Mathématiques spéciales

Corrigé de la feuille d'exercices n°6

1. Exercices importants

Exercice 1.

1. Soit $n, m \in \mathbb{Z}$. Montrer que $m|n$ (m divise n) si, et seulement si $n\mathbb{Z} \subset m\mathbb{Z}$.
2. a) Décrire les ensembles $3\mathbb{Z} \cap 4\mathbb{Z}$, $6\mathbb{Z} \cap 9\mathbb{Z}$, $4\mathbb{Z} \cap 8\mathbb{Z}$;
   b) Plus généralement, caractériser le sous-groupe $n\mathbb{Z} \cap m\mathbb{Z}$ pour $n, m \in \mathbb{N}$.
3. Soit $n, m \in \mathbb{Z}$.
   a) Montrer que
   $$n\mathbb{Z} + m\mathbb{Z} = \{nu + mv \mid u, v \in \mathbb{Z}\}$$
   est un sous-groupe de $\mathbb{Z}$;
   b) Caractériser ce sous-groupe.

Correction.

1. Soit $n, m \in \mathbb{Z}$.

   - ($\Rightarrow$). On suppose $m|n$. Alors il existe $p \in \mathbb{Z}$ tel que $n = mp$.
     Soit $k \in n\mathbb{Z}$. Alors il existe $q \in \mathbb{Z}$ tel que $k = nq$. Par suite,
     $$k = nq = (mp)q = m(pq) \in m\mathbb{Z},$$
     donc $n\mathbb{Z} \subset m\mathbb{Z}$.
   - ($\Leftarrow$). On suppose $n\mathbb{Z} \subset m\mathbb{Z}$. Alors, comme $n = n.1 \in n\mathbb{Z}$, n appartient à $m\mathbb{Z}$. Donc il existe $p \in \mathbb{Z}$ tel que $n = mp$ i.e. $m|n$.

2. a) On a :
   — $3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$
   — $6\mathbb{Z} \cap 9\mathbb{Z} = 18\mathbb{Z}$
   — $4\mathbb{Z} \cap 8\mathbb{Z} = 8\mathbb{Z}$

   b) Soit $n, m \in \mathbb{Z}$. Alors $n\mathbb{Z} \cap m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ comme intersection de sous-groupes de $\mathbb{Z}$. Ainsi, il existe $M \in \mathbb{Z}$ tel que $n\mathbb{Z} \cap m\mathbb{Z} = M\mathbb{Z}$.
   Montrons que $M = \text{ppcm}(n, m)$. Soit k un multiple commun de n et m. Alors $n|k$ et $m|k$ donc $k \in n\mathbb{Z} \cap m\mathbb{Z} = M\mathbb{Z}$. Par suite $M|k$. Il en résulte que $M = \text{ppcm}(n, m)$.
   Remarque : on a utilisé le résultat suivant (démontré en sup) : Soit $n, n \in \mathbb{Z}$ et $M \in \mathbb{N}$. Alors $M = \text{ppcm}(n, m)$ si, et seulement si, pour tout multiple commun k de n et m, $M|k$.

3. Soit $n, m \in \mathbb{Z}$.

a) On considère
$$n\mathbb{Z} + m\mathbb{Z} = \{nu + mv \mid u, v \in \mathbb{Z}\}.$$

i) On a $0 = n.0 + m.0 \in n\mathbb{Z} + m\mathbb{Z}$

ii) Soit $x, y \in n\mathbb{Z} + m\mathbb{Z}$. Alors il existe $u, v, p, q \in \mathbb{Z}$ tels que $x = nu + mv$ et $y = np + mq$. Montrons que $x + (-y) \in n\mathbb{Z} + m\mathbb{Z}$. On a :
$$x - y = nu + mv - (np + mq) = n(p - u) + m(v - q) \in n\mathbb{Z} + m\mathbb{Z}.$$
Donc $n\mathbb{Z} + m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

b) Comme $n\mathbb{Z} + m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, alors il est de la forme $d\mathbb{Z}$ avec $d \in \mathbb{N}$. Montrons que $d = \text{pgcd}(n, m)$.
D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $nu + mv = \text{pgcd}(n, m)$, donc $\text{pgcd}(n, m) \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Par suite, $d|\text{pgcd}(n, m)$. De plus $n = n.1 + m.0$ et $m = n.0 + m.1$, donc $n, m \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, donc $d|n$ et $d|m$. Ainsi, d est un diviseur commun positif de n, m qui est inférieur ou égal à pgcd(n,m) (car d positif et $d|\text{pgcd}(n, m)$) donc $d = \text{pgcd}(n, m)$.

Exercice 2. *Théorème de Lagrange*

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G.

1. Montrer que pour tout $a \in G$, H et $aH = \{ah;\ h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \varnothing$.
3. En déduire que le cardinal de H divise le cardinal de G.

Correction.

1. Soit $f : H \to aH$ définie par $f(h) = ah$. Il s'agit clairement d'une surjection de H sur aH. De plus, si $ah_1 = ah_2$, alors $h_1 = h_2$ car a est inversible, et donc f est aussi injective. f est donc une bijection de H sur aH ; ces deux ensembles ont le même nombre d'éléments.
2. Supposons que $aH \cap bH \neq \varnothing$ et prouvons que $aH = bH$. Par symétrie, il suffit de prouver que $aH \subset bH$. Soit $x \in aH \cap bH$, $x = ah_1 = bh_2$. Prenons $y = ah \in aH$. Alors $a = bh_2h_1^{-1}$ et donc $y = bh_2h_1^{-1}h \in bH$.
3. La réunion des ensembles aH est clairement égale à G (si $x \in G$, il est dans xH). On ne garde que les aH deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de G avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de H. Si k est le nombre d'ensembles nécessaires pour réaliser cette partition, on a
$$k\text{card}(H) = \text{card}(G)$$
et donc le cardinal de H divise celui de G.

2. Exercices basiques

a. Ordre d'un élément dans un groupe

Exercice 3.

Quel est l'ordre de $\bar{9}$ dans $\mathbb{Z}/12\mathbb{Z}$?

Correction.

On a (tenant compte du fait que la loi est notée additivement) :

$$2 \times \bar{9} = \bar{6},\ 3 \times \bar{9} = \bar{3},\ 4 \times \bar{9} = 0.$$

$\bar{9}$ est donc d'ordre 4.

Exercice 4.

Soit G un groupe et $x \in G$ d'ordre n. Quel est l'ordre de x^2 ?

Correction.

D'abord, on remarque que x^2 est d'ordre fini, car $(x^2)^n = (x^n)^2 = e^2 = e$. De plus, son ordre que nous allons noter d divise n. Distinguons alors deux cas :

- Si n est pair et s'écrit $2p$, alors $(x^2)^p = x^n = e$, et donc l'ordre de x^2 divise p. De plus, si l'ordre de x^2 est inférieur strict à p, on a $x^{2d} = e$ avec $1 \leq 2d < n$, ce qui contredit la définition de l'ordre de x. Donc, si n est pair, l'ordre de x est $n/2$.
- Si n est impair, alors on a $x^{2d} = e$ et donc $n|2d$. Mais comme n est premier avec 2, on a $n|d$. Puisqu'on avait déjà remarqué que $d|n$, on en déduit que $d = n$. En résumé, si n est impair, l'ordre de x^2 est n.

Exercice 5.

Soit G un groupe dont tous les éléments (sauf l'élément neutre) sont d'ordre au plus deux. Démontrer que G est abélien.

Correction.

Pour tous $x, y \in G$, on a $x^2y^2 = e = xyxy$ soit en simplifiant à gauche par x et à droite par y, $xy = yx$.

b. Idéaux

Exercice 6.

Soit $(A, +, \times)$ un anneau commutatif et M une partie de A. On appelle annulateur de M l'ensemble des $x \in A$ tels que $xy = 0$ pour tout $y \in M$. Démontrer que l'annulateur de M est un idéal de $(A, +, \times)$.

Correction.

Notons I cet ensemble. Il suffit d'appliquer la définition. En effet, prenons $u, v \in I$ et $a \in A$. Alors, pour tout $y \in M$, on a

$$(u - v)y = uy - vy = 0$$

et

$$(au)y = a(uy) = 0.$$

Ainsi, $u - v$ et au sont dans I qui est un idéal.

Exercice 7.

On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble de ses éléments nilpotents, c'est-à-dire l'ensemble des $x \in A$ pour lesquels il existe $n \geq 1$ de sorte que $x^n = 0$. Démontrer que le nilradical de A est un idéal de A.

Correction.

Notons $N(A)$ le nilradical de A. D'abord $0 \in N(A)$ qui est donc non vide. Prenons ensuite $a \in A$, $x, y \in N(A)$, et m, n de sorte que $x^m = y^n = 0$. Remarquons d'abord que

$$(ax)^m = a^m x^m = 0$$

et donc $ax \in N(A)$. De plus, par la formule du binôme de Newton, on a

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

Or, si $k \geq m$, alors $x^k = 0$ et si $k < m$, c'est-à-dire $k \leq m - 1$, alors $n + m - 1 - k \geq n$ et $y^{n+m-1-k} = 0$. On a bien $(x + y)^{n+m-1} = 0$ et $x + y \in N(A)$. Il est très facile de vérifier que l'on a aussi $-x \in N(A)$. Finalement, on a bien prouvé que $N(A)$ est un idéal de A.

Exercice 8.

Soit A un anneau commutatif.

1. On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrer que A est un corps.
2. On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

Correction.

1. Soit $x \in A \backslash \{0\}$. Alors l'idéal engendré par x ne peut pas être l'idéal $\{0\}$, donc c'est A tout entier. En particulier, il existe $y \in A$ tel que $yx = xy = 1_A$. C'est bien que A est un corps.
2. Prenons toujours $x \in A \backslash \{0\}$ et considérons les idéaux $I_n = x^n A$. Alors puisque A admet un nombre fini d'idéaux, il existe $n < p$ tel que $x^n A = x^p A$. En particulier, il existe $a \in A$ tel que $x^n = x^p a$. Ceci entraîne $x^n(1 - x^{p-n}a) = 0$. L'anneau étant intègre (et x étant non

nul), ceci entraine que $x^{p-n}a = 1$. x est alors inversible, d'inverse $x^{p-n-1}a$.

Exercice 9.

Soit (I_n) une suite croissante d'idéaux de $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps. Démontrer que la suite (I_n) est stationnaire.

Correction.

Méthode 1 : Il existe un unique polynôme unitaire P_n tel que $I_n = (P_n)$. De plus, la condition $I_n \subset I_{n+1}$ entraîne que $P_{n+1}|P_n$. La suite $(\deg(P_n))$ est donc une suite d'entiers naturels décroissante : elle est stationnaire. Soit $p \in \mathbb{N}$ tel que, pour tout $p \geq n$, on a $\deg(P_n) = \deg(P_p)$. On a alors $P_n|P_p$, P_n et P_p sont unitaires et de même degré, donc ils sont égaux et $I_n = I_p$. La suite (I_n) est bien stationnaire. Méthode 2 : Posons $I = \bigcup_n I_n$. Puisque la suite (I_n) est croissante, il est facile de vérifier que I est un idéal. Il existe $P \in \mathbb{K}[X]$ tel que $I = (P)$. Mais alors, il existe $N \in \mathbb{N}$ tel que $P \in I_N$. On prouve alors que pour tout $n \geq N$, on a $I_n = (P)$. En effet, on a $I_n \subset I = (P)$, et $P \in I_N \subset I_n \implies (P) \subset I_n$.

Exercice 10.

Soit $(\mathbb{D}, +, \times)$ l'anneau des nombres décimaux, c'est-à-dire l'ensemble des nombres de la forme $\frac{n}{10^k}$, avec $n \in \mathbb{Z}$ et $k \in \mathbb{N}$. Démontrer que cet anneau est principal.

Correction.

Soit I un idéal de $\mathbb{D}$. Alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$, qui est un anneau principal. Il existe donc $a \in \mathbb{Z}$ tel que $I \cap \mathbb{Z} = a\mathbb{Z}$. On va prouver que $I = a\mathbb{D}$. Il est d'abord clair que $a\mathbb{D} \subset I$ puisque $a \in I$ et que I est un idéal. Réciproquement, soit $x = \frac{n}{10^k} \in I$. Alors $n = 10^k x \in I \cap \mathbb{Z}$ et donc $n = am$ pour un certain $m \in \mathbb{Z}$. Ainsi, $x = \frac{m}{10^k} a \in a\mathbb{D}$. Les idéaux de $\mathbb{D}$ sont donc les parties de $\mathbb{D}$ du type $a\mathbb{D}$, avec $a \in \mathbb{Z}$.

Exercice 11.

On souhaite étudier dans cet exercice les idéaux de $\mathbb{Z}^2$.

1. Soit I un idéal de $\mathbb{Z}^2$ et $I_1 = \{x \in \mathbb{Z};\ (x, 0) \in I\}$, $I_2 = \{y \in \mathbb{Z};\ (0, y) \in I\}$. Démontrer que I_1 et I_2 sont deux idéaux de $\mathbb{Z}$.
2. Démontrer que $I = I_1 \times I_2$.
3. Conclure.

Correction.

1. I_1 est non-vide car $(0, 0) \in I$. Soient $x, y \in I$ et $k \in \mathbb{Z}$. Alors $(x - y, 0) = (x, 0) - (y, 0) \in I$ et $(kx, 0) = (k, 2025) \times (x, 0) \in I$ d'où $x - y$ et $kx \in I_1$. I_1 est un idéal de $\mathbb{Z}^2$ et la preuve

est similaire pour I_2.

2. Soit $(x,y) \in I_1 \times I_2$. Alors $(x,0) \in I$, $(0,y) \in I$ d'où $(x,y) = (x,0) + (0,y) \in I$. Ainsi, on a $I_1 \times I_2 \subset I$. Réciproquement, si $(x,y) \in I$, alors $(x,0) = (1,0) \times (x,y) \in I$ et donc $x \in I_1$. De même, $y \in I_2$ et donc $(x,y) \in I_1 \times I_2$.
3. $\mathbb{Z}$ étant principal, il existe des entiers a et b tels que $I_1 = a\mathbb{Z}$ et $I_2 = b\mathbb{Z}$. Alors d'après la question précédente, $I = a\mathbb{Z} \times b\mathbb{Z} = (a,b)\mathbb{Z}^2$.

3. Exercices d'entraînement

a. Ordre d'un élément dans un groupe

Exercice 12.

Soit G un groupe de cardinal $2n$.

1. Démontrer que la relation $\mathcal{R}$ définie sur G par
$$x\mathcal{R}y \iff x = y \text{ ou } x = y^{-1}$$
est une relation d'équivalence sur G.
2. En déduire que G admet des éléments d'ordre deux.

Correction.

1. La relation est clairement réflexive et symétrique. De plus, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors
   — si $x = y$ et $y = z$, on a $x = z$;
   — si $x = y$ et $y = z^{-1}$, on a $x = z^{-1}$;
   — si $x = y^{-1}$ et $y = z$, on a $x = z^{-1}$;
   — si $x = y^{-1}$ et $y = z^{-1}$, on a $x = z$.
   Dans tous les cas, on a $x\mathcal{R}z$ et la relation est transitive.
2. Une classe d'équivalence comporte
   — ou bien un seul élément, si $x = x^{-1}$;
   — ou bien deux élements, si $x \neq x^{-1}$; les éléments sont alors x et x^{-1}.
   Il y a au moins une classe d'équivalence avec un seul élément : la classe de l'élément neutre. De plus, les classes d'équivalence forment une partition de G, et G est de cardinal pair. Il doit donc y avoir une autre classe de cardinal 1 (sinon le cardinal de G serait impair). Cette autre classe de cardinal 1 donne un élément x égal à son inverse.

Exercice 13.

Soient G et H deux groupes.

1. Montrer que si g est un élément d'ordre p de G et h un élément d'ordre q de H, alors (g,h) est d'ordre $\text{ppcm}(p,q)$ dans $G \times H$.

2. On suppose que G et H sont cycliques. Démontrer que $G \times H$ est cyclique si et seulement si les ordres de G et H sont premiers entre eux.

Correction.

1. On a $(g,h)^n = (g^n, h^n) = (e,e)$ si et seulement si on a à la fois $p|n$ et $q|n$, donc si et seulement si $\text{ppcm}(p,q)|n$. Ainsi, l'ordre de (g,h) est bien le ppcm de p et q.
2. Soit p l'ordre de G et q l'ordre de H. Si $p \wedge q = 1$, si x est un générateur de G (d'ordre p donc) et si y est un générateur de H (d'ordre q donc), alors (x,y) est d'ordre $\text{ppcm}(p,q) = pq$. Puisque $G \times H$ est de cardinal pq, c'est bien un groupe cyclique. Réciproquement si $G \times H$ est cyclique, soit (g,h) un générateur de $G \times H$. Alors g est un générateur de G et h est un générateur de H. Leur ordre respectif est donc p (resp. q), et par la première question, (g,h) est d'ordre $\text{ppcm}(p,q)$. Puisqu'on sait qu'il est d'ordre pq, on a bien $\text{ppcm}(p,q) = pq$ qui implique que p et q sont premiers entre eux.

Exercice 14.

Soit G un groupe admettant un nombre fini de sous-groupes.

1. Démontrer que tout élément de G est d'ordre fini.
2. En déduire que G est fini.

Correction.

1. Supposons que G admette un élément x d'ordre infini et notons H le sous-groupe engendré par x. Alors H est isomorphe à $(\mathbb{Z}, +)$, qui contient une infinité de sous-groupes. On en déduit que H, et donc G, contiennent aussi une infinité de sous-groupes (les sous-groupes engendrés par les x^n, $n \geq 1$, qui ne sont pas deux à deux égaux).
2. Pour $x \in G$, notons H_x le sous-groupe engendré par x. Alors on a $G = \bigcup_{x \in G} H_x$. Mais puisque G contient seulement un nombre fini de sous-groupes, il y a un nombre fini de H_x différents, notons-les $H_{x_1}, \ldots, H_{x_p}$, d'où $G = \bigcup_{i=1}^{p} H_{x_i}$. Mais chacun des H_{x_i} est fini d'après la question précédente. Donc G est fini.

Exercice 15.

Soit $G = (\mathbb{Z}/20\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.

1. Donner la liste de tous les éléments de G.
2. Pour tout $a \in G$, déterminer le sous groupe $< a >$ engendré par a.
3. Déterminer un ensemble minimal de générateurs de $(G, \cdot)$.
4. $(G, \cdot)$ est-il un groupe cyclique ?
5. Déterminer tous les sous-groupes de G et, pour chaque sous-groupe, préciser un ensemble de générateurs.
6. Parmi les sous-groupes de $(G, \cdot)$, lesquels sont isomorphes à un groupe additif $(\mathbb{Z}/m\mathbb{Z}, +)$?

Correction.

1. Rappelons que par le théorème de Bézout, n est inversible dans $(Z/20\mathbb{Z}, \cdot)$ si et seulement si n est premier avec 20. On a donc $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$.
2. On prend un élément et toutes ses puissances, jusqu'à obtenir l'élément neutre 1. On obtient

$$\begin{aligned} <1> &= \{1\} \\ <3> &= \{1, 3, 7, 9\} \\ <7> &= \{1, 3, 7, 9\} \\ <9> &= \{1, 9\} \\ <11> &= \{1, 11\} \\ <13> &= \{1, 9, 13, 17\} \\ <17> &= \{1, 9, 13, 17\} \\ <19> &= \{1, 19\} \end{aligned}$$

3. On vient de voir qu'on ne peut pas engendrer le groupe avec un seul élément. Essayons avec deux éléments. C'est facile à voir. Si on prend par exemple 3 et 11, le groupe engendré comprend au moins $<3>$ et $<11>$, c'est-à-dire au moins 5 éléments. Comme son ordre doit diviser l'ordre du groupe, il contient au moins 8 éléments, c'est-à-dire que c'est G tout entier. Autrement dit, on a prouvé que $<3, 11>= G$ et donc $\{3, 11\}$ est un ensemble minimal de générateurs de G.
4. Aucun élément de G n'engendre seul le groupe. G n'est pas cyclique.
5. Les sous-groupes de G sont d'ordre 1,2,4 ou 8. Dans G, il y a un élément d'ordre 1, 4 éléments d'ordre 4 et 3 éléments d'ordre 2. Si on combine deux éléments d'ordre 4 qui n'engendrent pas le même sous-groupe, ou un élément d'ordre 4 avec un élément d'ordre 2 qui n'est pas dans le sous-groupe engendré (comme à la question 3), on obtiendra G tout entier. Reste à voir les sous-groupes engendrés par les éléments d'ordre 2 : on a

$$<11, 19>= \{1, 11, 19, 9\}$$

$$<3, 11>=<3, 13>=<3, 19>=<11, 13>=<13, 19>= G.$$

6. Parmi les sous-groupes de G, ceux de la deuxième question sont cycliques, donc isomorphes à $\mathbb{Z}/m\mathbb{Z}$ où $m = 1, 2, 4$ suivant le cas. Le sous-groupe $<11, 19>$ n'est pas cyclique, car il n'est pas engendré par un seul élément. De même, G n'est pas cyclique.

b. Idéaux

Exercice 16.

Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A, on note

$$\begin{aligned} I + J &= \{i + j;\ i \in I,\ j \in J\} \\ I.J &= \{i_1 j_1 + \cdots + i_n j_n;\ n \geq 1,\ i_k \in I,\ j_k \in J\} \end{aligned}$$

On dit que deux idéaux I et J sont étrangers si $I + J = A$.

1. Montrer que $I + J$ et IJ sont encore des idéaux de A.
2. Montrer que $I.J \subset I \cap J$.

3. Montrer que $(I+J).(I\cap J)\subset I.J$.
4. Montrer que si I et J sont étrangers, alors $I.J=I\cap J$.

Correction.

1. Commençons par $I+J$. Il faut d'abord démontrer que c'est un sous-groupe de $(A,+)$. Mais $0=0+0\in I+J$. D'autre part, si x et y sont éléments de $I+J$, on les écrit $x=i+j$, $y=i'+j'$, et on a
$$x-y=(i-i')+(j-j')\in I+J$$
puisque $i-i'\in I$ et $j-j'\in J$. D'autre part, pour $a\in A$, on a, par distributivité de $\times$ par rapport à $+$:
$$ax=ai+aj\in I+J$$
puisque, I et J étant deux idéaux, $ai\in I$ et $aj\in J$. Ceci prouve que $I+J$ est un idéal. Passons maintenant à $I.J$: $0\times 0=0$ est élément de $I.J$. De plus, si $x=\sum_{k=1}^{n} i_k j_k$ et $y=\sum_{l=1}^{m} i'_l j'_l$, en posant $i_k=-i'_{k-n}$ et $j'_k=-j'_{k-n}$ pour k allant de $n+1$ à $n+m$, on a
$$x-y=\sum_{k=1}^{n+m} i_k j_k$$
ce qui prouve que $I.J$ est un sous-groupe de $(A,+)$. Enfin, pour tout a dans A, on a
$$ax=\sum_{k=1}^{n}(ai_k)j_k\in I.J$$
puisque chaque ai_k (resp. j_k) est élément de I (resp. de J).
2. Soit $x=\sum_{k=1}^{n} i_k j_k$ un élément de $I.J$. Pour chaque k, $i_k j_k$ est un élément de I puisque I est un idéal. Comme I est de plus stable par la somme, $I.J$ est bien contenu dans I. Par symétrie du rôle joué par I et J, $I.J$ est aussi contenu dans J et donc $I.J$ est contenu dans $I\cap J$.
3. Soit $x\in(I+J).(I\cap J)$. On écrit $x=\sum_{k=1}^{n} a_k b_k$ avec $a_k\in I+J$ et $b_k\in I\cap J$. Puisque $I.J$ est un idéal, il suffit de prouver que $a_k b_k\in I.J$. On écrit $a_k=i_k+j_k$, de sorte que
$$a_k b_k=i_k b_k+b_k j_k.$$
C'est un élément de $I.J$, car $i_k\in I$, $b_k\in J$ et $b_k\in I$, $j_k\in J$.
4. Il suffit de prouver que $I\cap J\subset I.J$. D'après la question précédente, on a $A.(I\cap J)\subset I.J$. Prenons $x\in I\cap J$. Alors $x=1_A x\in A.(I\cap J)\subset I.J$ Ceci prouve l'inclusion restante.

Exercice 17.

Soit p un nombre premier. On note
$$\mathbb{Z}_p=\left\{x=\frac{m}{n};\ (m,n)\in\mathbb{Z}\times\mathbb{N}^*,\ p\wedge n=1\right\}.$$

1. Vérifier que $\mathbb{Z}_p$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

2. Soit $k \geq 0$. On note
$$J_{p^k} = \left\{ \frac{m}{n};\ (m,n) \in \mathbb{Z} \times \mathbb{N}^*,\ p \wedge n = 1,\ p^k | m \right\}.$$
Vérifier que J_{p^k} est un idéal de $\mathbb{Z}_p$.
3. Réciproquement, montrer que si I est un idéal de A, il existe $k \geq 1$ tel que $I = J_{p^k}$.

Correction.

1. La preuve est facile et laissée au lecteur : le point clé est que si p est premier avec n et avec n', alors p est premier avec le produit nn'.
2. D'abord, on peut remarquer que $0 \in J_{p^k}$. Prenons ensuite $x = \frac{m}{n}$ et $y = \frac{m'}{n'}$ deux éléments de J_{p_k}. Alors
$$x - y = \frac{mn' - m'n}{nn'}$$
avec $p \wedge (nn') = 1$ (voir plus haut) et $p^k | m$, $p^k | m'$ et donc $p^k | mn' - m'n$. Ensuite, si $z = \frac{a}{b} \in \mathbb{Z}_p$, alors $xz = \frac{am}{bn}$ est tel que $p^k | am$ et $p \wedge (bn) = 1$, et donc $xz \in J_{p^k}$. J_{p^k} est bien un idéal de $\mathbb{Z}_p$.
3. Posons $k = \max\{l \geq 0;\ \forall x \in I,\ \exists (m,n) \in \mathbb{Z} \times \mathbb{N}^*, x = \frac{m}{n},\ p^l | m,\ p \wedge n = 1\}$ et prouvons que $I = J_{p^k}$. D'abord, il est clair que $I \subset J_{p^k}$. Réciproquement, soit $x \in J_{p^k}$, il faut prouver que $x \in I$. Par définition de k, on sait que l'on peut trouver $y = \frac{a}{b} \in I$ tel que $a = p^k a'$ avec $a' \wedge p = b \wedge p = 1$. Mais alors, $\frac{a'}{b}$ est inversible dans $\mathbb{Z}_p$, d'inverse $\frac{b}{a'}$. Puisque I est un idéal, ceci entraine que $p^k = y \times \frac{b}{a'} \in I$. Mais alors, puisque x s'écrit $x = p^k \frac{m'}{n}$ avec $p \wedge n = 1$, on en déduit que $x \in I$. On a bien démontré que tous les idéaux de $\mathbb{Z}_p$ sont de la forme J_{p^k}.

Exercice 18.

Soit $n \geq 2$. Démontrer que tous les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont principaux. A quelle condition $\mathbb{Z}/n\mathbb{Z}$ est-il principal ?

Correction.

Soit I un idéal de $\mathbb{Z}/n\mathbb{Z}$, et $J = \{m \in \mathbb{Z};\ \bar{m} \in I\}$. Alors J est un idéal de $\mathbb{Z}$. Il est non-vide car I est non-vide, et si $u, v \in J,\ k \in \mathbb{Z}$, alors
$$\overline{u+v} = \bar{u} + \bar{v} \in I \implies u + v \in J$$
$$\overline{ku} = \bar{k} \times \bar{u} \in I \implies ku \in J.$$
Ainsi, il existe $a \in \mathbb{Z}$ tel que $J = a\mathbb{Z}$. De plus, on peut aussi remarquer que, puisque $n\mathbb{Z} \subset J$, on doit avoir $a | n$. Démontrons alors que $I = \bar{a}\mathbb{Z}/n\mathbb{Z}$. Puisque $\bar{a} \in I$, il est clair que $\bar{a}\mathbb{Z}/n\mathbb{Z} \subset I$. Réciproquement, soit $\bar{u} \in \bar{a}\mathbb{Z}/n\mathbb{Z}$. Alors $\bar{u} = \bar{a} \times \bar{k} = \overline{ak}$ et donc $u \in a\mathbb{Z} + n\mathbb{Z} = a\mathbb{Z}$ puisque $a | n$. Ainsi, $\bar{u} \in I$, ce qui prouve l'inclusion réciproque. Ainsi, on a prouvé que tous les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux. Pour que l'anneau lui-même soit principal, il faut encore qu'il soit intègre. Ceci n'est vrai que si n est premier.

Exercice 19.

Soit $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}^2\}$.

1. Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Soit $z \in \mathbb{C}$. Démontrer qu'il existe $\omega \in \mathbb{Z}[i]$ tel que $|z - \omega| < 1$.
4. Soient $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Démontrer qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
5. Démontrer que $\mathbb{Z}[i]$ est principal.

Correction.

1. Il suffit de vérifier les propriétés… La preuve est laissée au lecteur !
2. Soit $a + ib$ un élément de $\mathbb{Z}[i]$ inversible. Son inverse est nécessairement le même que dans $\mathbb{C}$, c'est-à-dire
$$\frac{1}{a+ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}.$$
On ne peut pas avoir $(a, b) = (0, 0)$. Si $|a| \geq 2$, alors $\frac{a}{a^2+b^2}$ ne peut pas être un entier, et de même si $|b| \geq 2$, $\frac{b}{a^2+b^2}$ ne peut pas être un entier. On a donc $|a| \leq 1$ et $|b| \leq 1$. Mais le cas $(a, b) = (\pm 1, \pm 1)$ ne convient pas non plus. Donc les seules possibilités sont $(\pm 1, 0)$ et $(0, \pm 1)$ qui donnent effectivement des éléments inversibles. $\mathbb{Z}[i]$ possède donc 4 éléments inversibles : $1, -1, i, -i$.
3. Écrivons $z = x + iy$. On approche x et y par l'entier le plus proche : il existe $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Mais alors, si on pose $\omega = a + ib$, on obtient
$$|z - \omega|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1.$$
4. D'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que
$$\left|\frac{u}{v} - q\right| < 1.$$
Posons $r = v\left(\frac{u}{v} - q\right)$. Alors $|r| < |v|$ et on a bien $u = qv + r$. On n'a pas en général unicité de cette "division euclidienne" car on n'a pas unicité dans l'approximation de la question précédente. Prenons par exemple $u = 1 + i$ et $v = 2$, de sorte que u/v peut être approché par 0 ou 1 (ou aussi par i et $1 + i$). On peut alors écrire les deux divisions
$$1 + i = 0 \times 2 + (1 + i)$$
$$1 + i = 1 \times 2 + (-1 + i)$$
avec chaque fois le module du reste inférieur strict à 2.
5. Soit I un idéal de $\mathbb{Z}[i]$ non réduit à $\{0\}$. On considère $a \in I \backslash \{0\}$ tel que $|a|$ est minimal. Ceci a un sens, car $|z| \geq 1$ pour tout $z \in \mathbb{Z}[i] \backslash \{0\}$, et il y a seulement un nombre fini d'éléments de $\mathbb{Z}[i]$ de module inférieur à un réel donné. On va alors démontrer que I est l'idéal engendré par a. Pour cela, prenons $u \in I$ et effectuons la division euclidienne donnée par la question précédente :
$$u = qa + r \text{ avec } |r| < |a|.$$
Mais alors, $u \in I$, $qa \in I$ et donc $r \in I$. Par minimalité de $|a|$, on doit avoir $|r| = 0$, ce qui prouve que $u \in a\mathbb{Z}[i]$.

4. Exercices d'approfondissement

a. Ordre d'un élément dans un groupe

Exercice 20.

Soit G un groupe abélien, x et y deux éléments de G d'ordres respectifs p et q.

1. On suppose que p et q sont premiers entre eux. Démontrer que xy est d'ordre pq.
2. Importance des hypothèses - 1 : Si $H = GL_2(\mathbb{R})$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, vérifier que A et B sont d'ordre fini, mais que AB n'est pas d'ordre fini.
3. Importance des hypothèses - 2 : Si p et q ne sont pas supposés premiers entre eux, démontrer que le produit xy n'est pas nécessairement d'ordre pq, ou d'ordre $\text{ppcm}(p, q)$.
4. Une application :
   (a) Soit d un diviseur de p. Démontrer qu'il existe un élément d'ordre d dans G.
   (b) En déduire que G admet des éléments d'ordre $\text{ppcm}(p, q)$.
   (c) On suppose de plus que G est fini. Démontrer que G admet un élément dont l'ordre est le ppcm de l'ordre des éléments de G.

Correction.

1. Notons d l'ordre de xy. Remarquons que $(xy)^{pq} = (x^p)^q(y^q)^p = e$, et donc $d|pq$. De plus, puisque $(xy)^d = e$, on en déduit que $x^d = y^{-d}$. Il vient alors
$$x^{dq} = (y^{-d})^q = (y^q)^{-r} = e.$$
Ainsi, $p|dq$ et puisque p et q sont premiers entre eux, on en déduit que $p|d$. De la même façon, on a $q|d$ et en utilisant à nouveau que p et q sont premiers entre eux, on conclut que $pq|d$. Ainsi, on a bien que $d = pq$.
2. On vérifie facilement que A est d'ordre 4, que B est d'ordre 3 et que
$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
On prouve alors par récurrence que, pour tout $n \geq 1$,
$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$
AB n'est pas d'ordre fini, et donc l'hypothèse que G est commutatif est importante.
3. Si x est un élément d'ordre $n \geq 2$ dans un groupe G, son inverse x^{-1} est aussi d'ordre n, et pourtant le produit xx^{-1} est d'ordre 1, et non d'ordre n ou n^2 !
4. Une application :
   (a) Considérons $a = x^{p/d}$. Alors on a $a^d = x^p = e$. D'autre part, si $a^r = e$, alors $x^{rp/d} = e$ et donc rp/d est un multiplie de p. En particulier r/d est un entier, ce qui signifie que $d|r$. a est donc bien d'ordre d.

(b) Décomposons p et q en facteurs premiers (pour avoir les mêmes facteurs, on s'autorise des exposants nuls) :

$$p = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad q = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

On sait qu'alors

$$\text{ppcm}(p, q) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

Par la question précédente, il est possible, pour chaque $i = 1, \ldots, r$, de fabriquer un élément a_i d'ordre $p_i^{\max(\alpha_i, \beta_i)}$ (on le fabrique à partir de x si $\alpha_i \geq \beta_i$, à partir de y sinon). En utilisant le résultat de la première question et une simple récurrence, le produit $a_1 \ldots a_r$ est bien d'ordre $\text{ppcm}(p, q)$.

(c) Notons $x_1, \ldots, x_r$ les éléments de G, d'ordres respectifs $q_1, \ldots, q_r$. Alors d'après la question précédente, il existe un élément d'ordre $ppcm(q_1, q_2)$. Puis appliquant une nouvelle fois la question précédente, il existe un élément d'ordre $ppcm(ppcm(q_1, q_2), q_3) = ppcm(q_1, q_2, q_3)$. Par une récurrence facile, on construit un élément d'ordre le ppcm que $q_1, \ldots, q_r$.

Exercice 21.

Soit G un groupe cyclique et soit H un sous-groupe de G. Démontrer que H est cyclique.

Correction.

Soit a un générateur de G. L'ensemble des entiers $p \geq 1$ tels que $a^p \in H$ est non-vide (puisque $a^{\text{card}(G)} = e \in H$). Il contient un plus petit élément que nous noterons n. On va alors prouver que H est le groupe engendré par a^n. Il est d'abord évident que le sous-groupe engendré par a^n est contenu dans H. Réciproquement, soit $x \in H$. x s'écrit $x = a^p$, et il suffit de prouver que $p = kn$. Effectuons la division euclidienne de p par n : $p = qn + r$ avec $0 \leq r < n$. Mais alors :

$$a^p = (a^n)^q a^r \implies a^r = a^p (a^n)^{-q} \in H.$$

Par minimalité de n, ceci n'est possible que si $r = 0$, donc que si p est un multiple de n. Remarquons la proximité entre cette démonstration et celle des sous-groupes de $\mathbb{Z}$.

Exercice 22.

1. Soit G un groupe et H, K deux sous-groupes de G d'ordre des entiers premiers. Démontrer que $H = K$ ou que $H \cap K = \{e\}$.
2. Démontrer que dans un groupe d'ordre 35, il existe un élément d'ordre 5 et un élément d'ordre 7.

Correction.

1. Soit p l'ordre de H, qui est premier. Puisque un élément de H a un ordre qui divise p, cet ordre ne peut être égal que à 1, si c'est l'élément neutre, ou à p. Autrement dit, tout élément de H autre que l'élément neutre génère H. Il en est de même pour tout élément de K. Ainsi, si $H \cap K$ contient un élément x différent de e, il contient toutes les puissances

de x, donc H et K, et $H = K$.

2. Soit G un tel groupe. Ses éléments peuvent être d'ordre 1, 5, 7 ou 35. Si G admet un élément d'ordre 35 (ie G est cyclique), que l'on appelle a, alors a^5 est d'ordre 7 et a^7 est d'ordre 5. Supposons donc que G n'est pas cyclique et qu'il n'admet pas d'éléments d'ordre 7. Alors tous ses éléments, sauf l'élément neutre, sont d'ordre 5, et G est réunion de sous-groupes d'ordre 5. D'après la première question, l'intersection de deux de sous-groupes, quand ils sont distincts, est restreinte à $\{e\}$. Notons $G_1, \dots, G_n$ ces sous-groupes distincts. Alors chaque G_i s'écrit $G_i = \{e\} \cup H_i$, et les $H_1, \dots, H_n$ sont deux à deux disjoints. Autrement dit,
$$G = \{e\} \cup H_1 \cup \cdots \cup H_n$$
est une partition de G. Comme chaque H_i est de cardinal 4, ceci implique que $35 = 4n + 1$. Mais alors 34 serait un multiple de 4, ce qui n'est pas le cas. Le raisonnement est similaire si on suppose que G n'admet pas d'éléments d'ordre 5. On aurait alors $35 = 6m + 1$ pour un entier m, ce qui n'est pas le cas puisque 34 n'est pas un multiple de 6.

b. Idéaux

Exercice 23.

Soit A un anneau commutatif (unitaire). Si I est un idéal de A, on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A;\ \exists n \geq 1,\ x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soient I, J deux idéaux de A et $p \geq 1$. Montrer que
$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J},\ \sqrt{\sqrt{I}} = \sqrt{I} \text{ et } \sqrt{I^p} = \sqrt{I}.$$
3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geq 1$, déterminer le radical de I.

Correction.

1. On commence par remarquer que si $x^n \in I$, alors pour tout $k \geq n$, $x^k = x^{k-n}x^n \in I$ (qui est un idéal). Montrons d'abord que $(\sqrt{I}, +)$ est un sous-groupe de $(A, +)$. En effet, $0 \in \sqrt{I}$ puisque $I \subset \sqrt{I}$ (prendre $n = 1$). De plus, si x est dans $\sqrt{I}$ alors $(-x)^n = (-1)^n x^n \in I$ puisque $x^n \in I$ et que I est un idéal. Prenons maintenant x, $y \in I$ et $n, m \in \mathbb{N}$ tels que $x^n \in I$, $y^m \in I$. Alors, par la formule du binôme que l'on peut appliquer dans l'anneau **commutatif** A, on a
$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$
Or, si $k \leq n$, alors $n + m - k \geq m$ et donc $y^{n+m-k} \in I$, ce qui entraine $x^k y^{n+m-k} \in I$. Si $k \geq n$, cette fois $x^k \in I$ et donc $x^k y^{n+m-k} \in I$. $(I, +)$ étant un sous-groupe de $(A, +)$, on en déduit que $(x+y)^{n+m} \in I$, c'est-à-dire $x + y \in \sqrt{I}$. Finalement, prouvons que pour $a \in A$ et $x \in \sqrt{I}$, alors $ax \in \sqrt{I}$. Soit $n \geq 0$ tel que $x^n \in I$. Alors $(ax)^n = a^n x^n \in I$, ce qui prouve le résultat.
2. <ul class="rien">

3. Soit $x \in \sqrt{I.J}$. Il existe $n \geq 1$ tel que $x^n \in I.J$, c'est-à-dire $x^n = \sum_k a_k b_k$ avec $a_k \in I$ et $b_k \in J$. Alors $x^n \in I$ puisque I est un idéal et $x^n = ab$, $a \in I$, et de même $x^n \in J$ (on utilise en fait que $I.J \subset I \cap J$). Ainsi, $x \in \sqrt{I \cap J}$. Soit maintenant $x \in \sqrt{I \cap J}$. Alors il existe $n \geq 1$ tel que $x^n \in I$ et $x^n \in J$. Donc $x \in \sqrt{I}$ et $x \in \sqrt{J}$, soit $x \in \sqrt{I} \cap \sqrt{J}$. Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors il existe $n, m \geq 1$ tels que $x^n \in I$ et $x^m \in J$. Alors $x^{n+m} = x^n x^m \in I.J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I.J}$.
4. On a $I \subset \sqrt{I}$ et donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement, prenons $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Posons $y = x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $y^m \in I$. Alors, $x^{nm} = y^m \in I$ et donc $x \in \sqrt{I}$.
5. La dernière égalité se prouve de façon tout à fait identique !
6. Soit $x \in \mathbb{Z}$. x est dans $\sqrt{k\mathbb{Z}}$ si et seulement si il existe $n \geq 1$ tel que $x^n \in k\mathbb{Z}$. Autrement dit, $k | x^n$. Décomposons k en produits de facteurs premiers : $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On obtient que $p_i | x^n \implies p_i | x$ pour tout $i = 1, \dots, r$ et donc $p_1 \dots p_r | x$, ce qui peut encore s'écrire $x \in (p_1 \dots p_r)\mathbb{Z}$. Réciproquement, si $x \in (p_1 \dots p_r)\mathbb{Z}$, alors, x s'écrit $x = p_1 \dots p_r m$. Notant $n = \max_{i \in \{1,\dots,r\}}(\alpha_i)$, on a $k | x^n$. Ainsi, on a prouvé que $\sqrt{I} = (p_1 \dots p_r)\mathbb{Z}$.

Exercice 24.

Soit $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}^2\}$.

1. Démontrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
3. Soit $z \in \mathbb{C}$. Démontrer qu'il existe $\omega \in \mathbb{Z}[i]$ tel que $|z - \omega| < 1$.
4. Soient $u, v \in \mathbb{Z}[i]$ avec $v \neq 0$. Démontrer qu'il existe $q, r \in \mathbb{Z}[i]$ avec $u = qv + r$ et $|r| < |v|$. A-t-on unicité ?
5. Démontrer que $\mathbb{Z}[i]$ est principal.

Correction.

1. Il suffit de vérifier les propriétés… La preuve est laissée au lecteur !
2. Soit $a + ib$ un élément de $\mathbb{Z}[i]$ inversible. Son inverse est nécessairement le même que dans $\mathbb{C}$, c'est-à-dire
$$\frac{1}{a+ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}.$$
On ne peut pas avoir $(a, b) = (0, 0)$. Si $|a| \geq 2$, alors $\frac{a}{a^2+b^2}$ ne peut pas être un entier, et de même si $|b| \geq 2$, $\frac{b}{a^2+b^2}$ ne peut pas être un entier. On a donc $|a| \leq 1$ et $|b| \leq 1$. Mais le cas $(a, b) = (\pm 1, \pm 1)$ ne convient pas non plus. Donc les seules possibilités sont $(\pm 1, 0)$ et $(0, \pm 1)$ qui donnent effectivement des éléments inversibles. $\mathbb{Z}[i]$ possède donc 4 éléments inversibles : $1, -1, i, -i$.
3. Écrivons $z = x + iy$. On approche x et y par l'entier le plus proche : il existe $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Mais alors, si on pose $\omega = a + ib$, on obtient
$$|z - \omega|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1.$$

4. D'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que

$$\left|\frac{u}{v} - q\right| < 1.$$

Posons $r = v\left(\frac{u}{v} - q\right)$. Alors $|r| < |v|$ et on a bien $u = qv + r$. On n'a pas en général unicité de cette "division euclidienne" car on n'a pas unicité dans l'approximation de la question précédente. Prenons par exemple $u = 1 + i$ et $v = 2$, de sorte que u/v peut être approché par 0 ou 1 (ou aussi par i et $1 + i$). On peut alors écrire les deux divisions

$$1 + i = 0 \times 2 + (1 + i)$$

$$1 + i = 1 \times 2 + (-1 + i)$$

avec chaque fois le module du reste inférieur strict à 2.

5. Soit I un idéal de $\mathbb{Z}[i]$ non réduit à $\{0\}$. On considère $a \in I\backslash\{0\}$ tel que $|a|$ est minimal. Ceci a un sens, car $|z| \geq 1$ pour tout $z \in \mathbb{Z}[i]\backslash\{0\}$, et il y a seulement un nombre fini d'éléments de $\mathbb{Z}[i]$ de module inférieur à un réel donné. On va alors démontrer que I est l'idéal engendré par a. Pour cela, prenons $u \in I$ et effectuons la division euclidienne donnée par la question précédente :

$$u = qa + r \text{ avec } |r| < |a|.$$

Mais alors, $u \in I$, $qa \in I$ et donc $r \in I$. Par minimalité de $|a|$, on doit avoir $|r| = 0$, ce qui prouve que $u \in a\mathbb{Z}[i]$.