2.6 Correction de quelques exercices

Dans ces premiers exercices, nous manipulons surtout des calculs ; peu de questions de fond

Exercice 2 :

1. *Soit $(R,+,\times)$ un anneau commutatif de caractéristique p où p est un nombre premier. Démontrer que $(a+b)^p = a^p + b^p$*

   Nous pouvons utiliser la formule du binôme :

   $$(a+b)^p = \sum_{k=0}^{p} \mathrm{C}_p^k a^k b^{p-k} = b^p + a^p + \sum_{k=1}^{p-1} \mathrm{C}_p^k a^k b^{p-k}$$

   Comme, pour $1 \leqslant q \leqslant p-1$, nous avons $\mathrm{C}_p^q = \binom{p}{q} = k_q p$, nous avons alors

   $$\mathrm{C}_p^k a^k b^{p-k} = k_q p a^k b^{p-k} = (pa)\, k_q a^{k-1} b^{p-k} = 0$$

   Et donc $(a+b)^p = a^p + b^p$
2. *En déduire que $(a-b)^p = a^p - b^p$*

   Pas si difficile ; en effet :

   $$a^p = ((a-b)+b)^p = (a-b)^p + b^p \Longleftrightarrow a^p - b^p = (a-b)^p$$

3. *Pour $a_1, a_2, \cdots, a_k$ k éléments de l'anneau R. Montrer que*

   $$(a_1 + a_2 + \cdots + a_k)^p = (a_1)^p + (a_2)^p + \cdots + (a_k)^p$$

   Nous allons faire cette démonstration par une récurrence sur k
   - ⋆ C'est évidemment vrai pour $k = 1$
   - ⋆ Supposons que c'est vrai pour k, c'est à dire que :

     $$(a_1 + a_2 + \cdots + a_k)^p = (a_1)^p + (a_2)^p + \cdots + (a_k)^p$$

   - ⋆ Démontrons l'affirmation pour $k+1$

     $(a_1 + a_2 + \cdots + a_k + a_{k+1})^p = ((a_1 + a_2 + \cdots + a_k) + a_{k+1})^p = (a_1 + a_2 + \cdots + a_k)^p + + a_{k+1}^p$

     D'après l'hypothèse de récurrence $(a_1 + a_2 + \cdots + a_k)^p = (a_1)^p + (a_2)^p + \cdots + (a_k)^p$ et donc :

     $(a_1 + a_2 + \cdots + a_k + a_{k+1})^p = (a_1 + a_2 + \cdots + a_k)^p + a_{k+1}^p = (a_1)^p + (a_2)^p + \cdots + (a_k)^p + (a_{k+1})^p$

     Ce que nous voulions
4. *p est toujours un nombre premier et $k \in \mathbb{N}$ quelconque. Démontrer que $k^p \equiv k\,[p]$*

   Nous nous posons dans l'anneau $(\mathbb{Z}/p\mathbb{Z},+,\times)$ qui est bien entendu de caractéristique p.

   Donc, pour tout $k \in \mathbb{Z}$, $k^p = \left(\underbrace{1+1+1+\cdots+1+1}_{k \text{ fois}}\right)^p$, et, dans $(\mathbb{Z}/p\mathbb{Z},+,\times)$, d'après les questions précédentes, dans $\mathbb{Z}/p\mathbb{Z}$, nous avons

   $$\left(\underbrace{1+1+1+\cdots+1+1}_{k \text{ fois}}\right)^p = \underbrace{(1)^p + (1)^p + \cdots + (1)^p}_{k \text{ fois}} = k$$

   Ce qui veut dire que $k^p \equiv k\,[p]$

Exercice 3 :

Soit $(R,+,\times)$ un anneau unitaire. Soient $a \in R$ et $b \in R$ tels que $ab+ba=1$ et $a^2b+ba^2=a$

1. *Montrer que $a^2b=ba^2$ et que $2aba=a$*

   $\Rightarrow$ De $ab+ba=1$, nous tirons, par la multiplication à gauche par a $a(ab+ba)=a \iff a^2b+aba=a$, d'où nous déduisons, de $a^2b+ba^2=a$ que $a^2b+aba=a^2+ba^2 \iff aba=ba^2$

   $\Rightarrow$ De même, de $ab+ba=1$, nous tirons, par la multiplication à droite par a $(ab+ba)a=a \iff aba+ba^2=a$, d'où nous déduisons, de $a^2b+ba^2=a$ que $aba+ba^2=a^2+ba^2 \iff aba=a^2b$

   $\Rightarrow$ De $aba=ba^2$ et $aba=a^2b$, nous déduisons que $ba^2=a^2b$, et en additionnant, $2aba=ba^2+ab^2=a$

   Et donc $a^2b=ba^2$ et $2aba=a$

2. *Etablir que a est inversible que son inverse est $2b$, c'est à dire $a^{-1}=2b$*

   $\Rightarrow$ Nous avons $(ab)^2=abab=(aba)b$; de $aba=ba^2$, nous tirons $(ab)^2=ba^2b$

   $\Rightarrow$ De même, $(ba)^2=baba=b(aba)$; de $aba=a^2b$, nous tirons $(ba)^2=ba^2b$

   $\Rightarrow$ De $ab+ba=1$, nous tirons $ab=1-ba$, c'est à dire $(ab)^2=(1-ba)^2=1+(ba)^2-2ba$. Nous en déduisons donc que

   $$ba^2b=1+ba^2b-2ba \iff 1-2ba=0 \iff 2ba=1 \iff a^{-1}=2b$$

   Ce que nous voulions

Exercice 4 :

Soit $(R,+,\times)$ un anneau unitaire.
On suppose que, pour tout $x \in R$ et tout $y \in R$, nous avons $(xy)^2=x^2y^2$

1. *Démontrer que, pour tout $x \in R$ et tout $y \in R$, nous avons $xyx=x^2y=yx^2$*

   Soient $x \in R$ et $y \in R$. Alors :

   $\Rightarrow$

   $$\begin{aligned}[(1+y)x]^2 &= [x+yx]^2\\ &= (x+yx)(x+yx)\\ &= x^2+xyx+yx^2+(yx)^2\end{aligned}$$

   $\Rightarrow$ Maintenant :

   $$\begin{aligned}(1+y)^2x^2 &= (1+y)(1+y)x^2\\ &= \left(1+2y+y^2\right)x^2\\ &= x^2+2yx^2+y^2x^2\end{aligned}$$

   $\Rightarrow$ De l'hypothèse, nous avons $(xy)^2=x^2y^2$ vraie pour tout $x \in R$ et tout $y \in R$, nous avons ;

   $$[(1+y)x]^2=(1+y)^2x^2 \iff x^2+xyx+yx^2+(yx)^2=x^2+2yx^2+y^2x^2 \iff xyx=yx^2$$

   Ainsi, nous avons $xyx=yx^2$

   Pour démontrer que $xyx=x^2y$, nous faisons, de la même manière, le calcul de $[x(1+y)]^2$ et $x^2(1+y)^2$

2. *En déduire que l'anneau R est commutatif*

   De l'identité $xyx=x^2y=yx^2$ vraie pour tout $x \in R$ et tout $y \in R$, nous avons :

   $$(1+x)^2y=y(1+x)^2$$

   $\Rightarrow$ $(1+x)^2y=\left(1+x^2+2x\right)y=y+x^2y+2xy$

   $\Rightarrow$ $y(1+x)^2=y\left(1+2x+x^2\right)=y+2yx+yx^2$

   $\Rightarrow$ Donc, $y+2yx+x^2y=y+x^2y+2xy \iff 2yx+yx^2=2xy+x^2y$. Comme, nous avons démontré que $x^2y=yx^2$, nous obtenons $2yx=2xy \iff yx=xy$

   L'anneau R est donc commutatif.

Exercice 5 :

Soit $(R,+,\times)$ un anneau unitaire.
Soit $a \in R$ un élément de R tel qu'il existe $b \in R$ tel que $ab = 1$

1. *Démontrer que, si pour tout $x \in R$ et tout $y \in R$ nous avons $ax = ay$, alors $x = y$*

   Soient $x \in R$ et $y \in R$ tels que $ax = ay$, alors $ax - ay + 1 = 1$ et donc :

   $$ax - ay + 1 = 1 \Longleftrightarrow ax - ay + ab = 1 \Longleftrightarrow a(x - y + b) = 1$$

   De l'unicité de l'existence de $b \in R$ tel que $ab = 1$, nous déduisons de $a(x - y + b) = 1$ que $x - y + b = b$
   De la régularité dans un groupe additif, nous déduisons que $x - y = 0$ et donc que $x = y$
   a est donc un élément régulier pour la multiplication.
2. *Démontrer que a est un élément inversible de R et que $b = a^{-1}$*

   Nous avons $a(ba) = (ab) = 1 \times a = a = a \times 1$, c'est à dire $a(ba) = a \times 1$.
   De la régularité de a, nous déduisons de $a(ba) = a \times 1$ que $ba = 1$.
   Nous avons donc $ab = ba = 1$ et donc $b = a^{-1}$.
   a est donc inversible et l'inverse de a est b, et donc $b = a^{-1}$

Exercice 6 :

Soit $(R,+,\times)$ un anneau unitaire. Nous appelons $\mathcal{U} \subset R$ l'ensemble des éléments inversibles de R.
Il faut démontrer que $(\mathcal{U},\times)$ est un groupe.

1. Tout d'abord, il est clair que $\mathcal{U} \neq \emptyset$ puisque $1 \in \mathcal{U}$
2. D'autre part, la loi $\times$ est associative, par construction des anneaux.
3. Ensuite, la loi $\times$ est interne ; en effet, si $a \in \mathcal{U}$ et $b \in \mathcal{U}$, alors $ab \in \mathcal{U}$

   En effet,
   Pour démontrer que $ab \in \mathcal{U}$, il faut démontrer que ab est inversible. Or, $(ab)^{-1} = b^{-1} \times a^{-1}$ puisque :
   $\rightarrow$ $(ab)\left(b^{-1} \times a^{-1}\right) = a\left(bb^{-1}\right)a = a \times 1 \times a^{-1} = a \times a^{-1} = 1$
   $\rightarrow$ Et $\left(b^{-1} \times a^{-1}\right)(ab) = b^{-1} \times \left(a^{-1} \times a\right)b = b^{-1} \times 1 \times b = b^{-1} \times b = 1$
4. De manière évidente, si $b \in \mathcal{U}$, alors $b^{-1} \in \mathcal{U}$, puisque $b = \left(b^{-1}\right)^{-1}$; b^{-1} est donc inversible et donc $b^{-1} \in \mathcal{U}$

$(\mathcal{U},\times)$ est donc un groupe.

Exercice 7 :

Montrer qu'un anneau $(R,+,\times)$ n'a pas de diviseurs de zéro si, et seulement si, tous ses éléments non nuls sont réguliers

1. On suppose que R n'admet pas de véritables diviseurs de zéro et soient 3 éléments $a \in R$ avec $a \neq 0$, $x \in R$ et $y \in R$ tels que $ax = ay$. Alors :

   $$ax = ay \Longleftrightarrow ax - ay = 0 \Longleftrightarrow a(x - y) = 0$$

   Comme $a \neq 0$ et que R est un anneau intègre, alors $x - y = 0$, c'est à dire $x = y$
2. Réciproquement, supposons que tous les éléments non nuls de R sont réguliers.
   Soient $x \in R$ et $y \in R$ tels que $xy = 0$. Alors

   $$xy = 0 \Longleftrightarrow xy = x \times 0$$

   De l'égalité et de la régularité, puisque $xy = x \times 0$, alors $x = 0$
   De la même manière $xy = 0 \Longleftrightarrow xy = 0 \times y$, et de cette régularité on déduit $y = 0$
   Nous avons donc $xy = 0 \Longrightarrow (x = 0)$ ou $(y = 0)$
   R est donc intègre

Exercice 8 :

Soient a et b deux éléments d'un anneau $(R,+,\times)$ tels que ab soit inversible et b non diviseur de 0. Montrer que a et b sont inversibles.

Soient a et b deux éléments d'un anneau $(R,+,\times)$ tels que ab soit inversible et b non diviseur de 0.

1. Soit $x = b\left(ab\right)^{-1}$. Montrons que x est l'inverse de a
   Nous avons donc :
   $$ax = a \times b\left(ab\right)^{-1} = \left(ab\right)\left(ab\right)^{-1} = 1$$
   D'autre part :
   $$xab = b\left(ab\right)^{-1}ab = b \Longleftrightarrow xab = b \Longleftrightarrow xab - b = 0 \Longleftrightarrow b\left(xa-1\right) = 0$$
   b n'étant pas un diviseur de zéro, $xa - 1 = 0 \Longleftrightarrow xa = 1$ et x est bien l'inverse de a
2. Nous avons $b = a^{-1}\left(ab\right)$. b apparaît comme le produit d'éléments inversibles et est donc inversible. Nous avons même $b^{-1} = \left(ab\right)^{-1} \times a$

Exercice 10 :

Soit $(R,+,\times)$ un anneau et nous considérons $Z\left(R\right)$, le centre de R, c'est à dire :

$$Z\left(R\right) = \{u \in R \text{ tels que, pour tout } x \in R \text{ nous avons } ux = xu\}$$

Il faut démontrer que $\left(Z\left(R\right),+,\times\right)$ est un sous-anneau de $(R,+,\times)$

Nous allons utiliser le théorème 2.1.7 pour démontrer que $\left(Z\left(R\right),+,\times\right)$ est un sous-anneau de $(R,+,\times)$
Soient $u \in Z\left(R\right)$ et $v \in Z\left(R\right)$. Alors, pour tout $x \in R$, $ux = xu$ et $vx = xv$

1. Montrons que $u - v \in Z\left(R\right)$. Soit donc $x \in R$; alors :
   $$\left(u-v\right)x = ux - vx = xu - xv = x\left(u-v\right)$$
   Ainsi $u - v$ commute avec tout $x \in R$ et $u - v \in Z\left(R\right)$
2. Montrons que $uv \in Z\left(R\right)$. Soit donc $x \in R$; alors :
   $$\left(uv\right)x = u\left(vx\right) = u\left(xv\right) = \left(ux\right)v = \left(xu\right)v = x\left(uv\right)$$
   Ainsi le produit uv commute avec tout $x \in R$ et $uv \in Z\left(R\right)$

Donc, $\left(Z\left(R\right),+,\times\right)$ est un sous-anneau de $(R,+,\times)$

Exercice 13 :

On pose $r = \sqrt[3]{2}$ et $A = \left\{x \in \mathbb{R} \text{ où } x = m + nr + pr^2 \text{ avec } m \in \mathbb{Z}, n \in \mathbb{Z}, p \in \mathbb{Z}\right\}$.
Il faut démontrer que $(A,+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$

Quelques remarques avant de commencer :

- $r = \sqrt[3]{2}$ est racine du polynôme $X^3 - 2$ qui se factorise en $\left(X^3-2\right) = \left(X-r\right)\left(X^2+rX+r^2\right)$ qui sont des polynômes irréductibles de $\mathbb{R}\left[X\right]$
- Nous aurons aussi à utiliser le fait que $r^3 = 2$
- Nous avons $A \neq \emptyset$ puisque $0 \in A$ et $1 \in A$

Démontrons maintenant que $(A,+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$
Le fait que $A \subset \mathbb{R}$, $(A,+,\times)$ récupère de toutes les propriétés d'anneau de $(\mathbb{R},+,\times)$, en particulier la distributivité de $\times$ par rapport à $+$

$\Rightarrow$ Soit $x \in A$ et $y \in A$; nous allons montrer que $x - y \in A$.
Nous avons $x = m + nr + pr^2$ et $y = m' + n'r + p'r^2$ avec $m \in \mathbb{Z}$, $m \in \mathbb{Z}$, $n \in \mathbb{Z}$,$p \in \mathbb{Z}$,$m' \in \mathbb{Z}$, $n' \in \mathbb{Z}$ et $p' \in \mathbb{Z}$.
Alors :
$$x - y = \left(m + nr + pr^2\right) - \left(m' + n'r + p'r^2\right) = \left(m-m'\right) + \left(n-n'\right)r + \left(p-p'\right)r^2$$
Bien entendu, nous avons $\left(m-m'\right) \in \mathbb{Z}$, $\left(n-n'\right) \in \mathbb{Z}$ et $\left(p-p'\right) \in \mathbb{Z}$ et donc $x - y \in A$

$\Rightarrow$ Maintenant, montrons que pour $x \in A$ et $y \in A$, $x \times y \in A$
En reprenant l'écriture de x et de y cidessus, nous avons :

$$\begin{aligned} x \times y = & \left(m + nr + pr^2\right) \times \left(m' + n'r + p'r^2\right) \\ = & \; mm' + mn'r + mp'r^2 + nm'r + nn'r^2 + 2np' + m'pr^2 + 2n'p + 2pp'r \\ = & \left(mm' + 2np' + 2n'p\right) + \left(mn' + nm' + 2pp'\right) r + \left(mp' + nn' + m'p\right) r^2 \end{aligned}$$

Comme $(mm' + 2np' + 2n'p) \in \mathbb{Z}$, que $(mn' + nm' + 2pp') \in \mathbb{Z}$ et que $(mp' + nn' + m'p) \in \mathbb{Z}$, nous avons $x \times y \in A$
$(A, +, \times)$ est un donc sous-anneau de $(\mathbb{R}, +, \times)$

Exercice 18 :

Soit $f : \mathbb{C} \longrightarrow \mathbb{C}$ un morphisme d'anneaux tel que pour tout $x \in \mathbb{R}$, $f(x) = x$. Montrer que f est l'identité ou la conjugaison complexe.

Posons $f(i) = \lambda$. Alors :
- $\rightarrow$ Pour $z = a + ib$, nous avons $f(z) = f(a) + f(i) = a + \lambda b$
- $\rightarrow$ D'autre part, $f\left(i^2\right) = (f(i))^2 = \lambda^2$
- $\rightarrow$ Mais, $f\left(i^2\right) = f(-1) = -f(1) = -1$
- $\rightarrow$ D'où $\lambda^2 = -1$, c'est à dire $\lambda = \pm i$

Si $f(i) = i$, alors $f(z) = f(a) + f(i) = a + ib = z$ et donc $f = \mathrm{Id}_{\mathbb{C}}$
Et, très simplement, si $f(i) = -i$, alors $f(z) = f(a) + f(i) = a - ib = \overline{z}$ et donc f est la conjugaison dans $\mathbb{C}$

Exercice 20 :

On note $\mathbb{D} = \left\{ \dfrac{m}{10^n} \text{ avec } m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$ l'ensemble des nombres décimaux

1. *Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +\times)$*
2. *Montrer que les idéaux de $\mathbb{D}$ sont principaux* (c'est-à-dire de la forme $a \times \mathbb{D}$ avec $a \in \mathbb{D}$)

Que $\mathbb{D}$ soit un sous-anneau de $(\mathbb{Q}, +\times)$ est évident ; il suffit d'en vérifier les axiômes.
Soit maintenant $I \subset \mathbb{D}$ un idéal de $\mathbb{D}$.
Alors, par définition, nous avons $(I, +)$ qui est un sous-groupe additif de $(\mathbb{D}, +)$; de la même manière, comme $\mathbb{Z} \subset \mathbb{D}$, $(\mathbb{Z}, +)$ est un sous-groupe additif de $(\mathbb{D}, +)$
L'intersection de 2 sous groupes est un sous-groupe, $I \cap \mathbb{Z}$ est un sous-groupe additif de $(\mathbb{D}, +)$; mais comme $I \cap \mathbb{Z} \subset \mathbb{Z}$, $(I \cap \mathbb{Z}, +)$ est un sous-groupe additif de $(\mathbb{Z}, +)$. Les seuls sous-groupes de $(\mathbb{Z}, +)$ étant du type $a\mathbb{Z}$ avec $a \in \mathbb{N}$, il existe donc $a \in \mathbb{N}$ tel que $I \cap \mathbb{Z} = a\mathbb{Z}$
- $\rightarrow$ Comme $a\mathbb{Z} \subset I$, alors $a = a \times 1 \in I$, et donc, pour tout $x \in \mathbb{D}$, du fait que I soit un idéal, $ax \in I$ et donc $a\mathbb{D} \subset I$
- $\rightarrow$ Réciproquement, soit $x \in I$ et nous allons démontrer que $x \in a\mathbb{D}$
  Si $x \in I$, alors $x \in \mathbb{D}$ et il existe $m \in \mathbb{Z}$ et $n \in \mathbb{N}$ tels que $x = \dfrac{m}{10^n}$
  De la notion d'idéal, nous pouvons écrire que $10^n \times x \in I$, c'est à dire $10^n \times \dfrac{m}{10^n} = m \in I$, c'est à dire que $m \in I \cap \mathbb{Z} = a\mathbb{Z}$. L'entier a est donc un diviseur de m. Il existe donc $k \in \mathbb{Z}$ tel que $m = ka$
  Dès lors $x = \dfrac{m}{10^n} = \dfrac{k \times a}{10^n} = a \times dfrack10^n$, ce qui signifie que $x \in a\mathbb{D}$ et donc $I \subset a\mathbb{D}$
- $\rightarrow$ De $a\mathbb{D} \subset I$ et $I \subset a\mathbb{D}$, nous en déduisons que $I = a\mathbb{D}$

Ainsi, les idéaux de $\mathbb{D}$ sont principaux et $\mathbb{D}$ est donc un anneau principal.

Exercice 21 :

Le nilradical d'un anneau commutatif $(R, +, \times)$, est l'ensemble N formé des éléments nilpotents de R, c'est à dire des $x \in R$ tels qu'il existe $n \in \mathbb{N}$ vérifiant $x^n = 0_R$. Montrer que N est un idéal de R

- $\rightarrow$ Il faut d'abord démontrer que $(N, +)$ est un sous-groupe de $(R, +)$.
  - $\star$ Il faut d'abord montrer que $N \neq \emptyset$
    Or, pour tout $n \in \mathbb{N}$, $0_R^n = 0$ et donc $0_R \in N$

⋆ Soient, maintenant, $x \in N$ et $y \in N$; il faut montrer que $x - y \in N$.
Il existe donc $m \in \mathbb{N}$ et $n \in \mathbb{N}$ tels que $x^m = 0_R$ et $y^n = 0_R$. Calculons $(x-y)^{m+n}$ et utilisons pour cela, la formule du binôme de Newton. Nous pouvons le faire puisque $(R, +, \times)$ est commutatif.

$$\begin{aligned}(x-y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} \\ &= \sum_{k=0}^{m} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k} + \sum_{k=m+1}^{m+n} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k}\end{aligned}$$

▷ Pour $0 \leqslant k \leqslant m$, nous avons $-m \leqslant -k \leqslant 0$
Ainsi, si $n \leqslant m+n-k \leqslant m+1$, et donc, si $0 \leqslant k \leqslant m$, nous avons $y^{m+n-k} = y^n \times y^{m-k} = 0_R$, et donc

$$\sum_{k=0}^{m} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k} = 0_R$$

▷ Pour $m+1 \leqslant k \leqslant m+n$, nous avons $x^k = x^m \times x^{k-m} = 0_R$ et donc

$$\sum_{k=m+1}^{m+n} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k} = 0_R$$

En conclusion,

$$\begin{aligned}\sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} &= \sum_{k=0}^{m} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k} + \cdots \\ &\quad \cdots \sum_{k=m+1}^{m+n} \binom{m+n}{k} (-1)^{m+n-k} x^k y^{m+n-k} \\ &= 0_R\end{aligned}$$

C'est à dire $(x-y)^{m+n} = 0_R$, c'est à dire que $x - y \in N$

→ Soit $a \in A$ et $x \in N$; il faut démontrer que $ax \in N$.
Il existe donc $n \in \mathbb{N}$ tel que $x^n = 0_R$; par la commutativité dans R, on peut écrire $(ax)^n = a^n \times x^n = 0_R$, et donc $ax \in N$

Et donc N est bien un idéal.

Exercice 22 :

Soient $(R, +, \times)$ un anneau commutatif et $a \in R$ un élément idempotent de R, c'est à dire tel que $a^2 = a$.

1. *Montrer que $J = \{x \in R \text{ tel que } ax = 0\}$ est un idéal de R.*

Il faut montrer que J est un idéal.
⇒ Tout d'abord, il faut montrer que $(J, +)$ est un sous-groupe.
⋆ Bien entendu, $J \neq \emptyset$ puisque $0_R \in J$
⋆ Soit $x \in J$ et $y \in J$; il faut, maintenant montrer que $x - y \in J$. Donc :

$$a(x-y) = ax - ay = 0_R - 0_R = 0_R$$

Donc, $x - y \in J$
Et, $(J, +)$ est un sous-groupe de $(R, +)$
⇒ Soit $y \in R$ et $z \in J$; il faut, maintenant, montrer que $yz \in J$, c'est à dire que $a(yz) = 0$
Comme $z \in J$, $az = 0$, et, par commutativité de $\times$ dans R :

$$a(yz) = (ay)z = (ya)z = y(az) = y \times 0 = 0$$

Donc $yz \in J$

Et pour conclure, J est un idéal de R

2. *On note $I = aR$ l'idéal principal de R engendré par a. Déterminer $I + J$ et $I \cap J$*

   $\Rightarrow$ Premièrement, il faut remarquer que $I + J \subset R$.
   Réciproquement, soit $r \in R$; alors $r = ar + r - ar$
   Nous avons, clairement $ar \in I$.
   Montrons que $r - ar \in J$
   $a(r - ar) = ar - a^2 r \overset{\text{idempotence}}{=} ar - ar = 0_R$, et donc $r - ar \in J$. Nous avons donc :

$$r = \underbrace{ar}_{\in I} + \underbrace{r - ar}_{\in J}$$

   Et donc, $\boxed{r \in I + J}$
   Et nous concluons donc que $R = I + J$

   $\Rightarrow$ Soit $y \in I \cap J$
   Alors, $y \in I$, et il existe $r \in R$ tel que $y = ar$. Comme $y \in J$, alors $ay = 0_R$, et donc :

$$0_R = ay = a(ar) = a^2 r = ar = y$$

   Donc, $y = 0_R$ et nous concluons, en disant que $\boxed{I \cap J = \{0_R\}}$

3. *Établir que pour tout idéal K de R : $(K \cap I) + (K \cap J) = K$.*

   $\Rightarrow$ Il est évident que $(K \cap I) + (K \cap J) \subset K$

   $\Rightarrow$ Réciproquement, soit $k \in K$
   Alors, nous avons $k = ak + k - ak$, et par définition des idéaux, nous avons $ak \in I$ et $ak \in K$, c'est à dire $ak \in I \cap K$
   D'après une démonstration précédente, $k - ak \in J$ et $k - ak \in K$ puisque K est un sous-groupe ; donc $k - ak \in J \cap K$.
   Nous avons bien $k \in (K \cap I) + (K \cap J)$ et donc $K \subset (K \cap I) + (K \cap J)$, c'est à dire, finalement, $(K \cap I) + (K \cap J) = K$

Exercice 24 :

Dans $\mathcal{M}_2(\mathbb{C})$, on considère l'ensemble $\mathbb{H}$ défini par :

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \text{ où } a \in \mathbb{C} \text{ et } b \in \mathbb{C} \right\}$$

Il faut montrer que $\mathbb{H}$ muni de l'addition et de la multiplication des matrices est un corps non commutatif.

$\Rightarrow$ Nous allons commencer par montrer que $(\mathbb{H}, +)$ est un sous-groupe de $(\mathcal{M}_2(\mathbb{C}), +)$

$\star$ Tout d'abord, $\mathbb{H} \neq \emptyset$ puisque $\mathcal{O}_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{H}$

$\star$ Ensuite, soient $M_1 \in \mathbb{H}$ et $M_2 \in \mathbb{H}$ avec $M_1 = \begin{pmatrix} a_1 & -\overline{b_1} \\ b_1 & \overline{a_1} \end{pmatrix}$ et $M_2 = \begin{pmatrix} a_2 & -\overline{b_2} \\ b_2 & \overline{a_2} \end{pmatrix}$.
Alors, un calcul très simple montre que $M_1 - M_2 = \begin{pmatrix} a_1 - a_2 & -\overline{(b_1 - b_2)} \\ b_1 - b_2 & \overline{(a_1 - a_2)} \end{pmatrix}$ et donc $M_1 - M_2 \in \mathbb{H}$

$(\mathbb{H}, +)$ est un donc sous-groupe additif de $(\mathcal{M}_2(\mathbb{C}), +)$

$\Rightarrow$ Notons $\mathbb{H}^* = \mathbb{H} \setminus \{\mathcal{O}_2\}$. Il est tout à fait loisible de penser que $\mathbb{H}^*$ est l'ensemble des matrices $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ telles que $|a|^2 + |b|^2 \neq 0$
Nous allons donc montrer que $(\mathbb{H}^*, \times)$ est un groupe multiplicatif.

$\star$ Tout d'abord $\mathbb{H}^* \neq \emptyset$ puisque $\mathrm{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}^*$

$\star$ La multiplication étant associative dans $\mathcal{M}_2(\mathbb{C})$, elle l'est aussi dans $(\mathbb{H}^*, \times)$

⋆ La multiplication est une loi de composition interne. En effet, si $M_1 \in \mathbb{H}$ et $M_2 \in \mathbb{H}$ avec $M_1 = \begin{pmatrix} a_1 & -\overline{b_1} \\ b_1 & \overline{a_1} \end{pmatrix}$ et $M_2 = \begin{pmatrix} a_2 & -\overline{b_2} \\ b_2 & \overline{a_2} \end{pmatrix}$, nous avons :

$$\begin{pmatrix} a_1 & -\overline{b_1} \\ b_1 & \overline{a_1} \end{pmatrix} \times \begin{pmatrix} a_2 & -\overline{b_2} \\ b_2 & \overline{a_2} \end{pmatrix} = \begin{pmatrix} a_1a_2 - \overline{b_1}b_2 & -a_1\overline{b_2} - \overline{b_1}\overline{a_2} \\ b_1a_2 + \overline{a_1}b_2 & -b_1\overline{b_2} + \overline{a_1}\overline{a_2} \end{pmatrix} = \begin{pmatrix} a_1a_2 - \overline{b_1}b_2 & -\overline{b_1a_2 + \overline{a_1}b_2} \\ b_1a_2 + \overline{a_1}b_2 & -a_1a_2 - \overline{b_1}b_2 \end{pmatrix}$$

Ce qui montre que le produite $M_1 \times M_2 \in \mathbb{H}^*$

⋆ La multiplication admet un élément neutre Id_2

⋆ Chaque élément $M \in \mathbb{H}^*$ admet un inverse.

En effet, si $M = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ avec $|a|^2 + |b|^2 \neq 0$, alors $M^{-1} = \dfrac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & \overline{b} \\ -b & a \end{pmatrix}$ et M^{-1} est bien un élément de $\mathbb{H}^*$

$(\mathbb{H}^*, \times)$ est donc un groupe multiplicatif.

⇒ La multiplication étant distributive par rapport à l'addition dans $\mathcal{M}_2(\mathbb{C})$, elle l'est aussi dans $(\mathbb{H}^*, \times)$

Nous venons de démontrer que $\mathbb{H}$ muni de l'addition et de la multiplication des matrices est un corps. Montrons que ce corps n'est pas commutatif.

Soient $M_1 = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$

▷ Alors $M_1 \times M_2 = \begin{pmatrix} 1-2i & i-2 \\ 2+i & 2i+1 \end{pmatrix}$

▷ Et $M_2 \times M_1 = \begin{pmatrix} 1+2i & -2+i \\ i+2 & -2i+1 \end{pmatrix}$

Clairement, nous avons $M_1 \times M_2 \neq M_2 \times M_1$ et $(\mathbb{H}^*, \times)$ est donc un groupe multiplicatif non commutatif, c'est à dire que $\mathbb{H}$ n'est pas un corps commutatif

Exercice 25 :

Soit $j = \dfrac{-1}{2} + i\dfrac{\sqrt{3}}{2} = e^{\frac{2i\pi}{3}}$ une racine cubique de 1. Nous rappelons que $1 + j + j^2 = 0$ et que $j^2 = \overline{j}$.
Nous notons $\mathbb{Z}[j] = \{z \in \mathbb{C} \text{ où } z = a + jb \text{ où } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$

1. *Démontrer que $(\mathbb{Z}[j], +\times)$ est un sous anneau de $(\mathbb{C}, +, \times)$*

⇒ Il est évident que $\mathbb{Z}[j]$ est non vide puisque $0 \in \mathbb{Z}[j]$ et $1 \in \mathbb{Z}[j]$ et stable pour l'addition.

⇒ Soit $u = a + bj \in \mathbb{Z}[j]$ et $v = c + dj \in \mathbb{Z}[j]$, il est clair que $u - v = (a - c) + (b - d)j \in \mathbb{Z}[j]$. Donc $(\mathbb{Z}[j], +)$ est un sous groupe de $(\mathbb{C}, +)$

⇒ Démontrons que $\mathbb{Z}[j]$ est stable pour la multiplication.

$$\begin{aligned} uv &= (a + bj)(c + dj) \\ &= ac + adj + bcj + bdj^2 \\ &= ac + adj + bcj + bd(-1 - j) \\ &= (ac - bd) + (ad + bc - bd)j \end{aligned}$$

La multiplication est bien une loi de composition interne

Donc, $(\mathbb{Z}[j], +\times)$ est un sous anneau de $(\mathbb{C}, +, \times)$

2. (a) *Pour $z = a + jb \in \mathbb{Z}[j]$, montrer que $(a + bj)\left(a + bj^2\right)$ est un entier positif*

Si $z = a + jb$, alors $\overline{z} = a + b\overline{j} = a + bj^2$, de telle sorte que $(a + bj)\left(a + bj^2\right) = z\overline{z} = |z|^2$

Maintenant, par le calcul :

$$(a + bj)\left(a + bj^2\right) = a^2 + abj^2 + abj + b^2j^3 == a^2 + b^2 + ab\left(j + j^2\right) = a^2 + b^2 - ab$$

Nous avons, bien entendu, $a^2 + b^2 - ab \in \mathbb{Z}$, et comme $a^2 + b^2 - ab = |z|^2 \geqslant 0$, nous avons $a^2 + b^2 - ab \in \mathbb{N}$

Il aurait aussi été possible d'utiliser d'un argument plus spécieux, d'une égalité de derrière les fagots : $a^2 + b^2 - ab = \dfrac{1}{4}(a + b)^2 + \dfrac{3}{4}(a - b)^2$. Et donc, nous en déduisons que $a^2 + b^2 - ab \geqslant 0$. Bof...

(b) *Nous considérons l'application suivante* $N : \mathbb{Z}[j] \longrightarrow \mathbb{N}$ *définie par :*

$$\begin{cases} N : \mathbb{Z}[j] & \longrightarrow & \mathbb{N} \\ z = a + jb & \longmapsto & N(z) = (a+bj)\left(a+bj^2\right) \end{cases}$$

Démontrer que, pour tout $z \in \mathbb{Z}[j]$ *et tout* $z' \in \mathbb{Z}[j]$*, nous avons* $N(zz') = N(z)N(z')$

Nous utilisons la remarque mettant en évidence que $a + bj^2 = a + b\overline{j} = \overline{a+bj}$, de telle sorte que $N(z) = z\overline{z} = |z|^2$, où $|z|$ désigne le module complexe de $z \in \mathbb{C}$.
Bien entendu, en utilisant les propriétés de ces modules, nous avons $N(zz') = N(z)N(z')$

(c) *Trouver tous les éléments inversibles de* $\mathbb{Z}[j]$

Si $z \in \mathbb{Z}[j]$ est inversible, ceci veut dire qu'il existe $u \in \mathbb{Z}[j]$ tel que $zu = 1$; en fait, nous avons $u = z^{-1}$, l'inverse de $z \in \mathbb{C}$.
Dans notre cas, en nous intéressant aux normes, nous avons $N\left(zz^{-1}\right) = N(z)N\left(z^{-1}\right) = 1$, ce qui signifie que $N(z)$ et $N\left(z^{-1}\right)$ sont des diviseurs de 1 dans $\mathbb{N}$ et nous n'avons donc pas d'autres choix pour $N(z)$ et $N\left(z^{-1}\right)$ que d'avoir $N(z) = 1$ et $N\left(z^{-1}\right) = 1$.
Si $z = a + bj$, $N(z) = (a+bj)\left(a+bj^2\right) = a^2 + b^2 - ab = 1$.

C'est ici que l'égalité de derrière les fagots : $a^2 + b^2 - ab = \dfrac{1}{4}(a+b)^2 + \dfrac{3}{4}(a-b)^2$ joue son rôle. Nous devons donc avoir :

$$\frac{1}{4}(a+b)^2 + \frac{3}{4}(a-b)^2 = 1$$

C'est une équation en nombres entiers qui peut nous jouer des tours !! Ne devons donc avoir

$$\begin{cases} (a+b)^2 = 4 \\ (a-b)^2 = 0 \end{cases} \text{ ou } \begin{cases} (a+b)^2 = 1 \\ (a-b)^2 = 1 \end{cases}$$

→ Dans le premier cas

$$\begin{cases} (a+b)^2 = 4 \\ (a-b)^2 = 0 \end{cases}$$

Nous tirons $a = b$ et $(2a)^2 = 4 \Longleftrightarrow a^2 = 1 \Longleftrightarrow a = \pm 1$
D'où une première rafale d'éléments inversibles : $\varepsilon_1 = 1 + j = -j^2 = -\overline{j}$ ou $\varepsilon_2 = -1 - j = j^2 = \overline{j}$

→ Dans le second cas

$$\begin{cases} (a+b)^2 = 1 \\ (a-b)^2 = 1 \end{cases}$$

Nous tirons de ce système, beaucoup d'autres systèmes

⋆ $\begin{cases} a+b = 1 \\ a-b = 1 \end{cases}$
D'où nous tirons $a = 1$ et $b = 0$ et donc $\varepsilon_3 = 1$

⋆ $\begin{cases} a+b = -1 \\ a-b = 1 \end{cases}$
D'où nous tirons $a = 0$ et $b = -1$ et donc $\varepsilon_4 = -j$

⋆ $\begin{cases} a+b = 1 \\ a-b = -1 \end{cases}$
D'où nous tirons $a = 0$ et $b = 1$ et donc $\varepsilon_5 = j$

⋆ $\begin{cases} a+b = -1 \\ a-b = -1 \end{cases}$
D'où nous tirons $a = -1$ et $b = 0$ et donc $\varepsilon_6 = -1$

Les éléments inversibles sont donc $\left\{1, -1, j, -j, j^2, -j^2\right\}$

3. *Soient* $x \in \mathbb{Z}[j]$ *et* $y \in \mathbb{Z}[j]$*. On dit que* y *divise* x *dans* $\mathbb{Z}[j]$ *s'il existe* $z \in \mathbb{Z}[j]$ *tel que* $x = yz$.
Un nombre $x \in \mathbb{Z}[j]$ *est dit* **premier** *si ses seuls diviseurs sont des nombres de la forme* ε *ou* $\mu\varepsilon$*,* ε *étant un élément inversible de* $\mathbb{Z}[j]$ *et* $\mu \in \mathbb{Z}[j]$ *tel que* $N(x) = N(\mu)$
On dit que $x \equiv y \mod z$ *si et seulement si* $x - y$ *est divisible par* z

(a) *Donner, en utilisant la fonction N, une condition nécessaire de divisibilité*

Si y divise x dans $\mathbb{Z}[j]$ s'il existe $z \in \mathbb{Z}[j]$ tel que $x = yz$, ce qui veut dire en termes de norme N, $N(x) = N(yz) = N(y) \times N(z)$ et donc $N(y)$ divise $N(x)$.

Si $N(y)$ ne divise pas $N(x)$ alors y ne divise pas x

(b) *On note $\lambda = 1 - j$. Démontrer que λ divise 3 et que λ est premier.*

▷ Il faut d'abord remarquer que $N(3) = 9$, et que, peut-être, 3 est divisible dans $\mathbb{Z}[j]$. Or :

$$(1-j)\left(1-\bar{j}\right) = (1-j)\left(1-j^2\right) = (1-j)(2+j) = |1-j|^2 = 3$$

3 est donc divisible dans $\mathbb{Z}[j]$, puisque nous avons $3 = \lambda(2+j)$

▷ Nous venons de montrer que $N(\lambda) = 3$; 3 étant un nombre premier dans $\mathbb{N}$, et si μ divise λ dans $\mathbb{Z}[j]$, alors $N(\mu)$ divise $N(\lambda)$ et donc $N(\mu) = 3$ ou $N(\mu) = 1$
Si $N(\mu) = 3$, alors si $\lambda = \mu \times z$, nous avons $N(z) = 1$ et $z \in \mathbb{Z}[j]$ est un élément inversible.
Et donc λ est bien premier dans $\mathbb{Z}[j]$

⋆ Nous avons, par exemple $\lambda = 1 \times \lambda$ et $\lambda = -1 \times -\lambda$
⋆ Puis $\lambda = j \times (-2-j)$ et $\lambda = -j \times (2+j)$
⋆ Et pour terminer $\lambda = j^2 \times (1+2j)$ et $\lambda = -j^2 \times (-1-2j)$

(c) *Démontrer que tout élément de $z \in \mathbb{Z}[j]$ est tel que $z \equiv 0 \mod \lambda$ ou $z \equiv 1 \mod \lambda$ ou $z \equiv -1 \mod \lambda$*

Soit $z \in \mathbb{Z}[j]$ où $z = a + bj$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.
Nous pouvons écrire $z = (a+b) - b(1-j) = (a+b) - b\lambda$
Comme $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, nous avons $a+b \equiv 0\,[3] \iff a+b = 3k$ ou $a+b \equiv 1\,[3] \iff a+b = 1+3k$ ou $a+b \equiv -1\,[3] \iff a+b = -1+3k$. De plus, $3 = \lambda(1+2j)$.
Ainsi :

⋆ Si $a+b \equiv 0\,[3] \iff a+b = 3k$, alors :

$$z = (a+b) - b(1-j) = (a+b) - b\lambda = 3k - b\lambda = \lambda k(1+2j) - b\lambda = \lambda(k(1+2j) - b)$$

Ce qui veut dire que z est divisible par λ et donc, nous avons $z \equiv 0 \mod \lambda$

⋆ Ensuite, si $a+b \equiv 1\,[3] \iff a+b = 3k+1$, alors :

$$z = (a+b) - b(1-j) = (a+b) - b\lambda = 3k+1-b\lambda = 1+\lambda k(1+2j) - b\lambda = 1+\lambda(k(1+2j) - b)$$

Ce qui veut dire que $z - 1$ est divisible par λ et donc, nous avons $z \equiv 1 \mod \lambda$

⋆ Pour terminer, si $a+b \equiv -1\,[3] \iff a+b = 3k-1$, alors :

$$z = (a+b) - b(1-j) = (a+b) - b\lambda = 3k-1-b\lambda = -1+\lambda k(1+2j) - b\lambda = -1+\lambda(k(1+2j) - b)$$

Ce qui veut dire que $z - (-1)$ est divisible par λ et donc, nous avons $z \equiv -1 \mod \lambda$

En conclusion, tout élément de $z \in \mathbb{Z}[j]$ est tel que $z \equiv 0 \mod \lambda$ ou $z \equiv 1 \mod \lambda$ ou $z \equiv -1 \mod \lambda$

(d) *Démontrer que 0, 1 et -1 sont distincts modulo λ*

La question est donc :

▷ Avons nous $1 \equiv 0 \mod \lambda$?

Il faut donc voir si $1 - 0 = 1$ est divisible par λ
Si λ divise 1, alors $N(\lambda)$ divise $N(1)$; comme $N(\lambda) = 3$ et $N(1) = 1$, et que 3 ne divise pas 1, 1 n'est pas congru à 0 modulo λ

▷ Par le même raisonnement, 1 n'est pas congru à -1 modulo λ puisque $1 - (-1) = 2$ et que $N(2) = 4$

▷ De la même manière, -1 n'est pas congru à 0 modulo λ

(e) *On suppose que $x \in \mathbb{Z}[j]$ est un élément non divisible par λ. Démontrer que $x^3 \equiv 1 \mod \lambda^4$ ou $x^3 \equiv -1 \mod \lambda^4$*

On vient de voir que tout $z \in \mathbb{Z}[j]$ est tel que $z \equiv 0 \mod \lambda$ ou $z \equiv 1 \mod \lambda$ ou $z \equiv -1 \mod \lambda$. Donc, si $x \in \mathbb{Z}[j]$ est un élément non divisible par λ, alors $x \equiv 1 \mod \lambda$ ou $x \equiv -1 \mod \lambda$. Nous avons donc $x = \pm 1 + \mu\lambda$ où $\mu \in \mathbb{Z}[j]$

Supposons $x = 1 + \mu\lambda$ où $\mu \in \mathbb{Z}[j]$.

Alors,

- $x - 1 = \mu\lambda$
- $x - j = x - 1 + 1 - j = \mu\lambda + \lambda = \lambda(\mu + 1)$
- $x - j^2 = x - 1 + 1 - j^2 = \mu\lambda + (1 + j)(1 - j) = \mu\lambda + (1 + j)\lambda = \lambda(\mu + 1 + j)$

Nous devons, maintenant, nous intéresser à $x^3 - 1$. Or :

$$\begin{aligned} x^3 - 1 &= (x-1)\left(x^2 + x + 1\right) \\ &= (x-1)(x-j)\left(x-j^2\right) \\ &= \mu\lambda \times \lambda(\mu+1) \times \lambda(\mu+1+j) \\ &= \lambda^3[\mu(\mu+1)(\mu+1+j)] \end{aligned}$$

Nous avons $\mu + 1 + j = \mu + 2 - 1 + j = \mu + 2 - \lambda$ de telle sorte que :

$$\begin{aligned} x^3 - 1 &= \lambda^3[\mu(\mu+1)(\mu+2-\lambda)] \\ &= \lambda^3[\mu(\mu+1)(\mu+2) - \lambda\mu(\mu+1)] \\ &= \lambda^3\mu(\mu+1)(\mu+2) - \lambda^4\mu(\mu+1) \end{aligned}$$

Nous avons démontré, dans une question précédente que tout élément de $\mu \in \mathbb{Z}[j]$ est tel que $\mu \equiv 0 \mod \lambda$ ou $\mu \equiv 1 \mod \lambda$ ou $\mu \equiv -1 \mod \lambda$

$\rightarrow$ Si $\mu \equiv 0 \mod \lambda$, alors $\mu = \lambda k$ où $k \in \mathbb{Z}[j]$; et donc

$$\mu(\mu+1)(\mu+2) = \lambda k(\lambda k+1)(\lambda k+2) = \lambda(k(\lambda k+1)(\lambda k+2)) = \alpha_1\lambda$$

$\rightarrow$ Si $\mu \equiv 1 \mod \lambda$, alors $\mu = \lambda k + 1$ où $k \in \mathbb{Z}[j]$; et donc

$$\mu(\mu+1)(\mu+2) = (\lambda k+1)(\lambda k+2)(\lambda k+3)$$

Or, nous avons vu que $3 = \lambda(2 + j)$, et donc

$$\begin{aligned} \mu(\mu+1)(\mu+2) &= (\lambda k+1)(\lambda k+2)(\lambda k+3) \\ &= (\lambda k+1)(\lambda k+2)(\lambda k+\lambda(2+j)) \\ &= \lambda[(\lambda k+1)(\lambda k+2)(k+(2+j))] \\ &= \alpha_2\lambda \end{aligned}$$

$\rightarrow$ La résolution est semblable si $\mu \equiv -1 \mod \lambda \iff \mu = -1 + \lambda k$ où $k \in \mathbb{Z}[j]$

Ainsi, pour tout $\mu \in \mathbb{Z}[j]$, nous avons $(\mu + 1)(\mu + 2) = \alpha\lambda$, de telle sorte que :

$$x^3 - 1 = \lambda^4\alpha - \lambda^4\mu(\mu+1) = \lambda^4(\alpha - \mu(\mu+1))$$

Ainsi, $x^3 - 1$ est divisible par λ^4 et donc $x^3 \equiv 1 \mod \lambda^4$

La démonstration est semblable si $x = -1 + \mu\lambda$ où $\mu \in \mathbb{Z}[j]$ pour prouver qu'alors $x^3 \equiv -1 \mod \lambda$.

Note : Dans le travail ci-dessus, je n'ai volontairement pas voulu appliquer à $\mathbb{Z}[j]$ la théorie des congruences que nous avons vues pour $\mathbb{Z}$; en effet, nous n'avons pas travaillé, pas établi, la relation d'équivalence compatible avec l'addition et la multiplication. J'ai donc voulu rester le plus proche possible de la définition.

Exercice 26 :

Nous appelons $\Sigma = \left\{n \in \mathbb{N} \text{ tels que il existe } a \in \mathbb{N} \text{ et } b \in \mathbb{N} \text{ tels que } n = a^2 + b^2\right\}$

1. *Montrer que si $n \equiv 3 \mod 4$, alors $n \notin \Sigma$.*

   Ce n'est pas une question très difficile.

   Remarquons que si a est pair, alors $a = 2k$ et $a^2 = 4k^2$ et donc $a^2 \equiv 0 \mod 4$ et si a est impair (et donc $a = 2k + 1$) alors $a^2 = 4\left(k^2 + k\right) + 1$, ce qui veut dire $a^2 \equiv 1 \mod 4$. Ainsi :

⋆ Si a et b sont pairs, alors $a^2+b^2 \equiv 0 \mod 4$
⋆ Si a et b sont impairs, alors $a^2+b^2 \equiv 2 \mod 4$
⋆ Si a est pair et b impair, ou a est impair et b pair alors $a^2+b^2 \equiv 1 \mod 4$

Ainsi, jamais a^2+b^2 n'est congru à 3 modulo 4 et donc, si $n \equiv 3 \mod 4$, alors il n'existe pas d'entiers a et b tels que $n = a^2+b^2$ et donc $n \notin \Sigma$

2. *Nous notons* $\mathbb{Z}[i] = \left\{x = a+bi \text{ où } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z} \text{ et } i^2 = -1\right\}$

   (a) *Démontrer que* $\mathbb{Z}[i]$ *est un sous-anneau intègre de* $(\mathbb{C}, +, \times)$

   La démonstration ne pose pas de grandes difficultés *(en fait, aucune)* puisque $\mathbb{Z}[i]$ hérite des propriétés de corps de $(\mathbb{C}, +, \times)$; d'autre part, il n'est pas anodin de remarquer que $\mathbb{Z}[i] \neq \emptyset$ puisque $\mathbb{Z} \subset \mathbb{Z}[i]$
   → Il est clair que $\mathbb{Z}[i]$ est intègre puisque $(\mathbb{C}, +, \times)$ l'est.
   → La multiplication est distributive par rapport à l'addition *(puisqu'elle l'est dans* $\mathbb{C}$*)*
   → Il est clair que si $z \in \mathbb{Z}[i]$ et $z_1 \in \mathbb{Z}[i]$ alors $z - z_1 \in \mathbb{Z}[i]$
   → Il est plus délicat *(quoique... !)* de montrer que si $z \in \mathbb{Z}[i]$ et $z_1 \in \mathbb{Z}[i]$ alors $z \times z_1 \in \mathbb{Z}[i]$.
   Soient donc $z = a+ib$ et $z_1 = a_1+ib_1$; alors $zz_1 = (a+ib)(a_1+ib_1) = (aa_1 - bb_1) + i(ab_1+ba_1)$.
   Comme $aa_1 - bb_1 \in \mathbb{Z}$ et $ab_1+ba_1 \in \mathbb{Z}$, nous avons $z \times z_1 \in \mathbb{Z}[i]$
   Ainsi, $\mathbb{Z}[i]$ est un sous-anneau intègre de $(\mathbb{C}, +, \times)$

   (b) *Pour* $z \in \mathbb{Z}[i]$*, nous définissons* $N(z) = z \times \bar{z} = |z|^2$.
   Démontrer que, pour tout $z \in \mathbb{Z}[i]$ *et tout* $z_1 \in \mathbb{Z}[i]$*, nous avons* $N(z) \in \mathbb{N}$ *et*

$$N(zz_1) = N(z) \times N(z_1)$$

   → De $z = a+ib$ où $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, nous avons $N(z) = z \times \bar{z} = |z|^2 = a^2+b^2$; comme $a^2+b^2 \in \mathbb{N}$, nous avons bien $N(z) \in \mathbb{N}$
   → La propriété $N(zz_1) = N(z) \times N(z_1)$ se déduit de celle des modules des nombres complexes

   (c) *Quels sont les éléments inversibles de* $\mathbb{Z}[i]$ *?*

   Soit $u \in \mathbb{Z}[i]$; il existe donc $v \in \mathbb{Z}[i]$ tel que $uv = 1$.
   Nous avons alors $N(uv) = N(u)N(v) = N(1) = 1$; de $N(u)N(v) = 1$, nous déduisons $N(u) \neq 0$ et $N(v) \neq 0$ et ce qui veut dire que $N(v) = \dfrac{1}{N(u)}$.
   Comme nous avons démontré que $N(v) \in \mathbb{N}$, nous ne pouvons avoir que $N(u) = 1$.
   Si $u = a+ib$, nous avons $N(u) = a^2+b^2 = 1$; les seules solutions sont les couples $(a,b) = (1,0)$, $(a,b) = (-1,0)$, $(a,b) = (0,1)$ et $(a,b) = (0,-1)$. D'où les éléments inversibles sont :

$$u = 1 \quad u = -1 \quad u = i \quad u = -i$$

   Réciproquement, il est clair que $u = 1$,$u = -1$, $u = i$ et $u = -i$ sont des éléments inversibles.

3. *Démontrer que* Σ *est stable par multiplication.*

   Soit $n \in \Sigma$; il existe donc $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $n = a^2+b^2$, c'est à dire qu'il existe $u = a+bi \in \mathbb{Z}[i]$ tel que $n = N(u)$.
   De même, si $m \in \Sigma$, il existe $v = c+di \in \mathbb{Z}[i]$ tel que $m = N(v)$, et donc :

$$mn = N(v) \times N(u) = N(vu)$$

   Ce qui montre déjà que mn est la somme de 2 carrés, mais allons plus loin :
   ⋆ $uv = (a+ib)(c+id) = (ac-bd) + i(ad+bc)$ et donc $mn = N(vu) = (ac-bd)^2 + (ad+bc)^2$
   ⋆ Nous avons $N(v) = c^2+d^2$ et $N(u) = a^2+b^2$ et nous venons de montrer la célèbre identité de Lagrange

$$\left(a^2+b^2\right)\left(c^2+d^2\right) = (ac-bd)^2 + (ad+bc)^2$$

4. *On dit qu'un élément* $x \in \mathbb{Z}[i]$ *est irréductible si* $x = \alpha \times \beta$ *alors* α *ou* β *est inversible.*

(a) *Montrer que pour tout $x \in \mathbb{Z}[i]$, si $N(x)$ est un entier premier, alors x est irréductible. La réciproque est-elle vraie ?*

Soit $x = \alpha\beta$ où $\alpha \in \mathbb{Z}[i]$, $\beta \in \mathbb{Z}[i]$ et $p = N(x)$ est un nombre entier premier
Nous avons $p = N(\alpha) N(\beta)$. Les nombres $N(\alpha)$ et $N(\beta)$ divisent p. L'un des deux nombres $N(\alpha)$ ou $N(\beta)$ est égal à p, et l'autre est égal à 1, car p est premier.
Or $u \in \mathbb{Z}[i]$ est inversible si et seulement si $N(u) = 1$. Donc α ou β est inversible. x est donc irréductible.
La réciproque est fausse : par exemple, 5 est irréductible, mais $N(5) = 25$ n'est pas premier.

(b) *Soit $p \in \mathbb{N}$ un nombre premier. Démontrer que nous avons l'équivalence suivante*

$$p \in \Sigma \Longleftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$

$\Rightarrow$ Soit p un nombre premier tel que $p \in \Sigma$
Alors, il existe $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$ tels que $p = a^2 + b^2 = (a+ib)(a-ib) = N(a+ib)$.
Comme $a \in \mathbb{N}^*$ et $b \in \mathbb{N}^*$, les éléments $a+ib$ et $a-ib$ ne sont pas inversibles et donc p n'est pas irréductible dans $\mathbb{Z}[i]$

$\Rightarrow$ Supposons que p ne soit pas irréductible dans $\mathbb{Z}[i]$
Il existe donc $\alpha \in \mathbb{Z}[i]$ et $\beta \in \mathbb{Z}[i]$ non inversibles tels que $p = \alpha\beta$.
Alors $N(p) = p^2 = N(\alpha\beta) = N(\alpha) N(\beta)$.
Remarquons que, comme $\alpha \in \mathbb{Z}[i]$ et $\beta \in \mathbb{Z}[i]$ ne sont pas inversibles, alors $N(\alpha) \neq 1$ et $N(\beta) \neq 1$.
$N(\alpha)$ et $N(\beta)$ étant des diviseurs de p^2, et p étant premier, nous avons $N(\alpha) = N(\beta) = p$ et donc $p = (\mathrm{Re}(\alpha))^2 + (\mathrm{Im}(\alpha))^2 = (\mathrm{Re}(\beta))^2 + (\mathrm{Im}(\beta))^2$ est donc la somme de 2 carrés, d'où $p \in \Sigma$

(c) *En déduire que si p est premier tel que $p \equiv 3 \mod 4$ alors p est iréductible*

Si $p \equiv 3 \mod 4$ alors $p \notin \Sigma$ et donc p est irréductible

5. (a) *Soient $x \in \mathbb{Z}[i]$ et $y \in \mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$.*
On pose $\dfrac{x}{y} = u + iv$ où $u \in \mathbb{Q}$ et $v \in \mathbb{Q}$. On prend $u_0 \in \mathbb{Z}$ et $v_0 \in \mathbb{Z}$ tels que $|u - u_0| \leqslant \dfrac{1}{2}$ et $|v - v_0| \leqslant \dfrac{1}{2}$.
Montrer qu'on a : $x = y(u_0 + iv_0) + r$ avec $N(r) < N(y)$.

En écrivant $\dfrac{x}{y} = u + iv$ où $u \in \mathbb{Q}$ et $v \in \mathbb{Q}$, on choisit $u_0 \in \mathbb{Z}$ et $v_0 \in \mathbb{Z}$ tels que $|u - u_0| \leqslant \dfrac{1}{2}$ et $|v - v_0| \leqslant \dfrac{1}{2}$; ces entiers $u_0 \in \mathbb{Z}$ et $v_0 \in \mathbb{Z}$ existent ; ce sont, en fait, les entiers les plus proches de u_0 et v_0.
De $x = y(u_0 + iv_0) + r$, nous tirons

$$\frac{x}{y} = (u_0 + iv_0) + \frac{r}{y} \Longleftrightarrow \frac{r}{y} = \frac{x}{y} - (u_0 + iv_0) = (u - u_0) + i(v - v_0)$$

En utilisant les normes, nous avons $N\left(\dfrac{r}{y}\right) = \dfrac{N(x)}{N(y)} = (u - u_0)^2 + (v - v_0)^2$.
Comme $|u - u_0| \leqslant \dfrac{1}{2}$ et $|v - v_0| \leqslant \dfrac{1}{2}$, nous avons

$$\frac{N(x)}{N(y)} = (u - u_0)^2 + (v - v_0)^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$$

Et donc $N(x) < N(y)$
Nous avons $x = y(u_0 + iv_0) + r$ avec $N(r) < N(y)$

(b) *Trouver $q \in \mathbb{Z}[i]$ et $r \in \mathbb{Z}[i]$ tels que $(7 + 2i) = q(2 + 3i) + r$ avec $N(r) < N(2 + 3i)$*

Il suffit d'appliquer la démonstration précédente ; on pose, simplement $x = 7 + 2i$ et $y = 2 + 3i$

- ⋆ Dans un premier temps $\dfrac{x}{y}=\dfrac{7+2i}{2+3i}=\dfrac{(7+2i)(2-3i)}{(2+3i)(2-3i)}=\dfrac{20-17i}{13}=\dfrac{20}{13}-\dfrac{7i}{13}$
- ⋆ L'entier $u_0\in\mathbb{Z}$ le plus proche de $\dfrac{20}{13}$ est 2 et l'entier $v_0\in\mathbb{Z}$ le plus proche de $-\dfrac{7}{13}$ est -1 de telle sorte que $q=u_0+iv_0=2-i$
- ⋆ Et maintenant, $r=7+2i-(2+3i)(2-i)=-2i$, de telle sorte que nous avons

$$(7+2i)=q(2+3i)+r\Longleftrightarrow(7+2i)=(2-i)(2+3i)-2i$$

- ⋆ Il faut, maintenant, montrer que $N(r)<N(2+3i)$. Or $N(r)=N(-2i)=4$ et $N(2-i)=13$.
  Nous avons bien $N(r)<N(2-i)$

6. *Démontrer que l'anneau $\mathbb{Z}[i]$ est principal*

L'anneau $\mathbb{Z}[i]$ est principal si et seulement si tous les idéaux de $\mathbb{Z}[i]$ sont principaux, c'est à dire que les idéaux sont des ensembles de multiples de la forme $u\times\mathbb{Z}[i]$ où $u\in\mathbb{Z}[i]$.
Soit donc $\mathcal{I}$ un idéal de $\mathbb{Z}[i]$ et $n=\min\limits_{x\in\mathcal{I}\setminus\{0\}}N(x)$. Soit $a\in\mathcal{I}$ tel que $n=N(a)$.

Soit $x\in\mathcal{I}$ un élément quelconque de l'idéal $\mathcal{I}$ et effectuons la « division euclidienne » dans $\mathbb{Z}[i]$ de x par a.

Il existe donc un nombre $u_0+iv_0\in\mathbb{Z}[i]$ et $r\in\mathbb{Z}[i]$ tels que $x=a(u_0+iv_0)+r$ avec $N(r)<N(a)$.
De là, nous avons $a(u_0+iv_0)\in\mathcal{I}$ puisque $\mathcal{I}$ est un idéal. Comme par hypothèse, $x\in\mathcal{I}$ et, d'après les propriétés de sous-groupe de $\mathcal{I}$, nous avons $r=x-a(u_0+iv_0)\in\mathcal{I}$.
De $N(r)<N(a)$ et $r\in\mathcal{I}$, nous tirons $N(r)=0$ et donc $r=0$, ce qui montre que $x=a(u_0+iv_0)$, que tout élément $x\in\mathcal{I}$ est un multiple de a et que donc l'idéal $\mathcal{I}$ est principal.
Ainsi, l'anneau $\mathbb{Z}[i]$ est principal