# Corrigé du DS 4



**Exercice 1.** Racines carrées matricielles.

1. Racines carrées d'une matrice diagonale.

   Dans cette question, on considère la matrice $D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$.

   (a) On a $DM = \begin{pmatrix} a & b \\ 4c & 4d \end{pmatrix}$ et $MD = \begin{pmatrix} a & 4b \\ c & 4d \end{pmatrix}$.
   Supposons que $DM = MD$. En égalant les coefficients non diagonaux, on obtient $b = 4b$ et $4c = c$, ce qui amène $b = c = 0$ et montre que $M$ est diagonale.
   La réciproque est vraie car deux matrices diagonales commutent toujours.

   (b) On l'a compris à la question précédente, il suffit de prouver que $X$ commute avec $D$. Et c'est le cas, puisque $X$ commute avec $X^2$, et donc avec $D$.

   (c) Analyse. Soit $X \in M_n(\mathbb{R})$ une matrice telle que $X^2 = D$.
   D'après (b), $X$ est diagonale, de la forme $X = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.
   L'équation $X^2 = D$ s'écrit $\begin{pmatrix} x^2 & 0 \\ 0 & y^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$ et amène $x^2 = 1$ et $y^2 = 4$, soit $x = \pm 1$ et $y = \pm 2$.
   Synthèse : il est clair que si $(x, y) \in \{(1, 2), (-1, 2), (1, -2), (-1, -2)\}$, alors

   $$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

   Conclusion : l'équation $X^2 = D$ possède quatre solutions dans $M_2(\mathbb{R})$ :

   $$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -2 \end{pmatrix}.$$

2. Racines carrées d'une matrice diagonalisable.

   Dans cette question, on considère les matrices $A = \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

   (a) On pouvait utiliser le pivot de Gauss pour répondre à cette question.
   On peut aussi profiter du fait qu'il s'agit d'une matrice de taille 2. On a $\det(P) = 1 \neq 0$, ce qui donne que $P$ est inversible et que $P^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$. Un calcul permet de vérifier que $A = PDP^{-1}$.

   (b) On a

   $$\begin{aligned} X^2 = A &\iff X^2 = PDP^{-1} \\ &\iff P^{-1}X^2P = D \\ &\iff \left(P^{-1}XP\right)\left(P^{-1}XP\right) = D \quad (\text{car } PP^{-1} = I_2) \\ &\iff \left(P^{-1}XP\right)^2 = D. \end{aligned}$$

   (c) Notons $\Delta_1, \Delta_2, \Delta_3, \Delta_4$ les quatre solutions de $X^2 = D$ (dans l'ordre où on les a écrites à la question 1). D'après la question précédente, pour $X \in M_2(\mathbb{R})$, on a

   $$X^2 = A \iff \exists i \in [\![1, 4]\!] \;\; P^{-1}XP = \Delta_i \iff \exists i \in [\![1, 4]\!] \;\; X = P\Delta_i P^{-1}.$$

   L'équation $X^2 = A$ possède donc les quatre solutions $\{P\Delta_i P^{-1} \mid i \in [\![1, 4]\!]\}$.
   On les calcule, ce sont les matrices

   $$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 3 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -2 & -3 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -2 & -1 \\ 0 & -1 \end{pmatrix}.$$

**Exercice 2.** Matrices de permutations.

1. (a) $P_\gamma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

   (b) $P_{\text{id}} = I_n$.

   (c) Soit $\sigma \in S_n$. Par définition de la trace, $\text{tr}(P_\sigma) = \sum_{i=1}^{n} \delta_{i,\sigma(i)}$.
   Pour $i \in [\![1, n]\!]$, on a $\delta_{i,\sigma(i)} = 1$ ssi $\sigma(i) = i$. Ainsi, la trace de $P_\sigma$ est le nombre des *points fixes* de la permutation $\sigma$.

2. Pour $M$ dans $M_n(\mathbb{R})$ et $(i, j) \in [\![1, n]\!]^2$, on note $[M]_{i,j}$ le coefficient de $M$ à la positions $(i, j)$.
   Soit $(\sigma, \sigma') \in (S_n)^2$ et $(i, j) \in\in [\![1, n]\!]^2$.

   $$\begin{aligned} [P_\sigma P_{\sigma'}]_{i,j} &= \sum_{k=1}^{n} [P_\sigma]_{i,k} [P_{\sigma'}]_{k,j} \\ &= \sum_{k=1}^{n} \delta_{i,\sigma(k)} \delta_{k,\sigma'(j)} \\ &= \delta_{i,\sigma(\sigma'(j))} \end{aligned}$$

À la dernière ligne on a seulement gardé le terme « $k = \sigma'(j)$ » car les autres termes sont nuls. Ceci démontre donc que

$$[P_\sigma P_{\sigma'}]_{i,j} = \delta_{i,\sigma\circ\sigma'(j)} = [P_{\sigma\circ\sigma'}]_{i,j}\,,$$

et achève donc de démontrer que

$$\boxed{P_\sigma P_{\sigma'} = P_{\sigma\circ\sigma'}.}$$

3. Soit $\sigma \in S_n$. Sa réciproque $\sigma^{-1}$ existe, ainsi que la matrice $P_{\sigma^{-1}}$ associée. On calcule

$$P_\sigma P_{\sigma^{-1}} = P_{\sigma\circ\sigma^{-1}} = P_{\mathrm{id}} = I_n.$$

$$P_{\sigma^{-1}} P_\sigma = P_{\sigma^{-1}\circ\sigma} = P_{\mathrm{id}} = I_n.$$

Ceci nous donne que

$$\boxed{P_\sigma \in GL_n(\mathbb{K}) \quad \text{et} \quad (P_\sigma)^{-1} = P_{\sigma^{-1}}}$$

4. Posons

$$\varphi : \left\{ \begin{array}{ccc} S_n & \to & GL_n(\mathbb{R}) \\ \sigma & \mapsto & P_\sigma \end{array} \right. .$$

L'application $\varphi$ est bien définie sur $S_n$ et prend bien ses valeurs dans $GL_n(\mathbb{R})$ d'après la question précédente. Il s'agit d'un morphisme de groupes de $(S_n, \circ)$ dans $(GL_n(\mathbb{R}), \times)$. En effet, d'après la question 2,

$$\forall (\sigma, \sigma') \in (S_n)^2 \quad \varphi(\sigma\circ\sigma') = P_{\sigma\circ\sigma'} = P_\sigma P_{\sigma'} = \varphi(\sigma) \times \varphi(\sigma').$$

L'ensemble $P_n(\mathbb{R})$ est par définition l'image de $S_n$ par $\varphi$. C'est donc un sous-groupe de $GL_n(\mathbb{R})$ comme image directe d'un (sous-)groupe par un morphisme de groupes. Notons donc

$$\widetilde{\varphi} : \left\{ \begin{array}{ccc} S_n & \to & P_n(\mathbb{R}) \\ \sigma & \mapsto & P_\sigma \end{array} \right. .$$

Il s'agit encore d'un morphisme de groupes, surjectif par définition.
Soit $\sigma \in S_n$ tel que $\widetilde{\varphi} = I_n$. On a donc $P_\sigma = I_n$. En lisant les coefficients diagonaux de $P_\sigma$, on obtient que

$$\forall i \in [\![1, n]\!] \quad \delta_{i,\sigma(i)} = 1 \quad \text{soit} \quad \sigma(i) = i.$$

On a donc que $\sigma = \mathrm{id}$. Le noyau de $\widetilde{\varphi}$ est trivial : $\widetilde{\varphi}$ est donc injectif.

L'application $\widetilde{\varphi}$ est donc un isomorphisme : $\boxed{P_n(\mathbb{R}) \text{ est isomorphe à } S_n}$.

# **Problème 2** : Entiers sommes de deux carrés.

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

1. Propriétés générales.
   (a) C'est un exemple du cours. On vérifie facilement que
   — $\forall (u, u') \in (\mathbb{Z}[i])^2 \quad u - u' \in \mathbb{Z}[i]$,
   — $\forall (u, v) \in (\mathbb{Z}[i])^2 \quad u \times v \in \mathbb{Z}[i]$,
   — $1 \in \mathbb{Z}[i]$.

   (b) i. Soit $u \in \mathbb{Z}[i]$, qui s'écrit $u = a + ib$, avec $a$ et $b$ deux entiers relatifs. On a $N(u) = u\overline{u} = |u|^2 = a^2 + b^2$ et donc $N(u) \in \mathbb{N}$.
   ii. Soit $(u, v) \in (\mathbb{Z}[i])^2$. On calcule

   $$N(uv) = |uv|^2 = |u|^2|v|^2 = N(u)N(v).$$

   (c) Supposons que $u$ est inversible dans $\mathbb{Z}[i]$. Alors il existe $v \in \mathbb{Z}[i]$ tel que $uv = 1$. On applique $N$ : on obtient $N(uv) = N(1)$, soit $N(u)N(v) = 1$. On obtient donc que $N(u)$ est un inversible de $\mathbb{Z}$. Puisqu'il est positif, il vaut nécessairement 1. Si on écrit $u = a + ib$, avec $a$ et $b$ entiers, on obtient $a^2 + b^2 = 1$, ce qui donne $(a^2, b^2) = (1, 0)$ ou $(a^2, b^2) = (0, 1)$. On obtient donc que $(a, b)$ vaut $(1, 0)$ ou $(-1, 0)$, ou $(0, 1)$, ou $(0, -1)$ et donc que

   $$u \in \{1, -1, i, -i\}\,.$$

   Réciproquement, ces quatre éléments sont inversibles dans $\mathbb{Z}[i]$ : les deux premiers sont leur propre inverse, et les suivants sont inverses l'un de l'autre.

2. Divisibilité dans l'anneau $\mathbb{Z}[i]$.
   On s'est donné $u$ et $v$ deux éléments de $\mathbb{Z}[i]$.
   (a) Tout ça s'écrit bien, de la même façon que dans $\mathbb{Z}$.
   (b) Idem, il suffit d'écrire ça tranquillement.
   (c) Supposons que $u \mid v$ et $v \mid u$. Il existe donc $s$ et $t$ dans $\mathbb{Z}[i]$ tels que $v = us$ et $u = vt$. Ceci amène $v = vst$, soit $v(1 - st) = 0$. On travaille dans $\mathbb{C}$, anneau intègre : on obtient donc $v = 0$ ou $st = 1$. Dans le premier cas, $v = 0$ puis $u = vt = 0$. On a bien $u = \pm v$. Dans le deuxième cas, $st = 1$, ce qui amène que $t \in U$ puis que $t = \pm 1$ ou $t = \pm i$ d'après 1-(c). On obtient bien que alors $u = \pm v$ ou $u = \pm iv$.

(d) Supposons que $u \mid v$. Il existe donc $s$ dans $\mathbb{Z}[i]$ tels que $v = us$. Appliquons $N$ : on obtient $N(v) = N(u)N(s)$. Puisque les trois images par $N$ sont des entiers, on a bien que $N(u)$ divise $N(v)$ dans $\mathbb{Z}$.

(e) Soit $u = a + ib$ un diviseur de $1 + i$. Alors $N(d)$ divise $N(1 + i)$, donc divise 2. On obtient donc $N(d) = 1$ ou $N(d) = 2$. Dans le premier cas, on a $a^2 + b^2 = 1$, qui conduit à $d \in U$. Il est facile de vérifier réciproquement que ces nombres dans $U$ sont des diviseurs de $1+i$. Dans le second cas, $N(d) = 2$, ce qui conduit à $a^2 = b^2 = 1$, soit $a = \pm 1$ et $b = \pm 1$, et donc $d = 1 + i$, ou $d = 1 - i$, ou $d = -1+i$ ou $d = -1 - i$. Il est facile de vérifier réciproquement que ce sont là des diviseurs de $1 + i$ dans $\mathbb{Z}[i]$. Par exemple $1 - i = (-i) \times (1 + i)$.
La liste des diviseurs de $1 + i$ est donc

$$1, \quad -1, \quad i, \quad -i \quad 1+i, \quad 1-i \quad -1+i \quad -1-i.$$

3. Division euclidienne dans $\mathbb{Z}[i]$.

(a) Soit $z \in \mathbb{C}$ ; on note $x$ et $y$ respectivement ses parties réelles et imaginaires.
Soit $a$ l'entier le plus proche de $x$ (en choisissant le plus grand si $x$ est la moyenne de deux entiers).

$$a = \begin{cases} \lfloor x \rfloor & \text{si } \lfloor x \rfloor \leq x < \lfloor x \rfloor + \frac{1}{2} \\ \lfloor x \rfloor + 1 & \text{si } \lfloor x \rfloor + \frac{1}{2} \leq x < \lfloor x \rfloor + 1 \end{cases}$$

De même on note $b$ l'entier le plus proche de $y$.
On pose alors $u = a + ib$ et on a

$$N(z-u) = (x-a)^2 + (y-b)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \leq \frac{1}{2} < 1.$$

Le nombre $u$ qu'on vient de définir n'est pas unique : par exemple $\frac{1}{2} + \frac{1}{2}i$ est à équidistance des quatre nombres 0, 1, $i$, $1 + i$.

(b) Soit $u \in \mathbb{Z}[i]$ et $v \in \mathbb{Z}[i]^*$. D'après la question précédente, il existe un élément $q$ dans $\mathbb{Z}[i]$ tel que $N\left(\frac{u}{v} - q\right) < 1$. Posons $r = u - vq$. On a donc $r = v\left(\frac{u}{v} - q\right)$, ce qui donne, en appliquant $N$,

$$N(r) = N(v)N\left(\frac{u}{v} - q\right) < N(v) \cdot 1.$$

L'inégalité stricte s'obtient car $N(v) > 0$ puisque $v \neq 0$.
On a bien défini $(q, r)$ tel que

$$u = vq + r \quad \text{et} \quad N(r) < N(v).$$

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

4. Il est clair que $\delta\mathbb{Z}[i] \subset \mathbb{Z}[i]$.
Puisque $0 \in \mathbb{Z}[i]$, on voit que $0 \in \delta\mathbb{Z}[i]$ en écrivant $0 = \delta \times 0$.
Soient $u'$ et $v'$ deux éléments de $\delta\mathbb{Z}[i]$. Ils s'écrivent $u' = \delta u$ et $v' = \delta v$, avec $u$ et $v$ dans $\mathbb{Z}[i]$. On a donc $u' - v' = \delta(u - v)$, ce qui donne $u' - v' \in \delta\mathbb{Z}[i]$ puisque $u - v \in \mathbb{Z}[i]$. Par caractérisation, $\delta\mathbb{Z}[i]$ est un sous-groupe de $(\mathbb{Z}[i], +)$.

5. Soit $u, v \in \mathbb{Z}[i]$ avec $u \neq 0$ ou $v \neq 0$. On note $I(u, v) = \{uz + vz' \mid z, z' \in \mathbb{Z}[i]\}$.

(a) $u = u \times 1 + v \times 0$ et $v = u \times 0 + v \times 1$ : puisque 0 et 1 sont dans $\mathbb{Z}[i]$, on a $u$ et $v$ dans $I(u, v)$.

(b) Puisque $u \in I(u, v)$, l'ensemble $A$ contient $N(u)$, qui est non nul. L'ensemble $A$ est donc une partie non vide de $\mathbb{N}^*$ : elle a un plus petit élément $d > 0$.

(c) L'inclusion $\delta\mathbb{Z}[i] \subset I(u, v)$ est simple : elle vient du fait que $\delta \in I(u, v)$ et que $(I(u, v), +)$ est un sous-groupe de $\mathbb{Z}[i]$.
Soit $z \in I(u, v)$. Puisque $\delta \neq 0$, on déduit de 3(b) l'existence d'un couple $(q, r)$ d'éléments de $\mathbb{Z}[i]$ tels que $z = \delta q + r$ avec $N(r) < N(\delta)$. Puisque $r = z - \delta q$ et que $z$ et $\delta$ sont dans $I(u, v)$, alors $r \in I(u, v)$ par propriété de sous-groupe.
Si $r$ est non nul, l'inégalité $N(r) < N(\delta)$ contredit la minimalité dans la définition de $\delta$. On en déduit que $r = 0$ et donc que $\delta$ divise $z$ : $z \in \delta\mathbb{Z}[i]$.
Par double inclusion, $I(u, v) = \delta\mathbb{Z}[i]$.

(d) Puisque $u$ et $v$ sont dans $I(u, v)$, ils sont donc dans $\delta\mathbb{Z}[i]$ : $\delta$ divise $u$ et $v$.
Soit $w \in \mathbb{Z}[i]$.
Si $w$ divise $\delta$, puisque $\delta$ divise $u$ et $v$, alors $w$ divise $u$ et $v$ par transitivité.
Si réciproquement $w$ divise $u$ et $v$, il divise toute combinaison $uz + vz'$ avec $z$ et $z'$ deux éléments de $\mathbb{Z}[i]$ (voir question 2-(b)). Puisque $\delta$ est une de ces combinaisons, $w$ divise $\delta$.

6. On a supposé que $u$ et $v$ sont premiers entre eux, soit

(a) Par définition de $\delta$, il existe $z$ et $z'$ dans $\mathbb{Z}[i]$ tels que $uz + vz' = \delta$.
- Si $\delta = 1$, on a le résultat voulu.
- Si $\delta = -1$, on remplace $(z, z')$ par $(-z, -z')$ (qui est encore dans $(\mathbb{Z}[i])^2$) et on a encore $uz + vz' = 1$.
- Si $\delta = i$, on remplace $(z, z')$ par $(-iz, -iz')$ et on a encore $uz + vz' = 1$.
- Si $\delta = -i$, on remplace $(z, z')$ par $(iz, iz')$ et on a encore $uz + vz' = 1$.

(b) Soit $w \in \mathbb{Z}[i]$.
En utilisant les nombres $z$ et $z'$ introduits dans la question précédente, on a $w = uwz + vwz'$.
Puisque $u$ divise $uwz$ et divise $vwz'$, il divise leur somme $w$.

7. (a) Soit $\delta$ un PGCD de $u$ et $v$. Puisque $\delta$ divise $u$ qui est irréductible, $\delta$ vaut $\pm 1$, $\pm i$, $\pm u$, $\pm iu$. Si $\delta$ vaut $\pm u$ ou $\pm iu$, puisque $\delta$ divise $v$, on aurait $u$ divise $v$ ce qui n'est pas. Ceci prouve que $\delta \in U$ : $u$ et $v$ sont premiers entre eux.
   (b) Supposons que $u$, qui est irréductible, ne divise pas $v$. La question précédente donne que $u$ et $v$ sont premiers entre eux. Puisque $u$ divise $vw$, il divise $w$ d'après la question 6-(b), qui est une sorte un « lemme de Gauss dans $\mathbb{Z}[i]$ ».

## Partie III : Nombres premiers sommes de deux carrés.

8. • Supposons que $p$ est somme de deux carrés : $p = a^2 + b^2$, avec $(a, b) \in \mathbb{Z}^2$. On a donc $p = (a + ib)(a - ib)$, et $a + ib$ n'est pas un élément de $U$ (on aurait sinon $p = 1$ en appliquant $N$). Ceci prouve que $p$ n'est pas irréductible dans $\mathbb{Z}[i]$.

   • Supposons que $p$ n'est pas irréductible dans $\mathbb{Z}[i]$.
   Alors, il existe $(a, b) \in \mathbb{Z}^2$ et $(c, d) \in \mathbb{Z}^2$ tels que $p = (a + ib)(c + id)$, avec $a + ib$ et $c + id$ qui ne sont pas dans $U$. Appliquons $N$ : on obtient

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

   Puisque $a+ib$ n'est pas dans $U$, $a^2+b^2 \neq 1$. De même $c^2+d^2 \neq 1$. Les deux facteurs valent donc $p$ ou $p^2$ puisque $p$ est premier. Puisque leur produit vaut $p^2$, ils valent $p$ tous les deux : $p = a^2 + b^2$.

9. (a) Soit $x \in [\![1, p-1]\!]$.
   <u>Existence</u> : Puisque $p$ (premier) ne divise pas $x$, il est premier avec $x$. D'après le théorème de Bézout, il existe deux entiers relatifs $r$ et $s$ tels que

$$xr + ps = 1.$$

   Passons modulo $p$ : on obtient $xr \equiv 1$ $[p]$. On peut supposer que $r \in [\![0, p-1]\!]$, quitte à remplacer $r$ par le reste dans la division euclidienne de $r$ par $p$. Puisque $xr$ vaut 1 modulo $p$, $r$ ne vaut pas 0. On peut donc poser $y = r$ : ce nombre appartient à $[\![1, p-1]\!]$.

   <u>Unicité</u>. Soient $y$ et $y'$ dans $[\![1, p-1]\!]$ tels que $xy \equiv 1$ $[p]$ et $xy' \equiv 1$ $[p]$. Par différence, $x(y-y') = 0$ $[p]$ donc $p$ divise $x(y-y')$. Puisque $x$ et $p$ sont premiers entre eux, $p$ divise $y - y'$. Or, la différence $y - y'$ est entre $p-1$ et son opposé : et le seul multiple de $p$ dans cet intervalle est 0 : on a $y = y'$.

   (b) Il est clair que $1^2 \equiv 1$ $[p]$. De même $p - 1 \equiv -1$ $[p]$ donc $(p-1)^2 \equiv 1$ $[p]$.
   Réciproquement, si $x$ est un entier de $[\![1, p-1]\!]$ tel que $x^2 \equiv 1$ $[p]$, alors $p$ divise $x^2 - 1 = (x+1)(x-1)$, et puisque $p$ est premier, $p$ divise $x+1$ ou $p$ divise $x - 1$. Puisque $x + 1 \in [\![2, p]\!]$ et $x + 1 \in [\![0, p-2]\!]$, on a nécessairement $x + 1 = p$ ou $x - 1 = 0$, soit $x = p - 1$ ou $x = 1$.

   (c) On veut évaluer modulo $p$ le produit

$$1 \times 2 \times \cdots \times (p-1).$$

   Nous avons montré en question (a) que tous ces entiers ont un inverse modulo $p$ entre 1 et $p-1$. Et comme 1 et $p-1$ sont les seuls facteurs qui sont leur propre inverse (question (b)) chaque facteur du produit

$$2 \times 3 \times \cdots (p-2)$$

   est présents avec son inverse (distinct de lui-même) : ce produit vaut 1. Ainsi,

$$(p-1)! \equiv 1 \times (p-1) \times 1 \ [p] \quad \text{donc} \quad \boxed{(p-1)! \equiv -1 \ [p]}.$$

10. Supposons que $p \neq 2$ et que $p$ est somme de deux carrés. Il existe $a$ et $b$ deux entiers tels que $p = a^2 + b^2$. Les entiers $a$ et $b$ sont de parité contraire, sinon $p$ serait pair, ce qui n'est pas puisque $p$ est premier et différent de 2. Sans perte de généralité, supposons que $a$ est pair. Il s'écrit alors $a = 2a'$ avec $a'$ entier, et donc $a^2 = 4a'^2$, soit $a^2 \equiv 0 \pmod 4$. Puisque $b$ est impair, on a $b \equiv 1$ $[4]$ ou $b \equiv 3$ $[4]$. Or, $1^2$ et $3^2$ valent tous les deux 1 modulo 4 : on a bien $p \equiv 1 \pmod 4$.

11. Supposons que $p \equiv 1$ $[4]$.
   (a) Puisque $p - 1$ est ici un multiple de 4, il est en particulier pair. On peut écrire

$$(p-1)! = \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)\left(\prod_{k=\frac{p-1}{2}+1}^{p-1} k\right) = \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)\left(\prod_{k=1}^{\frac{p-1}{2}} (p-k)\right)$$

   Modulo $p$, $p-k$ est l'opposé de $k$, c'est-à-dire que $p-k \equiv k$ $[p]$. De plus, d'après le théorème de Wilson, $(p-1)! \equiv -1$ $[p]$. En passant modulo $p$, on obtient donc

$$-1 = \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)\left(\prod_{k=1}^{\frac{p-1}{2}} -k\right) \ [p] \quad \text{soit encore} \quad -1 = (-1)^{\frac{p-1}{2}}\left(\prod_{k=1}^{\frac{p-1}{2}} k\right)^2 \ [p].$$

Or, puisque $p-1$ est un multiple de 4, on sait que $\frac{p-1}{2}$ est pair, de sorte que $(-1)^{\frac{p-1}{2}} = 1$, ce qui laisse le résultat demandé.

(b) On s'est donné un entier $a$ tel que $a^2 = -1$ $[p]$, c'est-à-dire tel que $p$ divise $a^2+1 = (a+i)(a-i)$. Si on suppose que $p$ est irréductible dans $\mathbb{Z}[i]$, alors $p$ divise $a+i$ ou $a-i$. Dans le premier cas, cela implique l'existence de deux entiers $c$ et $d$ tels que $p(c+id) = a+i$. On a donc $pd = 1$ et donc $p$ divise 1, ce qui est absurde. La contradiction est la même dans l'autre cas. Ceci démontre que $p$ n'est pas irréductible. Et donc que $p$ est une somme de deux carrés.

12. D'après la question 10, si $p$ est somme de deux carrés, alors il vaut 2 ou bien est congru à 1 modulo 4. Réciproquement, on remarque que $2 = 1^2 + 1^2$ est somme de deux carrés. De plus, d'après la question 11, tout nombre premier congru à 1 modulo 4 est somme de deux carrés. La conclusion mérite le nom de théorème.

$\boxed{\text{Théorème}}$ (de Fermat de Noël) Les nombres premiers sommes de deux carrés sont le nombre 2 ainsi que tous ceux congrus à 1 modulo 4.

## Partie IV : Nombres sommes de deux carrés.

13. (a) Soient $n, n' \in \Sigma$. Il existe $u$ et $u'$ dans $\mathbb{Z}[i]$ tels que $n = N(u)$ et $n' = N'(u')$. On a $nn' = N(u)N(u') = N(uu')$, ce qui amène $nn' \in \Sigma$ puisque $uu' \in \mathbb{Z}[i]$. Plus précisément, si on écrit $u = a+ib$ et $u' = c+id$, alors $uu' = (ac-bd) + i(ad+bc)$. L'égalité $N(u)N(u') = N(uu')$ s'écrit donc

$$\boxed{(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.} \quad \text{(identité de Diophante)}$$

(b) Soit $n \in \Upsilon$. On écrit $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.

Considérons $p$ un diviseur premier de $n$ ($v_p(n) \geq 1$)

— Si $p = 2$, puisque $2 \in \Sigma$, on a $2^{v_2(n)} \in \Sigma$ puisque $\Sigma$ est stable par produit.

— Si $p \equiv 1$ $[4]$, puisque $p \in \Sigma$ (d'après la partie III), on a $p^{v_p(n)} \in \Sigma$ puisque $\Sigma$ est stable par produit.

— Si $p \equiv 3$ $[4]$, puisque par hypothèse $v_p(n)$ est paire, on peut écrire

$$p^{v_p(n)} = \left(p^{v_p(n)/2}\right)^2 + 0^2.$$

Ce qui précède prouve que $n$ est un produit de facteurs tous dans $\Sigma$, ce qui démontre que $n \in \Sigma$, et puisque $\Upsilon$ ne contient pas 0, on a bien $\boxed{\Sigma \setminus \{0\} = \Upsilon}$.

14. $p$ est un nombre premier congru à 3 modulo 4 et divisant $n = a^2 + b^2$.

(a) Puisque $p$ n'est pas congru à 1 modulo 4, il n'appartient pas à $\Sigma$ (d'après 10-(a) par contraposée), et donc $p$ est irréductible dans $\mathbb{Z}[i]$ (d'après 8).
Par hypothèse, $p$ divise $a^2 + b^2$ dans $\mathbb{Z}$, a fortiori dans $\mathbb{Z}[i]$, ce qu'on peut écrire

$$p \mid (a+ib)(a-ib)$$

Par irréductibilité, $p \mid a+ib$ ou $p \mid a-ib$. Dans le second cas, on peut écrire $a - ib = pz$ avec $z \in \mathbb{Z}[i]$.
En conjuguant, on a $a + ib = p\bar{z}$. Ceci prouve que $p$ divise $a+ib$.

(b) Puisque $p$ divise $a+ib$, il existe $(a', b') \in \mathbb{Z}^2$ tel que $a+ib = p(a'+ib')$, ce qui donne $pa' = a$ et $pb' = b$. Ainsi $p$ divise $a$ et $p$ divise $b$ dans $\mathbb{Z}$. On a donc $a' = \frac{a}{p}$ et $b' = \frac{b}{p}$ puis

$$n = (a+ib)(a-ib) = p^2(a'+ib')(a'-ib') = p^2(a'^2 + b'^2).$$

Ceci démontre que $p^2$ divise $n$ et que $\dfrac{n}{p^2} = a'^2 + b'^2 \in \Sigma$.

(c) Supposons que $v_p(n)$ est impaire. On l'écrit alors $v_p(n) = 2k+1$ avec $k \in \mathbb{N}$. D'après la question précédente, $\frac{n}{p^2} \in \Sigma$. En itérant, on obtient que $\frac{n}{p^{2k}} \in \Sigma$.
Or, $v_p\left(\frac{n}{p^{2k}}\right) = v_p(n) - 2k = 1$. Ceci est absurde car si on applique le résultat de la question précédente à $\frac{n}{p^{2k}}$ (qui est dans $\Sigma$), on obtient que sa valuation $p$-adique est supérieure à 2. Cette contradiction amène que $v_p(n)$ est paire.

15. Voici le théorème établi par ce problème :

$\boxed{\text{Théorème}}$ Les entiers sommes de deux carrés sont 0, 2, et tous ceux dont les diviseurs premiers congrus à 3 modulo 4 sont associés à une valuation paire.

Application. 1789 est premier, et congru à 1 modulo 4 : il est somme de deux carrés, ainsi que $3578 = 2 \times 1789$ puisque 2 est aussi somme de deux carrés. En revanche, $5367 = 3 \times 1789$ n'est pas somme de deux carrés car $3 \equiv 3$ $[4]$ et ce nombre premier a une valuation impaire dans la décomposition primaire de 5367.