

Corrigé de la feuille d'exercices n°7

1. Exercices basiques**a. Ordre d'un élément dans un groupe****Exercice 1.**

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) :

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

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

Exercice 2.

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^2 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 3.

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 $x^2 y^2 = e = xyxy$ soit en simplifiant à gauche par x et à droite par y , $xy = yx$.

Exercice 4.

Dans un repère orthonormé $(O, \vec{i}, \vec{j}, \vec{k})$, on considère les droites \mathcal{D} et \mathcal{D}' d'équations paramétriques respectives

$$\begin{cases} x = 2 + t \\ y = 3 - 2t \\ z = 5 - t \end{cases} \quad t \in \mathbb{R} \quad \text{et} \quad \begin{cases} x = 4 - 3t' \\ y = 5 - 8t' \\ z = 7 - t' \end{cases} \quad t' \in \mathbb{R}.$$

1. Les droites \mathcal{D} et \mathcal{D}' sont-elles coplanaires ?
2. Vérifier que le point $A(2, 3, 5)$ est un point de \mathcal{D} . Soit M' un point quelconque de \mathcal{D}' . Quel est le lieu du point I , milieu de $[AM']$, lorsque M' décrit la droite \mathcal{D}' .
3. On considère un point M de \mathcal{D} et un point M' de \mathcal{D}' . Quel est le lieu du milieu du segment $[MM']$ lorsque M et M' décrivent respectivement les droites \mathcal{D} et \mathcal{D}' .

Correction.

1. Deux droites coplanaires sont ou bien parallèles, ou bien concourantes. On vérifie ici aisément que les deux droites ne sont pas concourantes, en résolvant le système d'équations

$$\begin{cases} 2 + t = 4 - 3t' \\ 3 - 2t = 5 - 8t' \\ 5 - t = 7 - t' \end{cases}$$

dont on vérifie qu'il n'admet pas de solutions. Elles ne sont pas parallèles non plus, puisque leurs vecteurs directeurs respectifs, $(1, -2, -1)$ et $(-3, -8, -1)$ ne sont pas colinéaires. Donc elles sont non coplanaires.

2. Notons \mathcal{L}_1 le lieu considéré. Alors $N(x, y, z) \in \mathcal{L}_1$ si et seulement s'il existe $t' \in \mathbb{R}$ tel que N est milieu de $[AM']$ où $M' = (4 - 3t', 5 - 8t', 7 - t')$, donc si et seulement s'il existe $t' \in \mathbb{R}$ tel que

$$\begin{cases} x = 3 - \frac{3}{2}t' \\ y = 4 - 4t' \\ z = 6 - \frac{1}{2}t'. \end{cases}$$

Le lieu recherché est donc la droite passant par $(3, 4, 6)$ et de vecteur directeur $(-3/2, -4, -1/2)$.

3. Notons \mathcal{L}_2 le lieu considéré. Alors $N(x, y, z) \in \mathcal{L}_2$ si et seulement s'il existe $t, t' \in \mathbb{R}$ tel que N est milieu de $[MM']$ où $M = (2 + t, 3 - 2t, 5 - t)$ et $M' = (4 - 3t', 5 - 8t', 7 - t')$, donc si et seulement s'il existe $t, t' \in \mathbb{R}$ tel que

$$\begin{cases} x = 3 + \frac{1}{2}t - \frac{3}{2}t' \\ y = 4 - t - 4t' \\ z = 6 - \frac{1}{2}t - \frac{1}{2}t'. \end{cases}$$

Le lieu recherché est donc le plan passant par $(3, 4, 6)$ et des vecteurs directeurs $(1/2, -1, -1/2)$ et $(-3/2, -4, -1/2)$.

b. Anneaux, sous-anneaux, idéaux

Exercice 5.

Un élément x d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. Montrer que xy est nilpotent.
2. Montrer que $x + y$ est nilpotent.
3. Montrer que $1_A - x$ est inversible.
4. Dans cette question, on ne suppose plus que A est commutatif. Soit $u, v \in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.

Correction.

Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.
2. Remarquons d'abord que pour $p \geq n$, on a $x^p = x^{p-n} x^n = 0$. D'après la formule du binôme, $(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$. Mais, pour $k \geq n$, $x^k = 0 \implies x^k y^{n+m-k} = 0$. D'autre part, pour $k < n$, on a $n + m - k \geq m$ et donc $y^{n+m-k} = 0 \implies x^k y^{n+m-k} = 0$. Ainsi, $(x + y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n + m - 1$.
3. L'idée est d'utiliser l'identité remarquable (toujours valable dans un anneau)

$$1 - x^p = (1 - x)(1 + x + \dots + x^{p-1}).$$

Si on l'applique pour $p = n$, alors on obtient

$$1 = (1 - x)(1 + x + \dots + x^{n-1})$$

ce qui implique que $1 - x$ est inversible d'inverse $1 + x + \dots + x^{n-1}$.

4. Soit $n \geq 1$ tel que $(uv)^n = 0$. Alors

$$(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0.$$

Ainsi, vu est nilpotent.

Exercice 6.

On dit qu'un anneau A est un anneau de Boole si, pour tout $x \in A$, $x^2 = x$. On fixe A un tel anneau.

1. Démontrer que, pour tout $x \in A$, $x = -x$.
2. Montrer que A est commutatif.

Correction.

1. On applique la propriété à l'élément $x + x$. Il vient

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x.$$

Après simplification, on trouve $x + x = 0$, soit $x = -x$.

2. Soient $x, y \in A$. On doit prouver $xy = yx$. Appliquons la propriété à l'élément $x + y$. On a

$$(x + y) = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx.$$

Après simplification, on trouve $xy + yx = 0$ soit $xy = -yx$, soit $xy = yx$ en appliquant le résultat de la question précédente.

Exercice 7.

Soit $(G, +)$ un groupe commutatif. On note $\text{End}(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : G \rightarrow G, x \mapsto f(x) + g(x)$. Démontrer que $(\text{End}(G), +, \circ)$ est un anneau.

Correction.

On remarque d'abord que $+$ et \circ sont bien des lois de composition interne sur $\text{End}(G)$. Ensuite, on vérifie tous les points de la définition d'un anneau.

1. $(\text{End}(G), +)$ est un groupe commutatif. En effet, la loi $+$ est associative, l'application $0_G : G \rightarrow G, g \mapsto 0$ est un élément neutre pour la loi $+$, et tout élément $f \in \text{End}(G)$ admet un inverse $-f : G \rightarrow G, x \mapsto -f(x)$.
2. La loi \circ est associative.
3. La loi \circ est distributive par rapport à la loi $+$: pour tous $f, g, h \in \text{End}(G)$ et tout $x \in G$,

$$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = (f \circ h + g \circ h)(x).$$

Ainsi, $(\text{End}(G), +, \circ)$ est un anneau.

Exercice 8.

Soit $A = \left\{ \frac{m}{n}; m \in \mathbb{Z}, n \in 2\mathbb{N} + 1 \right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair). Démontrer que $(A, +, \times)$ est un anneau. Quels sont ses éléments inversibles?

Correction.

On va démontrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$. Pour cela, soient $x = \frac{m}{n}$ et $y = \frac{m'}{n'} \in A$. Alors :

$$x - y = \frac{mn' - m'n}{nn'} \text{ et } xy = \frac{mm'}{nn'}.$$

Comme nn' , produit de deux nombres impairs, est impair, et que A est non vide puisqu'il contient 1, on en déduit que A est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons ensuite les inversibles de A . Soit $x = \frac{m}{n} \in A$ inversible, et soit $y = \frac{m'}{n'} \in A$ tel que $xy = 1$. On en déduit que $mm' = nn'$. En particulier, m est nécessairement impair. Réciproquement, si $x = \frac{m}{n}$ avec m impair, alors $y = \frac{n}{m}$ est dans A (si jamais $m < 0$, il suffit d'écrire $y = \frac{-n}{-m}$ pour vérifier qu'il est bien dans A), et $xy = 1$. Ainsi, les inversibles de A sont les éléments $\frac{m}{n}$ avec $m \in \mathbb{Z}, n \in \mathbb{N}^*$, et m, n impairs.

Exercice 9.

Pour $d \in \mathbb{N}$, on note $A_d = \{(x, y) \in \mathbb{Z}^2; y - x \in d\mathbb{Z}\}$.

1. Démontrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de \mathbb{Z}^2 .
2. Réciproquement, soit A un sous-anneau de \mathbb{Z}^2 . Démontrer que $H = \{x \in \mathbb{Z}; (x, 0) \in A\}$ est un sous-groupe de \mathbb{Z} .
3. En déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

Correction.

1. Il est clair que $0_{\mathbb{Z}^2}$ et $1_{\mathbb{Z}^2}$ sont éléments de A_d . Considérons ensuite $(x, y), (x', y') \in A_d$. Que $(x + x', y + y')$ reste élément de A_d ne pose pas de problèmes. Pour le produit, on a

$$(x, y) \times (x', y') = (xx', yy')$$

et on a $yy' - xx' = (y - x)y' + x(y' - x')$ d'où $d|yy' - xx'$.

2. $0 \in H$ et si $x, x' \in H$, alors $(x - x', 0) = (x, 0) - (x', 0) \in H$ et donc $x - x' \in H$. H est un sous-groupe de \mathbb{Z} .
3. Puisque \mathbb{Z} est principal, il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$. Démontrons que $A = A_d$. D'une part, si $(x, y) \in A$, alors

$$(x - y, 0) = (x, y) - y(1, 1) \in A$$

et donc $d|x - y$, c'est-à-dire $(x, y) \in A_d$. Réciproquement, si $(x, y) \in A_d$, alors $x - y \in d\mathbb{Z} = H$, ce qui signifie que $(x - y, 0) \in A$. On termine presque comme précédemment en écrivant que

$$(x, y) = (x - y, 0) + y(1, 1) \in A.$$

Les sous-anneaux de \mathbb{Z}^2 sont donc tous de la forme A_d .

Exercice 10.

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 11.

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 $-x \in A$. Finalement, on a bien prouvé que $N(A)$ est un idéal de A .

Exercice 12.

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 $x \in A \setminus \{0\}$. 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 $x \in A \setminus \{0\}$ 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 entraîne que $x^{p-n}a = 1$. x est alors inversible, d'inverse $x^{p-n-1}a$.

Exercice 13.

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 14.

Pour $1 \leq i, j \leq n$, on note $E_{i,j}$ la matrice élémentaire ayant tous ses coefficients nuls, sauf le coefficient de la i -ème ligne et de la j -ème colonne qui vaut 1.

1. Rappeler la formule donnant $E_{i,j}E_{k,l}$.
2. Soit $M = (a_{i,j}) \in \mathcal{M}_n(\mathbb{R})$. Que vaut $E_{i,j}M$? $ME_{k,l}$.
3. Démontrer que les seuls idéaux de $\mathcal{M}_n(\mathbb{R})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbb{R})$.

Correction.

1. C'est du cours! $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$.
2. Si on écrit $M = \sum_{k,l} a_{k,l}E_{k,l}$, on a $E_{i,j}M = \sum_{l=1}^n a_{j,l}E_{i,l}$. Autrement dit, toutes les lignes de $E_{i,j}M$ sont nulles, sauf la i -ème ligne constitué de la j -ième ligne de M . De même, écrivant $M = \sum_{i,j} a_{i,j}E_{i,j}$, on a $ME_{k,l} = \sum_{i,j} a_{i,j}E_{i,j}E_{k,l} = \sum_{i=1}^n a_{i,l}E_{i,l}$.
3. Soit I un idéal de $\mathcal{M}_n(\mathbb{R})$ et supposons le non réduit à $\{0\}$. Soit $M = (a_{i,j}) \neq 0$ un élément de I . Il existe donc i_0, j_0 tels que $a_{i_0, j_0} \neq 0$. Fixons ensuite i, j dans $\{1, \dots, n\}$. Par les formules précédents, on sait que

$$\frac{1}{a_{i_0, j_0}} E_{i, i_0} M E_{j_0, j} = E_{i, j}.$$

Mais puisque I est un idéal, c'est un élément de I . Donc $E_{i,j} \in I$. On en déduit alors facilement, par les propriétés d'idéal de I , que toute matrice est élément de I .

2. Exercices d'entraînement

a. Ordre d'un élément dans un groupe

Exercice 15.

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 éléments, 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 16.

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.

b. Anneaux, sous-anneaux, idéaux

Exercice 17.

Soit \mathbb{D} l'ensemble des nombres décimaux,

$$\mathbb{D} = \left\{ \frac{n}{10^k}; n \in \mathbb{Z}, k \in \mathbb{N} \right\}.$$

Démontrer que $(\mathbb{D}, +, \times)$ est un anneau. Quels sont ses éléments inversibles ?

Correction.

On va prouver que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$. On remarque d'abord que $\mathbb{D} \subset \mathbb{Q}$, puis que $1 \in \mathbb{D}$. De plus, soient $x = \frac{n}{10^k}$ et $y = \frac{m}{10^l}$ deux éléments de \mathbb{D} . Alors

$$x - y = \frac{n10^l - m10^k}{10^{k+l}} \text{ et } xy = \frac{nm}{10^{k+l}}$$

sont clairement des éléments de \mathbb{D} , et $(\mathbb{D}, +, \times)$ est bien un sous-anneau de $(\mathbb{Q}, +, \times)$. Déterminons ensuite les inversibles de $(\mathbb{D}, +, \times)$. Soit $x = \frac{n}{10^k}$ inversible, d'inverse $y = \frac{m}{10^l}$. Alors

$$xy = 1 \iff nm = 10^{k+l}.$$

On en déduit que les seuls diviseurs premiers de n sont 2 et 5, autrement dit que n s'écrit $\pm 2^p 5^q$ pour $p, q \in \mathbb{N}$. Réciproquement, soit $x = \frac{\pm 2^p 5^q}{10^k}$ et montrons que x est inversible dans \mathbb{D} . Posons $y = \frac{\pm 10^k}{2^p 5^q}$. Il suffit de vérifier que y est élément de \mathbb{D} . Mais on peut aussi écrire

$$y = \frac{\pm 10^k 2^q 5^p}{2^{p+q} 5^{p+q}} = \frac{\pm 10^k 2^q 5^p}{10^{p+q}} \in \mathbb{D}.$$

Ainsi, les inversibles de $(\mathbb{D}, +, \times)$ sont les éléments $\frac{\pm 2^p 5^q}{10^k}$, avec $p, q, k \in \mathbb{N}$.

Exercice 18.

On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.
2. On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.
3. En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.

Correction.

1. Il suffit de prouver que c'est un sous-anneau de $(\mathbb{R}, +, \times)$. Mais $\mathbb{Z}[\sqrt{2}]$ est
— stable par la loi $+$: $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$.
— stable par la loi \times :

$$(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$$

— stable par passage à l'opposé $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}$.

De plus, $1 \in \mathbb{Z}[\sqrt{2}]$, ce qui achève la preuve du fait que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de \mathbb{R} .

2. Posons $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue à la question précédente, on a

$$\begin{aligned} N(xy) &= (aa' + 2bb')^2 - 2(ab' + a'b)^2 \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2. \end{aligned}$$

D'autre part,

$$\begin{aligned} N(x) \times N(y) &= (a^2 - 2b^2)(a'^2 - 2b'^2) \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2. \end{aligned}$$

3. Soit $x = a + b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y . Alors $N(xy) = N(1) = 1$, et donc $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on a nécessairement $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée :

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm(a - b\sqrt{2})$$

ce qui montre que $a + b\sqrt{2}$ est inversible, d'inverse $\pm(a - b\sqrt{2})$.

Exercice 19.

Soit A un anneau. On appelle caractéristique de A l'ordre de 1_A dans le groupe additif $(A, +)$. Dans la suite, on supposera que A est de caractéristique finie n .

1. Démontrer que, pour tout $x \in A$, $nx = 0$.
2. Démontrer que si A est intègre, n est un nombre premier.
3. Démontrer que si A est intègre et commutatif, alors $x \mapsto x^n$ est un morphisme d'anneaux.

Correction.

1. Il s'agit juste d'un jeu d'écriture! On écrit en effet :

$$nx = n(1_A x) = (n1_A)x = 0_A x = 0_A.$$

2. Raisonnons par contraposée. Supposons que $n = pq$ avec $1 < p, q < n$. Alors posons $x = p1_A$ et $y = q1_A$. Ni x ni y ne sont nuls puisque 1_A est d'ordre exactement n . Pourtant, leur produit $xy = (pq)1_A$ est nul et A n'est pas intègre. On vient de démontrer que si n n'est pas premier, alors A n'est pas intègre. Donc A intègre entraîne n premier.
3. On va noter $n = p$ pour souligner que n est un nombre premier, et $f(x) = x^p$. Il n'y a pas de difficultés à vérifier que $f(1_A) = 1_A$ et $f(xy) = f(x)f(y)$ (par la commutativité de A) pour tous $x, y \in A$. D'autre part, on a

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

D'après le résultat de la première question, il suffit de vérifier que $p \mid \binom{p}{k}$ pour tout $k = 1, \dots, p-1$. Mais on a

$$p! = \binom{p}{k} \times k! \times (p-k)!.$$

On a donc

$$p \mid \binom{p}{k} \times k! \times (p-k)!.$$

Mais comme p est premier et que les décompositions en produits de facteurs premiers de $k!$ et de $(p-k)!$ ne font intervenir que des nombres premiers strictement inférieurs à p , p est premier avec le produit $k! \times (p-k)!$. Ainsi, $p \mid \binom{p}{k}$, et on a bien $f(x + y) = f(x) + f(y)$. f est bien un morphisme d'anneaux.

Exercice 20.

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

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

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 21.

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 entraîne 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} .

3. Exercices d'approfondissement

a. Ordre d'un élément dans un groupe

Exercice 22.

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 multiple 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 $i = 1, \dots, r$, 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 $a_1 \dots a_r$ est bien d'ordre $\text{ppcm}(p, q)$.

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

Exercice 23.

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-vidé (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 24.

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,

$$G = \{e\} \cup H_1 \cup \dots \cup H_n$$

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. Anneaux, sous-anneaux, idéaux

Exercice 25.

Soit A un anneau intègre commutatif fini. Démontrer que A est un corps.

Correction.

Fixons $a \in A$ et considérons le morphisme d'anneaux $A \rightarrow A$, $x \mapsto ax$. Alors ce morphisme d'anneaux est injectif, car son noyau est réduit à $\{0_A\}$ puisque A est intègre. Puisque A est fini, ce morphisme est nécessairement bijectif, et donc il existe $x \in A$ tel que $ax = 1_A$. Par commutativité de A , on a aussi $xa = 1_A$ et donc a admet un inverse : A est un corps. Remarquons que l'on peut se passer de l'hypothèse que A est commutatif, par exemple en faisant le même raisonnement avec $x \mapsto xa$, et en prouvant que l'inverse à droite et l'inverse à gauche coïncident.

Exercice 26.

Soit E un ensemble fini et $A = \mathcal{P}(E)$.

1. Montrer que (A, Δ, \cap) est un anneau commutatif. Est-il intègre ?
2. Soit $E' \subset E$. Démontrer que $I = \mathcal{P}(E')$ est un idéal de A .
3. Réciproquement, soit I un idéal de A . Prouver que

$$\begin{cases} \forall X \in I, \forall Y \subset X, Y \in I \\ \forall X \in I, \forall Y \in I, X \cup Y \in I. \end{cases}$$

4. En déduire qu'il existe $E' \subset E$ tel que $I = \mathcal{P}(E')$.
5. Si E est infini, démontrer que l'ensemble des parties finies de E forme un idéal de A qui n'est pas de la forme $\mathcal{P}(E')$.

Correction.

1. Il faut vérifier la définition, car A n'apparaît pas comme un sous-anneau d'un anneau connu. On remarque d'abord que les lois Δ et \cap sont deux lois internes, commutatives et associatives (ce n'est pas si facile pour Δ et cela mérite une petite démonstration...). De plus, (A, Δ) est un groupe commutatif dont l'élément neutre est \emptyset et le symétrique de $X \in A$ est X . Enfin, la loi \cap est distributive par rapport à la loi Δ : si $X, Y, Z \in A$, alors soit $x \in (X \Delta Y) \cap Z$, ce qui signifie $x \in Z$ et ($x \in X \setminus Y$ ou $x \in Y \setminus X$). Si $x \in X$, alors $x \in X \cap Z$ et $x \notin Y$ d'où $x \notin Y \cap Z$, et de même, si $x \in Y$, alors $x \in Y \cap Z$ mais $x \notin X \cap Z$. On en déduit que $x \in (X \cap Z) \Delta (Y \cap Z)$. L'inclusion réciproque se prouve exactement de la même façon, en séparant le cas $x \in (X \cap Z) \setminus (Y \cap Z)$ du cas $x \in (Y \cap Z) \setminus (X \cap Z)$.
2. D'abord, $(\mathcal{P}(E'), \Delta)$ est bien un groupe commutatif (démonstration similaire à celle de la question précédente). Ensuite, si $X \in \mathcal{P}(E')$ et $Y \in A$, alors $X \cap Y \subset X \subset E'$ et donc $X \cap Y \in \mathcal{P}(E')$. C'est bien que $\mathcal{P}(E')$ est un idéal de A .
3. D'abord, si $X \in I$ et si $Y \subset X$, par définition d'un idéal, $Y \cap X$ est dans I . Mais $Y \cap X = Y$, et donc $Y \in I$. Prenons ensuite $X, Y \in I$ et posons $X_1 = X \setminus Y$. Alors X_1 et Y sont disjoints, et donc $X_1 \Delta Y = X_1 \cup Y = X \cup Y$. De plus, puisque I est un idéal et que $X_1 \in I$ par la première partie de cette question, on en déduit que $X_1 \Delta Y \in I$. I est alors stable par réunion.
4. Posons E' la réunion de tous les éléments qui sont dans I . Cette réunion est nécessairement

finie, et en effectuant une petite récurrence à partir de la question précédente, on démontre que $E' \in I$. Par la question précédente, il est clair que $\mathcal{P}(E') \subset I$. Mais, si $X \in I$, alors $X \subset E'$ par définition de E' et donc $X \in \mathcal{P}(E')$. Ainsi, $I = \mathcal{P}(E')$.

5. Il est très facile de vérifier que l'ensemble des parties finies forme un idéal de A . Il n'est pas de la forme $\mathcal{P}(E')$: si c'était le cas, prenons $x \in E$, et $X = \{x\}$. Alors X est élément de l'idéal et donc $X \in \mathcal{P}(E')$ soit $x \in E'$. On aurait donc $E = E'$, mais dans l'idéal on n'a pas pris les parties infinies de E et l'idéal est différent de $\mathcal{P}(E)$.

Exercice 27.

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

$$\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}, \quad \sqrt{\sqrt{I}} = \sqrt{I} \quad \text{et} \quad \sqrt{I^p} = \sqrt{I}.$$

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 entraîne $x^k y^{n+m-k} \in I$. 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. — Soit $x \in \sqrt{I \cdot J}$. Il existe $n \geq 1$ tel que $x^n \in I \cdot J$, 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 $I \cdot J \subset I \cap J$). 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 $x^{n+m} = x^n x^m \in I \cdot J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cdot J}$.
 - 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 $x \in \sqrt{I}$.
 - La dernière égalité se prouve de façon tout à fait identique !

3. Soit $x \in \mathbb{Z}$. x est dans $\sqrt{n}\mathbb{Z}$ 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 $\sqrt{k} = (p_1 \dots p_r)\mathbb{Z}$.