

## TD – Structures algébriques

**Exercice de la banque CCINP n°94.** —

1. En raisonnant par l'absurde, montrer que le système  $(S) : \begin{cases} x \equiv 5 & [6] \\ x \equiv 4 & [8] \end{cases}$  n'a pas de solution  $x$  appartenant à  $\mathbf{Z}$ .

2. (a) Énoncer le théorème de Bézout dans  $\mathbf{Z}$ .

(b) Soit  $a$  et  $b$  deux entiers naturels premiers entre eux. Soit  $c \in \mathbf{Z}$ . Prouver que

$$(a \mid c \text{ et } b \mid c) \iff ab \mid c$$

3. On considère le système  $(S) : \begin{cases} x \equiv 6 & [17] \\ x \equiv 5 & [16] \\ x \equiv 4 & [15] \end{cases}$  dans lequel l'inconnue  $x$  appartient à  $\mathbf{Z}$ .

(a) Déterminer une solution particulière  $x_0$  de  $(S)$  dans  $\mathbf{Z}$ .

(b) Dédurre des questions précédentes la résolution dans  $\mathbf{Z}$  du système  $(S)$ . On exprimera les solutions en fonction de la solution particulière  $x_0$ .

**Exercice 1** ★☆☆ — Résoudre le système  $(S) : \begin{cases} 6x + 7y = 30 \\ 3x - 7y = 0 \end{cases}$  d'inconnue  $(x, y) \in (\mathbf{Z}/37\mathbf{Z})^2$ .

systemeLineaireZ37Z

**Exercice 2** ★☆☆ — Résoudre l'équation  $9x \equiv 6 \pmod{24}$  d'inconnue  $x \in \mathbf{Z}$ .

equationCongruenceAffineModulo24 [corrigé]

**Exercice 3** ★☆☆ — Résoudre l'équation  $n^{13} \equiv n \pmod{42}$  d'inconnue  $x \in \mathbf{Z}$ .

equationAlgebriqueDegre13Congruence

**Exercice 4** ★☆☆ — On s'intéresse à l'équation  $(E) : x^2 + x + 1 = 0$ , d'inconnue  $x \in \mathbf{Z}/n\mathbf{Z}$ , où  $n \in \mathbf{N}^*$ .

1. Résoudre l'équation  $(E)$  dans  $\mathbf{Z}/7\mathbf{Z}$ .

2. Résoudre l'équation  $(E)$  dans  $\mathbf{Z}/91\mathbf{Z}$ .

3. Résoudre l'équation  $(E)$  dans  $\mathbf{Z}/220\mathbf{Z}$ .

4. Soit  $p$  un nombre premier impair.

(a) Justifier que  $\bar{2}$  est inversible dans  $\mathbf{Z}/p\mathbf{Z}$ .

(b) On dit que  $x \in \mathbf{Z}/p\mathbf{Z}$  est un carré dans  $\mathbf{Z}/p\mathbf{Z}$  s'il existe  $y \in \mathbf{Z}/p\mathbf{Z}$  tel que  $y^2 = x$ . Démontrer que l'équation  $(E)$  possède une solution dans  $\mathbf{Z}/p\mathbf{Z}$  si et seulement si  $\bar{4}^{-1} - \bar{1}$  est un carré dans  $\mathbf{Z}/p\mathbf{Z}$ .

equationQuadratiqueAnneauZnZ

**Exercice 5** ★☆☆ — Soit  $(G, *)$  un groupe et  $H$  un sous-groupe strict de  $G$ . Déterminer le sous-groupe engendré par  $G \setminus H$ .

sousGroupeEngendreComplementaireSousGroupeStrict [indication(s)]

**Exercice 6** ★☆☆ — Déterminer tous les sous-groupes finis des groupes  $(\mathbf{C}^*, \times)$ .

sousGroupesFinisCEtoile [indication(s)]

**Exercice 7** ★☆☆ — Soit  $d$  un nombre entier qui n'est pas le carré d'un entier. Posons

$$\mathbf{Q}[\sqrt{d}] := \{a + b\sqrt{d} : (a, b) \in \mathbf{Q}^2\}$$

1. Démontrer que  $\mathbf{Q}[\sqrt{d}]$  est un sous-corps de  $\mathbf{C}$  et un sous- $\mathbf{Q}$ -espace vectoriel de dimension 2 de  $\mathbf{C}$ .
2. Déterminer les morphismes de corps de  $\mathbf{Q}[\sqrt{d}]$  dans  $\mathbf{Q}[\sqrt{d}]$ .

endomorphismesCorpsNombresDegre2 [indication(s)]

**Exercice 8** ★☆☆ — Soit  $A$  un anneau communitatif et  $I$  un idéal de  $A$ . La radical de  $I$ , noté  $\sqrt{I}$ , est défini par

$$\sqrt{I} := \{a \in A : \exists n \in \mathbf{N} \quad a^n \in I\}$$

1. Démontrer que  $\sqrt{I}$  est un idéal de  $A$ .
2. Calculer le radical  $\sqrt{107800\mathbf{Z}}$  de l'idéal  $107800\mathbf{Z}$  de l'anneau  $\mathbf{Z}$ .
3. Calculer le radical  $\sqrt{(X^5 + 5X^4 - 13X^3 + 7X^2)\mathbf{Q}[X]}$  de l'idéal  $(X^5 + 5X^4 - 13X^3 + 7X^2)\mathbf{Q}[X]$  de l'anneau  $\mathbf{Q}$ .
4. Soit  $J$  un autre idéal de  $A$ . Démontrer que

$$IJ := \bigcup_{n \in \mathbf{N}} \left\{ \sum_{k=1}^n a_k b_k : (a_k)_{k \in \llbracket 1, n \rrbracket} \in I^n \text{ et } (b_k)_{k \in \llbracket 1, n \rrbracket} \in J^n \right\}$$

est un idéal de  $A$ , puis que

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

radicalIdeal

**Exercice 9** ★★★ — Soient un entier naturel  $n \geq 2$  et  $d$  un diviseur positif de  $n$ .

1. Démontrer que  $(\mathbf{Z}/n\mathbf{Z}, +)$  possède un unique sous-groupe de cardinal  $d$ .
2. En déduire que tout groupe  $(G, *)$  cyclique de cardinal  $n$  possède un unique sous-groupe de cardinal  $d$ .
3. Quels sont les idéaux de l'anneau  $\mathbf{Z}/n\mathbf{Z}$  ?

sousGroupesIdeauxZnZ

**Exercice 10** ★★★ — Les groupes  $(\mathbf{R}, +)$  et  $(\mathbf{R}^*, \times)$  sont-ils isomorphes ?

reelsPlusVersusReelsNonNulsFois [indication(s)]

**Exercice 11** ★★★ — Soient  $(G, *)$  un groupe fini de cardinal  $n$ ,  $a \in G$  et  $m$  un entier relatifs premier à  $n$ . Démontrer que l'équation  $x^m = a$ , d'inconnue  $x \in G$ , possède une unique solution.

equationPuissanceGroupeFini [corrigé]

**Exercice 12** ★★★ — Soit  $\alpha$  un nombre complexe. On suppose que  $\alpha$  est algébrique sur  $\mathbf{Q}$ , i.e. qu'il existe  $P \in \mathbf{Q}[X] \setminus \{0\}$  tel que  $P(\alpha) = 0$ .

1. Démontrer que  $\text{Ann}(\alpha) := \{A \in \mathbf{Q}[X] : A(\alpha) = 0\}$  est un idéal de  $\mathbf{Q}[X]$ .
2. Démontrer que  $\mathbf{Q}[\alpha] := \text{Vect}_{\mathbf{Q}}\left((\alpha^k)_{k \in \mathbf{N}}\right)$  est un  $\mathbf{Q}$ -espace vectoriel de dimension finie, qui est un sous-corps de  $\mathbf{C}$ .

sousCorpsEngendreNombreAlgebrique [indication(s)]

**Exercice 13** ★★★ — Introduisons  $\mathbf{Z}[i] := \{a + ib : (a, b) \in \mathbf{Z}^2\}$ . et l'application norme  $\nu$  définie par

$$\nu \left| \begin{array}{l} \mathbf{Z}[i] \longrightarrow \mathbf{R}_+ \\ z \longmapsto |z|^2 \end{array} \right.$$

1. Démontrer que  $\mathbf{Z}[i]$  est un sous-anneau de  $(\mathbf{C}, +, \times)$ .

2. Notons  $U(\mathbf{Z}[i])$  le groupe des éléments inversibles de l'anneau  $\mathbf{Z}[i]$ . Démontrer que, pour tout  $x \in \mathbf{Z}[i]$ ,  $x \in U(\mathbf{Z}[i])$  si et seulement si  $\nu(x) = 1$ .
3. Déterminer  $U(\mathbf{Z}[i])$ .
4. Un élément  $x$  de  $\mathbf{Z}[i] \setminus \{0\}$  est dit irréductible s'il vérifie les deux conditions suivantes.
  - (a) Le nombre  $x$  n'est pas inversible dans  $\mathbf{Z}[i]$ .
  - (b) Pour tout  $(y, z) \in \mathbf{Z}[i]^2$  tel que  $x = yz$ ,  $y$  ou  $z$  est inversible dans  $\mathbf{Z}[i]$ .
 Le nombre 2 est-il irréductible dans  $\mathbf{Z}[i]$  ?
5. Soit  $(z, w) \in \mathbf{Z}[i] \times (\mathbf{Z}[i] \setminus \{0\})$ . Démontrer qu'il existe  $(q, r) \in \mathbf{Z}[i]^2$  tel que

$$z = qw + r \quad \text{et} \quad \nu(r) < \nu(w)$$

Un tel couple est-il nécessairement unique ?

6. Démontrer que les idéaux de  $\mathbf{Z}[i]$  sont principaux, i.e. qu'ils sont engendrés par un élément.

anneauEntiersGauss [indication(s)]

**Exercice 14** ★★☆☆ — Nous définissons la partie  $\mathbf{Z}[\sqrt{2}]$  de  $\mathbf{R}$  par  $\mathbf{Z}[\sqrt{2}] := \{a + b\sqrt{2} : (a, b) \in \mathbf{Z}^2\}$ .

1. Soit  $x \in \mathbf{Z}[\sqrt{2}]$ . Justifier que l'écriture de  $x$  sous la forme  $a + b\sqrt{2}$ , avec  $(a, b) \in \mathbf{Z}^2$ , est unique.
2. Démontrer que  $\mathbf{Z}[\sqrt{2}]$  est un sous-anneau de  $\mathbf{R}$ .
3. Démontrer qu'il existe un unique automorphisme d'anneaux  $\sigma$  de  $\mathbf{Z}[\sqrt{2}]$  qui est non trivial.
4. Soit l'application norme, notée  $N$ , définie par

$$N \left| \begin{array}{l} \mathbf{Z}[\sqrt{2}] \longrightarrow \mathbf{N} \\ x \longmapsto |x\sigma(x)| \end{array} \right.$$

5. Démontrer que, pour tout  $x \in \mathbf{Z}[\sqrt{2}]$ ,  $x \in \mathbf{Z}[\sqrt{2}]^\times$  si et seulement si  $N(x) = 1$ .
6. Soit  $x$  un élément non nul de  $\mathbf{Z}[\sqrt{2}]$  et  $y \in \mathbf{Z}[\sqrt{2}]$ . Démontrer qu'il existe  $(q, r) \in \mathbf{Z}[\sqrt{2}] \times \mathbf{Z}[\sqrt{2}]$  tel que

$$y = qx + r \quad \text{et} \quad N(r) < N(x)$$

Le couple  $(q, r)$  est-il nécessairement unique ?

7. Soit  $I$  un idéal de  $\mathbf{Z}[\sqrt{2}]$ . Démontrer qu'il existe  $x \in \mathbf{Z}[\sqrt{2}]$  tel que  $I = x\mathbf{Z}[\sqrt{2}]$ .
8. Justifier que  $1 + \sqrt{2} \in U(\mathbf{Z}[\sqrt{2}])$ .
9. Soit  $u \in U(\mathbf{Z}[\sqrt{2}])$  tel que  $u > 1$ . Démontrer que  $u \geq 1 + \sqrt{2}$  puis qu'il existe  $n \in \mathbf{N}^*$  tel que  $u = (1 + \sqrt{2})^n$ .
10. Démontrer que le groupe  $U(\mathbf{Z}[\sqrt{2}])$  est isomorphe à  $\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$ . Il s'agit d'un cas particulier du théorème des unités de Dirichlet.
11. Déterminer l'ensemble solution de l'équation de Pell-Fermat (E) :  $a^2 - 2b^2 = 1$ , d'inconnue  $(a, b) \in \mathbf{Z}^2$ .
12. Donner dix solutions distinctes de l'équation (E).

equationPellFermat

**Exercice 15** ★★☆☆ — Soit  $p$  un nombre premier. On note

$$\mathbf{Z}_{(p)} := \left\{ \frac{a}{b} : (a, b) \in \mathbf{Z} \times \mathbf{N}^*, p \nmid b \right\} \quad \text{et} \quad \mathfrak{M} := \left\{ \frac{a}{b} : (a, b) \in \mathbf{Z} \times \mathbf{N}^*, p \nmid b, p \mid a \right\}$$

1. Démontrer que  $\mathbf{Z}_{(p)}$  est un sous-anneau de  $(\mathbf{Q}, +, \times)$ .
2. Démontrer que  $U(\mathbf{Z}_{(p)}) = \mathbf{Z}_{(p)} \setminus \mathfrak{M}$ .
3. Démontrer que  $\mathfrak{M}$  est un idéal de l'anneau  $\mathbf{Z}_{(p)}$ .
4. Soit  $I$  un idéal de  $\mathbf{Z}_{(p)}$  distinct de  $\mathbf{Z}_{(p)}$ . Démontrer que  $I \subset \mathfrak{M}$ .
5. Déterminer tous les idéaux de l'anneau  $\mathbf{Z}_{(p)}$ , en prenant appui sur la description des idéaux de l'anneau  $\mathbf{Z}$ .

localisationAnneauZ

**Exercice 16** ★★☆☆ — Soit  $\mathbf{K}$  un corps. Soit  $(I_n)_{n \in \mathbf{N}}$  une suite d'idéaux de  $\mathbf{K}[X]$ .

1. On suppose que la suite  $(I_n)_{n \in \mathbf{N}}$  est croissante. Démontrer que cette suite est stationnaire.
2. Si la suite  $(I_n)_{n \in \mathbf{N}}$  est décroissante, est-elle nécessairement stationnaire ?

noetherianiteAnneauPolynomesCoefficientsCorps

**Exercice 17** ★★★ —

1. Le polynôme  $X^4 + 4$  est-il irréductible dans  $\mathbf{Q}[X]$  ?
2. Quels sont les entiers naturels  $n$  tels que  $n^4 + 4$  soit un nombre premier ?

irreductibilitePolynomeDegre4ApplicationArithmetique

**Exercice 18** ★★★ — Soit  $(G, *)$  un groupe fini. Pour  $a \in G$ , posons

$$\Phi_a \left| \begin{array}{l} G \longrightarrow G \\ x \longmapsto a * x * a^{-1} \end{array} \right. \quad [\text{conjugaison par } a]$$

1. Soit  $a \in G$ . Démontrer que  $\Phi_a$  est un automorphisme de groupes de  $G$ .
2. Démontrer que l'ensemble  $I := \{\Phi_a : a \in G\}$  est un sous-groupe du groupe  $(\mathfrak{S}(G), \circ)$ .
3. Supposons que le groupe  $I$  est cyclique. Démontrer que  $G$  est commutatif.

groupeAutomorphismesInterieursCycliqueGroupeAbelien [indication(s)]

**Exercice 19** ★★★ — Soient un entier  $n \geq 2$  et  $p$  un nombre premier. Calculer le cardinal de  $\mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$ .

cardinalGLnZpZ

**Exercice 20** ★★★ — Soient  $p$  un nombre premier impair. On note

$$C(p) := \{x^2 : x \in \mathbf{F}_p^*\} \quad [\text{ensemble des carrés de } \mathbf{F}_p^*]$$

1. Démontrer que  $|C(p)| = \frac{p-1}{2}$ .
2. Soit  $x \in \mathbf{F}_p^*$ . Démontrer que  $x \in C(p)$  si et seulement si  $x^{\frac{p-1}{2}} = \bar{1}$

nombreCarresZpZ

**Exercice 21** ★★★ — Soit  $P$  un polynôme irréductible dans  $\mathbf{Q}[X]$ . Démontrer que les racines complexes de  $P$  sont toutes de multiplicités 1.

multipliciteRacineComplexePolynomeIrreductibleSurQ

**Exercice 22** ★★★ — Soit  $(G, *)$  un groupe fini de cardinal  $p^\alpha \cdot m$ , avec  $p$  premier,  $\alpha \in \mathbf{N}^*$ ,  $m \geq 2$  et  $p \wedge m = 1$ . On se propose de démontrer que  $G$  possède un sous-groupe de cardinal  $p^\alpha$  (théorème de Sylow).Si  $g \in G$  et  $A$  est une partie de  $G$ , alors on pose  $g * A := \{g * a : a \in A\}$ .Soit  $E$  une partie de  $G$  de cardinal  $p^\alpha$ . On pose  $G(E) := \{g \in G : g * E = E\}$  et  $\mathcal{O}(E) := \{g * E : g \in G\}$ .

1. Démontrer que  $G(E)$  est un sous-groupe de  $G$  et que  $\text{card}(G(E)) \leq p^\alpha$ .
2. Démontrer que  $\text{card}(G) = \text{card}(G(E)) \cdot \text{card}(\mathcal{O}(E))$ .
3. Démontrer que les trois assertions suivantes sont équivalentes.
  - (a)  $p$  ne divise pas  $\text{card}(\mathcal{O}(E))$ .
  - (b)  $\text{card}(G(E)) = p^\alpha$
  - (c)  $\text{card}(\mathcal{O}(E)) = m$
4. On note  $X$  l'ensemble des parties de  $G$  de cardinal  $p^\alpha$ . Déterminer le cardinal de  $X$ , puis établir que  $p$  ne divise pas  $\text{card}(X)$ .
5. Démontrer que  $G$  possède un sous-groupe de cardinal  $p^\alpha$ .

unTheoremeSylow [indication(s)]

sousGroupeEngendreComplementaireSousGroupeStrict [\[énoncé\]](#)**Indication(s) pour l'exercice 5**

- Comme  $H$  est un sous-groupe strict de  $G$ , il existe un élément  $x$  appartenant à  $G \setminus H$ .
- Soit  $y \in G$ . On vérifie que  $y \in \langle G \setminus H \rangle$ , ce qui livrera  $G \subset \langle G \setminus H \rangle$ , puis  $G = \langle G \setminus H \rangle$  (l'autre inclusion étant claire).
  - Si  $y \in G \setminus H$ , alors  $y \in \langle G \setminus H \rangle$  est clair.
  - Si  $y \in H$ , alors démontrer que  $x * y \in G \setminus H$ . Ainsi

$$y = x^{-1} * (x * y) \in \langle G \setminus H \rangle$$

**Indication(s) pour l'exercice 6**

Raisonnement par analyse et synthèse.

- *Analyse.*

Soit  $G$  un sous-groupe fini de  $(\mathbf{C}^*, \times)$ , dont nous notons  $n$  le cardinal.

- Justifier que  $G \subset \{x \in \mathbf{C} : x^n = 1\}$ .
- En déduire que  $G = \mathbf{U}_n$ .

- *Synthèse.*

D'après le cours,  $\mathbf{U}_n$  est un sous-groupe de  $(\mathbf{C}^*, \times)$ .

## Indication(s) pour l'exercice 7

1. •  $\mathbf{Q}[\sqrt{d}]$  est un sous- $\mathbf{Q}$ -espace vectoriel de dimension 2 de  $\mathbf{C}$ .  
 On remarque que  $\mathbf{Q}[\sqrt{d}] = \text{Vect}_{\mathbf{Q}}(1, \sqrt{d})$ . Donc  $\mathbf{Q}[\sqrt{d}]$  est un sous- $\mathbf{Q}$ -espace vectoriel de  $\mathbf{C}$ , dont la famille  $(1, \sqrt{d})$  est génératrice sur  $\mathbf{Q}$ . Justifier que la famille  $(1, \sqrt{d})$  est libre sur  $\mathbf{Q}$ .
- $\mathbf{Q}[\sqrt{d}]$  est un sous-anneau de  $\mathbf{C}$ .  
 Comme nous savons déjà que  $\mathbf{Q}[\sqrt{d}]$  est un sous-groupe de  $(\mathbf{C}, +)$ , il reste à vérifier que
- le nombre 1 appartient à  $\mathbf{Q}[\sqrt{d}]$
  - $\mathbf{Q}[\sqrt{d}]$  est stable par produit
- pour conclure que  $\mathbf{Q}[\sqrt{d}]$  est un sous-anneau de  $\mathbf{C}$ .
- Tout élément non nul de  $\mathbf{Q}[\sqrt{d}]$  est inversible dans  $\mathbf{Q}[\sqrt{d}]$ .  
 Soit  $x \in \mathbf{Q}[\sqrt{d}] \setminus \{0\}$ . Il existe donc  $(a, b) \in \mathbf{Q}^2$  tel que  $x = a + b\sqrt{d}$ . Calculer

$$(a + b\sqrt{d})(a - b\sqrt{d})$$

puis justifier que le nombre entier  $a^2 - b^2d$  n'est pas nul, pour conclure que  $(a + b\sqrt{d})^{-1} \in \mathbf{Q}[\sqrt{d}]$ .

2. Raisonner par analyse et synthèse.

- *Analyse.*

Soit un morphisme de corps  $f: \mathbf{Q}[\sqrt{d}] \longrightarrow \mathbf{Q}[\sqrt{d}]$ .

- Justifier que, pour tout  $n \in \mathbf{N}$ ,  $f(n) = n$ .
- En déduire que, pour tout  $n \in \mathbf{Z}$ ,  $f(n) = n$ .
- En déduire que, pour tout  $(p, q) \in \mathbf{Z} \times \mathbf{N}^*$ ,  $f\left(\frac{p}{q}\right) = \frac{p}{q}$ .
- Démontrer que  $f(\sqrt{d})^2 = d$  et en déduire les deux valeurs possibles pour  $f(\sqrt{d})$ .
- En déduire que  $f$  égale l'une des deux applications suivantes

$$\text{id} \left| \begin{array}{l} \mathbf{Q}[\sqrt{d}] \longrightarrow \mathbf{Q}[\sqrt{d}] \\ a + b\sqrt{d} \longmapsto a + b\sqrt{d} \end{array} \right. \quad \sigma \left| \begin{array}{l} \mathbf{Q}[\sqrt{d}] \longrightarrow \mathbf{Q}[\sqrt{d}] \\ a + b\sqrt{d} \longmapsto a - b\sqrt{d} \end{array} \right.$$

- *Synthèse.*

Il est clair que  $\text{id}$  est un morphisme de corps. Vérifier que  $\sigma$  est également un morphisme de corps.

reelsPlusVersusReelsNonNulsFois [\[énoncé\]](#)**Indication(s) pour l'exercice 10**

Considérer un morphisme de groupes  $f: (\mathbf{R}, +) \longrightarrow (\mathbf{R}^*, \times)$  et un réel  $x$ . En remarquant que

$$x = \frac{x}{2} + \frac{x}{2}$$

démontrer que  $f(x) > 0$ .



## Indication(s) pour l'exercice 12

Commençons par deux observations, qui nous aideront dans l'étude du corps  $\mathbf{Q}[\alpha]$ .

(a) D'après le cours, « le morphisme d'évaluation d'un polynôme de  $\mathbf{Q}[X]$  en  $\alpha$  »

$$\text{eval}_\alpha \left| \begin{array}{l} \mathbf{Q}[X] \longrightarrow \mathbf{C} \\ P \longmapsto P(\alpha) := \sum_{k=0}^{+\infty} [P]_k \alpha^k \end{array} \right.$$

est un morphisme de  $\mathbf{Q}$ -algèbres.

(b) L'ensemble  $\mathbf{Q}[\alpha]$  possède la description alternative suivante

$$\mathbf{Q}[\alpha] = \{P(\alpha) : P \in \mathbf{Q}[X]\}$$

Passons à la résolution de l'exercice.

1. L'ensemble  $\text{Ann}(\alpha)$  est le noyau du morphisme d'anneaux  $\text{eval}_\alpha : \mathbf{Q}[X] \longrightarrow \mathbf{C}$ .

2. •  $\mathbf{Q}[\alpha]$  est une sous- $\mathbf{Q}$ -algèbre  $\mathbf{C}$ .

L'ensemble  $\mathbf{Q}[\alpha]$  est l'image de la  $\mathbf{Q}$ -algèbre  $\mathbf{Q}[X]$  par le morphisme de  $\mathbf{Q}$ -algèbres  $\text{eval}_\alpha : \mathbf{Q}[X] \longrightarrow \mathbf{C}$ .

•  $\mathbf{Q}[\alpha]$  est un  $\mathbf{Q}$ -espace vectoriel de dimension finie.

Nous savons déjà que  $\mathbf{Q}[\alpha]$  est un sous- $\mathbf{Q}$ -espace vectoriel de  $\mathbf{C}$ . Il reste à démontrer que ce sous-espace est de dimension finie. Comme  $\text{Ann}(\alpha)$  est un idéal non nul de  $\mathbf{Q}[X]$ , il existe un unique polynôme unitaire  $\mu$  tel que

$$\text{Ann}(\alpha) = \mu \mathbf{Q}[X]$$

Notons  $d := \deg(\mu) \geq 1$ . Démontrer que

$$(1, \alpha, \dots, \alpha^{d-1})$$

est une base de  $\text{Ann}(\alpha)$  (le caractère générateur suffit à répondre à la question).

• Tout élément non nul de  $\mathbf{Q}[\alpha]$  est inversible dans  $\mathbf{Q}[\alpha]$ .

Soit  $x \in \mathbf{Q}[\alpha]$ . On considère l'application « multiplication par  $x$  » définie sur  $\mathbf{Q}[\alpha]$  par

$$\text{mult}_x \left| \begin{array}{l} \mathbf{Q}[\alpha] \longrightarrow \mathbf{Q}[\alpha] \\ y \longmapsto yx \end{array} \right.$$

— Justifier que  $\text{mult}_x$  est bien définie.

— Démontrer que  $\text{mult}_x$  est bijective.

— En déduire qu'il existe  $y \in \mathbf{Q}[\alpha]$  tel que  $xy = yx = 1$ .

## Indication(s) pour l'exercice 13

1. On vérifie que

- les nombres  $0, 1$  appartiennent à  $\mathbf{Z}[i]$
- $\mathbf{Z}[i]$  est stable par somme tordue
- $\mathbf{Z}[i]$  est stable par produit

2.  $\boxed{\implies}$  Soit  $x \in U(\mathbf{Z}[i])$ . Il existe donc  $y \in \mathbf{Z}[i]$  tel que  $xy = 1$ . Nous en déduisons

$$1 = \nu(xy) = \nu(x) \nu(y)$$

On remarque alors que  $\nu(x)$  et  $\nu(y)$  sont des entiers naturels.

$\boxed{\impliedby}$  Soit  $x \in \mathbf{Z}[i]$  tel que  $\nu(x) = 1$ . Il existe  $(a, b) \in \mathbf{Z}^2$  tel que  $x = a + ib$ . On calcule

$$1 = \nu(x) = (a + ib)(a - ib) = x(a - ib)$$

3. Soit  $(a, b) \in \mathbf{Z}^2$ .

$$\begin{aligned} a + ib \in U(\mathbf{Z}[i]) &\iff a^2 + b^2 = 1 && \text{[cf. question précédente]} \\ &\iff (a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\} && \text{[car } a \text{ et } b \text{ sont des entiers]} \end{aligned}$$

4. Supposons qu'il existe  $x, y \in \mathbf{Z}[i] \setminus U(\mathbf{Z}[i])$  tels que  $2 = xy$ . Nous en déduisons que

$$4 = \nu(xy) = \nu(x) \nu(y)$$

Comme  $\nu(x)$  et  $\nu(y)$  sont des entiers naturels différents de 1, nécessairement  $\nu(x) = 2$  et  $\nu(y) = 2$ . Nous en déduisons que

$$x = \pm 1 \pm i \quad \text{et} \quad y = \pm 1 \pm i$$

5. • *Existence.*  
On observe qu'il existe  $(\alpha, \beta) \in \mathbf{Q}^2$  tel que

$$\frac{z}{w} = \frac{z \cdot \bar{w}}{|w|^2} = \alpha + i\beta$$

On considère deux entiers  $a, b$  (non nécessairement uniques) tels que  $|\alpha - a| \leq \frac{1}{2}$  et  $|\beta - b| \leq \frac{1}{2}$ , puis on vérifie que  $q := a + ib$  convient.

• *Défaut d'unicité.*

Il provient « du choix d'un entier le plus proche d'un nombre rationnel ». Un contre-exemple est donné par

$$\underbrace{1}_z = \underbrace{1}_q \times \underbrace{2}_w + \underbrace{(-1)}_r \quad \text{et} \quad \underbrace{1}_z = \underbrace{0}_q \times \underbrace{2}_w + \underbrace{1}_r$$

6. • On adapte les démonstrations données pour les idéaux de  $\mathbf{Z}$  et pour les idéaux de  $\mathbf{K}[X]$ , en prenant appui sur la « pseudo division euclidienne » construite à la question précédente.  
• Si  $I$  est un idéal non nul de  $\mathbf{Z}[i]$ , un générateur de  $I$  est un élément  $x$  de  $I$  tel que

$$\nu(x) = \min \{ \nu(y) : y \in I \setminus \{0\} \}$$

groupeAutomorphismesInterieursCycliqueGroupeAbelien [énoncé]

### Indication(s) pour l'exercice 18

1.
  - Vérifier que, pour tout  $(x, y) \in G^2$ ,  $\Phi_a(x * y) = \Phi_a(x) * \Phi_a(y)$ .
  - Calculer  $\Phi_a \circ \Phi_{a^{-1}}$  et  $\Phi_{a^{-1}} \circ \Phi_a$ .
2.
  - Calculer, pour tout  $(a, b) \in G^2$ ,  $\Phi_a \circ \Phi_b$ .
  - Qu'en déduire pour l'application suivante ?

$$\Phi \left| \begin{array}{ccc} (G, *) & \longrightarrow & (\mathfrak{S}(G), \circ) \\ a & \longmapsto & \Phi_a \end{array} \right.$$

- L'image d'un morphisme de groupes est un sous-groupe de son but.
3.
    - Fixons un élément  $g \in G$  tel que  $\Phi_g$  engendre  $I$ .
    - Remarquer que l'application

$$\tilde{\Phi} \left| \begin{array}{ccc} (G, *) & \longrightarrow & (I, \circ) \\ a & \longmapsto & \Phi_a \end{array} \right.$$

un morphisme de groupes surjectif et vérifier que son noyau est le centre de  $G$

$$Z(G) := \{x \in G : \forall y \in G \quad x * y = y * x\}.$$

- Soit  $a \in G$ . Comme  $I = \langle \Phi_g \rangle$ , il existe  $k \in \mathbf{Z}$  tel que  $\Phi_a = (\Phi_g)^k$ . À l'aide du point précédent, justifier qu'il existe  $x \in Z(G)$  tel que  $a = x * g^k$ .
- Soient  $(x_1, x_2) \in Z(G)^2$  et  $(k_1, k_2) \in \mathbf{Z}^2$ . Démontrer que les éléments  $x_1 * g^{k_1}$  et  $x_2 * g^{k_2}$  commutent.

**Indication(s) pour l'exercice 22**

- Vérifier que  $e_G \in G(E)$  et que, pour tout  $g_1, g_2 \in G(E)$ ,  $g_1 * g_2^{-1} \in G(E)$ , en démontrant des égalités d'ensembles par double inclusion.
  - Soit  $x$  un élément de  $E$  fixé. Justifier que l'application

$$\left| \begin{array}{ccc} G(E) & \longrightarrow & E \\ g & \longmapsto & g * x \end{array} \right.$$

est bien définie et injective.

2. Considérons l'application

$$p \left| \begin{array}{ccc} G & \longrightarrow & \mathcal{O}(E) \\ g & \longmapsto & g * E \end{array} \right.$$

Elle induit une partition de  $G$

$$G = \bigsqcup_{A \in \mathcal{O}(E)} p^{-1}(\{A\})$$

Pour chaque  $A \in \mathcal{O}(E)$ , que l'on peut écrire  $g * E$  pour un élément  $g \in G$ , construire une bijection entre  $A$  et  $E$ .

3. (a)  $\implies$  (b) Supposons que  $p$  ne divise pas  $\text{card}(\mathcal{O}(E))$ , i.e. que  $v_p(\text{card}(\mathcal{O}(E))) = 0$ . D'après la question 2

$$\alpha \underset{p \wedge m = 1}{=} v_p(\text{card}(G)) = v_p(\text{card}(G(E))) + v_p(\text{card}(\mathcal{O}(E))) = v_p(\text{card}(G(E))).$$

Ainsi  $p^\alpha$  divise  $\text{card}(G(E))$ , d'où  $p^\alpha \leq \text{card}(G(E))$ . Or d'après la question 1,  $p^\alpha \geq \text{card}(G(E))$ . Ainsi  $\text{card}(G(E)) = p^\alpha$ .

(b)  $\implies$  (c) Cette implication est conséquence de la question 2.

(c)  $\implies$  (a) Cette implication est conséquence de  $p \wedge m = 1$ .

4. • *Détermination de  $\text{card}(X)$  et stratégie.*

D'après le cours, l'ensemble des parties à  $p^\alpha$  éléments d'un ensemble à  $p^\alpha m$  éléments est  $\binom{p^\alpha m}{p^\alpha}$ . Ainsi

$$\text{card}(X) = \binom{p^\alpha m}{p^\alpha}$$

Pour achever notre réponse à cette question, il nous faut démontrer que  $p$  ne divise pas  $\binom{p^\alpha m}{p^\alpha}$ , i.e. que

$$\mathcal{P}(\alpha) : v_p((p^\alpha m)!) = v_p((p^\alpha)!) + v_p((p^\alpha m - p^\alpha)!)$$

- $v_p((ap)!) = a + v_p(a!)$ , pour tout  $a \in \mathbf{N}^*$ .  
Soit  $a \in \mathbf{N}^*$ . Nous observons

$$v_p((ap)!) = \sum_{i=1}^{ap} v_p(i)$$

Comme

$$[1, ap] = \bigsqcup_{i=0}^{a-1} \{1 + ip, 2 + ip, \dots, p - 1 + ip, p + ip\}$$

il vient

$$v_p((ap)!) = \sum_{i=1}^{ap} v_p(i) = \sum_{i=0}^{a-1} \left( \underbrace{v_p(1 + ip)}_{=0} + \underbrace{v_p(2 + ip)}_{=0} + \dots + \underbrace{v_p(p - 1 + ip)}_{=0} + \underbrace{v_p(p + ip)}_{=1 + v_p(i+1)} \right)$$

puis

$$(\star) \quad v_p((ap)!) = \sum_{i=0}^{a-1} 1 + \sum_{i=0}^{a-1} v_p(i + 1) = a + v_p\left(\prod_{i=0}^{a-1} i\right) = a + v_p(a!)$$

- *Initialisation de  $\mathcal{P}(\alpha)$  à  $\alpha = 0$*

L'assertion  $\mathcal{P}(0)$  s'écrit

$$v_p(m!) = \underbrace{v_p(1!)}_{=0} + v_p((m-1)!)$$

Comme  $p \wedge m = 1$ ,  $v_p(m) = 0$  et donc

$$v_p(m!) = v_p(m \cdot (m-1)!) = v_p(m) + v_p((m-1)!) = v_p((m-1)!)$$

ce qui établit  $\mathcal{P}(0)$ .

- *Caractère héréditaire de  $\mathcal{P}(\alpha)$ .*

Soit  $\alpha \in \mathbf{N}$  tel que  $\mathcal{P}(\alpha)$  est vraie. D'après  $(\star)$

$$v_p((p^{\alpha+1}m)!) - v_p((p^{\alpha+1})!) - v_p((p^{\alpha+1}m - p^{\alpha+1})!)$$

égale

$$p^\alpha m + v_p((p^\alpha m)!) - (p^\alpha + v_p((p^\alpha)!)) - (p^\alpha m - p^\alpha + v_p((p^\alpha m - p^\alpha)!))$$

ou encore, après simplification, égale

$$v_p((p^\alpha m)!) - v_p((p^\alpha)!) - v_p((p^\alpha m - p^\alpha)!).$$

Grâce à  $\mathcal{P}(\alpha)$ , ce dernier terme est nul et donc

$$v_p((p^{\alpha+1}m)!) = v_p((p^{\alpha+1})!) + v_p((p^{\alpha+1}m - p^{\alpha+1})!).$$

5. • On vérifie que la relation  $\sim$  définie sur  $X$  par

$$\forall (E_1, E_2) \in X^2 \quad E_1 \sim E_2 \iff (\exists g \in G \quad E_1 = g * E_2)$$

est une relation d'équivalence et que, pour tout  $E \in X$ , la classe  $\overline{E}$  de  $E$  est

$$\overline{E} = \mathcal{O}(E) = \{g * E : g \in G\}$$

La partition associée à la relation d'équivalence  $\sim$  sur  $X$  s'écrit

$$X = \bigsqcup_{i=1}^r \mathcal{O}(E_i)$$

où  $\mathcal{O}(E_1), \mathcal{O}(E_2), \dots, \mathcal{O}(E_r)$  est une liste exhaustive et sans répétition des classes d'équivalences de  $X$  pour la relation  $\sim$ . Nous en déduisons

$$(\star) \quad \text{card}(X) = \sum_{k=1}^r \text{card}(\mathcal{O}(E_k))$$

- D'après la question 4 et l'identité  $(\star)$ , il existe  $i \in \llbracket 1, r \rrbracket$  tel que  $p$  ne divise pas  $\text{card}(\mathcal{O}(E_i))$ .
- D'après les questions 1 et 3,  $G(E_i)$  est un sous-groupe de  $(G, *)$  de cardinal  $p^\alpha$ .

## Un corrigé de l'exercice 2

- Pour tout  $x \in \mathbf{Z}$ .

$$9x \equiv 6 \pmod{24} \iff \bar{9}^{[24]} \bar{x}^{[24]} = \bar{6}^{[24]}$$

- Comme  $24 = 3 \times 8$  et  $3 \wedge 8 = 1$ , le théorème chinois nous apprend que l'application

$$f \left| \begin{array}{l} \mathbf{Z}/24\mathbf{Z} \longrightarrow \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z} \\ \bar{x}^{[24]} \longmapsto (\bar{x}^{[3]}, \bar{x}^{[8]}) \end{array} \right.$$

est un isomorphisme d'anneaux. Ainsi, pour tout  $x \in \mathbf{Z}$

$$\begin{aligned} \bar{9}^{[24]} \bar{x}^{[24]} = \bar{6}^{[24]} &\iff \begin{cases} \bar{9}^{[3]} \bar{x}^{[3]} = \bar{6}^{[3]} \\ \bar{9}^{[8]} \bar{x}^{[8]} = \bar{6}^{[8]} \end{cases} \\ &\iff \bar{x}^{[8]} = \bar{6}^{[8]} \end{aligned}$$

- Des deux points précédents, nous déduisons

$$\{x \in \mathbf{Z} : 9x \equiv 6 \pmod{24}\} = 6 + 8\mathbf{Z}$$

## Un corrigé de l'exercice 11

- Il s'agit de démontrer que l'application

$$f \begin{cases} G & \longrightarrow & G \\ x & \longmapsto & x^m \end{cases}$$

est bijective ( $f$  peut ne pas être un morphisme de groupes, si  $G$  est anabélien). Comme  $G$  est un ensemble fini, il est équivalent de démontrer que l'application  $f$  est injective.

- Soit  $(x, y) \in G^2$  tel que  $f(x) = f(y)$ , i.e. tel que  $x^m = y^m$ . D'après le théorème de Bézout

$$\exists (u, v) \in \mathbf{Z}^2 \quad mu + nu = 1$$

Alors

$$\begin{aligned} x^m = y^m &\implies x^{mu} = y^{mu} && \text{[élévation à la puissance } u\text{]} \\ &\implies x^{mu+nu} = y^{mu+nu} && \text{[} x^n = y^n = e_G \text{ car les ordres de } x \text{ et } y \text{ divisent } n\text{]} \\ &\implies x = y \end{aligned}$$