qu'un espace topologique non vide $E$ est hyperconnexe si et seulement s'il existe une application continue surjective de $\mathbb{R}$ sur $E$. Un espace hyperconnexe est clairement connexe par arcs. Montrer que $\mathbb{R}^n$ est hyperconnexe pour tout $n$. Donner un exemple d'espace topologique (non vide) connexe par arcs mais non hyperconnexe.

**VIII3.** Soit une partie $M$ de $\mathbb{R}^n$ connexe non vide et dont tout point possède un voisinage homéomorphe à $\mathbb{R}$. Montrer que $M$ est homéomorphe à $\mathbb{R}$ ou au cercle $S^1$. Montrer que cette conclusion n'est plus valable si l'on suppose simplement que $M$ est un espace topologique.

**VIII4.** On se donne un corps topologique, c'est-à-dire un corps qui est également un espace topologique, et pour lequel l'addition, la soustraction, la multiplication et l'inverse sont continues. Montrer que s'il est compact, il est fini (donc discret).

## IX. Olympiades internationales de mathématiques et Concours Généraux.

**IX1.** (IMO87-3)Prouver qu'il n'existe aucune application $f\colon \mathbb{N} \to \mathbb{N}$, satisfaisant à : pour tout naturel $n$, $f(f(n)) = n + 1987$.

**IX2.** (IMO86-1)Soit $d$ un entier strictement positif n'appartenant pas à l'ensemble $\{2, 5, 13\}$. Montrer que l'on peut trouver un couple $(a, b)$ d'éléments distincts de l'ensemble $\{2, 5, 13, d\}$ tel que $ab - 1$ ne soit pas le carré d'un entier.

**IX3.** (IMO83-5)Peut-on trouver 1983 nombres entiers strictement positifs et distincts, inférieurs ou égaux à $10^5$ et tels que trois quelconques d'entre eux ne soient pas les termes consécutifs d'une progression arithmétique ? Justifier votre réponse.

**IX4.** (CG94-3)On définit une application $f$ de $\mathbb{N}^*$ dans $\mathbb{N}$ par : $f(1) = 0$ et, pour tout élément $n$ de $\mathbb{N}^*$ : $f(2n) = 2f(n) + 1$, $f(2n + 1) = 2f(n)$. Etant donné un entier strictement positif $p$ quelconque, on pose $u_0 = p$ et, tant que $u_k$ appartient à $\mathbb{N}^*$, $u_{k+1} = f(u_k)$.

1. Montrer que, pour tout choix de $p$, il existe un unique entier $v(p)$ tel que $u_{v(p)} = 0$.

2. a. Calculer $v(1994)$. Quel est le plus petit entier $p$ tel que $v(p) = v(1994)$ ?

2. b. Etant donné un entier $N$, déterminer le plus petit entier $p$ tel que $v(p) = N$.

## X. Amusons-nous avec les dérivées.

Dans toute cette section, "intervalle" signifiera toujours "intervalle non trivial de $\mathbb{R}$". Et une fonction sera toujours considérée comme définie sur un intervalle, et prenant ses valeurs dans $\mathbb{R}$.

Dès 1911, W. H. Young a posé le problème de la caractérisation des dérivées des fonctions réelles. Alors que la question semblable pour la variable complexe admet une réponse très simple (par exemple : si $\Omega$ est un ouvert simplement connexe de $\mathbb{C}$, une fonction $f:\Omega \to \mathbb{C}$ est la dérivée d'une fonction $F:\Omega \to \mathbb{C}$ si et seulement si $f$ est holomorphe), le problème dans $\mathbb{R}$ s'est révélé très difficile. Nous proposons ici de donner une condition nécessaire et une condition suffisante assez simples, puis une condition due à Neugebauer, nécessaire et suffisante, mais qui est à peu près totalement inutile.

On appelle fonction de Darboux sur un intervalle $I$ une fonction réelle $f$ qui vérifie la propriété des valeurs intermédiaires : l'image d'un connexe par $f$ est un connexe. En autres mots, si $a < b$ sont des points de $I$, $[f(a); f(b)] \subseteq f([a; b])$.

On dit qu'une fonction réelle $f$ définie sur un intervalle $I$ est dans la classe 1 de Baire ssi $f$ est la limite simple d'une suite de fonctions continues.

On rappelle brièvement la définition de la mesure de Lebesgue : si $\Omega$ est un ouvert, il s'écrit comme une réunion dénombrable d'intervalles deux-à-deux disjoints, et on définit $\mu(\Omega)$ comme la somme de la longueur de ces intervalles. Pour un ensemble $E \subseteq \mathbb{R}$ quelconque, on définit sa mesure extérieure de Lebesgue par :

$$\mu^*(E) = \inf_{\Omega \supseteq E} \mu(\Omega)$$

où la borne inférieure est prise sur l'ensemble des ouverts qui recouvrent $E$. On dit que $A \subseteq E$ est mesurable ssi pour toute partie $E$ de $\mathbb{R}$ on a :

$$\mu^*(E) = \mu^*(E \cap A) + \mu^*(E \setminus A)$$

On écrit alors $\mu(A)$ pour $\mu^*(A)$. On a alors les propriétés bien connues de $\mu$ : $\mu(\emptyset) = 0$, $\mu([a; b]) = b - a$ si $a < b$, $\mu(\alpha A + \beta) = |\alpha|\mu(A)$ pour tout ensemble mesurable $A$ et tous réels $\alpha$ et $\beta$ ; si $A$ est mesurable alors $\mathbb{R} \setminus A$ l'est ; si $A_0, A_1, \dots$ sont mesurables et deux-à-deux disjoints alors $\bigcup_{n=0}^{\infty} A_n$ est mesurable et

$$\mu\left(\bigcup_{n=0}^{\infty} A_n\right) = \sum_{n=0}^{\infty} \mu(A_n)$$

$A$ est dit négligeable ssi $\mu^*(A) = 0$ : $A$ est alors mesurable.

On définit la densité supérieure d'un ensemble mesurable $A$ en un point $x_0$ comme :

$$ds(A, x_0) = \limsup_{h \to 0+, k \to 0+, h+k \neq 0} \frac{\mu(A \cap [x_0 - h; x_0 + k])}{h + k}$$

On définit de manière semblable la densité inférieure $di(A, x_0)$. Lorsque $ds(A, x_0) = di(A, x_0)$, on appelle ce nombre la densité de $A$ en $x_0$ et on le note $d(A, x_0)$.

On dira qu'une fonction $f$ est approximativement continue en $x_0$ ss'il existe un ensemble $A$ mesurable contenant $x_0$ tel que $d(A, x_0) = 1$ et que $f|_A$ soit continue en $x_0$. On dira que $f$ est approximativement continue ssi elle est approximativement continue en tout point de son ensemble de définition.

**X1.** Montrer qu'une fonction de Darboux peut être discontinue en tout point, que son graphe peut ne pas être connexe, et que toute fonction est la somme de deux fonctions de Darboux.

**X2.** Si $f$ est une fonction de la classe 1 de Baire, $f$ est une fonction de Darboux ssi son graphe est connexe.

**X3.** Montrer que la somme ou le produit d'une fonction de Darboux de la classe 1 de Baire et d'une fonction continue, est une fonction de Darboux de la classe 1 de Baire.

**X4.** (CONDITION NECESSAIRE) Montrer que toute dérivée est une fonction de Darboux de la classe 1 de Baire. Montrer que la réciproque n'est pas vraie.

**X5.** Montrer que si $A$ est mesurable alors $d(A, x_0) = 1$ pour presque tout $x_0 \in A$ (c'est-à-dire que $\{x_0 \in A : di(A, x_0) < 1\}$ est négligeable), et $d(A, x_0) = 0$ pour presque tout $x_0 \notin A$.

**X6.** Montrer que pour $x_0 \in \mathbb{R}$, les ensembles $U$ contenant un ensemble mesurable $A$ tel que $d(A, x_0) = 1$ forment la famille des voisinages de $x_0$ pour une certaine topologie de $\mathbb{R}$, plus fine que la topologie ordinaire. On appellera topologie de la densité la topologie ainsi définie.

**X7.** Montrer qu'une fonction $f$ est approximativement continue ssi elle est continue pour la topologie de la densité, définie dans l'exercice précédent.

**X8.** Montrer qu'une fonction $f$ est mesurable (i.e. l'image réciproque d'un ouvert quelconque par $f$ est mesurable) ssi $f$ est approximativement continue presque partout (i.e. l'ensemble des points où $f$ n'est pas approximativement continue est négligeable).

**X9.** (CONDITION SUFFISANTE) Montrer qu'une fonction bornée approximativement continue est une dérivée. Montrer que la réciproque n'est pas vraie.

**X10.** Montrer qu'une fonction bornée semi-continue est approximativement continue ssi c'est une dérivée.

**X11.** (CRITERE DE NEUGEBAUER) Soit $f$ une fonction définie sur un intervalle $I_0$. Alors $f$ est une dérivée ssi à tout sous-intervalle fermé $I$ de $I_0$ il correspond un point $x_I$ intérieur à $I$ tel que

(i) $f(x_{[x-h;x+k]}) \to f(x)$ lorsque $h \to 0^+$, $k \to 0^+$ et $h + k \neq 0$.

(ii) $f(x_I) = (f(x_J)\mu(J) + f(x_K)\mu(K))/(\mu(J) + \mu(K))$ lorsque $I$, $J$ et $K$ sont des sous-intervalles de $I_0$ tels que $I = J \cup K$ et que les intérieurs de $J$ et $K$ sont disjoints.

## XI. Le seigneur des anneaux.

Nous nous proposons de démontrer ici quelques résultats classiques sur les anneaux non commutatifs. Tous les anneaux considérés ici seront supposés avoir un élément unité, noté 1. On rappelle que si $\mathcal{A}$ est un tel anneau, une partie $I$ de $\mathcal{A}$ est appelée idéal à gauche (resp. à droite) ssi $I$ est un sous-groupe additif de $\mathcal{A}$ et que $aI \subseteq I$ (resp. $Ia \subseteq I$) pour tout $a \in \mathcal{A}$. On dit que $I$ est un idéal bilatère ssi c'est un idéal à gauche et à droite.

Un idéal à gauche (resp. à droite) $I$ est dit maximal ssi $I$ n'est contenu dans aucun idéal à gauche (resp. à droite) sauf $I$ et $\mathcal{A}$.

Un anneau est dit artinien (resp. nœthérien) à gauche ssi toute suite décroissante $I_0 \supseteq I_1 \supseteq \cdots$ (resp. toute suite croissante $I_0 \subseteq I_1 \subseteq \cdots$) d'idéaux à gauche est stationnaire. On définit de même les anneaux artiniens (resp. nœthériens) à droite.

Un élément $a$ de $\mathcal{A}$ est appelé inversible à gauche (resp. à droite) ss'il existe un élément $b$ de $\mathcal{A}$ tel que $ba = 1$ (resp. $ab = 1$). $b$ est alors appelé un inverse à gauche (resp. à droite) de $a$. Un élément $a$ inversible à gauche et à droite est appelé inversible ; il a alors exactement un inverse à gauche, exactement un inverse à droite, et ceux-ci sont égaux : on les appelle l'invrse de $a$.

Le radical de Jacobson d'un anneau $\mathcal{A}$ est l'intersection de tous les idéaux à gauche maximaux de $\mathcal{A}$. On le note $rad\,\mathcal{A}$.

Un élément $a$ de $\mathcal{A}$ est dit nilpotent ss'il existe un naturel $n$ non nul tel que $a^n = 0$. Un idéal à gauche (resp. à droite) est dit nil ssi tous ses éléments sont nilpotents. Un idéal à gauche (resp. à droite) $I$ est dit nilpotent ss'il existe un naturel $n$ non nul tel que $I^n = \{0\}$, où $I^n$ désigne le groupe additif engendré par tous les produits de $n$ éléments (non nécessairement distincts) de $I$. Il est évident qu'un idéal nilpotent est nil, la réciproque n'étant pas vraie.

Un anneau est dit simple ssi ses seuls idéaux bilatères sont $\{0\}$ et lui-même.

**XI1.** Montrer que $y \in rad\,\mathcal{A}$ ssi $1 - xy$ est inversible à gauche pour tout $x \in \mathcal{A}$. Montrer que $rad\,\mathcal{A}$ est un idéal bilatère. Montrer que $y \in rad\,\mathcal{A}$ ssi $1 - xyz$ est inversible pour tous $x$ et $z$ de $\mathcal{A}$. En déduire que $rad\,\mathcal{A}$ est l'intersection de tous les idéaux à droite maximaux de $\mathcal{A}$.

**XI2.** (On pourra utiliser ici une partie des conclusions de l'exercice précédent.) Montrer que tout idéal à gauche nil de $\mathcal{A}$ est contenu dans $rad\,\mathcal{A}$. En déduire que dans un anneau artinien à gauche, tout idéal à gauche nil est nilpotent.

**XI3.** On suppose qu'un élément $a$ d'un anneau $\mathcal{A}$ a plus d'un inverse à gauche. Montrer qu'il en a une infinité.

**XI4.** Montrer qu'un anneau est simple et artinien à gauche ss'il est égal à l'anneau $\mathcal{M}_n(K)$ des matrices $n \times n$ sur un certain corps $K$ (non nécessairement commutatif), et que de plus $n$ et $K$ sont alors uniques. Pour cela, on pourra démontrer la proposition suivante, appelée lemme du "double centralisateur" : soit $\mathcal{A}$ un anneau simple, $I$ un idéal à gauche de $\mathcal{A}$, $\mathcal{D}$ l'anneau des applications $\mathcal{A}$-linéaires de $I$, considérées comme opérant à droite sur $I$ (i.e. des applications $f: I \to I$ telles que $(x+y)f = xf + yf$ et $(ax)f = a(xf)$ pour tous $x$ et $y$ de $I$ et $a$ de $\mathcal{A}$, en notant $xf$ l'image de $x$ par $f \in \mathcal{D}$) et $\mathcal{G}$ l'anneau des applications $\mathcal{D}$-linéaires de $I$, considérées comme opérant à gauche sur $I$ (i.e. des applications $g: I \to I$ telles que $g(x+y) = gx + gy$ et $g(xf) = (gx)f$ pour tous $x$ et $y$ de $I$ et $f$ de $\mathcal{D}$, en notant $gx$ l'image de $x$ par $g \in \mathcal{G}$) ; alors l'application canonique $\mathcal{A} \to \mathcal{G}$, qui à $a \in \mathcal{A}$ associe la multiplication à gauche par $a$, est un isomorphisme d'anneaux, $a \mapsto (x \mapsto ax)$.

**XI5.** On suppose que dans un anneau $\mathcal{A}$ tout idéal à gauche principal (i.e. tout idéal de la forme $\mathcal{A}a$ où $a \in \mathcal{A}$) est engendré par un idempotent (i.e. s'écrit $\mathcal{A}e$ où $e^2 = e$). Montrer alors que tout idéal à droite principal est engendré par un idempotent. (On pourra montrer au préalable que pour tout $a \in \mathcal{A}$ il existe $x \in \mathcal{A}$ tel que $a = axa$.) Un tel anneau s'appelle von Neumann-régulier. En utilisant les conclusions de l'exercice XI1, montrer que le radical de Jacobson d'un anneau von Neumann-régulier est réduit à $\{0\}$.

**XI6.** (Cet exercice est particulièrement difficile ; il utilise les résultats et définitions des exercices XI1 et XI5, et il est probablement utile d'avoir traité le XI4 avant de l'aborder.) Montrer qu'un anneau artinien à gauche est nœthérien à gauche. Montrer qu'un anneau nœthérien à gauche et von Neumann-régulier est artinien à gauche.

**XI7.** (Cet exercice utilise les résultats de l'exercice XI1.) Montrer qu'un anneau $\mathcal{A}$ a un seul idéal à gauche maximal ss'il a un seul idéal à droite maximal. Un tel anneau s'appelle un anneau local. Montrer que dans un anneau local les seuls idempotents (i.e. les seuls éléments $e$ vérifiant $e^2 = e$) sont 0 et 1.

## XII. Stéphane Hoguet in memoriam.

**XII1.** Soit $E$ un ensemble fini de points du cercle-unité, non diamétralement opposés, et $n$ un entier $\leq \frac{1}{2}|E|$ (où $|E|$ est le cardinal de $E$) ; soit $E'$ l'ensemble des points $x \in E$ tels que le cardinal de $E \cap \{xe^{i\theta} : \theta \in [0;\pi]\}$ soit $< n$. Prouver l'inégalité $|E'| \leq n$.

**XII2.** Soit $(\Sigma u_n)$ une série convergente et $\sigma$ une permutation de $\mathbb{N}$ telle que :

$$\lim_{n\to+\infty} \left( |\sigma(n) - n| \sup_{k\geq n} |u_{\sigma(k)}| \right) = 0$$

montrer que la série $(\Sigma u_{\sigma(n)})$ converge et a même somme que $(\Sigma u_n)$. La conclusion subiste-t-elle lorsqu'on remplace l'hyptothèse

$$\lim_{n\to+\infty} \left( |\sigma(n) - n| \sup_{k\geq n} |u_{\sigma(k)}| \right) = 0$$

par celle-ci :

$$\lim_{n\to+\infty} \left( |\sigma(n) - n| \sup_{k\geq n} |u_k| \right) = 0$$

(c'est ce que prétend Nicolas Bourbaki, Topologie Générale, Chapitre IV, exercice 12 page 60 du § 7).

**XII3.** Soit $S_0$ une suite finie d'entiers $> 0$ ; par récurrence sur $i \geq 0$, on définit une suite (infinie) de suites (finies) $S_i$ d'entiers $> 0$ comme suit : notant $m_k(i)$ le nombre d'occurrences de l'entier $k$ dans $S_i$ ($m_k(i) = 0$ sauf pour un nombre fini d'entiers $k$), la suite $S_{i+1}$ s'obtient en écrivant successivement les couples $m_k(i), k$ pour les $k$ tels que $m_k(i) > 0$ rangés en ordre croissant. Exemple : $S_0 = (1)$, $S_1 = (1,1)$, $S_2 = (2,1)$, $S_3 = (1,1,1,2)$, $S_4 = (3,1,1,2)$, $S_5 = (2,1,1,2,1,3)$, $S_6 = (3,1,2,2,1,3)$, $S_7 = (2,1,2,2,2,3)$, etc. Montrer que la suite $(S_i)_{i\in\mathbb{N}}$ est périodique à partir d'un certain rang, i.e. qu'il existe deux entiers $i_0 \geq 0$ et $p \geq 1$ tels que : $\forall i \geq i_0\ S_{i+p} = S_i$.

**XII4.** (ULM76)Un drapeau dans un $K$-espace vectoriel $E$ de dimension $n$ est une suite $(F_i)_{0\leq i\leq n}$ de sous-espaces de $E$ telle que : $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ et $(\forall i\ \dim F_i = i)$. (en particulier donc : $F_0 = \{0\}$ et $F_n = E$).

a) Soit $d = (F_i)_{0\leq i\leq n}$, $d' = (F'_i)_{0\leq i\leq n}$ deux drapeaux ; on pose $A_{i,j} = F_i + F'_j$ et pour chaque $i \in [\![1,n]\!]$ on note $s_{d,d'}(i)$ le plus petit entier $j$ tel que $A_{i,j} = A_{i-1,j}$ ; montrer que $s_{d,d'}$ est une permutation de $[\![1,n]\!]$.

b) Montrer qu'il existe une base $\mathcal{B}$ de $E$ adaptée à la fois à $d$ et à $d'$ (une base $\mathcal{B}$ est adaptée à un drapeau $(F_i)$ si chacun des sous-espaces $F_i$ est engendré par une partie de $\mathcal{B}$.)

**XIII. Nous aimons tous la topologie algébrique.**

On dit que deux applications continues $f, g: A \to B$ entre espaces topologiques sont homotopiques ss'il existe une application continue (appelée homotopie) $\Theta: [0;1] \times A \to B$ telle que $\Theta(0,\cdot) = f$ et $\Theta(1,\cdot) = g$. On note $f \simeq g$. Lorsque de plus $f$ et $g$ sont confondues sur une partie $A_0$ de $A$ et que $\Theta$ peut être choisie de façon que $\Theta(t,x) = f(x)$ pour tout $x \in A_0$, on dit que $f$ et $g$ sont homotopiques relativement à $A_0$, et on note $f \simeq g \ (\mathrm{rel}\, A_0)$. (Et $\Theta$ s'appelle alors une homotopie relative à $A_0$.)

Deux espaces $A$ et $B$ sont homéomorphes ss'il existe deux applications continues $f: A \to B$ et $g: B \to A$ telles que $gf = \mathrm{id}_A$ et $fg = \mathrm{id}_B$. Deux espaces $A$ et $B$ sont dits avoir le même type d'homotopie ss'il existe deux applications continues $f: A \to B$ et $g: B \to A$ telles que $gf \simeq \mathrm{id}_A$ et $fg \simeq \mathrm{id}_B$.

Une partie $A_0$ d'un espace topologique $A$ s'appelle un rétract de $A$ ss'il existe une application $r: A \to A_0$ (une rétraction) telle que $rj = \mathrm{id}_{A_0}$ où $j: A_0 \subseteq A$ est l'injection canonique. Une partie $A_0$ d'un espace topologique $A$ s'appelle un rétract faible de $A$ ss'il existe une application $r: A \to A_0$ (une rétraction faible) telle que $rj \simeq \mathrm{id}_{A_0}$ où $j: A_0 \subseteq A$ est l'injection canonique.

Une partie $A_0$ d'un espace topologique $A$ s'appelle une déformation de $A$ ss'il existe une application continue $f: A \to A_0$ telle que $jf \simeq \mathrm{id}_A$ où $j: A_0 \subseteq A$ est l'injection canonique.

Une partie $A_0$ d'un espace topologique $A$ s'appelle un déformation-rétract fort de $A$ ss'il existe une application continue $r: A \to A_0$ telle que $rj = \mathrm{id}_{A_0}$ et $jr \simeq \mathrm{id}_A \ (\mathrm{rel}\, A_0)$ où $j: A_0 \subseteq A$ est l'injection canonique. Une partie $A_0$ d'un espace topologique $A$ s'appelle un déformation-rétract de $A$ ss'il existe une application continue $r: A \to A_0$ telle que $rj = \mathrm{id}_{A_0}$ et $jr \simeq \mathrm{id}_A$ où $j: A_0 \subseteq A$ est l'injection canonique. Une partie $A_0$ d'un espace topologique $A$ s'appelle un déformation-rétract faible de $A$ ss'il existe une application continue $r: A \to A_0$ telle que $rj \simeq \mathrm{id}_{A_0}$ et $jr \simeq \mathrm{id}_A$ où $j: A_0 \subseteq A$ est l'injection canonique.

**XIII1.** Montrer que les concepts de rétract et de rétract faible sont distincts en général. Montrer que les concepts de déformation-rétract fort, de déformation-rétract et de déformation-rétract faible sont deux-à-deux distincts en général.

**XIII2.** Montrer que, si $S^1 = \{z \in \mathbb{C}: |z| = 1\}$ est le cercle topologique, les applications $\mathrm{id}_{S^1}$ et $c_1$ (application constante égale à 1) ne sont pas homotopiques. (On pourra se ramener à des applications continues $\alpha$ et $\beta$ de $[0;1]$ vers $S^1$ telles que $\alpha(0) = \alpha(1) = \beta(0) = \beta(1) = 1$, et à une homotopie entre $\alpha$ et $\beta$ relative à $\{0;1\}$. On démontrera alors un théorème de relèvement* qu'on appliquera à cette homotopie. Il ne reste alors qu'à conclure.) En déduire que $S^1$ n'est pas un rétract faible de $D^2 = \{z \in \mathbb{C}: |z| \leq 1\}$. En déduire le théorème de Brouwer : si $f$ est une application continue de $D^2$ dans lui-même, il existe $z \in D^2$ tel que $f(z) = z$.

**XIII3.** On se propose de montrer le théorème de d'Alembert-Gauss (tout polynôme non constant à coefficients complexes admet une racine) par des moyens de topologie algébrique. Soit $p: z \mapsto z^n + a_{n-1}z^{n-1} + \cdots + a_0$ un polynôme unitaire de degré $n$ à coefficients complexes. On suppose que $p$ ne s'annule pas. On pose $q: z \mapsto z^n$, et, pour $r > 0$, $C_r = \{z \in \mathbb{C}: |z| = r\}$. En utilisant le résultat de la première question de l'exercice précédent, montrer que pour tout $r > 0$, $q|_{C_r}: C_r \mapsto \mathbb{C}^*$ n'est pas homotopique à une application constante. Montrer que pour $r$ assez grand, $p|_{C_r}$ et $q|_{C_r}$ sont homotopiques en tant qu'applications de $C_r$ vers $\mathbb{C}^*$. En déduire le théorème voulu.

* C'est-à-dire un théorème permettant d'écrire une application continue $f: X \to S^1$ sous la forme $x \mapsto e^{2i\pi\theta(x)}$ où $\theta: X \to \mathbb{R}$ est continue.

**XIV. Culture générale et histoire des mathématiques.**

**XIV1.** Tout le monde connaît bien sûr le célèbre article de K. Gödel, *Uber Formal Unentscheidbare Sätze der* Principia Mathematica *und Verwandter Systeme I* ("Sur les Propositions Formellement Indécidables des *Principia Mathematica* et de Systèmes Apparentés I"). Que sont les *Principia Mathematica*, quels en sont les auteurs, et à quoi ce titre fait-il allusion ?

**XIV2.** Les *Cours d'Analyse de l'Ecole Polytechnique* par Augustin-Louis Cauchy sont restés célèbres comme modèle de rigueur du raisonnement. Ils contiennent cependant une erreur restée célèbre dans la démonstration de l'existence de primitives des fonctions continues : quelle est-elle ?

**XIV3.** Qui fut le premier à montrer (de façon assez peu rigoureuse, il est vrai) que :

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

**XIV4.** A quel siècle vivait Euclide, et où est-il né ?

**XV. La fonction $\zeta$.**

(In *Exercices de Mathématiques pour l'Agrégation*, Analyse 2, A. Chambert-Loir & S. Fermigier, Masson.)

**XV1.** Soit $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

1. Montrer que $\zeta(s)$ existe pour $\Re(s) > 1$ et définit dans ce demi-plan une fonction holomorphe. Calculer $\lim_{s\to 1} \zeta(s)$ et $\lim_{s\to 1}(s-1)\zeta(s)$.

2. On introduit la fonction $\theta(t) = \sum_{n\in\mathbb{Z}} e^{-n^2 t}$ définie pour $t > 0$, et on rappelle son équation fonctionnelle (qui sera admise) $\theta(\pi/x) = \sqrt{x}\theta(\pi x)$. En remarquant que $n^{-s}\Gamma(s) = \int_0^\infty e^{-nt}t^{s-1}dt$, montrer que $\zeta(s)$ se prolonge en une fonction méromorphe sur $\mathbb{C}$, admettant un unique pôle simple en 1.

3. On pose $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Montrer que $\xi(s) = \xi(1-s)$ (*équation fonctionnelle de la fonction zêta de Riemann*).

**XV2.** On utilise les notations et résultats de l'exercice précédent.

1. Montrer que $\zeta(s)$ peut s'écrire, pour $\Re s > 1$, sous la forme d'un produit infini (*produit eulérien*)

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1-p^{-s}} \tag{1}$$

2. Pour $\sigma > 1$ et $t$ réel, calculer $\log|\zeta(\sigma+it)|$ sous la forme d'une série. En déduire que $\zeta$ ne s'annule pas dans le demi-plan ouvert $\Re s > 1$ en minorant explicitement $|\zeta(\sigma+it)|$.

3. Pour $\sigma > 1$ et $t \in \mathbb{R}$, montrer l'inégalité

$$|\zeta(\sigma)|^3 \cdot |\zeta(\sigma+it)|^4 \cdot |\zeta(\sigma+2it)| \geq 1$$

En déduire que la fonction $\zeta$ de Riemann n'a pas de zéros dans le demi-plan fermé $\Re s \geq 1$.

4. Où sont les zéros complexes de $\zeta$ ?

**XV3.** On utilise les notations et résultats des deux exercices précédents.

1. Montrer, si $\Re(s) > 0$, que

$$\zeta(s) = \frac{s}{s-1} + s\int_1^\infty (\lfloor t\rfloor - t)t^{-s-1}dt$$

(où $\lfloor t\rfloor$ est la partie entière de $t$).

2. Montrer que pour $\Re(s) \geq \frac{1}{2}$, on a $\log|(1-s)\zeta(s)| \leq O(\log|s|+1)$, uniformément. En déduire, à l'aide d'une majoration simple de $|\Gamma(s)|$ pour $\Re(s) \geq \frac{1}{4}$, que la fonction $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ vérifie une majoration

$$\log|(s-1)\xi(s)| \leq |s|O(1+\log|s|)$$

3. On note $N(T)$ le nombre de zéros de $\zeta$ dans la bande $0 \leq \Re(s) \leq 1$ et $|\Im(s)| \leq T$. En utilisant la formule de Jensen (si $f$ est une fonction holomorphe dans le disque fermé $\bar{D}(0,r)$, que $f(0) \neq 0$ et que $a_1, \ldots, a_n \in \bar{D}(0,r)$ sont les zéros de $f$ répétés autant de fois que leur multiplicité, alors $\log|f(0)| + \log\frac{r^n}{|a_1a_2\cdots a_n|} = \frac{1}{2\pi}\int_0^{2\pi}\log|f(re^{i\theta})|d\theta$), montrer que $N(T) = O(T\log T)$.

**XV4.** On utilise les notations et résultats des trois exercices précédents.

1. Soit pour $t \in \mathbb{R}$ la fonction $f(t) = (1+4t^2)\xi(\frac{1}{2}+it)$. On pose $\omega(x) = (\theta(\pi x)-1)/2$. Montrer l'égalité

$$f(t) = 8\int_1^\infty \frac{d}{dx}\left(x^{3/2}\omega'(x)\right) x^{-1/4}\cos(t(\log x)/2)dx$$

2. On fait le changement de variables $x = e^{2u}$ et on définit $\varphi$ par la formule $f(t) = \int_0^\infty \varphi(u)\cos(ut)dt$. Montrer que $\varphi$ est holomorphe pour $|\Im u| \leq \pi/4$ et paire. Montrer que $\varphi(iu)$ et ses dérivées tendent vers 0 quand $u$ tend vers $\pi/4$.

3. Soit $g(u) = \varphi(iu) = \sum_n c_n u^{2n}$. On suppose que $f$ n'a qu'un nombre fini de zéros, montrer que $c_n \in \mathbb{R}$ a un signe constant pour $n$ assez grand. En déduire que $g^{(2n)}(u)$ est une fonction croissante de $u$ pour $n$ assez grand.

4. Montrer que la fonction $\zeta$ de Riemann a une infinité de zéros situés sur la droite critique $\Re(z) = \frac{1}{2}$.

## XVI. Théorie des nombres très très très élémentaire.

On rappelle qu'un entier $q$ est dit primitif modulo $n$ ssi pour tout entier $a$ premier avec $n$ il existe $k \geq 0$ tel que $q^k \equiv a \pmod{n}$. En autres mots, $a$ engendre le groupe multiplicatif $U_n$ des éléments inversibles modulo $n$. On rappelle de plus que $q$ est appelé un résidu quadratique modulo $n$ ss'il existe un entier $w$ tel que $w^2 \equiv q \pmod{n}$.

**XVI1.** On suppose que $p$ est un premier impair et que $(p-1)/2$ est premier. Montrer alors qu'un nombre non congru à $-1$ modulo $p$ est primitif modulo $p$ ss'il n'est pas un résidu quadratique modulo $p$. (Cet exercice est vraiment trop facile.)

**XVI2.** Soit $p$ un nombre premier $\geq 3$. Montrer que le numérateur réduit de

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$$

est divisible par $p$. Plus difficile : pour $p > 3$, il est divisible par $p^2$ (théorème de Wolstenholme).

**XVI3.** Pour $n$ entier naturel, on appelle $\tau(n)$ le nombre de diviseurs de $n$ (y compris 1 et $n$). Quelle est la limite de la suite

$$u_n = \frac{\tau(1)+\tau(2)+\cdots+\tau(n)}{n}$$

quand $n \to +\infty$ ?

**XVI4.** On appelle puissance parfaite un naturel de la forme $n^k$ où $n$ et $k$ sont des naturels $\geq 2$. Pour $x \in \mathbb{R}$, soit $N(x)$ ne nombre de puissances parfaites $\leq x$. Trouver un équivalent de $N(x)$ quand $x \to +\infty$.

**XVI5.** Montrer que $n > 1$ est premier ss'il existe un entier $a$ tel que $a^{n-1} \equiv 1 \pmod{n}$ mais $a^m \not\equiv 1 \pmod{n}$ pour tout facteur $m$ de $n-1$ différent de $n-1$. Ce résultat s'appelle le test de primalité de Lucas-Lehmer.

**XVII. Théorie des nombres un peu moins élémentaire.**

**XVII1.** Soit $\mu(n)$ la fonction de Möbius, avec la convention $\mu(0) = 0$. Montrer que la série $(\Sigma\mu(n))$ est sommable de somme $-2$ au sens de Mittag-Leffler (exercice III1).

**XVII2.** Montrer qu'il n'existe pas de polynôme à coefficients entiers à une seule variable dont la valeur en tout entier soit un nombre premier. Montrer qu'il existe un polynôme à plusieurs variables à coefficients entiers dont les valeurs positives prises sur les entiers soient exactement les nombres premiers. (Cette deuxième question est très difficile.)

**XVII3.** Montrer que pour tout naturel $n$ non nul il existe un nombre premier $p$ tel que $n \leq p \leq 2n$. (Indication donnée par Laurent Berger : c'est évident, il suffit de regarder le coefficient binomial $C_{2n}^{n}$.) Ce résultat est connu sous le nom de postulat de Bertrand. En donner une démonstration en une ligne au moyen de la conjecture de Goldbach.

**XVII4.** On rappelle qu'un nombre premier $p$ est dit régulier ssi $p$ ne divise le numérateur d'aucun des nombres de Bernoulli $B_2, B_4, \ldots, B_{p-3}$. Dans le cas contraire, $p$ est dit irrégulier. 3 est considéré comme régulier. Montrer qu'il existe une infinité de nombres premiers irréguliers. Montrer que si $p$ est un nombre premier régulier, pour tout triplet $(x, y, z)$ solution de l'équation diophantienne

$$x^p + y^p = z^p$$

$p$ divise $xyz$. Pour cela, on supposera qu'il existe une solution avec $p \not| xyz$, et $x, y, z$ premiers entre eux. On appellera $\zeta$ une racine primitive $p$-ième de l'unité. On montrera que pour tout idéal $A$ de $\mathbb{Z}[\zeta]$, si $A^p$ est principal, $A$ l'est aussi (i.e. $p$ ne divise pas le nombre de classe de $\mathbb{Z}[\zeta]$ ; cette condition équivaut d'ailleurs à dire que $p$ est régulier). On écrira $x^p + y^p = (x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y)$. On montrera que les idéaux engendrés par $x + \zeta^i y$ et $x + \zeta^j y$ sont premiers entre eux (engendrent $\mathbb{Z}[\zeta]$) lorsque $i$ et $j$ ne sont pas congrus modulo $p$. On montrera qu'il existe $s \in \mathbb{Z}$, $u \in \mathbb{Z}[\zeta]$ réel et inversible, $\beta \in \mathbb{Z}[\zeta]$ et $n \in \mathbb{Z}$ tels que $x + \zeta y = \zeta^s u \beta$ et $\beta \equiv n \pmod{l}$ (c'est-à-dire que $\beta - n \in l\mathbb{Z}[\zeta]$). On montrera alors que $x + \zeta y - \zeta^{2s} x - \zeta^{2s-1} y \in l\mathbb{Z}[\zeta]$, et on concluera. Si quelqu'un a compris ce charabia, il est très fort.

**XVIII. Théorie des nombres presque intéressante.**

Un corps local est par définition un corps topologique (c'est-à-dire un corps qui est également un espace topologique, et pour lequel l'addition, la soustraction, la multiplication et l'inverse sont continues) localement compact (c'est-à-dire dans lequel 0 a un voisinage compact). On admettra le résultat suivant : tout corps local commutatif et de caractéristique 0 est isomorphe à une algèbre de division de dimension finie sur un corps de nombres $p$-adiques $\mathbb{Q}_p$ ou sur le corps des réels $\mathbb{R}$.

On appellera corps de nombres une extension de degré fini de $\mathbb{Q}$ (i.e. un corps commutatif contenant $\mathbb{Q}$ qui en tant que $\mathbb{Q}$-espace vectoriel est de dimension finie). Une complétion d'un corps de nombres $k$ est un couple $(\lambda, K)$ où $K$ est un corps local et $\lambda\colon k \to K$ un isomorphisme de $k$ sur $\lambda(k) \subseteq K$ tel que $\lambda(k)$ soit dense dans $K$. Deux complétions $(\lambda, K)$ et $(\lambda', K')$ d'un même corps de nombres $k$ sont dites équivalentes ss'il existe un isomorphisme (bicontinu) $\rho$ de $K$ sur $K'$ tel que $\lambda' = \rho\lambda$. Les classes d'équivalence de complétions pour cette relation s'appelent les places du corps de nombres $k$. Les places d'un corps de nombres $k$ pour lesquelles les complétions sont (isomorphe à) des algèbres de division sur $\mathbb{R}$ (c'est-à-dire en fait à $\mathbb{R}$ ou $\mathbb{C}$ d'après le théorème de Frobenius puisque ces algèbres doivent être commutatives) s'appellent les places infinies. Celles pour lesquelles au contraire les complétions sont isomorphes à des algèbres de division sur le corps des nombres $p$-adiques s'appelent les places finies. Le nombre de places infinies est toujours fini est le nombre de places finies est toujours infini.

Lorsque $v$ est une place d'un corps de nombres $k$, on notera $k_v$ une complétion de $k$ selon cette place (n'importe laquelle, elles sont isomorphes). Si l'on est maniaque et que l'on veut faire les choses proprement : les topologies sur les complétions appartenant à une place donnée $v$ de $k$ déterminent sur $k$ une topologie, égale à la topologie induite sur $\lambda(k)$ par celle de $K$ (si $(\lambda, K)$ est une complétion de $v$), et le complété topologique de $k$ pour cette topologie (ou, plus exactement, pour la structure uniforme qu'elle détermine) est appelé $k_v$ : il est isomorphe (en tant que corps local) à $K$ pour chacune des complétions $(\lambda, K)$ dans $v$.

Le corps de nombres $\mathbb{Q}$ a exactement une place infinie, notée $\infty$, et $\mathbb{Q}_\infty = \mathbb{R}$. Ses places finies sont en bijection canonique avec les nombres premiers : pour $p$ premier, on notera $p$ la place finie déterminiée par : $\mathbb{Q}_p$ est le corps des nombres $p$-adiques.

Si $k$ est un corps de nombres et $P$ un ensemble fini de places contenant toutes les places infinies, on note $k(P)$ l'ensemble

$$\prod_{v\in P} k_v \times \prod_{v\notin P} r_v$$

où $r_v$, pour une place finie $v$, désigne l'anneau des entiers de $k_v$, c'est-à-dire, comme $k_v$ est (identifiable à) une algèbre de division sur $\mathbb{Q}_p$ pour un certain $p$, l'ensemble des éléments de $k_v$ dont toutes les coordonnées sont dans $\mathbb{Z}_p$ ; c'est encore la clôture intégrale de $\mathbb{Z}$ dans $k_v$. On munit $k(P)$ de sa structure d'anneau produit, et de sa topologie produit (de Tychonoff) : $k(P)$ devient ainsi un anneau topologique localement compact (d'après le théorème de Tychonoff). L'union des $k(P)$ où $P$ décrit l'ensemble des ensembles finis de places contenant toutes les places infinies, est alors noté $k_{\mathbb{A}}$ est s'appelle l'anneau des adèles de $k$. De manière plus rigoureuse, $k_{\mathbb{A}}$ est la limite inductive des $k(P)$ avec l'injection canonique de $k(P)$ dans $k(P')$ si $P \subseteq P'$. La structure d'anneau sur $k_{\mathbb{A}}$ est obtenue de manière évidente (si $a \in k(P)$ et $a' \in k(P')$, on a $a \in k(P \cup P')$ et $a' \in k(P \cup P')$ donc $aa' \in k(P \cup P')$). La topologie sur $k_{\mathbb{A}}$ est définie comme suit : les ouverts de $k_{\mathbb{A}}$ sont les réunions quelconques d'ouverts des $k(P)$. Les éléments de $k_{\mathbb{A}}$ s'appellent les adèles de $k$.

Par exemple, une adèle de $\mathbb{Q}$ est une suite $(x_\infty, x_2, x_3, x_5, x_7, x_{11}, \ldots)$ où $x_\infty$ est un nombre réel, $x_2$ un nombre 2-adique, $x_3$ un 3-adique, etc, et tel que presque tous les $x_p$ soient des entiers ($p$-adiques).

**XVIII1.** Si $k$ est un corps de nombres, on a pour toute place $v$ de $k$ une injection canonique $k \to k_v$. Le produit de ces injections sur toutes les places de $k$ détermine une injection canonique $\varphi\colon k \to \prod_v k_v$. Montrer que l'image de cette injection est incluse dans $k_{\mathbb{A}}$ (autrement dit, montrer que pour tout élément $x$ de $k$, pour presque toute place finie $v$ de $k$, $x$, considéré comme élément de $k_v$, est un entier). Montrer que $\varphi(k)$ est discret dans $k_{\mathbb{A}}$ et que $k_{\mathbb{A}}/\varphi(k)$ est compact. (On pourra tout d'abord le montrer pour $k = \mathbb{Q}$.)

**XVIII2.** On reprend les définitions, notations et résultats de l'exercice précédent ($\varphi$ est l'injection canonique de $k$ dans $k_{\mathbb{A}}$). Soit $k$ un corps de nombres et $\chi$ un caractère non trivial sur $k_{\mathbb{A}}$ (c'est-à-dire un morphisme continu non constant du groupe additif de $k_{\mathbb{A}}$ dans le groupe des nombres complexes de module 1) trivial sur $\varphi(k)$ (i.e. $\chi\varphi(x) = 1$ pour tout $x \in k$). Soit $k_{\mathbb{A}}^*$ le dual topologique de $k_{\mathbb{A}}$ (i.e. le groupe des caractères sur $k_{\mathbb{A}}$, l'addition étant définie par $\langle e, e_1^* + e_2^*\rangle = \langle e, e_1^*\rangle\langle e, e_2^*\rangle$, en notant $\langle e, e^*\rangle$ la valeur du caractère $e^*$ en $e$). Montrer que l'application $a \mapsto a^*$ de $k_{\mathbb{A}}$ vers $k_{\mathbb{A}}^*$ définie par

$$\langle e, a^*\rangle = \chi(ae)$$

est un isomorphisme, et que de plus si $a$ est tel que $\langle e, a^*\rangle$ pour tout $e \in \varphi(k)$ (i.e. que $a^*$ est trivial sur $\varphi(k)$), alors $a \in \varphi(k)$.

### XIX. Srinivasa Ramanujan.

**XIX1.** Montrer que $e^{\pi\sqrt{163}}$ est proche d'un entier (à savoir $640320^3 + 744$). On pourra pour cela utiliser le fait que l'anneau des entiers de $\mathbb{Q}(\sqrt{-163})$ est principal.

**XIX2.** Montrer que

$$\cfrac{1}{1+\cfrac{e^{-2\pi\sqrt{5}}}{1+\cfrac{e^{-4\pi\sqrt{5}}}{1+\cfrac{e^{-6\pi\sqrt{5}}}{1+\ddots}}}} = \left(\frac{\sqrt{5}}{1+\sqrt[5]{5^{3/4}\left(\frac{\sqrt{5}-1}{2}\right)^{5/2}-1}} - \frac{\sqrt{5}+1}{2}\right)e^{2\pi/\sqrt{5}}$$

**XIX3.** On appelle $\tau(n)$ le coefficient de $x^n$ dans le produit infini

$$x\prod_{k=1}^{\infty}(1-x^k)^{24}$$

Montrer que $\tau(n)$ est multiplicative. Montrer que $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ où $\sigma_{11}(n)$ est la somme des puissances 11-ièmes des diviseurs de $n$, que $7 \mid \tau(n)$ si $\left(\frac{n}{7}\right) = -1$ et que $23 \mid \tau(n)$ si $\left(\frac{n}{23}\right) = -1$.

**XX. Topologie différentielle.**

Si $U$ est un ouvert de $\mathbb{R}^m$ et $f: U \to \mathbb{R}^n$ une application de classe $C^\infty$, on dit que $x \in U$ est un point régulier ssi la différentielle de $f$ en $x$ est surjective (i.e. ssi $f$ est submersive en $x$). Dans le cas contraire, on dit que $x$ est un point singulier. On dit que $y \in \mathbb{R}^n$ est une valeur singulière ss'il existe un point singulier $x \in U$ tel que $f(x) = y$. Dans le cas contraire (notamment si $y$ n'est pas dans l'image de $f$) on dit que $y$ est une valeur régulière).

**XX1.** Soit $f: U \to \mathbb{R}^n$ de classe $C^\infty$ avec $U$ un ouvert de $\mathbb{R}^m$. Montrer qu'il existe une valeur régulière de $f$. Ce résultat est une forme faible du théorème de Morse-Sard. (On notera d'ailleurs que l'hypothèse faite sur la classe de $f$ peut être remplacée par $C^r$ avec $r > \min(0, m-n)$, mais pas par $C^1$ par exemple : Whitney a montré l'existence d'une application $C^1$ de $\mathbb{R}^2$ sur $\mathbb{R}$ pour laquelle tout point de $\mathbb{R}$ est valeur critique.)

**XX2.** En utilisant le résultat de l'exercice précédent, à savoir l'existence, pour toute application $f: U \to \mathbb{R}^n$ de classe $C^\infty$, d'une valeur régulière, montrer qu'il n'existe pas d'application $f: D^2 \to S^1$ de classe $C^\infty$ et égale à l'identité sur $S^1$ (où $D^2$ est l'ensemble des vecteurs de $\mathbb{R}^2$ de norme $\leq 1$ et $S^1$ l'ensemble des vecteurs de $\mathbb{R}^2$ de norme 1) ; on pourra pour cela définir un sens au terme de "valeur régulière" de $f$ en utilisant des projections stéréographiques (ou d'autres difféomorphismes soigneusement choisis) entre des parties de $S^1$ et $\mathbb{R}$, et pour une telle valeur régulière $y \in S^1$, montrer que $f^{-1}(\{y\}) \cap S^1$ doit avoir un nombre pair de points, ce qui est une contradiction car $f^{-1}(\{y\}) \cap S^1 = \{y\}$. En déduire, par un théorème d'approximation convenablement choisi, qu'il n'existe pas d'application $\varphi: D^2 \to S^1$ continue et égale à l'identité sur $S^1$. En déduire enfin le théorème du point fixe de Brouwer (toute application continue $\lambda: D^2 \to D^2$ possède un point fixe).

**XX3.** Soit $P$ un polynôme non constant à coefficients complexes. On identifie $\mathbb{C}$ à $\mathbb{R}^2$. Pour $y \in \mathbb{R}^2$, on note $\sharp P^{-1}(y)$ le cardinal de $P^{-1}(\{y\})$ l'ensemble des antécédents de $y$ par $P$. Montrer, par des arguments de compacité, que ce cardinal est toujours fini. Montrer que, si $R \subseteq \mathbb{R}^2$ désigne l'ensemble des valeurs régulières de $P$, $\sharp P^{-1}$ est continu sur $R$ (i.e. localement constant : pour tout point $y$ de $R$ il existe un voisinage $U$ de $y$ tel que si $y' \in U \cap R$, $\sharp P^{-1}(y') = \sharp P^{-1}(y)$). En déduire, par un argument de connexité, le théorème de d'Alembert-Gauss : $P$ est surjectif.

**XXI. Eléments de géométrie algébrique.**

Soit $k$ un corps algébriquement clos, que l'on pourra pour simplifier les choses supposer indénombrable.

Si $I$ est un idéal de $k[X_1, \ldots, X_n]$, on notera

$$V(I) = \{(x_1, \ldots, x_n) \in k^n : \forall P \in I(P(x_1, \ldots, x_n) = 0)\}$$

Si $I$ est un idéal principal engendré par un polynôme $P$, on notera $V(P)$ pour $V(I)$.

A l'inverse, si $V$ est une partie de $k^n$, on notera

$$I(V) = \{P \in k[X_1, \ldots, X_n] : \forall (x_1, \ldots, x_n) \in V(P(x_1, \ldots, x_n) = 0)\}$$

Il est clair que $I(V)$ est un idéal de $k[X_1, \ldots, X_n]$. De plus, cet idéal est radical, c'est-à-dire que si $P^r \in I(V)$ (avec $r \in \mathbb{N}^*$) alors $P \in I(V)$.

De manière générale, si $I$ est un idéal de $k[X_1, \ldots, X_n]$, on définie sa racine par $\sqrt{I} = \{P : \exists r \in \mathbb{N}^*(P^r \in I)\}$ : on vérifie immédiatement que c'est un idéal radical.

**XXI1.** Démontrer le résultat suivant : si $I$ est un idéal propre de $k[X_1, \ldots, X_n]$ alors $V(I)$ est non vide. Pour y arriver, on pourra (si on suppose $k$ indénombrable) tout d'abord montrer qu'une extension de dimension au plus dénombrable d'un corps indénombrable algébriquement clos, est triviale.

**XXI2.** En utilisant le résultat de l'exercice précédent, montrer que si $I$ est un idéal quelconque de $k[X_1, \ldots, X_n]$ alors $I(V(I)) = \sqrt{I}$. On pourra, pour $F \in I(V(I))$, introduire l'anneau $R_F$ dit "localisé de $k[X_1, \ldots, X_n]$ en $F$, qui n'est autre que l'ensemble des éléments du corps des fractions de $k[X_1, \ldots, X_n]$ qui s'écrivent $P/F^r$ avec $P \in [X_1, \ldots, X_n]$ et $r \in \mathbb{N}^*$ : en autres mots, c'est l'anneau $k[X_1, \ldots, X_n, T]/(1 - TF)$. Ce résultat est connu sous le nom de Nullstellensatz, et il est dû à David Hilbert.

**XXI3.** On se donne deux polynômes $P$ et $Q$ de $k[X, Y]$ premiers entre eux et sans facteur commun : montrer que $V(P) \cap V(Q)$ est fini. Pour cela, on pourra montrer l'existence de polynômes à une seule variable $f \in k[X]$ et $g \in k[Y]$ appartenant à l'idéal engendré par $P$ et $Q$ (lorsqu'on identifie $f$ et $g$ à des polynômes à deux variables).

### XXII. Divers agrégation.

**XXII1.** Montrer que tous les automorphismes de $\mathcal{S}_n$ (le groupe symétrique à $n$ éléments) sont intérieurs, sauf pour $n = 6$.

**XXII2.** Montrer que l'anneau $\mathbb{Z}[(1 + i\sqrt{19})/2]$ est principal mais n'est pas euclidien.

**XXII3.** Soit $K$ un carré fermé (y compris les points intérieurs) de sommets $ABCD$ (dans le sens trigonométrique) dans le plan euclidien. Montrer qu'il existe deux parties $U$ et $V$ de $K$ connexes telles que $U \cap V = \emptyset$, $U \cup V = K$, $A \in U$, $B \in V$, $C \in U$ et $D \in V$. Montrer que si $\gamma$ et $\gamma'$ sont deux arcs continus, $\gamma$ allant de $A$ à $C$ et $\gamma'$ allant de $B$ à $D$, alors il existe un point appartenant à l'immage de $\gamma$ et à l'image de $\gamma'$.

**XXII4.** Soit $K$ un espace métrique compact, et $f\colon K \to K$ une application telle que $d(f(x), f(y)) < d(x, y)$ pour tout couple $(x, y)$ de points distincts de $K$. Montrer que $f$ admet un point fixe unique.

On suppose à présent que $f$ vérifie $d(f(x), f(y)) \geq d(x, y)$ pour tout couple $(x, y)$ de points de $K$ ($K$ étant toujours un espace métrique compact). Montrer que $f$ est bijective, et qu'elle est une isométrie.

**XXII5.** Soit $\rho_n$ une suite de réels positifs, et $\alpha_n$ une suite de réels. On pose $A_n(x) = \rho_n \cos(nx + \alpha_n)$. On suppose qu'il existe un ensemble $E$ de mesure finie non nulle (voir section X) tel que $A_n(x) \to 0$ si $x \in E$. Montrer que $\rho_n$ tend vers 0.

**XXII6.** Soit $(\Sigma a_n)$ une série telle que $|a_n| \leq M/n$ pour tout $n$ (où $M$ est un certain réel positif). On suppose de plus que $(\Sigma a_n)$ est sommable de somme $S$ au sens de Cesàro (i.e. la suite $S_n = \frac{s_1+\ldots+s_n}{n}$ où $s_n = a_1 + \ldots + a_n$, converge vers $S$). Montrer alors que $(\Sigma a_n)$ converge et a pour somme $S$. (Ce résultat est dû à Godfrey Harold Hardy.)

**XXII7.** Soit $P$ un polynôme à coefficients complexes. Montrer que l'ensemble des zéros complexes de $P'$ est inclus dans l'enveloppe convexe de l'ensemble des zéros de $P$.

**XXII8.** Soit $f$ une fonction continue sur $\{z \in \mathbb{C}\colon \Im z \geq 0\}$, holomorphe sur $\{z \in \mathbb{C}\colon \Im z > 0\}$, et réelle sur $\mathbb{R}$. Montrer que $f$ se prolonge en une fonction holomorphe sur $\mathbb{C}$.

**XXII9.** Soit $K$ un compact de $\mathbb{C}$ et $f\colon K \to \mathbb{C}$ une fonction continue sur $K$ et holomorphe sur $K^\circ$ (l'intérieur de $K$). Montrer que si le complémentaire de $K$ est connexe, alors pour tout $\varepsilon > 0$ il existe un polynôme $P$ tel que $|f(z) - P(z)| < \varepsilon$ pour tout $x \in K$. (Cet exercice est difficile.) Donner un contre-exemple dans le cas où le complémentaire de $K$ n'est pas connexe. Ce résultat est connu sous le nom de théorème de Mergelyan.