Ce qui est marqué en jaune est corrigé à présent.
Je corrigerai le reste après.

Structures algébriques usuelles

Exercice 1 :
Soit $(G, .)$ un groupe de neutre e et vérifiant

$$\forall x \in G,\ x^2 = e$$

Montrer que G est abélien.

Exercice 2 :
Montrer que

1) H est un sous-groupe de $(\mathbb{C}, +)$ où

$$H = \{a + b\omega /\ a, b \in \mathbb{Z}\}\ et\ \omega \in \mathbb{C}\ fixé$$

2) H est un sous-groupe de $(\mathbb{C}^*, \times)$ où

$$H = \{\omega^m /\ m \in \mathbb{Z}\}\ et\ \omega \in \mathbb{C}^*\ fixé$$

3) H est un sous-groupe de $(S_E, \circ)$ où

$$H = \{f \in S_E /\ f(a) = a\}.\ a \in E\ fixé,\ et\ E\ en\ ensemble\ non\ vide$$

Exercice 3 :
Soit $(G, \times)$ un groupe. Montrer que

1) $aHa^{-1} = \{aha^{-1} /\ h \in H\}$ est un sous-groupe de $(G, \times)$ où

$$H\ un\ sous-groupe\ de\ G,\ et\ a \in G\ fixé$$

2) $\mathcal{C}$ est un sous-groupe de $(G, \times)$ où

$$\mathcal{C} = \{x \in G /\ \forall g \in G,\ x \times g = g \times x\}$$

$\mathcal{C}$ *s'appelle le* ***centre*** *de* G

Exercice 4 :
Pour tout $(a, b) \in \mathbb{C}^* \times \mathbb{C}$, $f_{a,b} : \mathbb{C} \longrightarrow \mathbb{C}\,;\ z \longmapsto az + b$.
Notons $H = \{f_{a,b}\ /\ (a, b) \in \mathbb{C}^* \times \mathbb{C}\}$. Montrer $(H, \circ)$ est un groupe.

Exercice 5 :
Soient H et K deux sous-groupes d'un groupe $(G, .)$.
Montrer que

$$(H \cup K \ est\ un\ sous-groupe\ de\ G) \Leftrightarrow\ (H \subset K\ ou\ K \subset H)$$

Exercice 6 : (Les sous-gropues de $(\mathbb{Z}, +)$)
Notation : $n\mathbb{Z} = \{nk\ /\ k \in \mathbb{Z}\}$; pour tout $n \in \mathbb{N}$.
On se propose de montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$. Autrement dit :

$$(H\ sous-groupe\ de\ \mathbb{Z})\ \Leftrightarrow\ (H\ est\ de\ la\ forme\ n\mathbb{Z},\ où\ n \in \mathbb{N})$$

I) Soit $n \in \mathbb{N}$. Vérifier que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.

II) *Réciproquement.* Soit H un sous-groupe de $(\mathbb{Z}, +)$.

1) Vérifier que si $H = \{0\}$, alors il est de la forme voulue.

2) Supposons que $H \neq \{0\}$

i) Justifier que $H^+ = \{h \in H\ /\ h \succ 0\}$ possède un plus petit élément. (Notons-le a).
On vérifiera que $H = a\mathbb{Z}$.

ii) Montrer que $a\mathbb{Z} \subset H$.

iii) En effectuant la division euclidienne d'un élément de H par a , montrer que $H \subset a\mathbb{Z}$.
H est ainsi de la forme voulue.

III) Montrer que pour tout sous-groupe H de $(\mathbb{Z}, +)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

Exercice 7 :
Soit $(A, +, \times)$ un anneau.
Un élément a de A est dit ***idempotent*** *si et seulement si $x^2 = x$;*
c-à-d $x \times x = x$.

1) Montrer que si x et y sont idempotents et commutent, alors $x \times y$ est aussi idempotent.

2) Montrer que si x est idempotent et inversible, alors x^{-1} est idempotent.

Exercice 8 :
Soit $(A, +, \times)$ un anneau de neutres 0 et 1.
Définition : Un élément a de A est dit *nilpotent* si et seulement il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.
Soient $a, b \in\ A$.

1) Supposons que a et b nilpotents et commutent.

i) Montrer que ab est nilpotent.

ii) Montrer que $(a+b)$ est nilpotent.

2) Montrer que

$$(ab\ nilpotent) \ \Rightarrow\ (ba\ nilpotent)$$

3) Montrer que

$$(a\ nilpotent) \ \Rightarrow\ ((1-a)\ inversible)$$

Préciser l'inverse $(1-a)^{-1}$ en fonction des puissances de a.

Exercice 9 : (Anneau de Boole)

Soit $(A,+,\times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

2) Considérons la relation binaire $\preceq$ défine sur A par

$$x \preceq y \Leftrightarrow\ yx = x$$

Montrer que $\preceq$ est une relation d'ordre.

3) a) Montrer que

$$\forall x, y \in A,\ xy(x+y) = 0$$

b) En déduire que si l'anneau de Boole A est en plus intègre, alors il ne contiendra que deux éléments.

Exercice 10 : (Anneau de Gauss)

Notons $\mathbb{Z}[i] = \{a + bi\ /\ a, b \in \mathbb{Z}\}$.

1) Montrer que $(\mathbb{Z}[i],+,\times)$ est un anneau commutatif.
Cet anneau s'appelle l'anneau de Gauss.

2) Montrer que le groupe des éléments inversibles de l'anneau de Gauss et $\{1,-1,i,-i\}$.
Indice : vous pouvez utiliser que si $z, z' \in \mathbb{C}$, alors $|z \times z'|^2 = |z|^2 \times |z'|^2$

Exercice 11 :

Soit $(A,+,\times)$ un anneau non nul, *commutatif et fini.*
Montrer que

$$A\ est\ intègre\ \Leftrightarrow\ A\ est\ un\ corps$$

<u>Indice</u> : On admet qu'une application injective d'un ensemble fini vers lui-même est bijective.

Exercice 1 :

Soit $(G, .)$ un groupe de neutre e et vérifiant

$$\forall x \in G,\ x^2 = e$$

Montrer que G est abélien.

Solution

On a : $(\forall x \in G,\ x \cdot x = e)$

Donc : $(\forall x \in G,\ x^{-1} = x)$ $(*)$

Soient x et $y \in G$. Montrons que $xy = yx$.

On a : $xy = (xy)^{-1}$ (d'après $(*)$)

$= y^{-1} \cdot x^{-1}$

$= y \cdot x$

Fin Ex 1

Exercice 2 :

Montrer que

1) H est un sous-groupe de $(\mathbb{C},+)$ où

$$H=\{a+b\omega/\ a,b\in\mathbb{Z}\}\ et\ \omega\in\mathbb{C}\ fixé$$

2) H est un sous-groupe de $(\mathbb{C}^*,\times)$ où

$$H=\{\omega^m/\ m\in\mathbb{Z}\}\ et\ \omega\in\mathbb{C}^*\ fixé$$

3) H est un sous-groupe de $(S_E,\circ)$ où

$$H=\{f\in S_E/\ f(a)=a\}.\ a\in E\ fixé,\ et\ E\ en\ ensemble\ non\ vide$$

Solution

1) H est un sous-groupe de $(\mathbb{C},+)$ où

$$H=\{a+b\omega/\ a,b\in\mathbb{Z}\}\ et\ \omega\in\mathbb{C}\ fixé$$

$$x\in H \overset{\text{par déf}}{\Longleftrightarrow} (\exists a,b\in\mathbb{Z},\ x=a+b\omega)$$

i) $0\in H$, en prenant $a=b=0$

ii) Soient $x,y\in H$. M. que $(x-y)\in H$

$$x\in H \Longleftrightarrow (\exists a,b\in\mathbb{Z},\ x=a+b\omega)$$

$$\text{et } y\in H \Longleftrightarrow (\exists a',b'\in\mathbb{Z},\ y=a'+b'\omega)$$

$x-y=(a-a')+(b-b')\omega\in H$, car $a-a'\in\mathbb{Z}$ et $b-b'\in\mathbb{Z}$.

Ainsi, H est un sous-groupe de $(\mathbb{C},+)$

2) H est un sous-groupe de $(\mathbb{C}^*,\times)$ où

$$H=\{\omega^m/\ m\in\mathbb{Z}\}\ et\ \omega\in\mathbb{C}^*\ fixé$$

On montrera que :

i) $1 \in H$

ii) Soient $x, y \in H$. M. que $xy^{-1} \in H$

Pour i) $1 \in H$ car $1 = w^0$ et $0 \in \mathbb{Z}$

Pour ii) On a x et $y \in H$.

$\Rightarrow \exists m, m' \in \mathbb{Z}$ tels que $\begin{cases} x = w^m \\ y = w^{m'} \end{cases}$

Alors $xy^{-1} = w^m \cdot (w^{m'})^{-1}$

$= w^m \cdot w^{-m'}$

$= w^{m-m'} \underline{\in H}$, car $(m-m') \in \mathbb{Z}$.

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

3) H est un sous-groupe de $(S_E, \circ)$ où

$H = \{f \in S_E / \ f(a) = a\}$. $a \in E$ *fixé, et* E *en ensemble non vide*

On a : $f \in H \Leftrightarrow (f \in S_E$ et $f(a) = a)$

Montrons que H est un sous-groupe du groupe $(S_E, \circ)$.

i) Montrons que $I_E \in H$:

On a $I_E \in S_E$ et $I_E(a) = a$

D'où $I_E \in H$.

ii) Soient $f, g \in H$. Montrons que $f \circ g^{-1} \in H$

On a $f, g \in S_E$, alors $f \circ g^{-1} \in S_E$.

Et on a :

$$(f \circ g^{-1})(a) = f(g^{-1}(a))$$

On a $g(a) = a$, alors $a = g^{-1}(a)$

$$\Rightarrow (f \circ g^{-1})(a) = f(g^{-1}(a))$$
$$= f(a)$$
$$= a \quad (\text{car } f \in H)$$

Ainsi : $(f \circ g^{-1}) \in H$.

Enfin : H est un sous-groupe du groupe $(S_E, \circ)$.

Fin Ex2

Exercice 3 :

Soit $(G, \times)$ un groupe. Montrer que

1) $aHa^{-1} = \{aha^{-1} / \ h \in H\}$ est un sous-groupe de $(G, \times)$ où

$$H \ un \ sous-groupe \ de \ G, \ et \ a \in G \ fixé$$

2) $\mathcal{C}$ est un sous-groupe de $(G, \times)$ où

$$\mathcal{C} = \{x \in G / \ \forall g \in G, \ x \times g = g \times x\}$$

$\mathcal{C}$ *s'appelle le* **centre** *de* G

Solution

1) $x \in aHa^{-1} \Leftrightarrow (\exists h \in H, \ x = aha^{-1})$

Notons e le neutre de $(G, \times)$.

On veut montrer que aHa^{-1} est un sous-groupe de $(G, \times)$.

Il s'agit de montrer que :

a) $e \in aHa^{-1}$

b) $\forall x, y \in aHa^{-1}, \ x \times y^{-1} \in aHa^{-1}$

Pour a) :

On a $e = a.e.a^{-1}$ et $e \in H$ car H sous-groupe de $(G, \times)$

D'où $e \in aHa^{-1}$

Pour b) :

Soient $x, y \in aHa^{-1}$. M. que $xy^{-1} \in aHa^{-1}$.

On a $x, y \in aHa^{-1} \Rightarrow \begin{cases} \exists h_1 \in H, \ x = ah_1a^{-1} \\ \exists h_2 \in H, \ y = ah_2a^{-1} \end{cases}$

D'où $xy^{-1} = ah_1a^{-1}.(ah_2a^{-1})^{-1}$

$= ah_1 \underbrace{a^{-1}.(a^{-1})^{-1}}_{=e} h_2^{-1} a^{-1}$

$= ah_1h_2^{-1}a^{-1} \in aHa^{-1}$

Car $h_1h_2^{-1} \in H$, puisque H s-groupe de G.

Enfin, aHa^{-1} est un sous-groupe de $(G, \times)$.

2) $\mathcal{C}$ est un sous-groupe de $(G, \times)$ où

$$\mathcal{C} = \{x \in G / \ \forall g \in G, \ x \times g = g \times x\}$$

$\mathcal{C}$ *s'appelle le* **centre** *de* G

$x \in C \iff (\forall g \in G, \ xg = gx)$

On veut montrer que C est un sous-groupe de $(G, \times)$.

Il s'agit alors de montrer que :

a) $e \in C$

b) $\forall x, y \in C, \ xy^{-1} \in C$

Pour a) On a : $(\forall g \in G, \ e \cdot g = g \cdot e = g)$

D'où $e \in C$

Pour b) Soient x et $y \in C$. M que $xy^{-1} \in C$.

Soit alors $g \in G$. Il s'agit de vérifier que $(xy^{-1})g = g(xy^{-1})$.

On a :

$$(xy^{-1})g = x \cdot y^{-1} g$$

Or $yg = gy$ car $y \in C$

$$\Rightarrow \underbrace{y^{-1}y}_{=e} g y^{-1} = y^{-1} g \underbrace{y y^{-1}}_{=e}$$

$$\Rightarrow gy^{-1} = y^{-1}g$$

Ainsi : $(xy^{-1})g = x \cdot gy^{-1}$

$= gxy^{-1}$ (car $xg = gx$, puisque $x \in C$)

$= g(xy^{-1})$

Enfin C est un sous-groupe de $(G, \times)$.

Fin 6x3

Exercice 4 :

Pour tout $(a,b) \in \mathbb{C}^* \times \mathbb{C}$, $f_{a,b} : \mathbb{C} \longrightarrow \mathbb{C}\,;\, z \longmapsto az+b$.
Notons $H = \{f_{a,b} \,/\, (a,b) \in \mathbb{C}^* \times \mathbb{C}\}$. Montrer $(H, \circ)$ est un groupe.

Solution

Pour montrer que $(H,\circ)$ est un groupe, il suffit de montrer que H est un sous-groupe du groupe $(S_{\mathbb{C}}, \circ)$.

Il s'agit de montrer les points suivants :

0) $H \subset S_{\mathbb{C}}$

1) $id_{\mathbb{C}} \in H$

2) $\forall g, h \in H$, $g \circ h^{-1} \in H$.

Pour 0) $H \subset S_{\mathbb{C}}$

Soit $(a,b) \in \mathbb{C}^* \times \mathbb{C}$. Montrons que $f_{a,b} \in S_{\mathbb{C}}$.

C'à d que $f_{a,b}$ est une bijection de $\mathbb{C}$ vers $\mathbb{C}$.

Soit $y \in \mathbb{C}$. M. qu'il existe un unique $z \in \mathbb{C}$ tel que $f_{a,b}(z) = y$.

Soit $z \in \mathbb{C}$. On a :

$$f_{a,b}(z) = y \iff az+b = y$$
$$\iff z = \frac{y-b}{a}$$

D'où l'existence un unique $z \in \mathbb{C}$ tel que $f_{a,b}(z) = y$, et qui est $z = \frac{y-b}{a}$.

Et on tire aussi que :

$$\forall y \in \mathbb{C},\ f_{a,b}^{-1}(y) = \frac{y-b}{a}$$

Pour 1) $id_{\mathbb{C}} \in H$

On a : $\forall z \in \mathbb{C},\ id_{\mathbb{C}}(z) = z = 1 \cdot z + 0$

$$\Rightarrow id_{\mathbb{C}} = f_{1,0} \in H$$

Pour 2) $\forall g, h \in H$, $g \circ h^{-1} \in H$.

Soient $g = f_{a,b}$ et $h = f_{c,d} \in H$.

Montrons $g \circ h^{-1} \in H$.

On a vu que : $\left(\forall y \in \mathbb{C},\ f_{a,b}^{-1}(y) = \frac{y-b}{a} = \frac{1}{a} \cdot y + \left(\frac{-b}{a}\right)\right)$

$$\Rightarrow f_{a,b}^{-1} = f_{\frac{1}{a}, \frac{-b}{a}}$$

Ainsi, $h^{-1} = (f_{c,d})^{-1} = f_{\frac{1}{c}, \frac{-d}{c}}$.

D'autre part, on a :

$$\forall z \in \mathbb{C},\ (g \circ h^{-1})(z) = g(h^{-1}(z))$$

$$= f_{a,b}\left(f_{\frac{1}{c}, \frac{-d}{c}}(z)\right)$$

$$= f_{a,b}\left(\frac{1}{c} z - \frac{d}{c}\right)$$

$$= a\left(\frac{1}{c} z - \frac{d}{c}\right) + b$$

$$\forall z \in \mathbb{C},\ (g \circ h^{-1})(z) = \frac{a}{c} z + \left(b - \frac{ad}{c}\right)$$

$$\Rightarrow g \circ h^{-1} = f_{\frac{a}{c}, b - \frac{ad}{c}} \in H$$

Enfin, $(H, \circ)$ est un groupe.

Fin Ex 4

Exercice 5 :

Soient H et K deux sous-groupes d'un groupe $(G, .)$.
Montrer que

$$(H \cup K \text{ est un sous-groupe de } G) \Leftrightarrow (H \subset K \text{ ou } K \subset H)$$

Solution

Raisonnons par double implication :

($\Leftarrow$) Supposons que $(H \subset K$ ou $K \subset H)$.

et montrons que $H \cup K$ est un sous-groupe de G.

On a $(H \subset K$ ou $K \subset H)$

alors $(H \cup K = K$ ou $H \cup K = H)$

est donc $H \cup K$ est un sous-groupe de G, car H et K sont des sous-groupes de G.

($\Rightarrow$) Supposons que $H \cup K$ est un sous-groupe de G.

et montrons que $(H \subset K$ ou $K \subset H)$.

Piste 1

Faisons par disjonction des cas.

On sait que $H \subset K$ ou $H \not\subset K$.

Cas 1 : Si $H \subset K$

Alors c'est fini.

Cas 2 : Si $H \not\subset K$

Montrons alors que $K \subset H$.

Soit $k \in K$. Montrons que $k \in H$.

On a $\begin{cases} k \in H \cup K \text{ (car } k \in K \text{ et } K \subset (H \cup K)) \\ H \cup K, H \text{ et } K \text{ sont des sous-groupes de } G. \\ H \not\subset K \Rightarrow (\exists h \in H, h \notin K) \end{cases}$

h et $k \in H \cup K \Rightarrow hk \in H \cup K$, car $H \cup K$ sous-groupe de G.

$\Rightarrow (hk \in H$ ou $hk \in K)$

$\rightsquigarrow$ Si $hk \in H$ et puisque $h \in H$, alors $h^{-1}(hk) \in H$, car H s-gr de G

$\Rightarrow \underline{k \in H}$ et c'est ce qu'on veut.

$\rightsquigarrow$ Si $hk \in K$, et puisque $k \in K$ alors $(hk).k^{-1} \in K$, car K s-gr de G.

$\Rightarrow \boxed{h \in K}$ ce qui est impossible.

D'où $k \in H$ CQFD

Piste 2

Supposons que $H \cup K$ est un sous-groupe de G.

Et montrons que $(H \subset K$ ou $K \subset H)$.

Raisonnons par l'absurde, et supposons que $\begin{cases} H \not\subset K \\ \text{et} \\ K \not\subset H \end{cases}$.

Alors $\begin{cases} \exists h \in H \text{ tel que } h \notin K \\ \text{et} \\ \exists k \in K \text{ tel que } k \notin H \end{cases}$

Ainsi $\begin{cases} h \text{ et } k \in H \cup K \\ H \cup K \text{ sous-groupe de } G \end{cases}$

D'où $hk \in H \cup K$.

$\Rightarrow \left(hk \in H \text{ ou } hk \in K \right)$

$\Rightarrow \left(h^{-1} \cdot hk \in H \text{ ou } hk \cdot k^{-1} \in K \right)$; car $\left(\begin{array}{l} h \in H, k \in K \text{ et } H \\ \text{et } K \text{ sous-groupes de } G \end{array} \right)$

$\Rightarrow \left(k \in H \text{ ou } h \in K \right)$

Ce qui est absurde, car $\left(k \notin K \text{ et } k \notin H \right)$

D'où la conclusion.

Fin Ex 5

Exercice 6 : (Les sous-gropues de $(\mathbb{Z},+)$)

Notation : $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$; pour tout $n \in \mathbb{N}$.

On se propose de montrer que les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$. Autrement dit :

$$(H \ sous-groupe \ de \ \mathbb{Z}) \Leftrightarrow (H \ est \ de \ la \ forme \ n\mathbb{Z}, \ où \ n \in \mathbb{N})$$

I) Soit $n \in \mathbb{N}$. Vérifier que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

(a) $0 \in n\mathbb{Z}$ car $0 = n \cdot 0$ et $0 \in \mathbb{Z}$

(b) Soient $x, y \in n\mathbb{Z}$. Mq que $x - y \in n\mathbb{Z}$.

On a $\begin{cases} x = nk \\ y = nk' \end{cases}$ où $k, k' \in \mathbb{Z}$

$\Rightarrow x - y = n(k-k') \in n\mathbb{Z}$, car $(k-k') \in \mathbb{Z}$

D'où $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.

II) *Réciproquement.* Soit H un sous-groupe de $(\mathbb{Z},+)$.

1) Vérifier que si $H = \{0\}$, alors il est de la forme voulue.

Supp que $H = \{0\}$.

On a $H = 0 \cdot \mathbb{Z}$ alors il est de la forme voulue.

2) Supposons que $H \neq \{0\}$

i) Justifier que $H^+ = \{h \in H \ / \ h \succ 0\}$ possède un plus petit élément. (Notons-le a).

Rappel

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

a) $H^+ \subset \mathbb{N}$ (Claire)

b) $H^+ \neq \emptyset$, en effet.

On a $H \neq \{0\} \Rightarrow (\exists p \in \mathbb{Z}^*$ tel que $p \in H)$

Or H sous-groupe de $\mathbb{Z}$, alors $\begin{cases} p \in H \\ -p \in H \end{cases}$

Et puisque $(p > 0$ ou $(-p) > 0)$

Alors $\boxed{H^+ \neq \emptyset}$

De a) et b) on tire que H^+ est une partie non vide de $\mathbb{N}$, donc possède un plus petit élément.

On vérifiera que $H = a\mathbb{Z}$.

ii) Montrer que $a\mathbb{Z} \subset H$.

On a $\begin{cases} H \text{ sous-groupe de } (\mathbb{Z}, +) \\ a \in H \end{cases}$

Alors : $(\forall k \in \mathbb{Z},\ ka \in H)$

$\Rightarrow \boxed{a\mathbb{Z} \subset H}$

iii) En effectuant la division euclidienne d'un élément de H par a , montrer que $H \subset a\mathbb{Z}$.

Soit $h \in H$. M que $h \in a\mathbb{Z}$

càd : M qu'il existe $q \in \mathbb{Z}$ tel que $h = aq$.

D'après la division euclidienne de h par a, il existe $(q, r) \in \mathbb{Z}^2$ tel que $\begin{cases} h = aq + r \\ 0 \leq r < a \end{cases}$

Pour finir la question, il suffit de montrer que $r=0$.

On a $\underbrace{b}_{\in H} = \underbrace{aq}_{\in H \text{ et } H \text{ s-gr de } \mathbb{Z}^+} + r$

$\Rightarrow r = b - aq \in H$, car H s-groupe $(\mathbb{Z},+)$.

Ainsi : $\begin{cases} r \in H \\ 0 \leq r < a \end{cases}$

Or $\begin{cases} a = \min(\{b \in H \,/\, b > 0\}) \\ \text{et } 0 \leq r < a \end{cases}$

alors $\boxed{r = 0}$ CQFD.

III) Montrer que pour tout sous-groupe H de $(\mathbb{Z},+)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

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

Supposons l'existence de n_1 et $n_2 \in \mathbb{N}$ tels que $\begin{cases} H = n_1\mathbb{Z} \\ H = n_2\mathbb{Z} \end{cases}$.

Et montrons que $n_1 = n_2$.

On a $n_1\mathbb{Z} = n_2\mathbb{Z} \Rightarrow \begin{cases} n_1 / n_2 \\ n_2 / n_1 \end{cases}$

$\Rightarrow \boxed{n_1 = n_2}$

Fin

Exercice 7 :

Soit $(A, +, \times)$ un anneau.

Un élément a de A est dit ***idempotent*** *si et seulement si* $x^2 = x$;

c-à-d $x \times x = x$.

1) Montrer que si x et y sont idempotents et commutent, alors $x \times y$ est aussi idempotent.

2) Montrer que si x est idempotent et inversible, alors x^{-1} est idempotent.

Solution

1) Supposons que $x^2 = x$, $y^2 = y$ et que $xy = yx$.

Montrons que $(xy)^2 = xy$

On a $xy = yx$, alors :

$$(xy)^2 = x^2 y^2$$

$$= xy \quad (\text{car } x^2 = x \text{ et } y^2 = y)$$

fin 1°)

2) Supposons que $x^2 = x$ et que x est inversible.

Montrons $(x^{-1})^2 = x^{-1}$.

On a :

$$(x^{-1})^2 = (x^2)^{-1}$$

$$= x^{-1} \quad (\text{car } x^2 = x$$

fin Ex 7

Exercice 8 :

Soit $(A, +, \times)$ un anneau de neutres 0 et 1.

Définition : Un élément a de A est dit *nilpotent* si et seulement il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

Soient $a, b \in A$.

1) Supposons que a et b nilpotents et commutent.

   i) Montrer que ab est nilpotent.

   ii) Montrer que $(a + b)$ est nilpotent.

2) Montrer que

$$(ab \ nilpotent) \Rightarrow (ba \ nilpotent)$$

3) Montrer que

$$(a \ nilpotent) \Rightarrow ((1 - a) \ inversible)$$

Préciser l'inverse $(1 - a)^{-1}$ en fonction des puissances de a.

Solution

1) Supposons que a et b sont nilpotents et que $ab = ba$.

i) M. que (ab) est nilpotent :

a et b nilpotents $\Rightarrow \begin{cases} \exists n \in \mathbb{N}^*, \ a^n = 0 \\ \exists p \in \mathbb{N}^*, \ b^p = 0 \end{cases}$

Et on a $(ab)^n = a^n . b^n$ (car $ab = ba$)

$= 0$ (car $a^n = 0$)

D'où (ab) est nilpotent.

ii) M. que $(a+b)$ est nilpotent.

a et b nilpotents $\Rightarrow \begin{cases} \exists n \in \mathbb{N}^*, \ a^n = 0 \\ \exists p \in \mathbb{N}^*, \ b^p = 0 \end{cases}$

Notons $N = n + p$.

On a $(a+b)^N = 0$; en effet :

$$(a+b)^N = \sum_{k=0}^{N} C_N^k a^k b^{N-k} \quad \text{(car } a \text{ et } b \text{ commutent)}$$

$$= \sum_{k=0}^{n-1} C_N^k a^k b^{N-k} + \sum_{k=n}^{N} C_N^k a^k b^{N-k}$$

On sait que $a^n = 0$ et donc $(\forall\, n \leq k \leq N,\ a^k = 0)$

Ainsi $\displaystyle\sum_{k=n}^{N} C_N^k a^k b^{N-k} = 0$

et $b^p = 0$, d'où $(\forall\, k \geq p,\ b^k = 0)$

Vérifions que $\displaystyle\sum_{k=0}^{n-1} C_N^k a^k b^{N-k} = 0$.

Il suffit de vérifier que :

$$(\forall\, 0 \leq k \leq n-1,\ b^{N-k} = 0)$$

et pour cela, il suffit de vérifier que :

$$(\forall\, 0 \leq k \leq n-1,\ N-k \geq p).$$

Ce qui est vrai, car : $N-k-p = (n+p)-k-p = n-k \geq 1 \geq 0$
car $k \leq n-1$

D'où $\displaystyle\sum_{k=0}^{n-1} C_n^k a^k b^{N-k} = 0$

et enfin : $(a+b)^N = 0$

---

2) Montrer que

$$(ab \text{ nilpotent}) \Rightarrow (ba \text{ nilpotent})$$

Supposons que (ab) est nilpotent.

Mq que (ba) est aussi nilpotent.

On a (ab) nilpotent $\Rightarrow \left(\exists n \in \mathbb{N}^*,\ (ab)^n = 0\right)$

$$\Rightarrow \underbrace{ab \cdot ab \cdots ab}_{n \text{ fois}} = 0$$

$$\Rightarrow b \cdot \underbrace{ab \cdot ab \cdots ab}_{n \text{ fois}} \cdot a = 0$$

$$\Rightarrow \underbrace{(ba) \cdot (ba) \cdots (ba)}_{(n+1) \text{ fois}} = 0$$

$$\Rightarrow (ba)^{n+1} = 0$$

D'où (ba) est nilpotent.

3) Montrer que

$$(a \text{ nilpotent}) \Rightarrow ((1-a) \text{ inversible})$$

Préciser l'inverse $(1-a)^{-1}$ en fonction des puissances de a.

Supposons que a est nilpotent.

Montrons que $(1-a)$ est inversible.

On a a nilpotent $\Rightarrow \left(\exists n \in \mathbb{N}^*,\ a^n = 0\right)$

La clé est :

$$1 = 1^n - a^n$$

$$\Rightarrow 1 = (1-a)(1 + a + \cdots + a^{n-1})$$

(C'est l'identité de Bernoulli.)
Puisque $1 \cdot a = a \cdot 1$

Et de même on a : $1 = (1 + a + \cdots + a^{n-1})(1-a)$

Fin Ex 8

D'où $(1-a)$ est inversible, et $(1-a)^{-1} = 1 + a + \cdots + a^{n-1}$

Exercice 9 : (Anneau de Boole)

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

2) Considérons la relation binaire $\preceq$ défine sur A par

$$x \preceq y \Leftrightarrow\ yx = x$$

Montrer que $\preceq$ est une relation d'ordre.

3) a) Montrer que

$$\forall x, y \in A,\ xy(x + y) = 0$$

b) En déduire que si l'anneau de Boole A est en plus intègre, alors il ne contiendra que deux éléments.

Solution

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

1) a) Soient $x, y \in A$. Mq que $xy + yx = 0$

On a $(x+y)^2 = (x+y)$

$\Rightarrow (x+y)(x+y) = x+y$

$\Rightarrow \underbrace{x^2}_{=x} + xy + yx + \underbrace{y^2}_{=y} = x+y$ (attention! n'écrivez pas "$2xy$" Car il faut avoir $xy = yx$; Ce qu'on n'a pas)

$\Rightarrow \cancel{x} + xy + yx + \cancel{y} = \cancel{x} + \cancel{y}$

$\Rightarrow \boxed{xy + yx = 0}$ $\square$

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

1) b) i) Soit $x \in A$. M que $2x = 0$.

On a $x.x + x.x = 0$ (d'après 1)a))

$\Rightarrow \underbrace{x^2}_{=x} + x^2 = 0$

$\Rightarrow \boxed{2x = 0}$

$\square$

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

1) b) ii) On déduire que l'anneau $(A, +, \times)$ est commutatif.

Soient $x, y \in A$. M. que $xy = yx$.

Piste 1 :

On a $xy + yx = 0$ (1) a))

$$\Rightarrow xy + xy + yx = xy$$

$$\Rightarrow \underbrace{2xy}_{=0} + yx = xy$$

↳ d'après 1) b) i)

$$\Rightarrow \boxed{yx = xy} \quad \square$$

Piste 2 :

On a : $xy = (xy)^2$

$$= x \underbrace{y\,x}_{=-xy} y$$

$$= -x \cdot xy \cdot y$$

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

$$= -xy$$

$$= yx \quad (\text{car } xy + yx = 0 \text{, d'après } 1)\ a))$$

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

2) Considérons la relation binaire $\preceq$ défine sur A par

$$x \preceq y \Leftrightarrow yx = x$$

Montrer que $\preceq$ est une relation d'ordre.

2) Montrons que $\leq$ est une relation d'ordre sur A :

$x \preceq y \Leftrightarrow yx = x$

i) M. que $\leq$ est réflexive :

Soit $x \in A$. On a :

$x \leq x \Leftrightarrow x \cdot x = x$

$\Leftrightarrow x^2 = x$, ce qui est vrai.

D'où : $(\forall x \in A,\ x \leq x)$

ii) M. que $\leq$ est anti-symétrique :

Soient $x, y \in A$. Supp que $(x \leq y$ et $y \leq x)$, et M que $x = y$.

On a : $x \leq y \Rightarrow yx = x$

$y \leq x \Rightarrow xy = y$

$x \preceq y \Leftrightarrow yx = x$

Alors $\begin{cases} yx = x \\ xy = y \end{cases}$

Or $xy = yx$ car A commutatif

Alors $x = y$

iii) Montrer que $\leq$ est transitive :

Soient $x, y, z \in A$.

Supp que ($x \leq y$ et $y \leq z$), et M que $x \leq z$.

$x \leq y \Leftrightarrow yx = x$

On a alors $\begin{cases} yx = x \\ zy = y \end{cases}$ et on veut M. que $zx = x$

On a $x = yx$

$= (zy)x$ (car $zy = y$)

$= z(yx)$

$= zx$ (car $yx = x$) $\square$

Enfin $\leq$ est une relation d'ordre.

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

2) Considérons la relation binaire $\preceq$ défine sur A par

$$x \preceq y \Leftrightarrow\ yx = x$$

Montrer que $\preceq$ est une relation d'ordre.

3) a) Montrer que

$$\forall x, y \in A,\ xy(x + y) = 0$$

3) a) Soient $x, y \in A$. M que $xy(x+y) = 0$

On a :

$xy(x+y) = xyx + xy^2$

$= x^2y + xy^2$ (car A commutatif)

$= xy + xy$ (car $x^2 = x$ et $y^2 = y$)

$= 2xy$

$= 0$, d'après 1)b)i)

Soit $(A, +, \times)$ un anneau de Boole ; c-à-d que c'est un anneau vérifiant :

$$\forall x \in A,\ x^2 = x$$

1) a) Montrer que

$$\forall x, y \in A,\ xy + yx = 0$$

b) En déduire que

i) $\forall x \in A,\ 2x = 0$

ii) L'anneau A est commutatif.

2) Considérons la relation binaire $\preceq$ défine sur A par

$$x \preceq y \Leftrightarrow\ yx = x$$

Montrer que $\preceq$ est une relation d'ordre.

3) a) Montrer que

$$\forall x, y \in A,\ xy(x + y) = 0$$

b) En déduire que si l'anneau de Boole A est en plus intègre, alors il ne contiendra que deux éléments.

3) b) Supposons que A est en plus intègre.

Montrons que A ne contient que deux éléments.

Puisque A contient déjà 0 et 1 ; les éléments neutres.

Alors on montrera que $A = \{0, 1\}$.

Soit $x \in A$. Montrons que $x \in \{0, 1\}$.

On a $x \cdot 1(x+1) = 0$ d'après 3) a) $\forall x, y \in A,\ xy(x+y) = 0$

$\Rightarrow x(x+1) = 0$

$\Rightarrow x = 0$ ou $x + 1 = 0$

$\Rightarrow x = 0$ ou $x = -1$

D'autre part, on a $2.1 = 0$ (d'après 1)b)i))

$\Rightarrow 1+1=0$

$\Rightarrow 1=-1$

Alors $x=0$ ou $x=1$

Enfin : $\boxed{A=\{0,1\}}$ (car $\{0,1\} \subset A$; évident)

Remarque

Soit $x \in A$. On a $x^2 = x$

$\Rightarrow x^2 - x = 0$

$\Rightarrow x(x-1)=0$

$\Rightarrow x=0$ ou $x=1$ (car A intègre)

$\Rightarrow x \in \{0,1\}$

D'où $A=\{0,1\}$ (car 0 et $1 \in A$)

C'est correct, mais on demande de déduire !

Fin exercice 9

Exercice 10 : (Anneau de Gauss)

Notons $\mathbb{Z}[i] = \{a + bi \ / \ a, b \in \mathbb{Z}\}$.

1) Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.
   Cet anneau s'appelle l'anneau de Gauss.

2) Montrer que le groupe des éléments inversibles de l'anneau de Gauss et $\{1, -1, i, -i\}$.
   Indice : vous pouvez utiliser que si $z, z' \in \mathbb{C}$, alors $|z \times z'|^2 = |z|^2 \times |z'|^2$

Solution :

1) Facile. Juste appliquez la définition d'un anneau...

0 et 1 sont respectivement les éléments neutres pour + et ×.

2) On veut montrer que $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, où

$U(\mathbb{Z}[i])$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}[i]$.

Soit $z \in U(\mathbb{Z}[i])$. Alors $z = a+bi$, où $a, b \in \mathbb{Z}$ et il existe

$z' = a'+b'i \in \mathbb{Z}[i]$ tel que $z \times z' = 1$.

On a $z \times z' = 1$, alors $|z| \times |z'| = 1$

$$\Rightarrow \sqrt{a^2+b^2} \times \sqrt{a'^2+b'^2} = 1$$

$$\Rightarrow (a^2+b^2) \times (a'^2+b'^2) = 1$$

$$\Rightarrow (a^2+b^2) \text{ divise } 1$$

$$\Rightarrow a^2+b^2 = 1$$

On a $\begin{cases} a^2, b^2 \in \mathbb{N} \\ a^2+b^2 = 1 \end{cases}$ alors $(a^2, b^2) = (1,0)$ ou $(a^2, b^2) = (0,1)$

$\Rightarrow (a,b) = (1,0)$ ou $(a,b) = (-1,0)$ ou $(a,b) = (0,1)$ ou $(a,b) = (0,-1)$

et avec $z = a+bi$, on a alors :

$$z = 1 \text{ ou } z = -1 \text{ ou } z = i \text{ ou } z = -i$$

On vient de montrer que :

$$\forall z \in U(\mathbb{Z}[i]),\ z \in \{1, -1, i, -i\}$$

Autrement dit : $\mathcal{U}(\mathbb{Z}[i]) \subset \{1, -1, i, -i\}$

Pour finir, il reste à vérifier que $1, -1, i$ et $(-i) \in \mathcal{U}(\mathbb{Z}[i])$.

Ce qui est claire, car :

$$\begin{cases} 1 \times 1 = 1 \\ (-1) \times (-1) = 1 \\ i \times (-i) \ 1 \end{cases}$$

Finalement :

$$\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$$

Fin

Exercice 11 :

Soit $(A, +, \times)$ un anneau non nul, *commutatif et fini.*
Montrer que

$$A \text{ est intègre } \Leftrightarrow A \text{ est un corps}$$

<u>Indice</u> : *On admet qu'une application injective d'un ensemble fini vers lui-même est bijective.*

Solution :

Procédons par double implication.

($\Leftarrow$) Supposons que $(A, +, \times)$ est un corps, et montrons que A est un anneau intègre.

Soient alors $a, b \in A$ tels que $ab = 0$.

M que ($a = 0$ ou $b = 0$).

Raisonnons par l'absurde, et supposons que ($a \neq 0$ et $b \neq 0$).

On a $ab = 0 \Rightarrow a^{-1} . ab = 0$ (a est inversible car $a \neq 0$ et A est un corps)

$\Rightarrow b = 0$

Ce qui est absurde, car $b \neq 0$.

($\Rightarrow$) Supp que $(A, +, \times)$ est un anneau intègre, et montrons que A est un corps.

Soit alors $a \in A$, avec $a \neq 0$.

M que a est <u>inversible</u>.

Càd : ($\exists b \in A$ tel que $ab = 1$)

Considérons l'application : $f : A \longrightarrow A$
$x \longmapsto ax$

Il s'agit alors de montrer que :

$(\exists b \in A$ tel que $f(b) = 1)$

Pour cela, il suffit de montrer que f est surjective.

On a $f : A \longrightarrow A$ et que A est fini

Alors : f injective $\Longleftrightarrow$ f bijective

Il nous reste alors à vérifier que f est injective.

Soient alors x et $y \in A$ tels que $f(x) = f(y)$.

M que $x = y$.

On a :

$$
\begin{aligned}
f(x) = f(y) &\Rightarrow ax = ay \\
&\Rightarrow ax - ay = 0 \\
&\Rightarrow a(x-y) = 0 \\
&\Rightarrow x - y = 0 \quad (\text{car } a \neq 0 \text{ et } A \text{ intègre}) \\
&\Rightarrow x = y
\end{aligned}
$$

Fin Exercice 11