

Devoir Surveillé N°4

Structures-Arithmétique

Fonctions Réelles

Durée : 4 heures

Problème 1 : Entiers somme de deux carrés

L'objectif de ce problème est de déterminer quels sont les entiers naturels qui sont somme de deux carrés.

Notations :

$\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{C}$ désignent respectivement les ensembles des entiers naturels, des entiers relatifs et des nombres complexes.

On pose $\mathbb{Z}[i] = \{a + ib / a \in \mathbb{Z}, b \in \mathbb{Z}\} \subset \mathbb{C}$ et $\mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$.

Pour $z \in \mathbb{C}$, on pose $N(z) = z\bar{z}$.

Partie I : Présentation de l'anneau de $\mathbb{Z}[i]$

1. Présentation de l'anneau $\mathbb{Z}[i]$.
 - 1.a Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ muni de l'addition et de la multiplication usuelles.
 - 1.b Etablir que pour tout $u, v \in \mathbb{Z}[i]$, $N(uv) = N(u)N(v)$ et que pour tout $u \in \mathbb{Z}[i]$, $N(u) \in \mathbb{N}$.
 - 1.c Un élément $u \in \mathbb{Z}[i]$ est dit inversible ssi il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
Montrer que si u est inversible alors $N(u) = 1$.
Déterminer alors l'ensemble, noté U , des éléments inversibles de $\mathbb{Z}[i]$.
2. Divisibilité dans l'anneau $\mathbb{Z}[i]$.
Soit $u, v \in \mathbb{Z}[i]$. On dit que u divise v dans $\mathbb{Z}[i]$, et on note $u \mid v$, ssi il existe $s \in \mathbb{Z}[i]$ tel que $v = su$.
 - 2.a Soit $u, v, w \in \mathbb{Z}[i]$. Etablir l'implication que si $u \mid v$ et $v \mid w$ alors $u \mid w$.
 - 2.b Soit $u, v \in \mathbb{Z}[i]$. Etablir que si $u \mid v$ et $v \mid u$ alors $u = \pm v$ ou $\pm iv$.
 - 2.c Soit $u, v \in \mathbb{Z}[i]$. Montrer que si u divise v alors $N(u)$ divise $N(v)$ dans $\mathbb{Z}$.
 - 2.d Déterminer les diviseurs de $1+i$, puis de $1+3i$ dans $\mathbb{Z}[i]$.
3. Division euclidienne dans $\mathbb{Z}[i]$.
 - 3.a Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[i]$ tel que $N(u-z) < 1$.
Ce u est-il unique ?
 - 3.b Montrer que pour tout $u \in \mathbb{Z}[i]$ et tout $v \in \mathbb{Z}[i]^*$, il existe $(q, r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ tel que :
 $u = vq + r$ avec $N(r) < N(v)$.
On pourra utiliser la division dans $\mathbb{C}$.

Partie II : Arithmétique dans $\mathbb{Z}[i]$

1. Soit $\delta \in \mathbb{Z}[i]$. On note $\delta\mathbb{Z}[i] = \{\delta u / u \in \mathbb{Z}[i]\}$.
Montrer que $\delta\mathbb{Z}[i]$ est un sous-groupe additif de $\mathbb{Z}[i]$.
2. Soit $u, v \in \mathbb{Z}[i]$ avec $u \neq 0$ ou $v \neq 0$. On note $I(u, v) = \{uz + vz' / z, z' \in \mathbb{Z}[i]\}$.
 - 2.a Observer que u et v appartiennent à l'ensemble $I(u, v)$.
 - 2.b Montrer que l'ensemble $A = \{N(w) / w \in I(u, v) \setminus \{0\}\}$ possède un plus petit élément $d > 0$.
 - 2.c Soit δ un élément de $I(u, v)$ tel que $N(\delta) = d$. Etablir que $I(u, v) = \delta\mathbb{Z}[i]$.
On pourra exploiter la division euclidienne présentée en I.3b.

- 2.d Montrer que δ divise u et v puis que pour tout $w \in \mathbb{Z}[i]$, on a l'équivalence : $(w|u \text{ et } w|v) \Leftrightarrow w|\delta$.
On dit que δ est un pgcd de u et v .
3. Soit $u, v \in \mathbb{Z}[i]$ avec $u \neq 0$ ou $v \neq 0$.
On dit que u et v sont premiers entre eux ssi le nombre δ défini en II.2.d appartient à $\{\pm 1, \pm i\}$.
Dans les questions 3.a et 3.b, on suppose que u et v sont premiers entre eux.
- 3.a Justifier qu'il existe $z, z' \in \mathbb{Z}[i]$ tel que $1 = uz + vz'$
- 3.b Soit $w \in \mathbb{Z}[i]$. Montrer que si u divise vw alors u divise w .
4. Soit $u \in \mathbb{Z}[i] - \{0, \pm 1, \pm i\}$.
On dit que u est irréductible ssi ses seuls diviseurs sont $\pm 1, \pm i, \pm u$ et $\pm iu$.
- 4.a Soit $v \in \mathbb{Z}[i]$. On suppose que u irréductible et ne divise pas v .
Montrer que u et v sont premiers entre eux.
- 4.b Soit $v, w \in \mathbb{Z}[i]$. On suppose que u est irréductible et divise vw .
Montrer que u divise v ou divise w .

Partie III : Nombres somme de deux carrés

1. On note $\Sigma = \{a^2 + b^2 / a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
- 1.a Montrer que $n \in \Sigma \Leftrightarrow \exists u \in \mathbb{Z}[i], n = N(u)$.
- 1.b En déduire que si $n, n' \in \Sigma$ alors $nn' \in \Sigma$.
2. p désigne un nombre premier strictement supérieur à 2.
- 2.a Montrer que $p \in \Sigma \Rightarrow p \equiv 1$ modulo 4.
Nous admettons que l'implication réciproque est vraie (quoique loin d'être immédiate).
Ainsi $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, ... sont des éléments de Σ .
- 2.b Montrer que si p n'est pas irréductible alors $p \in \Sigma$.
3. Soit $a, b \in \mathbb{Z}$ et $n = a^2 + b^2 \in \Sigma$. Soit $p \equiv 3$ modulo 4, un nombre premier diviseur de n .
- 3.a Montrer que $p|a + ib$ dans $\mathbb{Z}[i]$.
- 3.b En déduire que p^2 divise n .
4. Etablir que les entiers naturels non nuls appartenant à Σ sont les nombres de la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ avec $p_1, p_2, \dots, p_N$ nombres premiers deux à deux distincts et $\alpha_1, \alpha_2, \dots, \alpha_N$ entiers naturels tels que :
 $\forall 1 \leq i \leq N, p_i \equiv 3 \text{ modulo } 4 \Rightarrow \alpha_i \text{ est pair.}$

Problème 2 : Etude d'une équation fonctionnelle

Thèmes abordés : Continuité et dérivabilité des fonctions numériques.

Les parties I et II sont entièrement indépendantes.

En dehors de la dernière question, la partie III est indépendante de la partie II.

Dans tout le problème : on considère la fonction $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ définie par $\varphi(x) = \frac{e^{2x} - 1}{e^{2x} + 1}$.

Partie I : Etude de la fonction φ

- 1.a Etudier la parité de φ .
- 1.b Etudier les variations de φ sur $\mathbb{R}$ et préciser ses branches infinies en $+\infty$ et $-\infty$.
- 1.c Donner l'allure de la courbe représentative de φ .
- 2.a Justifier que φ est une bijection de $\mathbb{R}$ sur un intervalle I de $\mathbb{R}$ à préciser.
- 2.b Observer que pour tout $x \in \mathbb{R}$: $\varphi'(x) = 1 - \varphi^2(x)$.
- 2.c Montrer que $\varphi^{-1} : I \rightarrow \mathbb{R}$ est dérivable et exprimer simplement sa dérivée.

Partie II : Etude d'une première équation fonctionnelle

Le but de cette partie est de déterminer les fonctions $f : \mathbb{R} \rightarrow \mathbb{R}$ dérivables en 0 vérifiant :

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

On considère f une fonction solution.

1. Calculer $f(0)$.
2. Soit $x \in \mathbb{R}^*$. On définit une suite réelle (u_n) par : $\forall n \in \mathbb{N}, u_n = \frac{f\left(\frac{x}{2^n}\right)}{\frac{x}{2^n}}$.
- 2.a Montrer que (u_n) converge et exprimer sa limite.
- 2.b Exprimer u_{n+1} en fonction de u_n .
3. Conclure qu'il existe $\alpha \in \mathbb{R}$ tel que $\forall x \in \mathbb{R}, f(x) = \alpha x$.

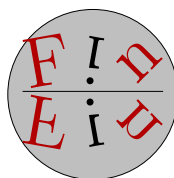
Partie III : Etude d'une seconde équation fonctionnelle

Le but de cette partie est de déterminer les fonctions $f : \mathbb{R} \rightarrow \mathbb{R}$ dérivable en 0 vérifiant :

$$\forall x \in \mathbb{R}, f(2x) = \frac{2f(x)}{1 + (f(x))^2}.$$

1. Montrer que φ est solution du problème posé.
2. On considère dans cette question f une solution du problème posé.
- 2.a Déterminer les valeurs possibles de $f(0)$.
- 2.b Montrer que $-f$ est aussi solution

- 2.c Montrer que $\forall x \in \mathbb{R}, -1 \leq f(x) \leq 1$.
(indice : on pourra exprimer $f(x)$ en fonction de $f\left(\frac{x}{2}\right)$).
3. On suppose dans cette question que f est solution du problème posé et que $f(0) = 1$.
On considère $x \in \mathbb{R}$ et l'on définit la suite (u_n) par $\forall n \in \mathbb{N}, u_n = f\left(\frac{x}{2^n}\right)$.
- 3.a Montrer que la suite (u_n) est convergente et préciser sa limite.
- 3.b Etablir une relation entre u_n et u_{n+1} .
- 3.c En déduire que la suite (u_n) garde un signe constant et préciser celui-ci.
- 3.d Etudier la monotonie de la suite (u_n) et en déduire que celle-ci est constante égale à 1.
- 3.e Qu'en déduire quant à la fonction f ?
- 3.f Que peut-on dire si l'hypothèse « $f(0) = 1$ » est remplacée par « $f(0) = -1$ » ?
4. On suppose dans cette question que f est solution du problème posé et que $f(0) = 0$.
- 4.a En raisonnant par l'absurde et en considérant une suite du même type que ci-dessus, montrer que $\forall x \in \mathbb{R}, f(x) \neq 1$ et $f(x) \neq -1$.
- 4.b On introduit la fonction $g : \mathbb{R} \rightarrow \mathbb{R}$ définie par $g(x) = \varphi^{-1}(f(x))$.
Montrer que $\forall x \in \mathbb{R}, g(2x) = 2g(x)$ et que g est dérivable en 0.
- 4.c En déduire une expression de $f(x)$ dépendant d'un paramètre $\alpha \in \mathbb{R}$.



Correction Problème 1 :

Partie I

- 1.a $\mathbb{Z}[i] \subset \mathbb{C}$, $1 = 1 + 0i \in \mathbb{Z}[i]$ et $\forall u, v \in \mathbb{Z}[i]$, on peut écrire $u = a + ib$, $v = c + id$ avec $a, b, c, d \in \mathbb{Z}$.
On a $u - v = (a - c) + i(b - d) \in \mathbb{Z}[i]$ (car $a - c, b - d \in \mathbb{Z}$),
et $uv = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$ car $ac - bd, ad + bc \in \mathbb{Z}$.
Ainsi $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$.
- 1.b $\forall u, v \in \mathbb{Z}[i]$, $N(uv) = \overline{uvuv} = \overline{u} \overline{v} v \overline{u} = N(u)N(v)$
 $\forall u \in \mathbb{Z}[i]$, on peut écrire $u = a + ib$ avec $a, b \in \mathbb{Z}$ donc $N(u) = u\overline{u} = a^2 + b^2 \in \mathbb{N}$.
- 1.c Supposons $u \in \mathbb{Z}[i]$ inversible et introduisons $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
On a $N(uv) = N(1) = 1$ et $N(uv) = N(u)N(v)$ donc $N(u)N(v) = 1$ avec $N(u), N(v) \in \mathbb{N}$.
Par suite $N(u) = N(v) = 1$.
On peut écrire $u = a + ib$ avec $a, b \in \mathbb{Z}$.
 $N(u) = a^2 + b^2 = 1$ donne $(a, b) = (1, 0), (-1, 0), (0, 1)$ ou $(0, -1)$ donc $u = \pm 1$ ou $u = \pm i$.
Inversement, ses éléments sont inversibles car $1 \times 1 = 1$, $(-1) \times (-1) = 1$, $i \times (-i) = 1$ et $(-i) \times i = 1$.
 $U = \{1, i, -1, -i\}$.
- 2.a Si $u \mid v$ et $v \mid w$ alors il existe $s, t \in \mathbb{Z}[i]$ tel que $v = su$ et $w = tv$.
On a alors $w = (st)u$ avec $st \in \mathbb{Z}[i]$ et par suite $u \mid w$.
- 2.b Si $u \mid v$ et $v \mid u$ alors il existe $s, t \in \mathbb{Z}[i]$ tel que $v = su$ et $u = tv$.
Par suite $u = (ts)u$.
Si $u \neq 0$, on obtient $ts = 1$ donc t est inversible et alors $t = \pm 1$ ou $t = \pm i$.
Par suite $u = \pm v$ ou $u = \pm iv$.
Si $u = 0$ alors $v = su = u$ et donc $u = v$.
- 2.c Si $u \mid v$ alors il existe $s \in \mathbb{Z}[i]$ tel que $v = su$. On a alors $N(v) = N(su) = N(s)N(u)$ avec $N(s) \in \mathbb{N}$ donc $N(u) \mid N(v)$.
- 2.d $N(1+i) = 2$ et $\text{Div}(2) \cap \mathbb{N} = \{1, 2\}$.
Si u divise $1+i$ alors $N(u) = 1$ ou $N(u) = 2$.
Si $N(u) = 1$ alors $u = \pm 1$ ou $u = \pm i$.
Si $N(u) = 2$ alors $u = 1+i, 1-i, -1+i$ ou $-1-i$.
Inversement, les nombres proposés sont diviseurs de $1+i$.
 $N(1+3i) = 10$ et $\text{Div}(10) \cap \mathbb{N} = \{1, 2, 5, 10\}$.
Si $N(u) = 1$ alors $u = \pm 1$ ou $u = \pm i$.
Si $N(u) = 2$ alors $u = 1+i, 1-i, -1+i$ ou $-1-i$.
Si $N(u) = 5$ alors $u = 1+2i, 1-2i, -2+i$ ou $-2-i$.
Si $N(u) = 10$ alors $u = 1+3i, 1-3i, -3+i$ ou $-3-i$.
Inversement, les nombres proposés sont diviseurs de $1+3i$.
- 3.a Soit a et b les entiers respectivement les plus proches de $\text{Re}(z)$ et $\text{Im}(z)$.
Pour $u = a + ib \in \mathbb{Z}[i]$, on a $N(u - v) = (a - \text{Re}(z))^2 + (b - \text{Im}(z))^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1$.
Il n'y a pas unicité de u . Par exemple, pour $z = \frac{1+i}{2}$, les quatre complexes $0, 1, i$ et $1+i$ conviennent.

3.b Soit $q \in \mathbb{Z}[i]$ tel que $N\left(q - \frac{u}{v}\right) < 1$ et $r = u - vq \in \mathbb{Z}[i]$.

On a $u = vq + r$ et $N(r) = N(u - vq) = N(v)N\left(\frac{u}{v} - q\right) < N(v)$ (sachant $N(v) > 0$).

Partie II

1. $\delta\mathbb{Z}[i] \subset \mathbb{Z}[i]$. $0 = \delta \cdot 0 \in \delta\mathbb{Z}[i]$. $\forall x, y \in \delta\mathbb{Z}[i]$, on peut écrire $x = \delta u$ et $y = \delta v$ avec $u, v \in \mathbb{Z}[i]$.

On a $x - y = \delta(u - v) \in \delta\mathbb{Z}[i]$ car $u - v \in \mathbb{Z}[i]$. Ainsi $\delta\mathbb{Z}[i]$ est un sous groupe de $(\mathbb{Z}[i], +)$.

2.a $u = u \cdot 1 + v \cdot 0 \in I(u, v)$ et $v = u \cdot 0 + v \cdot 1 \in I(u, v)$.

2.b $A = \{N(w) / w \in I(u, v) \setminus \{0\}\}$ est une partie de $\mathbb{Z}$, minorée par 1 et non vide car $N(u)$ ou $N(v)$ appartient à cet ensemble (selon que $u \neq 0$ ou $v \neq 0$). Par suite A possède un plus petit élément $d > 0$.

2.c $\delta \in I(u, v)$ donc on peut écrire $\delta = u\xi + v\xi'$ avec $\xi, \xi' \in \mathbb{Z}[i]$.

$\forall x \in \delta\mathbb{Z}[i]$, on peut écrire $x = \delta y$ avec $y \in \mathbb{Z}[i]$.

On a alors $x = u(\delta\xi) + v(\delta\xi') \in I(u, v)$. Ainsi $\delta\mathbb{Z}[i] \subset I(u, v)$.

Inversement, soit $x \in I(u, v)$. On peut écrire $x = uz + vz'$ avec $z, z' \in \mathbb{Z}[i]$.

Réalisons la division euclidienne de x par δ : $x = \delta q + r$ avec $N(r) < N(\delta)$.

Or $r = x - \delta q = u(z - \xi q) + v(z' - \xi' q) \in I(u, v)$ donc si $r \neq 0$, on a $N(r) \in A$. Ceci contredit la définition de $d = \min A$ car $N(r) < N(\delta) = d$. Nécessairement $r = 0$ et par suite $x \in \delta\mathbb{Z}[i]$.

2.d $u \in I(u, v) = \delta\mathbb{Z}[i]$ donc on peut écrire $u = \delta z$ avec $z \in \mathbb{Z}[i]$. Ainsi $\delta | u$. De même $\delta | v$.

Si $w | \delta$ alors $w | u$ et $w | v$ par transitivité de la divisibilité.

Inversement si $w | u$ et $w | v$ alors on peut écrire $u = ws$ et $v = wt$ avec $s, t \in \mathbb{Z}[i]$ et donc l'écriture $\delta = u\xi + v\xi'$ avec $\xi, \xi' \in \mathbb{Z}[i]$ introduite ci-dessus donne $\delta = w(s\xi + t\xi')$. Ainsi $w | \delta$.

3.a $I(u, v) = \delta\mathbb{Z}[i] = \mathbb{Z}[i]$ car $\delta \in \{\pm 1, \pm i\}$.

Or $1 \in \mathbb{Z}[i]$ donc $1 \in I(u, v)$ et par suite $\exists z, z' \in \mathbb{Z}[i]$ tels que $1 = uz + vz'$.

3.b Supposons $u | vw$. On a $w = w \times 1 = uwz + vwz'$, or $u | uwz$ et $u | vwz'$ donc sans difficultés $u | w$.

4.a Posons δ un pgcd de u et v . δ est un diviseur de l'élément irréductible u .

Si $\delta = \pm u$ ou $\delta = \pm iu$ alors, puisque $\delta | v$, $u | v$. Ceci est exclu.

Il reste $\delta = \pm 1$ ou $\delta = \pm i$ et donc u et v sont premiers entre eux.

4.b Si u divise v : ok

Sinon, u est premier avec v et donc puisque $u | vw$ on a $u | w$ en vertu de II.3b.

Partie III

1.a Si $n \in \Sigma$ alors on peut écrire $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$ et alors $n = N(u)$ avec $u = a + ib \in \mathbb{Z}[i]$.

Inversement, si $n = N(u)$ avec $u \in \mathbb{Z}[i]$, alors on peut écrire $u = a + ib$ avec $a, b \in \mathbb{Z}$ et on a $N(u) = a^2 + b^2 \in \Sigma$.

1.b Si $n, n' \in \Sigma$ alors on peut écrire $n = N(u)$ et $n' = N(v)$ avec $u, v \in \mathbb{Z}[i]$.

On a alors $nn' = N(u)N(v) = N(uv)$ avec $uv \in \mathbb{Z}[i]$ donc $nn' \in \Sigma$.

2.a Puisque p est premier et strictement supérieur à 2, il n'est pas divisible par 2.

Par suite $p \equiv 1$ ou $p \equiv 3$ modulo 4.

Puisque $p \in \Sigma$, on peut écrire $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$.

Or les seuls valeurs possibles de a^2 modulo 4 sont 0 ou 1 donc $p = 0, 1$ ou 2 modulo 4.

Compte tenu de ce qui précède, il reste $p \equiv 1$ modulo 4.

- 2.b Si p n'est pas irréductible alors on peut écrire $p = uv$ avec $u, v \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$.
On a alors $p^2 = N(p) = N(u)N(v)$. Puisque $N(u) \neq 1$, $N(v) \neq 1$ et p premier, on a $N(u) = N(v) = p$ et donc $p \in \Sigma$.
- 3.a Puisque $p \equiv 3$ modulo 4, p n'appartient pas à Σ (via III.2a) et donc p est irréductible (via III.2b)
On a $p \mid a^2 + b^2 = (a + ib)(a - ib)$ or p est irréductible donc $p \mid (a + ib)$ ou $p \mid (a - ib)$.
Or il est clair que $p \mid z \Rightarrow p \mid \bar{z}$, donc $p \mid (a + ib)$ et $p \mid (a - ib)$.
- 3.b Suite à ce qui précède $p^2 \mid (a + ib)(a - ib) = n$.
Cette dernière divisibilité a lieu a priori dans $\mathbb{Z}[i]$, mais puisque n/p^2 est le rapport de deux entiers, sera un entier et donc la divisibilité a lieu dans $\mathbb{Z}$.
4. Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ de la forme proposée. $\forall 1 \leq i \leq N$:
Si $p_i = 2$ ou $p_i \equiv 1$ modulo 4 alors $p_i \in \Sigma$ (car $2 = 1^2 + 1^2$ et par la réciproque admise en III.2a)
Par suite $p_i^{\alpha_i} \in \Sigma$ car Σ est stable par produit (III.1.b)
Si $p_i \equiv 3$ modulo 4 alors $\alpha_i = 2\beta_i$ et $p_i^{\alpha_i} = p_i^{2\beta_i} = (p_i^2)^{\beta_i} \in \Sigma$ car $p_i^2 = p_i^2 + 0^2 \in \Sigma$.
Puisque tous les $p_1^{\alpha_1}, \dots, p_N^{\alpha_N}$ appartiennent à Σ , $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ appartient à Σ .
Inversement : Soit $n \in \Sigma \cap \mathbb{N}^*$. Si $n = 1$, n est de la forme voulue.
Si $n \geq 2$, introduisons sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$.
Pour tout $1 \leq i \leq N$ tel que $p_i \equiv 3$ modulo 4.
Si $\alpha_i = 0$ alors α_i est pair.
Si $\alpha_i > 0$ alors $p_i \mid n$. Écrivons $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$.
Comme vu en III.3a, on a $p_i \mid (a + ib)$ ce qui permet d'écrire $a + ib = p_i(c + id)$.
On a alors $n = p_i^2(c^2 + d^2) = p_i^2 n'$ avec $n' = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i - 2} \dots p_N^{\alpha_N} \in \Sigma$.
On peut alors reprendre la démarche avec n' et, champagne !, α_i est pair.

Correction Problème 2 :

Partie I

1.a $\forall x \in \mathbb{R}, -x \in \mathbb{R}$ et $\varphi(-x) = \frac{e^{-2x} - 1}{e^{-2x} + 1} = \frac{1 - e^{2x}}{1 + e^{2x}} = -\varphi(x)$, φ est impaire.

1.b φ est C^∞ et $\varphi'(x) = \left(1 - \frac{2}{e^{2x} + 1}\right)' = \frac{4e^{2x}}{(e^{2x} + 1)^2} > 0$.

φ est donc strictement croissante sur $\mathbb{R}$.

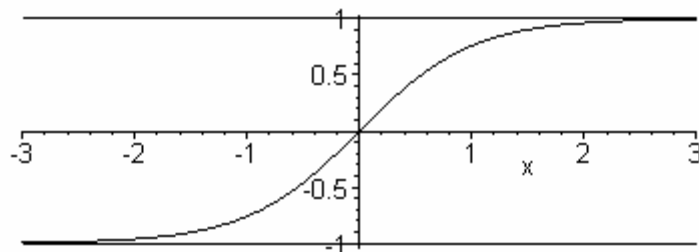
Quand $x \rightarrow +\infty$, $\varphi(x) \sim \frac{e^{2x}}{e^{2x}} \rightarrow 1$ donc $\lim_{x \rightarrow +\infty} \varphi(x) = 1$.

La droite d'équation $y = 1$ est asymptote φ en $+\infty$.

Puisque $1 - \varphi(x) = \frac{2}{e^{2x} + 1} > 0$, Γ_φ est en dessous de cette asymptote.

Par imparité, la droite d'équation $y = -1$ est asymptote à φ en $+\infty$ avec Γ_φ au dessus de cette asymptote.

1.c



2.a φ est continue et strictement croissante sur $\mathbb{R}$ donc φ réalise une bijection de $\mathbb{R}$ sur

$$I = \left] \lim_{-\infty} \varphi, \lim_{+\infty} \varphi \right[=]-1, 1[.$$

2.b $\varphi'(x) = \frac{4e^{2x}}{(e^{2x} + 1)^2}$ et $1 - \varphi^2(x) = 1 - \frac{e^{4x} - 2e^{2x} + 1}{e^{4x} + 2e^{2x} + 1} = \frac{4e^{2x}}{(e^{2x} + 1)^2}$.

2.c Puisque φ est dérivable sur $\mathbb{R}$ et $\forall x \in \mathbb{R}, \varphi'(x) \neq 0$ on peut affirmer que φ^{-1} est dérivable et de plus :

$$(\varphi^{-1})'(x) = \frac{1}{\varphi'(\varphi^{-1}(x))} = \frac{1}{1 - (\varphi(\varphi^{-1}(x)))^2} = \frac{1}{1 - x^2}.$$

Partie II

1. L'équation fonctionnelle pour $x = 0$ donne $f(0) = 2f(0)$ d'où $f(0) = 0$.

2.a $u_n = \frac{f(h) - f(0)}{h}$ avec $h = \frac{x}{2^n}$.

Quand $n \rightarrow +\infty$, on a $h \rightarrow 0$ et par composition $u_n \rightarrow f'(0)$.

2.b De part l'équation fonctionnelle : $f\left(\frac{x}{2^n}\right) = 2f\left(\frac{x}{2^{n+1}}\right)$. Donc $u_n = u_{n+1}$.

3. De part l'étude précédente : $u_0 = f'(0)$ et donc $\forall x \in \mathbb{R}^*, f(x) = \alpha x$ avec $\alpha = f'(0)$. De plus cette relation est encore vraie pour $x = 0$.

Partie III

1. φ est dérivable en 0 .

$$\forall x \in \mathbb{R}, \frac{2\varphi(x)}{1+\varphi^2(x)} = \frac{2(e^{2x}-1)(e^{2x}+1)}{(e^{2x}+1)^2 + (e^{2x}-1)^2} = \frac{e^{4x}-1}{e^{4x}+1} = \varphi(2x).$$

- 2.a L'équation fonctionnelle pour $x=0$ donne $f(0) = \frac{2f(0)}{1+f^2(0)}$ d'où

$$f(0)(f^2(0)-1)=0. \text{ Par suite } f(0)=0, 1 \text{ ou } -1.$$

- 2.b $-f$ est dérivable en 0 puisque f l'est.

$$\forall x \in \mathbb{R}, -f(2x) = -\frac{2f(x)}{1+(f(x))^2} = \frac{2(-f(x))}{1+(-f(x))^2}.$$

- 2.c $f(x) = \frac{2a}{1+a^2}$ avec $a = f(x/2)$. Or $(a-1)^2 \geq 0$ et $(a+1)^2 \geq 0$ donnent : $-(1+a^2) \leq 2a \leq (1+a^2)$ et par suite $-1 \leq f(x) \leq 1$.

- 3.a Quand $n \rightarrow +\infty$, on a $\frac{x}{2^n} \rightarrow 0$ et puisque f est continue en 0 (car dérivable en 0) on a

$$u_n = f\left(\frac{x}{2^n}\right) \rightarrow f(0) = 1.$$

- 3.b
$$u_n = f\left(\frac{x}{2^n}\right) = \frac{2f\left(\frac{x}{2^{n+1}}\right)}{1+\left(f\left(\frac{x}{2^{n+1}}\right)\right)^2} = \frac{2u_{n+1}}{1+u_{n+1}^2}.$$

- 3.c Par la relation ci-dessus :

$$(u_n \geq 0 \Rightarrow u_{n+1} \geq 0) \text{ et } (u_n \leq 0 \Rightarrow u_{n+1} \leq 0).$$

Par suite (u_n) est de signe constant et puisque $u_n \rightarrow 1$ on peut affirmer que la suite (u_n) est positive.

- 3.d
$$u_{n+1} - u_n = \frac{u_{n+1}(u_{n+1}^2 - 1)}{1 + u_{n+1}^2} \leq 0 \text{ car } u_{n+1} = f\left(\frac{x}{2^{n+1}}\right) \in [-1, 1].$$

Par suite (u_n) est décroissante.

$$(u_n) \text{ décroît vers } 1, \text{ donc } \forall n \in \mathbb{N}, u_n \geq 1.$$

$$\text{Or } u_n = f\left(\frac{x}{2^n}\right) \in [-1, 1] \text{ donc } \forall n \in \mathbb{N}, u_n = 1.$$

- 3.e Puisque $u_0 = 1$, on obtient $f(x) = 1$ et ceci pour tout $x \in \mathbb{R}^*$. Comme ceci est de plus vrai pour $x = 0$, f s'avère être constante égale à 1.

- 3.f Dans le cas où $f(0) = -1$, on applique l'étude ci-dessus à $-f$ pour conclure que f est constante égale à -1 .

- 4.a Supposons $\exists x \in \mathbb{R}$ tel que $f(x) = 1$.

$$\text{Considérons } (u_n) \text{ de terme général : } u_n = f\left(\frac{x}{2^n}\right).$$

$$\text{Comme ci-dessus } u_n = \frac{2u_{n+1}}{1+u_{n+1}^2}.$$

Par récurrence on montre alors $u_n = 1$.

Or $u_n \rightarrow f(0) = 0$, c'est absurde.

Par suite $\forall x \in \mathbb{R}, f(x) \neq 1$.

De même : $\forall x \in \mathbb{R}, f(x) \neq -1$.

4.b $\varphi(g(2x)) = f(2x) = \frac{2f(x)}{1+(f(x))^2}$ et $\varphi(2g(x)) = \frac{2\varphi(g(x))}{1+(\varphi(g(x)))^2} = \frac{2f(x)}{1+(f(x))^2}$.

L'application φ étant injective : $g(2x) = 2g(x)$.

De plus, par composition, γ est dérivable en 0.

4.c De part la partie II :

$\exists \alpha \in \mathbb{R}$ tel que $\forall x \in \mathbb{R}, g(x) = \alpha x$ et donc $f(x) = \varphi(\alpha x) = \frac{e^{2\alpha x} - 1}{e^{2\alpha x} + 1}$.