Devoir de contrôle N°1

Q1. Soit $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ n \in \mathbb{Z} \right\}$.

1. Montrer que H est un sous-groupe de $(\mathcal{GL}_2(\mathbb{R}), \times)$.

$\forall n \in \mathbb{Z}$, $\det \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = 1 \neq 0$, donc $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$ c.à.d $H \subset GL_2(\mathbb{R})$.

on a : $I_2 \in H$;

$\forall \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in H$, $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in H$; on a : $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} \in H$

$\forall \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in H$, on a : $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \in H$

D'où H est un ss-gpe de $GL_2(\mathbb{R})$.

2. Montrer que H est monogène et, déterminer un groupe qui lui soit isomorphe.

on a : $\forall n \in \mathbb{Z}$, $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$

donc $H = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n,\ n \in \mathbb{Z} \right\} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ c.à.d H est monogène

Par le théorème de classification des gpes monogène, H est isomorphe à $\mathbb{Z}$.

Q2. Soit $\varphi : (\mathbb{Z}/3\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/4\mathbb{Z}, +)$ un morphisme de groupes.

1. Montrer que l'ordre de $\varphi(\bar{1})$ divise 3 et divise 4.

on a $\varphi(\bar{1}) \in \mathbb{Z}/4\mathbb{Z}$ donc : l'ordre de $\varphi(\bar{1})$ divise 4 (voir le cours).

or $\bar{0} = \varphi(\bar{0}) = \varphi(\bar{3}) = \varphi(\bar{1}+\bar{1}+\bar{1}) = 3\varphi(\bar{1})$ donc l'ordre de $\varphi(\bar{1})$ divise 3.

2. En déduire que $\varphi(\bar{1}) = \bar{0}$.

on a l'ordre $\varphi(\bar{1})$ divise $3 \wedge 4 = 1$, donc : l'ordre de $\varphi(\bar{1})$ égal à 1 c.à.d $\varphi(\bar{1}) = \bar{0}$.

3. Déterminer alors φ.

$\forall \bar{n} \in \mathbb{Z}/3\mathbb{Z}$, on a : $\varphi(\bar{n}) = \varphi(\bar{1} + \cdots + \bar{1}) = n\varphi(\bar{1}) = \bar{0}$

D'où φ est le morphisme nul.

Q3. Soit G un groupe multiplicatif et H un sous-groupe non trivial de G. Montrer que $< G \setminus H >= G$.

on a : $G \setminus H \subset G$ donc $\langle G \setminus H \rangle \subset G$. Réciproquement, soit $x \in G$.

Si $x \in G \setminus H$, alors $x \in \langle G \setminus H \rangle$.

Supposons $x \in H$. Comme $H \neq G$, il existe $a \in G \setminus H$, on a alors $ax \in G \setminus H$

Car sinon $a = ax \cdot x^{-1} \in H$ ce qui est absurde et par suite,

$x = a^{-1}(ax) \in \langle G \setminus H \rangle$. D'où $G = \langle G \setminus H \rangle$

Q4. Soit G un groupe multiplicatif d'ordre 4.

1. Supposons G contient un élément d'ordre 4. Montrer que G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

$\exists a \in G$ d'ordre 4 donc : $\langle a \rangle = \{e, a, a^2, a^3\} \subset G$, par suite,

$G = \langle a \rangle$ car ont même ordre.

donc G est cyclique d'ordre 4, par le théorème de classification des gpes monogène, G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

2. Supposons que G ne contient aucun élément d'ordre 4.

a. Montrer que $\forall x \in G$, $x^2 = e$.

$\forall x \in G$, on a : l'ordre de x divise 4 donc l'ordre de x égal à 2 ou 4

Comme G ne contient aucun élément d'ordre 4, alors l'ordre de x égal à 2, et par suite $\forall x \in G$; $x^2 = e$.

b. En déduire que G est abelien.

Si $(x,y)\in G^2$, on a : $x^2=y^2=e$ donc $x=x^{-1}$ et $y=y^{-1}$

donc $xy=x^{-1}y^{-1}=(yx)^{-1}=yx$ donc G est abélien.

c. Si on note $G=\{e,a,b,c\}$, remplir alors le tableau suivant :

On a : $a^2=b^2=c^2=e$;
$ab=ba=c$;
$bc=cb=a$;
$ac=ca=b$;

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

d. Déterminer un groupe ismorphe à G.

puisque $\forall x\in G : x^2=e$, alors G n'est pas cyclique

$+$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$

la table de gpe $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$

On remarque que les tables sont identique »

donc le gpe G et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ sont isomorphes

3. En déduire, à isomorphisme près, tous les groupes d'ordre 4.

D'après ce qui précède, à isomorphisme près, les gpes d'ordre 4 sont $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

Q5. Soit $B=\left\{\begin{pmatrix}\alpha & 0\\ 0 & 0\end{pmatrix},\ \alpha\in\mathbb{R}\right\}$.

question commune

1. Montrer que B est un anneau.

Il est clair que $(B,+)$ est un gpe abélien de neutre O_2

La loi $\times$ est distributive sur $+$.

La loi $\times$ est associative mais ne possède pas un élément neutre (1.)

2. B est-il un sous-anneau de l'anneau $(\mathcal{M}_2(\mathbb{R}),+,\times)$?

Non car $I_2\notin B$.

Q6. Soit A un anneau et $(x,y)\in A^2$. Montrer que, si $1-xy$ est inversible, il en est de même de $1-yx$, et comparer leurs inverses.

Supposons $1-xy$ est inversible d'inverse z, on a alors $z(1-xy)=1$, on multiplie par y à gauche et par x à droite, on obtient $1-yz(1-xy)x=1-yx$.

donc $1-(1-yx)yzx=1-yx$ (car $xyz=zxy=z-1$),

Par suite $1=(1-yx)(1+yzx)$, on montre de même que

$(1+yzx)(1-yx)=1$, donc $1-yx$ est inversible d'inverse $1+yzx$.

Q7. Rappeler le théorème d'Euler vu dans le cours puis, montrer pour tout $k \in \mathbb{N}$, $k \wedge n = 1 \Longrightarrow k^{n!} \equiv 1\ [n]$.

Soit n un entier ≥ 2 et $k \in \mathbb{N}$ tq $k \wedge n = 1$ alors $k^{\varphi(n)} \equiv 1\ [n]$ (th d'Euler).
Soit $k \in \mathbb{N}$ tq $k \wedge n = 1$, on a $\varphi(n) < n$, donc dans le produit $n! = n(n-1)\cdots \times 1$ il y a le facteur $\varphi(n)$ càd $\varphi(n)$ divise $n!$.
par suite $k^{n!} \equiv 1\ [n]$.

Q8. Soit A un anneau commutatif intègre fini et $a \in A \setminus \{0\}$. On considère l'application $f_a : A \longrightarrow A$ définie par $f_a(x) = ax$.

1. Montrer que f_a est injectif.

Soit $(x,y) \in A^2$ tq $f_a(x) = f_a(y)$ donc $ax = ay$ càd $a(x-y) = 0$;
donc $a = 0$ ou $x - y = 0$, mais $a \neq 0$ donc $x = y$ càd f injective.

2. En déduire que A est un corps.

f_a est injective et A est fini donc f_a A bijective, donc en particulier, il existe $b \in A$ tq : $f(b) = 1$ càd $ab = 1 = ba$ donc a est inversible donc A est un corps.

Q9. Soit $f : \mathbb{C} \longrightarrow \mathbb{C}$ un morphisme d'anneaux tel que $\forall x \in \mathbb{R},\ f(x) = x$.

Montrer que $f = \mathrm{Id}_{\mathbb{C}}$ ou $f(z) = \overline{z}$ pour tout $z \in \mathbb{C}$.

on a : $(f(i))^2 = f(i^2) = f(-1) = -1$, donc $f(i) = i$ ou $-i$
si $f(i) = i$, soit $z \in \mathbb{C}$, $z = a + ib$, $(a,b) \in \mathbb{R}^2$
$f(z) = f(a+ib) = f(a) + f(i) f(b) = a + ib = z$ donc $f = \mathrm{Id}_{\mathbb{C}}$
si $f(i) = -i$ alors $f(z) = f(a) + f(i) f(b) = a - ib = \overline{z}$ donc $f(z) = \overline{z}$.

Q10. Soit $(a,b) \in \mathbb{Z}^2$.

1. Montrer qu'il existe $m \in \mathbb{N}^*$ unique tel que : $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

$a\mathbb{Z}$ et $b\mathbb{Z}$ sont deux idéaux de $\mathbb{Z}$ donc $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$
donc il existe $m \in \mathbb{Z}$ tq $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$
si $m \in \mathbb{N}^*$ alors m est unique

2. Montrer que m est caractérisé par : $\begin{cases} a \mid m \\ b \mid m \end{cases}$ et $\left(\forall c \in \mathbb{Z},\ \begin{cases} a \mid c \\ b \mid c \end{cases} \Longrightarrow m \mid c\right)$. (*).

On a : $m\mathbb{Z} \subset a\mathbb{Z}$ et $m\mathbb{Z} \subset b\mathbb{Z}$ donc a/m et b/m
Soit $c \in \mathbb{Z}$ tq a/c et b/c donc $c\mathbb{Z} \subset a\mathbb{Z}$ et $c\mathbb{Z} \subset b\mathbb{Z}$ donc $c\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$
càd $c\mathbb{Z} \subset m\mathbb{Z}$ donc m/c
Inversement, supposons (*) et montrons que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$?
Posons $a\mathbb{Z} \cap b\mathbb{Z} = \delta\mathbb{Z}$ avec $\delta \in \mathbb{N}^*$;
on a a/m et b/m donc $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = \delta\mathbb{Z}$ càd $m\mathbb{Z} \subset \delta\mathbb{Z}$
or a/δ et b/δ donc m/δ càd $\delta\mathbb{Z} \subset m\mathbb{Z}$, par suite $m\mathbb{Z} = \delta\mathbb{Z}$
Or $m, \delta \in \mathbb{N}$ alors $m = \delta$ d'où $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Q11. Déterminer $U(\mathbb{Z}/7\mathbb{Z})$, le groupe des éléments inversibles de l'anneau $\mathbb{Z}/7\mathbb{Z}$. Le groupe $U(\mathbb{Z}/7\mathbb{Z})$ est-il cyclique ?

D'après le cours $U(\mathbb{Z}/7\mathbb{Z}) = \{\bar{k} \in \mathbb{Z}/7\mathbb{Z} ; k \wedge 7 = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

On a : $\bar{3}^0 = \bar{1}$; $\bar{3}^1 = \bar{3}$, $\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{6}$, $\bar{3}^4 = \bar{4}$; $\bar{3}^5 = \bar{5}$

Ainsi $U(\mathbb{Z}/7\mathbb{Z}) = \langle \bar{3} \rangle$ c.à.d $U(\mathbb{Z}/7\mathbb{Z})$ est cyclique d'ordre 6.

Q12. Résoudre le système de congruence suivant $\begin{cases} 3x+2 \equiv -1 \ [5] \\ 3x-1 \equiv 3 \ [7] \end{cases}$ (S),

$(S) \Leftrightarrow \begin{cases} 3x \equiv -3 \ [5] \\ 3x \equiv 4 \ [7] \end{cases} \Leftrightarrow \begin{cases} x \equiv -1 \ [5] \\ 3x \equiv 4 \ [7] \end{cases}$ Car $3 \wedge 5 = 1$;

$\Leftrightarrow \begin{cases} x \equiv -1 \ [5] \\ 6x \equiv 8 \ [7] \end{cases}$

$\Leftrightarrow \begin{cases} x \equiv -1 \ [5] \\ x \equiv -1 \ [7] \end{cases} \Leftrightarrow \boxed{x \equiv -1 \ [35]}$

Q13. Soit $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers, on pose

$$I = \left\{(1+X^2)A + 2XB, \ (A,B) \in (\mathbb{Z}[X])^2\right\}.$$

1. Montrer que I est un idéal de $\mathbb{Z}[X]$.

Notons $I_1 = (1+X^2).\mathbb{Z}[X]$ et $I_2 = 2X.\mathbb{Z}[X]$;

On a d'après $I = I_1 + I_2$ or I_1 et I_2 sont deux idéaux de $\mathbb{Z}[X]$ donc I est un idéal de $\mathbb{Z}[X]$.

2. I est-il engendré par un élément de $\mathbb{Z}[X]$?

Supposons qu'il existe $P \in \mathbb{Z}[X]$ tq $I = P.\mathbb{Z}[X]$

On a $2X \in P.\mathbb{Z}[X]$ donc P divise $2X$ donc $P = \pm 2, \pm X, \pm 2X$

Par ailleurs $P \in I$ donc $P = (1+X^2).A + 2X.B$ avec $A, B \in \mathbb{Z}[X]$

$P(1) = 2(A(1) + B(1))$ pair, soit alors $P = \pm 2$ ou $\pm X$.

Q14. Montrer que le polynôme $P = X^3 + X + 1$ est irréductible sur $\mathbb{Q}$.

Si $\frac{p}{q} \in \mathbb{Q}$ est une racine de P ; $p \wedge q = 1$

donc $p^3 + pq^2 + q^3 = 0$ c.à.d $p^3 = -q(pq + q^2)$

donc q/p^3 donc q/p (1) absurde

donc P est irréductible sur $\mathbb{Q}$.

or P divise X^2+1 ;

donc $P = (X^2+1).Q$, $Q \in \mathbb{Z}[X]$

$P(0)Q(0) = 1$,

mais $P(0) = 0$ ou ± 2

Ce qui est absurde

d'où I n'est pas engendré par un élément de $\mathbb{Z}[X]$.

Q15. Factoriser dans $\mathbb{R}[X]$ les polynômes : X^6+1 et X^8+X^4+1.

$X^6+1 = (X^2)^3+1 = (X^2+1)(X^4-X^2+1)$

$= (X^2+1)(X^4+2X^2+1-3X^2)$

$= (X^2+1)((X^2+1)^2-(\sqrt{3}X)^2)$

$= (X^2+1)(X^2+\sqrt{3}X+1)(X^2-\sqrt{3}X+1)$

et les trinômes obtenus sont à discriminant <0

$X^8+X^4+1 = (X^4+1)^2-X^4$

$= (X^4-X^2+1)(X^4+X^2+1)$

$= ((X^2+1)^2-3X^2)((X^2+1)^2-X^2)$

$= (X^2-\sqrt{3}X+1)(X^2+\sqrt{3}X+1)(X^2-X+1)(X^2+X+1)$

et les quatres trinômes obtenus sont à discriminant <0

Q16. Soit $(m,n)\in\mathbb{N}^2$ non nuls. Montrer que $(X^m-1)\wedge(X^n-1)=X^{m\wedge n}-1$ dans $\mathbb{K}[X]$.

On applique l'algorithme d'Euclide : supposons par exemple $n>m$, et on écrit $n=mq+r$ avec $0\leq r<m$. Alors on a :

$X^n-1 = X^{mq+r}-1 = X^r(X^{mq}-1)+X^r-1$,

Or :

$X^{mq}-1 = (X^m)^q-1 = (X^m-1)(X^{m(q-1)}+X^{m(q-2)}+\dots+X^m+1)$.

donc X^m-1 divise $X^{mq}-1$,

Ainsi :

$(X^n-1)\wedge(X^m-1) = (X^m-1)\wedge(X^r-1)$. Puisque $n\wedge m = m\wedge r$

On en déduit finalement que $(X^n-1)\wedge(X^m-1) = X^{n\wedge m}-1$.

Q17. Chercher m pour que X^2+X+1 divise $(X+1)^m-X^m-1$ (sur $\mathbb{C}$).

On pose $P=(X+1)^m-X^m-1$, les racines de X^2+X+1 sont j, j^2 avec $j=e^{2i\pi/3}$;

Donc : X^2+X+1 divise P (SSI) $P(j)=P(j^2)=0$.

or $P(j) = (j+1)^m-j^m-1 = (-j^2)^m-j^m-1$

En étudiant les congruences de m modulo 6, on obtient :

X^2+X+1 divise P (SSI) $m\equiv\pm1[6]$.