Arithmétique et groupes 12 janvier 2023
L3 Parcours Mathématiques pour l'enseignement Contrôle Terminal
Université Claude Bernard (Lyon 1) Durée : **2 heures**

Corrigé du CT1

I (7 points)

1. Comme $\alpha+\beta=1$ et $\alpha\beta=-1$, pour tout $n\in\mathbb{N}$, on a
$$L_{n+2}-L_{n+1}=\alpha^{n+1}(\alpha-1)+\beta^{n+1}(\beta-1)=(-\alpha\beta)\alpha^n+(-\alpha\beta)\beta^n=L_n.$$
2. Par la relation de récurrence ci-dessus, on obtient $L_0=1+1=2$, $L_1=\alpha+\beta=1$ et déduit que $L_n\in\mathbb{N}^*$ par rcurrence.
3. Comme $\alpha\beta=-1$, $L_2=L_0+L_1=3$, $L_3=L_1+L_2=4$, $L_4=L_2+L_3=7$ et $L_5=L_3+L_4=11$, on a
$$(1-\alpha^5x^5)(1-\beta^5X^5)=1-(\alpha^5+\beta^5)X^5+(\alpha\beta)^5X^{10}=1-11X^5-X^{10}.$$
4. De même on a $P(X)=-(\alpha\beta)^5(X^5-\alpha^{-5})(X^5-\beta^{-5})=(X^5+\alpha^5)(X^5+\beta^5)$. On rappelle que $X^5-1=\prod_{k=0}^4(X-\xi^k)$ avec $\xi=e^{2\pi i/5}$. D'où, les factorisations en produit de polynômes unitaires et irréductibles dans $\mathbb{C}[X]$:
$$P(X)=\prod_{k=0}^4(X+\alpha\xi^k)(X+\beta\xi^k)$$
et dans $\mathbb{R}[X]$:
$$\begin{aligned}P(X)=(X+\alpha)(X+\beta)(X^2+2\alpha\cos\frac{2\pi}{5}X+\alpha^2)(X^2+2\alpha\cos\frac{4\pi}{5}X+\alpha^2)\\ \times(X^2+2\beta\cos\frac{2\pi}{5}X+\beta^2)(X^2+2\beta\cos\frac{4\pi}{5}X+\beta^2).\end{aligned}$$

II (7 points)

Soit n un entier ≥ 3. On note A_n le sous-groupe de S_n formé par les permutations paires.

a) Soient $\alpha=(i,j)$ et $\beta=(k,l)$ deux transpositions distinctes. Si elles ne sont pas disjointes, disons $k=j$, alors $(i,j)(j,l)=(l,i,j)$, sinon, on a $(i,j)(l,k)=(l,j,i)(l,k,i)$.

b) Par définition, chaque permutation dans A_n est un produit d'un nombre pair de transpositions, on déduit de a) qu'elle peut s'écrire comme un produit de 3-cycles.

c) Si i,j,k sont deux à deux distincts et ≥ 3, on a
$$\begin{aligned}(1\,2\,i)\,(2\,j\,k)\,(1\,2\,i)^{-1}&=(12i)(2jk)(21i)=(ijk);\\ (1\,2\,j)\,(1\,2\,k)\,(1\,2\,j)^{-1}&=(12j)(12k)(21j)=(2jk).\end{aligned}$$

d) D'après b) et c) le group A_n est engendré par les 3-cycles dans la liste :
$$(123),(124),\ldots,(12n)$$
et leurs inverses. D'où le résultat.

III (10 points)

1. Si $a \equiv 0 \pmod 2$, alors il existe un $m \in \mathbb{N}$ tel que $a^2 = (2m)^2 \equiv 0 \pmod 4$, si $a \equiv 1 \pmod 2$, alors il existe un $m \in \mathbb{N}$ tel que $a^2 = (2m+1)^2 \equiv 1 \pmod 4$.
2. Soit $d = \text{pgcd}(x_0, y_0, z_0)$ et u,v,w des entiers tels que $x_0 = du$, $y_0 = dv$ et $z_0 = dw$. Comme $d \geq 1$, il est clair que $(du)^2 = (dv)^2 + (dw)^2$ implique que $u^2 = v^2 + w^2$. Soit $\text{pgcd}(u,v,w) = \delta$, qui est ≥ 1. Alors δd est un diviseur de d, ce qui implique que $\delta = 1$.
3. Supposons le contraire, disons que u et v sont pairs, alors $w^2 = u^2 - v^2$ est un multiple de 4 et puis w est pair. Ce qui contredit le point 2. De même, on montre que u et w (ou v et w) ne peuvent pas être pairs.
4. Si v et w sont impairs, alors $v^2 \equiv w^2 \equiv 1 \pmod 4$, ce qui implique que $u^2 \equiv 2 \pmod 4$. C'est impossible d'après le point 1.
   (*On montre de même que si* $\text{pgcd}(u,v,w) = 1$*, alors* u,v *et* w *sont deux à deux premiers entre eux.*)
5. On note $\delta = \text{pgcd}(u - v, u + v)$. Comme u et v sont impairs, $u + v$ et $u - v$ sont tous pairs, on pose $\delta = 2\delta'$. Soient $u + v = \delta\alpha$ et $u - v = \delta\beta$, où α et β sont des nombres naturels premiers entre eux.
   i) On a $u = \delta'(\alpha + \beta)$ et $v = \delta'(\alpha - \beta)$.
   ii) De $u + v = 2\delta'\alpha$ et $u - v = 2\delta'\beta$, on déduit $u^2 - v^2 = 4\delta'^2\alpha\beta = 4w^2$, et puis $w^2 = \delta'^2\alpha\beta \Longrightarrow \delta'^2 | w^2 \Longrightarrow \delta' | w$. D'où $\delta' = 1$ car $\text{pgcd}(u,v,w) = 1$. Ceci montre que $\text{pgcd}(u - v, u + v) = 2$.
   Chaque diviseur premier de $w^2 = \alpha\beta$ ne peut diviser à la fois α et β ; comme w^2 est un carré, l'exposant de ce diviseur premier est pair dans celui des deux nombres où ce diviseur premier figure. Il résulte que α et β sont effectivement des carrés d'entiers naturels, puisque chacun de leurs diviseurs premiers a un exposant pair. On a donc $\alpha = m^2$ et $\beta = n^2$ avec m et n premiers entres eux. Il s'en suit que

$$u + v = 2m^2, \quad u - v = 2n^2, \quad w = 2mn$$

   avec m et n premiers entre eux.
6. On vérifie que les triplets (x,y,z), où

$$x = m^2 + 1, \quad y = m^2 - 1, \quad z = 2m \quad (m \geq 2),$$

   vérifient $x^2 = y^2 + z^2$ et $\text{pgcd}(x, y, z) = 1$.
