Corrigé du Équation de Pell-Fermat

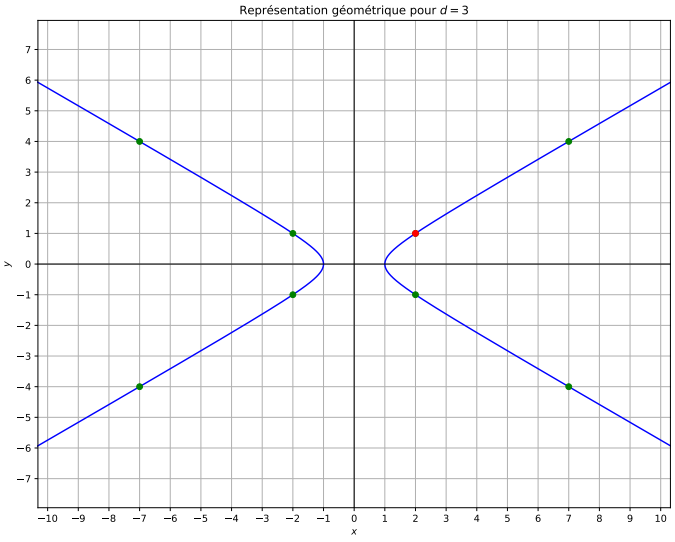
En cas d'erreur de corrigé, n'hésitez pas à me le signaler.

Contexte

L'objectif de ce problème est de d'étudier l'équation diophantienne de Pell-Fermat, c'est à dire de déterminer tous les couples $(x, y) \in \mathbb{Z}^2$ tels que

$$x^2 - dy^2 = 1. \tag{PF}$$

- La partie 0 établit un disjonction de cas selon la valeur de d.
- La partie 1 étudie la structure de l'anneau $\mathbb{Z}[\sqrt{d}]$, et relie un sous-groupe G du groupe de ses inversibles à l'ensemble des solutions de l'équation de Pell-Fermat.
- La partie 2 étudie la structure du groupe G obtenu à la partie précédente.
- La partie 3 déterminer une asymptotique du nombre de solutions $(x, y) \in \mathbb{N}^2$ telles que $x \leq k$.
- Enfin la partie 4 démontre l'existence d'une solution non triviale admise dans les parties précédentes, en se ramenant à un problème d'approximation d'irrationnels quadratiques par des rationnels.
- Facultativement, la partie 5 interprète géométriquement les parties précédentes.



Notations

Dans tout le devoir on utilisera les notations suivantes:

- Dans tout le sujet $d \in \mathbb{N}^*$ est un entier naturel non nul fixé.
  On peut remarquer dès à présent qu'en dehors de la partie 0 on supposera de plus que d n'est pas un carré parfait.
- On note (PF) l'équation dite de Pell-Fermat:
  $$x^2 - dy^2 = 1. \tag{PF}$$
  d'inconnue $(x, y) \in \mathbb{Z}^2$.
- On note $\mathcal{S}_{(\text{PF})}$ l'ensemble des solutions de l'équation (PF), c'est à dire
  $$\mathcal{S}_{(\text{PF})} = \left\{(x, y) \in \mathbb{Z}^2 \middle| x^2 - dy^2 = 1\right\}.$$
- On appellera ensemble des solutions *non triviales* de (PF) l'ensemble $\mathcal{S}_{(\text{PF})} \backslash \{(1, 0), (-1, 0)\}$ (voir partie 0).
- On notera
  $$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d}, (a, b) \in \mathbb{Z}^2\right\}.$$
- Pour $x \in \mathbb{R}$ on notera $\lfloor x \rfloor$ la partie entière de x, c'est à dire le plus grand entier plus petit que x.
- Pour $x \in \mathbb{R}$ on notera $\{x\} = x - \lfloor x \rfloor$ la partie fractionnaire de x.

---

0 Préliminaires arithmétiques

0.1. Montrer que $(1, 0)$ et $(-1, 0)$ sont solutions de l'équation de Pell-Fermat (PF).

On a $(1, 0), (-1, 0) \in \mathbb{Z}^2$ et

$$1^2 - d0^2 = (-1)^2 - d0^2 = 1$$

d'où $\boxed{(1, 0) \text{ et } (-1, 0) \text{ sont solutions de l'équation (PF)}}$.

On appellera ces solutions *solutions triviales* et toute autre solution *solution non triviale*.

0.2. On suppose dans cette question que d est un carré parfait (c'est à dire qu'il existe $\delta \in \mathbb{N}$ tel que $d = \delta^2$).
Montrer que l'équation de Pell-Fermat (PF) n'admet pas de solution non triviale.

Soit $\delta \in \mathbb{N}$ tel que $d = \delta^2$.
Alors soit $(x, y) \in \mathbb{Z}^2$ vérifiant

$$x^2 - dy^2 = 1$$

i.e

$$x^2 - \delta^2 y^2 = 1.$$

On a alors (identité remarquable)

$$(x - \delta y)(x + \delta y) = 1.$$

Comme $x - \delta y, x + \delta y \in \mathbb{Z}$ on a nécessairement $x - \delta y = 1 = x + \delta y = \pm 1$.
Par conséquent $2x = \pm 2$ d'où $x = \pm 1$.
Et donc $dy^2 = 1 - (\pm 1)^2$ d'où $y = 0$.
Donc $(a, b) = (\pm 1, 0)$.
Donc $\boxed{\text{si } d \text{ est un carré, alors équation (PF) n'admet pas de solution non triviale}}$.

0.3. On suppose dans cette question que d n'est pas un carré parfait.
Montrer que $\sqrt{d} \notin \mathbb{Q}$.

Procédons par contraposée.
Supposons $\sqrt{d} \in \mathbb{Q}$ (donc $\mathbb{Q}_+$), et soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$ tels que $\sqrt{d} = \frac{a}{b}$.
Alors $d = \frac{a^2}{b^2}$ d'où $db^2 = a^2$.
Pour tout nombre premier p on a donc $\nu_p(db^2) = \nu_p(a^2)$ c'est à dire

$$\nu_p(d) + 2\nu_p(b) = 2\nu_p(a)$$

ou encore

$$\nu_p(d) = 2(\nu_p(a) - \nu_p(b)).$$

Donc $\nu_p(d)$ est pair et $d = \left(\prod_{p \text{ premier}} p^{\frac{\nu_p(d)}{2}} \right)^2$ est un carré parfait.
Par contraposée on a donc

$$\boxed{(d \text{ n'est pas un carré parfait}) \Rightarrow \sqrt{d} \notin \mathbb{Q}}.$$

Dans la suite on suppose que d n'est pas un carré parfait.
De plus dans les parties 2 et 3 on admettra que, dans ce cas, l'équation (PF) admet au moins une solution non-triviale.
Ce résultat sera démontré en partie 4.

---

1 Étude de $\mathbb{Z}[\sqrt{d}]$

1.4. Montrer que $\mathbb{Z}[\sqrt{d}]$ muni des opérations + et × usuelles est un anneau commutatif.

On a $\mathbb{Z}[\sqrt{d}] \subset \mathbb{R}$ et $\mathbb{R}$ est un anneau pour les opérations + et × usuelles.
Montrons que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de l'anneau commutatif $(\mathbb{R}, +, \times)$.

- On a $\mathbb{Z}[\sqrt{d}] \subset \mathbb{R}$.
- On a $0 = 0 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
- On a $1 = 1 + 0\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
- Soit $(z_1, z_2) \in \left(\mathbb{Z}[\sqrt{d}]\right)^2$.
  Soient $(a_1, b_1) \in \mathbb{Z}^2$ et $(a_2, b_2) \in \mathbb{Z}^2$ tels que $z_1 = a_1 + b_1\sqrt{d}$ et $z_2 = a_2 + b_2\sqrt{d}$.
  Alors

▷ $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
▷ $z_1 \times z_2 = (a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
D'où $\mathbb{Z}[\sqrt{d}]$ est stable par somme et stable par produit.

- Soit $z \in \mathbb{Z}[\sqrt{d}]$.
Soient $(a, b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
Alors
▷ $-z = (-a) + (-b)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.
D'où $\mathbb{Z}[\sqrt{d}]$ est stable par opposé.

Par conséquent $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
Et en particulier $\boxed{(\mathbb{Z}[\sqrt{d}], +, \times) \text{ est un anneau}}$.

1.5. Montrer que l'application

$$\varphi : \begin{array}{c} \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{d}] \\ (a, b) \mapsto a + b\sqrt{d} \end{array}$$

est un isomorphisme de groupes additifs.

Par définition de $\mathbb{Z}[\sqrt{d}]$ on a $\boxed{\varphi \text{ bien défini et surjectif}}$.
Soient $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}^2$.
Alors

$$\begin{aligned} \varphi((a_1, b_1) + (a_2, b_2)) &= \varphi(a_1 + a_2, b_1 + b_2) \\ &= (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \\ &= (a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) \\ &= \varphi((a_1, b_1)) + \varphi((a_2, b_2)). \end{aligned}$$

Donc $\boxed{\varphi \text{ est un morphisme de groupes additifs}}$.
Soient $(a, b) \in \mathrm{Ker}(\varphi) \subset \mathbb{Z}^2$, c'est à dire tel que $\varphi((a, b)) = 0$.
Alors

$$a + b\sqrt{d} = 0.$$

Supposons par l'absurde $b \neq 0$.
Alors

$$\sqrt{d} = \frac{-a}{b} \in \mathbb{Q}$$

ce qui est ABSURDE par la question **0.3.**.
Donc $b = 0$. Donc $a + 0\sqrt{d} = 0$ i.e $a = 0$.
On a donc $\mathrm{Ker}(\varphi) \subset \{(0, 0)\}$. L'autre inclusion étant immédiate,

$$\boxed{\mathrm{Ker}(\varphi) = \{(0, 0)\}}$$

et donc $\boxed{\varphi \text{ est injective}}$.

Traduire l'injectivité de φ en termes d'unicité.

On a donc, pour tout $z \in \mathbb{Z}[\sqrt{d}]$, $\boxed{\text{il existe un } \textbf{unique} \text{ couple } (a, b) \in \mathbb{Z}^2 \text{ tel que } z = a + b\sqrt{d}}$.

1.6. Montrer que l'on peut définir une application

$$\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$$

telle que

$$\forall (a, b) \in \mathbb{Z}^2, \sigma\left(a + b\sqrt{d}\right) = a - b\sqrt{d}.$$

Soit $z \in \mathbb{Z}[\sqrt{d}]$.
Par la question **1.5.**, il existe un **unique** couple $(a, b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
Ainsi $a - b\sqrt{d}$ ne dépend que de z et on peut définir $\sigma(z) = a - b\sqrt{d}$.
Très (trop ?) formellement on a défini σ par $\sigma = \varphi \circ \tau \circ \varphi^{-1}$ où τ est l'application de $\mathbb{Z}^2$ dans $\mathbb{Z}^2$ définie par $\tau(a, b) = (a, -b)$.

D'où $\boxed{\text{l'existence d'une telle application}}$.
On remarque par ailleurs que l'unicité est immédiate par surjectivité de φ.

1.7. Montrer que

$$\sigma : \begin{array}{c} \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}] \\ z \mapsto \sigma(z) \end{array}$$

est un automorphisme d'anneaux de $\mathbb{Z}[\sqrt{d}]$.

On a vu à la question **1.6.** que $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ est bien défini.

- On a $\sigma(1) = \sigma(1 + 0\sqrt{d}) = 1 - 0\sqrt{d} = 1$.
- Soient $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$.
  Soient $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}^2$ tels que $z_1 = a_1 + b_1\sqrt{d}$ et $z_2 = a_2 + b_2\sqrt{d}$.
  Alors

$$\begin{aligned} \sigma(z_1 + z_2) &= \sigma((a_1 + a_2) + (b_1 + b_2)\sqrt{d}) \\ &= (a_1 + a_2) - (b_1 + b_2)\sqrt{d} \\ &= (a_1 - b_1\sqrt{d}) + (a_2 - b_2\sqrt{d}) \\ &= \sigma(z_1) + \sigma(z_2). \end{aligned}$$

  et de plus

$$\begin{aligned} \sigma(z_1 \times z_2) &= \sigma((a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d}) \\ &= (a_1a_2 + db_1b_2) - (a_1b_2 + a_2b_1)\sqrt{d} \\ &= (a_1a_2 + (-b_1))(-b_2) + (a_1(-b_2) + a_2(-b_1))\sqrt{d} \\ &= (a_1 - b_1\sqrt{d}) \times (a_2 - b_2\sqrt{d}) \\ &= \sigma(z_1) \times \sigma(z_2). \end{aligned}$$

Donc $\boxed{\sigma \text{ est un endomorphisme d'anneaux}}$.
De plus on a pour tout $z \in \mathbb{Z}[\sqrt{d}]$, avec $(a, b) \in \mathbb{Z}^2$ tels que $z = a + b\sqrt{d}$,

$$\begin{aligned} \sigma(\sigma(z)) &= \sigma(\sigma(a + b\sqrt{d})) \\ &= \sigma(a - b\sqrt{d}) \\ &= a - (-b)\sqrt{d} \\ &= a + b\sqrt{d} \\ &= z. \end{aligned}$$

Donc

$$\sigma \circ \sigma = \mathrm{Id}_{\mathbb{Z}[\sqrt{d}]}$$

et en particulier $\boxed{\sigma \text{ est bijective}}$ (de bijection réciproque σ).
Remarque: alternativement si on avait défini σ comme $\sigma = \varphi \circ \tau \circ \varphi^{-1}$, il suffit de remarquer que φ est un isomorphisme d'anneaux (attention pas pour la structure de groupe produit mais pour le produit $(a_1, b_1) \times (a_2, b_2) = (a_1a_2 + db_1b_2, a_1b_2 + a_2b_1)$) et que τ est un automorphisme d'anneaux.

1.8. Soit $z \in \mathbb{Z}[\sqrt{d}]$ et $(a, b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
Exprimer a et b en fonction de z et $\sigma(z)$.

On a

$$\begin{cases} a + b\sqrt{d} = z \\ a - b\sqrt{d} = \sigma(z) \end{cases}$$

d'où (système somme-différence)

$$\begin{cases} 2a = z + \sigma(z) \\ 2b\sqrt{d} = z - \sigma(z) \end{cases}$$

c'est à dire

$$\boxed{\begin{cases} a = \dfrac{z+\sigma(z)}{2} \\ b = \dfrac{z-\sigma(z)}{2\sqrt{d}} \end{cases}}.$$

On pourra noter dans la suite $\pi_1(z) = a$ et $\pi_2(z) = b$.

Cette notation a bien un sens par unicité de la question **1.5.**.

Commenter.

On observe les mêmes règles de calculs que dans $\mathbb{R}[i] = \mathbb{C}$, en remplaçant d par -1 et $\sqrt{d}$ par i.
Par exemple σ correspond à l'application conjugué $z \mapsto \overline{z}$, π_1 à Re et π_2 à Im.
Par ailleurs la quantité $N(z)$ de la question suivante peut s'interpréter comme un module au carré, avec la différence que $N(z)$ est n'est pas forcément positif.

Pour $z \in \mathbb{Z}[\sqrt{d}]$, on définit la *norme* de z, notée $N(z)$, par $N(z) = z \times \sigma(z)$.

On remarque que formellement ce n'est pas une norme mais plutôt une «norme au carré». Par exemple pour $\lambda \in \mathbb{Z}$ et $z \in \mathbb{Z}[\sqrt{d}]$, $N(\lambda z) = \lambda^2 N(z)$.

1.9. Montrer que

$$\forall z \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z) \in \mathbb{Z}$$

et

$$\forall z \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z) = 0 \Leftrightarrow z = 0.$$

Soit $z \in \mathbb{Z}[\sqrt{d}]$.
Soit $(a,b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
Alors $\sigma(z) = a - b\sqrt{d}$ d'où

$$N(z) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}.$$

Ainsi $\boxed{N(z) \in \mathbb{Z}}$.
Si $z = 0 = 0 + \sqrt{0}$, alors $N(z) = (0+\sqrt{0})(0-\sqrt{0}) = 0$.
Si $N(z) = 0$, alors $z \times \sigma(z) = 0$. D'où (intégrité de $\mathbb{R}$), $z = 0$ ou $\sigma(z) = 0$. Comme σ injectif $\sigma(z) = 0$ ssi $z = 0$. Dans tous les cas $z = 0$.
Donc $\boxed{N(z) = 0 \Leftrightarrow z = 0}$.

1.10. Montrer que

$$\forall (z_1, z_2) \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z_1 z_2) = N(z_1)N(z_2)$$

Soient $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$.
On a (commutativité du produit dans $\mathbb{R}$)

$$\begin{aligned} N(z_1z_2) &= z_1z_2 \times \sigma(z_1z_2) \\ &= z_1z_2 \times \sigma(z_1)\sigma(z_2) \\ &= z_1 \times \sigma(z_1) \times z_2 \times \sigma(z_2) \\ &= N(z_1)N(z_2). \end{aligned}$$

Donc

$$\boxed{\forall (z_1, z_2) \in \mathbb{Z}[\sqrt{d}]\ ,\quad N(z_1 z_2) = N(z_1)N(z_2)}.$$

Remarque: de plus $N(1) = 1$, et par conséquent $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ est un morphisme de monoïdes multiplicatifs.

1.11. Soit $z \in \mathbb{Z}[\sqrt{d}]$.
Montrer que

$$z \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times \ \Leftrightarrow\ N(z) \in \{-1, +1\}.$$

On procède par double implication.

- $\boxed{\Leftarrow}$ Supposons $N(z) \in \{-1,+1\}$ (c'est à dire $N(z)$ inversible dans $\mathbb{Z}$)
  Alors par définition de $N(z)$, comme $\frac{1}{N(z)} \in \mathbb{Z}[\sqrt{d}]$ on a
  $$z \underbrace{\frac{\sigma(z)}{N(z)}}_{\in \mathbb{Z}[\sqrt{d}]} = 1$$
  et par conséquent $\boxed{z \text{ est inversible dans } \mathbb{Z}[\sqrt{d}]}$, d'inverse $\frac{\sigma(z)}{N(z)}$.
- $\boxed{\Rightarrow}$ Supposons $z \in \left(\mathbb{Z}[\sqrt{d}]^\times\right)$.
  Alors
  $$zz^{-1} = 1$$
  d'où comme
  $$N(zz^{-1}) = N(1)$$
  c'est à dire (questions **1.9.** et **1.10.**)
  $$\underbrace{N(z)}_{\in\mathbb{Z}} \underbrace{N(z^{-1})}_{\in\mathbb{Z}} = 1.$$
  En particulier $N(z)$ est inversible dans $\mathbb{Z}$ c'est à dire $\boxed{N(z) \in \mathbb{Z}^\times = \{-1,+1\}}$.

On a donc bien montré que

$$\boxed{z \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times \Leftrightarrow N(z) \in \{-1,+1\}}.$$

1.12. Montrer que
$$G = \left\{ z \in \mathbb{Z}[\sqrt{d}] \middle| N(z) = 1 \right\}$$
muni du produit $\times$ est un groupe.

Montrons que G est un sous-groupe du groupe des inversibles $\left((\mathbb{Z}[\sqrt{d}])^\times, \times\right)$.

- Par la question **1.11.**.
- Comme $N(1) = N(1 + 0\sqrt{d}) = 1$, on a $1 \in G$.
- Soient $z_1, z_2 \in G$.
  Alors $N(z_1 z_2) = N(z_1)N(z_2) = 1 \times 1 = 1$.
  Ainsi $z_1 z_2 \in G$.
  Donc G est stable par produit.
- Soit $z \in G$.
  On a a vu à la question **1.11.** que $N(z)N(z^{-1}) = 1$ d'où $N(z^{-1}) = 1$.
  Ainsi $z^{-1} \in G$.
  Donc G est stable par inverse.

Donc $\boxed{G \text{ est un sous-groupe de } \left((\mathbb{Z}[\sqrt{d}])^\times, \times\right)}$.

Remarque: alternativement $G = \mathrm{Ker}(N)$ avec $N : ((\mathbb{Z}[\sqrt{d}])^\times, \times) \to (\mathbb{Z}^\times, \times)$ un morphisme de groupes.

1.13. Expliciter une bijection entre G et l'ensemble $\mathcal{S}_{(\mathrm{PF})}$.

Montrons qu'avec les notations de la question **1.5.**, l'application
$$\left(\varphi^{-1}\right)_{|G}^{\mathcal{S}_{(\mathrm{PF})}} : G \to \mathcal{S}_{(\mathrm{PF})}$$
est bien définie et bijective.

Remarque: Informellement il s'agit de l'application qui «à $a + b\sqrt{d}$ associe (a,b)».

- Soit $z \in G$. Alors avec $z = a + b\sqrt{d}$ où $(a,b) \in \mathbb{Z}^2$ on a $N(z) = 1$ et $N(z) = a^2 - db^2$.
  D'où $(a,b) \in \mathcal{S}_{(\mathrm{PF})}$.
  D'où la $\boxed{\text{bonne définition}}$.
- On a vu que φ^{-1} est injective (car bijective car bijection réciproque d'une bijection).
  La restriction et co-restriction d'une application injective est injective.
  D'où l'$\boxed{\text{injectivité}}$
- Soit $(a,b) \in \mathcal{S}_{(\mathrm{PF})}$. Alors $a^2 - db^2 = 1$. Avec $z = a + b\sqrt{d}$ on a $N(z) = 1$ i.e $z \in G$. Et l'image de z est (a,b).

D'où la surjectivité.
Remarque: en munissant $\mathcal{S}_{(\mathrm{PF})}$ du produit de la partie 5 on obtient même qu'il s'agit d'un morphisme de groupes multiplicatifs.

2 Structure du groupe G

On rappelle que l'on admet dans cette partie que $\mathcal{S}_{(\mathrm{PF})} \neq \{(1,0),(-1,0)\}$.

2.14. Montrer que

$$H = G \cap]0, +\infty[$$

est un groupe.

On a vu à la question **1.12.** que G est un sous-groupe de $(\mathbb{R}^*, \times)$.
De plus $]0,+\infty[$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
Une intersection de sous-groupes étant un sous-groupe on en déduit que H est un sous-groupe de $(\mathbb{R}^*, \times)$.

2.15. Expliciter un isomorphisme de groupe entre G et $H \times \{-1, +1\}$.

Considérons

$$\psi : \begin{array}{c} G \to H \times \{-1,+1\} \\ z \mapsto \left(|z|, \dfrac{z}{|z|}\right) \end{array}$$

- Soit $z \in G$.
  Alors $z \neq 0$ donc $\varepsilon = \frac{z}{|z|}$ est bien défini et dans $\{-1,1\}$.
  Donc, comme $\varepsilon \in G$ (car $\{-1,1\} \subset G$, cf question **0.1.**), on a $|z| = \varepsilon z \in G$.
  Et comme $|z| > 0$ on a bien $|z| \in H$.
  D'où la bonne définition.
- Soient $z_1, z_2 \in G$.
  Alors

$$\begin{aligned} \psi(z_1 z_2) &= \left(|z_1 z_2|, \frac{z_1 z_2}{|z_1 z_2|}\right) \\ &= \left(|z_1||z_2|, \frac{z_1}{|z_1|}\frac{z_2}{|z_2|}\right) \\ &= \left(|z_1|, \frac{z_1}{|z_1|}\right) \times \left(|z_2|, \frac{z_2}{|z_2|}\right) \\ &= \psi(z_1) \times \psi(z_2). \end{aligned}$$

  Donc ψ est un morphisme de groupes.
- Soit

$$\gamma : \begin{array}{c} H \times \{-1,+1\} \to G \\ (\rho, \varepsilon) \mapsto \varepsilon\rho \end{array}$$

  alors γ est bien défini.
  Et de plus, comme les éléments de H sont positifs

$$\forall (\rho,\varepsilon) \in H \times \{-1,+1\}, \psi(\gamma((\rho,\varepsilon))) = \left(\rho|\varepsilon|, \frac{\rho\varepsilon}{\rho}\right) = (\rho,\varepsilon)$$

  et

$$\forall z \in H, \gamma(\psi(z)) = |z|\frac{z}{|z|} = z$$

  c'est à dire

$$\psi \circ \gamma = \mathrm{Id}_{H \times \{-1,+1\}}$$

  et

$$\gamma \circ \psi = \mathrm{Id}_G$$

  d'où en particulier la bijectivité.
  Remarque: on aurait pu être légèrement plus efficace en remarquant que γ est un morphisme par commutativité du produit et en déduire ensuite que ψ est un morphisme.

Remarque: ce morphisme ressemble au morphisme $\mathbb{C}^* \to \mathbb{R}_+^* \times \mathbb{U}$ qui à $z \in \mathbb{C}^*$ associe $(|z|, \frac{z}{|z|})$ vu dans le chapitre de nombres complexes.

2.16. Montrer que

$$H\cap]1,+\infty[\neq\emptyset.$$

On rappelle que l'on a admis que (PF) admet des solutions non triviales.
C'est à dire par la question **1.13.**

$$G\neq\{-1,+1\}.$$

Soit $z\in G\backslash\{-1,+1\}$.
Comme $N(-z)=1$ (car $-1\in G$) on a $-z\in G$. Donc quitte à considérer $-z$ on peut supposer que $z>0$.
De plus $N(z^{-1})=1$, quitte à considérer z^{-1} on peut supposer que $z>1$.
On a donc $z\in H\cap]1,+\infty[$.
Par conséquent

$$\boxed{H\cap]1,+\infty[\neq\emptyset}$$

2.17. Soient $z_1,z_2\in H$ et $(a_1,b_1),(a_2,b_2)\in\mathbb{Z}^2$ tels que $z_1=a_1+b_1\sqrt{d}$ et $z_2=a_2+b_2\sqrt{d}$.
Montrer que

$$z_1<z_2\Rightarrow b_1<b_2.$$

Interpréter ce résultat en termes de l'application π_2.

Supposons que

$$z_1<z_2.$$

Comme $z_1\in H$, $\sigma(z_1)=\frac{1}{z_1}$ et de même $\sigma(z_2)=\frac{1}{z_2}$.
Comme de plus comme $z_1,z_2\in H$, $\underline{z_1>0 \text{ et } z_2>0}$ on en déduit donc que

$$\sigma(z_1)=\frac{1}{z_1}>\frac{1}{z_2}=\sigma(z_2)$$

et donc

$$-\sigma(z_1)<-\sigma(z_2).$$

Par conséquent

$$\frac{z_1-\sigma(z_1)}{2\sqrt{d}}<\frac{z_2-\sigma(z_2)}{2\sqrt{d}}$$

ce qui se réécrit par la question **1.8.**

$$b_1<b_2.$$

On a donc bien montré

$$\boxed{z_1<z_2\Rightarrow b_1<b_2}.$$

On obtient donc que $\boxed{\pi_{2|H} \text{ est croissante}}$.

2.18. En déduire que

$$\xi=\min\left(H\cap]1,+\infty[\right)$$

est bien défini.

On a $1=1+0\sqrt{d}\in H$.
Donc pour $z\in H\cap]1,+\infty[$, $\pi_2(z)>\pi_2(1)=0$ par la question **2.17.**.
L'ensemble

$$\{\pi_2(z),z\in H\cap]1,+\infty[\}$$

est par conséquent une partie de $\mathbb{N}^*$, non vide par la question **2.16.**.
Il admet donc un minimum.
Il $\boxed{\text{existe}}$ donc $\xi\in H\cap]1,+\infty[$ tel que

$$\pi_2(\xi)=\min\left\{\pi_2(z),z\in H\cap]1,+\infty[\right\}.$$

Soit $z\in H\cap]1,+\infty[$. Supposons par l'absurde que $z<\xi$. Alors $\pi_2(z)<\pi_2(\xi)$ par la question **2.17.**, et donc $\pi_2(z)<\min\left\{\pi_2(z'),z'\in H\cap]1,+\infty[\right\}$, ce qui est absurde.
D'où

- $\xi \in H \cap]1, +\infty[$,
- $\forall z \in H \cap]1, +\infty[, z \geq \xi$.

D'où

$$\boxed{\xi = \min\left(H \cap]1, +\infty[\right)}.$$

2.19. Expliquer succinctement pourquoi, pour tout $n \in \mathbb{Z}$, $\xi^n \in H$.

Comme $\xi \in H$ et H est un sous-groupe de $(\mathbb{R}^*, \times)$, on a par récurrence immédiate, pour tout $n \in \mathbb{N}$, $\xi^n \in H$. Et par stabilité par inverse on obtient alors $\boxed{\text{pour tout } n \in \mathbb{Z},\ \xi^n \in H}$.

2.20. Soit $x \in H$.
Montrer qu'il existe et un unique $n \in \mathbb{Z}$ tel que

$$\xi^n \leq x < \xi^{n+1}.$$

On procède par analyse-synthèse.

- **Analyse**
  Soit $n \in \mathbb{Z}$ tel que
  $$\xi^n \leq x < \xi^{n+1}.$$
  Alors par stricte croissance de ln sur $]0, +\infty[$
  $$\ln(\xi^n) \leq \ln(x) < \ln(\xi^{n+1})$$
  c'est à dire
  $$n\ln(\xi) \leq \ln(x) < (n+1)\ln(\xi)$$
  ce qui revient, comme $\ln(\xi) > 0$ (car $\xi > 1$), à
  $$n \leq \frac{\ln(x)}{\ln(\xi)} < n+1$$
  et donc
  $$n = \left\lfloor \frac{\ln(x)}{\ln(\xi)} \right\rfloor.$$
  D'où $\boxed{\text{l'unicité}}$.
- **Synthèse**
  Posons
  $$n = \left\lfloor \frac{\ln(x)}{\ln(\xi)} \right\rfloor.$$
  Alors $n \in \mathbb{Z}$ et par définition de la partie entière, $n \leq \frac{\ln(x)}{\ln(\xi)} < n+1$.
  Donc comme $\ln(\xi) > 0$ on a$n\ln(\xi) \leq \ln(x) < (n+1)\ln(\xi)$ d'où (stricte croissance de exp)
  $$\xi^n \leq x < \xi^{n+1}.$$
  Donc n convient et $\boxed{\text{l'existence}}$.

Remarque: On aurait en fait pu ici procéder directement par équivalences (par stricte croissance de ln et stricte positivité de $\ln(\xi)$):

$$\begin{aligned}
\xi^n \leq x < \xi^{n+1} &\Leftrightarrow \ln(\xi^n) \leq \ln(x) < \ln(\xi^{n+1}) \\
&\Leftrightarrow n\ln(\xi) \leq \ln(x) < (n+1)\ln(\xi) \\
&\Leftrightarrow n \leq \frac{\ln(x)}{\ln(\xi)} < n+1 \\
&\Leftrightarrow n = \left\lfloor \frac{\ln(x)}{\ln(\xi)} \right\rfloor.
\end{aligned}$$

2.21. Soit $x \in H$ et n tel que $\xi^n \leq x < \xi^{n+1}$.
Montrer que $x = \xi^n$.

Par la question **2.19.** on a $\xi^{-n} \in H$ et donc (stabilité par produit) $x\xi^{-n} \in H$.
Comme de plus $\xi^{-n} > 0$ on déduit de $\xi^n \leq x < \xi^{n+1}$ que

$$\xi^n \xi^{-n} \leq x\xi^{-n} < \xi^{n+1}\xi^{-n}$$

i.e

$$1 \leq x\xi^{-n} < \xi.$$

Si par l'absurde $x\xi^{-n} \neq 1$ alors $x\xi^{-n} \in H \cap]1, +\infty[$ et $x\xi^{-n} < \min(H \cap]1, +\infty[)$ ce qui est absurde.
Donc $x\xi^{-n} = 1$ i.e

$$\boxed{x = \xi^n}.$$

2.22. Déduire des question précédentes que

$$H = \{\xi^n, n \in \mathbb{Z}\}$$

- Par la question **2.19.** on a $H \supset \{\xi^n, n \in \mathbb{Z}\}$.
- Soit $x \in H$. Par la question **2.21.** il existe $n \in \mathbb{Z}$ tel que $x = \xi^n$.
  Donc $H \subset \{\xi^n, n \in \mathbb{Z}\}$.
- Par double inclusion on a donc

$$\boxed{H = \{\xi^n, n \in \mathbb{Z}\}}$$

Remarque: il s'agit exactement de la même preuve (version multiplicative) que pour la structure des sous-groupes additifs de $\mathbb{Z}$ ou celle pour la structure des sous-groupe additifs de $\mathbb{R}$ dans le cas non dense.

2.23. Conclure qu'il existe un et unique $(a_1, b_1) \in \mathbb{Z}^2$ tels que $a_1 + b_1\sqrt{d} > 1$ et

$$G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n, \varepsilon) \in \mathbb{Z} \times \{-1, +1\}\right\}.$$

Commenter.

- **Analyse**
  Soit $(a_1, b_1) \in \mathbb{Z}^2$ tel que $a_1 + b_1\sqrt{d} > 1$ et $G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n, \varepsilon) \in \mathbb{Z} \times \{-1, +1\}\right\}$.
  Alors $H = \left\{(a_1 + b_1\sqrt{d})^n, n \in \mathbb{Z}\right\}$, et par conséquent $H \cap]1, +\infty[= \left\{(a_1 + b_1\sqrt{d})^n, n \in \mathbb{N}^*\right\}$ d'où $a_1 + b_1\sqrt{d} = \min(H \cap]1, +\infty[) = \xi$.
  D'où $\boxed{\text{l'unicité}}$.
- **Synthèse**
  Soit $(a_1, b_1) \in \mathbb{Z}^2$ tel que $\xi = a_1 + b_1\sqrt{d}$.
  Alors par la question **2.22.** on a $H = \left\{(a_1 + b_1\sqrt{d})^n, n \in \mathbb{Z}\right\}$.
  Et par l'isomorphisme construit à la question **2.15.** on a alors

$$G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n, \varepsilon) \in \mathbb{Z} \times \{-1, +1\}\right\}$$

  d'où $\boxed{\text{l'existence}}$.

Remarque: Un sujet légèrement moins détaillé on pourrait se contenter des **2.17.** et **2.23.** sans étapes intermédiaires. Il s'agit en effet d'une preuve très proche de celle classique sur la structure des sous-groupes additifs de $\mathbb{R}$, plus précisément le cas non dense.

3 Estimée asymptotique du nombre de solutions

On rappelle le résultat suivant démontré à la partie 2:

Il existe un et unique $(a_1, b_1) \in \mathbb{Z}^2$ tels que $a_1 + b_1\sqrt{d} > 1$ et $G = \left\{\varepsilon(a_1 + b_1\sqrt{d})^n, (n, \varepsilon) \in \mathbb{Z} \times \{-1, +1\}\right\}$.

3.24. Montrer que pour tout $n \in \mathbb{N}$ on a

$$(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$$

où $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ sont définies par

$$\begin{cases} a_0 = 1 \\ b_0 = 0 \end{cases}$$

et

$$\forall n \in \mathbb{N}, \begin{cases} a_{n+1} = a_n a_1 + d b_n b_1 \\ b_{n+1} = a_n b_1 + a_1 b_n \end{cases}$$

Définissons les suites $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ par la récurrence

$$\begin{cases} a_0 = 1 \\ b_0 = 0 \end{cases}$$

et

$$\forall n \in \mathbb{N}, \begin{cases} a_{n+1} = a_n a_1 + d b_n b_1 \\ b_{n+1} = a_n b_1 + a_1 b_n \end{cases}$$

et vérifions que par récurrence sur $n \in \mathbb{N}$ que pour tout $n \in \mathbb{N}$, $(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$.

► **Initialisation**
Pour $n = 0$ on a bien $(a_1 + b_1\sqrt{d})^0 = 1 = a_0 + b_0\sqrt{d}$.

► **Hérédité**
Soit $n \in \mathbb{N}$ et supposons que $(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$. Alors

$$\begin{aligned} (a_1 + b_1\sqrt{d})^{n+1} = (a_1 + b_1\sqrt{d})^n (a_1 + b_1\sqrt{d}) & \\ &= (a_n a_1 + d b_n b_1) + \sqrt{d}(a_n b_1 + a_1 b_n) \\ &= a_{n+1} + b_{n+1}\sqrt{d} \end{aligned}$$

et donc $(a_1 + b_1\sqrt{d})^{n+1} = a_{n+1} + b_{n+1}\sqrt{d}$.

► **Conclusion**
La proposition étant initialisée et héréditaire, on en déduit que pour tout $n \in \mathbb{N}$, $\boxed{(a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}}$.

3.25. Pour tout $n \in \mathbb{N}$ on pose $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.
Expliciter une matrice $A \in \mathrm{M}_2(\mathbb{Z})$ telle que

$$\forall n \in \mathbb{N}, X_{n+1} = AX_n.$$

Posons

$$\boxed{A = \begin{pmatrix} a_1 & d b_1 \\ b_1 & a_1 \end{pmatrix}}.$$

Alors le résultat de la question **3.24.** se réécrit bien par le produit matriciel, $\forall n \in \mathbb{N}$, $X_{n+1} = AX_n$. : Remarque: de toute façon la question suivant donne l'expression explicite de $A = A^1$.

3.26. Montrer que

$$\forall n \in \mathbb{N},\ A^n = \begin{pmatrix} \dfrac{\xi^n + \sigma(\xi)^n}{2} & d\dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} \\ \dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} & \dfrac{\xi^n + \sigma(\xi)^n}{2} \end{pmatrix}.$$

Remarque: l'expression explicite étant donnée par le sujet, le plus simple est de procéder par récurrence sur $n \in \mathbb{N}$.
Comme vous savez toutes et tous rédiger une récurrence on propose ici une preuve alternative.
Posons $B = \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}$. On constate que $A = a_1 I_2 + b_1 B$.
Alors $B^2 = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = dI_2$. Et donc pour tout $k \in \mathbb{N}$,

- Si k est pair, on $B^k = (B^2)^{\frac{k}{2}} = d^{\frac{k}{2}} I_2$.
- Si k est impair, on $B^k = (B^2)^{\frac{k-1}{2}} B = d^{\frac{k-1}{2}} B$.

Soit $n \in \mathbb{N}$. Comme $a_1 I_2$ et $b_1 B$ commutent, par formule du binôme on a

$$\begin{aligned}A^n &= (a_1 I_2 + b_1 B)^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (a_1 I_2)^{n-k} (b_1 B)^k \\ &= \sum_{k=0}^{n} \binom{n}{k} {a_1}^{n-k} {b_1}^k B^k \\ &= \sum_{\substack{k\in[\![0,n]\!] \\ k\text{pair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k B^k + \sum_{\substack{k\in[\![0,n]\!] \\ k\text{impair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k B^k \\ &= \sum_{\substack{k\in[\![0,n]\!] \\ k\text{pair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k}{2}} I_2 + \sum_{\substack{k\in[\![0,n]\!] \\ k\text{impair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k-1}{2}} B\end{aligned}$$

Or comme on a de plus

$$\xi^n = (a_1 + b_1\sqrt{d})^n = \sum_{k=0}^{n} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k}{2}}$$

$$\sigma(\xi)^n = (a_1 - b_1\sqrt{d})^n = \sum_{k=0}^{n} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k}{2}} (-1)^k$$

on en déduit (système somme-différence) que

$$\sum_{\substack{k\in[\![0,n]\!] \\ k\text{pair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k}{2}} = \frac{\xi^n + \sigma(\xi)^n}{2}$$

$$\sum_{\substack{k\in[\![0,n]\!] \\ k\text{impair}}} \binom{n}{k} {a_1}^{n-k} {b_1}^k d^{\frac{k}{2}} = \frac{\xi^n - \sigma(\xi)^n}{2}.$$

Par conséquent

$$\boxed{A^n = \frac{\xi^n + \sigma(\xi)^n}{2} I_2 + \frac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} B}$$

ce qui se réécrit

$$\boxed{A^n = \begin{pmatrix} \dfrac{\xi^n + \sigma(\xi)^n}{2} & d\dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} \\ \dfrac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} & \dfrac{\xi^n + \sigma(\xi)^n}{2} \end{pmatrix}}.$$

Remarque: il y a d'autres méthodes, par exemple constater $A = \begin{pmatrix} -\sqrt{d} & \sqrt{d} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \xi & 0 \\ 0 & \sigma(\xi) \end{pmatrix} \begin{pmatrix} -\sqrt{d} & \sqrt{d} \\ 1 & 1 \end{pmatrix}^{-1}$ et élever à la puissance n.

3.27. Soit $n \in \mathbb{N}$.
Déduire de la question précédente une expression explicite de a_n et b_n en fonction de ξ et de n.

Comme pour tout $n \in \mathbb{N}$ on a $X_{n+1} = AX_n$, par récurrence immédiate,

$$\forall n \in \mathbb{N}, X_n = A^n X_0$$

et comme $X_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ on a donc

$$\forall n \in \mathbb{N}, \boxed{\begin{aligned} a_n &= \frac{\xi^n + \sigma(\xi)^n}{2} \\ b_n &= \frac{\xi^n - \sigma(\xi)^n}{2\sqrt{d}} \end{aligned}}.$$

Remarque: le passage matriciel n'est pas nécessaire.

En effet on a $\xi^n = a_n + b_n\sqrt{d}$ d'où par la question **1.8.**,

$$a_n = \frac{\xi^n + \sigma(\xi^n)}{2}$$
$$b_n = \frac{\xi^n - \sigma(\xi^n)}{2\sqrt{d}}$$

et on conclut car d'après la question **1.7.**

$$\sigma(\xi^n) = \sigma(\xi)^n.$$

3.28. Donner un équivalent simple quand $k \to +\infty$ de

$$\operatorname{card}\left(\mathcal{S}_{(\mathrm{PF})} \cap [\![-k, k]\!] \times \mathbb{R}\right)$$

On a par les parties précédentes et par les symétries

$$\begin{aligned}\operatorname{card}\left(\mathcal{S}_{(\mathrm{PF})} \cap [\![-k, k]\!] \times \mathbb{R}\right) &= 2\operatorname{card}\left(\mathcal{S}_{(\mathrm{PF})} \cap [\![0, k]\!] \times \mathbb{R}\right) \\ &= 4\operatorname{card}\left(\{n \in \mathbb{N} | 0 \leq a_n \leq k\}\right) - 2\end{aligned}$$

(Le facteur 4 est issu des symétries $z \mapsto -z$ et $z \mapsto \frac{1}{z}$ et le facteur -2 des solution $(1, 0)$ et $(-1, 0)$ comptées deux fois par ces symétries.).
Soit $k > 1$.
Soit $n \in \mathbb{N}$. Comme $\sigma(\xi) = \frac{1}{\xi}$ on a, par étude de trinôme,

$$\begin{aligned}0 \leq a_n \leq k &\Leftrightarrow 0 \leq \xi^n + \frac{1}{\xi^n} \leq 2k \\ &\Leftrightarrow (\xi^n)^2 - 2k(\xi^n) + 1 \leq 0 \\ &\Leftrightarrow \xi^n \in \left[k - \sqrt{k^2-1}, k + \sqrt{k^2-1}\right] \\ &\Leftrightarrow n\ln(\xi) \in \left[\ln\left(k - \sqrt{k^2-1}\right), \ln\left(k + \sqrt{k^2-1}\right)\right]\end{aligned}$$

Or lorsque $k \to +\infty$ on a

$$\begin{aligned}\ln\left(k + \sqrt{k^2-1}\right) &= \ln\left(k\left(1 + \sqrt{1 - \frac{1}{k^2}}\right)\right) \\ &= \ln(k) + \ln(2 + o_{k\to+\infty}(1)) \\ &= \ln(2k) + o_{k\to+\infty}(1)\end{aligned}$$

et comme $\ln\left(k - \sqrt{k^2-1}\right) + \ln\left(k + \sqrt{k^2-1}\right) = 0$ on en déduit de même que

$$\ln\left(k - \sqrt{k^2-1}\right) = -\ln(2k) + o_{k\to+\infty}(1)$$

Par conséquent l'équivalent asymptotique est (à détailler si nécessaire)

$$\boxed{\operatorname{card}\left(\mathcal{S}_{(\mathrm{PF})} \cap [\![-k, k]\!] \times \mathbb{R}\right) \sim \frac{4\ln(2k)}{\ln(\xi)}}.$$

4 Existence d'une solution non triviale

4.29. Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et $C \in \mathbb{R}_+$. Montrer que

$$\left|\frac{a}{b} - \sqrt{d}\right| \leq \frac{C}{b^2} \Rightarrow |a^2 - db^2| \leq (2\sqrt{d} + C)C.$$

Supposons que

$$\left|\frac{a}{b} - \sqrt{d}\right| \leq \frac{C}{b^2}.$$

Alors par inégalité triangulaire

$$\left|\frac{a}{b} + \sqrt{d}\right| \leq \frac{C}{b^2} + 2\sqrt{d} \leq C + 2\sqrt{d}.$$

Par produit d'inégalités positives

$$\left|\left(\frac{a}{b}-\sqrt{d}\right)\left(\frac{a}{b}+\sqrt{d}\right)\right| \leq \frac{C}{b^2}\left(C+2\sqrt{d}\right)$$

ce qui en multipliant par b^2 donne

$$\boxed{|a^2-db^2| \leq (2\sqrt{d}+C)C}.$$

4.30. Soit $x \in \mathbb{R}$ et $N \in \mathbb{N}^*$.
Montrer qu'il existe $k, l \in [\![0, N]\!]$ tels que $k \neq l$ et

$$|\{kx\}-\{lx\}| \leq \frac{1}{N}.$$

On partitionne l'intervalle $[0,1[$ en N intervalles $\left(\left[\frac{i}{N}, \frac{i+1}{N}\right[\right)_{i\in[\![0,N-1]\!]}$.
Comme il y à $N+1$ éléments de la forme $\{kx\}$, $k \in [\![0,N]\!]$, par le principe des tiroirs, il existe $k, l \in [\![0,N]\!]$ tels que $k \neq l$ et $\{kx\}$ et $\{lx\}$ appartiennent au même intervalle.
Et avec $i \in [\![0, N-1]\!]$ tel que $\{kx\}$ et $\{lx\}$ appartiennent à $\left[\frac{i}{N}, \frac{i+1}{N}\right[$ on a en particulier

$$\boxed{|\{kx\}-\{lx\}| \leq \frac{1}{N}}$$

4.31. Soit $x \in \mathbb{R}$ et $N \in \mathbb{N}^*$.
En déduire qu'il existe $p, q \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|x-\frac{p}{q}\right| \leq \frac{1}{Nq}.$$

Soient k et l comme à la question **4.30.**. Sans perte de généralité on a $k > l$.
Alors

$$|(kx-\lfloor kx\rfloor)-(lx-\lfloor lx\rfloor)| \leq \frac{1}{N}$$

c'est à dire

$$|(k-l)x-(\lfloor kx\rfloor-\lfloor lx\rfloor)| \leq \frac{1}{N}$$

ou encore comme $k > l$,

$$\left|x-\frac{\lfloor kx\rfloor-\lfloor lx\rfloor}{k-l}\right| \leq \frac{1}{N(k-l)}$$

ce qui en posant

$$p = \lfloor kx\rfloor - \lfloor lx\rfloor$$
$$q = k-l$$

est

$$\boxed{\left|x-\frac{p}{q}\right| \leq \frac{1}{Nq}}.$$

4.32. Soit $x \in \mathbb{R}\backslash\mathbb{Q}$.
Montrer qu'il existe une infinité de couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|x-\frac{p}{q}\right| \leq \frac{1}{q^2}.$$

On remarque que comme $q \in [\![1, N]\!]$, le couple (p, q) construire à la question **4.31.**

$$\left|x-\frac{p}{q}\right| \leq \frac{1}{Nq} \leq \frac{1}{q^2}.$$

On construit par récurrence une suite $((p_n, q_n))_{n\in\mathbb{N}}$ vérifiant de plus

$$\forall n \in \mathbb{N}, \left|x - \frac{p_{n+1}}{q_{n+1}}\right| < \left|x - \frac{p_n}{q_n}\right|$$

ce qui assure que les couples sont distincts.

► **Initialisation**
On prend par exemple $(p_0, q_0) = (\lfloor x \rfloor, 1)$.

► **Hérédité**
Soit $n \in \mathbb{N}$. Supposons que $((p_0, q_0), \dots, (p_n, q_n))$ construits vérifiant la propriété.
Comme x est irrationnel on a $\left|x - \frac{p_n}{q_n}\right| > 0$.
Posons $N = \left\lfloor \frac{1}{\left|x - \frac{p_n}{q_n}\right|} \right\rfloor + 1$ et construisons (p_{n+1}, q_{n+1}) comme à la question **4.31.**.
Alors $\frac{1}{Nq_{n+1}} \leq \frac{1}{N}$ et donc

$$\left|x - \frac{p_{n+1}}{q_{n+1}}\right| < \left|x - \frac{p_n}{q_n}\right|.$$

Et on donc (p_{n+1}, q_{n+1}) convient bien.

► **Conclusion**
On a donc construit une suite $((p_n, q_n))_{n\in\mathbb{N}}$ de couples deux à deux distincts vérifiant pour tout $n \in \mathbb{N}$,

$$\forall n \in \mathbb{N}, \boxed{\left|x - \frac{p_n}{q_n}\right| \leq \frac{1}{{q_n}^2}}$$

4.33. En utilisant les questions précédentes montrer qu'il existe $\eta \in \mathbb{Z}$ tel que l'ensemble

$$\left\{z \in \mathbb{Z}[\sqrt{d}] \middle| N(z) = \eta\right\}$$

est infini.

On applique la question **4.32.** à $x = \sqrt{d}$ et on obtient une infinité de couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|\sqrt{d} - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

et donc par la question **4.29.** donne une infinité de $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que

$$\left|p^2 - dq^2\right| \leq (2\sqrt{d} + 1) \times 1 \leq \lceil 2\sqrt{d} + 1 \rceil.$$

On a donc une infinité de couples (p, q) tels que $N(p + q\sqrt{d}) \in [\![-\lceil 2\sqrt{d} + 1\rceil, \lceil 2\sqrt{d} + 1\rceil]\!]$ qui est fini.
Par le principe des tiroirs (infinité de chaussettes dans un nombre fini de tiroirs),

$$\boxed{\exists \eta \in \mathbb{Z}, \left\{z \in \mathbb{Z}[\sqrt{d}] \middle| N(z) = \eta\right\} \text{ est infini}}.$$

On fixe dans la suite un tel $\eta \in \mathbb{Z}$.

4.34. Montrer qu'il existe $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ tels que
- $|z_1| \neq |z_2|$,
- $N(z_1) = N(z_2) = \eta$,
- $\pi_1(z_1) \equiv \pi_1(z_2)[\eta]$,
- $\pi_2(z_1) \equiv \pi_2(z_2)[\eta]$.

L'ensemble des $z \in \mathbb{Z}[\sqrt{d}]$ tels que $N(z) = \eta$ est infini.
De plus l'ensemble des valeurs prises par $(\pi_1(z), \pi_2(z))$ modulo η est de cardinal majoré par η^2 et donc fini.
Donc par principe des tiroirs (infinité de chaussettes dans un nombre fini de tiroirs), il existe une infinité de z_1, z_2 tels que $N(z) = \eta$,$\pi_1(z_1) \equiv \pi_1(z_2)[\eta]$ et $\pi_2(z_1) \equiv \pi_2(z_2)[\eta]$.
En particulier il existe de tels z_1, z_2.

On fixe désormais de tels z_1, z_2.

4.35. Montrer que $\dfrac{z_1\sigma(z_2)}{\eta} \in \mathbb{Z}[\sqrt{d}]$.

Posons $(a_1, b_1) = (\pi_1(z_1), \pi_2(z_1))$ et $(a_2, b_2) = (\pi_1(z_2), \pi_2(z_2))$.
Alors on a

$$\frac{z_1\sigma(z_2)}{\eta} = \frac{a_1a_2 - db_1b_2}{\eta} + \frac{-a_1b_2 + a_2b_1}{\eta}\sqrt{d}.$$

Or par on a $a_1 \equiv a_2[\eta]$ et $b_1 \equiv b_2[\eta]$.
Et donc

$$a_1b_2 \equiv a_2b_1[\eta]$$

d'où $\frac{-a_1b_2+a_2b_1}{\eta} \in \mathbb{Z}$. De même

$$\begin{aligned} a_1a_2 - db_1b_2 &\equiv (a_1)^2 - d(b_1)^2[\eta] \\ &\equiv \eta[\eta] \\ &\equiv 0[\eta] \end{aligned}$$

d'où $\frac{a_1a_2-db_1b_2}{\eta} \in \mathbb{Z}$.
Par conséquent

$$\boxed{\frac{z_1\sigma(z_2)}{\eta} \in \mathbb{Z}[\sqrt{d}]}.$$

4.36. Conclure que (PF) admet au moins une solution non triviale.

On a comme si $\frac{z_1\sigma(z_2)}{\eta} = \pm 1$ alors en multipliant par z_2, $z_1\frac{N(z_2)}{\eta} = \pm z_2$ i.e $z_2 = \pm z_1$.
Par contraposée

$$\boxed{\frac{z_1\sigma(z_2)}{\eta} \neq \pm 1}.$$

De plus $N\left(\frac{z_1\sigma(z_2)}{\eta}\right) = \frac{1}{\eta^2}N(z_1)N(z_2)$ d'où

$$\boxed{N\left(\frac{z_1\sigma(z_2)}{\eta}\right) = 1}$$

ce qui revient par la question **1.13.** à $\boxed{\text{(PF) admet au moins une solution non triviale}}$.

5 Bonus facultatif: Interprétation géométrique

Ne traiter cette partie que si toutes les autres parties ont été traitée.
De nombreux schémas sont attendus dans cette partie.

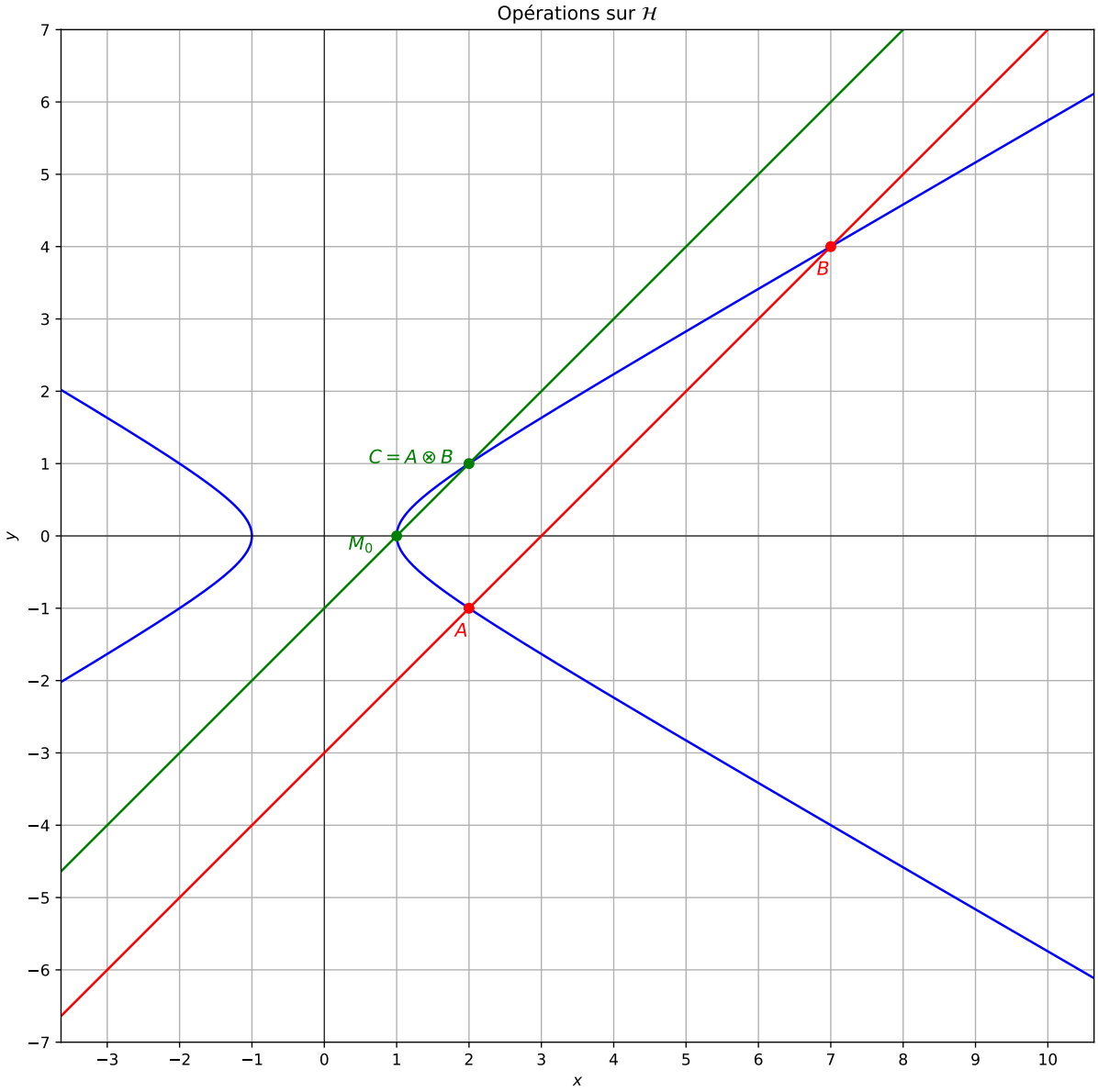
Dans cette partie on note

$$\mathcal{H} = \left\{(x, y) \in \mathbb{R}^2 \middle| x^2 - dy^2 = 1\right\}$$

et

$$\mathcal{H}^{\mathbb{Z}} = \mathcal{H} \cap \mathbb{Z}^2.$$

On note aussi M_0 le point de coordonnées $(1, 0)$.
Soient A, B deux points de $\mathcal{H}$.
On note Δ_{AB} la droite passant par A et B si $A \neq B$ et la tangente à $\mathcal{H}$ en A si $A = B$.
On note aussi $\widetilde{\Delta_{AB}}$ la droite parallèle à Δ_{AB} et passant par M_0.



5.37. Soient A, B de points de $\mathcal{H}$.

Montrer qu'il existe un unique point C tel que $\widetilde{\Delta_{AB}} \cap \mathcal{H} = \{M_0, C\}$.

On note alors

$$A \otimes B = C.$$

5.38. Interpréter géométriquement les résultats des parties précédentes.