Université Ibn Tofail
Ecole Nationale des Sciences Appliquées
Kénitra, Maroc

Mathématiques, Algèbre 1, 2011-2012

Cycle préparatoire

Série $n^\circ : 3$

Exercice 3. Etudier les propriétés (associativité, commutativité, élément neutre, éléments inversibles) des lois de composition internes suivantes :
a) $m * n = m^n$ sur $\mathbb{N}$.
b) $m * n = max(m, n)$ sur $\mathbb{N}$.
c) $m * n = max(m, n)$ sur $\mathbb{Z}$.
d) $m * n = (m + n)^2$ sur $\mathbb{Z}$.

Exercice 4. Soit $(G, .)$ un groupe avec $G = \{1, a, b, c, d, f\}$ où 1 est l'élément neutre de G.
1) Sachant que l'on a : $a^2 = 1$, $b^2 = 1$, $c = ab$, $d = ba$, $f = ca$ et $ca = bc$, Trouver la table de la loi $\cdot$ sur G (i.e calculer le composé xy pour x et y dans G).
2) En utilisant cette table, déterminer les inverses des éléments de G.

Exercice 5: Les ensembles suivants sont-ils des groupes pour les lois considérées?
1) $\mathbb{R}$ muni de la loi $*$ définie par $\forall$ a,b $\in \mathbb{R}$, $a * b = a + b + ab$.
2) L'ensemble $E = \{-1, 1, i, -i\} \subset \mathbb{C}$, muni de la multiplication usuelle.

Exercice 6. Soit $C = \{(x, y) \in \mathbb{R}^2 \ / x^2 + y^2 = 1\}$ le cercle unité dans $\mathbb{R}^2$. On définit une loi $*$ sur C par : $\forall (a, b),\ (c, d) \in C,\ (a, b) * (c, d) = (ac - bd, ad + bc)$.
1) Montrer que la loi $*$ est une loi de composition interne sur C.
2) Montrer que $(C, *)$ est un groupe. Est-il commutatif ?.

Exercice 7$^{(*)}$: Soit $(G, .)$ un groupe. On note $Z(G) = \{g \in G / \forall x \in G\ xg = gx\}$.
1) Montrer que $Z(G)$ est un sous -groupe abélien de G. ($Z(G)$ est appelé centre de G).
2) Soit $(G', .)$ un groupe et $f : G \to G'$ un homomorphisme de groupes . Montrer que si f est surjectif, alors $f(Z(G)) \subset Z(G')$
3) On suppose que G possède un seul élément a d'ordre 2. Montrer que $a \in Z(G)$.

Exercice 8$^{(*)}$:

1) Montrer que si p est un nombre premier et G un groupe d'ordre p, alors G est cyclique engendré par l'un quelconque de ses éléménts différents de e.

2) Soit G un groupe fini d'ordre pq, où p et q sont deux nombres premiers. Montrer que tout sous-groupe propre de G est cyclique.

3) Montrer que tout sous-groupe d'un groupe cyclique est cyclique.

Exercice 9:

1) Calculer $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ dans S_4.

2) Calculer $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 3 \end{pmatrix}^{-1}$ dans S_4.

3) Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix} \in S_6$ en produit de cycles disjoints puis en produit de transpositions et déterminer l'ordre de σ.

Exercice10: Soit σ l'élément de S_{12} défini par:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 10 & 7 & 1 & 2 & 6 & 4 & 5 & 12 & 8 & 9 & 11 \end{pmatrix}$$

1) Décomposer σ en produit de cycles disjoints puis en produit de transpositions.
2) Déterminer les orbites de σ.
3) Donner la signature de σ.
4) Déterminer σ^{2005}.

Exercie 11$^{(*)}$: Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 1 & 4 & 2 & 6 & 9 & 8 & 5 & 10 \end{pmatrix} \in S_{10}$

1) décomposer σ en produit de cycles disjoints et en produit de transpositions.
2) Calculer σ^{2007}.

Exercice 12: Soit G un groupe, H et K deux sous-groupes de G.
1) Montrer que $H \cup K$ est un sous groupe de G si et seulement si $H \subset K$ ou $K \subset H$
2) En déduire que G n'est jamais la réunion de deux de ses sous-groupes propres.

Exercice 13$^{(*)}$: Soit $G =< a >$ un sous cyclique d'ordre n.
1) Soit $H \neq \{e\}$ un sous-groupe de G et m le plus petit entier strictement positif tel que $a^m \in H$. Montrer que $m|n$ et que $|H| = \dfrac{n}{m}$
2) Montrer que si $d \in \mathbb{N}$ est tel que $d|n$, alors G possède un unique sous-groupe d'ordre d.
Application: Déterminer le sous-groupe de $\mathbb{Z}/104\mathbb{Z}$ d'ordre 4.

Exercice 14$^{(*)}$. Soit $(G, .)$ un groupe et soient $f, h, g : G \to G$ trois applications définies par $f(x) = x^{-1}$ (l'inverse de x) , $h(x) = x^2$ et $g(x) = axa^{-1}$ $(a \in G)$.
1) Montrer que f est un homomorphisme de groupes si et seulement si G est abélien.
2) Montrer que h est un homomrphisme de groupes si et seulement si G est abélien.
3) En déduire qu'un groupe dans lequel tout élément est son propre inverse est abélien.
4) Montrer que g est un homomorphisme de groupes et que G est abélien si et seulement si $g = id_G, \forall a \in G$.

Exercice 15: Soit A un anneau unitaire tel que tout élément de A est idempotent, i e , $\forall\ a \in A, a^2 = a$.
1) Montrer que $\forall\ a \in A,\ a + a = 0$.
2) En déduire que A est commutatif.
3) Montrer que si $a, b \in A$, alors $ab(a + b) = 0$.
4) On suppose que A est intègre. Montrer que A a au plus deux éléments.

Exercice 19: Soient A, B deux anneaux et $f : A \to B$ un homomorphisme d'anneaux.
On rapelle que $\{0\}$ et A sont des idéaux de A. et que si J est un idéal de B, alors $f^{-1}(J)$ est un idéal de A.En particulier que $kerf = f^{-1}(\{0\})$ est un idéal de A.
1) Donner un exemple d'un idéal I de A tel que $f(I)$ n'est pas un idéal de B.
2) Soit I un idéal de A. Montrer que si f est surjectif, alors $f(I)$ est un idéal de B.
3) On suppose que A est commutatif, unitaire et unifère. Montrer que A est un corps si, et seulement si, les seuls idéaux de A sont $\{0\}$ et A.

Exercice 20 . Equations linéaires
Résoudre, dans $\mathbb{Z}/37\mathbb{Z}$, les équations ou systèmes d'équations suivants :
1) $7x = 2$.
2) $\begin{cases} 3x + 7y = 3 \\ 6x - 7y = 0 \end{cases}$

Exercice 21. Equation du second degré
Résoudre
1) $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2) $x^2 - \overline{4}x + \overline{3} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Université Ibn Tofail
Ecole Nationale des Sciences Appliquées
Kénitra, Maroc

Mathématiques, Algèbre 1, 2011-2012

Cycle préparatoire

Série n° : 3 Correction

Exercice 1. a) non associative-par exemple $(2*3)*2 = 64 \neq 512 = 2*(3*2)$;non commutative, pas d'élément neutre.
b)associative, commutative, élément neutre 0 qui est le seul élément inversible.
c)associative, commutative, pas d'élément neutre.
d)non associative-par exemple $(-1)*(1*1) = 9 \neq 1 = ((-1)*1)*1$; commutative, pas d'élément neutre

Exercice 2. On trouve la table suivante :

·	1	a	b	c	d	f
1	1	a	b	c	d	f
a	a	1	c	b	f	d
b	b	d	1	f	a	c
c	c	f	a	d	1	b
d	d	b	f	1	c	a
f	f	c	d	a	b	1

(Exemple : pour trouver $d.a$, on observe que $d = b.a$, et donc par associativité, $d.a = (b.a).ab.(a.a) = b.1 = b$). On peut déduire de cette table que G n'est pas commutatif, puisque, par exemple, $a\Delta f = d$ alors que $f\Delta a = c$. On voit aussi facilement les inverses : $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = d$, $d^{-1} = c$ et $f^{-1} = f$.

Exercice 3:

1) Non ($*$ est associaitive, admet un élément neutre ($e = 0$), mais (-1) n'est pas inversible).

2) oui.

Exercice 4.

a) Supposons que (a, b) et (c, d) appartiennent à C. Alors $a^2 + b^2 = 1$ et $c^2 + d^2 = 1$. Il faut montrer que leur produit $(ac-bd, ad+bc)$ appartient à C. On a $(ac-bd)^2+(ad+bc)^2 = a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2 = (a^2 + b^2)(c^2 + d^2) = 1$, donc $(ac - bd, ad + bc)$ appartient à C, et C est stable pour $*$.
b) On a $((a, b) * (c, d)) * (p, q) = ((ac - bd)p - (ad + bc)q, (ac - bd)q + (ad + bc)p)$, et $(a, b) * ((c, d) * (p, q)) = (a(cp - dq) - b(cq + dp), a(cq + dp) + b(cp - dq))$, qui sont égaux. Donc $*$ est associative. L'élément neutre est $(1, 0)$ et l'inverse de (a, b) est $(a, -b)$ (il faut résoudre l'équation $(a, b) * (x, y) = (1, 0)$ pour x et y, et tenir compte de $a^2 + b^2 = 1$ et $x^2 + y^2 = 1$).

Exercice 5

1) On a $Z(G) \neq \oslash$ (car $e \in Z(G)$). Soient $x, y \in Z(G)$, alors $\forall g \in G$, $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$ d'où $xy \in Z(G)$.

Soit $x \in Z(G)$, alors $\forall g \in G, xg^{-1} = g^{-1}x$ d'où $gx^{-1} = (xg^{-1})^{-1} = (g^{-1}x)^{-1} = x^{-1}g$ et ainsi $x^{-1} \in Z(G)$. Alors $Z(G)$ est un sous-groupe de G et il est évident que $Z(G)$ est abélien.

2) Soit $x \in Z(G)$, $\forall g\prime \in G\prime$, $\exists g \in G : f(g) = g'$. D'où $f(x)g' = f(x)f(g) = f(xg) = f(gx) = f(g)f(x) = g'f(x)$.

3) Soit $x \in G$, on a $(xax^{-1})^2 = xa^2x^{-1} = xx^{-1} = e$ d'où $o(xax^{-1}) = 2$ (car $xax^{-1} \notin e$, sinon $a = e$) et ainsi $xax^{-1} = a$, i.e $xa = ax$, et donc $a \in Z(G)$.

Exercice 6:

1) Soit $a \in G - \{e\}$. Puisque $|< a >|$ divise $|G|$ et $|G|$ est premier, $|< a >| = 1$ ou p. Or, $|< a >| \neq 1$ car $a \neq e$ et donc $|< a >| = p$ et par suite $< a >= G$.

2) Soit H un sous-groupe propre de G, alors $|H|$ divise pq et $|H| \neq pq$, alors $|H| = 1$ ou p ou q (si $p = q$, $|H| = 1$ ou p) et ainsi, d'après 1), H est cyclique (si $|H| = 1$, $H =< e >$).

3) Soient $G =< a >$ un groupe cyclique et H un sous-groupe de G, supposons que $H \neq \{e\}$ (si $H = \{e\}$, alors $H =< e >$). Posons

$A = \{s \in \mathbb{N}^* / a^* \in H\}$, alors A possède un plus petit élément qu'on note m ($A \subset \mathbb{N}$ et $A \neq \varnothing$ car $H \neq \{e\}$). Pour montrer que $H =< a^m >$, il suffit de vérifier que $H \subset < a^m >$ car $a^m \in H$, soit $x = a^t \in H$, alors $\exists (q, r) \in \mathbb{N}^2 : t = mq + r$, avec $0 \leq r < m$ d'où $a^t.(a^{mq})^{-1} = a^r \in H$ et ainsi $r = 0$ car m est le plus petit entier > 0 tel que $a^m \in H \Longrightarrow a^t = (a^m)^q \in < a^m. >$.

Exercice 7:

1) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (2\ 3\ 4)$

2) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^{-1} = (1\ 3\ 4\ 2)$

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix} = (1\ 6\ 5\ 4) = (16)(65)(54)(23) = (14)(15)(16)(23)$.

On calcule $\sigma^1 = \sigma \neq e$, $\sigma^2 = (15)(46)$, $\sigma^3 = (1456)(23)$, $\sigma^4 = e$, alors $o(\sigma) = 4$.

Exercice 8.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 10 & 7 & 1 & 2 & 6 & 4 & 5 & 12 & 8 & 9 & 11 \end{pmatrix}$$

1) $\sigma = (1\ 3\ 7\ 4)(2\ 10\ 8\ 5)(9\ 12\ 11) = (1\ 3)(3\ 7)(7\ 4)(2\ 10)(10\ 8)(8\ 5)(9\ 12)(12\ 11)$

La décomposition en produit de transpositions n'est pas unique !

2) $O(1) = \{1, 3, 4, 7\} = O(3) = O(4) = O(7)$, puis $O(2) = \{2, 5, 8, 10\}$ puis $O(6) = \{6\}$ et $O(9) = \{9, 11, 12\} = O(11) = O(12)$.

σ a 4 orbites, deux de cardinal 4, une de cardinal 3 et un singleton (correspondant à un point fixe).

3) La signature de σ est $\varepsilon(\sigma) = (-1)^{n-n_1}$ où n_1 est le nombre d'orbites de σ donc $\varepsilon(\sigma) = 1$ c'est une permutation paire.

4) σ est donc le produit commutatif des cycles $c_1 = (1\ 3\ 7\ 4)$, $c_2 = (2\ 10\ 8\ 5)$,et $c_3 = (9\ 12\ 11)$

On a $c_1^4 = c_2^4 = Id$ et $c_3^3 = Id$. Or, $2005 = 4 \times 501 + 1$. Donc, $c_1^{2005} = c_1^{4\times 501+1} = c_1$, de même $c_2^{2005} = c_2^{4\times 501+1} = c_2$. Puis, $c_3^{2005} = c_3^{3\times 668} c_3 = c_3$

Puisque c_1, c_2 et c_3 commutent, $\sigma^{2005} = c_1^{2005} c_2^{2005} c_3^{2005} = c_1 c_2 c_2 = \sigma$.

Exercice 9:

1) $\sigma = (13)(2795)$ est une décomposition de σ en un produit de cycles disjoints et $\sigma = (13)(27)(79)(95)$ est une décomposition de σ en un produit de transpositions.

2) Puisque (13) et (2795) sont des cycles disjoints, (13) et (2795) commutent et ainsi $\sigma^2 = (2795)^2 = (29)(75)$. On a aussi

$\sigma^3 = (13)(2795)(29)(75) = (13)(2597)$, $\sigma^4 = (13)(2795)(13)(2597) = (2795)(2597) = e$ et ainsi $o(\sigma) = 4$.

Comme $2007 = 4.501 + 3, \sigma^{2007} = (\sigma^4)^{501}\ \sigma^3 == e\sigma^3 = \sigma^3 = (13)(2597)$.

Exercice 10:

1) Si $H \subset K$ (resp. $K \subset H$), alors $H \cup K = K$ (resp. $H \cup K = H$). Supposons que $H \subsetneq K$ et que $K \subsetneq H$, alors $\exists h \in H : h \notin K$ et $\exists k \in K : k \notin K$. Alors $hk \notin H \cup K$, car si $hk \in H$ alors $k = h^{-1}(hk) \in H$, de même si $hk \in K$.

2) Supposons q'il existe H et K deux sous-groupes de G, tels que $HK = G$. Alors d'après 1), $H \subset K$ ou $K \subset H$ et ainsi $K = G$ ou $H = G$.

Exercice 11:

1) On a d'près l'exercice 6) 3), $H =< a^m >$. En effectuant la division euclidienne de n par m, on obtient $n = mq + r$, avec $(q, r) \in \mathbb{N} \times \mathbb{N}$ et

$0 \leq r < m$.

Puisque $G = < a >$ est d'ordre n, $e = a^n$ d'où $e = a^{mq}.a^r \in H$, et comme $a^{mq} = (a^m)^q \in H$ car $a^m \in H$, $a^r = (a^{mq})^{-1} \in H$. Etant donné que m est le plus petit entier strictement positif tel que $a^m \in H$ et que $0 \leq r < m$, alors $r = 0$ et ainsi m/n.

Posons $|H| = o(a^n) = s$. On a $a^{ms} = (a^m)^s = e$ d'où $n|ms$ et puisque $m|n$ $\frac{n}{m}|s$. D'autre part $(a^m)^{\frac{n}{m}} = a^n = e$ d'où $s|\frac{n}{m}$. Alors $s = \frac{n}{m}$.

2) Si $d = 1$, alors $H = \{e\}$est l'unique sous-groupe de G d'ordre 1. Supposons que $d > 1$. Soit $H =< a^{\frac{n}{d}} >$. Puisque $d|n$, $\frac{n}{d}$ est le plus petit entier strictement positif tel que $a^{\frac{n}{d}} \in H$, en effet si $a^s \in H =< a^{\frac{n}{d}} >$, $a^s = (a^{\frac{n}{d}})^t$ d'où $a^{sd} = e$ ainsi $n|sd$ et puisque $d|n$, $\frac{n}{d}|s$. Alors d'après b), $|H| = \frac{n}{\frac{n}{d}} = d$.

De plus . Si K est sous-groupe de G (d'ordre d) alors $K =< a^m >$ où m est le plus petit entier strictement positif tel que $a^m \in K$ et , d'après b), on a $d = \frac{n}{m}$ d'où $K =< a^m >=< a^{\frac{n}{d}} > = H$.

Application: $\mathbb{Z}/104\mathbb{Z}$ est un groupe cyclique. Alors d'après c), $\mathbb{Z}/104\mathbb{Z}$ possède un unique sous-groupe H d'ordre 4 et $H =< \frac{104}{4}.\overline{1} > =< \overline{26} >= \left\{\overline{0}, \overline{26}, \overline{52}, \overline{78}\right\}$.

Exercice 12.

1) f est un homomorphisme de groupes si et seulement si $(xy)^{-1} = x^{-1}y^{-1}$ pour tout $x \in G$ ou encore $y^{-1}x^{-1} = x^{-1}y^{-1}$ c.à.d $xy = yx$

Exercice 13:

1) Puisque $(a + a)^2 = a + a$ et $a^2 = a$, $a + a = 0$.

2) On a $(a + b)^2 = a + b$ d'où $ab + ba = 0$ et puisque $ab + ab = 0$, alors $ab = -ab = ba$.

3) $ab(a + b) = aba + ab^2 = a^2b + ab^2 = ab + ab = 0$.

4) Soit $c \in A$, alors $c^2 = c$ d'où $c(c - 1) = 0$ et donc $c = 0$ ou $c = 1$.

Exercice 14.

1) On prend $i : \mathbb{Z} \to \mathbb{Q}$, $a \to a$, i est un homorphisme d'anneaux, $2\mathbb{Z}$ est un idéal de $\mathbb{Z}$, mais $i(2\mathbb{Z}) = 2\mathbb{Z}$ n'est pas un idéal
de $\mathbb{Q}$.

2) $(I, +)$ est un sous-groupe de $(A, +)$ et f est un homorphisme de groupes de $(A, +)$ vers $(B, +)$ d'où $f(I)$ est un sous-groupe de $(B, +)$. On a aussi $\forall b \in B$, $\forall y \in f(I)$, $b = f(a)$, où $a \in A$ car f est surjectif et $y = f(x)$, avec $x \in I$. Alors, $by = f(a)f(x) = f(ax)$ et puisque
$ax \in I$, $by \in f(I)$. De même pour $yb \in I$.

3) Supposons que A est un corps. Soit I un idéal non nul de A, alors $\exists x \in A - \{0\} : x \in I$ d'où x est inversible donc $1 = x^{-1}x \in I$ et par suite $I = A$ ($\forall a \in A$, $a = a.1 \in I$). Réciproquement, Soit $x \in A - \{0\}$, alors $(x) = Ax$ est un idéal non nul de A donc $(x) = A$ d'où $\exists x' \in A : xx' = 1$.

Exercice 15. Equations linéaires .

1) On cherche d'abord l'inverse de 7 dans $\mathbb{Z}/37\mathbb{Z}$. Cela revient à résoudre l'équation de Bezout $7u + 37v = 1$. En appliquant l'algorithme d'Euclide, on trouve qu'une solution particulière est donnée par $16 \times 7 - 3 \times 37 = 1$. Ainsi, 16 est inverse de 7 dans $\mathbb{Z}/37\mathbb{Z}$. Il vient
$7x = 2 \Leftrightarrow 16 \times 7x = 16 \times 2 \Leftrightarrow x = 32$.

2) On additionne la première et la deuxième ligne pour trouver $9x = 3$. Or, $1 = 37 - 4 \times 9$
et donc -4 est un inverse de 9 dans $\mathbb{Z}/37\mathbb{Z}$. On trouve donc
$9x = 3 \Leftrightarrow x = -4 \times 3 = -12 = 25$.
Si on reporte dans la première équation, on obtient
$3 \times (-12) + 7y = 3 \Leftrightarrow y = 39 = 2$.
Le résultat de la question précédente nous donne y = 2.

Exercice 16. Equation du second degré.

L'idée est de procéder comme pour la résolution habituelle d'une équation du second degré.

On applique donc la méthode qui conduit au discriminant, c'est-à-dire que l'on met le trinome sous forme canonique.

1) On peut remarque pour cette question que $\overline{14} = \overline{1}$. Ainsi,
$x^2 + x + \overline{7} = \overline{0} \Leftrightarrow x^2 + \overline{14}x + \overline{7} = \overline{0} \Leftrightarrow (x + \overline{7})^2 - \overline{42} = 0$
soit encore $(x + \overline{7})^2 = \overline{3}$. On remarque alors que $42 = 3$. Ainsi, l'équation est équivalente à
$(x + \overline{7})^2 - \overline{42} = \overline{0} \Leftrightarrow (x + \overline{7} + \overline{4})(x + \overline{7} - \overline{4}) = \overline{0}$.
Puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, et donc en particulier est intègre, ceci est encore équivalent
à $x + \overline{11} = \overline{0}$ ou $x + \overline{3} = \overline{0}$. L'ensemble des solutions est donc $\{\overline{2}, \overline{10}\}$.

2) On procède de la même façon. L'équation est équivalente à
$(x - \overline{2})^2 - \overline{1} = \overline{0}$.
On peut bien sûr factoriser encore et obtenir que l'équation est équivalente à

$(x-\overline{2}-\overline{1})(x-\overline{2}+\overline{1})=0$.

Mais cette fois, on ne peut pas aller plus loin car $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. Il faut plutôt écrire $(x-\overline{2})^2=\overline{1}$ et chercher les t dans $\mathbb{Z}/12\mathbb{Z}$ avec $t^2=\overline{1}$. Pour cela on dresse le tableau :

t	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
t^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{-3}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

(on a bien sûr $(-t)^2=t^2$). Ainsi, l'équation est équivalente $x-\overline{2}\in\{-\overline{5},-\overline{1},\overline{1},\overline{5}\}$. L'ensemble des solutions est donc $\{-\overline{5},-\overline{3},\overline{1},\overline{5}\}$.