Autres structures

I — Anneaux, corps et algèbre

1) Généralités

a) Définitions et caractérisation

Définition d'un anneau *(1)*

Un anneau est un ensemble A muni de deux lois de composition internes telles que :
(1) : *la première loi, notée $+$ est une loi de groupe commutatif (on note 0_A son élément neutre),*
(2) : *la seconde loi, notée généralement $\times$ ou $\circ$ est associative, admet un élément neutre (noté 1_A), et doit être distributive sur la première loi ($a \times (b+c) = a \times b + a \times c$).*

Exemples et contre-exemples *(2)*

(1) : $(\mathbb{Z}, +, \times)$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $\mathbb{R}$, $\mathbb{C}$ *sont des anneaux commutatifs*
(2) : *L'ensemble des fonctions $(\mathcal{F}(E, A) = A^E, +, \times)$ pour A anneau (commutatif) est un anneau (commutatif).*
(3) : *En particulier, l'ensemble $\mathcal{S}_{\mathbb{K}}$ des suites à valeurs dans $\mathbb{K}$ est un anneau commutatif.*
(4) : *Anneau des polynômes $(A[X], +, \times)$ et pour A anneau.*
(5) : *Anneau des fractions rationnelles $(\mathbb{K}(X), +, \times)$ pour un corps quelconque $\mathbb{K}$.*
(6) : *Anneau NON commutatif des matrices $(\mathcal{M}_n(\mathbb{K}), +, \times)$.*
(7) : *Anneau NON commutatif des endomorphismes d'un espace vectoriel $(\mathcal{L}(E), +, \circ)$.*

Anneau produit *(3)*

(1) (Dm) : *Soit $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. Le triplet $(A \times B, +, \times)$*
où $(a_1, b_1) + (a_2, b_2) = (a_1 +_A a_2, b_1 +_B b_2)$ et $(a_1, b_1) \times (a_2, b_2) = (a_1 \times_A a_2, b_1 \times_B b_2)$ est un anneau.
(2) (Dm) : *Par récurrence, tout produit cartésien d'un nombre fini d'anneaux est un anneau.*

Définition d'un sous-anneau *(4)*

(1) : *Soit A un anneau et $A' \subset A$. On dit que A' est un sous-anneau de A si et seulement si*
$\star$ *$(A', +)$ est un sous-groupe de $(A, +)$,*
$\star$ *A' est stable par la seconde loi.*
$\star$ $1_A \in A'$
(2) (Dm) : *Un sous-anneau est un anneau.*

Exemples *(5)*

(1) : *Si $\mathbb{Z}[i] = \{a + ib | (a, b) \in \mathbb{Z}^2\}$, alors $(\mathbb{Z}[i], +, \times)$ est un sous-anneau commutatif de $(\mathbb{C}, +, \times)$.*
(2) : *L'ensemble des suites réelles convergentes est un sous anneau de $\mathcal{S}_{\mathbb{R}}$.*
(3) : *L'ensemble des homothéties de E est un sous anneau commutatif de $(\mathcal{L}(E), +, \circ)$.*
(4) : *A est un sous anneau de A.*
(5) : *Si $A \neq \{0_A\}$, le singleton $\{0_A\}$ N'est PAS un sous anneau.*
(6) : *$(2\mathbb{Z}, +, \times)$ N'est PAS un sous anneau de $(\mathbb{Z}, +, \times)$, bien que stable par somme et produit.*

Définitions de corps et sous-corps *(6)*

On appelle corps tout anneau $\mathbb{K}$ non réduit à $\{0_\mathbb{K}\}$ dans lequel tout élément non nul est inversible.
Un sous-corps de $\mathbb{K}$ est un sous-anneau de $\mathbb{K}$ qui est un corps.

Exemples : *(7)*

$(\mathbb{Q},+,\times)$ est un sous corps de $(\mathbb{R},+,\times)$ qui est un sous corps de $(\mathbb{C},+,\times)$ qui est un corps.

Définition d'une algèbre : *(8)*

Soit $\mathbb{K}$ un corps. Une $\mathbb{K}$-algèbre est un ensemble A muni de deux lois internes $+$ et $\times$ et d'une loi externe $\cdot$ (de $\mathbb{K}\times A$ dans A) telles que :
- *le triplet $(A,+,\times)$ est un anneau*
- *le triplet $(A,+,\cdot)$ est un $\mathbb{K}$-espace vectoriel*
- *propriété d'associativité mixte : $\lambda\cdot(x\times y)=(\lambda\cdot x)\times y=x\times(\lambda\cdot y)$ pour tout $\lambda\in\mathbb{K}$, $(x,y)\in A^2$.*

Exemples *(9)*

(1) : *$(\mathbb{K}[X],+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.*
(2) : *$(\mathcal{L}(E),+,\circ,\cdot)$ est une $\mathbb{K}$-algèbre si E est un $\mathbb{K}$-ev.*
(3) : *$(\mathcal{M}_n(\mathbb{K}),+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.*

2) Morphismes.

Définitions : morphismes d'anneaux et d'algèbres *(10)*

(1) : *Un morphisme d'anneaux est une application $f:A\to B$ telle que*
- *$\forall(a,a')\in A^2, f(a+a')=f(a)+f(a')$ et $f(aa')=f(a)f(a')$*
- *$f(1_A)=1_B$ (à ne pas oublier !)*

Remarque : le transport du zéro n'est pas à vérifier, il résulte du transport de l'addition.
(2) : *Un morphisme d'algèbre transporte en plus la multiplication externe. Un morphisme d'algèbre est donc un morphisme d'anneaux ET une application linéaire.*

Propriétés : *(11)*

(1) : *L'image directe et l'image réciproque d'un sous-anneau par un morphisme d'anneaux est un anneau.*
(2) : *L'image directe et l'image réciproque d'une sous-algèbre par un morphisme d'algèbre est une sous algèbre.*
(3) : *La composée de deux morphismes d'anneaux est un morphisme d'anneau.*
(4) : *La réciproque d'un isomorphisme est un (iso)morphisme d'anneaux.*

Exemples et contre-exemples : *(12)*

(1) : *la conjugaison dans $\mathbb{C}$ est un morphisme d'anneaux.*
(2) : *la projection $\phi:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ définie par $\phi(k)=k\text{mod}n$ est un morphisme d'anneaux.*
(3) : *l'application $k\mapsto k\cdot 1$ de $\mathbb{Z}$ dans A est un morphisme d'anneaux.*
(4) : *si $P\in GL_n(\mathbb{K})$, $\phi_P:M\mapsto PMP^{-1}$ est un automorphisme de l'anneau des matrices $M_n(\mathbb{K})$ mais aussi de l'algèbre des matrices.*
(5) : *L'application nulle N'est PAS en général un morphisme d'anneaux même si les deux opérations sont préservées.*
(6) : *De même pour l'application $n\mapsto\begin{pmatrix}n&0\\0&0\end{pmatrix}$.*
(7) : *Soit $A\in M_n(\mathbb{K})$. L'application $\phi_A:\mathbb{K}[X]\to M_n(\mathbb{K})$ définie par $\phi(P)=P(A)$ est un morphisme d'algèbres*

Théorème : automorphismes des corps $\mathbb{Q},\mathbb{R},\mathbb{C}$: *(13)*

(1) : *$\mathbb{Q}$ et $\mathbb{R}$ admettent* id *comme seul automorphisme de corps.*
(2) : *$\mathbb{C}$ admet une infinité d'automorphismes (admis) mais* id *et $z\mapsto\bar{z}$ sont les seuls automorphismes du corps $\mathbb{C}$ conservant $\mathbb{R}$.*

Attention : *(14)*

On définit le noyau d'un morphisme d'anneaux $f : A \to B$ par $kerf = \{x \in A | f(x) = 0_B\}$.
Le noyau d'un morphisme d'anneau N'est PAS en général un sous anneau.
Le noyau d'un morphisme d'algèbre est un sous espace vectoriel.

3) Intégrité

Diviseur de zéro / Anneau intègre / Division *(15)*

Soit A un anneau et $a \in A \setminus \{0_A\}$.
(1) : *On dit que a est un diviseur de zéro s'il existe $b \in A \setminus \{0_A\}$ tel que $ab = 0_A$ ou $ba = 0_A$.*
(2) : *Un anneau non réduit à $\{0_A\}$, commutatif et sans diviseur de zéro est un anneau intègre.*
(3) : **Si A un anneau intègre** *et $(x, y) \in A^2$, on dit que x divise y s'il existe $a \in A$ tel que $y = ax$.*
Notation : *$x|y$.*

Exemple *(16)*

(1) : *L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.*
(2) : *L'anneau $\mathbb{Z}/10\mathbb{Z}$ n'est pas intègre car 2 et 5 sont diviseurs de zéro.*
(3) : *L'anneau $(\mathcal{M}_2(\mathbb{R}), +, \times)$ n'est pas intègre car $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro.*
(4) : *Un corps est un anneau intègre. Un produit de facteurs y est nul ssi l'un au moins des facteurs est nul.*

4) Calculs dans un anneau

a) Dans un anneau quelconque

Calcul élémentaire *(17)*

Soit A un anneau et $x, y, z \in A$. Les règles de calculs suivantes sont valides :
(1) : *$0_A x = x 0_A = 0$ (on dit que 0_A est un élément absorbant),*
(2) : *$x(-y) = (-x)y = -(xy)$ (règle des signes),*
(3) : *$x(y - z) = xy - xz$ et $(y - z)x = yx - zx$.*
Notation : *Soit A un anneau et $(x_i)_{i \in [\![1 , n]\!]} \in A^n$. La somme $x_1 + \cdots + x_n$ peut se noter $\sum_{i=1}^{n} x_i$. Par commutativité, on peut aussi écrire, $\sum_{1 \leqslant i \leqslant n} x_i$ ou $\sum_{i \in [\![1 , n]\!]} x_i$. De manière générale, si I désigne un ensemble* **fini** *d'indices, on pourra utiliser la notation $\sum_{i \in I} x_i$.*

Régles pour les sommes finies *(18)*

On considère des éléments d'un anneau A et des ensembles I et J finis d'indices. Alors :
(1) : *$\sum_{i \in I}(x_i + y_i) = (\sum_{i \in I} x_i) + (\sum_{i \in I} y_i)$,*
(2) : *si $(I_k)_{k \in K}$ désigne une partition de I, alors $\sum_{i \in I} x_i = \sum_{k \in K} \left(\sum_{i \in I_k} x_i \right)$,*
(3) : *$\sum_{i \in I} \left(\sum_{j \in J} x_{i,j} \right) = \sum_{j \in J} \left(\sum_{i \in I} x_{i,j} \right)$, ce qu'on notera $\sum_{(i,j) \in I \times J} x_{i,j}$,*
(4) : *$\left(\sum_{i \in I} x_i \right) \left(\sum_{j \in J} y_j \right) = \sum_{i \in I} \left(x_i \left(\sum_{j \in J} y_j \right) \right) = \sum_{i \in I} \left(\sum_{j \in J} (x_i y_j) \right) = \sum_{(i,j) \in I \times J} (x_i y_j)$.*

Produits finis *(19)*

Dans un anneau commutatif, les produits **finis** *peuvent se noter à l'aide du symbole Π, avec les mêmes règles de fonctionnement que celles relatives au symbole Σ dans le cas des additions finies.*

Identités remarquables *(20)*

Soient $(a, b) \in A^2$ et $n \in \mathbb{N}$.
(1) : *$1 - a^{n+1} = (1 - a) \sum_{i=0}^{n} a^i$. De plus, si $1 - a$ est inversible, alors $\sum_{i=0}^{n} a^i = (1 - a)^{-1}(1 - a^{n+1})$.*
(2) : *Si $ab = ba$, alors pour tout entier naturel n, $a^{n+1} - b^{n+1} = (a - b) \sum_{k=0}^{n} a^k b^{n-k}$.*
(3) : *Si $ab = ba$, $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.*

II — Arithmétique dans un anneau principal

1) Idéaux et divisibilité dans un anneau commutatif

Définition *(21)*

Soit A un anneau. I est un idéal de A ssi :
(1) : $(I, +)$ *est un sous-groupe (additif)*
(2) : $\forall a \in A, \forall i \in I, a \times i \in I$ *(absorbant pour la multiplication).*

Propriété *(22)*

Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ

Exemples *(23)*

(1) : $(a) = aA$ *(idéal monogène engendré par a),*
(2) : $(I \cup J) = I + J$,
(3) : *Un idéal contenant l'unité ou un inversible est égal à A.*

Définition : divisibilité *(24)*

(1) : *Lorsque A est intègre, on dit que a divise b et on note $a|b$ ssi $\exists\, c \in A$ tel que $b = ac$*
(2) : *Traduction en termes d'idéaux : $a|b \Longleftrightarrow b \in (a) \Longleftrightarrow (b) \subset (a)$.*
(3) : *Si $a \neq 0$, il y a unicité de c qui est alors noté b/a.*
(4) : *La notion de divisibiliité est réflexive et transitive mais pas antisymétrique en général !*

Exemples *(25)*

Dans $\mathbb{Z}$, dans $\mathbb{K}[X]$.

Définition : éléments associés *(26)*

(1) : *a et b sont dits associés lorsqu'ils engendrent le même idéal, c'est à dire $a \mid b$ et $b \mid a$.*
(2) : *Si A est intègre, a et b sont associés si et seulement s'il existe $u \in A^*$ tel que $b = ua$.*
(3) : *Pour $A = \mathbb{Z}$, a et b sont associés si et seulement si $b = \pm a$.*
(4) : *Pour $A = \mathbb{K}[X]$, a et b sont associés si et seulement s'ils sont proportionnels.*
(5) : *Tout polynôme non nul est associé à un unique polynôme unitaire.*

Théorèmes *(27)*

(1) : *Les idéaux de $\mathbb{Z}$ sont exactement ses sous-groupes additifs, soit les ensembles $(n) = \langle n \rangle = n\mathbb{Z}$, $n \in \mathbb{N}$.*
(2) : *Les idéaux de $\mathbb{K}[X]$ sont les idéaux monogènes, soit les ensembles (P) avec $P = 0$ ou P unitaire, entièrement déterminé par l'idéal considéré.*

III — Arithmétique modulaire

1) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème-Définition *(28)*

Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Théorème : éléments inversibles, réguliers, générateurs *(29)*

Pour $x \in \mathbb{Z}$, on a
$x \bmod n$ *est inversible* $\Longleftrightarrow$ $x \bmod n$ *est régulier* $\Longleftrightarrow$ $x \bmod n$ *engendre* $(\mathbb{Z}/n\mathbb{Z}, +) \Longleftrightarrow x \wedge n = 1$.

Conséquences *(30)*

(1) : $(\mathbb{Z}/n\mathbb{Z})^* = \{x \bmod n \text{ tel que } x \wedge n = 1\}$ *est un groupe multiplicatif de cardinal* $\varphi(n)$.
(2) : *Pour* $n \geqslant 2$, $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si* n *est premier. Dans le cas contraire, c'est un anneau non intègre.*
(3) : *Pour* $x \in \mathbb{Z}$ *et* $x \wedge n = 1$, *on a* $x^{\varphi(n)} \equiv 1\ [n]$ *(Théorème d'*Euler*).*
(4) : *Pour* $x \in \mathbb{Z}$ *et* n *premier, on a* $x^n \equiv x \bmod n$ *(Petit théorème de* Fermat*).*

Test de primalité de Fermat **:** *(31)*

Commençons par remarquer qu'il existe des entiers composés tels que pour tout $x \in \mathbb{Z}$, $x^n = x \bmod n$. *Par exemple* $561 = 3 \times 11 \times 17$ *est un tel entier. Ces nombres sont appelés nombre de Carmichaël et forment un ensemble infini.*
Malgré tout, si n *est composé, alors* x^n *est très peu probablement congru à* x *modulo* n. *Étant donné un (grand) entier* n *choisi au hasard - par exemple par un ordinateur - on examine les valeurs* $2^{n-1}, 3^{n-1}, 5^{n-1}$ *et* 7^{n-1} *modulo* n. *Si ces quatre valeurs sont égales à 1, on peut prétendre que* n *est probablement premier.*

Théorème chinois, version anneaux : *(32)*

Soient $(n, p) \in (\mathbb{N}^*)^2$ *tels que* $n \wedge p = 1$.
L'application $(x \bmod np) \mapsto (x \bmod n, x \bmod p)$ *est bien définie et est un isomorphisme entre les anneaux* $\mathbb{Z}/np\mathbb{Z}$ *et* $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. *Elle induit un isomorphisme entre les groupes multiplicatifs* $(\mathbb{Z}/np\mathbb{Z})^*$ *et* $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$.
En particulier $\varphi(np) = \varphi(n)\varphi(p)$.

Conséquence : *(33)*

Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *avec* $p_1, \dots, p_k$ *premiers positifs distincts et* $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$.
Alors $\varphi(n) = p_1^{\alpha_1 - 1} \dots p_k^{\alpha_k - 1}(p_1 - 1) \dots (p_k - 1)$, *soit* $\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

Cryptage RSA : *(34)*

Soient $n \in \mathbb{N}^*$ *sans facteur carré et* $d, e \in \mathbb{N}^*$ *tels que* $de \equiv 1 \bmod \varphi(n)$. *Alors les applications* $x \mapsto x^d$ *et* $x \mapsto x^e$ *sont deux permutations de* $\mathbb{Z}/n\mathbb{Z}$ *réciproques.*

IV — Exercices TD

Exercice 1 : Groupe des inversibles d'un anneau

Soit $(A, +, \cdot)$ *un anneau. L'ensemble des éléments de* A *inversibles (i.e. symétrisables par la multiplication) forme un groupe multiplicatif, appelé groupe des éléments inversibles de* A *ou encore groupe des unités de* A.
Notation : A^* *ou parfois* $\mathcal{U}(A)$.

Exercice 2 : Morphisme stabilisant $\mathbb{R}$

Soit $f : \mathbb{C} \to \mathbb{C}$ *un morphisme d'anneaux tel que*

$$\forall x \in \mathbb{R}, f(x) = x$$

Montrer que f *est l'identité ou la conjugaison complexe.*

Exercice 3 :

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

Exercice 4 : Théorème : idéal engendré

(1) : *L'intersection d'une famille d'idéaux est un idéal.*
(2) : *L'intersection de tous les idéaux contenant une partie X est le plus petit idéal contenant X, noté (X). C'est l'ensemble des combinaisons linéaires finies à coefficients dans A des éléments de X.*

Exercice 5 : Idéaux triviaux

Soit A un anneau commutatif non nul dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps.

Exercice 6 : Idéaux premiers

Un idéal I d'un anneau A est dit premier si : $\forall (x,y) \in A^2$, $xy \in I \Rightarrow x \in I$ ou $y \in I$.
(1) : *Quels sont les idéaux premiers de $\mathbb{Z}$?*
(2) : *Montrer que si A est commutatif non nul et si tous les idéaux de A sont premiers alors A est un corps.*

Exercice 7 : Thm de Gauss

Soit A un anneau commutatif et $(a,b) \in A^2$. On dit que a divise b si $b \in aA$ et a est premier à b si $aA + bA = A$. Montrer que si a est premier à b et a divise bc, alors a divise c.

Exercice 8 : Congruences

Résoudre les systèmes suivants :

1. $\begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 2 \bmod 7 \end{cases}$

2. $\begin{cases} 3x \equiv 2 \bmod 5 \\ 5x \equiv 1 \bmod 6 \end{cases}$

3. $3x + 5 = 0$ *dans* $\mathbb{Z}/10\mathbb{Z}$

4. $x^2 = 1$ *dans* $\mathbb{Z}/8\mathbb{Z}$

5. $x^2 + 2x + 2 = 0$ *dans* $\mathbb{Z}/5\mathbb{Z}$.

Exercice 9 : Indicatrice d'Euler

(1) : *Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$?*
(2) : *Montrer que pour tout entier $n \geqslant 3$, $\varphi(n)$ est un nombre pair.*

Exercice 10 : Eléments nilpotents

Soit A un anneau commutatif, et $a \in A$. On dit que a est nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.
(1) : *Exemple : Déterminer les éléments nilpotents de $\mathbb{Z}/36\mathbb{Z}$.*
(2) : *Montrer que l'ensemble des éléments nilpotents est un idéal de A.*
(3) : *Soit a nilpotent. Montrer que $1 - a$ est inversible.*
(4) : *Soient a nilpotent et b inversible. Montrer que $a + b$ est inversible.*

Exercice 11 : Radical d'un idéal

Soit A un anneau commutatif et I un idéal de A.
On note $\sqrt{I} = \{x \in A$ tel que $\exists n \in \mathbb{N}$ tel que $x^n \in I\}$ (radical de I).
(1) : *Montrer que $\sqrt{I}$ est un idéal de A.*
(2) : *Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.*
(3) : *Montrer que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I + J} \supset \sqrt{I} + \sqrt{J}$.*

(4) : *Exemple : $A = \mathbb{Z}$, $I = 3648\mathbb{Z}$. Trouver $\sqrt{I}$.*

Exercice 12 : Produit de deux idéaux

Soit A un anneau commutatif et I, J deux idéaux de A. On note $IJ = \{a_1 b_1 + \cdots + a_n b_n$ tel que $a_i \in I, b_i \in J\}$.
(1) : *Montrer que IJ est un idéal de A.*
(2) : *Montrer que $I(J + K) = IJ + IK$.*
(3) : *On suppose $I + J = A$. Montrer que $IJ = I \cap J$.*
(4) : *Pour $A = \mathbb{Z}$, $I = n\mathbb{Z}$, $J = p\mathbb{Z}$, qu'est-ce que IJ ?*

Exercice 13 : Fonctions trigonométriques

Soit $A = \{f \ : \ \mathbb{R} \to \mathbb{R}$ *de la forme* $f(x) = a_0 + \sum_{k=1}^{n} a_k \cos(kx),\ n \in \mathbb{N},\ a_i \in \mathbb{R}\}$.
(1) : *Montrer que* A *est un sous-anneau de* $\mathbb{R}^{\mathbb{R}}$.
(2) : *Soit* $f \in A$. *Calculer* $\int_{t=0}^{2\pi} f(t)\cos(nt)\,\mathrm{d}t$ *en fonction des* a_k.

(3) : *En déduire que* A *est intègre.*

(4) : *Soit* $\Phi : \begin{cases} \mathbb{R}[X] & \longrightarrow & A \\ P & \longmapsto & x \mapsto P(\cos x). \end{cases}$ *Montrer que* Φ *est un isomorphisme d'anneaux. En déduire que* A *est principal.*

Exercice 14 : Endomorphismes d'un groupe commutatif

Soit G *un groupe additif et* $A = \{$*morphismes* $G \to G\}$.
(1) : *Montrer que* $(A, +, \circ)$ *est un anneau.*
(2) : *On prend* $G = \mathbb{Z}/n\mathbb{Z}$, $n \geqslant 2$. *Montrer que* A *est l'ensemble des applications* $x \mapsto kx$ *avec* $k \in G$, *et que* A *est isomorphe à l'anneau* $\mathbb{Z}/n\mathbb{Z}$.

Exercice 15 : Entiers 2-adiques

Soit $A = \{m/n \in \mathbb{Q}$ *tel que* n *est impair*$\}$.
(1) : *Montrer que* A *est un sous-anneau de* $\mathbb{Q}$.
(2) : *Chercher les éléments inversibles dans* A.
(3) : *Montrer que les idéaux non nuls de* A *sont tous monogènes engendrés par les nombres de la forme* 2^k, $k \in \mathbb{N}$.

Exercice 16 : Algèbres

Soit

$$E = \left\{ M(a,b,c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} / (a,b,c) \in \mathbb{R}^3 \right\}$$

Montrer que E *est une sous-algèbre commutative de* $\mathcal{M}_3(\mathbb{R})$ *dont on déterminera la dimension.*

V — Sujets d'oraux de concours autres que CCP

Exercice 17 : Centrale

Soit un entier $n \geqslant 2$. *Combien le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$ *admet-il de sous-groupes ?*

Exercice 18 : Mines

1. *Déterminer l'ensemble des inversibles de l'anneau* $\mathbb{Z}/8\mathbb{Z}$. *De quelle structure peut-on munir cet ensemble ?*
2. *Y a-t-il, à isomorphisme près, d'autres groupes de cardinal 4 ?*

Exercice 19 : Mines

Soit $(G, .)$ *un groupe fini tel que*

$$\forall g \in G, g^2 = e$$

où e *est le neutre de* G. *On suppose* G *non réduit à* $\{e\}$.
Montrer qu'il existe $n \in \mathbb{N}^*$ *tel que* G *est isomorphe à* $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Exercice 20 : Mines

Si p *est un nombre premier, quel est le nombre de carrés dans* $\mathbb{Z}/p\mathbb{Z}$ *?*

Exercice 21 : ENTPE

Donner l'ensemble G *des inversibles de l'anneau* $\mathbb{Z}/20\mathbb{Z}$.
Montrer que $(G, \times)$ *est isomorphe à* $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$