Université Chouaïb Doukkali
Faculté des Sciences- El Jadida.
Filière SMIA - Semestre 1 - A.U : 09-10
Module Algèbre I

EXERCICES CORRIGES

1. Enoncés

Exercice 1.

Soit E une partie non vide de $\mathbb{R}$. Pour $x, y \in E$, on pose

$$x * y = \frac{x + y + |x - y|}{2}$$

Montrer que $*$ définit une loi de composition interne sur E et étudier ses propriétés.

Exercice 2.

Sur $E = \mathbb{Q}^2$, on défini la loi $\perp$ par : $(a, b) \perp (a', b') = (aa', ba' + b')$. Citer les propriétés de cette loi. On étudiera en particulier les éléments symétrisables.

Exercice 3.

1 - Montrer que $\mathbb{Z}$ est un monoïde pour la loi $*$ définie par :

$$x * y = x + y - xy$$

2 - Trouver les éléments inversibles de $(\mathbb{Z}, *)$.

3 - Calculer pour la loi $*$, les puissances d'un élément $a \in \mathbb{Z}$.

Exercice 4.

Dire si les ensembles suivants sont des monoïdes pour la multiplication des entiers.

1 - $E = \{x = a^2 + b^2 \in \mathbb{N} : a, b \in \mathbb{N}\}$.

2 - $F = \{x = a^2 + b^2 + c^2 \in \mathbb{N} : a, b, c \in \mathbb{N}\}$.

Exercice 5.

Soit X un ensemble. On considère $(\mathcal{F}(X), \circ)$, le monoïde des applications de X dans lui-même. Soit $f \in \mathcal{F}(X)$. Montrer que :

1 - f est régulière à gauche $\Leftrightarrow$ f est injective $\Leftrightarrow$ f est inversible à gauche.

2 - f est régulière à droite $\Leftrightarrow$ f est surjective $\Leftrightarrow$ f est inversible à droite.

3 - f est bijective $\Leftrightarrow$ f est régulière $\Leftrightarrow$ f est inversible.

Exercice 6.

Soit E un monoïde d'élément neutre e.

1 - Montrer que tout élément inversible à gauche et régulier à droite est inversible.

2 - Donner un exemple d'un monoïde contenant un élément inversible à gauche non inversible à droite.

3 - Montrer que dans un monoïde fini tout élément régulier à gauche ou à droite est inversible.

Exercice 7.

Soit E lintervalle ouvert $]-1,1[$. Pour $x, y \in E$, on pose $x * y = \frac{x+y}{1+xy}$. Montrer que $*$ définit une l.c.i. sur E et que $(E, *)$ est un groupe abélien isomorphe à $(\mathbb{R}, +)$.

Exercice 8.

Soit n un entier ≥ 2. Pour tout $k \in \mathbb{Z}$, montrer que $\overline{k}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \cdot)$, si et seulement si, k est premier avec n.

Exercice 9.

On appelle application affine de $\mathbb{R}$, toute application de la forme $f_{a,b} : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$.

1 - Montrer que l'ensemble Aff($\mathbb{R}$), des applications affines est un monoïde pour la composition des applications.

2 - Soit $f_{a,b}$ une application affine. Montrer que $f_{a,b}$ est bijective, si et seulement si, $a \neq 0$. On a alors $f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$.

3 - Montrer que l'ensemble des bijections affines, GA($\mathbb{R}$), muni de la composition des applications est un groupe.

Exercice 10.

1 - Soit $(E, .)$ un ensemble fini muni d'une l.c.i associative pour laquelle tout élément est régulier. Montrer que $(E, \cdot)$ est un groupe.

2 - Le résultat précédent reste-il vrai si on suppose seulement que tout élément est régulier à gauche ?

Exercice 11.

Une table d'une l.c.i sur un ensemble fini E est dite carré latin si dans chaque ligne et dans chaque colonne, tout élément de E figure une et une seule fois.

Montrer que la table d'un groupe fini est un carré latin et étudier la réciproque.

Exercice 12.

Soit G un groupe, H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G, si et seulement si, $H \subset K$ ou $K \subset H$.

Exercice 13.

Montrer que les groupes $(\mathbb{Q}_+^*, \times)$ et $(\mathbb{Q}, +)$ ne sont pas isomorphes.

Exercice 14.

Soit $(G, \cdot)$ un groupe d'élément neutre e, H un sous-groupe de G. On définit la relation binaire $\mathcal{R}$ sur G de la façon suivante.

$$\forall x, y \in G : x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$$

1 - Montrer que $\mathcal{R}$ est une relation d'équivalence.

(On l'appellera dans la suite relation d'équivalence modulo H).

2 - Pour tout $a \in G$, on note $C(a)$ la classe d'équivalence de a modulo $\mathcal{R}$.

a - Montrer que pour tout $x \in H$, on a $xa \in C(a)$.

b - Soit l'application $\phi_a : H \to C(a)$, définie par $\phi_a(x) = xa$. Montrer que ϕ_a est une bijection.

3 - Dans la suite on suppose que G est fini, on note $o(G)$ son ordre et $o(H)$ celui de H. On se propose de montrer que l'ordre de H divise

l'ordre de G. (Ce résultat est appelé le théorème de Lagrange).

Soit $E = \{C_1, \ldots, C_k\}$, l'ensemble quotient pour la relation d'équivalence modulo H.

a - Montrer que toutes les classes d'équivalence modulo H ont le même cardinal égal à $o(H)$.

b - Justifier que $G = C_1 \cup \ldots \cup C_k$ et montrer que $o(G) = k.o(H)$.

Exercice 15.

1 - Dire si les ensembles suivants sont des sous-anneaux de $\mathbb{R}$.

$A = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\}$.

$B = \{a + b\sqrt[3]{2} \in \mathbb{R} : a, b \in \mathbb{Z}\}$.

2 - Montrer que $D = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$, où $i^2 = -1$, est un sous-anneau de $\mathbb{C}$. Trouver ses éléments inversibles.

Exercice 16.

Soit $\alpha \in \mathbb{R}$. Donner une condition nécessaire et suffisante sur α pour que l'ensemble $\{a + b\alpha \in \mathbb{R} : a, b \in \mathbb{Q}\}$, soit un sous-anneau de $\mathbb{R}$.

Exercice 17.

On appelle anneau de Boole un anneau A un anneau tel que $\forall x \in A$, on a : $x^2 = x$.

1 - Montrer qu'un anneau de Boole A vérifie $\forall x \in A$, on a : $x + x = 0$ et qu'il est commutatif.

2 - Montrer que si un anneau de Boole A contient au moins trois éléments, alors il n'est pas intègre.

Exercice 18.

Soit $(A, +, \cdot)$ un anneau commutatif. On désigne par 0, l'élément neutre de $(A, +)$ et par 1, l'élément neutre de $(A, \cdot)$. On dit que $a \in A$ est **nilpotent** s'il existe $k \in \mathbb{N}$ tel que $a^k = 0$.

1 - Montrer que si a et b sont nilpotents alors $a + b$ est nilpotent.

2 - Montrer que si a est nilpotent alors $1-a$ est inversible. Calculer alors son inverse.

Exercice 19.

Montrer que tout anneau fini sans diviseur de zéro est un corps.

Exercice 20.

Soit $\mathbb{H} = \{\begin{pmatrix} z & -\overline{z'} \\ z' & \overline{z} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})\}$. Montrer que $\mathbb{H}$ est un corps non commutatif pour les opérations usuelles sur les matrices.

($\mathbb{H}$ est appelé le corps des quaternions).

Exercice 21.

Dans tout cet exercice, on considère les ensembles $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Q}\}$ et $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Z}\}$

1 - Montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$ et que $\mathbb{Q}[\sqrt{2}]$ est son corps de fractions.

2 - Soit $\sigma : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]\,;\, a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Montrer que σ est un automorphisme du corps $\mathbb{Q}[\sqrt{2}]$.

3 - Pour tout $z = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, on pose $N(z) = |z\sigma(z)| = |a^2 - 2b^2|$ qu'on appelle norme de z. Montrer que $N(\mathbb{Q}[\sqrt{2}]) \subset \mathbb{Q}^+$ et que $N(zz') = N(z).N(z')$ pour tous $z, z' \in \mathbb{Q}[\sqrt{2}]$.

4 - Soit $z \in \mathbb{Z}[\sqrt{2}]$. Montrer z est inversible dans $\mathbb{Z}[\sqrt{2}]$, si et seulement si, $N(z) = 1$.

5 - Prouver que l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ est infini.

6 - Soit $z \in \mathbb{Q}[\sqrt{2}]$. Montrer qu'il existe $u \in \mathbb{Z}[\sqrt{2}]$, tel que $N(z-u) < 1$. (montrer d'abord que pour tout x dans $\mathbb{Q}$, il existe $s \in \mathbb{Z}$ tel que $|x - s| \leq \frac{1}{2}$).

7 - Montrer que, pour tous $z, u \in \mathbb{Z}[\sqrt{2}]$, avec $u \neq 0$, il existe $q, r \in \mathbb{Z}[\sqrt{2}]$, tels que $z = qu + r$ et $N(r) < N(q)$.

Exercice 22.

Montrer que pour tout $P \in \mathbb{K}[X]$ on a $P(X) - X$ divise $P(P(X)) - X$.

Exercice 23.

Pour quelles valeurs de $n \in \mathbb{N}^*$, le polynôme $(X^n+1)^n - X^n$ est-il divisible par X^2+X+1 ?

Exercice 24.

Factoriser le polynôme X^4+4 dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 25.

Soit α une racine de $P = X^4+X^3+X^2+X+1$. On pose $\beta = \alpha + \frac{1}{\alpha}$.

1 - Montrer que β est racine d'un polynôme du second degré de $\mathbb{Q}[X]$ que l'on déterminera.

2 - En déduire l'expression de β puis celles de $\cos\frac{2\pi}{5}$ et $\sin\frac{2\pi}{5}$ par radicaux.

Exercice 26.

Factoriser le polynôme $X^{n+2} - 2X^{n+1} + X^n - nX^2 + 2nX - n$ dans $\mathbb{C}[X]$, sachant qu'il possède 1 comme racine multiple.

Exercice 27.

1 - Soit $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$. Montrer que $x \in \mathbb{Z}$ est racine de P alors $a - x \mid P(a)$, pour tout $a \in \mathbb{Z}$. En particulier, montrer qu'on a $x \mid a_0$.

2 - Trouver les racines entières de $P = X^6 + X^5 - 3X^4 + 3X^3 - 16X^2 + 2X - 12$, puis factoriser ce polynôme.

Exercice 28.

Soit le polynôme $A(X) = X^6 - 3X^4 - 8X^3 - 9X^2 - 6X - 2 \in \mathbb{C}[X]$.

1 - Calculer $A(j)$ et $A'(j)$, où $j = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

2 - Factoriser A dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 29.

On considère le polynôme $B(X) = 2X^4 - 5X^3 + 4X^2 - 5X + 2$ dans $\mathbb{C}[X]$.

1 - Montrer que si $\alpha \in \mathbb{C}$ est une racine de B, alors $\alpha \neq 0$ et $\frac{1}{\alpha}$ est aussi racine de B.

2 - Montrer que B possède une racine entière que l'on déterminera.

(Utiliser le fait que si $a \in \mathbb{Z}$ est une racine de B, alors a divise $B(0)$).

3 - Factoriser B dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

Exercice 30.

Soit $P(X) = X^6 + X^3 + 1 \in \mathbb{C}[X]$. On pose $\xi = e^{\frac{2\pi i}{9}}$.

1 - Calculer $P(\xi)$ et déterminer toutes les racines de P.

2 - On pose $\theta = 2\cos\frac{2\pi}{9} = \xi + \xi^{-1}$.

a - Montrer que θ est racine d'un polynôme $Q(X)$ unitaire à coefficients entiers de degré 3 que l'on déterminera.

b - Calculer $Q(\frac{1}{1-\theta})$.

c - Exprimer les racines de Q en fonction de θ.

Exercice 31.

Soit $P \in \mathbb{C}[X]$.

1 - Montrer qu'il existe deux polynômes P_1 et P_2 dans $\mathbb{R}[X]$, tels que $P(X) = P_1(X) + iP_2(X)$.

2 - Soit $\alpha \in \mathbb{R}$. Montrer que α est racine de P, si et seulement si, α est racine de P_1 et de P_2.

3 - Soit $P = X^4 + 4X^3 + (6+i)X^2 + (5+3i)X + 2 + 2i \in \mathbb{C}[X]$. Vérifier que P possède des racines réelles et factoriser P.

Exercice 32.

1 - Factoriser le polynôme $X^4 + 4$ dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

2 - Soit $P = X^6 - 4X^5 + 6X^4 - 12X^2 + 16X - 8 \in \mathbb{C}[X]$.

a - Déterminer le quotient et le reste de la division euclidienne de P par $X^4 + 4$.

b - Montrer que P et $X^4 + 4$ possèdent deux racines communes que l'on déterminera.

c - Déterminer les multiplicités de ces racines communes dans P.

d - Factoriser P dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

2. Corrigés des Exercices

Corrigé de l'exercice 1.

Remarquons que si $x \geq y$, alors $x * y = x$ et si $x \leq y$, alors $x * y = y$. Par conséquent $x * y = \sup(x, y)$.

Commutativité. $\forall x, y \in E$, $x * y = \sup(x, y) = \sup(y, x) = y * x$. La loi $*$ est donc commutative.

Associativité. $\forall x, y, z \in E$, on a :$(x * y) * z = \sup(\sup(x, y), z) = \sup(x, y, z) = \sup(x, \sup(y, z)) = x * (y * z)$. La loi $*$ est donc associative.

Elément neutre. Pour que $*$ admette un élément neutre e, il faut que $x * e = x$, $\forall x \in E$, i.e. $x \geq e$ $\forall x \in E$. Ce qui veut dire que e doit être un plus petit élément de E. (Cette condition n'est pas toujours vérifiée c'est le cas par exemple pour $E = \mathbb{R}$.)

Eléments réguliers. Soit $a \in E$, alors a est régulier si $a * x = a * y \Rightarrow x = y$, $\forall x, y \in E$. En prenant $x < a$ et $y = a$, on a $a * x = a = a * a$, mais $x \neq a$. Donc dans ce cas là, a n'est pas régulier. Par conséquent, pour que a soit régulier, il faut que $a \leq x$, $\forall x \in E$, i.e. a doit être l'élément neutre de $*$.

Eléments symétrisables. On suppose que E possède un élément neutre e. Puisque $(E, *)$ est un monoïde, tout élément symétrisable est régulier. Comme e est le seul élément régulier de $(E, *)$, il en découle que e est le seul élément symétrisable.

Corrigé de l'exercice 2.

Associativité. Soient $(a, b), (a', b'), (a'', b'') \in E$. On a :

$((a, b) \perp (a', b')) \perp (a'', b'') = (aa', ba' + b') \perp (a'', b'') = (aa'a'', (ba' + b')a'' + b'') = (aa'a'', ba'a'' + b'a'' + b'')$.

$(a, b) \perp ((a', b') \perp (a'', b'')) = (a, b) \perp (a'a'', b'a''+b'') = (aa'a'', ba'a''+ b'a'' + b'')$.

Donc $((a, b) \perp (a', b')) \perp (a'', b'') = (a, b) \perp ((a', b') \perp (a'', b''))$, par conséquent, $\perp$ est associative.

Commutativité. On a $(a, b) \perp (a', b') = (aa', ba' + b')$ et $(a', b') \perp (a, b) = (a'a, b'a + b)$. Il est facile de voir que la loi $\perp$ n'est pas commutative. En effet, $(1, 1) \perp (0, 1) = (0, 1)$ alors que $(0.1) \perp (1, 1) = (0, 2)$.

Elément neutre. Soit $(e, e') \in E$ tel que $\forall (a, b) \in E$, on a : $(a, b) \perp (e, e') = (e, e') \perp (a, b) = (a, b)$. Alors $ae = ea = a$ et $be + e' = e'a + b = b$, $\forall a, b \in \mathbb{Q}$. Ainsi $e = 1$ et $e' = 0$. On vérifie ensuite que $(a, b) \perp (1, 0) = (1, 0) \perp (a, b) = (a, b)$. Donc $\perp$ possède un élément neutre qui est $(1, 0)$.

En conclusion $(E, \perp)$ est un monoïde non commutatif.

Eléments symétrisables. Soit $(a, b) \in E$ un élément symétrisable. Il existe alors $(a', b') \in E$ tel que $(a, b) \perp (a', b') = (a', b') \perp (a, b) = (1, 0)$. Par conséquent, $aa' = a'a = 1$ et $ba' + b' = b'a + b = 0$. Il en résulte que $a \neq 0$, $a' = a^{-1}$ et $b' = -b.a^{-1}$. Réciproquement, si $a \neq 0$, alors $(a, b) \perp (a^{-1}, -b.a^{-1}) = (a^{-1}, -b.a^{-1}) \perp (a, b) = (1, 0)$. En conclusion, (a, b) est symétrisable, si et seulement si, $a \neq 0$ et on a alors $(a, b)^{-1} = (a^{-1}, -b.a^{-1})$.

Eléments réguliers. Les éléments symétrisables sont réguliers. Réciproquement, si (a, b) n'est pas symétrisable, on a $a = 0$ et $(a, b) = (0, b)$. Par ailleurs $(0, b) \perp (1, -b) = (0, 0) = (0, b) \perp (0, 0)$, alors que $(1, -b) \neq (0, 0)$. Ce qui veut dire que $(0, b)$ n'est pas régulier. Donc dans ce monoïde, nous avons tout élément régulier est symétrisable.

Corrigé de l'exercice 3.

1 - *Associativité.* Soient $x, y, z \in \mathbb{Z}$, on a :
$(x * y) * z = (x + y - xy) * z = x + y - xy + z - xz - yz + xyz$ et
$x * (y * z) = x * (y + z - yz) = x + y + z - yz - xy - xz + xyz$. Donc $(x * y) * z = x * (y * z)$. $*$ est associative.

Commutativité. $\forall x, y \in \mathbb{Z}$, $x * y = x + y - xy = y + x - yx = y * x$. $*$ est commutative.

Elément neutre. Soit e tel que $x * e = x$, $\forall x \in \mathbb{Z}$. On a $x + e - ex = x$. Donc $ex = 0$, par suite $e = 0$. On vérifie alors que $x * 0 = 0 * x = x$. Ainsi 0 est l'élément neutre de $*$.

En conclusion, $(\mathbb{Z}, *)$ est un monoïde commutatif.

2 - Un élément x de $\mathbb{Z}$ est inversible pour $*$, s'il existe $x' \in \mathbb{Z}$ tel que $x * x' = x + x' - xx' = 0$. Ou encore, $1 - (1 - x)(1 - x') = 0$. Ce qui implique que $(1 - x)(1 - x') = 1$. Par conséquent $1 - x = 1$ ou $1 - x = -1$, $\Rightarrow x = 0$ ou $x = 2$. Les éléments inversibles de $(\mathbb{Z}, *)$ sont 0 et 2.

3 - En remarquant que $x * y = 1 - (1 - x)(1 - y)$, montrons par récurrence que $x^{*n} = 1 - (1 - x)^n$. C'est vrai pour $n = 0$, $x^{*0} = 0$. Supposons la propriété vraie pour n. On a $x^{*(n+1)} = x * x^{*n} = 1 - (1 - x)(1 - x)^n = 1 - (1 - x)^{n+1}$.

Corrigé de l'exercice 4.

1 - Soient $a, b, c, d \in \mathbb{N}$, on a : $(a^2+b^2)(c^2+d^2) = a^2c^2+a^2d^2+b^2c^2+b^2d^2 = a^2c^2+b^2d^2+2abcd+a^2d^2+b^2c^2-2abcd = (ac+bd)^2+(ad-bc)^2$.

On a $ac + bd, ad - bc \in \mathbb{N}$, donc $(a^2 + b^2)(c^2 + d^2) \in E$. E est stable par multiplication. Par ailleurs on a, $1 = 1^2 + 0^2$. Donc $1 \in E$. Puisque la multiplication des entiers est associative, $(E, .)$ est un monoïde.

2 - Nous allons montrer que F n'est pas stable par multiplication. On a $3 = 1^2 + 1^2 + 1^2$ et $5 = 2^2 + 1^2 + 0^2$. Donc 3 et 5 sont dans F. Montrons que $15 = 3.5$ n'est pas un élément de F. Sinon, $15 = a^2 + b^2 + c^2$. Nécessairement $a, b, c \leq 3$. D'autre part, un des entiers a, b, c est supérieur strictement à 2. Il en résulte qu'un des entiers, par exemple a, est égal à 3. On a alors $15 = 9 + b^2 + c^2$. Ce qui entraîne que $b^2 + c^2 = 6$. Ce qui est absurde. Donc $15 \notin F$.

Corrigé de l'exercice 5.

1 - *f régulière à gauche $\Rightarrow$ f injective.* Supposons que f est régulière à gauche, soient $y, y' \in X$ tels que $f(y) = f(y')$. Montrons que $y = y'$. Considérons les applications constantes $g, h \in \mathcal{F}(X)$, telles que $\forall x \in X,\ g(x) = y$ et $h(x) = y'$. On a $\forall x \in X.\ f \circ g(x) = f(g(x)) = f(y) = f(y') = f(h(x)) = f \circ h(x)$. Donc $f \circ g = f \circ h$. Comme f est régulière à gauche, $g = h$. Donc $y = y'$. f est injective.

f injective $\Rightarrow$ f inversible à gauche. Supposons que f est injective. Pour tout $y \in x$, $f^{-1}\{y\}$ est un singleton ou vide. Fixons $a \in X$ et définissons $g \in \mathcal{F}(X)$ par : $g(y) = x$ si $f^{-1}\{y\} = \{x\}$, $g(y) = a$, si $f^{-1}\{y\} = \varnothing$. Alors $\forall x \in X$, on a : $g \circ f(x) = x, \forall x \in X$. Donc $g \circ f = I_X$.

f inversible à gauche $\Rightarrow$ f régulière à gauche. Cette implication est vraie dans tout monoïde.

2 - *f régulière à droite $\Rightarrow$ f surjective.* Par contraposition, supposons que f ne soit pas surjective. Il existe $y \in X$ tel que $y \notin f(X)$. Soient $a, b \in X$, $a \neq b$. On considère $g, h \in \mathcal{F}(X)$ définies par : g est l'application constante $g(x) = a$, $\forall x \in X$, h est définie par $h(x) = a$ si $x \in f(X)$, $h(x) = b$ sinon. On a $g \circ f(x) = h \circ f(x) = a$, $\forall x \in X$, mais $g \neq h$. Donc f n'est pas régulière à droite.

f surjective $\Rightarrow$ *f inversible à droite.* Supposons que f est surjective. Alors $\forall y \in X$, on a $f^{-1}\{y\}$ est non vide. Les ensembles $f^{-1}\{y\}$ forment une partition de X, on "choisit" dans chaque $f^{-1}\{y\}$ un élément z. On définit ainsi une application par $z = g(y)$. Alors $f \circ g = I_X$.

L'implication *f inversible à droite* $\Rightarrow$ *f régulière à droite* est vraie dans tout monoïde.

3 - Les équivalences f est bijective $\Leftrightarrow$ f est régulière $\Leftrightarrow$ f est inversible, sont une conséquence de 2 et 3.

Corrigé de l'exercice 6.

1 - Soit $x \in E$ inversible à gauche et régulier à droite. Il existe $x' \in E$ tel que $x'x = e$. On a $(xx')x = x(x'x) = xe = x = ex$. Puisque x est régulier à droite, on a : $xx' = e$. Donc x est inversible.

2 - En utilisant l'exercice 5, il suffit de considérer $\mathcal{F}(X)$ avec X infini et une application injective non surjective. Par exemple $X = \mathbb{N}$ et $f : \mathbb{N} \to \mathbb{N}$, définie par $f(n) = n + 1$.

3 - On suppose que E est fini et $a \in E$ régulier à droite. Soit l'application $\rho_a : E \to E$, définie par $\rho_a(x) = xa$. Puisque a est régulier à droite, ρ_a est injective. Or E et fini, donc ρ_a est bijective. Il existe $a' \in E$ tel que : $a'a = e$. Donc a est inversible à gauche et régulier à droite. On applique alors 1.

Par la même méthode on démontre que régulier à gauche $\Rightarrow$ inversible.

Autre méthode. On considère l'application $\phi : \mathbb{N} \to E$ définie par $\phi(n) = a^n$. Puisque E et fini, ϕ ne peut pas être injective. Donc il existe $m > n$ tels que $a^n = a^m$. Donc, puisque a est régulier à gauche ou à droite, il en est de même de a^n. Donc $a^{m-n} = e$. Ou encore $a.a^{m-n-1} = a^{m-n-1}.a = e$. Donc a est inversible.

Corrigé de l'exercice 7.

$*$ *est une l.c.i.* D'abord si $x, y \in E$ on a $-1 < xy < 1$ et $0 < 1+xy < 2$. D'où $x+y+1+xy = (x+1)(y+1) > 0$. Donc $\frac{x+y}{1+xy} > -1$. De même $x+y-1-xy = (x-1)(1-y) < 0$. Donc $\frac{x+y}{1+xy} < 1$. D'où $x*y \in]-1, 1[$.

Associativité . Soient $x, y, z \in E$. On a :

$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{1+xy+xz+yz}$.

$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{1+yz+xy+xz}$.

Donc $(x * y) * z = x * (y * z)$. La loi $*$ est associative.

Commutativité. On a $x * y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y * x$, $\forall x, y \in E$.
Donc $*$ est commutative.

Elément neutre. On a $x * 0 = 0 * x = x$, donc 0 est l'élément neutre de la loi $*$.

Eléments symétrisables. Pour tout $x \in E$ on a $-x \in E$ et $x * (-x) = (-x) * x = 0$.

En conclusion, $(E, *)$ est un groupe abélien.

On cherche une application bijective $f : \mathbb{R} \to]-1, 1[$, telle que $f(x + y) = f(x) * f(y) = \frac{f(x)+f(y)}{1+f(x)f(y)}$. Une application qui répond à cette propriété est $\text{th}(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ (la tangente hyperbolique).

Corrigé de l'exercice 8.

$$\begin{aligned} \overline{k} \text{ est inversible dans } (\mathbb{Z}/n\mathbb{Z}, .) &\Leftrightarrow \text{ Il existe } \overline{m} \in \mathbb{Z}/n\mathbb{Z} : \overline{k}\overline{m} = \overline{1}, \\ &\Leftrightarrow \text{ Il existe } \overline{m} \in \mathbb{Z}/n\mathbb{Z} : n | km - 1 \\ &\Leftrightarrow \text{ il existe } \alpha \in \mathbb{Z} : km - 1 = \alpha n \\ &\Leftrightarrow n \text{ et } k \text{ sont premiers entre eux} \end{aligned}$$

Corrigé de l'exercice 9.

1 - On a $I = f_{1,0}$ est une application affine. Si $f_{a,b}, f_{c,d}$ sont des applications affines, on a : $\forall x \in \mathbb{R}$, $f_{a,b} \circ f_{c,d}(x) = a(cx + d) + b = acx + ad + b = f_{ac,ad+b}(x)$. Donc $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. $\text{Aff}(\mathbb{R})$ est donc stable par La loi $\circ$ et contient I. La loi $\circ$ étant associative, $(\text{Aff}(\mathbb{R}), \circ)$ est un monoïde.

2 - Soit $f_{a,b}$ une application affine. Si $a \neq 0$, on a, d'après 1, $f_{a,b} \circ f_{a^{-1},-a^{-1}b} = f_{a^{-1},-a^{-1}b} \circ f_{a,b} = f_{1,0} = I$, donc $f_{a,b}$ est inversible.

Réciproquement, si $a = 0$, on a $f_{0,b}(0) = f_{0,b}(1) = b$, donc $f_{0,b}$ n'est pas bijective.

3 - Puisque la réciproque d'une bijection affine est une bijection affine, $\text{GA}(\mathbb{R})$ est le groupe des éléments inversibles du monoïde $\text{Aff}(\mathbb{R})$.

Corrigé de l'exercice 10.

1 - Nous allons montrer que $(E, \cdot)$ possède un élément neutre. Soit $a \in E$ fixé. On considère les applications $\lambda_a, \rho_a : E \to E$, définies par

$\lambda_a(x) = ax$ et $\rho_a(x) = xa$. Puisque a est régulier , λ_a et ρ_a sont injectives. Comme E est fini, elles sont bijectives. Donc $\exists e \in E$ tel que $ae = \lambda_a(e) = a$. Soit $x \in E$. Comme ρ_a est bijective, il existe $x' \in E$ tel que $x = x'a$. On a $xe = (x'a)e = x'(ae) = x'a = x$. De même on a $a(ex) = (ae)x = ax$, donc par régularité de a on a $ex = x$. Par conséquent, $(E, \cdot)$ possède un élément neutre e.

$(E, \cdot)$ est un monoïde fini dans lequel tout élément est régulier, on utilise alors l'exercice 6 question 3, pour conclure que tout élément de E et inversible. Donc $(E, \cdot)$ est un groupe.

2 - Soit E un ensemble fini de cardinal ≥ 2. on définit sur E la loi $*$ par $x * y = y$. $*$ est associative et tout élément de e est régulier à gauche car $a * x = a * y \Rightarrow x = y$. Mais $(E, *)$ n'est pas un groupe (il ne possède pas d'élément neutre).

Corrigé de l'exercice 11.

Une table d'une l.c.i $*$ est un carré latin $\Leftrightarrow$, tout élément est régulier pour $*$. Ceci est vraie pour un groupe. la réciproque est fausse, il suffit de considérer la table :

$\curvearrowright *$	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

Ce n'est pas la table d'un groupe, l'associativité est en défaut car $a(bc) = aa = b$, mais $(ab)c = ac = c$.

Corrigé de l'exercice 12.

Montrons que, si $H \cup K$ est un sous-groupe, alors $H \subset K$ ou $K \subset H$. Par contraposition. Si $H \not\subseteq K$ et $K \not\subseteq H$. Il existe $x \in H$ $x \notin K$ et $y \in K$, $y \notin H$. Montrons que $xy^{-1} \notin H \cup K$. Sinon, $xy^{-1} \in H$ ou $xy^{-1} \in K$. Si $xy^{-1} \in H$ on a $x^{-1}xy^{-1} \in H$, ce qui entraîne $y^{-1} \in H$. Absurde. De même, $xy^{-1} \in K$ entraîne $x = xy^{-1}y \in K$ c'est encore une absurdité. Donc $xy^{-1} \notin H \cup K$. Par suite $H \cup K$ n'est pas un groupe.

La réciproque est évidente.

Corrigé de l'exercice 13.

Supposons qu'il existe un isomorphisme $f : (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$. Il existe $\alpha \in \mathbb{Q}$, tel que $f(\alpha) = 2$. On a $2 = f(\alpha) = f(\frac{\alpha}{2} + \frac{\alpha}{2}) = f(\frac{\alpha}{2})^2$. Posons $\beta = f(\frac{\alpha}{2})$, alors $\beta \in \mathbb{Q}$, et $\beta^2 = 2$, ce qui est absurde.

Corrigé de l'exercice 14.

1 - Réflexivité : On a $\forall x \in G$, $xx^{-1} = e \in H$, donc $x\mathcal{R}x$. $\mathcal{R}$ est donc réflexive.

Symétrie : Soient $x, y \in G$ tels que $x\mathcal{R}y$. On a $xy^{-1} \in H$. Donc $yx^{-1} = (xy^{-1})^{-1} \in H$, car H est un sous-groupe. Donc $y\mathcal{R}x$. Par suite, $\mathcal{R}$ est symétrique.

Transitivité : Soient $x, y, z \in G$, tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $xy^{-1} \in H$ et $yz^{-1} \in H$. Donc $xz^{-1} = xy^{-1}yz^{-1} \in H$. Toujours du fait que H est un sous-groupe. $\mathcal{R}$ est donc transitive.

En conclusion, $\mathcal{R}$ est une relation d'équivalence.

2 - a. Soit $x \in H$, on a $(xa)a^{-1} = a \in H$. Donc $xa\mathcal{R}a$. D'où $xa \in C(a)$.

b - Montrons que ϕ_a est bijective.

Injection : soient $x, y \in H : \phi_a(x) = \phi_a(y)$. On a $xa = ya$. Or dans un groupe tout élément est régulier. Donc $x = y$. Par suite ϕ_a est injective.

Surjection : soit $y \in C(a)$. Posons $x = ya^{-1}$. Puisque $y\mathcal{R}a$, on a $x \in H$ et $y = xa = \phi_a(x)$. Donc ϕ_a est surjective.

En conclusion, ϕ_a est bijective.

2 - a. Soit $i \in \{1, \ldots, k\}$ et $a \in C_i$. Puisque ϕ_a est une bijection de H dans $C(a) = C_i$, on a $\text{card}C_i = o(H)$.

b - On a $C_1 \cup \ldots \cup C_k \subset G$ et tout élément de G est contenu dans une classe d'équivalence. Donc $G = C_1 \cup \ldots \cup C_k$. D'autre part les classes d'équivalence sont deux à deux disjointes, donc $o(G) = \sum_{i=1}^{k} \text{card}C_i$. Or pour tout $i = 1, \ldots, k$, on a $\text{card}C_i = o(H)$, par conséquent $o(G) = k.o(H)$.

Corrigé de l'exercice 15.

1 - On a $1 \in A$. Soient $a + b\sqrt{2}, a' + b'\sqrt{2} \in A$, alors :

$(a+b\sqrt{2})-(a'+b'\sqrt{2}) = (a-a')+(b-b')\sqrt{2} \in A$, car $(a-a'), (b-b') \in \mathbb{Z}$.

$(a+b\sqrt{2})(a'+b'\sqrt{2}) = (aa'+2bb')+(ab'+ba')\sqrt{2} \in A$, car $aa'+2bb', ab'+ba' \in \mathbb{Z}$.

En conclusion, A est un sous-anneau de $\mathbb{R}$.

Nous allons montrer que B n'est pas un sous-anneau. Plus précisément que $(\sqrt[3]{2})^2 = \sqrt[3]{4} \notin B$. Supposons que $\sqrt[3]{4} = a+b\sqrt[3]{2} \in B$. On multiplie par $\sqrt[3]{2}$ on obtient $\sqrt[3]{8} = 2 = a\sqrt[3]{2}+b\sqrt[3]{4}$. Donc, $a\sqrt[3]{2}+b\sqrt[3]{4} = a\sqrt[3]{2}+b(a+b\sqrt[3]{2}) = ab+(a+b^2)\sqrt[3]{2} = 2$.

- Si $a+b^2 = 0$, on a $-b^3 = 2$, ce qui est impossible.

- Si $a+b^2 \neq 0$, alors $\sqrt[3]{2} = \frac{2-ab}{a+b^2} \in \mathbb{Q}$, ce qui est encore impossible.

En conséquence, $(\sqrt[3]{2})^2 \notin B$. B n'est pas un sous-anneau de $\mathbb{R}$.

2 - On a $1 \in D$. Soient $a+bi, a'+b'i \in D$, alors :

$(a+bi)-(a'+b'i) = (a-a')+(b-b')i \in D$, car $(a-a'),(b-b') \in \mathbb{Z}$.

$(a+b\sqrt{2})(a'+b'i) = (aa'-bb')+(ab'+ba')i \in D$, car $aa'-bb', (ab'+ba') \in \mathbb{Z}$.

D est donc un sous-anneau de $\mathbb{C}$.

Soit $z = a+bi \in D$ un élément inversible. Il existe $z' = c+di \in D$ tel que $zz' = 1$. En prenant les modules, on obtient $\mid zz' \mid^2 = \mid z \mid^2 \mid z' \mid^2 = 1$. Par conséquent $(a^2+b^2)(c^2+d^2) = 1$. Il en résulte que $a^2+b^2 = 1$. D'où $(a,b) = (0,1),(1,0),(0,-1)$ ou $(-1,0)$. Les éléments inversibles sont donc $1, -1, i$ et $-i$.

Corrigé de l'exercice 16.

Soit $A = \{a+b\alpha \in \mathbb{R} : a,b \in \mathbb{Q}\}$.

On a $1 \in A$ et il est clair que A est toujours un sous-groupe de $(\mathbb{R},+)$.
Supposons que A soit un sous-anneau de $\mathbb{R}$, alors $\forall a,b,a',b' \in \mathbb{Q}$, on a : $(a+b\alpha)(a'+b'\alpha) = aa'+(ab'+ba')\alpha+bb'\alpha^2 \in A$, ce qui entraîne $\alpha^2 \in A$. i.e $\alpha^2 = c\alpha+d$, avec $c,d \in \mathbb{Q}$.

Cette condition est aussi suffisante, car si $\alpha^2 = c\alpha+d$, on a $(a+b\alpha)(a'+b'\alpha) = aa'+(ab'+ba')\alpha+bb'\alpha^2 \in A$

Corrigé de l'exercice 17.

1 - $(x+1)^2 = x+1 = x^2+x+x+1 = x+x+x+1$, ce qui implique $x+x=0$, i.e. $-x=x$.

D'autre part, $x+y=(x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y$, ce qui entraîne $xy+yx=0$. Mais $yx=-yx$, donc $yx=xy$. A est commutatif.

2 - Soient $x \neq 0, 1$. On a $x(x+1) = x+x = 0$, mais $x \neq 0$ et $x+1 \neq 0$. A n'est pas intègre.

Corrigé de l'exercice 18.

1 - Soient $a, b \in A$ nilpotents. Il existe $k, m \in \mathbb{N}$ tels que $a^k = b^m = 0$. D'après la formule du binôme, qui s'applique puisque A est commutatif, on a :

$$\begin{array}{rcl}(a+b)^{k+m} & = & \sum_{i=0}^{k+m} C_{k+m}^i a^i b^{k+m-i} \\ & = & \sum_{i=0}^{k} C_{k+m}^i a^i b^{k+m-i} + \sum_{i=k+1}^{k+m} C_{k+m}^i a^i b^{k+m-i} \\ & = & b^m \sum_{i=0}^{k} C_{k+m}^i a^i b^{k-i} + a^k \sum_{i=k+1}^{k+m} C_{k+m}^i a^{i-k} b^{k+m-i}\end{array}$$

Donc : $(a+b)^{k+m} = 0$

En conclusion on a $(a+b)^{k+m} = 0$, d'où $a+b$ est nilpotent.

2 - Soit $a \in A$, On a $(1-a)(1+a+a^2+\ldots+a^{k-1}) = 1-a^k$. Donc si $a^k = 0$, $(1-a)(1+a+a^2+\ldots+a^{k-1}) = 1$. Ce qui entraîne que $(1-a)$ est inversible et que $(1-a)^{-1} = (1+a+a^2+\ldots+a^{k-1})$.

Corrigé de l'exercice 19.

Un élément qui n'est pas diviseur de zéro est régulier dans $(A, \cdot)$. Soient $x, y \in A^*$. Puisque A est sans diviseurs de zéro, on a $xy \in A^*$. Donc $(A^*, \cdot)$ est un monoïde fini dans lequel tout élément est régulier. $(A^*, \cdot)$ est donc un groupe.

Corrigé de l'exercice 20.

Montrons que $\mathbb{H}$ est un sous-anneau de $\in \mathcal{M}_2(\mathbb{C})\}$.

On a $I_2 \in \mathbb{H}$. Soient $\begin{pmatrix} z & -\overline{z'} \\ z' & \overline{z} \end{pmatrix}, \begin{pmatrix} u & -\overline{v'} \\ v' & \overline{u} \end{pmatrix} \in \mathbb{H}$. On a :

$\begin{pmatrix} z & -\overline{z'} \\ z' & \overline{z} \end{pmatrix} - \begin{pmatrix} u & -\overline{u'} \\ u' & \overline{u} \end{pmatrix} = \begin{pmatrix} z-u & -(\overline{z'-u'}) \\ z'-u' & \overline{z-u} \end{pmatrix} \in \mathbb{H}$.

$\begin{pmatrix} z & -\overline{z'} \\ z' & \overline{z} \end{pmatrix} \cdot \begin{pmatrix} u & -\overline{u'} \\ u' & \overline{u} \end{pmatrix} = \begin{pmatrix} zu-\overline{z'}u' & -(z\overline{u'}+\overline{z'u}) \\ z'u+\overline{z}u' & -z'\overline{u'}+\overline{zu} \end{pmatrix} = \begin{pmatrix} v & -\overline{v'} \\ v' & \overline{v} \end{pmatrix} \in \mathbb{H}$, où $v = zu - \overline{z'}u'$ et $v' = z'u + \overline{z}u'$.

Par conséquent, $(\mathbb{H}, +, \cdot)$ est un anneau.

Montrons que$(\mathbb{H}, +, \cdot)$ est un corps. Soit $M = \begin{pmatrix} z & -\overline{z'} \\ z' & \overline{z} \end{pmatrix} \neq 0$. Donc z ou $z' \neq 0$. Posons $z = a + bi$ et $z' = c + di$, avec $a, b, c, d \in \mathbb{R}$ non tous nuls. On a $\det M = z\overline{z} + z'\overline{z'} = |z|^2 + |z'|^2 = a^2 + b^2 + c^2 + d^2 \neq 0$. Donc M est inversible.

Il reste à montrer que $M^{-1} \in \mathbb{H}$. On a $M^{-1} = (\det M)^{-1}.{}^t\mathrm{Com}(M)$. Posons $\alpha = \det(M)^{-1}$. On a $\alpha \in \mathbb{R}$ et $M^{-1} = \begin{pmatrix} \overline{\alpha z} & -\alpha\overline{z'} \\ \alpha z' & \alpha z \end{pmatrix} \in \mathbb{H}$.

$(\mathbb{H}, +, \cdot)$ n'est pas commutatif, il suffit de prendre :

$M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $M' = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. On a $MM' = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$, $M'M = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$.

On a bien $MM' \neq M'M$.

Corrigé de l'exercice 21.

1 - On a $1 \in \mathbb{Z}[\sqrt{2}]$. Soient $a + b\sqrt{2}, a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, alors :

$(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, car $(a - a'), (b - b') \in \mathbb{Z}$.

$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + ba')\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, car $aa' + 2bb', ab' + ba' \in \mathbb{Z}$.

En conclusion, $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

En général, si A est un anneau intègre contenu dans un corps, alors l'ensemble $F = \{\frac{a}{b} \in K : a \in A, b \in A^*\}$, est un sous-corps de K et c'est un corps de fractions de A.

Soient $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}], c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, alors :

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 + 2d^2} \in \mathbb{Q}[\sqrt{2}]$$

Réciproquement, tout élément $\frac{a}{b} + \frac{c}{d}\sqrt{2}$, de $\mathbb{Q}[\sqrt{2}]$ s'écrit, $\frac{(ad+bc)\sqrt{2}}{bd}$, c'est donc un quotient de deux éléments de $\mathbb{Z}[\sqrt{2}]$. Par conséquent, $\mathbb{Q}[\sqrt{2}] = \{\frac{x}{y} \in \mathbb{R} : x \in \mathbb{Z}[\sqrt{2}], y \in \mathbb{Z}[\sqrt{2}]^*\}$. C'est donc le corps de fraction de $\mathbb{Z}[\sqrt{2}]$.

2 - $\sigma : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]\,;\, a+b\sqrt{2} \mapsto a-b\sqrt{2}$.

Soient $x = a+b\sqrt{2}, y = a'+b'\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. On a :

$\sigma(x+y) = \sigma((a+a')+(b+b')\sqrt{2}) = a+a'-(b+b')\sqrt{2} = a-b\sqrt{2}+a'-b'\sqrt{2} = \sigma(x)+\sigma(y)$.

$\sigma(xy) = \sigma((aa'+2bb'))+(ab'+ba')\sqrt{2} = (aa'+2bb')-(ab'+ba')\sqrt{2} = (a-b\sqrt{2})(a'-b'\sqrt{2}) = \sigma(x)\sigma(y)$.

σ est un morphisme de corps, donc nécessairement injectif. Il est aussi surjectif car $\forall x = a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, on a $\sigma(a-b\sqrt{2}) = x$.

Finalement, σ est un automorphisme.

3 - Pour tout $z = a+b\sqrt{2}, \in \mathbb{Q}[\sqrt{2}]$, il est clair que $N(\mathbb{Q}[\sqrt{2}]) \subset \mathbb{Q}^+$. Par ailleurs, $N(zz') = |zz'\sigma(zz')| = |zz'\sigma(z')\sigma(z') = |z\sigma(z).z'\sigma(z')| = |z\sigma(z)|.|z'\sigma(z')| = N(z)N(z')$.

4 - Soit $z \in \mathbb{Z}[\sqrt{2}]$. z est inversible dans $\mathbb{Z}[\sqrt{2}]$, si et seulement si, il existe $z' \in \mathbb{Z}[\sqrt{2}] : zz' = 1$. Ce qui entraîne que $N(zz') = N(z)N(z') = 1$. Comme $z, z' \in \mathbb{Z}[\sqrt{2}]$, on a $N(z), N(z') \in \mathbb{N}$. Ce qui entraîne que $N(z) = 1$.

Réciproquement, supposons que $N(z) = 1$, on a $z = a+b\sqrt{2}$, et $a^2-2b^2 = \pm 1$. Posons $z' = a-b\sqrt{2}$, alors $zz' = \pm 1$, ce qui entraîne que z est inversible.

5 - L'élément $z = 1+\sqrt{2}$ est inversible car $N(z) = -1$. On a $\forall n \in \mathbb{N}, z^n$ est aussi inversible. D'autre part, $z^n \neq z^m$, $\forall n \neq m$, sinon $z^{n-m} = 1$, ce qui implique, puisque $z \in \mathbb{R}$, que $z = \pm 1$ ce qui est absurde. Donc l'ensemble $\{z^n : n \in \mathbb{N}\}$ est infini.

6 - Soit $x \in \mathbb{Q}$. Notons $E(x)$, la partie entière de x. Posons $\phi(x) = E(x)$, si $x \in [E(x), E(x)+\frac{1}{2}[$ et $\phi(x) = E(x)+1$, si $x \in [E(x)+\frac{1}{2}, E(x)+1[$. On a toujours $|x-\phi(x)| \leq \frac{1}{2}$.

Pour $z = x+y\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, posons $u = \phi(x)+\phi(y)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. On a $N(z-u) = |(x-\phi(x))^2-2(y-\phi(y))^2| \leq |\frac{1}{4}-\frac{1}{2}| < 1$.

7 - Soient $z, u \in \mathbb{Z}[\sqrt{2}]$, avec $u \neq 0$. On a $\frac{z}{u} \in \mathbb{Q}[\sqrt{2}]$, donc, d'après 6, il existe $q \in \mathbb{Z}[\sqrt{2}]$, tel que $N(\frac{z}{u}-q) < 1$. Posons $r = z-qu$, alors $z = qu+r$, et $N(\frac{z-qu}{u}) = N(\frac{r}{u}) < 1$. Ce qui entraîne que $N(r) < N(q)$.

Corrigé de l'exercice 22.

Posons $P = \sum_{k=0}^{n} a_k X^k$. On a $P(P(X)) - X = P(P(X)) - P(X) + P(X) - X$. Il suffit donc de montrer que $P(X) - X$ divise $P(P(X)) - P(X)$.

On a $P(P(X)) - P(X) = \sum_{k=0}^{n} a_k P^k - \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} a_k (P^k - X^k)$. Comme $P - X$ divise $P^k - X^k$ pour tout $k \in \mathbb{N}$, on a alors $P(X) - X$ divise $P(P(X)) - P(X)$.

Corrigé de l'exercice 23.

Les racines de X^2+X+1 sont $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et $\bar{j}$. Donc $X^2+X+1 = (X-j)(X-\bar{j})$. Posons $P = (X^n+1)^n - X^n$. Pour que P soit divisible par $X^2 + X + 1$, il faut et il suffit que $P(j) = P(\bar{j}) = 0$. Comme P est à coefficient réels, on a $P(j) = 0 \Rightarrow P(\bar{j}) = 0$. Donc il suffit d'avoir $P(j) = 0$.

Notons d'abord que $j^{3k+r} = (j^3)^k \cdot j^r = j^r$, pour $r = 0, 1, 2$.

• Si $n = 3k$, $P(j) = (j^{3k} + 1)^{3k} - j^{3k} = 2^{3k} - j^{3k} \neq 0$.

• Si $n = 3k+1$, $P(j) = (j^{3k+1} + 1)^{3k+1} - j^{3k+1} = (j+1)^{3k+1} - j$
$P(j) = (-j^2)^{3k+1} - j = (-1)^{3k+1} j^{6k+2} - j = (-1)^{3k+1} j^2 - j \neq 0$.

• Si $n = 3k+2$, $P(j) = (-j)^{3k+2} - j^2 = (-1)^{3k+2} j^{3k+2} - j^2 = (-1)^{3k} j^2 - j^2 = ((-1)^k - 1) j^2$
Il en résulte que dans ce cas $P(j) = 0 \Leftrightarrow k$ est pair.

Finalement P est divisible par $X^2 + X + 1$, si et seulement si, $n = 6k + 2$.

Corrigé de l'exercice 24.

On a $X^4 + 4 = X^4 + 4X^2 + 4 - 4X^2 = (X^2 + 2)^2 - 4X^2 = (X^2 - 2X^2 + 2)(X^2 + 2X^2 + 2)$.

Les polynômes $(X^2 - 2X^2 + 2)$ et $(X^2 + 2X^2 + 2)$ sont irréductibles dans $\mathbb{R}[X]$ car le descriminant $2^2 - 4.2 = -4 < 0$. Donc $X^4 + 4 = (X^2 - 2X^2 + 2)(X^2 + 2X^2 + 2)$, est la factorisation dans $\mathbb{R}[X]$.

Les racines de $(X^2 - 2X^2 + 2)$ sont $1 + i = \alpha$ et $\bar{\alpha}$.

Les racines de $(X^2 + 2X^2 + 2)$ sont $-\alpha$ et $-\bar{\alpha}$.

Donc la factorisation dans $\mathbb{C}[X]$ est :

$$X^4+4=(X-\alpha)(X-\bar{\alpha})(X+\alpha)(X+\bar{\alpha})$$

Corrigé de l'exercice 25.

1 - On a $\beta=\alpha+\frac{1}{\alpha}=\frac{\alpha^2+1}{\alpha}=\frac{\alpha^3+\alpha}{\alpha^2}$, et $\beta^2=\alpha^2+\frac{1}{\alpha^2}+2=\frac{\alpha^4+2\alpha^2+1}{\alpha^2}$, d'où $\beta^2+\beta=1$

2 - Soit $\alpha=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$, alors α est racine de $X^5-1=(X-1)(X^4+X^3+X^2+X+1)$. Comme $\alpha\neq 1$, on a α est racine de $X^4+X^3+X^2+X+1$. Il en résulte que $2\cos\frac{2\pi}{5}=\alpha+\frac{1}{\alpha}$ est racine de X^2+X-1. Donc $2\cos\frac{2\pi}{5}=\frac{-1\pm\sqrt{5}}{2}$. Comme $0<\frac{2\pi}{5}<\frac{\pi}{2}$, on a $\cos\frac{2\pi}{5}>0$ et $\cos\frac{2\pi}{5}>0$. Donc $\cos\frac{2\pi}{5}=\frac{-1+\sqrt{5}}{4}$ et $\sin\frac{2\pi}{5}=\sqrt{1-\cos^2\frac{2\pi}{5}}=\frac{\sqrt{10+2\sqrt{5}}}{4}$

Corrigé de l'exercice 26.

Posons $P=X^{n+2}-2X^{n+1}+X^n-nX^2+2nX-n$. On a $P(1)=1-2+1-n+2n-n=0$.

$P'=(n+2)X^{n+1}-2(n+1)X^n+nX^{n-1}-2nX+2n$; $P'(1)=n+2-2(n+1)+n-2n+2n=0$

$P''=(n+1)(n+2)X^n-2(n+1)nX^{n-1}+n(n-1)X^{n-2}-2n$
$P''(1)=(n+1)(n+2)-2(n+1)n+n(n-1)-2n=n^2+3n+2-2n^2-2n+n^2-n-2n=2-2n$

Si $n=1$, alors $P''(1)=0$ et $P=(X-1)^3$.

Si $n>1$, alors $P''(1)\neq 0$. Donc 1 est racine double de P. La division euclidienne de P par $(X-1)^2$, donne $P=(X-1)^2(X^n-n)$
Les racines (X^n-n) sont $\sqrt[n]{n}\xi_k$, où les ξ_k sont les racines n-èmes de l'unité, pour $k=0,\ldots,n-1$.

Corrigé de l'exercice 27.

1 - On a $P(X)-P(a)=\sum_{k=0}^{n}a_k(X^k-a^k)$. Comme $X^k-a^k=(X-a)(X^{k-1}+aX^{k-2}+\ldots+a^{k-2}X+a^{k-1})$, il est clair que $X-a$ divise $P(X)-P(a)$ dans $\mathbb{Z}[X]$. D'où il existe $Q\in\mathbb{Z}[X]$ tel que $P(X)-P(a)=(X-a)Q$. Donc, si $x\in\mathbb{Z}$ est racine de P, alors $-P(a)=(x-a)Q(a)$. D'où $x-a$ divise $P(a)$. En particulier, pour $a=0$, x divise $P(0)=a_0$.

2 - Si P possède des racines entières, alors elles divisent 12. Donc appartiennent à l'ensemble $\{1,-1,2,-2,3,-3,4,-4,6,-6,12,-12\}$.

On vérifie que 2 et -3 sont racines de P. Ainsi P est divisible par $(X-2)(X+3) = X^2+X-6$. La division euclidienne de P par X^2+X-6 donne $P = (X^2+X-6)(X^4+3X^2+2)$

Par ailleurs, on a $X^4+3X^2+2 = (X^2+1)(X^2+2)$, d'où les factorisations :

$P = (X-2)(X+3)(X-i)(X+i)(X-i\sqrt{2})(X+i\sqrt{2})$ dans $\mathbb{C}[X]$.

$P = (X-2)(X+3)(X^2+1)(X^2+2)$ dans $\mathbb{R}[X]$.

Corrigé de l'exercice 28.

1 - $A(j) = j^6-3j^4-8j^3-9j^2-6j-2 = 1-3j-8-9j^2-6j-2 = -9-9j-9j^2 = 0$.

$A'(X) = 6X^5-12X^3-24X^2-18X-6$ et $A'(j) = 6j^2-12-24j^2-18j-6 = -18j^2-18j-18 = 0$.

2 - Il en résulte que j est une racine au moins double de A. Comme A est un polynôme réel, $\bar{j}$ est aussi racine au moins double. Par conséquent, A est divisible par $(X-j)^2(X-\bar{j})^2 = ((X-j)(X-\bar{j}))^2 = (X^2+X+1)^2$.

La division euclidienne de A par $(X^2+X+1)^2$ donne
$A = (X^2+X+1)^2(X^2-2X-2)$

Les racines de X^2-2X-2 sont $\alpha_1 = 1+\sqrt{3}$ et $\alpha_2 = 1-\sqrt{3}$ et sont réelles.

En conclusion A se factorise de la manière suivante :

$A = (X-j)^2(X-\bar{j})^2(X-\alpha_1)(X-\alpha_2)$ dans $\mathbb{C}[X]$.

$A = (X^2+X+1)^2(X-\alpha_1)(X-\alpha_2)$ dans $\mathbb{R}[X]$.

Corrigé de l'exercice 29.

1 - Soit $\alpha \in \mathbb{C}$ une racine de B. Puisque $B(0) = 2 \neq 0$, on a $\alpha \neq 0$. Calculons $B(\frac{1}{\alpha})$. On a $B(\frac{1}{\alpha}) = 2\frac{1}{\alpha^4} - 5\frac{1}{\alpha^3} + 4\frac{1}{\alpha^2} - 5\frac{1}{\alpha} + 2 = \frac{1}{\alpha^4}(2-5\alpha+4\alpha^2-5\alpha^3+2\alpha^4) = \frac{1}{\alpha^4}B(\alpha) = 0$.

2 - Si α est une racine entière alors α divise $B(0) = 2$. (voir exercice 6). Donc $\alpha \in \{1,-1,2,-2\}$. On vérifie que $B(2) = 32-40+16-10+2 = 0$.

3 - On a 2 est racine de B et d'après 2, $\frac{1}{2}$ est aussi racine de B. Il en découle que B est divisible par $(X-2)(X-\frac{1}{2})$, donc aussi par $2(X-2)(X-\frac{1}{2}) = 2X^2-5X+2$. La division euclidienne donne $B = (2X^2-5X+2)(X^2+1)$. On obtient les factorisations :

$B = 2(X-2)(X-\frac{1}{2})(X-i)(X+i)$ dans $\mathbb{C}[X]$.

$B = 2(X-2)(X-\frac{1}{2})(X^2+1)$ dans $\mathbb{R}[X]$.

Corrigé de l'exercice 30.

1 - $P(X) = X^6+X^3+1 \in \mathbb{C}[X]$ et $\xi = e^{\frac{2\pi i}{9}}$.

On a $P(\xi) = \xi^6+\xi^3+1 = e^{\frac{4\pi i}{3}} + e^{\frac{2\pi i}{3}} + 1 = j^2+j+1 = 0$

Soit $\alpha \in \mathbb{C}$ une racine de P. On a $\alpha^6+\alpha^3+1=0$. Posons $\beta = \alpha^3$, alors $\beta^2+\beta+1=0$. Donc $\beta = j$ ou $\beta = \bar{j}$, où $j = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$. Donc $\alpha^3 = j$ ou $\alpha^3 = \bar{j}$.

On obtient $\alpha = e^{\frac{2i\pi}{9}+\frac{2ki\pi}{3}}$, $k=0,1,2$, ou $\alpha = e^{\frac{4i\pi}{9}+\frac{2ki\pi}{3}}$, $k=0,1,2$

Finalement les 6 racines de P sont : $\xi = e^{\frac{2i\pi}{9}}$, $e^{\frac{8i\pi}{9}}$, $e^{\frac{14i\pi}{9}}$, et leurs conjugués.

2 - a- Posons $\theta = 2\cos\frac{2\pi}{9} = \xi+\xi^{-1}$. On a :

$\theta^3 = \xi^3+3\xi+3\xi^{-1}+\xi^{-3} = \xi^{-3}(\xi^6+3\xi^4+3\xi^2+1)$.

$\theta = \xi^{-3}(\xi^4+\xi^2)$.

Donc $\theta^3-3\theta = \xi^{-3}(\xi^6+1) = -1$. Donc si on pose $Q = X^3-3X+1$, alors $Q(\theta)=0$.

b - $Q(\frac{1}{1-\theta}) = (\frac{1}{1-\theta})^3 - 3\frac{1}{1-\theta}+1 = (\frac{1}{1-\theta})^3(1-3(1-\theta)^2+(1-\theta)^3) = (\frac{1}{1-\theta})^3(1-3-3\theta^2+6\theta+1-3\theta+3\theta^2-\theta^3) = (\frac{1}{1-\theta})^3(-1+3\theta-\theta^3) = 0$.

c - D'après b, $\frac{1}{1-\theta}$ est aussi racine de Q. On a $\frac{1}{1-\theta} \neq \theta$, sinon, $\theta^2-\theta+1=0$, ce qui absurde car θ est un nombre réel. Donc θ et $\frac{1}{1-\theta}$ sont deux racines distinctes. Soit u la troisième racine de Q, on a $Q = (X-\theta)(X-\frac{1}{1-\theta})(X-u)$. On a $Q(0) = 1 = \frac{\theta}{1-\theta}u$, d'où $u = \frac{1-\theta}{\theta}$

Corrigé de l'exercice 31.

1 - Soit $P = \sum_{k=0}^{n}(a_k + b_k i)X^k \in \mathbb{C}[X]$, avec $a_k, b_k \in \mathbb{R}$. Posons $P_1 = \sum_{k=0}^{n} a_k X^k$ et $P_2 = \sum_{k=0}^{n} b_k X^k$, alors $P(X) = P_1(X) + iP_2(X)$.

2 - Soit $\alpha \in \mathbb{R}$ racine de P. Alors $0 = P(\alpha) = P_1(\alpha)+iP_2(\alpha)$. Puisque $P_1(\alpha)$ et $P_2(\alpha)$ sont des nombres réels, on a $P_1(\alpha) = P_2(\alpha) = 0$.

3 - $P = X^4+4X^3+6X^2+5X+2+i(X^2+3X+2) = P_1(X)+iP_2(X)$. Si $\alpha \in \mathbb{R}$ est racine de P, on a $\alpha^2 + 3\alpha + 2 = 0$. Donc $\alpha \in \{-1, -2\}$. On vérifie que $P_1(-1) = P_1(-2) = 0$. Donc -1 et -2 sont racines de P. La division euclidienne de P par $X^2 + 3X + 2$ donne $P = (X^2 + 3X + 2)(X^2 + X + 1 + i)$.

Le discriminant du polynôme $X^2+X+1+i$ est égal à $\Delta = 1-4-4i = -3-4i$. On cherche d'abord les racines carrées de Δ. Soit $u = a+ib \in \mathbb{C}$ $a, b \in \mathbb{R}$, tel que $u^2 = \Delta$. Alors $a^2 - b^2 + 2abi = -3 - 4i$. D'autre part on a $\mid u \mid^2 = a^2 + b^2 = \mid \Delta \mid = \sqrt{3^2 + 4^2} = 5$. Donc $a^2 = 1$ et $b^2 = 4$ et $ab < 0$. Ce qui donne $a = 1$ et $b = -2$ ou $a = -1$ et $b = 2$. Les racines du polynôme $X^2+X+1+i$ sont donc $-i$ et $i-1$. D'où la factorisation

$$P = (X + 1)(X + 2)(X + i)(X + 1 - i)$$

Corrigé de l'exercice 32.

1 - Factorisons le polynôme $X^4 + 4$ dans $\mathbb{R}[X]$.

On a $X^4 + 4 = X^4 + 4X^2 + 4 - 4X^2 = (X^2 + 2)^2 - 4X^2 = (X^2 - 2X^2 + 2)(X^2 + 2X^2 + 2)$.

Les polynômes $(X^2 - 2X^2 + 2)$ et $(X^2 + 2X^2 + 2)$ sont irréductibles dans $\mathbb{R}[X]$ car le descriminant $2^2 - 4.2 = -4 < 0$. Donc la factorisation dans $\mathbb{R}[X]$ est :

$$X^4 + 4 = (X^2 - 2X^2 + 2)(X^2 + 2X^2 + 2)$$

Factorisons le polynôme $X^4 + 4$ dans $\mathbb{C}[X]$.

Les racines de $(X^2 - 2X^2 + 2)$ sont $1 + i = \alpha$ et $\bar{\alpha}$.

Les racines de $(X^2 + 2X^2 + 2)$ sont $-\alpha$ et $-\bar{\alpha}$.

Donc la factorisation dans $\mathbb{C}[X]$ est :

$$X^4 + 4 = (X - \alpha)(X - \bar{\alpha})(X + \alpha)(X + \bar{\alpha})$$

2 - a. Soit Q le quotient et R le reste de la division euclidienne de P par X^4+4. Le calcul donne : $Q = X^2-4X+6$ et $R = -16X^2+32X-32$.

b - Puisque $P = Q \cdot (X^4+4) + R$, si $z \in \mathbb{C}$ est une racine commune de P et X^4+4, alors $R(z) = P(z) - Q \cdot (z^4+4) = 0$. Donc z est aussi racine de $R = -16(X^2-2X+2)$. i. e $z = \alpha = 1+i$ ou $z = \bar{\alpha}$. Or d'après la question 1, le polynôme X^2-2X+2 divise X^4+4. Donc X^2-2X+2 divise $Q \cdot (X^4+4)+R = P$. D'où α et $\bar{\alpha}$ sont aussi racines de P.

c - On $P' = 6X^5-20X^4+24X^3-24X+16$ et $P'(\alpha) = 6(-4-4i)+80+24(-2+2i)-24(1+i)+16 = 0$.

$P'' = 30X^4-80X^3+72X^2-24$. et $P''(\alpha) = -120-80(-2+2i)+72.2i-24 = 16+16i \neq 0$

En conclusion, α et $\bar{\alpha}$ sont deux racines doubles de P.

d - Puisque α et $\bar{\alpha}$ sont deux racines doubles de P. On a :

$(X-\alpha)^2(X-\bar{\alpha})^2 = [(X-\alpha)(X-\bar{\alpha})]^2 = (X^2-2X+2)^2 = X^4-4X^3+8X^2-8X+4$ divise P. Le quotient de la division euclidienne de P par $(X^2-2X+2)^2$ est X^2-2. On obtient alors les factorisations :

Dans $\mathbb{C}[X]$, $P = (X-\alpha)^2(X-\bar{\alpha})^2(X-\sqrt{2})(X+\sqrt{2})$.

Dans $\mathbb{R}[X]$, $P = (X^2-2X+2)^2(X-\sqrt{2})(X+\sqrt{2})$.