DS1

Un corrigé

Exercice

1. **a.** Pour tout $(x, y) \in \mathbb{Z}$, on pose $x\mathcal{R}y$ ssi 37 divise $(y - x)$.

b. La classe d'équivalence de 4 est l'ensemble des entiers x tels que $x - 4$ est un multiple de 37. Autrement dit $\overline{4} := \{4 + k \cdot 37 | k \in \mathbb{Z}\}$.

c. Pour $\overline{x}$ et $\overline{y}$ dans $\mathbb{Z}/37\mathbb{Z}$, on pose sous réserve de cohérence $\overline{x} + \overline{y} := \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \cdot y}$.

La multiplication est définie de manière cohérente, car la classe de xy ne dépend pas des choix des représentants x et y. En effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $x' = x + 37k_1$ et $y' = y + 37k_2$ et $x'y' = xy + 37k_3$ avec $k_3 = k_1 y + k_2 x + k_1 k_2 \in \mathbb{Z}$.

2. **a.** Pour tout $x \in [1, 36]$, x et 37 sont premiers entre eux, donc il existe u, v entiers tels que $ux + 37v = 1$. Dans $\mathbb{Z}/37\mathbb{Z}$, cela devient $\overline{xu} = \overline{xu} = \overline{1}$.

Ainsi, si $\overline{x} \neq \overline{0}$, $\overline{x}$ admet un inverse dans $\mathbb{Z}/37\mathbb{Z}$ qui est donc un corps.

b. Donc $card(U) = card(\mathbb{Z}/37\mathbb{Z}) - 1 = 36$

c. Attention : U ne peut pas être vu comme un sous groupe. Il faut donc repartir de la définition d'un groupe.

Comme la multiplication des entiers est associative, l'opération $\cdot$ est aussi associative.

$\cdot$ est une loi interne car si $(a, b) \in U$ alors il existe a^{-1} et b^{-1}. Posons $c = b^{-1}a^{-1}$. On a $(ab)c = (ab)(b^{-1}a^{-1}) = \overline{1}$ par associativité.

U n'est pas vide car contient $\overline{1}$.

Si $a \in U$, posons $b = a^{-1}$. Alors, par définition, $ab = ba = \overline{1}$.

Donc $(U, \cdot)$ est un groupe.

d. L'ensemble U est de cardinal fini égal à 36. D'après le théorème de Lagrange sur les groupes finis, si $\overline{x} \in U$, son ordre est un diviseur de 36, donc $O(x) \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

e. On remarque que $2^{18} = 2^{16} \cdot 2^2$. Alors $\overline{2^{16}} = (((\overline{2^2})^2)^2)^2 = ((\overline{4})^2)^2)^2 = (\overline{16^2})^2 = (\overline{256^2}) = \overline{-3^2} = \overline{9}$ et $(\overline{2^{18}}) = \overline{16} \cdot \overline{4} = \overline{36} = \overline{-1}$.

On a vérifié que $O(\overline{2}) \notin \{\{1, 2, 3, 4, 6, 9, 12, 18\}$ Donc $O(\overline{2}) = 36$.

f. $\overline{10^2} = \overline{100} = \overline{-11}$ et $\overline{10^3} = \overline{1}$. Donc $O(\overline{10}) = 3$.

3. **a.** On applique l'algorithme d'Euclide étendu pour déterminer des coefficients de Bézout u et v tels que $8u + 37v = 1$.

On trouve par exemple $14 * 8 - 3 * 37 = 1$ donc l'inverse de $\overline{8}$ est $\overline{14}$.

b. $\mathbb{Z}/37\mathbb{Z}$ est un corps donc intègre. Il suffit donc de factoriser le polynôme $X^3 + 1$ dans $\mathbb{Z}/37\mathbb{Z}$. (-1) est racine évidente. Par ailleurs, on a vu que $2^{18} \equiv -1$ donc $(2^6)^3 \equiv -1$ et $\overline{2^6} =\equiv 27$ est racine.

Donc $X^3 + 1 = (X + 1)(X^2 - X + 1) = (X + 1)(X - 27)(X + a)$. On cherche donc b tels que $X^2 - X + 1 = (X - 27)(X - b)$ dans $\mathbb{Z}/37\mathbb{Z}$, c'est à dire $27 + b \equiv 1$ et $27b \equiv 1$. Par exemple, $b = 11$.

Finalement, les racines de P sont $\overline{-1}, \overline{27}$ et $\overline{11}$.

4. **a.** Si $\overline{x} = \overline{x}^{-1}$, alors $x^2 = 1$ et $\overline{(x-1)(x+1)} = 0$. Comme $\mathbb{Z}/37\mathbb{Z}$ et intègre, $\overline{x} \in \{-1, 1\}$. Ces éléments conviennent effectivement.

b. Donc -1 et 1 sont les seuls éléments de $\mathbb{Z}/37\mathbb{Z}$ égaux à leur inverse.

De plus, $36! = 1 \times 2 \times 3 \times \ldots \times 36$. Dans le produit commutatif et associatif $2 \times 3 \times \ldots \times 35$, on peut rassembler les termes 2 par 2 en les associant avec leur inverse (distinct). Donc

$$36! \equiv 1 \times 2 \times 3 \times \ldots \times 36 \equiv 1 \times 36 \times 1 \equiv -1.$$

5. Voir le cours.

I- Définitions et propriétés usuelles

I-A Polynômes de première espèce

I-A-1 Les polynômes T_0, T_1, T_2 et T_3

- On a les relations $\forall \theta \in \mathbb{R}$, $T_0(\cos(\theta)) = 1$, $T_1(\cos(\theta)) = \cos(\theta)$, $T_2(\cos(\theta)) = 2\cos^2(\theta) - 1$ et $T_3(\cos(\theta)) = 4\cos^3(\theta) - 3\cos(\theta)$.

Donc par unicité, on obtient $T_1 = 1$, $T_2 = X$, $T_2 = 2X^2 - 1$ et $T_3 = 4X^3 - 3X$.

I-A-2 Expression de T_n

$\forall \theta \in \mathbb{R}, \forall n \in \mathbb{N}$, $e^{in\theta} = (\cos(\theta) + i\sin(\theta))^n = \sum\limits_{k=1}^{n} \binom{n}{k} \cos^{n-k}(\theta) i^k sin^k(\theta)$.

En prenant la partie réelle des deux membres, on obtient

$cos(n\theta) = \sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} (-1)^k cos^{n-2k}(\theta) sin^{2k}(\theta) = \sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} (-1)^k cos^{n-2k}(\theta)(1 - cos^2(\theta))^k$.

Et par unicité on aura $T_n = \sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} (-1)^k X^{n-2k} (1 - X^2)^k = \sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} X^{n-2k} (X^2 - 1)^k$.

I-A-3 Une relation de récurence entre les T_n

$\forall n \in \mathbb{N}$, $T_{n+2}(cos(\theta)) + T_n(cos(\theta)) = cos((n+2)\theta) + cos(n(\theta)) = 2cos((n+1)\theta)cos(\theta) = 2cos(\theta)T_{n+1}(cos(\theta))$.

Ce qui entraine par unicité $T_{n+2} + T_n = 2XT_{n+1}$.

Degré et coefficient dominant de T_n.

On va montrer par une récurrence forte sur n que $dom(T_n) = 2^{n-1}$ et $deg(T_n) = n$.

- La propriété est vrai pour $n = 0, 1, 2$ et 3.

- Supposons que pour un certain $n \geqslant 2$, $dom(T_n) = 2^{n-1}$, $dom(T_{n+1}) = 2^n$, et $deg(T_n) = n$, $deg(T_{n+1}) = n + 1$, alors, $deg(T_{n+2}) = deg(2XT_{n+1} - T_n) = deg(XT_{n+1}) = 1 + n + 1 = n + 2$. $dom(T_{n+2}) = dom(2XT_{n+1}) = 2dom(T_{n+1}) = 22^n = 2^{n+1}$.

Une méthode qui utilise l'expression de T_n.

On a $\forall n \in \mathbb{N}$, $T_n = \sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} X^{n-2k} (X^2 - 1)^k$.

On remarque que $\forall k \in [0, n/2]$, $n - 2k + 2k = n$, de plus le coefficient de X^n est $\sum\limits_{0 \leqslant k \leqslant n/2} \binom{n}{2k} = \frac{1}{2}(\sum\limits_{k=0}^{n} (1 + (-1)^k)\binom{n}{k}) = \frac{1}{2}\sum\limits_{k=0}^{n} \binom{n}{k} + \frac{1}{2}\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} = \frac{1}{2}(1+1)^n + \frac{1}{2}(1-1)^n = 2^{n-1}$.

En conclusion $deg(T_n) = n$ et $dom(T_n) = 2^{n-1}$.

I-A-4 Les racines de T_n

$\forall n \in \mathbb{N}^*$, $T_n(cos(\theta)) = 0 \iff cos(n\theta) = 0 \iff \theta = \dfrac{(2k+1)\pi}{2n}$, $k \in \mathbb{Z}$.

On a donc $\forall k \in [[0, n-1]]$, $T_n(cos(\theta_k)) = 0$ où $\theta_k = \dfrac{(2k+1)\pi}{2n}$, de plus $\forall k \in [[0, n-1]], \theta_k \in$

$]0,\pi[$ et la fonction cosinus est bijective de $]-1,1[$ vers $]0,\pi[$, donc T_n admet n racines distinctes sur $]-1,1[$, à savoir les $cos(\theta_k)$ où $k \in [[0, n-1]]$.

I-B **Polynômes de deuxième espèce**

I-B-1 **Expression de $U_n(cos(\theta))$**

- En dérivant l'expression $T_{n+1}(cos(\theta)) = cos((n+1)\theta)$ par rapport à la variable θ, on obtient $-sin(\theta)T'_{n+1}(cos(\theta)) = -(n+1)sin((n+1)\theta)$, ce qui entraine que
$\forall \theta \in \mathbb{R} \setminus \pi\mathbb{Z}$, $\forall n \in \mathbb{N}$, $\dfrac{T'_{n+1}(cos(\theta))}{n+1} = \dfrac{sin((n+1)\theta)}{sin(\theta)}$, c'est à dire $U_n(cos(\theta)) = \dfrac{sin((n+1)\theta)}{sin(\theta)}$.

I-B-2 .

a) **Une relation de récurence entre les U_n**

- $\forall n \in \mathbb{N}$, $U_{n+2}(cos(\theta)) + U_n(cos(\theta)) = \dfrac{1}{sin(\theta)}(sin((n+2)\theta) + sin(n\theta)) =$
$= \dfrac{2}{sin(\theta)}(cos(\theta)sin((n+1)\theta)) = 2cos(\theta)U_{n+1}(cos(\theta))$
ce qui donne par unicité des U_n que $U_{n+2} + U_n = 2XU_{n+1}$.

b) **Racines de U_n**

- Les racines de U_n sont celles de T'_{n+1}, or T_{n+1} admet $n+1$ racines distinctes sur $]-1,1[$, donc par application du théorème des accroissements finies entre deux zéros consécutifs de T_{n+1}, on obtient un zéro de T'_{n+1}, ce qui prouve que U_n admet n racines distinctes sur $]-1,1[$.
$\forall n \in \mathbb{N}$, $U_n(cos(\theta)) = 0 \iff sin((n+1)\theta) = 0 \iff (n+1)\theta = k\pi \quad , \quad k \in \mathbb{Z}$.
Donc $\forall k \in [[1, n]]$, $U_n(cos(\varphi_k)) = 0$ où $\varphi_k = \dfrac{k\pi}{n+1}$, les $cos(\varphi_k)$ sont distincts deux à deux grâce à la bijectivité de *cosinus* de $]-1,1[$ vers $]0,\pi[$.
Donc les racines de U_n sont les $cos(\varphi_k)$ où $k \in [[1, n]]$.

II- Arithmétique des polynômes de Tchebychev

II-A **Division euclidienne**

II-A-1 - $\forall m, n \in \mathbb{N}$ tel que $0 \leqslant m \leqslant n$, $cos((n+m)\theta) + cos((n-m)\theta) = 2cos(n\theta)cos(m\theta)$, donc
$T_{n+m}T_{n-m} = 2T_nT_m$.
$\forall n, m \in \mathbb{N}$ tel que $0 \leqslant m < n$, $sin((n+m-1)\theta) + sin((n-m-1)\theta) = 2cos(m\theta)sin((n-1)\theta)$, donc
$U_{n+m-1} + U_{n-m-1} = 2U_{n-1}T_m$.

II-A-2 a) - Si $m < n < 2m$, alors $0 < n-m < m$, donc d'après $(II-A-1)$, $T_mT_{n-m} = \dfrac{1}{2}(T_n + T_{2m-n})$, c'est à dire $T_n = 2T_{n-m}T_m - T_{2m-n} = 2T_{n-m}T_m - T_{|n-2m|}$ avec $0 < 2m - n < 2m - m = m = deg(T_m)$.
- Si $2m \leqslant n < 3m$, alors $m \leqslant n-m < 2m$, donc toujours d'après $(II-A-1)$,
$T_{n-m}T_m = \dfrac{1}{2}(T_n + T_{n-2m})$, c'est à dire $T_n = 2T_{n-m}T_m - T_{n-2m} = 2T_{n-m}T_m - T_{|n-2m|}$ avec $0 \leqslant n - 2m < 3m - 2m = m = deg(T_m)$.
On conclut que $Q_{n,m} = 2T_{n-m}$ et $R_{n,m} = -T_{|n-2m|}$.

b) - Soit $n = (2p+1)m$ où $p \in \mathbb{N}^*$, on applique l'égalité de $(II-A-1)$ au couple $(n,m) \longleftarrow (2km, m)$ où $k \in [[1,p]]$, on obtient $2T_{2km}T_m = T_{(2k+1)m} + T_{(2k-1)m}$, ce qui entraine que
$2(-1)^{p-k}T_{2km}T_m = (-1)^{p-k}T_{(2k+1)m} - (-1)^{p-k+1}T_{(2k-1)m}$, ce qui donne en sommant de

$k=1$ à $k=p$, on obtient par téléscopie

$T_n-(-1)^pT_m = T_{(2p+1)m}-(-1)^pT_m = \sum\limits_{k=1}^{p}\left((-1)^{p-k}T_{(2k+1)m}-(-1)^{p-k+1}T_{(2k-1)m}\right) = 2T_m\sum\limits_{k=1}^{p}(-1)^{p-k}T_{2km}$.

Donc $T_n = T_m\left((-1)^pT_m+2\sum\limits_{k=1}^{p}(-1)^{p-k}T_{2km}\right)$, donc

$Q_{n,m}=(-1)^pT_m+2\sum\limits_{k=1}^{p}(-1)^{p-k}T_{2km}$ et $R_{n,m}=0$.

c) - On considère l'ensemble $A_{n,m}=\{k\in\mathbb{N}^*\ /\ (2k-1)m<n\}$. Par hypothèse $n\neq(2(0)+1)m$, donc $1\in A_{n,m}$ de plus $A_{n,m}$ est majoré par $1+E\left(\dfrac{n/m+1}{2}\right)$, donc admet un maximum p.

$p\in A_{n,m}$ et $p+1\notin A_{n,m}$ donc $(2p-1)m<n\leqslant(2p+1)m$, or n n'est pas produit de m par un entier impair, donc $(2p-1)m<n<(2p+1)m$, c'est à dire $|n-2pm|<m$.

- $\forall k\in[[0,p-2]]$, $n-(2k+1)m\geqslant n-(2p-3)m\geqslant 2m>m$, donc

$\forall k\in[[0,p-2]]$, $2T_mT_{n-(2k+1)m}=T_{n-2km}+T_{n-(2k+2)m}$, donc

$2(-1)^kT_mT_{n-(2k+1)m}=(-1)^kT_{n-2km}-(-1)^{k+1}T_{n-(2k+2)m}$, ce qui donne par téléscopie en sommant de $k=0$ à $k=p-2$

$T_n=2T_m\sum\limits_{k=0}^{p-2}(-1)^kT_{n-(2k+1)m}+(-1)^{p-1}T_{n-(2p-2)m}$.

Or $m<n-(2p-2)m<3m$, donc d'après la question a),

$T_{n-(2p-2)m}=2T_mT_{n-(2p-1)m}-T_{|n-2pm|}$ et par suite

$T_n=2T_m\sum\limits_{k=0}^{p-1}(-1)^kT_{n-(2k+1)m}+(-1)^pT_{|n-2pm|}$, ce qui donne le résultats puisque $|n-2pm|<m=deg(T_m)$.

II-B **Plus grand commun diviseur**

II-B-1 **Pgcd de U_n et U_m**

- Posons $n+1=hn_1$ et $m+1=hm_1$.
- Soit r une racine de U_{h-1}, alors $\exists k\in[[0,h]]$ tel que $r=cos\left(\dfrac{k\pi}{h}\right)=cos\left(\dfrac{kn_1\pi}{n+1}\right)=cos\left(\dfrac{km_1\pi}{m+1}\right)$, donc r est une racine commune de U_n et de U_m.
- Réciproquement si r est une racine commune de U_n et de U_m, alors $\exists(k,k')\in[[1,n]]\times[[1,m]]$ tel que $r=cos\left(\dfrac{k\pi}{n+1}\right)=cos\left(\dfrac{k'\pi}{m+1}\right)$, donc $\dfrac{k\pi}{n+1}=\dfrac{k'\pi}{m+1}$ et par suite $km_1=k'n_1$, or n_1 et m_1 sont premiers entre eux, donc par le théorème de Gauss, n_1 divise k, ce qui entraine en posant $\dfrac{k}{n_1}=k''$ que $r=cos\left(\dfrac{k''\pi}{h}\right)$ c'est à dire que r est une racine de U_{h-1}.
- En conclut que U_{h-1} est le pgcd de U_n et U_m.

II-B-2 **Pgcd de T_n et T_m**

a) - Soit r une racine de T_g, alors $\exists k\in[[0,g-1]]$ tel que
$r=cos\left(\dfrac{(2k+1)\pi}{2g}\right)=cos\left(\dfrac{(2k+1)m_1\pi}{2m}\right)=cos\left(\dfrac{(2k+1)n_1\pi}{2n}\right)$, or $(2k+1)m_1$ et $(2k+1)n_1$ sont impairs, donc r est une racine commune de T_n et T_m.

- Réciproquement si r est une racine commune de T_n et T_m, alors $\exists(k,k')\in[[0,n-1]]\times[[0,m-1]]$ tel que $r=cos\left(\dfrac{(2k+1)\pi}{2n}\right)=cos\left(\dfrac{(2k'+1)\pi}{2m}\right)$, donc $\dfrac{(2k+1)\pi}{2n}=\dfrac{(2k'+1)\pi}{2m}$, c'est à dire

$(2k'+1)n_1=(2k+1)m_1$, or n_1 et m_1 sont premiers entre eux, donc n_1 divise $2k+1$ et par suite si on pose $\dfrac{2k+1}{n_1}=n_2$ qui est impair, on aura $r=cos\left(\dfrac{n_2\pi}{2g}\right)$ et l'imparité de n_2 entraine que r est une racine de T_g.

- On conclut que T_g est le pgcd de T_n et T_m.

b) - Soit r une racine commune de T_n et T_m, alors le raisonnement précédent aboutit à l'existence de k, k' tel que $(2k'+1)n_1 = (2k+1)m_1$, donc n_1 et m_1 sont de même parité, ce qui exige par hypothèse que n_1 et m_1 sont pairs, ce qui contredit qu'ils sont premiers entre eux.

- On conclut que T_n et T_m sont premiers entre eux.

c) • - Cas n, m impairs

- Cette condition exige que n_1 et m_1 sont impairs, donc d'après a), le pgcd de T_n et T_m est T_g où g est le pgcd de m et n.

• - Cas n, m des puissances de 2.

- Dans ce cas l'un des n_1 et m_1 est pair et l'autre vaut 1, donc d'après b) T_n et T_m sont premiers entre eux.

III- **Un théorème**

III-A **Préliminaires**

III-A-1 $(T_n)_n$ **est suite commutante**

- $deg(T_n) = n$.

- $\forall \theta \in \mathbb{R}, \forall n, m \in \mathbb{N}$, $T_n o T_m(cos(\theta)) = T_n(cos(m\theta)) = cos(nm\theta) = T_{nm}(cos(\theta))$, donc par unicité $T_n o T_m = T_{nm} = T_{mn} = T_m o T_n$.

III-A-2 G **est un groupe**

- $\forall P, Q \in G$, $deg(PoQ) = deg(P).deg(Q) = 1$, donc la loi o est une loi de composition interne qui est associative.

- $\forall P \in G$, $PoX = XoP = P$, donc X est l'élément neutre de G.

- L'inverse de $P = aX + b$ est $P^{-1} = \dfrac{x-b}{a} \in G$.

- On conclut que G est un groupe.

III-B **Commutant de X^2 et T_2**

III-B-1 Q **est unitaire**

Soit Q de degré $n \geqslant 1$ et de coefficient dominant $q \neq 0$, tel que $P_\alpha o Q = Q o P_\alpha$, alors en égalisant les coefficients dominants de ces deux membres, on obtient $q^2 = q$, donc $q = 1$.

III-B-2 **Commutant de X^2**

• - Soit Q_1 et Q_2 deux polynômes de degré $n \geqslant 1$ commutant avec P_α, alors d'après la question précédente, ils sont unitaires, donc si in pose $R = Q_1 - Q_2$, on aura $deg(R) < n$.

- $RoP_\alpha = Q_1 o P_\alpha - Q_2 o P_\alpha = P_\alpha o Q_1 - P_\alpha o Q_2 = Q_1^2 - Q_2^2 = (Q_1 - Q_2)(Q_1 + Q_2) = R(Q_1 + Q_2)$, ce qui donne par passage aux degrés que

$2deg(R) = deg(RoP_\alpha) = deg(R(Q_1 + Q_2)) = deg(R) + n$, donc $deg(R) = n$, ce qui est contradictoire avec $deg(R) < n$.

• - $\forall n \in \mathbb{N}^*$, X^n commute avec X^2 et c'est l'unique polynôme de degré n.

- Si $P = \lambda$ est un polynôme constant qui commute avec X^2, alors $\lambda^2 = X^2 o P = P o X^2 = \lambda$, donc $\lambda \in \{0, 1\}$.

- En conclut que $\mathcal{C}(X^2) = \{0\} \cup \{X^n \ \ / \ \ n \in \mathbb{N}\}$.

III-B-3 **Existence de U et α**

- Soit $P = aX^2 + bX + c$ et $U = \gamma X + \beta$ avec $a \neq 0$ et $\gamma \neq 0$.

- $UoP = P_\alpha o U \iff \gamma(aX^2 + bX + c) + \beta = (\gamma X + \beta)^2 + \alpha$, ce qui aboutit à un système qui

admet une unique solution à savoir $U = aX + \dfrac{b}{2}$ et $P_\alpha = X^2 + \dfrac{4ac + 2b - b^2}{4}$.
- Le cas $P = T_2 = 2X^2 - 1$, donne $U = 2X$ et $P_\alpha = X^2 - 2$.

III-B-4 **Commutant de** T_2

- Soit Q de degré $n \geqslant 1$.

La question précédente entraine que $UoT_2oU^{-1} = P_{-2}$, donc
$Q \in \mathcal{C}(T_2) \iff QoT_2 = T_2oQ \iff UoQoU^{-1}oP_{-2} = P_{-2}oUoQoU^{-1} \iff UoQoU^{-1} \in \mathcal{C}(P_{-2})$.
- D'après la question $(II - B - 2)$, P_{-2} admet au plus un commutant de degré $n \geqslant 1$, or $\forall n \geqslant 1$, T_n commute avec T_2, donc UoT_noU^{-1} commute avec P_{-2} par unicité c'est le seul de degré $n \geqslant 1$, donc $Q = T_n$.
- De plus si $P = \lambda$ commute avec T_2, alors $\lambda = 2\lambda^2 - 1$, ce qui exige que $\lambda \in \{-\dfrac{1}{2}, 1\}$.
- En conclusion $\mathcal{C}(T_2) = \{-\dfrac{1}{2}\} \cup \{T_n \ / \ n \in \mathbb{N}\}$.