TD 13 - Algèbre générale

Exercice 46 Montrer que les applications suivantes définissent des morphismes de groupes (on précisera pour quelles lois). Déterminer leur noyau et leur image.

$\mathcal{A}(\mathbf{R})$ désigne l'ensemble des applications affines réelles, G désigne un groupe quelconque et a est un élément de G donné.

$f_1 : \begin{array}{c}\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \\ k \mapsto \bar{k}\end{array}$ $f_2 : \begin{array}{c}\mathbf{C}^* \to \mathbf{C}^* \\ z \mapsto z^2\end{array}$ $f_3 : \begin{array}{c}\mathbf{Z} \to \mathbf{Q}^* \\ n \mapsto 2^n\end{array}$ $f_4 : \begin{array}{c}\mathcal{A}(\mathbf{R}) \to \mathbf{R}^* \\ [x \mapsto \alpha x + \beta] \mapsto \alpha\end{array}$ $f_5 : \begin{array}{c}G \to G \\ x \mapsto axa^{-1}\end{array}$

Cours Définition morphisme de groupe :

Soient $(G, *)$et $(H, \circ)$ deux groupes,

$f: G \to H$, f est un morphisme de groupe si $\forall (x, y) \in G^2$, $f(x * y) = f(x) \circ f(y)$

Conséquences :

- $f(e_G) = e_H$ car $f(x * e_G) = f(x) \circ f(e_G) = f(x)$

  donc $(f(x))^{-1} \circ f(x) \circ f(e_G) = (f(x))^{-1} \circ f(x)$ et $f(e_G) = e_H$
- $(f(x))^{-1} = f(x^{-1})$ car $f(x * x^{-1}) = f(e_G) = e_H = f(x) \circ f(x^{-1})$ ainsi $f(x^{-1}) = (f(x))^{-1}$ par unicité de l'inverse

Cours : $f: (E, +) \to (F, *)$

- Définition de $Ker\, f = \{x \in E \ tq\ f(x) = e_F\}$, c'est un sous-groupe de E
- Définition de $Im f = \{y \in F \,/\, \exists x \in E \ tq\ f(x) = y\}$, c'est un sous-groupe de F

- $f_1: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ k \to \bar{k}$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$

Morphisme de groupe :

$\forall (k, k') \in \mathbb{Z}^2$, $f_1(k + k') = \overline{k + k'} = \bar{k} + \overline{k'} = f_1(k) + f_1(k')$ par définition de la loi + dans $(\mathbb{Z}/n\mathbb{Z}, +)$

Noyau de f_1 :

- Soit $k \in ker\, f_1$ alors $f_1(k) = \bar{0}$ donc $\exists p \in \mathbb{Z}$ tq $k = np$ soit $k \in n\mathbb{Z}$ ainsi $kerf_1 \subset n\mathbb{Z}$
- Soit $k \in n\mathbb{Z}$ alors il existe $p \in \mathbb{Z}$ tq $k = np$ et $f_1(k) = f_1(np) = \overline{np} = \bar{0}$ donc $k \in kerf_1$, ainsi $n\mathbb{Z} \subset Kerf_1$

au final : $Kerf_1 = n\mathbb{Z}$

Image de f_1 :

- Soit $y \in Imf_1$ alors $\exists k \in \mathbb{Z},\ tq\ f(k) = \bar{k} = y$ donc $y \in \mathbb{Z}/n\mathbb{Z}$ ainsi $Imf_1 \subset \mathbb{Z}/n\mathbb{Z}$
- Soit $y \in \mathbb{Z}/n\mathbb{Z}$ alors il existe $k \in \mathbb{Z}$ tq $y = \bar{k}$ donc $y = f(k)$ et $y \in Imf_1$ ainsi $\mathbb{Z}/n\mathbb{Z} \subset Imf_1$

Pour toute classe, on peut trouver un représentant dans $\mathbb{Z}$.

au final : $Imf_1 = \mathbb{Z}/n\mathbb{Z}$

- $f_2 : \mathbb{C}^* \to \mathbb{C}^*,\ z \to z^2$ est un morphisme de $(\mathbb{C}^*, \times)$ dans lui-même

Morphisme de groupe : $\forall (z, z') \in \mathbb{C}^*,\ f_2(zz') = (zz')^2 = z^2 \times (z')^2 = f_2(z) \times f_2(z')$

Noyau de f_2 :

- Soit $z \in kerf_2$ alors $f_2(z) = 1$ soit $z^2 = 1$ donc $z = \pm 1$ ainsi $kerf_2 \subset \{-1\,;\,1\}$
- Pour $z = 1$, $f_2(1) = 1^2 = 1$ donc $1 \in kerf_2$
  Pour $z = -1$, $f_2(-1) = (-1)^2 = 1$ donc $-1 \in kerf_2$ ainsi $\{-1\,;\,1\} \subset kerf_2$

au final : $Kerf_2 = \{-1\,;\,1\}$

Image de f_2 :

- Soit $y \in Imf_2$ alors $\exists z \in \mathbb{C}^*$ tq $y = f(z) = z^2$ donc $y \in \mathbb{C}^*$ et $Imf_2 \subset \mathbb{C}^*$
- Soit $y \in \mathbb{C}^*$, on peut toujours trouver $z \in \mathbb{C}^*$ tq $y = z^2$ ainsi il existe $z \in \mathbb{C}^*$ tq $y = f(z)$ alors $\mathbb{C}^* \subset Imf_2$

au final : $Imf_2 = \mathbb{C}^*$

- $f_3 : \mathbb{Z} \to \mathbb{Q}^*,\ n \to 2^n$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Q}^*, \times)$

Morphisme de groupe : $\forall (n, n') \in \mathbb{Z}^2,\ f_3(n + n') = 2^{n+n'} = 2^n \times 2^{n'} = f_3(n) \times f_3(n')$

Noyau de f_3 :

- Soit $n \in Kerf_3$ alors $f_3(n) = 1$ soit $2^n = 1 = 2^0$ donc $n = 0$ ainsi $Kerf_3 \subset \{0\}$
- Pour $n = 0$, $f_3(0) = 2^0 = 1$ donc $0 \in Kerf_3$ ainsi $\{0\} \subset Kerf_3$

au final : $Kerf_3 = \{0\}$

Image de f_3 :

- Soit $y \in Imf_3$ alors $\exists n \in \mathbb{Z}$ tq $y = f_3(n) = 2^n$ ainsi $y \in \{2^n,\ n \in \mathbb{Z}\}$ donc $Imf_3 \subset \{2^n,\ n \in \mathbb{Z}\}$
- Soit $y \in \{2^n,\ n \in \mathbb{Z}\}$ alors il existe $n \in \mathbb{Z}$ tq $y = 2^n = f_3(n)$ donc $y \in Imf_3$ et $\{2^n,\ n \in \mathbb{Z}\} \subset Imf_3$

au final : $Imf_3 = \{2^n,\ n \in \mathbb{Z}\}$

- $f_4 : A(\mathbb{R}) \to \mathbb{R}^*,\ g : (x \to \alpha x + \beta) \to \alpha$ est un morphisme de $(A(\mathbb{R}), \circ)$ dans $(\mathbb{R}^*, \times)$

En l'état ce n'est pas un morphisme de groupe car ce n'est pas une application
En revanche, si on prend $A(\mathbb{R})$ avec $\alpha \neq 0$, c'est une application.

Morphisme de groupe :
$\forall (g, g') \in A(\mathbb{R}),\ \forall x \in \mathbb{R}\ (g \circ g')(x) = \alpha\alpha' x + \alpha\beta' + \beta$, donc $f_4(g \circ g') = \alpha\alpha' = f_4(g) \times f_4(g')$

Noyau de f_4 :

- Soit $g \in Kerf_4$ alors $f_4(g) = 1$ soit $g(x) = x + \beta$, $\forall x \in \mathbb{R}$ donc $g \in \{h : x \to x + \beta, \beta \in \mathbb{R}\}$ alors $Kerf_4 \subset \{h : x \to x + \beta, \beta \in \mathbb{R}\}$
- Soit $g \in \{h : x \to x + \beta, \beta \in \mathbb{R}\}$ alors $f_4(g) = 1$ donc $g \in Kerf_4$ et $\{h : x \to x + \beta, \beta \in \mathbb{R}\} \subset Kerf_4$

au final : $Kerf_4 = \{h : x \to x + \beta, \beta \in \mathbb{R}\}$

Image de f_4 :

- Soit $\alpha \in Imf_4$ alors $\alpha \in \mathbb{R}^*$ et $Imf_4 \subset \mathbb{R}^*$
- Soit $\alpha \in \mathbb{R}^*$, il suffit de prendre $g(x) = \alpha x$ alors $f_4(g) = \alpha$ donc $\alpha \in Imf_4$ et $\mathbb{R}^* \subset Imf_4$

au fnal : $Imf_4 = \mathbb{R}^*$

- $f_5 : G \to G,\ x \to axa^{-1}$ est un morphisme de $(G,.)$ dans lui-même

Morphisme de groupe : $\forall (x, x') \in G^2,\ f_5(xx') = a(xx')a^{-1} = axa^{-1}ax'a^{-1} = f_5(x)f_5(x')$

Noyau de f_5 :

- Soit $x \in Kerf_5$ alors $f_5(x) = axa^{-1} = e$ donc $x = a^{-1}a = e$ $x \in \{e\}$ ainsi $Kerf_5 \subset \{e\}$
- Soit $x = e$, alors $f(e) = e$ $e \in Kerf_5$ ainsi $\{e\} \subset Kerf_5$

au final : $Kerf_5 = \{e\}$

Image de f_5 :

- Soit $y \in Imf_5$ alors il existe $x \in G$ tq $y = f_5(x) = axa^{-1}$ donc $y \in G$ et $Imf_5 \subset G$
- Soit $y \in G$, en prenant $x = a^{-1}ya \in G$ alors $f_5(x) = a(a^{-1}ya)a^{-1} = y$ donc $y \in Imf_5$ donc $G \subset Imf_5$

Au final : $Imf_5 = G$

C'est un isomorphisme de G dans G donc un automorphisme.

Exercice 47 **Inverses**

1. Chercher les inverses (pour la multiplication) de $\bar{4}$ et $\bar{5}$ dans $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/11\mathbf{Z}$, $\mathbf{Z}/14\mathbf{Z}$ et $\mathbf{Z}/43\mathbf{Z}$.
2. Chercher également les ordres de $\bar{4}$ et $\bar{5}$ dans les groupes multiplicatifs correspondants ainsi que les sous-groupes qu'ils engendrent.
3. Le théorème de Lagrange est-il bien satisfait ?

Cours : Groupe fini

Si le groupe G admet un nombre fini d'éléments, on appelle card G ou ordre de G son nombre d'éléments.

Théorème de Lagrange : Soit H un sous-groupe d'un groupe fini G, alors H est fini et son ordre divise l'ordre du groupe G.

Théorème : $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi a et n sont premiers entre eux.

1. Inverse de $\bar{4}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$

- On "voit" que $\bar{4}.\bar{2} = \bar{8} = \bar{1}$ donc l'inverse de $\bar{4}$ est $\bar{2}$ dans $\mathbb{Z}/7\mathbb{Z}$
- Autre méthode : Algorithme d'Euclide

4 est premier avec 7 donc d'après le théorème de Bézout $\exists\, u,\ v \in \mathbb{Z},\ 4u + 7v = 1$

Pour déterminer u et v, on utilise l'algorithme d'Euclide

$$7 = 1 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$
$$3 = 1 \times 3 + 0$$

donc $1 = 4 - 1 \times 3 = 4 - 1 \times (7 - 1 \times 4) = 2 \times 4 - 1 \times 7$

On passe aux modulos 7

$$\bar{1} = \bar{2} \times \bar{4} - \bar{1} \times \bar{7}$$
$$\bar{1} = \bar{2} \times \bar{4}$$

donc l'inverse de $\bar{4}$dans $\mathbb{Z}/7\mathbb{Z}$ est $\bar{2}$.

Ordre de $\bar{4}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$

$\bar{4}^2 = \overline{16} = \bar{2}$

$\bar{4}^3 = \bar{8} = \bar{1}$ L'ordre de $\bar{4}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$ est donc 3.

ou bien : $< \bar{4} >= \{\bar{1}\,;\ \bar{4}\,;\ \bar{4}^2 = \bar{2}\}$ donc $card(< \bar{4} >) = o(\bar{4}) = 3$

car le cardinal du sous-groupe engendré par $\bar{4}$ est l'ordre de l'élément $\bar{4}$.

Comme 7 est premier, alors tous les éléments de $\mathbb{Z}/7\mathbb{Z}$ sont inversibles à part $\bar{0}$.

Le groupe $(\mathbb{Z}/7\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/7\mathbb{Z}$ est d'ordre 6, comme $card(< \bar{4} >) = o(\bar{4}) = 3$ et que 3 divise 6 donc le théorème de Lagrange est bien vérifié.

Inverse de $\bar{5}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$

- On "voit" que $\bar{5}.\bar{3} = \overline{15} = \bar{1}$ donc l'inverse de $\bar{5}$ est $\bar{3}$ dans $\mathbb{Z}/7\mathbb{Z}$
- 5 est premier avec 7 donc d'après le théorème de Bézout $\exists\, u,\ v \in \mathbb{Z},\ 5u + 7v = 1$

Pour déterminer u et v, on utilise l'algorithme d'Euclide

$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$
$$2 = 1 \times 2 + 0$$

donc $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 1 \times 5) = 3 \times 5 - 2 \times 7$

On passe aux modulos 7

$$\bar{1} = \bar{3} \times \bar{5} - \bar{2} \times \bar{7}$$
$$\bar{1} = \bar{3} \times \bar{5}$$

donc l'inverse de $\bar{5}$dans $\mathbb{Z}/7\mathbb{Z}$ est $\bar{3}$.

Ordre de $\bar{5}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$

$\bar{5}^2 = \overline{25} = \bar{4}$
$\bar{5}^3 = \overline{20} = \bar{6}$
$\bar{5}^4 = \overline{30} = \bar{2}$
$\bar{5}^5 = \overline{10} = \bar{3}$
$\bar{5}^6 = \overline{15} = \bar{1}$

L'ordre de $\bar{5}$ dans $(\mathbb{Z}/7\mathbb{Z})^{\times}$ est donc 6.

Le groupe $(\mathbb{Z}/7\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/7\mathbb{Z}$ est d'ordre 6, comme $card(< \bar{5} >) = o(\bar{5}) = 6$ et que 6 divise 6 donc le théorème de Lagrange est bien vérifié.

Inverse de $\bar{4}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$

- On "voit" que $\bar{4}.\bar{3} = \overline{12} = \bar{1}$ donc l'inverse de $\bar{4}$ est $\bar{3}$ dans $\mathbb{Z}/11\mathbb{Z}$
- 4 est premier avec 11 donc d'après le théorème de Bézout $\exists\, u,\ v \in \mathbb{Z},\ 4u + 11v = 1$

Pour déterminer $u$et v, on utilise l'algorithme d'Euclide

$$11 = 2 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$
$$3 = 1 \times 3 + 0$$

donc $1 = 4 - 1 \times 3 = 4 - 1 \times (11 - 2 \times 4) = 3 \times 4 - 1 \times 11$

On passe aux modulos 11

$$\bar{1} = \bar{3} \times \bar{4} - \bar{1} \times \overline{11}$$
$$\bar{1} = \bar{3} \times \bar{4}$$

donc l'inverse de $\bar{4}$dans $\mathbb{Z}/11\mathbb{Z}$ est $\bar{3}$.

Ordre de $\bar{4}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$

$\bar{4}^2 = \overline{16} = \bar{5}$ $\quad$ $\bar{4}^3 = \bar{5} \times \bar{4} = \overline{20} = \bar{9}$ $\quad$ $\bar{4}^4 = \bar{9} \times \bar{4} = \overline{36} = \bar{3}$ $\quad$ $\bar{4}^5 = \bar{3} \times \bar{4} = \overline{12} = \bar{1}$

L'ordre de $\bar{4}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$ est donc 5.

Le groupe $(\mathbb{Z}/11\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/11\mathbb{Z}$ est d'ordre 10.

comme $card(< \bar{4} >) = o(\bar{4}) = 5$ et que 5 divise 10 donc le théorème de Lagrange est bien vérifié.

Inverse de $\bar{5}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$

- On "voit" que $\bar{5}.\bar{9} = \overline{45} = \bar{1}$ donc l'inverse de $\bar{5}$ est $\bar{9}$ dans $\mathbb{Z}/11\mathbb{Z}$
- 5 est premier avec 11 donc d'après le théorème de Bézout $\exists\, u,\, v \in \mathbb{Z},\, 5u + 11v = 1$

Pour déterminer $u$et v, on utilise l'algorithme d'Euclide

$11 = 2 \times 5 + 1$

$5 = 1 \times 5 + 0$ donc $1 = 11 - 2 \times 5$

On passe aux modulos 11

$\bar{1} = \overline{-2 \times 5}$

$\bar{1} = \bar{9} \times \bar{5}$

donc l'inverse de $\bar{5}$ dans $\mathbb{Z}/11\mathbb{Z}$ est $\bar{9}$.

Ordre de $\bar{5}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$

$\bar{5}^2 = \overline{25} = \bar{3}$ $\quad$ $\bar{5}^3 = \bar{3} \times \bar{5} = \overline{15} = \bar{4}$ $\quad$ $\bar{5}^4 = \bar{4} \times \bar{5} = \overline{20} = \bar{9}$ $\quad$ $\bar{5}^5 = \bar{9} \times \bar{5} = \overline{45} = \bar{1}$

L'ordre de $\bar{5}$ dans $(\mathbb{Z}/11\mathbb{Z})^{\times}$ est donc 5.

Le groupe $(\mathbb{Z}/11\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/11\mathbb{Z}$ est d'ordre 10.

Comme $card(< \bar{5} >) = o(\bar{5}) = 5$ et que 5 divise 10 donc le théorème de Lagrange est bien vérifié.

Inverse de $\bar{4}$ dans $U(\mathbb{Z}/14\mathbb{Z})$ c'est l'ensemble des inversibles de $\mathbb{Z}/14\mathbb{Z}$

$U(\mathbb{Z}/14\mathbb{Z}) = \{\bar{1}\,;\,\bar{3}\,;\,\bar{5}\,;\,\bar{9}\,;\,\overline{11}\,;\,\overline{13}\}$ c'est un ensemble à 6 éléments.

$\bar{a} \in U(\mathbb{Z}/14\mathbb{Z})$ lorsque a et 14 sont premiers entre eux.

4 n'est premier avec 14 donc $\bar{4}$ n'appartient pas à $U(\mathbb{Z}/14\mathbb{Z})$

Il n'a donc ni inverse ni ordre

Inverse de $\bar{5}$ dans $U(\mathbb{Z}/14\mathbb{Z}) = (\mathbb{Z}/14\mathbb{Z})^{\times}$

- On "voit" que $\bar{5}.\bar{3} = \overline{15} = \bar{1}$ donc l'inverse de $\bar{5}$ est 3 dans $\mathbb{Z}/14\mathbb{Z}$
- 5 est premier avec 14 donc d'après le théorème de Bézout $\exists\, u,\, v \in \mathbb{Z},\, 5u + 14v = 1$

Pour déterminer u et v, on utilise l'algorithme d'Euclide

$14 = 2 \times 5 + 4$

$5 = 1 \times 4 + 1$

$4 = 1 \times 4 + 0$

donc $1 = 5 - 1 \times 4 = 5 - 1\ (14 - 2 \times 5) = (-14 + 3 \times 5)$

On passe aux modulos 14

$$\overline{1} = \overline{3} \times \overline{5}$$

donc l'inverse de $\overline{5}$ dans $\mathbb{Z}/14\mathbb{Z}$ est $\overline{3}$.

Ordre de $\overline{5}$ dans $(\mathbb{Z}/14\mathbb{Z})^{\times}$

Le groupe des inversibles de $\mathbb{Z}/14\mathbb{Z}$ est d'ordre 6.

$\overline{5}^2 = \overline{25} = \overline{11}$ $\overline{5}^3 = \overline{11} \times \overline{5} = \overline{55} = \overline{13}$ $\overline{5}^4 = \overline{13} \times \overline{5} = \overline{65} = \overline{9}$ $\overline{5}^5 = \overline{9} \times \overline{5} = \overline{45} = \overline{3}$

$\overline{5}^6 = \overline{3} \times \overline{5} = \overline{15} = \overline{1}$ donc 5 est d'ordre 6

$U(\mathbb{Z}/14\mathbb{Z}) = \{\overline{1}\,;\,\overline{3}\,;\,\overline{5}\,;\,\overline{9}\,;\,\overline{11}\,;\,\overline{13}\}$ c'est un ensemble à 6 éléments.

Comme $card(<\overline{5}>) = o(\overline{5}) = 6$ et que 6 divise 6 donc le théorème de Lagrange est bien vérifié.

Inverse de $\overline{4}$ dans $(\mathbb{Z}/43\mathbb{Z})^{\times}$

- On "voit" que $\overline{4}.\overline{11} = \overline{44} = \overline{1}$ donc l'inverse de $\overline{4}$ est $\overline{11}$ dans $\mathbb{Z}/43\mathbb{Z}$
- 4 est premier avec 43 donc d'après le théorème de Bézout $\exists\, u,\, v \in \mathbb{Z},\, 4u + 43v = 1$

Pour déterminer $u$et v, on utilise l'algorithme d'Euclide

$$43 = 10 \times 4 + 3$$
$$4 = 1 \times 3 + 1$$
$$3 = 1 \times 3 + 0$$

donc $1 = 4 - 1 \times 3 = 4 - 1 \times (43 - 10 \times 4) = 11 \times 4 - 1 \times 43$

On passe aux modulos 43

$$\overline{1} = \overline{11} \times \overline{4}$$

donc l'inverse de $\overline{4}$dans $\mathbb{Z}/43\mathbb{Z}$ est $\overline{11}$.

Ordre de $\overline{4}$ dans $(\mathbb{Z}/43\mathbb{Z})^{\times}$

$\overline{4}^7 = \overline{16384} = \overline{1}$ l'ordre ne peut pas être inférieur car c'est un diviseur de 7

L'ordre de $\overline{4}$ dans $(\mathbb{Z}/43\mathbb{Z})^{*}$ est donc 7.

Le groupe $(\mathbb{Z}/43\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/43\mathbb{Z}$ est d'ordre 42.

comme $card(<\overline{4}>) = o(\overline{4}) = 7$ et que 7 divise 42 donc le théorème de Lagrange est bien vérifié.

Inverse de $\overline{5}$ dans $(\mathbb{Z}/43\mathbb{Z})^{\times}$

- On "voit" que $\overline{5}.\overline{26} = \overline{130} = \overline{1}$ donc l'inverse de $\overline{5}$ est $\overline{26}$ dans $\mathbb{Z}/43\mathbb{Z}$
- 5 est premier avec 43 donc d'après le théorème de Bézout $\exists\, u,\, v \in \mathbb{Z},\, 5u + 43v = 1$

Pour déterminer $u$et v, on utilise l'algorithme d'Euclide

$$43 = 8 \times 5 + 3$$
$$5 = 1 \times 3 + 2$$
$$3 = 1 \times 2 + 1$$
$$2 = 2 \times 1 + 0$$

donc $1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 1 \times 3) = 43 - 8 \times 5 - 1 \times (5 - 1 \times (43 - 8 \times 5))$
donc $1 = 2 \times 43 - 17 \times 5$ On passe aux modulos 43

$\overline{1} = \overline{-17} \times \overline{5}$

$\overline{1} = \overline{26} \times \overline{5}$ donc l'inverse de $\overline{5}$ dans $\mathbb{Z}/43\mathbb{Z}$ est $\overline{26}$.

Ordre de $\overline{5}$ dans $(\mathbb{Z}/43\mathbb{Z})^{\times}$

Soit on les essaye dans l'ordre, c'est long mais ça fait des petits nombres, soit on utilise la calculatrice du PC et on commence par 21

$\overline{5}^{21} = \overline{476\,837\,158\,203\,125} = \overline{42}$ $\overline{5}^{14} = \overline{6\,103\,515\,625} = \overline{36}$ $\overline{5}^{6} = \overline{16}$

Comme les ordres plus petits doivent diviser 6, 14 ou 21

l'ordre de $\overline{5}$ dans $(\mathbb{Z}/43\mathbb{Z})^{\times}$ est 42.

Le groupe $(\mathbb{Z}/43\mathbb{Z})^{\times}$ des inversibles de $\mathbb{Z}/43\mathbb{Z}$ est d'ordre 42.

comme $card(< \overline{5} >) = o(\overline{5}) = 42$ et que 42 divise 42 donc le théorème de Lagrange est bien vérifié.

Exercice 48 On note $\mathbf{Q}[\sqrt{2}]$ l'ensemble $\mathbf{Q}[\sqrt{2}] = \{p + q\sqrt{2} \mid p, q \in \mathbf{Q}\}$.

1. Montrer que $(\mathbf{Q}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbf{R}, +)$.
2. Montrer que $(\mathbf{Q}[\sqrt{2}]^*, \times)$ est un sous-groupe de $(\mathbf{R}^*, \times)$.
   On définit de manière analogue l'ensemble $\mathbf{Q}[\sqrt{3}]$ et on considère l'application

$$f : \begin{array}{ccc} \mathbf{Q}[\sqrt{2}] & \to & \mathbf{Q}[\sqrt{3}] \\ p + q\sqrt{2} & \mapsto & p + q\sqrt{3} \end{array}$$

3. Cette application est-elle bien définie ?
4. Montrer que f est une bijection.
5. Montrer que f est un isomorphisme entre les groupes $(\mathbf{Q}[\sqrt{2}], +)$ et $(\mathbf{Q}[\sqrt{3}], +)$?
6. Que vaut $f(\sqrt{2}^2)$? La fonction f définit-elle un isomorphisme entre les groupes $(\mathbf{Q}[\sqrt{2}]^*, \times)$ et $(\mathbf{Q}[\sqrt{3}]^*, \times)$?

Définition sous-groupe : Soit $(G, *)$ un groupe et $H \subset G$.
H est un sous-groupe de G si :

- stabilité de la loi : si $(x, y) \in H$ alors $x * y \in H$
- élément neutre : $e \in H$
- symétrique : si $x \in H$ alors $x^{-1} \in H$

Ou bien si $(x, y) \in H$ alors $x * y^{-1} \in H$

1. Montrer que $(\mathbf{Q}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbf{R}, +)$.
2. Montrer que $(\mathbf{Q}[\sqrt{2}]^*, \times)$ est un sous-groupe de $(\mathbf{R}^*, \times)$.

1. **Méthode 1** :

- Stabilité de la loi : Soient $(p + q\sqrt{2})$ et $(p' + q'\sqrt{2})$ deux éléments de $\mathbb{Q}[\sqrt{2}]$, alors

$p + q\sqrt{2} + p' + q'\sqrt{2} = (p + p') + (q + q')\sqrt{2}$ avec $p + p' \in \mathbb{Q}$ et $q + q' \in \mathbb{Q}$ donc

$p + q\sqrt{2} + p' + q'\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, la loi est stable.

- Elément neutre : $e = 0 = 0 + 0\sqrt{2}$ donc $e \in \mathbb{Q}[\sqrt{2}]$
- Symétrique : si $p + q\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ alors $-p - q\sqrt{2}$ est le symétrique de $p + q\sqrt{2}$ et il appartient bien à $\mathbb{Q}[\sqrt{2}]$

Donc $(\mathbb{Q}[\sqrt{2}], +)$ est donc un sous-groupe de $(\mathbb{R}, +)$

Méthode 2 : Soit $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ et $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$\mathbb{Q}[\sqrt{2}]$est stable par addition et passage à l'opposé car

$$a + b\sqrt{2} + (-c - d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$$

$(\mathbb{Q}[\sqrt{2}], +)$ est donc un sous-groupe de $(\mathbb{R}, +)$.

On a utilisé que si $(x, y) \in H$ et $x * y^{-1} \in H$ alors (H,+) est un sous-groupe de (G,+)

2. **Méthode 1 :**

- Stabilité de la loi : Soient $(p + q\sqrt{2})$ et $(p' + q'\sqrt{2})$ deux éléments de $\mathbb{Q}[\sqrt{2}]$, alors

$(p + q\sqrt{2})(p' + q'\sqrt{2}) = pp' + 2qq' + (pq' + p'q)\sqrt{2}$ avec $pp' + 2qq' \in \mathbb{Q}$ et $pq' + p'q \in \mathbb{Q}$ donc

$(p + q\sqrt{2})(p' + q'\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$, la loi est stable.

- Elément neutre : $e = 1 = 1 + 0\sqrt{2}$ donc $e \in \mathbb{Q}[\sqrt{2}]$
- Symétrique : si $p + q\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ alors on cherche y tel que $(p + q\sqrt{2}) \times y = 1$

ce qui donne $y = \frac{1}{p+q\sqrt{2}} = \frac{(p-q\sqrt{2})}{(p+q\sqrt{2})(p-q\sqrt{2})} = \frac{p-q\sqrt{2}}{p^2-2q^2} = \frac{p}{p^2-2q^2} - \frac{q}{p^2-2q^2}\sqrt{2}$ et il appartient bien à $\mathbb{Q}[\sqrt{2}]$

Donc $(\mathbb{Q}[\sqrt{2}], +)$ est donc un sous-groupe de $(\mathbb{R}, +)$

Méthode 2 :

$(\mathbb{Q}[\sqrt{2}]^*, \times)$ est stable par multiplication et passage à l'inverse car

si $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]^*$ et $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$$\frac{c+d\sqrt{2}}{a+b\sqrt{2}} = \frac{(c+d\sqrt{2})(a-b\sqrt{2})}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{ac-2bd+(ad+bc)\sqrt{2}}{a^2-2b^2} = \frac{ac-2bd}{a^2-2b^2} - \frac{(ad+bc)\sqrt{2}}{a^2-2b^2}$$

$(\mathbb{Q}[\sqrt{2}]^*, \times)$est donc un sous-groupe de $(\mathbb{R}^*, \times)$

On a utilisé que si $(x, y) \in H$ et $x * y^{-1} \in H$ alors (H,+) est un sous-groupe de (G,+)

On définit de manière analogue l'ensemble $\mathbf{Q}[\sqrt{3}]$ et on considère l'application

$$f : \begin{array}{ccc} \mathbf{Q}[\sqrt{2}] & \to & \mathbf{Q}[\sqrt{3}] \\ p+q\sqrt{2} & \mapsto & p+q\sqrt{3} \end{array}$$

3. Cette application est-elle bien définie ?
4. Montrer que f est une bijection.

3. Un nombre ne peut avoir deux écritures différentes de la forme

$$p + q\sqrt{2}$$

Si c'était le cas, on aurait

$$p + q\sqrt{2} = p' + q'\sqrt{2} \text{donc } \frac{p-p'}{q'-q} = \sqrt{2}$$

ce qui n'est pas possible car $\sqrt{2}$est irrationnel.
Il en est de même pour $p + q\sqrt{3}$
Pour une application, tout élément de l'ensemble de départ doit être associé à un unique élément de l'ensemble d'arrivée.
Ici, un élément de $\mathbb{Q}[\sqrt{2}]$est déterminé par son écriture $p + q\sqrt{2}$et il est associé à $p + q\sqrt{3}$ qui est déterminé de manière unique par son écriture donc la fonction est bien définie.

4. Surjection : Soit $y \in \mathbb{Q}[\sqrt{3}]$, alors il existe $(p, q) \in \mathbb{Q}^2$ tel que $y = p + q\sqrt{3}$
Prenons $x = p + q\sqrt{2}$ alors $f(x) = y$ ainsi pour tout $y \in \mathbb{Q}[\sqrt{3}]$, il existe $x \in \mathbb{Q}[2]$ tq $f(x) = y$
on en déduit que f est surjective,

Injection : Soient $(x, x') \in \mathbb{Q}[\sqrt{2}]$ avec $x = p + q\sqrt{2}$ et $x' = p' + q'\sqrt{2}$, et $p \neq p'$ et $q \neq q'$
tels que $f(x) = f(x')$ alors $p + q\sqrt{3} = p' + q'\sqrt{3}$ implique $\sqrt{3} = \frac{p-p'}{q'-q}$ce qui est absurde car $\sqrt{3}$ n'est pas rationnel donc $p = p'$ et $q = q'$, ce qui veut dire que $x = x'$, donc f est injective.
Ainsi f est surjective et injective, c'est une bijection

5. Montrer que f est un isomorphisme entre les groupes $(\mathbf{Q}[\sqrt{2}], +)$ et $(\mathbf{Q}[\sqrt{3}], +)$?
6. Que vaut $f(\sqrt{2}^2)$? La fonction f définit-elle un isomorphisme entre les groupes $(\mathbf{Q}[\sqrt{2}]^*, \times)$ et $(\mathbf{Q}[\sqrt{3}]^*, \times)$?

5. $f(p + q\sqrt{2} + (p' + q'\sqrt{2}) = f(p + p' + (q + q')\sqrt{2}) = p + p' + (q + q')\sqrt{3}$
$f(p + q\sqrt{2}) + f(p' + q'\sqrt{2}) = p + q\sqrt{2} + (p' + q'\sqrt{3}) = p + p' + (q + q')\sqrt{3}$
$f$est donc bien un morphisme du groupe additif $\mathbb{Q}[\sqrt{2}]$dans le groupe additif $\mathbb{Q}[\sqrt{3}]$, c'est donc un isomorphisme, à savoir un morphisme bijectif.

6. $f(\sqrt{2}^2) = f(2) = 2$ et $f(\sqrt{2})^2 = \sqrt{3}^2 = 3$ donc $f(\sqrt{2} \times \sqrt{2}) \neq f(\sqrt{2}) \times f(\sqrt{2})$
f n'est pas un morphisme entre les groupes multiplicatifs