

## 10.5 Relation d'équivalence modulo un sous-groupe

DANS CETTE SECTION, NOUS REPRENONS ET APPROFONDISSEONS DES NOTIONS VUES EN  $L_1$  ; NOUS ALLONS COMMENCER PAR TRAVAILLER UN EXEMPLE : LES SOUS-GROUPES DE  $\mathbb{Z}$

### Etude des sous-groupes de $\mathbb{Z}$

On sait que  $(\mathbb{Z}, +)$  est un groupe additif. L'objet de ce qui suit est de s'intéresser aux sous groupes de  $\mathbb{Z}$

#### 10.5.1 Définition

Soit  $m \in \mathbb{Z}$ . L'ensemble des multiples de  $m$  est défini par :

$$m\mathbb{Z} = \{u \in \mathbb{Z} \text{ tel qu'il existe } k \in \mathbb{Z} \text{ tel que } u = mk\}$$

#### Remarque 15 :

1. Nous avons, de manière évidente  $m\mathbb{Z} = -m\mathbb{Z}$ . Nous allons donc, désormais, ne considérer que des ensembles du type  $m\mathbb{Z}$  avec  $m \in \mathbb{N}$
2. Pour  $b \in \mathbb{Z}$ , on définit l'ensemble  $m\mathbb{Z} + b$  par :

$$m\mathbb{Z} + b = \{u \in \mathbb{Z} \text{ tel qu'il existe } k \in \mathbb{Z} \text{ tel que } u = mk + b\}$$

#### Exercice 12 :

Confirmez ou infirmez les égalités suivantes :

1.  $3\mathbb{Z} + 2 = 3\mathbb{Z}$
2.  $2\mathbb{Z} + 4 = 2\mathbb{Z}$
3.  $5\mathbb{Z} + 25 = 5\mathbb{Z}$
4.  $7\mathbb{Z} + 7\mathbb{Z} = 7\mathbb{Z}$

#### 10.5.2 Théorème

Les sous groupes de  $(\mathbb{Z}, +)$  sont tous de la forme  $a\mathbb{Z}$  avec  $a \in \mathbb{N}$   
Les seuls sous groupes de  $\mathbb{Z}$  sont donc les ensembles de multiples

#### Démonstration

1. Soit  $a \in \mathbb{N}$  Montrons que  $a\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ 
  - (a) Premièrement,  $a\mathbb{Z} \neq \emptyset$ , puisque  $0 \in a\mathbb{Z}$
  - (b) Soient  $x \in a\mathbb{Z}$  et  $y \in a\mathbb{Z}$ , alors, nous avons  $x = ak$  et  $y = ak'$ , avec  $k \in \mathbb{Z}$  et  $k' \in \mathbb{Z}$  Donc :

$$x - y = ak - ak' = a(k - k')$$

Ce qui montre que  $x - y$  est un multiple de  $a$  et que  $x - y \in a\mathbb{Z}$

Nous en concluons que  $a\mathbb{Z}$  est un sous groupe de  $(\mathbb{Z}, +)$

2. Réciproquement, soit  $H$  un sous-groupe de  $(\mathbb{Z}, +)$

Tout d'abord,  $0 \in H$ .

Soit  $a \in H$  ; alors, de la structure de groupe de  $H$ , on déduit que  $-a \in H$ . Soit donc  $a$  le plus petit élément positif de  $H$ . Alors, tout multiple de  $a$  est dans  $H$ .

Soit  $k \in H$ . Effectuons la division euclidienne de  $k$  par  $a$  :

$$k = qa + r \text{ avec } 0 \leq r < a$$

Or,  $r = k - qa$  est dans  $H$ , ce qui contredit le fait que si  $r \neq 0$ ,  $a$  soit le plus petit élément positif de  $H$  ; donc  $r = 0$  et  $k = qa$

$H$  est donc l'ensemble des multiples de  $a$

## 10.5.3 Proposition

La relation  $\equiv$  définie dans  $\mathbb{Z}$  par

$$x \equiv y [n] \iff x - y \in n\mathbb{Z}$$

est une relation d'équivalence.

C'est la relation de congruence modulo  $n$ .

Cette relation est compatible avec l'addition dans  $\mathbb{Z}$ , c'est à dire :

$$(\forall z \in \mathbb{Z}) (x \equiv y [n] \implies x + z \equiv y + z [n])$$

**Démonstration**

La démonstration est évidente

**Remarque 16 :**

$x \equiv y [n] \iff x - y \in n\mathbb{Z}$ , c'est à dire qu'il existe  $q \in \mathbb{Z}$  tel que  $x - y = qn \iff x = qn + y$ . On reconnaît là, la division euclidienne dans  $\mathbb{Z}$ . On appelle  $\mathbb{Z}/n\mathbb{Z}$  l'ensemble quotient donc  $n$  éléments. Donc :

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + 0; n\mathbb{Z} + 1; \dots; n\mathbb{Z} + (n-1)\} = \{\bar{0}; \bar{1}; \dots; \overline{(n-1)}\}$$

$\mathbb{Z}/n\mathbb{Z}$  muni de l'addition est un groupe ; c'est un groupe fini à  $n$  éléments.

**Exemple 10 :**

1. Etudions la congruence modulo 6, en faisant la table d'addition.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

2. Il y a, dans  $\mathbb{Z}/6\mathbb{Z}$ , deux sous-groupes :  $\{\bar{0}, \bar{2}, \bar{4}\}$  et  $\{\bar{0}, \bar{3}\}$

**Généralisation**

## 10.5.4 Notations

Soit  $G$  un groupe (non forcément commutatif) et  $H \subset G$  un sous-ensemble de  $G$ . Dans cette section nous noterons, pour  $x \in G$  :

$$xH = \{z \in G \text{ tel que } z = xy \text{ où } y \in H\} \text{ et } Hx = \{z \in G \text{ tel que } z = yx \text{ où } y \in H\}$$

**Remarque 17 :**

Que se passe-t-il dans  $(\mathbb{Z}, +)$ ? En fait, si  $p\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$  nous avons  $xH$  se traduit par

$$x + p\mathbb{Z} = \{z \in \mathbb{Z} \text{ tel que } z = x + py \text{ où } y \in \mathbb{Z}\}$$

## 10.5.5 Définition

Soit  $G$  un groupe et  $\mathfrak{R}$  une relation d'équivalence sur  $G$ .

1. On dit que  $\mathfrak{R}$  est régulière à gauche si

$$(\forall x \in G) (\forall y \in G) (\forall z \in G) ((x\mathfrak{R}y) \implies (zx\mathfrak{R}zy))$$

2. On dit que  $\mathfrak{R}$  est régulière à droite si

$$(\forall x \in G) (\forall y \in G) (\forall z \in G) ((x\mathfrak{R}y) \implies (xz\mathfrak{R}yz))$$

$\mathfrak{R}$  est dite régulière si elle est à la fois régulière à droite et régulière à gauche

## 10.5.6 Proposition

Soit  $G$  un groupe d'élément neutre  $e$  et  $\mathfrak{R}$  une relation d'équivalence régulière à gauche sur  $G$   
Alors  $\dot{e}$  est un sous groupe de  $G$

**Démonstration**

1. Tout d'abord,  $\dot{e} \neq \emptyset$  puisque  $e \in \dot{e}$
2. Soit  $y \in \dot{e}$ . Alors, nous avons  $y\mathfrak{R}e$   
De la régularité à gauche de  $\mathfrak{R}$ , nous avons  $y\mathfrak{R}e \implies y^{-1}y\mathfrak{R}y^{-1}e$ , c'est à dire  $y^{-1}\mathfrak{R}e$  et donc  $y^{-1} \in \dot{e}$ .  
Ainsi, si  $y \in \dot{e}$ , alors  $y^{-1} \in \dot{e}$
3. Soient  $x \in \dot{e}$  et  $y \in \dot{e}$ ; alors, nous avons  $x\mathfrak{R}e$  et  $y\mathfrak{R}e$   
De la régularité à gauche de  $\mathfrak{R}$ , nous avons  $y\mathfrak{R}e \implies y^{-1}x\mathfrak{R}y^{-1}e$ , c'est à dire  $y^{-1}x\mathfrak{R}y^{-1}$ . Comme  $y^{-1} \in \dot{e}$ , c'est à dire  $y^{-1}\mathfrak{R}e$ , par transitivité de la relation d'équivalence  $\mathfrak{R}$ , nous avons  $y^{-1}x\mathfrak{R}e$ , c'est à dire  $y^{-1}x \in \dot{e}$

Donc  $\dot{e}$  est un sous groupe de  $G$

**Remarque 18 :**

De la même manière, si  $\mathfrak{R}$  une relation d'équivalence régulière à droite sur  $G$ ,  $\dot{e}$  est un sous groupe de  $G$ . (Démonstration sans difficulté)

## 10.5.7 Proposition

Soit  $G$  un groupe et  $H \subset G$ , un sous-groupe de  $G$ .  
Soit  $\mathfrak{R}$  la relation ainsi définie :

$$(\forall x \in G) (\forall y \in G) (x\mathfrak{R}y) \iff (x^{-1}y \in H)$$

Alors,  $\mathfrak{R}$  est une relation d'équivalence

**Démonstration**1. **Réflexivité**

Soit  $x \in G$ ; alors  $xx^{-1} = e \in H$  et donc  $x\mathfrak{R}x$

2. **Symétrie**

Soient  $x \in G$  et  $y \in G$  tels que  $x\mathfrak{R}y$ .

Alors, par la définition de  $\mathfrak{R}$ ,  $x^{-1}y \in H$ .  $H$  étant un sous groupe de  $G$ , alors l'inverse de  $x^{-1}y$  est aussi dans  $H$ , et donc nous avons :

$$x\mathfrak{R}y \iff x^{-1}y \in H \iff (x^{-1}y)^{-1} \in H \iff y^{-1}x \in H \iff y\mathfrak{R}x$$

Et donc,  $\mathfrak{R}$  est symétrique

## 3. Transitivité

Soient  $x \in G$ ,  $y \in G$  et  $z \in G$  tels que  $x\mathfrak{R}y$  et  $y\mathfrak{R}z$ . Alors :

—  $x\mathfrak{R}y$  est équivalent à  $x^{-1}y \in H$

—  $y\mathfrak{R}z$  est équivalent à  $y^{-1}z \in H$

$H$  étant un sous-groupe, le produit de 2 éléments de  $H$  est encore un élément de  $H$ , et donc  $(x^{-1}y)(y^{-1}z) \in H$ ; c'est à dire  $x^{-1}z \in H$ , et donc, nous avons  $x\mathfrak{R}z$ .

La relation  $\mathfrak{R}$  est donc transitive

En conclusion, la relation  $\mathfrak{R}$  est bien une relation d'équivalence.

**Remarque 19 :**

La définition de la relation définie en 10.5.7 est équivalente à  $(x\mathfrak{R}y) \iff (y^{-1}x \in H)$ , puisque  $y^{-1}x$  est l'inverse de  $x^{-1}y$  et que  $H$  est un sous-groupe de  $G$ .

**Exemple 11 :**

Le premier exemple de telle relation est la relation d'équivalence dans  $\mathbb{Z}$  liée à la congruence modulo  $n$  :

$$x \equiv y \pmod{n} \iff x - y \in n\mathbb{Z}$$

## 10.5.8 Proposition

Soit  $G$  un groupe et  $H \subset G$ , un sous-groupe de  $G$ . Soit  $\mathfrak{R}$  la relation définie en 10.5.7.  
Alors  $\mathfrak{R}$  est régulière à gauche

**Démonstration**

Soient  $x \in G$  et  $y \in G$  tels que  $x\mathfrak{R}y$ ; alors  $x^{-1}y \in H$

Soit  $z \in G$ ; alors  $x^{-1}y = x^{-1}z^{-1}zy$  et donc  $x^{-1}z^{-1}zy \in H$ . Comme  $x^{-1}z^{-1} = (zx)^{-1}$ , nous avons alors  $(zx)^{-1}zy \in H$ , c'est à dire  $zx\mathfrak{R}zy$

$\mathfrak{R}$  est donc régulière à gauche

**Remarque 20 :**

Soit  $G$  un groupe et  $H \subset G$  sous-groupe de  $G$ ; on définit la relation  $\mathfrak{S}$  par :

$$(\forall x \in G) (\forall y \in G) (x\mathfrak{S}y) \iff (xy^{-1} \in H)$$

Alors,  $\mathfrak{S}$  est aussi **une relation d'équivalence**, mais régulière à droite.

## 10.5.9 Proposition

Soit  $G$  un groupe et  $H \subset G$ , un sous-groupe de  $G$ . Soit  $\mathfrak{R}$  la relation définie en 10.5.7.  
Alors  $H$  est la classe d'équivalence de l'élément neutre  $e$

**Démonstration**

— Soit  $\dot{e}$  la classe de  $e$  et  $x \in \dot{e}$ . Alors,  $e\mathfrak{R}x$ , c'est à dire  $e^{-1}x \in H$ ; comme  $e^{-1}x = x$ , nous avons  $x \in H$ ; nous en déduisons  $\dot{e} \subset H$

— Soit  $x \in H$ ; alors, comme  $H$  est un sous groupe,  $x^{-1} \in H$ ; comme  $x^{-1} = x^{-1}e$ , nous avons  $x^{-1}e \in H$  et donc  $x\mathfrak{R}e$  et donc  $x \in \dot{e}$ ; nous en déduisons  $H \subset \dot{e}$

En conclusion,  $H = \dot{e}$

**Remarque 21 :**

On démontrerait de même, que dans la relation d'équivalence  $\mathfrak{S}$ ,  $H$  est aussi la classe d'équivalence de l'élément neutre  $e$

## 10.5.10 Proposition

Soit  $G$  un groupe et  $H \subset G$ , un sous-groupe de  $G$ . Soit  $\mathfrak{R}$  la relation définie en 10.5.7.  
Alors la classe d'équivalence de  $y \in G$  est  $yH$

**Démonstration**

Soit  $\dot{y}$  la classe de  $y$ .

1. Soit  $x \in \dot{y}$ ; alors  $x\mathfrak{R}y$  et donc  $y^{-1}x \in H$ , c'est à dire qu'il existe  $z \in H$  tel que  $y^{-1}x = z$  et donc  $yy^{-1}x = yz$ , c'est à dire  $x = yz$  et donc  $x \in yH$

Nous avons donc  $\dot{y} \subset yH$

2. Soit  $u \in H$ ; alors  $u\mathfrak{R}e$  et donc, par régularité à gauche de  $\mathfrak{R}$ , nous avons  $yu\mathfrak{R}y$ ; et donc  $yu \in \dot{y}$ ; c'est à dire  $yH \subset \dot{y}$

Nous avons donc  $\dot{y} = yH$

**Remarque 22 :**

1. Pour  $\mathfrak{S}$  la relation d'équivalence, il est facile de démontrer que la classe d'équivalence de  $y \in G$  est  $Hy$
2. Il est évident que le plus souvent, les ensembles  $yH$  ou  $Hy$  ne sont pas des sous-groupes
3.  $\Rightarrow$  Il y a une correspondance biunivoque entre les sous-groupes  $H \subset G$  et les relations d'équivalence régulière à gauche.  
 $\Rightarrow$  De même, il y a une correspondance biunivoque entre les sous-groupes  $H \subset G$  et les relations d'équivalence régulière à droite.  
 $\Rightarrow$  En définitive, à tout sous-groupe  $H$ , est attaché une relation d'équivalence régulière à gauche, et une relation d'équivalence régulière à droite. Elles sont, en général, différentes si  $G$  n'est pas abélien

## 10.5.11 Proposition

Soient  $G$  un groupe et  $H \subset G$ , un sous-groupe de  $G$   
Alors, il existe une bijection de l'ensemble des classes à droite modulo  $H$  sur l'ensemble des classes à gauche modulo  $H$ , et donc, si  $G$  est un groupe d'ordre fini :

$$\text{Card } G/\mathfrak{S} = \text{Card } G/\mathfrak{R}$$

**Démonstration**

Soit  $\varphi : G/\mathfrak{R} \rightarrow G/\mathfrak{S}$  définie par

$$\begin{cases} \varphi : G/\mathfrak{R} & \rightarrow & G/\mathfrak{S} \\ xH & \mapsto & \varphi(xH) = Hx^{-1} \end{cases}$$

1.  $\varphi$  est injective

Supposons que  $\varphi(xH) = \varphi(yH)$ , c'est à dire  $Hx^{-1} = Hy^{-1}$ ; il faut montrer que  $xH = yH$

Si  $Hx^{-1} = Hy^{-1}$ , alors  $x^{-1}\mathfrak{S}y^{-1}$  et donc,  $x^{-1}(y^{-1})^{-1} \in H$ , c'est à dire  $x^{-1}y \in H$ .

Nous avons donc  $x\mathfrak{R}y$  et donc  $xH = yH$

2.  $\varphi$  est surjective

Soit  $Hy \in G/\mathfrak{S}$ ; alors,  $y^{-1}H$  est tel que  $\varphi(y^{-1}H) = Hy$

$\varphi$  est donc surjective

$\varphi$  étant injective et surjective, est donc bijective.

Si  $G$  est fini,  $G/\mathfrak{S}$  et  $G/\mathfrak{R}$  sont des ensembles finis qui sont en bijection et qui ont donc le même nombre d'éléments, c'est à dire  $\text{Card } G/\mathfrak{S} = \text{Card } G/\mathfrak{R}$

## 10.5.12 Définition

Soit  $G$  un groupe fini et  $H \subset G$  un sous groupe de  $G$ .  
 Le nombre de classes d'équivalence modulo  $H$  (c'est à dire  $\text{Card } G/\mathfrak{R} = \text{Card } G/\mathfrak{S}$ ) s'appelle indice de  $H$  en  $G$   
 On le note :  $i(H) = [G : H]$

## 10.5.13 Théorème de Lagrange

1. L'ordre d'un groupe est le nombre d'éléments de ce groupe (cf 10.8.1)
2. Soit  $G$  un groupe d'ordre fini et  $H \subset G$  un sous-groupe de  $G$   
 Alors, l'ordre du sous-groupe divise l'ordre du groupe

**Démonstration**

Soit  $\mathfrak{R}$  la relation d'équivalence modulo  $H$  et  $G/\mathfrak{R}$  l'ensemble des classes d'équivalence.

1.  $G/\mathfrak{R}$  est un ensemble fini ; soit  $i = [G : H]$  son cardinal (c'est l'indice de  $H$  en  $G$ )
2.  $G/\mathfrak{R}$  forme une partition de  $G$
3. Chaque élément de  $G/\mathfrak{R}$  est de type  $xH$ , avec  $x \in G$  et est un ensemble de même cardinal que  $H$
4. Donc, si  $G/\mathfrak{R} = \{x_1H, \dots, x_iH\}$ , nous avons :

$$G = \bigcup_{k=1}^i x_k H \text{ et si } k \neq k', x_k H \cap x_{k'} H = \emptyset$$

Donc,  $\text{card } G = i \times \text{Card } H$

L'ordre de  $H$  divise donc l'ordre de  $G$

**Remarque 23 :**

1. Nous avons donc :  $\text{Card } G = [G : H] \times \text{Card } H$
2. On dit souvent, pour les groupes finis :

**L'ordre d'un sous-groupe divise l'ordre du groupe**

**Exercice 13 :**

Soient  $H$  et  $K$  deux sous-groupes finis d'un groupe  $G$  d'élément neutre  $e$ . Si  $H$  et  $K$  sont d'ordres premiers entre eux, montrer que  $H \cap K = \{e\}$ .

## 10.5.14 Applications du théorème de Lagrange

Soit  $G$  un groupe fini.

1. Soient  $S \subset G$  et  $T \subset G$ , 2 sous groupes de  $G$  tels que  $S \subset T$ . Alors :

$$[G : S] = [G : T] \times [T : S]$$

2. Soient  $H \subset G$  et  $K \subset G$ , 2 sous-groupes de  $G$ . Alors :

$$\text{Card } KH = \frac{\text{Card } H \times \text{Card } K}{\text{Card } H \cap K}$$

Où  $KH = \{g \in G \text{ tel qu'il existe } h \in H \text{ et } k \in K \text{ tels que } g = hk\}$

**Démonstration**

Ces applications peuvent être considérées comme des exercices résolus

## 1. Montrons le premier point

En utilisant le théorème de Lagrange, nous avons :

$$\star \text{Card } T = \text{Card } S \times [T : S]$$

$$\star \text{Card } G = \text{Card } T \times [G : T]$$

$$\star \text{Card } G = \text{Card } S \times [G : S]$$

Ce qui nous donne :

$$\text{Card } S \times [G : S] = \text{Card } T \times [G : T] = \text{Card } S \times [T : S] \times [G : T]$$

On peut alors simplifier par  $\text{Card } S$ , qui est non nul, et nous obtenons :  $[G : S] = [T : S] \times [G : T]$

Ce que nous voulions

2. Montrons que  $\text{Card } KH = \frac{\text{Card } H \times \text{Card } K}{\text{Card } H \cap K}$ 

(a)  $G$  étant fini, il en est de même de  $H$ , de  $K$  et de  $H \cap K$ . Comme  $(H \cap K) \subset K$ , considérons les classes d'équivalence à gauche modulo  $H \cap K$  :

$$k_1(H \cap K), k_2(H \cap K), \dots, k_n(H \cap K)$$

où  $n = [K \cap K : H]$ , et nous avons  $\text{Card } K = \text{Card } (H \cap K) \times [K \cap K : H]$

(b) Nous allons montrer que les ensembles  $k_1H, k_2H, \dots, k_nH$  forme une partition de  $KH$

Si nous montrons cela, alors  $\text{Card } KH = n \times \text{Card } H = [K \cap K : H] \times \text{Card } H$ . Comme

$$[K \cap K : H] = \frac{\text{Card } K}{\text{Card } (H \cap K)}, \text{ nous avons :}$$

$$\text{Card } KH = [K \cap K : H] \times \text{Card } H = \frac{\text{Card } K}{\text{Card } (H \cap K)} \times \text{Card } H = \frac{\text{Card } K \text{Card } H}{\text{Card } (H \cap K)}$$

Ce que nous voulions.

i. Montrons que  $\bigcup_{j=1}^n k_jH = KH$ 

— Soit  $u \in \bigcup_{j=1}^n k_jH$

Alors, il existe  $j \in \{1, \dots, n\}$  tel que  $u \in k_jH$ ; il existe donc  $x \in H$  tel que  $u = k_jx$ .

Donc  $u \in KH$ , et donc  $\bigcup_{j=1}^n k_jH \subset KH$

— Réciproquement, soit  $g \in KH$ ; alors, il existe  $k \in K$  et  $h \in H$  tels que  $g = kh$ .

Comme les  $k_1(H \cap K), k_2(H \cap K), \dots, k_n(H \cap K)$  forment une partition de  $K$ , il existe  $j \in \{1, \dots, n\}$  tel que  $k = k_j\lambda$  où  $\lambda \in H \cap K$ , et donc  $g = k_j \times \lambda \times h$ . Comme

$\lambda h \in H$ , nous avons  $g \in k_jH$  et donc  $g \in \bigcup_{j=1}^n k_jH$ , et ainsi, nous avons  $KH \subset \bigcup_{j=1}^n k_jH$

Nous en déduisons que  $\bigcup_{j=1}^n k_jH = KH$

ii. Démontrons, maintenant que si  $i \neq j$ , alors  $k_iH \cap k_jH = \emptyset$ 

Soit  $z \in k_iH \cap k_jH$ . Il existe alors  $h_1 \in H$  et  $h_2 \in H$  tels que  $z = k_ih_1 = k_jh_2$ . Or :

$$k_ih_1 = k_jh_2 \iff (k_j)^{-1}k_i = h_2(h_1)^{-1}$$

Nous avons alors  $(k_j)^{-1}k_i \in K \cap H$ , ce qui nous entend, que, dans la relation d'équivalence définie dans le groupe  $K$ , modulo  $H \cap K$ , nous avons  $k_i \mathfrak{R} k_j$ , c'est à dire  $k_i(H \cap K) = k_j(H \cap K)$ , ce qui est contradictoire.

Donc  $k_iH \cap k_jH = \emptyset$

Donc, la famille d'ensembles  $k_1H, k_2H, \dots, k_nH$  forme une partition de  $KH$

Et donc,  $\text{Card } KH = \frac{\text{Card } H \times \text{Card } K}{\text{Card } H \cap K}$

**Remarque 24 :**

1. Attention!! Si  $H \subset G$  et  $K \subset G$ ,  $KH$  ou  $HK$  ne sont pas forcément des sous-groupes de  $G$
2. Nous pourrions démontrer, de la même manière que  $\text{Card } HK = \frac{\text{Card } H \times \text{Card } K}{\text{Card } H \cap K}$

**Exercice 14 :**

$\text{GL}_n(\mathbb{R})$  est l'ensemble des matrices inversibles de dimension  $n$  et à coefficients réels.  $\text{GL}_n^+(\mathbb{R})$  est le sous groupe des matrices de déterminants strictement positifs. Montrer que  $\text{GL}_n^+(\mathbb{R})$  est d'indice 2 dans  $\text{GL}_n(\mathbb{R})$

**Exercice 15 :**

Soit  $n \in \mathbb{N}^*$  et on appelle  $F_n = \left\{ q = \frac{a}{n} \text{ où } a \in \mathbb{Z} \right\}$

1. Démontrer que  $F_n$  est un sous-groupe de  $(\mathbb{Q}, +)$  contenant  $\mathbb{Z}$
2. Quel est l'indice  $[F_n : \mathbb{Z}]$  de  $\mathbb{Z}$  dans  $F_n$

**Exercice 16 :**

1.  $(2\pi\mathbb{Z}, +)$  est un sous-groupe du groupe additif  $(\mathbb{R}, +)$ . On considère la relation d'équivalence modulo  $2\pi\mathbb{Z}$ , vraie pour tout  $x \in \mathbb{R}$  et tout  $y \in \mathbb{R}$  :

$$x\mathcal{R}y \iff x - y \in 2\pi\mathbb{Z} \iff x = y + k \times 2\pi \text{ où } k \in \mathbb{Z}$$

L'ensemble des classes d'équivalence  $\mathbb{R}/2\pi\mathbb{Z}$  est l'intervalle  $[0; 2\pi[$

La relation d'équivalence  $x\mathcal{R}y$  s'écrit de préférence  $x \equiv y \pmod{2\pi}$

On appelle  $\mathbb{U}$  l'ensemble des nombres complexes de module 1, c'est à dire :

$$\mathbb{U} = \{z \in \mathbb{C} \text{ tels que } |z| = 1\}$$

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

Il faut montrer que  $(\mathbb{R}/2\pi\mathbb{Z}, +)$  et  $(\mathbb{U}, \times)$  sont isomorphes

2.  $(\mathbb{Z}, +)$  est un sous-groupe du groupe additif  $(\mathbb{R}, +)$ . On considère la relation d'équivalence modulo  $\mathbb{Z}$ , vraie pour tout  $x \in \mathbb{R}$  et tout  $y \in \mathbb{R}$  :

$$x\mathcal{R}y \iff x - y \in \mathbb{Z} \iff x = y + k \text{ où } k \in \mathbb{Z}$$

L'ensemble des classes d'équivalence  $\mathbb{R}/\mathbb{Z}$  est l'intervalle  $[0; 1[$

Il faut montrer que  $(\mathbb{R}/2\pi\mathbb{Z}, +)$  et  $(\mathbb{R}/\mathbb{Z}, +)$  sont isomorphes

3. Montrer que  $(\mathbb{R}/\mathbb{Z}, +)$  et  $(\mathbb{U}, \times)$  sont isomorphes

**Exercice 17 :**

Pour reprendre les notations habituelles, nous avons, dans cet exercice, pour tout groupe multiplicatif  $(G, \times)$  et tout  $a \in G$  :

$$aG = \{y \in G \text{ tel qu'il existe } g \in G \text{ tel que } y = ag\}$$

Avons nous  $(2(\mathbb{Z}/12\mathbb{Z}), +)$  isomorphe à  $(\mathbb{Z}/6\mathbb{Z}, +)$ ?

**Exercice 18 :**

On considère  $\text{SL}_2(\mathbb{R})$  le sous-groupe de  $\text{GL}_2(\mathbb{R})$  formé des matrices de déterminant +1

On considère les sous-groupes  $H$  et  $K$  de  $\text{SL}_2(\mathbb{R})$  engendrés respectivement par

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Déterminer les éléments des espaces quotients  $\text{SL}_2(\mathbb{R})/H$  et  $\text{SL}_2(\mathbb{R})/K$