ALGÈBRE GÉNÉRALE

TD 1

par David Blottière, le 26 octobre 2023 à 07h13

SOMMAIRE

§ 1. EXERCICES ISSUS DES ORAUX DU CCINP

ÉNONCÉ DE L'EXERCICE 1

Soit $p \in \mathbf{N}^*$. On considère dans $\mathbf{Z}$ la relation d'équivalence $\mathscr{R}$ définie par

$$\forall (x,y) \in \mathbf{Z}^2, \quad x \mathscr{R} y \iff p \mid (x-y).$$

On note $\mathbf{Z}/p\mathbf{Z}$ l'ensemble des classes d'équivalence pour cette relation d'équivalence.

Q1. — Quelle est la classe d'équivalence de 0 ? Quelle est celle de p ?

Q2. — Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbf{Z}/p\mathbf{Z}$.

Q3. — On admet que muni de ces opérations, $\mathbf{Z}/p\mathbf{Z}$ est un anneau. Démontrer que $\mathbf{Z}/p\mathbf{Z}$ est un corps si et seulement si p est premier.

□

ÉNONCÉ DE L'EXERCICE 2

On note S_n l'ensemble des permutations sur l'ensemble $[\![1,n]\!]$.

Q1. — Démontrer que $(S_n, \circ)$ est un groupe.

On note σ l'élément de S_8 défini de la manière suivante :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 7 & 8 & 6 & 2 & 3 \end{pmatrix}$$

l'image de chaque terme de la première ligne étant écrit juste en-dessous.

Q2. — Démontrer que la permutation σ est la composée de deux cycles que l'on précisera.

Q3. — On note $\sigma^n = \underbrace{\sigma \circ \ldots \circ \sigma}_{n \text{ fois}}$. Déterminer σ^{12}, σ^{24}, σ^4 et σ^{2016}.

□

ÉNONCÉ DE L'EXERCICE 3

Q1. — Résoudre l'équation :

$$3n+5 \equiv 0 \quad [10]$$

d'inconnue $n \in \mathbf{Z}$.

Q2. — Résoudre l'équation :

$$n^2 \equiv 1 \quad [8]$$

d'inconnue $n \in \mathbf{Z}$.

Q3. — Résoudre l'équation :

$$n^2+2n+2 \equiv 0 \quad [5]$$

d'inconnue $n \in \mathbf{Z}$.

□

ÉNONCÉ DE L'EXERCICE 4

Q1. — Résoudre le système :

$$\begin{cases} n \equiv 1\ [6] \\ n \equiv 2\ [7] \end{cases}$$

d'inconnue $n \in \mathbf{Z}$.

Q2. — Résoudre le système :

$$\begin{cases} 3n \equiv 2\ [5] \\ 5n \equiv 1\ [6] \end{cases}$$

d'inconnue $n \in \mathbf{Z}$.

Q3. — Résoudre le système :

$$\begin{cases} n+m \equiv 4\ [11] \\ nm \equiv 10\ [11] \end{cases}$$

d'inconnue $(n,m) \in \mathbf{Z}^2$.

□

ÉNONCÉ DE L'EXERCICE 5

Démontrer que pour tout $n \in \mathbf{N}^*$:

$$12^{12^n} \equiv 1\ [7] \qquad \text{et} \qquad 10^{10^n} \equiv 4\ [7].$$

□

ÉNONCÉ DE L'EXERCICE 6

Soient $(G,\cdot)$ un groupe et $a \in G$. Pour tout $(x,y) \in G^2$, posons :

$$x \star y = x \cdot a \cdot y\,.$$

Démontrer que $(G,\star)$ est un groupe.

□

ÉNONCÉ DE L'EXERCICE 7

Soient $(A,+,\times)$ un anneau commutatif et I un idéal de A.

Q1. — L'ensemble $\{x \in A : x^2 \in I\}$ est-il un idéal de A?

Q2. — L'ensemble $\{x \in A : \exists n \in \mathbf{N},\ x^n \in I\}$ est-il un idéal de A?

□

ÉNONCÉ DE L'EXERCICE 8

Existe-t-il un couple $(a,b) \in \mathbf{N}^2$ tel que $a^2+b^2 = 2023$?

□

§ 2. EXERCICES ISSUS DES ORAUX DU CONCOURS TPE

ÉNONCÉ DE L'EXERCICE 9 INDICATIONS

Résoudre $x^2+x+1=0$ dans $\mathbf{Z}/7\mathbf{Z}$, puis dans $\mathbf{Z}/6\mathbf{Z}$. Que dire dans $\mathbf{Z}/n\mathbf{Z}$, où $n \in \mathbf{N}^*$?

□

ÉNONCÉ DE L'EXERCICE 10

Démontrer que l'ensemble des entiers premiers congrus à -1 modulo 4 est infini. On pourra raisonner par l'absurde et considérer $N = 4 \cdot p_1 \cdot \ldots \cdot p_r - 1$, où $p_1, \ldots, p_r$ sont des nombres premiers « bien choisis ».

□

ÉNONCÉ DE L'EXERCICE 11

Soit A un anneau tel que pour tout $x \in A$, $x^3 = x$.

Q1. — Démontrer que pour tout $x \in A$, $6x = 0$.

Q2. — Notons $B = \{x \in A : 2x = 0\}$ et $C = \{x \in A : 3x = 0\}$. Démontrer que $B + C = A$.

□

ÉNONCÉ DE L'EXERCICE 12

Résoudre dans $\mathbf{Z}^2$ l'équation :

$$11 \cdot (n \wedge m) + n \vee m = 203.$$

□

ÉNONCÉ DE L'EXERCICE 13

Soit $p \geq 3$ un nombre premier. On considère l'équation

$$(E) \quad x^2 + ax + b = 0$$

d'inconnue $x \in \mathbf{Z}/p\mathbf{Z}$.

Q1. — Démontrer que (E) possède une solution si et seulement si $a^2 - 4b$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$.

Dans la suite, on suppose qu'il existe $u \in \mathbf{N}^*$ tel que $p = 3 \cdot u + 1$.

Q2. — Démontrer qu'il existe $a \in (\mathbf{Z}/p\mathbf{Z})^*$ tel que $a^u \neq 1$.

Q3. — En déduire que -3 est un carré dans $\mathbf{Z}/p\mathbf{Z}$.

□

ÉNONCÉ DE L'EXERCICE 14

Résoudre dans $\mathbf{Z}/37\mathbf{Z}$ le système suivant.

$$\begin{cases} \overline{6}\,x + \overline{7} \cdot y &= \overline{30} \\ \overline{3}\,x - \overline{7} \cdot y &= \overline{0} \end{cases}$$

□

ÉNONCÉ DE L'EXERCICE 15

Résoudre dans $\mathbf{N}^* \times \mathbf{N}^*$ le système suivant.

$$\begin{cases} n \wedge m &= n - m \\ n \vee m &= 300 \end{cases}$$

□

§ 3. EXERCICES ISSUS DES ORAUX DU CONCOURS CENTRALESUPÉLEC

ÉNONCÉ DE L'EXERCICE 16

Notons :

$$\mathbf{Z}[i] := \left\{a + i \cdot b : (a,b)_i n \mathbf{Z}^2\right\}$$

et

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

Q1. — Déterminer les éléments inversibles de $\mathbf{Z}[i]$. On pourra utiliser ν.

Q2. — Démontrer que 2 est réductible dans $\mathbf{Z}[i]$.

Q3. — 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 $z = qw + r$, avec $\nu(r) < \nu(w)$. Un tel couple est-il nécessairement unique ?

Q4. — Démontrer que les idéaux de $\mathbf{Z}[i]$ sont principaux, i.e. qu'ils sont engendrés par un élément.

□

ÉNONCÉ DE L'EXERCICE 17

Pour tout $n \in \mathbf{N}^*$, on note D_n l'ensemble des diviseurs positifs de n.
Soient n et m premiers entre eux. Posons :

$$\varphi_{n,m} \left| \begin{array}{ccc} D_n \times D_m & \longrightarrow & D_{nm} \\ (d,d') & \longmapsto & d \cdot d' \end{array} \right. \quad \text{et} \quad \psi_{n,m} \left| \begin{array}{ccc} D_{nm} & \longrightarrow & D_n \times D_m \\ q & \longmapsto & (n \wedge q, m \wedge q) \end{array} \right. .$$

Q1. — Démontrer que $\varphi_{n,m}$ et $\psi_{n,m}$ sont des applications bien définies et inverses l'une de l'autre.

Q2. — Qu'en déduire pour le cardinal de D_{nm} ?

□

ÉNONCÉ DE L'EXERCICE 18

Soit $(G,\cdot)$ un groupe fini. Pour $a \in G$, posons :

$$\Phi_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \cdot x \cdot a^{-1} \end{array} \right. \qquad [\textit{conjugaison par } a] .$$

Q1. — Démontrer que Φ_a est un automorphisme de groupes de G.

Q2. — Démontrer que l'ensemble :

$$I := \{\Phi_a : a \in G\}$$

est un sous-groupe du groupe des automorphismes de G.

Q3. — Supposons I cyclique. Démontrer que G est commutatif.

□

ÉNONCÉ DE L'EXERCICE 19

Soient $(G,\cdot)$ un groupe fini de cardinal n, d'élément neutre e et p un diviseur premier de n.
Posons :

$$E = \left\{(x_1,...,x_p) \in G^p : x_1 \cdot \ldots \cdot x_p = e\right\}.$$

Q1. — Démontrer que $\text{Card}\,(E) = n^{p-1}$.

Notons $\sigma \in \mathfrak{S}_p$ le p-cyle $(1,\ldots,p)$. Pour tout $X = \left(x_1,\ldots,x_p\right) \in G^p$ et tout $k \in \mathbf{Z}$, on note :

$$\sigma^k X := \left(x_{\sigma^k(1)},\ldots,x_{\sigma^k(p)}\right).$$

Q2. — Démontrer :

$$\forall\, X \in E, \quad \forall\, k \in \mathbf{Z}, \quad \sigma^k X \in E.$$

Soit $X \in E$. On pose

$$\mathrm{o}(X) := \left\{Y \in E : \exists k \in \mathbf{Z} \textit{ tel que } \sigma^k X = Y\right\}.$$

Q3. — Démontrer que $\mathrm{o}(Y) = \mathrm{o}(X)$, pour tout $Y \in o(X)$.

Q4. — Démontrer qu'il existe une famille $(X_i)_{1\le i\le m}$ telle que $(\mathrm{o}(X_i))_{1\le i\le m}$ forme une partition de E.

Q5. — Soit $X \in E$. Démontrer que $\mathrm{o}(X)$ contient soit p éléments, soit un unique élément.

Q6. — Démontrer que G posséde un élément d'ordre p. Ce résultat est connu sous le nom de Lemme de Cauchy.

□

§ 4. EXERCICES ISSUS DES ORAUX DU CONCOURS MINES PONTS

ÉNONCÉ DE L'EXERCICE 20 **INDICATIONS**

Résoudre dans $\mathbf{N}^3$ le système suivant.

$$\begin{cases} x^3 - y^3 - z^3 &= 3xyz \\ x^2 &= 2y + 2z \end{cases}$$

□

ÉNONCÉ DE L'EXERCICE 21

Déterminer les couples d'entiers $(p,q) \in \mathbf{Z}^2$ tels que 7 divise $2p+3q$.

□

ÉNONCÉ DE L'EXERCICE 22

Soit $n \in \mathbf{N}^*$. Déterminer le maximum et le minimum, lorsque σ parcourt l'ensemble $\mathfrak{S}_n$, de $\sum_{k=1}^{n} k \cdot \sigma(k)$.

□

ÉNONCÉ DE L'EXERCICE 23

Posons :

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

Démontrer que $\mathbf{Q}\left[\sqrt{2}\right]$ est un corps et déterminer les morphismes d'anneaux de $\mathbf{Q}\left[\sqrt{2}\right]$ dans $\mathbf{Q}\left[\sqrt{2}\right]$.

□

ÉNONCÉ DE L'EXERCICE 24

Posons $j = e^{i\frac{2\pi}{3}}$ *et :*

$$\mathbf{Z}[j] := \{a + b \cdot j \,:\, (a,b) \in \mathbf{Z}^2\}.$$

Q1. — Démontrer que $\mathbf{Z}[j]$ est un sous-anneau de $\mathbf{C}$.

On note U l'ensemble des inversibles de $\mathbf{Z}[j]$.

Q2. — Démontrer que pour tout $z \in \mathbf{Z}[j]$, $z \in U$ si et seulement si $|z| = 1$.

Q3. — Déterminer U.

□

INDICATIONS POUR L'EXERCICE 9 — ÉNONCÉ

Résolution dans $\mathbf{Z}/7\mathbf{Z}$ via la forme canonique de $X^2+X+\overline{1}$ dans $\mathbb{F}_7[X]$. Comme 7 est un nombre premier, l'anneau $\mathbb{F}_7=\mathbf{Z}/7\mathbf{Z}$ est un corps. Dans ce corps $\overline{2}\neq\overline{0}$ a pour inverse $\overline{4}$. Ainsi :

$$X^2+X+\overline{1}=\left(X+\overline{4}\right)^2-\overline{1} \qquad \left[\text{forme canonique dans } \mathbb{F}_7[X]\right].$$

Résolution dans $\mathbf{Z}/7\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z}$ en testant tous les éléments. On peut également tester les 7 (resp. 6) éléments de $\mathbb{F}_7$ (resp. de $\mathbf{Z}/6\mathbf{Z}$), pour savoir lesquels sont solutions de l'équation.

Résolution dans $\mathbf{Z}/n\mathbf{Z}$. On pose, pour tout entier $n\geqslant 2$:

$$\mathrm{Sol}_n:=\left\{x\in\mathbf{Z}/n\mathbf{Z}\,:\,x^2+x+\overline{1}=\overline{0}\right\}.$$

On propose six pistes de réflexion pour étudier ces ensembles.

(1) Soit un entier naturel pair $n\geqslant 2$. Alors :

$$\mathrm{Sol}_n=\varnothing.$$

Considérer la parité de x^2+x pour un nombre entier x.

(2) Soit un nombre entier $n=p_1^{k_1}\dots p_r^{k_r}$, où $p_1,\dots,p_r$ sont des nombres premiers impairs distincts et $k_1,\dots,k_r$ sont des nombres entiers naturels non nuls. On a une bijection naturelle :

$$\mathrm{Sol}_n\longrightarrow \mathrm{Sol}_{p_1^{k_1}}\times\dots\times\mathrm{Sol}_{p_r^{k_r}}.$$

Convoquer le théorème des restes chinois.

(3) Soit un nombre premier $p\geqslant 3$. Alors :

$$\mathrm{Sol}_p=\begin{cases}\varnothing & \text{si } \overline{-3} \text{ n'est pas un carré dans } \mathbb{F}_p\,;\\ \left\{-\overline{2}^{-1}\left(\overline{1}+\overline{\delta}\right),-\overline{2}^{-1}\left(\overline{1}-\overline{\delta}\right)\right\} & \text{si } \overline{-3} \text{ est le carré d'un élément } \overline{\delta} \text{ de } \mathbb{F}_p.\end{cases}$$

Considérer la forme canonique de $X^2+X+\overline{1}$ dans $\mathbb{F}_p[X]$.

(4) Pour tout nombre entier $k\geqslant 2$:

$$\mathrm{Sol}_{3^k}=\varnothing.$$

Établir d'abord le résultat pour Sol_9.

(5) Soit un nombre premier $p\geqslant 5$ tel que $\overline{-3}$ n'est pas un carré dans $\mathbb{F}_p$. Alors, pour tout $k\in\mathbf{N}^*$:

$$\mathrm{Sol}_{p^k}=\varnothing.$$

(6) Soient un nombre premier $p\geqslant 5$ tel que $\overline{-3}$ est un carré dans $\mathbb{F}_p$ et δ un un entier tel que $\delta^2\equiv -3 \bmod p$. D'après (3) :

$$\mathrm{Sol}_p=\left\{\overline{x_1}:=-\overline{2}^{-1}\left(\overline{1}+\overline{\delta}\right),\ \overline{y_1}:=-\overline{2}^{-1}\left(\overline{1}-\overline{\delta}\right)\right\}.$$

Il existe un unique élément $(x_k)_{k\geqslant 2}$ de $\displaystyle\prod_{k=2}^{+\infty}\mathbf{Z}/p^k\mathbf{Z}$ tel que, pour tout nombre entier $k\geqslant 2$:

$$x_k^2+x_k+1\equiv 0 \bmod p^k \qquad \text{et} \qquad x_k=x_{k-1} \bmod p^{k-1}$$

et un unique élément $(y_k)_{k\geqslant 2}$ de $\displaystyle\prod_{k=2}^{+\infty}\mathbf{Z}/p^k\mathbf{Z}$ tel que, pour tout nombre entier $k\geqslant 2$:

$$y_k^2+y_k+1\equiv 0 \bmod p^k \qquad \text{et} \qquad y_k=y_{k-1} \bmod p^{k-1}$$

de sorte que, pour tout nombre entier $k\geqslant 2$:

$$\mathrm{Sol}_{p^k}=\left\{\overline{x_k}\,,\,\overline{y_k}\right\}.$$

Construire les nombres entiers x_k par récurrence, les nombres entiers y_k pouvant être obtenus de même.

Les éléments $(x_k)_{k\geqslant 1}$ et $(y_k)_{k\geqslant 1}$ de $\displaystyle\prod_{k=1}^{+\infty}\mathbf{Z}/p^k\mathbf{Z}$ que l'on a construits sont des nombres p-adiques et on établit ici un cas particulier du lemme de Hensel.

Remarque. Soit un nombre premier $p\geqslant 5$. On peut démontrer que :

$$\left(\overline{-3}\text{ est un carré dans }\mathbb{F}_p\right)\iff 3\mid p-1.$$

INDICATIONS POUR L'EXERCICE 20 ÉNONCÉ

Nous raisonnons par analyse et synthèse. Considérons des entiers naturels x, y, z solutions de :

$$(S) \quad \begin{cases} x^3 - y^3 - z^3 &= 3xyz \\ x^2 &= 2y + 2z \end{cases}$$

La première équation évoque des relations coefficients-racines (formules de Viète). Comme :

$$(X-x)(X+y)(X+z) = X^3 - (x-y-z)X^2 + (yz-xy-xz)X - xyz$$

il vient :

$$\begin{array}{rcrcrcrcl} x^3 & - & (x-y-z)\,x^2 & + & (yz-xy-xz)\,x & - & xyz & = 0 \\ -y^3 & - & (x-y-z)\,y^2 & - & (yz-xy-xz)\,y & - & xyz & = 0 \\ -z^3 & - & (x-y-z)\,z^2 & - & (yz-xy-xz)\,z & - & xyz & = 0 \end{array}$$

puis, en sommant :

$$x^3 - y^3 - z^3 - 3xyz = (x-y-z)\left(x^2 + y^2 + z^2 + xy + xz - yz\right).$$

Ainsi x, y, z sont solutions de l'un des deux systèmes suivants.

$$(S_1) \quad \begin{cases} x &= y + z \\ x^2 &= 2(y+z) \end{cases} \qquad (S_2) \quad \begin{cases} x^2 + \left(y^2 + z^2 - yz\right) + xy + xz &= 0 \\ x^2 &= 2y + 2z. \end{cases}$$

Pour (S_2), on pourra s'intéresser au signe de $y^2 + z^2 - yz$.