

On soignera la rédaction et on sera rigoureux et précis dans les raisonnements. Bien lire le sujet il y a des questions indépendantes. Dans le cas d'utilisation d'abréviations merci de les définir en 1ère page. (pas plus de 5) Je ne lis pas le crayon à papier les résultats doivent être soulignés.

La machine est interdite +1 point si votre rédaction est soignée, votre copie n'est pas sale et que la rédaction est correcte, -1 dans le cas contraire

Algèbre linéaire

Cette partie est très courte, il s'agit d'y passer le moins de temps possible.

Soit $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$
 $(x, y, z) \mapsto (y + 2z, -x + 2y + 2z, x - y - z)$

1. Montrer que f est linéaire.
2. Montrer que f est une involution linéaire.
3. En déduire le support et la direction de la symétrie f . On donnera pour chacun une famille génératrice
4. On pose $p = \frac{f + id}{2}$. Justifier sans trop de calculs que p est un projecteur. Déterminer sans calculs supplémentaires le support et la direction de la projection p .

Algèbre générale

Equation Pell Fermat

Ce problème s'intéresse à la résolution d'une équation de Pell-Fermat : $a^2 - 2b^2 = 1$ d'inconnue $(a, b) \in \mathbb{Z}^2$

On rappelle que :

- $\sqrt{2}$ est un nombre irrationnel
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, (a, b) \in \mathbb{Z}^2\}$
- Soit A un anneau et $f : A \rightarrow A$.

On dit que f est un automorphisme d'anneau de A si $\forall (x, y) \in A^2$,
$$\begin{cases} f(x + y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \\ f(1_A) = 1_A \\ f \text{ est bijective} \end{cases}$$

1. Exemples et structures
 - (a) Donner quelques exemples de solutions de l'équation de Pell-Fermat. Vous donnerez notamment les solutions (a, b) avec a et b entiers et $b \in \llbracket 0, 5 \rrbracket$
 - (b) Justifier rapidement que (a, b) est solution de cette équation de Pell-Fermat ssi $(\pm a, \pm b)$ est solution de l'équation de Pell-Fermat
 - (c) Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous anneau de \mathbb{R}
 - (d) Montrer que $\forall x \in \mathbb{Z}[\sqrt{2}], \exists!(a, b) \in \mathbb{Z}^2, x = a + b\sqrt{2}$
2. Applications et inversibles.

Lorsque $x = a + b\sqrt{2}$ on note $\bar{x} = a - b\sqrt{2}$ et $N(x) = x\bar{x}$

 - (a) Montrer que l'application $x \mapsto \bar{x}$ est un automorphisme de $\mathbb{Z}[\sqrt{2}]$
 - (b) Montrer que $\forall x \in \mathbb{Z}[\sqrt{2}], N(x) \in \mathbb{Z}$
 - (c) Montrer que $\forall (x, y) \in \mathbb{Z}[\sqrt{2}]^2, N(xy) = N(x)N(y)$
 - (d) En déduire que $\forall x \in \mathbb{Z}[\sqrt{2}]$ x est inversible dans $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(x) = \pm 1$

(e) Montrer que $G = \{a + b\sqrt{2}, (a, b) \in \mathbb{Z}^2 \text{ et } a^2 - 2b^2 = 1\}$ est un sous groupe de $U(\mathbb{Z}[\sqrt{2}])$ (ensemble des inversibles de $\mathbb{Z}[\sqrt{2}]$)

Pour $x \in G$, que vaut l'inverse de x ?

3. Inversibles

(a) Soit $x = a + b\sqrt{2} \in G \cap]1, +\infty[$. Calculer $x + \bar{x}$ et en déduire que $a > 0$. Calculer $x - \bar{x}$ et en déduire le signe de b . Peut-on avoir $b = 1$?

(b) En déduire que $G \cap]1, +\infty[$ possède un plus petit élément et que ce plus petit élément est $3 + 2\sqrt{2}$

(c) Soit $x = a + b\sqrt{2} \in G \cap]1, +\infty[$.

i. Montrer que $\exists n \in \mathbb{N}^*, (3 + 2\sqrt{2})^n \leq x < (3 + 2\sqrt{2})^{n+1}$

ii. En déduire que $x = (3 + 2\sqrt{2})^n$

(d) Montrer que finalement $G = \{\pm(3 + 2\sqrt{2})^n, n \in \mathbb{Z}\}$

4. Question subsidiaire :

Montrer que $\mathbb{Z}[\sqrt{2}]$ est dense dans \mathbb{R}

Arithmétique

Dans ce sujet on note \mathbb{P} l'ensemble des nombres premiers et on admettra que si $f : E \rightarrow F$ et si E et F sont des ensembles finis de même cardinal alors f est bijective ssi f est injective ssi f est surjective. Dans ce problème il y a des questions indépendantes (2.3.4) et ces résultats servent pour la question 5. Le préliminaire est utile pour les questions suivantes.

1. Préliminaires

(a) Soit $(x, y) \in \mathbb{N}^2$ et $p \in \mathbb{P}$. Montrer que si $p|xy$ alors $p|x$ ou $p|y$

(b) Soit $(x, y) \in \mathbb{N}^2$ tels que xy est un carré parfait et $x \wedge y = 1$. Montrer que x et y sont des carrés parfaits.

2. Soit $(x, y) \in \mathbb{N}^2$ et $p \in \mathbb{P}$. On suppose que $x \wedge y = 1$ et $xy = pz^2$. Montrer l'existence de deux entiers naturels a et b tels que $(x, y) = (pa^2, b^2)$ ou $(x, y) = (a^2, pb^2)$

3. Une première équation

On considère l'équation $x^4 - 2y^2 = 1$ d'inconnues $(x, y) \in \mathbb{N}^2$

(a) Montrer que x est impair. On considère n l'entier naturel tel que $x = 2n + 1$

(b) Factoriser y^2 en déduire que $n(n + 1)$ est un carré parfait (on n'oubliera pas le préliminaire)

(c) En déduire x et y . (On n'oubliera pas le préliminaire)

4. Un résultat

ici $p \in \mathbb{P}$ et p est impair. On note $r = \frac{p-1}{2}$

(a) On note \mathcal{I} l'ensemble des entiers naturels impairs.

Montrer que $\Phi : \begin{matrix} \llbracket 1, r \rrbracket \cap \mathcal{I} & \longrightarrow & \llbracket r+1, p-1 \rrbracket \cap 2\mathbb{Z} \\ k & \longmapsto & p-k \end{matrix}$ est bijective

(b) En déduire que $\prod_{k=1}^r ((-1)^k k) \equiv 2^r r! [p]$ (cette question est difficile n'y passez pas trop de temps) puis que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} [p]$$

(c) En déduire que si $\exists u \in \mathbb{Z}$ tels que $2 \equiv u^2 [p]$ alors p est congru à ± 1 modulo 8

5. Une autre équation

Ici $(x, y) \in \mathbb{N}^2$ et $p \in \mathbb{P}$ non congru à ± 1 modulo 8. On suppose que $4x^4 - py^2 = 1$

(a) Montrer l'existence de deux entiers naturels a et b tels que $2x^2 + 1 = pa^2$ et $2x^2 - 1 = b^2$

(b) Montrer l'existence de deux entiers naturels c et d et d'un élément $\epsilon \in \{-1, 1\}$ tels que $2x + \epsilon b = pc^2$ et $2x - \epsilon b = d^2$

(c) Que valent $pc^2 + d^2$ et $pc^2 - d^2$? En déduire que $8d^4 - (pc^2 - 3d^2)^2 = 8$

(d) En déduire que $pc^2 - 3d^2$ est un multiple de 4 puis en déduire la valeur de p de x et de y