Ethan Rapport de colle semaine 3

D

Exercice 3. gro14
M. S propose l'algorithme suivant pour savoir si un entier est divisible par 7 :
Sépare en unités et dizaines puis cherche la différence entre le double des unités et les dizaines. Agis ainsi tant que tu as des dizaines sans tenir compte du signe du résultat.
Si tu obtiens 0 ou 7 alors le nombre du départ est divisible par 7
Par exemple 364 devient 28 puis 14 puis enfin 7
Qu'en pensez vous ?

On pose

$$\varphi \left| \begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} & \to & \mathbb{Z}/7\mathbb{Z} \\ \bar{x} & \mapsto & \overline{2x} \end{array} \right.$$

- φ bien définie car $\forall \bar{x} \in \mathbb{Z}/7\mathbb{Z} \quad 2 \cdot \bar{x} = \overline{2x} \in \mathbb{Z}/7\mathbb{Z}$

- Montrer que φ revient à appliquer l'algorithme
  Soit $x \in \mathbb{Z}$
  On pose $d \in \mathbb{Z}$ le nombre de dizaine de x
  $u \in [\![0 ; 9]\!]$ le nombre d'unité de x

$$\begin{aligned} \varphi(\bar{x}) &= \varphi(\overline{10d+u}) \\ &= \overline{20d+2u} \\ &= \overline{20d+2u-21d} \\ &= \overline{-d+2u} \end{aligned}$$

✓

- Montrer que

$$\varphi(\bar{x}) = \bar{0} \iff \bar{x} = \bar{0}$$

$\Rightarrow$ Soit $x \in \mathbb{Z}/7\mathbb{Z} \setminus \{\bar{0}\}$

7 premier $\Rightarrow x \wedge 7 = 1$ } par lemme de Gauß $\Rightarrow 2x \wedge 7 = 1$
$2 \wedge 7 = 1$ }

$\Rightarrow \varphi(\bar{x}) \neq 0$

$\Leftarrow$ Si $\bar{x} = \bar{0}$ alors $\varphi(\bar{x}) = \overline{2.0}$
$= \bar{0}$

L'algorithme fonctionne

Colle de la semaine 3

Adam M.

Exercice 2 :

Pour tout $x \in \mathbb{R}$, on pose $M_x = \begin{pmatrix} 1 & 0 & 0 \\ x^2 & 1 & x \\ 2x & 0 & 1 \end{pmatrix}$.

Soit $G = \{M_x \ , \ x \in \mathbb{R}\}$.

Montrer que G est un sous-groupe de $GL_3(\mathbb{R})$ isomorphe à $(\mathbb{R},+)$.

Solution :

Soit $f \left| \begin{array}{l} \mathbb{R} \to \mathcal{M}_3(\mathbb{R}) \\ x \to M_x \end{array} \right.$

Montrons que f morphisme de groupes

Soit $(x,y) \in \mathbb{R}^2$

$f(x)f(y) = M_x M_y = \begin{pmatrix} 1 & 0 & 0 \\ x^2 & 1 & x \\ 2x & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ y^2 & 1 & y \\ 2y & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ (x+y)^2 & 1 & x+y \\ 2(x+y) & 0 & 1 \end{pmatrix}$

$f(x)f(y) = M_{x+y} = f(x+y)$

Donc f morphisme de groupes

Soit $x \in Ker(f)$

$f(x) = M_x = I_3$

en particulier $[M_x]_{2,3} = x = 0 = [I_3]_{2,3}$

Donc $x = 0$

Comme $\{0\} \subset Ker(f)$, on a $Ker(f) = \{0\}$, donc f est injective

Ainsi $f^{|Im(f)}$ est isomorphisme des groupes

ou $Im(f)$ sous groupe de $\mathcal{M}_3(\mathbb{R})$

Or $Im(f) = G$ donc G est bien sous groupe de $\mathcal{M}_3(\mathbb{R})$

Montrons que $G \subset GL_3(\mathbb{R})$

Soit $M_x \in G$ où $x \in \mathbb{R}$

$\det(M_x) = \begin{vmatrix} 1 & 0 & 0 \\ x^2 & 1 & x \\ 2x & 0 & 1 \end{vmatrix} = 1 \begin{vmatrix} 1 & x \\ 0 & 1 \end{vmatrix} = 1 \neq 0$

donc $M_x \in GL_3(\mathbb{R})$

Donc G est un sous groupe de $\mathcal{M}_3(\mathbb{R})$

Lina. A.

Colle n° = 1 , S 3.

Exercice 1 :

1. Soit G un groupe cyclique de cardinal n engendré par a et $p \in \mathbb{N}^*$ un diviseur de n.
Montrer qu'il existe un unique sous-groupe de cardinal p de G et que ce sous-groupe est cyclique engendré par $a^{n/p}$.

2. En déduire en particulier que tout sous groupe d'un groupe cyclique est cyclique.

Solution :

1. $G = \langle a \rangle$, $\text{ord}(a) = n$.

comme $p \mid n$, alors $\exists q \in \mathbb{Z}$ $n = qp$.

Posons $F = \{ a \in G : a^d = e \}$.

Soit $g \in G$, alors il existe $k \in [\![0, n-1]\!]$ tel que

$$g = a^k.$$

$$g^p = e \iff a^{kp} = e.$$

$$\iff \text{ord}(a) = n \mid kp.$$

$$\iff qp \mid kp$$

$$\iff q \mid k.$$

$$\iff \exists u \in [\![0, n-1]\!] \quad k = qu.$$

Donc $F = \{ (a^q)^u : u \in [\![0, n-1]\!] \}$ ⊛

$$= \langle a^q \rangle$$

$$= \langle a^{n/p} \rangle.$$

Ainsi $|F| = n$ (d'après ⊛)

- Soit K un sous-groupe de cardinal p.

Montrons que $K = F$

Soit $k \in K$,

alors $\text{ord}(k) \mid p$

Donc $k^p = e$.

D'où $k \in F$, $K \subset F$.

Comme $|K| = |F|$ alors $K = F$.

Ainsi on obtient l'unicité d'un tel sous-groupe.

2. Soit H un sous-groupe de G un groupe cyclique.
Alors, par le théorème de Lagrange :
$d = \text{Card}(H) \mid \text{Card}(G) = n$. Posons $G = \langle a \rangle$.
Donc par ①, H est engendré par $a^{n/d}$.
Ainsi H est cyclique.

Raphaël Mouchonnet MPI semaine de colle n° 3

1) $\overline{19}$ est il inversible dans $\mathbb{Z}/49\mathbb{Z}$?

$$\begin{cases} 49 = 19\times 2 + 11 \\ 19 = 11\times 1 + 8 \\ 11 = 8\times 1 + 3 \\ 8 = 3\times 2 + 2 \\ 3 = 2\times 1 + \underline{1} \end{cases}$$

Donc $49 \wedge 19 = 1 \Longrightarrow 19 \in U(\mathbb{Z}/49\mathbb{Z})$

2) Inverse de $\overline{19}$ dans $\mathbb{Z}/49\mathbb{Z}$. On remonte l'algorithme d'euclide.

$$\begin{aligned} 1 &= 3 - 2\times 1 \\ &= 3 - (8\times 1 - 3\times 2) \\ &= 3\times(11-8) - 8 \\ &= 11\times 3 - 4\times(19 - 11\times 1) \\ &= 7\times(49 - 19\times 2) - 4\times 19 \\ &= 7\times 49 - 18\times 19 \end{aligned}$$

Donc $19\times(-18) \equiv 1\ [49]$

$\Longrightarrow \overline{19}\times\overline{-18} = \overline{1}$ dans $\mathbb{Z}/49\mathbb{Z}$

Jules R. Colle de la semaine 3

Enoncé: De combien d'éléments au minimum un groupe non-commutatif se compose-t-il?

Solution:

(A) Soit $(G,*)$ un groupe non-commutatif.

Si $\text{Card}(G)=1$, alors $G=\{e_G\}$ donc G est commutatif car:

$$e_G * e_G = e_G = e_G * e_G$$

où on note e_G le neutre du groupe $(G,*)$

Si $\text{Card}(G)=2$, alors $G=\{e_G, x_1\}$ où x_1 est son propre inverse ainsi:

$$x_1 * e_G = x_1 = e_G * x_1$$
$$\text{et} \quad e_G * e_G = e_G = e_G * e_G$$
$$\text{et} \quad x_1 * x_1 = e_G = x_1 * x_1$$

donc G est commutatif.

Si $\text{card}(G)=3$, alors on sait que e_G est d'ordre 1 et que les autres éléments sont d'ordre 3 (dû à la divisibilité de 3), ainsi:

Soit $x_1 \in G$ tel que $x_1 \neq e_G$ alors:

$$x_1^1 \neq x_1^2$$

Sinon, si $x_1^1 = x_1^2$ alors $x_1 = e_G$.

Ainsi, $G=\{e_G, x_1, x_1^2\}$ donc G est commutatif car monogène.

Si $\text{Card}(G)=4$, alors G est fait de e_G et de 3 éléments d'ordre 2 ou 4.

Disjonction de cas:

1er cas: G a un élément d'ordre 4.

2ème cas: G n'a pas d'élément d'ordre 4, donc n'a que des éléments d'ordre 2.

1er cas: Soit $x_1 \in G$ un élément d'ordre 4.

Ainsi : x_1, x_1^2 et x_1^3 sont deux à deux distincts et appartiennent à G.
Donc G est monogène donc abélien.
2ème cas : Tous les éléments de G sauf e_G sont d'ordre 2.
On a donc :

$$\forall x \in G \quad x * x = e_G$$
$$\Rightarrow \forall x \in G \quad x = x^{-1}$$

Soit $(x_1, x_2) \in G^2$

$$x_1 * x_2 = x_1^{-1} * x_2^{-1}$$
$$= (x_2 * x_1)^{-1}$$
$$= x_2 * x_1 \quad \text{car } x_2 * x_1 \in G \ (G \text{ groupe})$$

Donc G commutatif.
Si $\text{Card}(G) = 5$, alors G est fait de e_G et de 4 éléments d'ordre 5.
Soit $x_1 \in G$ différent de e_G.
Ainsi : x_1, x_1^2, x_1^3 et x_1^4 sont deux à deux distincts et appartiennent à G
Donc G est monogène donc abélien.
Si $\text{Card}(G) = 6$, on a $(S_3, \circ)$ comme candidat pour un groupe à 6 éléments non commutatif.
② Montrons que S_3 est non commutatif.
Prenons les applications suivantes appartenant à S_3 :

σ_1 | $[\![1,3]\!] \to [\![1,3]\!]$, $k \mapsto \begin{cases} 2 & \text{si } k=1 \\ 1 & \text{si } k=2 \\ 3 & \text{si } k=3 \end{cases}$ et σ_2 | $[\![1,3]\!] \to [\![1,3]\!]$, $k \mapsto \begin{cases} 3 & \text{si } k=1 \\ 2 & \text{si } k=2 \\ 1 & \text{si } k=3 \end{cases}$

Ainsi :

$$\sigma_1(\sigma_2(1)) = \sigma_1(3) = 3$$
$$\sigma_2(\sigma_1(1)) = \sigma_2(2) = 2$$
$$3 \neq 2 \quad \text{donc } (S_3, \circ) \text{ non commutatif.}$$

Nicolas H — Colle de la semaine 3

Énoncé :

A est un anneau (unitaire) fini de cardinal n ; son groupe additif est cyclique.

Mq $A \simeq \mathbb{Z}/n\mathbb{Z}$

Ce résultat persiste-t-il avec un (quasi-)anneau non unitaire ?

Indices : essayez $(2\mathbb{Z}/8\mathbb{Z})$ ou, encore plus caricatural, $(n\mathbb{Z}/n^2\mathbb{Z})$

Solution :

• $(A,+)$ étant cyclique, il existe $x \in A$ tel que

$$\langle x \rangle := \{kx : k \in [\![0, n-1]\!]\} = A$$

Soit 1_A le neutre de $(A,\times)$.

Montrons que $\langle 1_A \rangle = A$.

Soit $p = \mathrm{ord}(1_A)$, $p \in [\![1, n]\!]$ car A est fini, de cardinal n.

$$p \times x = 1_A \times p \times x = (1_A \times p)\, x$$

$$= \underbrace{(1_A + \cdots + 1_A)}_{\mathrm{ord}(1_A) = p}\, x$$

$$= 0 \times x$$

$$= 0$$

or, $\mathrm{ord}(x) = n$, car x engendre A.

Comme $p \in [\![1, n]\!]$, $p = n$.

Donc $\langle 1_A \rangle = A$

Soit $\varphi \mid \mathbb{Z}/n\mathbb{Z} \longrightarrow A$

$\overline{k} \longmapsto k \times 1_A$

Montrons que φ est bien définie et est un isomorphisme d'anneaux.

Bien définie :

Soit $(k_1, k_2) \in \mathbb{Z}^2$ tels que $\overline{k_1} = \overline{k_2}$

alors $k_1 \equiv k_2 \ [n]$ donc il existe $q \in \mathbb{Z}$ tel que $k_1 = k_2 + qn$.

$\varphi(\overline{k_1}) = (k_1 \times 1_A) = (k_2 +_A qn) \times_A 1_A$

$= k_2 \times_A 1_A$

$= \varphi(\overline{k_2})$

Morphisme d'anneau :

- $\varphi(\overline{1}) = 1_{\mathbb{Z}} 1_A = 1_A$
- Soit $(\overline{x}, \overline{y}) \in \mathbb{Z}/n\mathbb{Z}^2$

$\varphi(\overline{x} + \overline{y}) = (x +_A y) \times 1_A$

$= x \times_A 1_A + y \times_A 1_A$

$= \varphi(\overline{x}) +_A \varphi(\overline{y})$

- Soit $(\overline{k_1}, \overline{k_2}) \in \mathbb{Z}/n\mathbb{Z}^2$

$\varphi(\overline{k_1} \times \overline{k_2}) = \varphi(\overline{k_1 \times k_2})$

$= k_1 \times_A k_2 \times_A 1_A$

$= k_1 \times_A 1_A \times k_2 \times_A 1_A$ (1_A neutre pour $\times$)

$= \varphi(\overline{k_1}) \times_A \varphi(\overline{k_2})$

- Montrons que φ est bijective
  - Soit $(\overline{k_1}, \overline{k_2}) \in \mathbb{Z}/n\mathbb{Z}^2$ tels que $\varphi(\overline{k_1}) = \varphi(\overline{k_2})$

$\varphi(\overline{k_1}) = \varphi(\overline{k_2}) \Rightarrow k_1 \times 1_A = k_2 \times 1_A$

$\Rightarrow k_1 = k_2$

$\Rightarrow \overline{k_1} = \overline{k_2}$

- $|\mathbb{Z}/n\mathbb{Z}| = n$ et $|A| = n$. φ est injective

Par cardinalité - dimension, φ est bijective

- Un anneau non unitaire ne possède pas de neutre pour $\times$
- Donc $\forall f \in \mathcal{L}(A, \mathbb{Z}/n\mathbb{Z})$

f ne respecte pas la condition des unités pour $\times$. Donc f n'est pas un morphisme d'anneau

Alexandre M.

Colle S3

Enoncé :

Soit $(G,*)$ un groupe et H un sous-groupe strict de G.

Déterminer le sous-groupe engendré par $G \setminus H$

Solution :

Comme H est un sous-groupe strict de G,

on a $H \neq G$ donc $G \setminus H \neq \emptyset$

on pose $(G \setminus H)^{-1} := \{ a^{-1} : a \in G \setminus H \}$

on a $\langle G \setminus H \rangle = \{ g \in G : \exists n \in \mathbb{N}^* \exists (a_1, \dots, a_n) \in (G \setminus H) \cup (G \setminus H)^{-1}$

$g = a_1 * \dots * a_n \}$

[caractérisation des sous-groupes engendrés]

On conjecture, en prenant $(G,*) = (\mathbb{Z},+)$ et $H = 2\mathbb{Z}$, que $\langle G \setminus H \rangle = G$

Montrons ce résultat en toutes généralités :

Montrons $\langle G \setminus H \rangle = G$

[C] clair car $\langle G \setminus H \rangle$ sous-groupe de G [bien défini car $G \setminus H \neq \emptyset$ et $G \setminus H \subset G$]

[D] Soit $g \in G$

Comme $G \setminus H \neq \emptyset$, $\exists \beta \in G \setminus H \subset G$

on note que β, en tant qu'élément de G, possède un inverse noté β^{-1}

On a (*) $g = \beta^{-1} * (\beta * g)$ [* asso]

- on remarque $\beta^{-1} \in G \setminus H$

(dans le cas contraire $\beta = (\beta^{-1})^{-1} \in H$ ↯)

Montrons $\beta * g \in G \setminus H$, par l'absurde

Supposons $\beta * g \in H$

alors $\beta * g * g^{-1} \in H$ ($g \in H$ sous-groupe et stabilité de H par $*$)

donc $\beta \in H$ ↯

(*) livre $g = \underbrace{\beta^{-1}}_{\in G \setminus H} * \underbrace{(\beta * g)}_{\in G \setminus H}$

D'après la description de $\langle G \setminus H \rangle$, $g \in \langle G \setminus H \rangle$

donc $\boxed{\langle G \setminus H \rangle = G}$ q.e.d.

Louis Guillaume S.

Feuille de la semaine 1

EXERCICE 1

Soient $(G, *)$ un groupe fini de cardinal n et m un entier premier à n.

Démontrer que, pour tout $a \in G$, l'équation :

$$x^m = a$$

d'inconnue $x \in G$, possède une unique solution. □

Solution : Pour démontrer ce résultat nous pouvons considérer une application

$$\varphi \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & x^m \end{array} \right. \quad \text{et montrer qu'elle est bijective.}$$

- Le caractère bien défini est clair car $x^m = \underbrace{x * \dots * x}_{m \text{ fois}} \in G$
- Comme G est de cardinal fini $n \geq 1$, il suffit de montrer que φ est injective pour qu'elle soit bijective.
- **Injectivité** : Démontrons l'injectivité de φ en nous ramenant à la définition.

  Soit $(x_1; x_2) \in G^2$ tel qu'on suppose $\varphi(x_1) = \varphi(x_2)$. Montrons que $x_1 = x_2$.

  $\Rightarrow {x_1}^m = {x_2}^m$

  Comme $n \wedge m = 1$, nous savons d'après le théorème de Bezout que :

  $\exists (u; v) \in \mathbb{Z}^2 \quad mu + nv = 1$

  $\Rightarrow ({x_1}^m)^u = ({x_2}^m)^u$

  $\Rightarrow (x_1)^{1-nv} = (x_2)^{1-nv}$

  $\Rightarrow (x_1) * (\underbrace{{x_1}^n}_{e_G})^{-v} = (x_2) * (\underbrace{{x_2}^n}_{e_G})^{-v}$ où e_G est le neutre de $(G, *)$

  $\Rightarrow x_1 = x_2$ [G de cardinal n]

Conclusion : Ainsi par égalité des cardinaux de la source et du but de φ, étant injective elle est également bijective.

Ainsi, nous pouvons affirmer que $\forall a \in G, \ \exists! x \in G \quad \varphi(x) = x^m = a$

Stanislas G

Semaine de colle n°3

EXERCICE 1

Soient $(G, *)$ un groupe fini de cardinal n et m un entier premier à n.

Démontrer que, pour tout $a \in G$, l'équation :

$$x^m = a$$

d'inconnue $x \in G$, possède une unique solution.

Solution :

Comme $n \wedge m = 1$ par Bézout $\exists (u,v) \in \mathbb{Z}^2$ $un + mv = 1$

De plus comme G fini

$\forall x \in G$ $\text{ord}(x) \mid n \Rightarrow \exists q \in \mathbb{Z}$ $n = q\,\text{ord}(x)$

donc $a^{un+mv} = a$

$= a^{un} * a^{mv} = a$

$= \underbrace{a^{u\,q\,\text{ord}(x)}} * (a^v)^m = a$

$= (\underbrace{a^v}_{x})^m = a$

donc $x^m = a$ possède au moins une solution : a^v

Rapport de Colle, semaine n°4

MAKNE
W.

Pun nombre premier

$$\mathbb{Z}_p = \left\{ \frac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{N}^* \text{ et } p \nmid b \right\}$$

$$J_p = \left\{ \frac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{N}^* \text{ et } p \nmid b \text{ et } p \mid a \right\}$$

1) Montrer que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$
2) Montrer que J_p est un idéal de $\mathbb{Z}_p$
3) Montrer que tout idéal autre que $\mathbb{Z}_p$ est inclus dans J_p de $\mathbb{Z}_p$

1)

- $1 = \frac{b}{b}$ avec $b \in \mathbb{N}^* \subset \mathbb{Z}$ et $p \nmid b$

- Stabilité par somme tordue :

Soit $(x, y) \in \mathbb{Z}_p^2$ alors $\exists (a_1, a_2, b_1, b_2) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \times \mathbb{N}^*$

tel que $p \nmid b_1$ et $p \nmid b_2$, $x = \frac{a_1}{b_1}$ $y = \frac{a_2}{b_2}$

$$x - y = \frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{\overbrace{a_1 b_2 - a_2 b_1}^{\in \mathbb{Z}}}{\underbrace{b_1 b_2}_{\in \mathbb{N}^*}} \quad \text{et} \quad p \nmid b_1 b_2 \text{ (Théorème de Gauss)}$$

1 - Stabilité par produit :

Soit $(x,y) \in \mathbb{Z}_{(p)}^2$ $\exists (a_1, a_2, b_1, b_2) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}^*\times\mathbb{N}^*$ tel que

$p \nmid b_1$, $p \nmid b_2$ et $x = \frac{a_1}{b_1}$ $y = \frac{a_1}{b_2}$

$x \times y = \underbrace{\frac{a_1 a_2}{b_1 b_2}}_{\substack{\in\mathbb{Z} \\ \in\mathbb{N}^*}}$ de même $p \nmid b_1 b_2$

2) Il suffit de montrer que $\mathcal{I}_p$ est un sous groupe de $\mathbb{Z}$

. $\mathcal{I}_p$ non vide car $0 = \frac{0}{b}$ avec $b \in \mathbb{N}^*$ $p \nmid b$ et $p \mid 0$

. Soit $(x,y) \in \mathcal{I}_p$ $\exists (a_1, a_2, b_1, b_2) \in \mathbb{N}^* \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}^*\times\mathbb{N}^*$

tel que $p \mid a_1$, $p \mid a_2$, $p \nmid b_1$, $p \nmid b_2$ et $x = \frac{a_1}{b_1}$ $y = \frac{a_2}{b_2}$

$x - y = \underbrace{\frac{\overbrace{a_1 b_2}^{\in\mathbb{Z}} - \overbrace{a_2 b_1}^{\in\mathbb{Z}}}{b_1 b_2}}_{\in\mathbb{N}^*}$

Par le théorème de Gauss $p \mid a_1 b_2$, $p \mid a_2 b$, et $p \nmid b_1 b_2$

3). Soit I idéal de $\mathbb{Z}_{(p)}$ non inclus dans $\mathcal{I}_p$

Soit $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tq $\frac{a}{b} \in I$ et $p \nmid a$, $p \nmid b$

alors $\frac{b}{a} \in \mathbb{Z}_{(p)}$, par absorbance $\frac{a}{b} \times \frac{b}{a} = 1 \in I$

si I contient 1 alors par absorbance il contient tous les

éléments de $\mathbb{Z}_{(p)}$ donc $I = \mathbb{Z}_{(p)}$

. Si $I \subset \mathcal{I}_p$ ✓

Robin G- Colle de la semaine 3

Soit $(A,+,\times)$ un anneau.
Soient x et y deux éléments nilpotents de A tels que $x \times y = y \times x$. Montrer que $x \times y$ et $x+y$ sont nilpotents.

• Soit $n \geq 2$ décomposé en produit de facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.
Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$?

1) Soient $(n,m) \in \mathbb{N}^{*2}$ tq $x^n = 0_A$ et $y^m = 0_A$.

• $(xy)^n = x^n y^n = 0_A y^n = 0_A$

• $(x+y)^{n+m} = \sum_{h=0}^{n+m} \binom{n+m}{h} x^h y^{n+m-h}$ (x et y commutent)

Soit $h \in [\![0, n+m]\!]$:
si $h \geq n$, $x^h = 0_A$ et $\binom{n+m}{h} x^h y^{n+m-h} = 0$

si $h \leq n$, $n+m-h \geq m$, $y^{n+m-h} = 0_A$ et $\binom{n+m}{h} x^h y^{n+m-h} = 0$

Donc tous les termes de la somme sont nuls, $(x+y)^{n+m} = 0_A$

2) Soit $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. Montrons :

$\exists p \in \mathbb{N}^* \ \bar{x}^p = \bar{0} \iff \exists q \in \mathbb{Z} \ x = q \prod_{i=1}^{k} p_i$

$\Leftarrow$ Soit $q \in \mathbb{Z}$ tq $x = q \prod_{i=1}^{k} p_i$.

On pose $p := \max\{\alpha_i \mid i \in [\![1,k]\!]\} \in \mathbb{N}^*$.

$$x^p = \underbrace{q^p \prod_{i=1}^{k} p_i}_{\in \mathbb{Z}} \cdot \underbrace{\prod_{i=1}^{k} p_i^{\alpha_i}}_{= n}$$

Donc $\overline{x^p} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$.

$\Rightarrow$ Soit $p \in \mathbb{N}^*$ tel que $\overline{x^p} = \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$.
Si $x = 0$, le résultat est clair.
On pose la décomposition en produit de facteurs premiers de x :

$$x = \prod_{i=1}^{m} q_i^{\beta_i}, \text{ où } m \in \mathbb{N}^*$$
$$q_1, \dots, q_m \in \mathcal{P}$$
$$\beta_1, \dots, \beta_m \in \mathbb{N}^*$$

$\overline{x^p} = \overline{0}$ donc n divise x^p.
Donc
$$\exists q \in \mathbb{Z} \quad x^p = q \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{m} q_i^{\beta_i + p}$$

Par unicité de la décomposition en produit de facteurs premiers, $k \leq m$ et
$$\forall i \in [\![1,k]\!] \ \exists! j \in [\![1,m]\!] \ p_i = q_j \text{ et } \alpha_i \leq \beta_j + p$$

en posant $J = \{j \in [\![1,m]\!] : \exists i \in [\![1,k]\!] \ p_i = q_j\} \subset [\![1,m]\!]$ et $|J| \leq k$

$$x = \prod_{j \in J} q_j \cdot \left(\prod_{j \in J} q_j^{\beta_j - 1} \cdot \prod_{i \in [\![1,m]\!] \setminus J} q_i^{\beta_i} \right)$$

$$x = \prod_{i=1}^{k} p_i \cdot y, \quad y \in \mathbb{Z}$$

Donc x est nilpotent $\Leftrightarrow \prod_{i=1}^{k} p_i$ divise x (dans $\mathbb{Z}/n\mathbb{Z}$).

Pierre V. Colle de la semaine 3

Exercice 2 : Soit A une algèbre intègre sur $\mathbb{R}$ de dimension finie $n \geqslant 2$. Dans la suite, on assimile $\mathbb{R}$ à $\mathbb{R}.1$ où 1 est l'élément neutre de A pour le produit.

1. Montrer que tout élément non nul de A est inversible.
   Indication : Pour a élément non nul de A, considérer l'application définie sur A : $x \mapsto ax$.
2. Soit a un élément de A non situé dans $\mathbb{R}$. Montrer que $(1, a)$ est libre tandis que $(1, a, a^2)$ est liée.
   Indication : Pour montrer que la famille $(1, a, a^2)$ est liée, considérer la famille $(1, a, .., a^n)$.
3. En déduire l'existence d'un élément i_A de A tel que $i_A^2 = -1$.
4. Montrer que si A est commutative alors A est isomorphe à $\mathbb{C}$.
   Indication : Commencer par prouver que $n = 2$.

Solution

1) Soit $a \in A \setminus \{0_A\}$, posons $\varphi \left| \begin{array}{ccc} A & \to & A \\ x & \mapsto & ax \end{array} \right.$

*) Soit $(u,v) \in A^2$, $(\lambda,\mu) \in \mathbb{R}^2$ $\varphi(\lambda u + \mu v) = a(\lambda u + \mu v) = \lambda \underbrace{au}_{\varphi(u)} + \mu \underbrace{av}_{\varphi(v)}$

donc φ est linéaire

*) Soit $x \in \ker(\varphi)$, $\varphi(x) = \underbrace{a}_{\neq 0_A} x = 0$, par intégrité de A, $x = 0$

On a clairement $\{0_A\} \subset \ker(\varphi)$. Donc $\ker(\varphi) = \{0_A\}$, ainsi φ est injective

*) φ est un endomorphisme et A est de dimension finie donc φ est surjective

· $1_A \in A$ donc $\exists b \in A$ $\varphi(b) = ab = 1_A$

de plus, $\varphi(ba) = \underbrace{ab}_{=1_A} a = a$ et $\varphi(1_A) = a 1_A = a$

Par injectivité de φ $ba = 1_A$.

Ainsi a est inversible

2) $a \neq 0$ sinon $a = 0 = 0.1 \in \mathbb{R}$ ↯ Donc $1 \neq 0$ et $a \neq 0$

·) Supposons que $(1,a)$ est liée, $\exists (\lambda_1, \lambda_2) \in \mathbb{R}^2 \setminus \{(0,0)\}$ tel que $\lambda_1 . 1 + \lambda_2 . a = 0$

$\lambda_2 . a = -\lambda_1 . 1$, si $\lambda_2 = 0$, alors $\lambda_1 = 0$, il y a contradiction,

si $\lambda_2 \neq 0$, $a = -\frac{\lambda_1}{\lambda_2} . 1 \in \mathbb{R}$, il y a contradiction.

donc $(1,a)$ est libre

• $(1, a, \dots, a^n)$ a $n+1 > \dim(A)$ vecteurs donc est liée,
$\exists (\nu_0 \dots \nu_n) \in \mathbb{R}^{n+1} \setminus \{(0\dots0)\}$ tel que $\sum_{i=0}^{n} \nu_i a^i = 0$
Posons le polynome $P = \sum_{i=0}^{n} \nu_i X^i \in \mathbb{R}[X]$
On a donc $P(a) = 0$.
P peut se decomposer en produit de facteurs irreductibles de degré 1 ou 2. Donc il existe un facteur irreductible Q dont a est racine. Q n'est pas de degré 1 car $(1, a)$ est libre donc Q est de degré 2. Donc $\exists (\nu_0, \nu_1) \in \mathbb{R}^2$ tel que (F) et
$Q = X^2 + \nu_1 X + \nu_0$ ainsi $Q(a) = a^2 + \nu_1 a + \nu_0 = 0$
donc $(1, a, a^2)$ est liée. (F) $\Delta = \nu_1^2 - 4\nu_0 < 0$

3) $Q(a) = a^2 + \nu_1 a + \nu_0 = 0$ (on reprend le a introduit en 2))
donc $\left(a + \frac{\nu_1}{2}\right)^2 - \frac{\nu_1^2 - 4\nu_0}{4} = 0$
donc $\left(a + \frac{\nu_1}{2}\right)^2 = \frac{\nu_1^2 - 4\nu_0}{4} = -\left(\frac{4\nu_0 - \nu_1^2}{4}\right)$
<0 par (F) $\quad >0$
donc $\left(\frac{2a + \nu_1}{\sqrt{4\nu_0 - \nu_1^2}}\right)^2 = -1$
donc $i_a = \frac{2a + \nu_1}{\sqrt{4\nu_0 - \nu_1^2}} \in \mathrm{Vect}(1, a)$

4) Supposons que $n > 2$, $\exists (a, b) \in A^2$ tel que $(1, a, b)$ est libre,
De l'étude precedente, on peut introduire $i_a \in \mathrm{Vect}(1, a)$ et $i_b \in \mathrm{Vect}(1, b)$ tel que $i_a^2 = -1$ et $i_b^2 = -1$, on a donc $i_a^2 - i_b^2 = (i_a - i_b)(i_a + i_b) = 0$
(A commutative)
donc par integrité de A, $i_a = i_b$ ou $i_a = -i_b$
donc $\mathrm{Vect}(1, i_a) = \mathrm{Vect}(1, i_b)$ donc $(a, b) \in \mathrm{Vect}(1, i_a)^2$, donc $(1, a, b)$ n'est pas libre, il y a contradiction. Donc $n = 2$.
Posons $\varphi \mid A \to \mathbb{C}$, $x = a \cdot 1_A + b \cdot i_a \to a \cdot 1_{\mathbb{C}} + b i$ est un isomorphisme de $\mathbb{C}$ (car image de A donne une base de $\mathbb{C}$)
est linéaire et injective car $(\varphi(1_A), \varphi(i_a))$ $= 1_{\mathbb{C}}$ $\quad = i$

MATHEO.N

Rapport de colle S3

Exercice 12. Soit $n \in \mathbb{N}^*$. On note d le nombre de diviseurs de n et N le produit de tous les diviseurs de n.

Montrer que $N^2 = n^d$.

On introduit $Div(n) = \{a \in [\![1, n]\!] : \exists q \in [\![1,n]\!] \ aq = n\}$ (partie non vide de $\mathbb{N}$) l'ensemble des diviseurs de n, nous avons $d = |Div(n)|$

Nous avons alors :

$$N^2 \overset{(*)}{=} \left(\prod_{a \in Div(n)} a \right)^2$$

Soit $\varphi \left| \begin{array}{ccc} Div(n) & \longrightarrow & Div(n) \\ a & \longmapsto & \frac{n}{a} \end{array} \right.$

- bien définie car : $\frac{n}{a} \times a = n$ avec $\frac{n}{a} \in \mathbb{N}$ $(a \in Div(n))$
- est bijective étant sa propre réciproque :
  Soit $a \in Div(n)$ $\varphi(\varphi(a)) = \varphi\left(\frac{n}{a}\right) = \frac{n}{\frac{n}{a}} = a$.

Ainsi nous avons par changement d'indice $a \leftrightarrow \varphi(a)$ dans l'une des deux produit :

$$N^2 = \left(\prod_{a \in Div(n)} a \right) \times \left(\prod_{a \in Div(n)} \varphi(a) \right)$$

$$= \left(\prod_{a \in Div(n)} a \times \frac{n}{a} \right)$$

$$= \prod_{a \in Div(n)} n \qquad [|Div(n)| = d]$$

$$= n^d$$

Ainsi : $\boxed{N^2 = n^d}$

Léon

Rapport de colle de la semaine n°1

Soit $(A,+,\times)$ anneau fini unitaire de cardinal n ; $(A,+)$ cyclique.
Montrer que $A \simeq \mathbb{Z}/n\mathbb{Z}$ au sens d'anneau.

Ce résultat persiste-t-il lorsque l'anneau n'est pas unitaire ?

Solution : on commence par montrer que $\langle 1_A \rangle = A$.
On a $\langle 1_A \rangle \subset A$
Par le théorème de Lagrange $\text{CARD}(\langle 1_A \rangle) \mid \text{Card}(A) = n$

Soit $a \in A$ $\langle a \rangle = A$.
Ainsi il existe $l \in \mathbb{N}$ tel que $1_A = la$

$$\underbrace{1_A + \dots + 1_A}_{n \text{ fois}} = n1_A = \underbrace{la + \dots la}_{n \text{ fois}}$$

$$= \underbrace{na + \dots + na}_{l \text{ fois}}$$

On $\text{ord}(a) = \text{Card}(\langle a \rangle) = n$
ainsi $n1_A = 0$
On en déduit que $n \mid \text{ord}(1_A) = \text{Card}(\langle 1_A \rangle)$
Par antisymétrie de $\mid$, $\text{Card}(A) = \text{Card}(\langle 1_A \rangle)$

Par inclusion et égalité des cardinaux $A = \langle 1_A \rangle$

Ainsi $\varphi \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & A = \langle 1_A \rangle \\ \bar{\ell} & \longmapsto & \ell 1_A \end{array} \right.$ est bien définie et

est un isomorphisme de groupes (pour la loi $+$), par classification des groupes monogènes, dans le cas fini.

- multiplicativité : soit $(\bar{k}, \bar{\ell}) \in (\mathbb{Z}/n\mathbb{Z})^2$

$$\begin{aligned} \varphi(\bar{k}\bar{\ell}) &= \varphi(\overline{k\ell}) \\ &= k\ell 1_A \\ &= k 1_A \times \ell 1_A \\ &= \varphi(\bar{k}) \times \varphi(\bar{\ell}) \end{aligned}$$

1_A commute

$\times$ associative

1_A neutre (mériterait une récurrence)

- caractère unitaire :

$$\varphi(\bar{1}) = 1 1_A = 1_A$$

Ainsi φ est un isomorphisme d'anneaux unitaires.

$$A \simeq \mathbb{Z}/n\mathbb{Z}$$

REUTER Robin

Copie du 18/09

Exercice 6. gro43 **Centrale**

Soit G un groupe fini. Pour $a \in G$, posons

$$\Phi_a \mid \begin{array}{ccc} G & \longrightarrow & G \\ x & \longrightarrow & a \cdot x \cdot a^{-1} \end{array}$$

1. Démontrer que Φ_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 des automorphismes de G.
3. Supposons I cyclique. Démontrer que G est commutatif.

Ex 6 :

1. • $\forall x \in G$, $a \cdot x \cdot a^{-1} \in G$
donc ϕ_a est bien définie.

• $\phi_a(e_G) = a \cdot e_G \cdot a^{-1} = e_G$

• Soit $(x, y) \in G$.
$\phi_a(x \cdot y) = a \cdot x \cdot y \cdot a^{-1}$
$= a \cdot x \cdot a^{-1} \cdot a \cdot y \cdot a^{-1}$.
$= \phi_a(x) \cdot \phi_a(y)$.

Donc ϕ_a est bien un morphisme de groupe.

Soit $x \in \ker(\phi_a)$.
$\phi_a(x) = a \cdot x \cdot a^{-1} = e_G$
donc $x \cdot a^{-1} = a^{-1}$
puis $x = e_G$.
Ainsi ϕ_a est injective.

Puisque G est de cardinal fini, ϕ_a est bijective et sa réciproque est $\phi_{a^{-1}}$.

2. En notant $(E, \circ)$ le groupe des automorphisme de G, on a :

- $I \subset E$ par la question 1.
- $id \in I$ car $id = \phi_{e_G}$
- Soit $(a, b) \in G^2$ tel que $(\phi_a, \phi_b) \in I^2$.

Soit $x \in G$,

$$\begin{aligned}(\phi_a \circ \phi_b^{-1})(x) &= \phi_a(\phi_{b^{-1}}(x)) \\ &= \phi_a(b^{-1} \cdot x \cdot b) \\ &= a \cdot b^{-1} \cdot x \cdot b \cdot a^{-1} \\ &= \phi_{a \cdot b^{-1}}(x)\end{aligned}$$

car $(a \cdot b^{-1})^{-1} = b \cdot a^{-1}$

Ainsi, $(\phi_a \circ \phi_b^{-1}) \in I$.

Donc I est ss-groupe de $(E, \circ)$.

3. I est cyclique.

Donc $\exists\, \alpha \in G$ tel que $\langle \phi_\alpha \rangle = I$.

Soit $(a, b) \in G^2$, $(\phi_a, \phi_b) \in I^2$.

Alors, $\exists\, (n, m) \in (\mathbb{N}^*)^2$ tel que $\phi_a = \phi_\alpha^{\,n}$ et $\phi_b = \phi_\alpha^{\,m}$.

On a donc,

$$\begin{aligned}\phi_a \circ \phi_b &= \phi_\alpha^{\,n+m} \quad \text{or } n+m \in \mathbb{Z} \\ &= \phi_\alpha^{\,m+n} \\ &= \phi_b \circ \phi_a\end{aligned}$$

Donc I est commutatif.

$$\begin{aligned}\phi_a \circ \phi_b &= \phi_b \circ \phi_a \\ &= \phi_{a \cdot b} \\ &= \phi_{b \cdot a}\end{aligned}$$

Donc $a \cdot b = b \cdot a$.

Ainsi G est commutatif.

MANGIALOMINI
Aurélien

Rapport de Colle 53

MANGIALOMINI Aurélien

Question de cours. Classification des groupes monogènes.

Exercice. Soient G un groupe et H_1, H_2 deux sous-groupes de G.

1. On suppose que $H_1 \cup H_2$ est un sous-groupe de G. Montrer : $H_1 \subseteq H_2$, ou : $H_2 \subseteq H_1$.
2. On suppose que les cardinaux de H_1 et H_2 sont finis et premiers entre eux. Décrire $H_1 \cap H_2$.

Exercice. Soit $\mathbb{D} = \left\{ \frac{a}{10^n} \mid (a,n) \in \mathbb{Z} \times \mathbb{N} \right\}$ l'ensemble des nombres décimaux. Montrer que $\mathbb{D}$ est un anneau commutatif et décrire ses idéaux.

Traiter les exercices dans l'ordre indiqué.

$(\mathbb{D}, +, \times)$ anneau commutatif ( )

$\mathbb{D}$ anneau : $0 = \frac{0}{10^0} \in \mathbb{D}$

$1 = \frac{1}{10^0} \in \mathbb{D}$

Soit $x_1, x_2 \in \mathbb{D}^2$ donc $\exists\, a_1, n_1 \in \mathbb{Z} \times \mathbb{N}$
$a_2, n_2 \in \mathbb{Z} \times \mathbb{N}$

tq $x_1 = \frac{a_1}{10^{n_1}}$ quitte à échanger on peut supposer $n_1 \geq n_2$
$x_2 = \frac{a_2}{10^{n_2}}$

on a $x_1 + x_2 = \frac{a_1 + 10^{n_1 - n_2} a_2}{10^{n_1}} \in \mathbb{Z}$ ($10^{n_1} \in \mathbb{N}$)

$= x_2 + x_1$ (comm. dif.)

$x_1 x_2 = \frac{a_1 a_2}{10^{\underbrace{n_1 + n_2}_{\in \mathbb{N}}}} \in \mathbb{Z} = x_2 x_1$ (comm. dif.)

Donc $(\mathbb{D}, \times, +)$ est un anneau commut. dif.

Corollaire : soit I un idéal de $\mathbb{D}$
$\exists ! \, a \in \mathbb{Z}$ tq $I = a\mathbb{D}$

Soit I un idéal de $\mathbb{D}$

$I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc
$\exists ! \, a \in \mathbb{Z}$ tq $I \cap \mathbb{Z} = a\mathbb{Z}$

$I \boxed{\supset} a\mathbb{D}$

$a \in I \cap \mathbb{Z} \subset I$ donc $a \in I$.
Par absorption on conclut $a\mathbb{D} \subset I$.

$I \boxed{\subset} a\mathbb{D}$
Soit $x \in I$ donc $\exists a, n \in \mathbb{Z} \times \mathbb{N}$ tq
$x = \frac{a}{10^n}$

donc $10^n \underbrace{x}_{\in I} \in \mathbb{Z}$ et $\in I$ par absorption

donc $10^n x \in \mathbb{Z} \cap I = a\mathbb{Z}$

donc $\exists q \in \mathbb{Z}$ tq $10^n x = aq$

ie $x = a \underbrace{\frac{q}{10^n}}_{\in \mathbb{D}} \in \mathbb{Z}$

donc $I \subset a\mathbb{D}$.

Ibrahim K.

Rapport de Colle de la semaine 1.

Exercice 1 :

On considère un groupe $(G,*)$ d'élément neutre e tel que $\forall x \in G, x * x = e$.

1. Montrer que G est commutatif.
2. Montrer que $H = (\mathbb{Z}/2\mathbb{Z})^n$ vérifie cette condition.

1- Soit $(x,y) \in G^2$

On considère

$$x * y = y * (y * x) * (y * x) * x$$

($*$ est associative)

$$= y * e * x$$

$$= y * x$$

2- on a $H = (\mathbb{Z}/2\mathbb{Z})^n = \{\bar{0}, \bar{1}\}^n$

Soit $x \in (\mathbb{Z}/2\mathbb{Z})^n$

ainsi

$$\exists (x_1, \dots, x_n) \in \{\bar{0}, \bar{1}\}^n \text{ tq } x = (x_1, \dots, x_n)$$

on remarque que $\bar{0} + \bar{0} = \bar{0}$

$\bar{1} + \bar{1} = \bar{2} = \bar{0}$

ainsi $\forall i \in [\![1, n]\!] \quad x_i + x_i = \bar{0} \quad (x_i \in \{\bar{0}, \bar{1}\})$

donc $x + x = (\bar{0}, \dots, \bar{0})$

$(\mathbb{Z}/2\mathbb{Z})^n$ vérifie bien la condition

Paul C. Colle de la semaine 3.

Enoncé :

Déterminer les sous groupes finis de $\mathbb{C}^*$ et $\mathbb{R}^*$

Solution :

1) Sous groupes finis de $(\mathbb{C}^*, \times)$.

On raisonne par analyse et synthèse.

Analyse :

Soit G_1 sous groupe fini de $(\mathbb{C}^*, \times)$, $n := \mathrm{Card}(G_1)$.

G_1 est fini donc $\forall x \in G_1$, x est d'ordre fini, et $\underline{\mathrm{ord}(x)} \mid \mathrm{Card}(G_1) = n$.

donc $\forall x \in G_1$, $x^n = 1$. ($\mathrm{Card}(\langle x \rangle)$ sous groupe de G_1, Théorème de Lagrange)

Alors $\forall x \in G_1$, $x \in \mathbb{U}_n$ i.e. $G_1 \subset \mathbb{U}_n$.

de plus $\mathrm{Card}(\mathbb{U}_n) = \mathrm{Card}(G_1) = n$, d'où $G_1 = \mathbb{U}_n$.

Synthèse

Soit $n \in \mathbb{N}^*$, montrons $\mathbb{U}_n$ sous groupe fini de $(\mathbb{C}^*, \times)$

- $\mathbb{U}_n = \{ e^{i\frac{2k\pi}{n}} : k \in [\![0, n-1]\!] \}$ fini, $\mathbb{U}_n \subset \mathbb{C}^*$
- $1 \in \mathbb{U}_n$ $\left(1 = e^{i\frac{2\times 0 \times \pi}{n}}\right)$
- Soient $(z_1, z_2) \in \mathbb{U}_n$. $\exists (k_1, k_2) \in [\![0, n-1]\!]^2$: $z_1 = e^{i\frac{2k_1\pi}{n}}$, $z_2 = e^{i2k_2\pi/n}$.

$$z_1 \times z_2^{-1} = e^{i2k_1\pi/n} \times e^{-i2k_2\pi/n}$$
$$= e^{i2(k_1-k_2)\pi/n}.$$

Soit $\ell \in [\![0, n-1]\!]$: $\ell = k_1 - k_2 \ [n]$. $\exists p \in \mathbb{Z}$: $\ell = k_1 - k_2 + pn$.

$$z_1 \times z_2^{-1} = e^{i2(\ell - pn)\pi/n}$$
$$= e^{i2\ell\pi/n} \times \underbrace{e^{-i2\pi p}}_{=1}$$
$$= e^{i2\ell\pi/n} \in \mathbb{U}_n.$$

$\mathbb{U}_n$ est un sous groupe fini de $(\mathbb{C}^*, \times)$

Conclusion : L'ensemble des sous groupes finis de $(\mathbb{C}^*, \times)$ sont : $\{ \mathbb{U}_n : n \in \mathbb{N}^* \}$.

Sous groupes de $(\mathbb{R}^*, \times)$: tout sous groupe de $(\mathbb{R}^*, \times)$ est sous groupe de $(\mathbb{C}^*, \times)$.

L'ensemble des sous groupes finis de $(\mathbb{R}^*, \times)$ est donc

$\{U_n : n \in \mathbb{N}^*, U_n \subset \mathbb{R}\} =$ ~~$\{U_1, U_2\}$~~

$= \{U_1, U_2\}$.

Célia A.

Semaine n°3

Colle n°1

Combien existe-t-il de structures de groupe à 6 éléments différentes ; donnez un exemple de chacune.

Posons G un ensemble à six éléments : 1, 2, 3, 4, 5 et 6. On munit G d'une loi de composition interne *, et (G, *) est un groupe dont le neutre est 1.

Comme G est un groupe de cardinal fini, tous ses éléments sont d'ordre fini.

On peut alors supposer que G possède un élément d'ordre 6, noté x. Le sous-groupe engendré par cet élément est de cardinal 6. Or, puisque <x> est inclus dans G et Card(<x>) = Card(G), <x> = G. Ainsi, G est cyclique et est isomorphique à $\mathbb{Z}/6\mathbb{Z}$.

Supposons maintenant que G ne possède aucun élément d'ordre 6.

Par l'absurde, supposons que G ne possède aucun élément d'ordre 3. Selon le théorème de Lagrange, tous ses éléments sont alors d'ordre 2 ou 1, car les sous-groupes qu'ils engendrent doivent avoir des cardinaux divisant 6. Or, le neutre est l'unique élément d'ordre 1.

Montrons que H = (1, 2, 3, 2*3) est un sous-groupe de G.

H contient l'élément neutre.

Montrons que H est stable par produit :

*	**1**	**2**	**3**	**2*3**
1	1	2	3	2*3
2	2	1	2*3	3
3	3	2*3	1	2
2*3	2*3	3	2	1

De plus, $\forall\, x \in H \;\; x^2 = 1$. Donc $\forall\, x \in H \;\; x^{-1} = x$, et H est stable par passage au symétrique.

Par conséquent, H est un sous-groupe de G de cardinal 4, ce qui n'est pas car 4 ne divise pas 6.

Ainsi, G possède au moins un élément d'ordre 3, noté 6. Pour que 6 puisse avoir un inverse dans G, G doit posséder un autre élément d'ordre 3, noté 5. Réalisons alors la table du groupe.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	6	* 3	4
3	3	6	1	5	4	2
4	4	5	6	1	2	3
5	5	4	2	3	6	1
6	6	* 3	4	2	1	5

6*6*6 = 1 et 6*5 = 1, donc 6*6 = 5 (raisonnement analogue pour 5*5 = 6)

6*2 = 6*2*3*3 = 6*5*3 = 1*3 = 3 ← 6*2 = 6*2*3*3 = 6*5*3 = 1*3 = 3 *

2*5 = 2*5*2*2 = 2*4*2 = 6*2 = 3 ← 2*5 = 2*5*2*2 = 2*4*2 = 6*2 = 3 ✡

Or, la table de S_3 :

*	Id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
Id	Id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	Id	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	Id	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	Id	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	Id
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	Id	(1 2 3)

En renomant les éléments de G, nous obtenons les mêmes tables. G est donc isomorphique à S_3.

Conclusion

Si un groupe à 6 éléments possède un élément d'ordre 6, alors il est isomorphique à $\mathbb{Z}/6\mathbb{Z}$.

Sinon, il possède 3 éléments d'ordre 2, 2 éléments d'ordre 3 et un élément d'ordre 1, le neutre, et est isomorphique à S_3.

Pelion — Semaine de colle n°3

Enoncé :

Déterminer tous les morphismes de groupes de $(S_3, \circ)$ vers $(\mathbb{C}^*, \times)$.

Solution :

(A) Soit $f : (S_3, \circ) \to (\mathbb{C}^*, \times)$ un morphisme de groupes.

Soit $(i, j) \in [\![1, n]\!]^2$

$$f((ij)^2) = f((ij))^2$$
$$= f(id) = 1$$

Donc $f((ij)) \in \{-1, 1\}$

- Si $f((ij)) = 1$
  Alors par décomposition de tout cycle en produit de permutations on a :
  $\forall \sigma \in S_3$, $f(\sigma) = 1$
  et f est la fonction constante 1.

- Si $f((ij)) = -1$
  Alors par le cours, f est ε, l'unique morphisme de groupe qui prend la valeur -1 sur les transpositions.

On a ainsi deux candidats.

⑤ Les deux candidats sont clairement des morphismes de groupes de $(S_3, \circ)$ vers $(\mathbb{C}^*, \times)$

Exercice 116. Soit p un nombre premier. On note

- Z_p l'ensemble des a/b avec $a \in \mathbf{Z}$, $b \in \mathbf{N}$ tel que p ne divise pas b.
- J_p l'ensemble des a/b avec $a \in \mathbf{Z}$, $b \in \mathbf{N}$ tel que p ne divise pas b et p divise a.

1. Montrer que Z_p est un sous-anneau de $\mathbf{Q}$.
2. Montrer que J_p est un idéal de Z_p et que tout idéal de Z_p autre que Z_p est inclus dans J_p.
3. Déterminer tous les idéaux de Z_p.

1) • $1 \in Z_p$

• Soit $(x_1, x_2) \in Z_p^2$ tel que $\exists (a_1, a_2, b_1, b_2) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \times \mathbb{N}^*$ $x_1 = \frac{a_1}{b_1}$ et $x_2 = \frac{a_2}{b_2}$ et $p \nmid b_1$ $p \nmid b_2$ alors :

$x_1 - x_2 = \frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1 b_2 - b_1 a_2}{b_1 b_2} \in \mathbb{Z}$ or d'après le lemme de Gauß $p \nmid b_1$, $p \nmid b_2 \Rightarrow p \nmid b_1 b_2$

• Soit $(x_1, x_2) \in Z_p^2$ alors $\exists (a_1, a_2, b_1, b_2) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \times \mathbb{N}^*$ tel que $x_1 = \frac{a_1}{b_1}$ et $x_2 = \frac{a_2}{b_2}$ ainsi $x_1 \times x_2 = \frac{a_1 \times a_2 \in \mathbb{Z}}{b_1 b_2 \in \mathbb{N}^*}$ et $p \nmid b_1 b_2$

2) • On remarque que $J_p = \langle p \rangle$ or $p \in Z_p$ ainsi J_p est un sous groupe de Z_p

• Soit $(x, y) \in Z_p \times J_p$ alors $\exists (a_1, a_2, b_1, b_2) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \times \mathbb{N}^*$

$x = \frac{a_1}{b_1}$ et $y = \frac{a_2}{b_2}$ et $p \nmid b_1$, $p \nmid b_2$ $p \mid a_2$

$x \times y = \frac{a_1 a_2 \in \mathbb{Z}}{b_1 b_2 \in \mathbb{N}^*}$ or $p \mid a_1$ donc $p \mid a_1 a_2$ et $p \nmid b_1 b_2$

ainsi J_p est un idéal de Z_p

Soit un idéal I de Z_p autre que Z_p, par l'absurde supposons que $I \subset J_p$ alors $\exists x \in I \subset Z_p$ tel que $\exists (a_1, b_1) \in \mathbb{Z}^* \times \mathbb{N}^*$ $x = \frac{a_1}{b_1}$ $p \nmid b_1$ et $p \nmid a_1$. On observe que $\frac{b_1}{a_1} \neq 0$ est son inversible donc il existe un élement inversible dans I.

D'après le cours $I = Z_p$ ce qui contradit l'hypothèse de départ.

3) On sait que Z_p est un anneau commutatif : Ainsi $\forall x \in Z_p$ $x Z_p$ est un idéal de Z_p or $x Z_p \subset J_p$ ie si $x = \frac{a_1}{b_1}$ où $(a_1, b_1) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \nmid b_1$ alors $\forall y \in x Z_p$ $\exists (a_2, b_2) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $y = \frac{a_1 a_2}{b_1 b_2}$ et $a_1 a_2$ divisible par p. Or comme

$y \in J_p$ $\exists k \in \mathbb{N}^*$ tel que $p^k = y = \frac{a_1 a_2}{b_1 b_2}$ et $p^k \mid a_1 a_2$, $p^k \nmid b_1 b_2$. Enfin on obtient que tous les idéaux de Z_p peuvent s'écrire de la forme J_p^k où $k \in \mathbb{N}^*$ en plus de Z_p un idéal de Z_p

Exercice 108. Soit p un nombre premier tel que $p \geqslant 3$.

1. Soit $a, b \in \mathbf{Z}/p\mathbf{Z}$. Montrer que l'équation $x^2 + ax + b = 0$ a une solution (dans $\mathbf{Z}/p\mathbf{Z}$) si et seulement si $a^2 - 4b$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$.
2. On suppose qu'il existe $u \in \mathbf{Z}$ tel que $p = 3u + 1$.
   (a) Montrer qu'il existe $a \in \mathbf{Z}/p\mathbf{Z}$ tel que $a^u \neq 1$.
   (b) En déduire que -3 est un carré dans $\mathbf{Z}/p\mathbf{Z}$. On pourra considérer le polynôme $X^3 - 1$.

Solution :

1) $\Rightarrow$ Supposons que $(E) : x^2 + ax + b = 0$ admet une solution $k \in \mathbb{Z}/p\mathbb{Z}$.

$$x^2 + ax + b = 0$$
$$\Rightarrow (2x)^2 + 4ax + 4b = 0$$
$$\Rightarrow (2x - a)^2 - a^2 + 4b = 0$$
$$\Rightarrow (2x - a)^2 = a^2 - 4b$$

$\Leftarrow$ Supposons que $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ donc il existe $z \in \mathbb{Z}/n\mathbb{Z}$ tel que $z^2 = a^2 - 4b$

$$x^2 + ax + b = 0$$
$$\Rightarrow (2x - a)^2 - (a^2 - 4b) = 0$$
$$\Rightarrow (2x - a - z)(2x - a + z) = 0$$

Or 2 est inversible dans $\mathbb{Z}/p\mathbb{Z}$ car $p \geq 3$

donc $x = 2^{-1}(a + z)$ est solution de (E)

2) (a) Supposons que pour tout $a \in \mathbb{Z}/p\mathbb{Z}$,

$$a^u = 1$$

alors le polynome $X^u - 1$ admet p solution or $u < p$ ce qui est absurde.

(b) $1^2 - 4 \times 1 = -3$ dans $\mathbb{Z}/p\mathbb{Z}$

donc il faut montrer que $x^2 + x + 1 = 0$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$

$x \in \mathbb{Z}/p\mathbb{Z}$, $(x - 1)(x^2 + x + 1) = (x^3 - 1)$

en évaluant en a^u, comme dans (a) / $(a^u - 1)((a^u)^2 + a^u + 1) = a^{3u} - 1$

$\neq 0$ p

or $a(a^{3u} - 1) = a^{3u+1} - a = 0$

a

or $a \neq 0$ donc $a^{3u} - 1 = 0$

Ainsi $(a^u)^2 + a^u + 1 = 0$

Par Q_1, on en déduit que -3 est un carré.

Léa N.

Colle de la semaine n°23

Énoncé :

Exercice 1 :

Soit $(G,*)$ un groupe cyclique à $n \geqslant 2$ éléments engendré par a.
Pour $r \in \mathbb{N}^*$, on introduit l'application $f : G \to G$ définie par $f(x) = x^r$ pour tout x appartenant à G.
On pose $d = n \wedge r$.

1. Vérifier que f est un morphisme du groupe $(G,*)$.
2. Déterminer son noyau.
3. Montrer que son image est le sous groupe engendré par a^d.
4. Pour $y \in G$, combien l'équation $x^r = y$ possède-t-elle de solutions ? (Faire des cas).

Solution :

1/ Soit $(x_1, x_2) \in G^2$.

$$f(x_1 * x_2) = (x_1 * x_2)^r$$
$$= x_1^r * x_2^r \qquad ((G,*) \text{ est un groupe cyclique})$$
$$= f(x_1) * f(x_2)$$

Donc $\boxed{f \text{ est un morphisme du groupe } (G,*)}$.

2/ Soit $x \in \ker(f)$. $\exists k \in \mathbb{Z} \quad x = a^k$

$$f(x) = e_G \iff a^{kr} = e_G$$

On a est d'ordre n.

$$f(x) = e_G \iff n \mid kr$$

On $d = n \wedge r$ alors $\exists (u,v) \in \mathbb{Z}^2$

$n = du$ et $r = dv$ et $u \wedge v = 1$.

Alors par lemme de Gauß :

$$n \mid kr \iff u \mid k$$

Donc $\boxed{\ker(f) = \langle a^u \rangle}$

3/ $d = n \wedge r$

. Par théorème de Bézout :

$\exists (p,q) \in \mathbb{Z}^2 \quad np + rq = d$

alors $a^d = \underbrace{a^{np}}_{= e_G} * a^{rq}$

$= a^{rq}$

$= f(a^q) \quad \in Im(f)$

Comme $Im(f)$ est un sous-groupe, $\langle a^d \rangle \subset Im(f)$

. Soit $y \in Im(f)$, $\exists x \in G$

$y = x^r$ où $x = a^k$, $k \in \mathbb{Z}$

Alors $y = a^{kr}$

On a $d \mid r$ donc $y \in \langle a^d \rangle$

On en déduit que $\boxed{Im(f) = \langle a^d \rangle}$

4/ . Si $y \notin Im(f)$ alors l'équation n'a pas de solution

. Si $y \in Im(f)$, $\exists x_0 \in G$ tel que :

$x_0^r = y$

alors $x^r = y \iff (x * x_0^{-1})^r = e_G$

donc $(x * x_0^{-1}) \in Ker(f) = \langle a^u \rangle$

L'ensemble des solutions est en bijection avec le noyau.

$\boxed{\text{Alors, il y a } \frac{n}{u} = d \text{ solutions.}}$

Anaë D.

Rapport de colle S3

Exercice : Q1. L'élément $\overline{19}$ est-il inversible dans l'anneau $\mathbb{Z}/49\mathbb{Z}$?
Q2. Si oui, quel est son inverse ?

Q1. On sait que $U(\mathbb{Z}/49\mathbb{Z}) = \{\bar{a} \in \mathbb{Z}/49\mathbb{Z} \ : \ a \wedge 49 = 1\}$
Or $19 \wedge 49 = 1$
Donc l'élément $\overline{19}$ est inversible dans l'anneau $\mathbb{Z}/49\mathbb{Z}$

Q2. On cherche $\bar{a} \in \mathbb{Z}/49\mathbb{Z}$ tel que $\overline{19} \times \bar{a} = \bar{1}$.

$49 = 19 \times 2 + 11$
$19 = 11 \times 1 + 8$
$11 = 8 \times 1 + 3$
$8 = 3 \times 2 + 2$
$3 = 2 \times 1 + 1$

En remontant l'algorithme d'Euclide, on obtient

$1 = 3 - 2$
$1 = 3 - (8 - 3 \times 2)$
$1 = 3 \times 3 - 8$
$1 = 3 \times (11 - 8) - 8$
$1 = 3 \times 11 - 4 \times 8$
$1 = 3 \times 11 - 4 \times (19 - 11)$
$1 = 7 \times 11 - 4 \times 19$
$1 = 7 \times (49 - 19) - 4 \times 19$
$1 = 7 \times 49 - 18 \times 19$

Donc l'inverse de $\overline{19}$ dans $\mathbb{Z}/49\mathbb{Z}$ est $\overline{-18}$

Mehdi B. Celle de la semaine

Soit A un anneau commutatif, I un idéal de A.

$$\sqrt{I} := \{ a \in A : \exists n \in \mathbb{N} \ a^n \in I \} \subset A.$$

Démontrer que $\sqrt{I}$ est un idéal de A

Solution : • $0 = 0^1 \in I$ sous-groupe de A donc $0 \in \sqrt{I}$ et $\underline{\sqrt{I} \neq \emptyset}$

• Soit $(a,b) \in \sqrt{I}$. Montrons que $a-b \in \sqrt{I}$.

$\exists (n,m) \in \mathbb{N}^2$ tel que $a^n \in I$ et $b^m \in I$.
On veut montrer qu'il existe $r \in \mathbb{N}$ tel que $(a-b)^r \in I$.

Comme A est un anneau commutatif nous pouvons appliquer la formule du binôme de Newton :

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} (-1)^k b^k a^{n+m-k}$$

Si on montre que chaque terme de cette somme appartient à I, puisque I est stable par somme, alors $(a-b)^{n+m} \in I$.

Soit $l \in [\![0, n+m]\!]$. Montrons que $\underbrace{\binom{n+m}{l} (-1)^l b^l a^{n+m-l}}_{:= x} \in I$.

• $\underline{\text{Si } l \geq m}$

$$b^l = b^{m+l-m} = \underbrace{b^m}_{\in I} \underbrace{b^{l-m}}_{\in A} \in I \text{ absorbant.}$$

$l - m \geq 0$

Donc $x \in I$.

• Si $l < m$

$a^{n+m-l} = a^n a^{\overbrace{m-l}^{>0}} \in I$ et $x \in I$.

Donc : $\forall l \in [\![0, n+m]\!]$ $\binom{n+m}{l} (-1)^l a^{n+m-l} b^l \in I$. Ainsi :

$$\underbrace{(a-b)^{\overbrace{n+m}^{\in \mathbb{N}}} \in I}_{} \text{ et } a-b \in \sqrt{I}$$

Donc $\sqrt{I}$ est un sous-groupe de A (1)

• Montrons que $\sqrt{I}$ est absorbant.

Soit $x \in A$, $a \in \sqrt{I}$.

$\exists n \in \mathbb{N}$ $a^n \in I$.

$$(xa)^n = \underbrace{x^n}_{\in A} \underbrace{a^n}_{\in I} \in I \text{ absorbant.}$$

Donc $xa \in \sqrt{I}$ et $\sqrt{I}$ absorbant (2)

D'après (1) et (2) :

$\boxed{\sqrt{I} \text{ est un idéal de } A}$

Rayon 6
MPI*

Colle de la semaine n°3

Enoncé : Soit A un anneau tel que
$\forall x \in A \; x^3 = x$

1) Montrer que
$\forall x \in A \quad 6x = 0$

2) Montrer que
~~$\forall (x,y)$~~ $\forall x \in A$ tel que $x^2 = -x$
Alors
$x = -x = x^2 = -x^2$

3) Montrer que
$\forall (x,y) \in A^2$ tel que $2x = 2y = 0$
Alors
$xy = yx$

4) Déduire de ce qui précède que $\forall (x,y) \; xy = 0$

5) Montrer que
$\forall (x,y) \in A^2 \quad 2(xy - yx) = 0$

6) Conclure

7) Donner un exemple d'anneau infini correspondant à l'hypothèse de l'énoncé.

Solution :

1) Soit $x \in A$

$0 = 2x - 2x = (2x)^3 - 2x = 8x^3 - 2x = 8x - 2x = 6x$

2) Soit $x \in A$ tel que $x^2 = -x$

$(x^2+x)^2 = x^4 + 2x^3 + x^2$

Or $x^3 = x$ donc $x^4 = x^2$

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

~~Ainsi~~

Sont correspondants :

$(x^2+x) = (x^2+x)^3 = 4(x^2+x)$

Donc

$3x^2 + 3x = 0$

$\Rightarrow x^2 + x + 2x^2 + 2x = 0$

Or $x = -x$ donc $2x = 0$

donc $2x^2 = 0$

Ainsi

$x = -x^2$

On remarque que

$x = -x$ donne $x^2 = -x^2$

Finalement :

$x = -x = x^2 = -x^2$

3) Soit $(x,y) \in A^2$

On suppose que $z_x = z_y = 0$

$z_x = 0 \Rightarrow x = -x$

De même $y = -y$ | $\times$

Donc

$$x+y = -(x+y)$$

On applique φ à $(x+y)$:

$$x+y = |x+y|^2 = x^2 + xy + yx + y^2$$

φ livre par (1) que $x = x^2$ et $y = y^2$

Donc

$$xy + yx = 0$$

En appliquant $y = -y$:

$$xy = yx$$

4) Soit $(x,y) \in A^2$

$G_y = G_x = 0$ par (1)

Or $G_y = z_x(\beta_y)$ et $G_x = z_x(\beta_x)$

On applique (3) à β_y et β_x :

$$\beta_y(\beta_x) = \beta_x(\beta_y)$$

$$\Rightarrow \gamma_{yx} = \gamma_{xy}$$

$$\Rightarrow \varphi(xy - yx) = 0$$

5) Soit $(x,y) \in A^2$

$(x+y)^3 - (x+y) = 0$

On $(x+y)^3 = (x^2 + xy + yx + y^2)(x+y)$

$(x+y)^3 = x^3 + x^2y + yx^2 + yxy + x^2y + xyy + yxy + y^3$

Et donc alors :

$(1) \quad x^3 + yx^2 + yxy + y^2x + x^2y + xyy + yxy + y^3$

De manière analogue avec $(x-y)$ nous avons :

$(2) \quad -x^3 - yx^2 - yxy - y^2x + x^2y + xyy + yxy + y^3$

En faisant $(1) - (2)$ nous avons :

$$2xyx + 2yx^2 + 2x^2y = 0$$

On multiplie par x à gauche :

$(\alpha) \quad 2x^2yx + 2xyx^2 + 2xy = 0$

On multiplie par x à droite :

$(\beta) \quad 2xyx^2 + 2x^2yx + 2yx = 0$

En faisant $(\alpha) - (\beta)$:

$$2(xy - yx) = 0$$

6) Soit $(x,y) \in A^2$

Sur $\mathbb{Q}$:

$$z(x_y - y_n) = 0$$

$$\Rightarrow \varphi(x_y - y_n) = 0$$

Sur $\mathbb{Q}[i]$: $\varphi(x_y - y_n) = 0$

Ainsi

$$(x_y - y_n) = (\varphi - \varphi)(x_y - y_n) = \varphi(x_y - y_n) - \varphi(x_y - y_n) = 0$$

Donc $x_y = y_n$

L'anneau est commutatif

7) $\mathbb{Z}/6\mathbb{Z}$ est un anneau fini qui respecte la propriété

On remarque que $(\mathbb{Z}/6\mathbb{Z})^{\mathbb{N}}$ est un anneau respectant aussi la propriété et infini

Hugo D.

Semaine de colle n°3

Exercice 2 : Soit A une algèbre intègre sur $\mathbb{R}$ de dimension finie $n \geqslant 2$. Dans la suite, on assimile $\mathbb{R}$ à $\mathbb{R}.1$ où 1 est l'élément neutre de A pour le produit.

1. Montrer que tout élément non nul de A est inversible.
   Indication : Pour a élément non nul de A, considérer l'application définie sur A : $x \mapsto ax$.
2. Soit a un élément de A non situé dans $\mathbb{R}$. Montrer que $(1, a)$ est libre tandis que $(1, a, a^2)$ est liée.
   Indication : Pour montrer que la famille $(1, a, a^2)$ est liée, considérer la famille $(1, a, .., a^n)$.
3. En déduire l'existence d'un élément i_A de A tel que $i_A^2 = -1$.
4. Montrer que si A est commutative alors A est isomorphe à $\mathbb{C}$.
   Indication : Commencer par prouver que $n = 2$.

Solution : 1) Soit $a \in A \setminus \{0_A\}$ $\quad f_a \left| \begin{array}{l} A \to A \\ x \mapsto ax \end{array} \right.$ bien définie

Injective Soit $(x_1, x_2) \in A^2$ tel que $ax_1 = ax_2$

$\Rightarrow a(x_1 - x_2) = 0$

$\Rightarrow x_1 = x_2$ (A intègre, $a \neq 0$)

Donc f_a surjective par égalité des dimensions finies de la source et du but. Or $1_A \in A$ donc $\exists B \in A \quad f_a(B) = aB = 1$

De plus $f_a(Ba) = a = f_a(1_A)$ Donc $Ba = 1_A$ car f_a injective donc a inversable

2) Absurde Supposons $\exists (\lambda_1, \lambda_2) \in \mathbb{R}^2 \setminus \{(0,0)\}$ tel que $\lambda_1 \cdot 1 + \lambda_2 \cdot a = 0$

Si $\lambda_2 = 0$ $\lambda_1 = 0$ ↯

Sinon $a = -\underbrace{\frac{\lambda_1}{\lambda_2}}_{\in \mathbb{R}}$ ↯ car a non situé dans $\mathbb{R}$

Donc $(1, a)$ libre

La famille $(1, a, .., a^n)$ ayant $n+1$ éléments est liée

$\exists (\lambda_0, .., \lambda_n) \in \mathbb{R}^{n+1} \setminus \{(0, .., 0)\} \quad \sum_{i=0}^{n} \lambda_i a^i = 0$

On pose $P = \sum_{i=0}^{n} \lambda_i X^i$ non nul $\deg(P) \geqslant 2$

$P = \text{dom}(P) \prod_{k=1}^{n} (X + \gamma_k) \prod_{k=1}^{p} (X^2 + \alpha_k X + \beta_k)$ où $(\gamma_1, .., \gamma_n) \in \mathbb{R}^n$, $(p, q) \in \mathbb{N}^2$, $(\alpha_1, .., \alpha_p) \in \mathbb{R}^p$, $(\beta_1, .., \beta_p) \in \mathbb{R}^p$

Pour $X = a$, on a $0 = \underbrace{\dim(P)}_{\neq 0} \prod_{k=1}^{n} (a + \gamma_k) \prod_{k=1}^{p} (a^2 + \alpha_k a + \beta_k)$

Par intégrité $\begin{cases} \exists i \in [\![1,p]\!] \quad a^2 + \alpha_i a + \beta_i = 0 \\ \text{ou} \\ \underbrace{\exists j \in [\![1,n]\!] \quad a + \gamma_j = 0}_{\text{Impossible car } (1,a) \text{ libre}} \end{cases}$

Donc $(1, a, a^2)$ liée

3) On sait $\exists (\alpha, \beta) \in \mathbb{R}^2 \quad a^2 + \alpha a + \beta < 0$ et $\Delta = \alpha^2 - 4\beta < 0$ car irréductible

$$\Rightarrow \left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2 - 4\beta}{4} < 0$$

$$\Rightarrow \left(a + \frac{\alpha}{2}\right)^2 = -\left(\frac{\sqrt{4\beta - \alpha^2}}{2}\right)^2$$

$$\Rightarrow \left(\underbrace{\frac{2}{\sqrt{4\beta - \alpha^2}} \cdot a + \frac{\alpha}{\sqrt{4\beta - \alpha^2}} \cdot 1}_{i_a \in A}\right)^2 = -1$$

4) Absurde Supposons $n \geq 3$

$(1, a)$ libre $\Rightarrow \exists B \in A \quad (1, a, B)$ libre (car $\dim(A) = 2 < 3$)

On considère i_a et i_B résultant de 3)

$\exists (\lambda_1, \lambda_2, \mu_1, \mu_2) \in \mathbb{R}^4 \quad i_a = \lambda_1 \cdot a + \lambda_2 \cdot 1 \quad i_B = \mu_1 \cdot B + \mu_2 \cdot 1$

On $-1 = i_a^2 = i_B^2$

$\Rightarrow (i_a - i_B)(i_a + i_B) = 0$ (Commutativité)

$\Rightarrow i_a = \varepsilon i_B$ avec $\varepsilon \in \{-1, 1\}$ (intégrité)

$\Rightarrow (\lambda_2 - \varepsilon \mu_2) \cdot 1 + \lambda_1 \cdot a - \mu_1 \cdot B = 0$

$\Rightarrow \lambda_1 = 0$ par liberté { car nous avons vu que la composante en a doit être $\neq 0$

Donc A de dimension 2 (et $\mathbb{C}$ de dimension 2 en tant que $\mathbb{R}$-ev)

$(1, i_A)$ base de A car non colinéaire et de même cardinal que $\dim(A)$

$\varphi \left| \begin{array}{ccc} A & \to & \mathbb{C} \\ 1_A & \to & 1 \\ i_A & \to & i \end{array} \right.$ envoie une base sur une base donc bijective Donc $A \simeq \mathbb{C}$

Sophie G

Semaine de colle n°1.

Exercice

Soient $p \in \mathbb{P}_{\geq 3}$, $(a,b) \in \mathbb{Z}/p\mathbb{Z}$

Montrer $(E) : x^2 + ax + b = 0$ a une solution dans $\mathbb{Z}/p\mathbb{Z}$ $\Leftrightarrow$ $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow$ Supposons $x^2 + ax + b = 0$ a une solution que l'on note $\alpha \in \mathbb{Z}/p\mathbb{Z}$

alors $\exists c \in \mathbb{Z}/p\mathbb{Z}$ tel que

$x^2 + ax + b = (x - \alpha)(x - c)$

$= x^2 - xc - \alpha x + \alpha c = x^2 + x(-c - \alpha) + c\alpha$

Posons $\Delta := a^2 - 4b = (-c - \alpha)^2 - 4c\alpha$

$= c^2 + \alpha^2 - 2c\alpha = \underbrace{(c - \alpha)^2}_{=: k}$

donc $a^2 - 4b$ est un carré.

$\Leftarrow$ Supposons $\exists k \in \mathbb{Z}/p\mathbb{Z}$ $k^2 = a^2 - 4b$

Montrons $\overline{2}^{-1}(k - a)$ est solution de E

$\overline{4}^{-1}(k-a)^2 + \overline{2}^{-1}a(k-a) + b = \overline{4}^{-1}k^2 - \overline{2}^{-1}ka + \overline{4}^{-1}a^2 + \overline{2}^{-1}ak - \overline{2}^{-1}a^2 + b$

$= \overline{4}^{-1}(a^2 - 4b) + \overline{4}^{-1}a^2 - \overline{2}^{-1}a^2 + b$

$= -\overline{1}b + b + \overline{4}^{-1}a^2 + \overline{4}^{-1}a^2 - \overline{2}^{-1}a^2$ $\rightarrow \overline{2} \times \overline{4}^{-1}a^2$

(car $\overline{4} \times \overline{4}^{-1} = \overline{2}^{-1} \times \overline{2}^{-1} \times \overline{2} \times \overline{2} = \overline{1}$)

$= \overline{2}^{-1}a^2(\underbrace{\overline{2}^{-1} \times \overline{2}}_{1} - 1) = 0$

Louis B — Khôlle de la semaine 3

Exercice 114. Soit A un anneau commutatif et I un idéal de A. On appelle radical de I l'ensemble suivant

$$\sqrt{I} = \{a \in A \mid \exists n \in \mathbf{N},\ a^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Soit $\alpha \in \mathbf{Z}$. Prenons $A = \mathbf{Z}$ et $I = \alpha\mathbf{Z}$. Déterminer $\sqrt{I}$.

1) • $0_A = 0_A^1 \in I$ donc $0_A \in \sqrt{I}$

• Soit $(x,y) \in \sqrt{I}^2$

Alors $\exists (n,m) \in \mathbb{N}^2$ tq $x^n \in I$ et $y^m \in I$

Alors $(x-y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k (-y)^{n+m-k}$ (A est un anneau commutatif)

$= \sum_{k=0}^{n} \binom{n+m}{k} x^k (-y)^{\geq m} + \sum_{k=n+1}^{n+m} \binom{n+m}{k} x^{\geq n} (-y)^{n+m-k}$

Comme I est un idéal de A, $n-k \geq 0$

$\forall k \in [\![0, n]\!]$ $\binom{n+m}{k} x^k (-y)^{n-k} (-y)^m \in I$

$\forall k \in [\![n+1, n+m]\!]$ $\binom{n+m}{k} (-y)^{n+m-k} x^{k-n} x^n \in I$

Donc comme I ss-grp de A $(x-y)^{n+m} \in I$

et donc $(x-y) \in \sqrt{I}$

• Soit $x \in \sqrt{I}$, $a \in A$

$\exists n \in \mathbb{N}$ tq $x^n \in I$

alors $(ax)^n = a^n x^n \in I$ car I absorbant et A stable par $\times$ (A commutatif)

Donc $ax \in \sqrt{I}$

Donc $\sqrt{I}$ est un idéal de A

2) Soit $r \in \mathbb{N}^*$, $(p_1, \dots, p_r) \in \mathcal{P}$ 2 à 2 distincts
$(m_1, \dots, m_r) \in \mathbb{N}^*$

tq $\alpha = \prod_{i=1}^{r} p_i^{m_i}$

Alors Montrons que $\sqrt{\alpha\mathbb{Z}} = \prod_{i=1}^{r} p_i \mathbb{Z}$

[b] Soit $x \in \prod_{i=1}^{r} p_i \mathbb{Z}$

Soit $n = \max\{m_1, \dots, m_r\}$

Alors $\alpha \mid x^n$ i.e. $\exists q \in \mathbb{Z}$ tq $x^n = \alpha q$

[c] Soit $x \in \sqrt{\alpha\mathbb{Z}}$
$\exists n \in \mathbb{N}$ tq $x^n = q\alpha$, $q \in \mathbb{Z}$

Alors $qx = q \prod_{i=1}^{r} p_i^{m_i}$

Soit $\left.\begin{matrix}(t_1, \dots, t_s) \in \mathcal{P} \\ (u_1, \dots, u_s) \in \mathbb{N}\end{matrix}\right\}$ tq $x = \prod_{i=1}^{s} t_i^{u_i}$

alors $x^n = \prod_{i=1}^{s} t_i^{u_i n}$

Par unicité de la décomposition en facteurs premiers : $s \geq r$ et
$\forall i \in [\![1, r]\!]$ $\exists ! j \in [\![1, s]\!]$ tq $p_i = t_j$

$\Rightarrow x \in \prod_{i=1}^{r} p_i \mathbb{Z}$

Donc $\sqrt{\alpha\mathbb{Z}} = \prod_{i=1}^{r} p_i \mathbb{Z}$

Maximilien . T.

Colle Semaine 3

Exercice 3 :

Soit $(A, +, \times)$ un anneau, on dit qu'un élément a de A est nilpotent si il existe un entier naturel k non nul tel que $a^k = 0_A$.

1. Soit x et y deux éléments nilpotents de A tels que $x \times y = y \times x$. Montrer que $x \times y$ et $x + y$ sont nilpotents.

2. Soit n un entier supérieur à 2 que l'on décompose en produits de facteurs premiers $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ avec $\alpha_i \in \mathbb{N}^*$.
Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.

Solution :

1/ x nilpotent $\Rightarrow \exists h_1 \in \mathbb{N}^* \quad x^{h_1} = 0_A$

y nilpotent $\Rightarrow \exists h_2 \in \mathbb{N}^* \quad y^{h_2} = 0_A$

$(x \times y)^{h_1} = x^{h_1} \times y^{h_2} = 0_A$

(x et y commutent)

Posons $k = (h_1 h_2)$

$(x+y)^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} x^i y^{2k-i} = \underbrace{\sum_{i=0}^{k} \binom{2k}{i} x^i y^{2k-i}}_{2k-i \geq h_2} + \underbrace{\sum_{i=k+1}^{2k} \binom{2k}{i} x^i y^{2k-i}}_{i \geq h_1}$

(x et y commutent)

$= 0$

2/ Posons $A = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists k \in \mathbb{N}^* \quad \bar{a}^k = \bar{0} \}$

et $B = \{ \overline{\prod_{i=1}^{k} p_i} \, q : q \in \mathbb{Z} \}$

Montrons $A = B$

(D) Soit $b \in B$ alors $\exists q \in \mathbb{Z}$ tel que $b = \prod_{i=1}^{k} p_i \, q$

$\alpha = \max(\alpha_1, \dots, \alpha_k) \in \mathbb{N}^*$

alors $\overline{b^\alpha} = \overline{\prod_{i=1}^{k} p_i^\alpha \, q}$

$\Rightarrow n \mid b^\alpha$ d'où $\overline{b}^\alpha = 0$

(C) Soit $\bar{a} \in A$ alors $\exists k \in \mathbb{N}^*$ tq $\overline{a^k} = 0$

$\Rightarrow \exists q \in \mathbb{Z}$ tel que $a^k = qn$

En regardant la décomposition en facteurs premiers des 2 termes on obtient $\prod_{i=1}^{k} p_i \mid a$ D-

Youssef B.

Colle de la semaine 3

On appelle « nombres de Fermat » les nombres

$$F_i = 2^{2^i} + 1$$

$$\forall (m \neq n) \Longrightarrow (F_m \wedge F_n = 1)$$

En déduire qu'il existe une infinité de nombres premiers

Solution :

quitte à échanger le rôle de n et m, supposons $n > m$

$\Rightarrow \exists p \in \mathbb{N} \quad n = m + p$

$$\begin{aligned} F_n &= 2^{2^n} + 1 \\ &= 2^{2^{m+p}} + 1 \\ &= 2^{2^m \times 2^p} + 1 \\ &= \left(2^{2^m} + 1 - 1\right)^{2^p} + 1 \\ &= \left(F_m - 1\right)^{2^p} + 1 \\ &= \sum_{k=0}^{2^p} \binom{2^p}{k} \left(2^{2^m}\right)^k (-1)^{2^p - k} + 1 \end{aligned}$$

$$F_n \equiv (-1)^{2^p} + 1 \ [F_m]$$

$$F_n \equiv 2 \ [F_m]$$

$\Rightarrow \exists q \in \mathbb{Z} \quad F_n = 2 + q F_m$

Soit d un diviseur positif de F_n et F_m

Alors $d \mid 2$

$\Rightarrow d = 1$ ou $d = 2$

Or, les nombres de Fermat sont impairs, donc $d = 1$

Ainsi, F_n et F_m sont premiers entre eux

$\forall m \in \mathbb{N}$, soit p_m diviseur premier de F_m

p_m existe car tout nombre entier plus grand que 2 possède un diviseur premier.

Or, les F_i et F_j pour $(i,j) \in \mathbb{N}^2$ sont premiers entre eux

Donc tous les p_m sont 2 à 2 distincts.

Ainsi, il existe une infinité de nombre premiers