Correction Alg. et arithm. Avancée.

Exercice 1 — 4/4

1/ On a $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$ muni de l'opération "$\circ$" composition des applications.

avec $\pi_1 = (1)$, $\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,

$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

- On a $\pi_1^1 = \pi_1 = 1_{S_3} \Rightarrow \text{ord}(\pi_1) = 1 \Rightarrow \langle \pi_1 \rangle = \{\pi_1\} \leq S_3$.

- $\pi_2 \neq 1_{S_3} \Rightarrow \pi_2^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \pi_3 \neq \pi_1$ — 1,5

$\Rightarrow \pi_2^3 = \pi_3 \circ \pi_2 = \pi_4$

$\Rightarrow \text{ord}\,\pi_2 = 3$

$\Rightarrow \langle \pi_2 \rangle = \{\pi_1, \pi_2, \pi_3\}$

- De même $\pi_3^3 = \pi_1 \Rightarrow \text{ord}(\pi_3) = 3$ et on a $\langle \pi_3 \rangle = \{\pi_1, \pi_2, \pi_3\}$

- $\text{ord}\,\pi_4 = 2 \Rightarrow \langle \pi_4 \rangle = \{\pi_1, \pi_4\} \leq S_3$

- $\text{ord}\,\pi_5 = 2 \Rightarrow \langle \pi_5 \rangle = \{\pi_1, \pi_5\} \leq S_3$

- $\text{ord}\,\pi_6 = 2 \Rightarrow \langle \pi_6 \rangle = \{\pi_1, \pi_6\} \leq S_3$

2/ $\langle \pi_2, \pi_4 \rangle = \{\pi_2, \pi_4, \pi_3, \pi_5, \pi_1, \pi_6\} = S_3$

1/6, 2/6 | 3/6, 6/1 — 1,5 + 1,5 + 1 + 1

Exercice 2 (6 pts)

Soit $m > 0$ (entier) et $a, b \in \mathbb{Z}$

On a $a \mathcal{R} b \Leftrightarrow m \mid (a-b)$ [relation d'équivalence]

(m divise $a-b$)

noté $a \equiv b \,[m]$.

1/ Si $a \equiv b\,[m]$ et $c \equiv d\,[m]$

$\Rightarrow \exists k_1 \in \mathbb{Z} : a = b + k_1 m$

$\exists k_2 \in \mathbb{Z} : c = d + k_2 m$ (0.5)

On a $a + c = (b + k_1 m) + (d + k_2 m)$

$= (b+d) + (k_1 + k_2) m \equiv (b+d) \bmod m$

De même, (0.5)

1.2 $ac = (b + k_1 m)(d + k_2 m)$

$= bd + bk_2 m + dk_1 m + k_1 k_2 m^2$

$= bd + (bk_2 + dk_1 + k_1 k_2 m) m \equiv bd \bmod m$

c/ Si $a \equiv b\,[m] \Rightarrow a^2 \equiv b^2\,[m]$ (D'après 1.2)

En multipliant n fois ($n > 0$) (0.5)

On obtient $a^n \equiv b^n\,[\bmod m]$

d/ If $ac \equiv bc \bmod m$ with $\gcd(c, m) = 1$

then $a \equiv b\,[m]$. (1)

En effet, si $ac \equiv bc \pmod m \Rightarrow m \mid (a-b)c$.

et si $\gcd(m, c) = 1 \Rightarrow m \mid (a-b) \Rightarrow a \equiv b\,[m]$.

Mais si $ac \equiv bc\ [m]$ avec $pgcd(m,c) = d > 1$

dans ce cas on peut pas tjs simplifier c.

En effet, si $a=1$, $b=3$, $c=4$ et $m=8$

On a : $ac = 1\times 4 = 4$, $bc = 3\times 4 = 12$

On a bien $ac \equiv 4\ [8]$

et $bc \equiv 12\ [8] \equiv 4\ [8]$

c'è $ac \equiv bc\ [8]$ mais on a ~~pas~~

$1\times 4 \equiv 3\times 4\ [8]$ Vrai (1)

mais $1 \not\equiv 3\ [8]$ est fausse.

(On peut pas simplifier le 4)

Car $pgcd(4,8) = 4 \neq 1$.

(c.à.d $ac=4$, $bc=12$, $4 \equiv 12\ [8]$ car $8 \mid 12-4$

On a pas $1\times 4 \equiv 3\times 4\ [8] \not\Rightarrow 1 \equiv 3\ [8]$ (fausse).

* On $7\ [6] \equiv 1\ [6] \Rightarrow 7^{200} \equiv \underbrace{1\times\cdots\times 1}_{200\text{ fois}} \equiv 1\ [6]$ (0,5)

2/ $\forall a \in \mathbb{Z}$, on a $a = mq + r$, $0 \leq r < m$

$\Rightarrow \forall \bar{a} = \overline{mq+r} = \overline{mq}$ ou $\bar{r}$ $0 \leq r \leq m-1$

$\Rightarrow \forall \bar{a} \equiv \bar{r}\ [m]$ avec $0 \leq r \leq m-1$

$\Rightarrow \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$. (1)

* $\overline{2} \bmod 8 = 2+8\mathbb{Z} = \{2+8k / k \in \mathbb{Z}\}$ 0,5

$= \{\ldots, -14, -6, 2, 10, 18, \ldots\}$

* $\overline{3} \bmod 8 = 3+8\mathbb{Z} = \{3+8k / k \in \mathbb{Z}\}$

$= \{\ldots, -13, -5, 3, 11, 19, \ldots\}$ 0,5

Exercice 3

On Considère le groupe $(\mathbb{Q}^*, \times, 1)$.

On $Ord(1) = 1$ car $1^1 = 1$

$Ord(-1) = 2$ car $(-1)(-1) = (-1)^2 = 1 \Rightarrow Ord(-1) = 2$.

$Ord(i) = 4$ car $(i)^1 = i \neq 1$

1 $(i)^2 = -1 \neq 1$

$(i)^3 = (i)^2 i = -1\, i = -i \neq 1$

$(i)^4 = (i^2)(i^2) = (-1) \times (-1) = 1$

$\Rightarrow Ord(i) = 4$.

$Ord(2) = \infty$, $\forall i > 0$, on a $2^i \neq 1$.

Soit $H = \{(e^{i 2\pi/n})^k, 0 \leq k \leq n-1\} = \langle e^{i2\pi/n} \rangle$

avec $|H| = n$

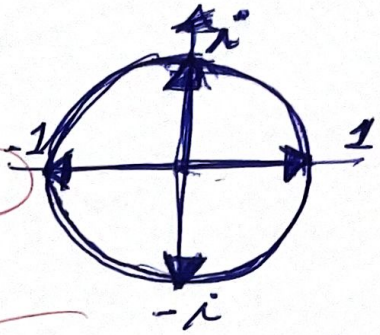
et on a $H = \langle (e^{i 2\pi/n})^k \rangle$ 1 ssi $pgcd(k, n) = 1$

↑ racine primitive nième de l'unité.

Pour $n=4$, on a

$$H=\left\{\left(e^{\frac{2\pi}{4}i}\right)^k \;/\; 0\le k\le 3\right\}$$

$$=\left\{\underset{1}{k=0},\ \underset{i}{k=1},\ \underset{-1}{k=2},\ \underset{-i}{k=3}\right\}$$



avec $H=\langle i\rangle=\langle -i\rangle$ 1,5

$$=\left\{i,\ i^2=-1,\ i^3=-1.i,\ i^4=i^2\times i^2=(-1)(-1)=1\right\}$$

les générateurs sont les $\left(e^{\frac{2\pi}{4}i}\right)^k$ avec $0\le k\le 3$ 0,5

$pgcd(k,4)=1$

$\Rightarrow$ $k=1$ ou bien $k=3$.

Exercice 4 ~~7pts~~ ~~8pts~~ 8pts

a/ On a $\forall a,b\in\mathbb{N}$ $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ avec $d=pgcd(a,b)$.

Comme $d\in d\mathbb{Z}$ (on a $d=d.1,\ 1\in\mathbb{Z}$)

$\Rightarrow$ on a aussi $d\in a\mathbb{Z}+b\mathbb{Z}$ 1

$\Rightarrow \exists u,v\in\mathbb{Z}:\ \boxed{au+bv=d}$

En particulier si $pgcd(a,b)=1 \Rightarrow \exists u,v\in\mathbb{Z}:\ \boxed{au+bv=1}$ 0,5

b/ si $d=1$ alors $\exists u,v\in\mathbb{Z}$ $au+bv=1$

si $pgcd(a,n)=1 \Rightarrow \exists u,v\in\mathbb{Z}:\ au+nv=1$

$\Rightarrow$ $\overline{au+nv}\equiv\overline{1}\ [n]$

$\Rightarrow$ $\overline{a}\odot\overline{u}+\overline{0}=\overline{1}\ [n] \Rightarrow \overline{a}\odot\overline{u}\equiv\overline{1}\ [n]$

$\Rightarrow$ $\boxed{\overline{a}^{-1}=\overline{u}\ [n]}$ 1,5

Comment obtenir $\bar{a}^{-1}$?

Si n est petit, on peut construire la table de $(\mathbb{Z}_n, \odot)$ et voir dans la table l'élément $\bar{u}$ tq $\bar{a} \odot \bar{u} = \bar{1}$ et donc $\bar{a}^{-1} = \bar{u}$.

Sinon on peut calculer l'inverse de $\bar{a}$ ie $\bar{a}^{-1}$ par l'algorithme d'Euclide étendu.

On calcule le pgcd(a, n) par l'algorithme d'Euclide, ensuite on cherche (on calcule) $u, v \in \mathbb{Z}$ tq : $au + nv = 1$ (Coefficients de Bezout)

Exemple $26 = 11 \times 2 + 4$

$11 = 4 \times 2 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$ ⇑ du bas en haut

$\Rightarrow 1 = 4 - 3 \times 1 = 4 - (11 - 4 \times 2) \times 1$

$= 4 - 11 + 4 \times 2 = 4 \times 3 - 11$

$= (26 - 11 \times 2) \times 3 - 11 = \boxed{26 \times 3 - 7 \times 11 = 1}$

$\Rightarrow \overline{-7 \times 11} = \bar{1}\ [26] \Rightarrow \bar{-7} \odot \bar{11} = \bar{1}\ [26]$

$\Rightarrow \bar{19} \odot \bar{11} = \bar{1}\ [26] \Rightarrow \boxed{\bar{11}^{-1} = \bar{19}\ [26]}$

1,5

c/ Le groupe $(\mathbb{Z}/n\mathbb{Z}^*, \odot, \bar{1})$ d'ordre $\varphi(n)$
l'indicatrice d'Euler
avec $\varphi(n) = |\{1 \leq k < n \mid pgcd(k,n)=1\}|$

D'après le corollaire de Lagrange,
On a dans un groupe fini d'ordre n

$\forall a \in G, \quad a^n = 1_G$

et comme $|\mathbb{Z}/n\mathbb{Z}^*| = \varphi(n)$

$\Rightarrow \forall a \in \mathbb{Z}, \quad \bar{a}^{\varphi(n)} \equiv 1 [n]$

c'est $\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}^*$, on a $\boxed{\bar{a}^{\varphi(n)} \equiv \bar{1}[n]}$

formules d'Euler

et si n est premier
alors $\varphi(n) = n-1$
et on a $\boxed{\bar{a}^{(n-1)} \equiv \bar{1}[n]}$

1 0,5

* Pourquoi $8^{50} - 1 \equiv 0 [11]$.
On a 11 est un nbre premier et $pgcd(8,11) = 1$

$\Rightarrow 8^{11-1} \equiv 1 [11]$ c'est $8^{10} \equiv 1 [11]$

$\Rightarrow (8^{10})^5 \equiv (1^5) [11] \Rightarrow 8^{50} \equiv 1 [11]$

$\Rightarrow 8^{50} - 1 \equiv 0 [11] \Rightarrow 11 / (8^{50} - 1)$ (11 divise $8^{50}-1$) 0,5

e/ $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ avec $1^{-1} = 1$, $3^{-1} = 3$ car $3 \times 3 \equiv 1 [8]$
$5^{-1} = 5$ car $5 \times 5 = 25 \equiv 1 [3]$, $7 \times 7 = 49 \equiv 1 [8]$
$\Rightarrow 7^{-1} = 7 [8]$ (7)

1,5