

Defraiteur
Mascence

Devoir à la Maison
en M51.

Exercice 3

On veut montrer tout nombre premier congru à 1 modulo 4 est somme de deux carrés.

Première partie : Soit Y un ensemble fini et φ une involution sur Y , i.e. $\varphi: Y \rightarrow Y$ tq $\varphi \circ \varphi = \text{Id}_Y$. Posons $Y^{\varphi} := \{y \in Y, \varphi(y) = y\}$.

On veut montrer que $\text{card}(Y)$ et $\text{card}(Y^{\varphi})$ ont la même parité.

Définissons une relation d'équivalence $x R y$ sur $Y \setminus Y^{\varphi}$, c'est-à-dire $(x = \varphi(y))$ ou $(x = y)$.

On peut vérifier assez facilement que les propriétés de symétrie, réflexivité et transitivité sont bien vérifiées pour cette relation d'équivalence.

Ensuite prenons un élément x dans $Y \setminus Y^{\varphi}$, on veut montrer que

$$\bar{x} = \{x, \varphi(x)\} : y \in \bar{x} \Leftrightarrow y = x \text{ ou } y = \varphi(x) \Leftrightarrow \bar{x} = \{x, \varphi(x)\}.$$

Ainsi on vient de montrer que la classe d'équivalence $Y \setminus Y^{\varphi}$ ne possède que 2 éléments. D'après la proposition du cours, les k classes d'équivalence forment une partition. D'où $|Y \setminus Y^{\varphi}| = 2k$.

$$\text{Ainsi on obtient } |Y| = |Y^{\varphi}| + |Y \setminus Y^{\varphi}| = |Y^{\varphi}| + 2k$$

Quelque soit la parité de $|Y^{\varphi}|$, $|Y|$ et $|Y^{\varphi}|$ seront de même parité car sommer un nombre pair ne va pas influer sur le résultat.

Seconde partie : Fixons un nombre premier p congru à 1 modulo 4.

On définit $X := \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz\}$.

a) Montrons que X est non vide et fini.

Prenons le nombre premier $p = 13$, 13 est bien congru à 1 modulo 4 et d'autre part $13 = 3^2 + 4$ avec $(x, y, z) = (3, 1, 1) \in \mathbb{N}^3$.

Donc X est non-vide. Ensuite, montrons que X est fini.

Prenons y, z fixes, $p = x^2 + 4yz$: 1 seul x vérifie cette égalité.

Prenons x, z fixes, $p = x^2 + 4yz$: 1 seul y vérifie cette condition.

Prenons x, y fixes, $p = x^2 + 4yz$: 1 seul z vérifie cette condition.

Suivant ce dénombrement, X est bien un ensemble fini.

b) Montrons que $f: \mathbb{N}^3 \rightarrow \mathbb{N}^3$ définie par $f(x, y, z) = (x, z, y)$ se restreint en une involution sur X , notée $\sigma: X \rightarrow X$.

Soit σ une involution sur X , $X^\sigma = \{x \in X, \sigma(x) = x\} = \{(x, y, z) \in X, \sigma((x, y, z)) = (x, y, z)\}$

Montrons que $\delta|_X$ est une involution.

D'abord, on doit montrer que $\delta|_X(\delta|_X(x, y, z)) = (x, y, z)$

$$\cdot \delta|_X(\delta|_X(x, y, z)) = \delta|_X(x, z, y) = (x, y, z)$$

Deuxièmement, on doit montrer que $\delta|_X(x, y, z) \in X$.

$$\delta|_X(x, y, z) = (x, z, y) \quad \text{Car } X = \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz\}$$

Puis pour $(x, y, z) = (x, z, y)$, on a $p = x^2 + 4zy = x^2 + 4yz$.

Donc $\delta|_X(x, y, z) \in X$. Et ainsi $\delta|_X$ est bien une involution et $\delta|_X = \sigma$.

c) Montrons que si X^σ est non vide alors p est somme de deux carrés.

Soit $X^\sigma = \{(x, y, z) \in X, \sigma((x, y, z)) = (x, y, z)\}$ \emptyset est non-vide.

Puis $X^\sigma = \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz, \sigma((x, y, z)) = (x, y, z)\}$.

$$\sigma(x, y, z) = \delta|_X(x, y, z) = (x, z, y) = (x, y, z) \quad \text{d'où } z = y$$

De $p = x^2 + 4yz$ avec $z = y$ $p = x^2 + 4z^2 = x^2 + (2z)^2$: donc p est bien la somme de 2 carrés.

d) Soit $(x, y, z) \in X$. Vérifions les 3 inégalités suivantes :

$$(i) y-z < 2y \quad (ii) x \neq y-z \quad (iii) x \neq 2y$$

(i) soit $(x, y, z) \in X$, $y-z < 2y \Leftrightarrow -y+z < 0 \Leftrightarrow -y < z$. La dernière inégalité est toujours vraie car $(x, y, z) \in \mathbb{N}^3$.

(ii) Raisonnons par l'absurde et supposons $x = y-z$,

$$\text{soit } (y-z, y, z) \in X, \text{ on a } p = (y-z)^2 + 4yz = y^2 - 2yz + z^2 + 4yz \\ = y^2 + 2yz + z^2 = (y+z)^2$$

On a obtenu $p = \text{un carré}$ or

d'après la c), $p = \text{somme de 2 carrés}$. Ce qui montre la contradiction de l'hypothèse de départ donc $x \neq y-z$.

(iii) Raisonnons par l'absurde et supposons $x = 2y$, soit $(2y, y, z) \in X$,

on a $p = 4y^2 + 4yz = 4(y^2 + yz)$, c'est-à-dire $p \mid 4$ or 4 n'est pas un nombre premier donc cela montre bien la contradiction. Ainsi $x \neq 2y$. (car p premier n'est divisible que par p ou 1).

e) Soit $g: X \rightarrow \mathbb{Z}^3$ l'application définie par

$$g(x, y, z) = \begin{cases} (x+2z, z, y-x-z) & \text{si } x < y-z \\ (2y-x, y, x-y+z) & \text{si } y-z < x \leq 2y \\ (x-2y, x-y+z, y) & \text{si } x > 2y \end{cases}$$

Montrons que g se restreint en une involution sur X , notée $\mathcal{T}: X \rightarrow X$.

On a $\mathcal{T} = g|_X$. D'abord montrons que $g(X) \subset X$, i.e. on veut montrer que $(x, y, z) \in X \Rightarrow g(x, y, z) \in X$.

soit $(x, y, z) \in X$, pour $x < y-z$, on a $p = (x+2z)^2 + 4z(y-x-z) \in X$
pour $y-z < x \leq 2y$, on a $p = (2y-x)^2 + 4y(x-y+z) \in X$
pour $x > 2y$, on a $p = (x-2y)^2 + 4(x-y+z)(y) \in X$

Donc $g(x, y, z) \in X$.

Ensuite, on doit montrer que $g|_X(g|_X(x, y, z)) = \text{Id}$.

Calculons $g(g(x, y, z)) = \begin{cases} \textcircled{a} & x < y - z \\ \textcircled{b} & x - y - z < x < 2y \\ \textcircled{c} & x > 2y \end{cases}$ où $\textcircled{a}, \textcircled{b}, \textcircled{c}$ désignent des systèmes de 3 lignes.

Pour \textcircled{a} , calculons $g(x+2z, z, y-x-z)$;

$$\textcircled{a} = \begin{cases} (x+2z)+2(y-x-z), y-x-z, z-x-2z-y+n+z \\ (2z-x-2z), z, x+2z-z+y-x-z \\ x+2z-2z, x+2z-z+y-x-z, z \end{cases} = \begin{cases} -x+2y, y-x-z, -y & si x < y - z \\ -x, z, y & si y - z < x < 2y \\ x, y, z & si x > 2y \end{cases}$$

Pour \textcircled{b} , calculons $g(2y-x, y, x-y+z)$;

$$\textcircled{b} = \begin{cases} 2y-x+2x-2y+2z, x-y+z, y-2y+x-x+y-z \\ 2y-2y+x, y, 2y-x-y+x-y+z \\ 2y-x-2y, 2y-x-y+x-y+z, y \end{cases} = \begin{cases} x+2z, x-y+z, -2y-z & si x < y - z \\ x, y, z & si y - z < x < 2y \\ -x, z, y & si x > 2y \end{cases}$$

Pour \textcircled{c} , calculons $g(x-2y, x-y+z, y)$;

$$\textcircled{c} = \begin{cases} x-2y+2y, y, x-y+z-x+2y-y \\ x-2y+2z-x+2y, x-y+z, x-2y-x+y-z+y \\ x-2y-2x+2y-2z, x-2y-x+y-z+y, x-y+z \end{cases} = \begin{cases} x, y, z & si x < y - z \\ x+2z, x-y+z, -2y-z & si y - z < x < 2y \\ -x-2z, -z, x-y+z & si x > 2y \end{cases}$$

$$\begin{cases} -x+2y, y-x-z, -y & (1) si x < y - z \\ -x, z, y & (2) si y - z < x < 2y \\ x, y, z & (3) si x > 2y \end{cases}$$

$$\text{D'où } g(g(x, y, z)) = \begin{cases} x+2z, x-y+z, -2y-z & (4) si x < y - z \\ x, y, z & (5) si y - z < x < 2y \\ -x, z, y & (6) si x > 2y \\ x, y, z & (7) si x < y - z \\ x+2z, x-y+z, -2y-z & (8) si y - z < x < 2y \\ -x-2z, -z, x-y+z & (9) si x < y - z \end{cases}$$

On va montrer assez aisément que les lignes (1), (2), (4), (6), (8), (9) sont absurdes et impossibles car elles ne vérifient pas les conditions et (4) inégalités de la question d) et la définition de $(x, y, z) \in X$.

Département
Maxence

Devoir à la Maison en M51.

L3 - Maths

$$\text{D'où } g(g(x, y, z)) = \begin{cases} x, y, z & \text{si } x < y - z \\ x, y, z & \text{si } y - z < x < 2y \\ x, y, z & \text{si } x > 2y \end{cases}$$

Donc on a bien obtenu $g(g(x, y, z)) = \text{Id}$. Donc g se restreint en une involution sur X .

j) Désirons l'ensemble X^{σ} .

$$X^{\sigma} = \{x \in X, \sigma(x) = x\} = \{(x, y, z) \in X, \sigma|_X(x, y, z) = (x, y, z)\}$$

On veut montrer que $X^{\sigma} = \{(1, 1, k)\}$ d'après l'indication.

(C) On note $p = 1 + 2k$, $k \in \mathbb{N}$; vérifions que $(1, 1, k) \in X^{\sigma}$.

$$\sigma(1, 1, k) = (2 \cdot 1 - 1, 1, 1 - 1 + k) = (1, 1, k) \in X^{\sigma}.$$

(C) Soit $(x, y, z) \in X^{\sigma}$ alors on a :

$$\begin{cases} (x+2z, z, y-x-z) = (x, y, z) & \text{si } x < y - z \\ (2y-x, y, x-y+z) = (x, y, z) & \text{si } y - z < x < 2y \\ (x-2y, x-y+z, y) = (x, y, z) & \text{si } x > 2y. \end{cases}$$

$$\Leftrightarrow \begin{cases} x+2z = x \\ z = y & \text{si } x < y - z \\ y-x-z = z \\ 2y-x = x \\ y = y & \text{si } y - z < x < 2y \\ x-y+z = z \\ x-2y = x \\ x-y+z = y & \text{si } x > 2y \\ y = z \end{cases}$$

$$\Leftrightarrow \begin{cases} (x, y, z) = (0, 0, 0) & \text{si } x < y - z \quad (1) \\ y = n & \text{si } y - z < x < 2y \quad (2) \\ (x, z) \in \mathbb{N}^2 & \\ (x, y, z) = (0, 0, 0) & \text{si } x > 2y \quad (3) \end{cases}$$

Si les lignes (1) et (3) sont absurdes car elles ne vérifient pas les conditions attendues. Ainsi l'élément appartient bien à X^{σ} .

En partant de $\begin{cases} y=x \\ (x,y) \in TN^2 \end{cases}$ on prenant $(x,y,z)=(1,1,k)$ alors vérifie bien le système souhaité.

Donc on a bien démontré l'inclusion (C).

g) On veut en déduire de la première partie que les cardinaux des 3 ensembles X^σ , X et X^τ sont impairs.

D'après la question f), $|X^\sigma| = 1$ (impair) car l'ensemble X^σ est seulement constitué d'un singleton. Puis d'après la première partie, les cardinaux de X^σ et de X sont de même parité ; de même pour X^τ et X .

Donc $|X^\sigma|$ impair $\Rightarrow |X|$ impair $\Rightarrow |X^\tau|$ impair.

Exercice L: Soit G un groupe d'ordre $p_1^{d_1} \dots p_m^{d_m}$ où p_1, \dots, p_m sont m nombres premiers tel que $p_1 < \dots < p_m$ et $d_i > 0$, $i=1, \dots, m$ ($m \geq 2$). Soit U un sous-groupe de G d'indice p_1 .

a) Montrons que le pgcd de $p_1^{d_1} \dots p_m^{d_m}$ et de $p_1!$ est p_1 .

soit $a = (p_1)^{d_1} \times \dots \times p_m^{d_m}$ avec $d_i > 0$, $i = [1, m]$, $m \geq 2$

$$b = p_1! = p_1 \times \dots \times 2 \times 1 = p_1!$$

Par définition le plus grand commun diviseur de a et b est p_1 .

On note G/U l'ensemble des classes à gauche xU de G modulo U ($x \in G$).

b) Montrons que la formule $\tau(g)(xU) = gxU$ ($g, x \in G$) définit une action $\tau: G \rightarrow \text{Bij}(G/U)$ du groupe G sur l'ensemble G/U .

soit $\tau: G \rightarrow \text{Bij}(G/U)$

$$gt \mapsto gxU$$

Montrons que τ est un morphisme de groupe. Soit $g, h \in G$,

$$g \cdot \tau(h)(xU) = \tau(g)\tau(h)(xU) = \tau(g)(hxU) = ghxU = \tau(gh)(xU) = (gh)(xU).$$

Donc τ est bien un morphisme de groupe.

On cherche maintenant à expliciter une réciproque :

$$\tau^{-1}(g)(xU) = \tau(g^{-1})(xU).$$

$$\tau(gg^{-1})(xU) = xU \leftarrow \text{Identité'}$$

Donc $\tau(g)(xU)$ définit bien une action de groupe G sur l'ensemble G/U .

c) On veut montrer que $|G/\ker(\tau)| = p_1$.

D'après le 1^{er} théorème d'isomorphisme, $G/\ker(\tau) \cong \text{Im}(\tau)$.

(On peut l'appliquer car $\tau: G \rightarrow \text{Bij}(G/U)$ est un morphisme de groupe, $\ker(\tau) \trianglelefteq G$ d'après la proposition du cours et $\ker \tau \subset \ker \tau$).

On veut montrer que $|\text{Im}(\tau)| = p_1$. La stratégie serait de procéder par double inclusion. (Inachevée)

d) Non réalisée.

Exercice 1: Étant donnés 2 nombres premiers distincts p et q , on considère les groupes suivants :

$$G_1 = \mathbb{Z}/p^m\mathbb{Z} \quad (m \geq 1), \quad G_2 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \quad G_3 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

a) Pour chacun de ces 3 groupes, déterminons l'ensemble de leurs sous-groupes.

D'après la proposition du cours, les sous-groupes de $\mathbb{Z}/p^m\mathbb{Z}$ sont les groupes $\mathbb{Z}/k\mathbb{Z}$ avec $k \mid p^m$ où $k = p^m$, $m \geq 0$.

D'où les sous-groupes de G_1 sont $\mathbb{Z}/p^m\mathbb{Z} / \mathbb{Z}/p^n\mathbb{Z}$ pour $m > 0$, $n > 1$.

Puis $G_2 = \underbrace{\mathbb{Z}/p\mathbb{Z}}_{\text{par le Théorème des restes chinois}} \times \underbrace{\mathbb{Z}/q\mathbb{Z}}_{\text{ils ont }} \cong \mathbb{Z}/pq\mathbb{Z}$

ils ont le même nombre de sous-groupes (4).

• 1^o sous-groupe: $\bar{0} \times \bar{0}$ 2^o sous-groupe: $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Puis G_2 est un produit direct de 2 groupes $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/q\mathbb{Z}$,

$G_2 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ alors $\widetilde{\mathbb{Z}/p\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z} \times \bar{0}$ et $\widetilde{\mathbb{Z}/q\mathbb{Z}} = \bar{0} \times \mathbb{Z}/q\mathbb{Z}$

sont des sous-groupes de G_2 .

D'où 3^o sous-groupe: $\mathbb{Z}/p\mathbb{Z} \times \bar{0}$, 4^o sous-groupe: $\bar{0} \times \mathbb{Z}/q\mathbb{Z}$.

Puis $G_3 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, par le même raisonnement que pour G_2 ,

on obtient: 1^o sous-groupe: $\bar{0} \times \bar{0}$; 2^o sg: $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$; 3^o sg: $\mathbb{Z}/p^2\mathbb{Z} \times \bar{0}$;
 4^o sg: $\bar{0} \times \mathbb{Z}/q\mathbb{Z}$, 5^o sg: $\mathbb{Z}/p^2\mathbb{Z} \times \bar{0}$, 6^o sg: $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

b) Pour $i = 1, 2, 3$; déterminons les groupes $\overline{\Phi}(G_i)$.

On a $\mathbb{Z}/p^m\mathbb{Z} = p^0\mathbb{Z}/p^m\mathbb{Z} \supset p^1\mathbb{Z}/p^m\mathbb{Z} \supset \dots \supset p^m\mathbb{Z}/p^m\mathbb{Z} = \{0\}$

Car $p^1\mathbb{Z}/p^m\mathbb{Z}$ est le seul sous-groupe $\subset G_1$ contenant strictement G_1 .

Comme $\overline{\Phi}(G_1)$ est l'intersection de tous les sous-groupes maximaux $\Rightarrow \overline{\Phi}(G_1) = \mathbb{Z}/p\mathbb{Z}$.

Puis $\bar{0} \times \bar{0} \subset \mathbb{Z}/p\mathbb{Z} \times \bar{0} \subset \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

pour G_2 , $\bar{0} \times \bar{0} \subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Par le même raisonnement que pour G_1 , les sous-groupes maximaux de G_2

sont $\bar{0} \times \mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \bar{0}$. D'où $\overline{\Phi}(G_2) = \{\bar{0} \times \bar{0}\}$.

Puis pour G_3 , $\bar{0} \times \bar{0} \subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$\bar{0} \times \bar{0} \subset \mathbb{Z}/p^2\mathbb{Z} \times \bar{0} \subset \mathbb{Z}/p^2\mathbb{Z} \times \bar{0} \subseteq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$\bar{0} \times \bar{0} \subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Donc les sous-groupes maximaux de G_3 sont:

$\bar{0} \times \mathbb{Z}/q\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \bar{0}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. D'où $\overline{\Phi}(G_3) = \{\bar{0} \times \bar{0}\}$.

⑧ c) Non-traitée.

14,5/20

Bon devoir

Exercice 3

On veut montrer que tout nombre premier congru à 1 modulo 4 est somme de deux carrés.

Première partie : Soit Y un ensemble fini et φ une involution sur Y , i.e. $\varphi : Y \rightarrow Y$ tq $\varphi \circ \varphi = \text{Id}_Y$. Posons $Y^{\varphi} := \{y \in Y, \varphi(y) = y\}$.

On veut montrer que $\text{card}(Y)$ et $\text{card}(Y^{\varphi})$ ont la même parité.

Définissons une relation d'équivalence $x R y$ sur $Y \setminus Y^{\varphi}$, c'est-à-dire $(x = \varphi(y))$ ou $(x = y)$.

On peut vérifier assez facilement que les propriétés de symétrie, réflexivité et transitivité sont bien vérifiées pour cette relation d'équivalence. ✓

Ensuite prenons un élément x dans $Y \setminus Y^{\varphi}$, on veut montrer que $\bar{x} = \{x, \varphi(x)\} : y \in \bar{x} \Leftrightarrow y = x \text{ ou } y = \varphi(x) \Leftrightarrow \bar{x} = \{x, \varphi(x)\}$.

Ainsi on vient de montrer que la classe d'équivalence $Y \setminus Y^{\varphi}$ ne possède que 2 éléments. D'après la proposition du cours, les k classes d'équivalence forment une partition. D'où $|Y \setminus Y^{\varphi}| = 2k$.

Ainsi on obtient $|Y| = |Y^{\varphi}| + |Y \setminus Y^{\varphi}| = |Y^{\varphi}| + 2k$

Quelque soit la parité de $|Y^{\varphi}|$, $|Y|$ et $|Y^{\varphi}|$ seront de même parité car sommer par un nombre pair ne va pas influer sur le résultat.

2

Seconde partie: Fixons un nombre premier p congru à 1 modulo 4.

$$\text{On définit } X := \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz\}.$$

a) Montrons que X est non vide et fini.

Prenons le nombre premier $p = 13$, 13 est bien congru à 1 modulo 4 et d'autre part $13 = 3^2 + 4$ avec $(x, y, z) = (3, 1, 1) \in \mathbb{N}^3$.

Donc X est non-vide. Ensuite, montrons que X est fini. Il faut le montrer pour tout $p \equiv 1 \pmod{4}$

Prenons y, z fixes, $p = x^2 + 4yz$: 1 seul x vérifie cette égalité. Ca ne peut pas dire que

Prenons x, z fixes, $p = x^2 + 4yz$: 1 seul y vérifie cette condition. Il faut le montrer pour tout $p \equiv 1 \pmod{4}$

Prenons x, y fixes, $p = x^2 + 4yz$: 1 seul z vérifie cette condition. X est fini

Suivant ce dénombrement, X est bien un ensemble fini.

b) Montrons que $f: \mathbb{N}^3 \rightarrow \mathbb{N}^3$ définie par $f(x, y, z) = (x, z, y)$ se restreint en une involution sur X , notée $\sigma: X \rightarrow X$.

Soit σ une involution sur X , $X^\sigma = \{x \in X, \sigma(x) = x\} = \{(x, y, z) \in X, \sigma((x, y, z)) = (x, y, z)\}$

Montrons que $\sigma|_X$ est une involution.

Premièrement, on doit montrer que $\sigma|_X (\sigma|_X (x, y, z)) = (x, y, z)$

$$\cdot \sigma|_X (\sigma|_X (x, y, z)) = \sigma|_X (x, z, y) = (x, y, z) \quad \checkmark$$

Deuxièmement, on doit montrer que $\sigma|_X (x, y, z) \in X$.

$$\sigma|_X (x, y, z) = (x, z, y) \quad \text{Car } X = \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz\}$$

$$\text{Puis pour } (x, y, z) = (x, z, y), \text{ on a } p = x^2 + 4zy = x^2 + 4yz.$$

Donc $\sigma|_X (x, y, z) \in X$. Et ainsi $\sigma|_X$ est bien une involution et $\sigma|_X = \sigma$.

c) Montrons que si X^σ est non vide alors p est somme de deux carrés.

Soit $X^\sigma = \{(x, y, z) \in X, \sigma((x, y, z)) = (x, y, z)\}$ est non-vide.

Puis $X^\sigma = \{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz, \sigma((x, y, z)) = (x, y, z)\}$.

$$\sigma((x, y, z)) = \sigma|_X (x, y, z) = (x, z, y) = (x, y, z) \quad \text{d'où } z = y \quad \checkmark$$

De $p = x^2 + 4zy$ avec $z = y$ $p = x^2 + 4z^2 = x^2 + (2z)^2$: donc p est bien la somme de 2 carrés.

d) Soit $(x, y, z) \in X$. Vérifions les 3 inégalités suivantes:

$$(i) y-z < 2y \quad (ii) x \neq y-z \quad (iii) x \neq 2y$$

$$(i) \text{ soit } (x, y, z) \in X, y-z < 2y \Leftrightarrow -y+z < 0 \Leftrightarrow -y < z.$$

La dernière inégalité est toujours vraie car $(x, y, z) \in \mathbb{N}^3$. 0,75

(ii) Raisonnons par l'absurde et supposons $x = y-z$,

$$\text{soit } (y-z, y, z) \in X, \text{ on a } p = (y-z)^2 + 4yz = y^2 - 2yz + z^2 + 4yz = y^2 + 2yz + z^2 = (y+z)^2$$

On a obtenu $p = \text{un carré}$ or

d'après la c), $p = \text{somme de 2 carrés}$. Ce qui montre la contradiction de l'hypothèse de départ donc $x \neq y-z$. 0,75

(iii) Raisonnons par l'absurde et supposons $x = 2y$, soit $(2y, y, z) \in X$,

on a $p = 4y^2 + 4yz = 4(y^2 + yz)$, c'est-à-dire $p \mid 4$ ou 4 n'est pas un nombre premier donc cela montre bien la contradiction. Et ainsi $x \neq 2y$. 0,75

(car p premier n'est divisible que par p ou 1).

e) Soit $g: X \rightarrow \mathbb{Z}^3$ l'application définie par

$$g(x, y, z) = \begin{cases} (x+2z, z, y-x-z) & \text{si } x < y-z \\ (2y-x, y, x-y+z) & \text{si } y-z < x < ly \\ (x-2y, x-y+z, y) & \text{si } x > 2y \end{cases}$$

Montrons que g se restreint en une involution sur X , notée $\mathcal{T}: X \rightarrow X$.

On a $\mathcal{T} = g|_X$. D'abord montrons que $g(X) \subset X$, ie on veut montrer que $(x, y, z) \in X \Rightarrow g(x, y, z) \in X$.

Soit $(x, y, z) \in X$, pour $x < y-z$, on a $p = (x+2z)^2 + 4z(y-x-z) \in X$

pour $y-z < x < ly$, on a $p = (2y-x)^2 + 4y(x-y+z) \in X$

pour $x > 2y$, on a $p = (x-2y)^2 + 4(x-y+z)(y) \in X$

Donc $g(x, y, z) \in X$.

0,75 ✓

②

③

Ensuite, on doit montrer que $g|_X (g|_X (x, y, z)) = \text{Id}$

Calculons $g(g(x, y, z)) = \begin{cases} @ & x < y - z \\ @ & x - y - z < x < 2y \\ @ & x > 2y \end{cases}$ où @, @, @ désignent des systèmes de 3 lignes.

Pour @, calculons $g(x+2z, z, y-x-z)$;

$$@ = \begin{cases} (x+2z)+2(y-x-z), y-x-z, z \cdot z \cdot x-2z-y+n+z & x < y-z \\ (2z-x-2z), z, x+2z-z+y-x-z & x - y - z < x < 2y \\ x+2z-2z, x+2z-z+y-x-z, z & x > 2y \end{cases} = \begin{cases} -x, z, y & x - y - z < x < 2y \\ x, y, z & x > 2y \end{cases}$$

Pour b, calculons $g(2y-x, y, x-y+z)$;

$$b = \begin{cases} 2y-x+2x-2y+2z, x-y+z, y-2y+x-x+y-z & x < y-z \\ 2y-2y+x, y, 2y-x-y+x-y+z & x - y - z < x < 2y \\ 2y-x-2y, 2y-x-y+x-y+z, y & x > 2y \end{cases} = \begin{cases} x+2z, x-y+z, -2y-z & x < y-z \\ x, y, z & x - y - z < x < 2y \\ -x, z, y & x > 2y \end{cases}$$

Pour c, calculons $g(x-2y, x-y+z, y)$;

$$c = \begin{cases} x-2y+2y, y, x-y+z-x+2y-y & x < y-z \\ x-2y+2z-x+2y, x-y+z, x-2y-x+y-z+y & x - y - z < x < 2y \\ x-2y-2x+2y-2z, x-2y-x+y-z+y, x-y+z & x > 2y \end{cases} = \begin{cases} x, y, z & x < y-z \\ x+2z, x-y+z, -2y-z & x - y - z < x < 2y \\ -x-2z, -z, x-y+z & x > 2y \end{cases}$$

$$\begin{cases} -x+2y, y-x-z, -y & (1) \text{ si } x < y-z \\ -x, z, y & (2) \text{ si } y-z < x < 2y \\ x, y, z & (3) \text{ si } x > 2y \end{cases}$$

$$\text{D'où } g(g(x, y, z)) = \begin{cases} x+2z, x-y+z, -2y-z & (4) \text{ si } x < y-z \\ x, y, z & (5) \text{ si } y-z < x < 2y \\ -x, z, y & (6) \text{ si } x > 2y \\ x, y, z & (7) \text{ si } x < y-z \\ x+2z, x-y+z, -2y-z & (8) \text{ si } y-z < x < 2y \\ -x-2z, -z, x-y+z & (9) \text{ si } x < y-z \end{cases}$$

On va montrer assez aisément que les lignes (1), (2), (4), (6), (8), (9) sont absurdes et impossibles car elles ne vérifient pas les conditions et (4) inégalités de la question d) et la définition de $(x, y, z) \in X$.

Définition
Maxence

Devan à la Maison en M51

L3 - Maths

$$\text{D'où } g(g(x, y, z)) = \begin{cases} x, y, z & \text{si } x < y - z \\ x, y, z & \text{si } y - z < x < 2y \\ x, y, z & \text{si } x > 2y \end{cases}$$

Donc on a bien obtenu $g(g(x, y, z)) = \text{Id}$, donc g se restreint en une involution sur X . 0,75

j) Dénisons l'ensemble X^{σ} .

$$X^{\sigma} = \{x \in X, \overline{G}(x) = x\} = \{(x, y, z) \in X, \overline{g}|_X(x, y, z) = (x, y, z)\}$$

On veut montrer que $X^{\sigma} = \{(1, 1, k)\}$ d'après l'indication.

(C) On note $\rho = 1 + 4k$, $k \in \mathbb{N}$; vérifions que $(1, 1, k) \in X^{\sigma}$.
 $\overline{G}(1, 1, k) = (\rho \cdot 1 - 1, 1, 1 - 1 + k) = (1, 1, k) \in X^{\sigma}$.

(C) Soit $(x, y, z) \in X^{\sigma}$ alors on a :

$$\begin{cases} (x+2z, z, y-x-z) = (x, y, z) & \text{si } x < y - z \\ (2y - x, y, x - y + z) = (x, y, z) & \text{si } y - z < x < 2y \\ (x - 2y, x - y + z, y) = (x, y, z) & \text{si } x > 2y. \end{cases}$$

$$\begin{aligned} & \left\{ \begin{array}{l} x+2z = x \\ z = y \\ y-x-z = z \end{array} \right. \quad \text{si } x < y - z \\ \Leftrightarrow & \left\{ \begin{array}{l} 2y - x = x \\ y = y \\ x - y + z = z \end{array} \right. \quad \text{si } y - z < x < 2y \\ & \left\{ \begin{array}{l} x - 2y = x \\ x - y + z = y \\ y = z \end{array} \right. \quad \text{si } x > 2y \end{aligned}$$

$$\begin{aligned} & \Leftrightarrow \left\{ \begin{array}{l} (x, y, z) = (0, 0, 0) \\ y = n \\ (x, z) \in \mathbb{N}^2 \end{array} \right. \quad \text{si } x < y - z \quad (1) \\ & \qquad \qquad \qquad \quad \text{si } y - z < x < 2y \quad (2) \\ & \qquad \qquad \qquad \quad (x, y, z) = (0, 0, 0) \quad \text{si } x > 2y \quad (3) \end{aligned}$$

On les lignes (1) et (3) sont absurdes car elles ne vérifient pas les conditions attendues. Ainsi l'élément appartient bien à X^{σ} . 1,5 (5)

En partant de $\{ \begin{array}{l} y=x \\ (x,y) \in TN^2 \end{array} \}$ en prenant $(x,y,z)=(1,1,k)$ alors
on vérifie bien le système souhaité.

Donc on a bien démontré l'inclusion (C).

g) On veut en déduire de la première partie que les cardinaux des 3 ensembles X^σ , X et X^τ sont impairs.

D'après la question f), $|X^\sigma| = 1$ (impair) car l'ensemble X^σ est seulement constitué d'un singleton. Puis d'après la première partie, les cardinaux de X^τ et de X sont de même puissance ; de même pour X^σ et X .

Donc $|X^\sigma|$ impair $\Rightarrow |X|$ impair $\Rightarrow |X^\tau|$ impair. *Et la conclusion?*

Exercice 2: Soit G un groupe d'ordre $p_1^{d_1} \dots p_m^{d_m}$ où p_1, \dots, p_m sont m nombres premiers tels que $p_1 < \dots < p_m$ et $d_i > 0$, $i=1, \dots, m$ ($m \geq 1$). Soit U un sous-groupe de G d'indice p_1 .

a) Montrez que le pgcd de $p_1^{d_1} \dots p_m^{d_m}$ et de $p_1!$ est p_1 .

Soit $a = (p_1)^{d_1} \times \dots \times (p_m)^{d_m}$ avec $d_i > 0$, $i \in [1, m]$, $m \geq 1$.
 $b = (p_1) \times \dots \times 2 \times 1 = p_1!$

Par définition le plus grand commun diviseur de a et b est p_1 . *0,5/1,5*

Tu as juste mis p_1 divise les deux, pas que c'est le plus grand
On note G/U l'ensemble des classes à gauche xU de G modulo U ($x \in G$).

b) Montrez que la forme $\gamma(g)(xU) = gxU$ ($g, x \in G$) définit une action $\gamma: G \rightarrow \text{Bij}(G/U)$ du groupe G sur l'ensemble G/U .

soit $\gamma: G \rightarrow \text{Bij}(G/U)$

$$g \mapsto gxU$$

Montrez que γ est un morphisme de groupe. Soit $g, h \in G$,

$$g \cdot \gamma(h)(xU) = \gamma(g)\gamma(h)(xU) = \gamma(g)(h \cdot xU) = gh \cdot xU = \gamma(gh)(xU) = (gh)(xU).$$

Donc γ est bien un morphisme de groupe. ✓

On cherche maintenant à expliciter une réciproque : *Pas nécessaire si $\gamma: G \rightarrow \text{Bij}(G/U)$ est un morphisme,*

$$\gamma^{-1}(g)(xU) = \gamma(g^{-1})(xU).$$

$$\gamma(gg^{-1})(xU) = xU \leftarrow \text{Identité}.$$

Donc $\gamma(g)(xU)$ définit bien une action de groupe G sur l'ensemble G/U . *1,5*

c) On veut montrer que $|G/\ker(\gamma)| = p_1$.

D'après le 1^{er} théorème d'isomorphisme, $G/\ker(\gamma) \cong \text{Im}(\gamma)$

(On peut l'appliquer car $\gamma: G \rightarrow \text{Bij}(G/U)$ est un morphisme de groupe, $\ker(\gamma) \trianglelefteq G$ d'après la proposition du cours et $\ker \gamma \subset \ker \gamma$)

On veut montrer que $|\text{Im}(\gamma)| = p_1$. La stratégie serait de procéder par double inclusion. (Inachevée)

c) Non réalisée.

Exercice 1: Étant donné 2 nombres premiers distincts p et q , on considère les groupes suivants :

$$G_1 = \mathbb{Z}/p^n\mathbb{Z} \quad (n \geq 1), \quad G_2 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \quad G_3 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

a) Pour chacun de ces 3 groupes, déterminons l'ensemble de leurs sous-groupes.

D'après la proposition du cours, les sous-groupes de $\mathbb{Z}/p^n\mathbb{Z}$ sont les groupes $\mathbb{Z}/p^k\mathbb{Z}$ avec $k \mid n$ où $k = p^m$, $m \geq 0$.

D'où les sous-groupes de G_1 sont $\mathbb{Z}/p^m\mathbb{Z} / \mathbb{Z}/p^n\mathbb{Z}$ pour $m \geq 0$, $n \geq 1$. *0,5*

$$\text{Puis } G_2 = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}}_{\substack{\text{il} \\ \text{ont}}} \simeq \mathbb{Z}/pq\mathbb{Z} \quad (\text{par le Théorème des restes chinois})$$

il ont le même nombre de sous-groupes (4).

$$\cdot 1^{\circ} \text{sous-groupe: } \bar{0} \times \bar{0} \quad \cdot 2^{\circ} \text{sous-groupe: } \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Puis G_2 est un produit direct de 2 groupes $\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}$,

$$G_2 = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \text{ alors } \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \bar{0} \text{ et } \mathbb{Z}/q\mathbb{Z} = \bar{0} \times \mathbb{Z}/q\mathbb{Z} \quad 0,5$$

sont des sous-groupes de G_2 .

$$\text{D'où } 3^{\circ} \text{sous-groupe: } \mathbb{Z}/p\mathbb{Z} \times \bar{0}, \quad 4^{\circ} \text{sous-groupe: } \bar{0} \times \mathbb{Z}/q\mathbb{Z}.$$

Puis $G_3 = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, par le même raisonnement que pour G_2 ,

$$\text{on obtient: } 1^{\circ} \text{sous-groupe: } \bar{0} \times \bar{0}; \quad 2^{\circ} \text{sg: } \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}; \quad 3^{\circ} \text{sg: } \mathbb{Z}/p^2\mathbb{Z} \times \bar{0};$$

$$4^{\circ} \text{sg: } \bar{0} \times \mathbb{Z}/q\mathbb{Z}, \quad 5^{\circ} \text{sg: } p\mathbb{Z}/p^2\mathbb{Z} \times \bar{0}, \quad 6^{\circ} \text{sg: } p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \quad 0,5$$

b) Pour $i = 1, 2, 3$, déterminons les groupes $\Phi(G_i)$.

$$\text{On a } \mathbb{Z}/p^m\mathbb{Z} = p^0\mathbb{Z}/p^m\mathbb{Z} \supset p^1\mathbb{Z}/p^m\mathbb{Z} \supset \dots \supset p^m\mathbb{Z}/p^m\mathbb{Z} = \{0\}$$

$\overset{\text{G}_1}{\underset{\text{sous-groupe maximal}}{\supset}}$

Car $p^1\mathbb{Z}/p^m\mathbb{Z}$ est le seul sous-groupe de G_1 contenant strictement G_1 .

Comme $\Phi(G_1)$ est l'intersection de tous les sous-groupes maximaux $\Rightarrow \Phi(G_1) = \frac{p\mathbb{Z}}{p^m\mathbb{Z}} \quad 0,5$.

$$\begin{aligned} \text{Puis } \bar{0} \times \bar{0} &\subset \mathbb{Z}/p\mathbb{Z} \times \bar{0} \subset \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \text{pour } G_2, \quad \bar{0} \times \bar{0} &\subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \end{aligned}$$

Par le même raisonnement que pour G_1 , les sous-groupes maximaux de G_2

sont $\bar{0} \times \mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \bar{0}$. D'où $\Phi(G_2) = \{\bar{0} \times \bar{0}\} \quad 0,5$.

$$\text{Puis pour } G_3, \quad \bar{0} \times \bar{0} \subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

$$\bar{0} \times \bar{0} \subset p\mathbb{Z}/p^2\mathbb{Z} \times \bar{0} \subset \mathbb{Z}/p^2\mathbb{Z} \times \bar{0} \subseteq \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

$$\bar{0} \times \bar{0} \subset \bar{0} \times \mathbb{Z}/q\mathbb{Z} \subset p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Donc les sous-groupes maximaux de G_3 sont:

$$\bar{0} \times \mathbb{Z}/q\mathbb{Z}, \quad \mathbb{Z}/p^2\mathbb{Z} \times \bar{0}, \quad p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}. \quad \text{D'où } \Phi(G_3) = \{\bar{0} \times \bar{0}\}.$$

pas maximaux

(8) c) Non traitée.