



G

O

D

O

O

O

O

D

Exercice 1

$$E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$u := (1\ 2\ 3) \circ (4\ 5\ 6) \circ (7\ 8\ 9)$$

$$v := (4\ 5\ 6) \circ (7\ 8\ 9)$$

$$w := (1\ 4\ 7) \circ (2\ 5\ 8) \circ (3\ 6\ 9)$$

(a) Soit $1 \leq a_1 < a_2 < a_3 \leq 9$
et $\sigma = (a_1 \rightarrow a_2 \rightarrow a_3)$

Méthode 1

$$\sigma(\sigma) = 3 \quad \text{et} \quad \sigma^{\circ(\sigma)} = \text{Id} \quad \Rightarrow \quad \sigma^3 = \text{Id}$$

Méthode 2

$$\sigma \circ \sigma \circ \sigma =$$

$$\begin{pmatrix} a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow a_1 \\ a_2 \rightarrow a_3 \rightarrow a_1 \rightarrow a_2 \\ a_3 \rightarrow a_1 \rightarrow a_2 \rightarrow a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \end{pmatrix} = \text{Id}$$

b) (d'après (a)) $\sigma^{-1} (\sigma \circ \sigma^2 = \text{Id})$

$$\Rightarrow \underline{\underline{\sigma^2 = \sigma^{-1}}}$$

c) Or u, v, w sont composées de cycles à supports disjoints, donc ils commutent

$$\begin{aligned} \text{Alors } u^3 &= u \circ u^2 = (1\ 2\ 3)^3 \circ (4\ 5\ 6)^3 \circ (7\ 8\ 9)^3 \\ &= (1\ 2\ 3)(1\ 2\ 3)^2 \circ (4\ 5\ 6)(4\ 5\ 6)^2 \circ (7\ 8\ 9)(7\ 8\ 9)^2 \\ \text{(d'après (b))} &= (1\ 2\ 3)(1\ 2\ 3)^{-1} \circ (4\ 5\ 6)(4\ 5\ 6)^{-1} \circ (7\ 8\ 9)(7\ 8\ 9)^{-1} \\ &= \text{Id} \circ \text{Id} \circ \text{Id} = \text{Id} \end{aligned}$$

Idem avec v et w
d'où $u^3 = \text{Id} = v^3 = w^3$

Autre méthode

$$o(u) = \text{ppcm}(o((1\ 2\ 3)), o((4\ 5\ 6)), o((7\ 8\ 9))) = \\ = \text{ppcm}(3, 3, 3) = 3$$

le plus $u^{o(u)} = \text{Id} = u^3$ comme $\underline{o(u) = 3}$

d) (d'après (b))

$$w^{-1} = w^2 = \begin{pmatrix} 1 & 4 & 7 \\ 7 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 & 8 \\ 8 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 6 & 9 \\ 9 & 3 & 6 \end{pmatrix}$$

wordow⁻¹

$$\begin{pmatrix} 1 \rightarrow 7 \rightarrow 8 \rightarrow 2 \\ 2 \rightarrow 8 \rightarrow 9 \rightarrow 3 \\ 3 \rightarrow 9 \rightarrow 7 \rightarrow 1 \\ 4 \rightarrow 1 \rightarrow 1 \rightarrow 4 \\ 5 \rightarrow 2 \rightarrow 2 \rightarrow 5 \\ 6 \rightarrow 3 \rightarrow 3 \rightarrow 6 \\ 7 \rightarrow 4 \rightarrow 5 \rightarrow 8 \\ 8 \rightarrow 5 \rightarrow 6 \rightarrow 9 \\ 9 \rightarrow 6 \rightarrow 4 \rightarrow 7 \end{pmatrix} = \begin{pmatrix} 1 \rightarrow 2 \rightarrow 3 \end{pmatrix} \circ \begin{pmatrix} 4 \rightarrow 4 \end{pmatrix} \circ \begin{pmatrix} 5 \rightarrow 5 \end{pmatrix} \circ \begin{pmatrix} 6 \rightarrow 6 \end{pmatrix} \\ \circ \begin{pmatrix} 7 \rightarrow 8 \rightarrow 9 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3 \end{pmatrix} \circ \begin{pmatrix} 7\ 8\ 9 \end{pmatrix}$$

$\underbrace{\hspace{10em}}_{w^{-1}} \quad \underbrace{\hspace{10em}}_w$
 $\underbrace{\hspace{10em}}_v$

e) $w^{-1} = w^2 = \begin{pmatrix} 1 & 4 & 7 \\ 7 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 & 8 \\ 8 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 6 & 9 \\ 9 & 3 & 6 \end{pmatrix}$

$$w^{-1} \circ v \circ w = \begin{pmatrix} 1 \rightarrow 4 \rightarrow 5 \rightarrow 2 \\ 2 \rightarrow 5 \rightarrow 6 \rightarrow 3 \\ 3 \rightarrow 6 \rightarrow 7 \rightarrow 1 \\ 4 \rightarrow 7 \rightarrow 8 \rightarrow 4 \\ 5 \rightarrow 8 \rightarrow 9 \rightarrow 5 \\ 6 \rightarrow 9 \rightarrow 7 \rightarrow 6 \\ 7 \rightarrow 1 \rightarrow 1 \rightarrow 7 \\ 8 \rightarrow 2 \rightarrow 2 \rightarrow 8 \\ 9 \rightarrow 3 \rightarrow 3 \rightarrow 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 5 & 6 & 4 & 9 & 8 & 7 \end{pmatrix} \\ = \begin{pmatrix} 1\ 2\ 3 \end{pmatrix} \circ \begin{pmatrix} 4\ 5\ 6 \end{pmatrix}$$

$\underbrace{\hspace{10em}}_w \quad \underbrace{\hspace{10em}}_v \quad \underbrace{\hspace{10em}}_{w^{-1}}$

$$f) (w \circ v \circ w^{-1}) \circ (w^{-1} \circ v \circ w) = w \circ v \circ w^{-2} \circ v \circ w$$

$$= (1 \ 2 \ 3) \circ (7 \ 8 \ 9) \circ (1 \ 2 \ 3) \circ (4 \ 5 \ 6)$$

$$= (1 \ 2 \ 3)^2 \circ (4 \ 5 \ 6) \circ (7 \ 8 \ 9)$$

$$u^2 \circ v^{-1} = (1 \ 2 \ 3)^2 \circ (4 \ 5 \ 6)^2 \circ (7 \ 8 \ 9)^2 \circ (7 \ 8 \ 9)^{-1} \circ (4 \ 5 \ 6)^{-1}$$

$$= (1 \ 2 \ 3)^2 \circ (4 \ 5 \ 6) \circ (7 \ 8 \ 9)$$

$$\text{d'où } u^2 \circ v^{-1} = w \circ v \circ w^{-2} \circ v \circ w$$

$$(w \circ v)^2 \circ w = w \circ v \circ w \circ w \circ w$$

$$w^{-2} = (w^2)^{-1} = (w^{-1})^{-1} = w$$

$$\text{car } w^2 = w^{-1} \text{ (d'après } \beta)$$

$$\text{d'où } \underline{\underline{(w \circ v)^2 \circ w = w \circ v \circ w^{-2} \circ w \circ w}}$$

$$g) u^2 \circ v^{-1} = (w \circ v)^2 \circ w = w \circ v \circ w^{-2} \circ w \circ w$$

$$u^2 \circ v^{-1} \circ v = (w \circ v)^2 \circ w \circ v$$

$$= u^2 = (w \circ v)^3 \quad \text{car } u^{-2} = (u^2)^{-1} = ((w \circ v)^3)^{-1} \\ = (w \circ v)^{-3} = u$$

$$\text{mais } u^2 = u^{-1} \quad \text{d'où } u^{-2} = (u^2)^{-1} = (u^{-1})^{-1} = u$$

$$\text{donc } u = (w \circ v)^{-3}$$

Exercice 4

Soit $N \geq 1$ et S_N le groupe de permutations de $E = \{1, 2, \dots, N\}$

Soit $\sigma \in S_N$ cycle avec $d(\sigma) = n$ où $2 \leq n \leq N$

$$m \geq 1 \quad \tau = \sigma^m$$

(a)

(a) On peut étudier le cas où $N = n$ car
 si $N > n$ alors
 $\sigma = (1 \dots n)$ et $E = \{1, 2, \dots, n, n+1, \dots, N\}$
 où $n+1, \dots, N$ sont points fixes et ne sont pas
 affectés par σ donc on peut décomposer σ en cycles
 et $n+1, \dots, N$ ne seront pas affectés
 De plus on peut étudier le cas $\sigma = (1 \dots n)$
 et puis utiliser les conjugaisons pour changer
 les coordonnées.

b) Soit $n \geq 2$ et $\sigma = (1 \dots n) \in S_n$
 $\Rightarrow \sigma(i) = i+1 \pmod n$
 $m = d m'$ $n = d n'$ où $d = \text{pgcd}(m, n)$ $m' \wedge n' = 1$

$$\begin{aligned} \sigma^m(i) &= \sigma^m(i) = \sigma^{m-1}(\sigma(i)) = \sigma^{m-1}(i+1) = \sigma^{m-2}(\sigma(i+1)) = \sigma^{m-2}(i+2) \\ \text{d'où } \sigma^m(i) &= i+m \\ \sigma^{lm}(i) &= \sigma^{lm}(i) = i+lm \end{aligned}$$

D'où $\text{Orb}_\sigma(i) = \{i, i+m, i+2m, \dots, i+(q-1)m\}$ avec tous les éléments
 distincts.
 avec un nombre q à déterminer

D'après le cours $q = \min \{l \in \mathbb{Z} : \sigma^l(i) = i\}$
 Soit $j \in E$, d'après le cours $\text{Orb}_\sigma(i) = \text{Orb}_\sigma(j)$ ou bien
 $\text{Orb}_\sigma(i) \cap \text{Orb}_\sigma(j) = \emptyset$

$$\begin{aligned} \text{On cherche } q \text{ tq } i+qm &\equiv i \pmod n \\ \Leftrightarrow qm &\equiv 0 \pmod n \end{aligned}$$

$$\begin{aligned} d n' \mid q d m' &\text{ car } d n' \mid q d m' \text{ car } m' \wedge n' = 1 \\ \Leftrightarrow n' \mid q m' &\Rightarrow n' \mid q \text{ car } m' \wedge n' = 1 \\ \Rightarrow q &= \frac{n}{d} = n' \end{aligned}$$

$$\text{d'où } q = \frac{n}{\text{pgcd}(n, m)} = n'$$

donc $\text{Orb}_\sigma(i)$ est constitué de n' éléments distincts.

c) Soient $1 \leq i, j \leq n$
et

$$Orb_G(i) = \{i, i+m, \dots, i+(n'-1)m\}$$

$$Orb_G(j) = \{j, j+m, \dots, j+(n'-1)m\}$$

D'après le cours $Orb_G(i) = Orb_G(j)$ ou bien
 $Orb_G(i) \cap Orb_G(j) = \emptyset$

Supposons que $Orb_G(i) = Orb_G(j)$

alors $j \in Orb_G(i) = \{i, i+m, i+2m, \dots, i+(n'-1)m\}$

$$\Rightarrow j = i + qm \quad \text{avec } 0 \leq q \leq n'-1$$

$$i + qm = i + qdm' \equiv i \pmod{d} \quad \text{car } qdm' \equiv 0 \pmod{d}$$

$$Orb_G(j) = i + qm \quad \text{et } i + qm \equiv i \pmod{d}$$

donc $i \equiv j \pmod{d}$.

d) Dans (c) on a montré que $Orb_G(i) = Orb_G(j) \Rightarrow i \equiv j \pmod{d}$
alors si $i \not\equiv j \pmod{d}$ donc $Orb_G(i) \neq Orb_G(j)$
 $\Rightarrow Orb_G(i) \cap Orb_G(j) = \emptyset$

$\forall 1 \leq k \neq l \leq d$ $k \not\equiv l \pmod{d}$ ce qui implique
 $Orb_G(k) \cap Orb_G(l) = \emptyset$

D'où la réunion $Orb_G(1) \cup \dots \cup Orb_G(d)$ est disjointe

De plus $1 \in Orb_G(1)$, $2 \in Orb_G(2)$, ..., $d \in Orb_G(d)$

$$d+1 \in Orb_G(1) \text{ car } d+1 \equiv 1 \pmod{d}$$

$$n = dn' \equiv 0 \pmod{d} \text{ donc } n \in Orb_G(d)$$

donc tout nombre entre 1 et n appartient
à l'une des orbites $Orb_G(1)$, ..., $Orb_G(d)$

$$\text{D'où } Orb_G(1) \cup \dots \cup Orb_G(d) = \{1, \dots, n\}$$

e) Soit $\sigma \in S_N$ n cycle avec $n \geq 2$ et $m \geq 1$ Soit $\gamma = \sigma^m$

• Supposons que $m|n \Rightarrow d = \text{pgcd}(m, n) = m$

d'après (b) $\forall i$ $\text{Orb}_\gamma(i)$ est de longueur $\frac{n}{\text{pgcd}(m, n)} = \frac{n}{m}$

D'après (d) $\{1, \dots, n\} = \underbrace{\text{Orb}_\gamma(1) \cup \dots \cup \text{Orb}_\gamma(d)}_{d \text{ orbites}}$

mais $d = m$, donc $\gamma = \sigma^m$ se décompose en m cycles de longueur $\frac{n}{m}$

• Supposons $m \wedge n = 1$, d'après (b) $\text{Orb}_\gamma(i)$ est de longueur $\frac{n}{\text{pgcd}(m, n)} = \frac{n}{1} = n$

D'après (d) $\{1, \dots, n\} = \text{Orb}_\gamma(1) \cup \dots \cup \text{Orb}_\gamma(d)$ mais $d = 1$, donc $\{1, \dots, n\} = \text{Orb}_\gamma(1)$ de longueur n .

(f) Oui, car d'après le cours on peut utiliser les conjugaisons pour changer des coordonnées de $\sigma \in S(E)$ en format $(1, \dots, n)$ et puis les retourner au format initial.

(g) $\sigma \in S_{25}$ de type $(12, 8, 6, 1)$

Alors les longueurs n sont

	n	12	8	6	1
les nombre de cycles	$\text{pgcd}(4, n)$	4	4	2	1
longeurs de cycles		3	2	3	1

Alors le type de σ^4 est :

$(3, 3, 3, 3, 2, 2, 2, 2, 3, 3, 1)$

2
.

Exercice 2

(a) Déterminer le reste de la division euclidienne de $X^{36} - X^{25}$ par $X^2 + 1$

Soit $Q(X)$, on veut calculer $R(X)$ tq
$$X^{36} - X^{25} = (X^2 + 1)Q(X) + R(X)$$

Calculons $X^{36} - X^{25} \text{ mod } X^2 + 1$

$$X^2 \equiv -1 \text{ mod } X^2 + 1$$

$$X^{36} = (X^2)^{18} \equiv (-1)^{18} \equiv 1 \text{ mod } X^2 + 1$$

$$X^{25} = X^{24} X = (X^2)^{12} X \equiv (-1)^{12} X \equiv X \text{ mod } X^2 + 1$$

$$\text{d'où } X^{36} - X^{25} \equiv 1 - X \text{ mod } X^2 + 1$$

D'où le reste est: $1 - X = -(X - 1)$

b) Déterminer $n \geq 1$ tq

$$X^3 - X^2 + X - 1 \mid (X^2 - X + 1)^n - X^{2n} + X^n - 1$$

$$X^3 - X^2 + X - 1 = (X^2 + 1)(X - 1)$$

$$(X^2 + 1) \mid (X - 1) = X^3 - X^2 + X - 1$$

Alors les racines de $X^3 - X^2 + X - 1$
sont: $1, i, -i$

$$\text{Notons } P(X) = X^3 - X^2 + X - 1$$

$$\text{et } Q(X) = (X^2 - X + 1)^n - X^{2n} + X^n - 1$$

$P(X) \mid Q(X)$ si $Q(X) = 0$ pour toute racine de $P(X)$

$$\begin{aligned}
 Q(1) &= (1^2 - 1 + 1)^n - (1)^{2n} + 1^n - 1 \\
 &= 1^n - (1)^{2n} + 1^n - 1 \\
 &= 2 - 2 = 0
 \end{aligned}$$

Donc $Q(1) = 0 \quad \forall n$

$$\begin{aligned}
 Q(i) &= (i^2 - i + 1)^n - (i^2)^n + i^n - 1 \\
 &= (-1 - i + 1)^n - (-1)^n + i^n - 1 \\
 &= (-i)^n - (-1)^n + i^n - 1 = (-i)^n + (i)^n - ((-1)^n + 1)
 \end{aligned}$$

$$\begin{aligned}
 \text{Si } n = 2n' \quad (-1)^{n'} - 1 + (-1)^{n'} - 1 &= i^{2n'} + (-i)^{2n'} - ((-1)^{2n'} + 1) \\
 = 1 - 1 + 1 - 1 = 0 &= 0 \quad \text{si } n = 2n' + 1
 \end{aligned}$$

$Q(i) = 0$ si $4 | n$ ou $n = 4n'$

$$\begin{aligned}
 Q(-i) &= ((-i)^2 + i + 1)^n - ((-i)^2)^n + (-i)^n - 1 \\
 &= i^n - (-1)^n + (-i)^n - 1 \\
 &= i^n + (-i)^n - (-1)^n - 1 \\
 &= i^n(1 + (-1)^n) - ((-1)^n + 1) = 0 \quad \text{si } n \text{ est impair}
 \end{aligned}$$

Alors $P(X) \mid Q(X) \quad \forall n \in \mathbb{N}$ tq $4 | n$ ou n est impair.

Sol. TD

$$(x^2 - x + 1)^n - x^{2n} + x^n - 1 = Q_n$$

$$\begin{aligned}
 P \mid Q_n &\Leftrightarrow x-1 \mid Q_n \\
 &\quad \text{et} \\
 &\quad x^2+1 \mid Q_n
 \end{aligned}$$

$$\text{car } (x-1) \wedge (x^2+1) = 1$$

$$Q_n(1) = 1^n - 1^{2n} + 1^n - 1 = 1 - 1 + 1 - 1 = 0 \quad \forall n \in \mathbb{N}^*$$

$$\begin{aligned}
 Q_n &\equiv (-1-x+1)^{2n} - (-1)^n + x^n - 1 \quad [x^2+1] \\
 &\equiv (-x)^{2n} - (-1)^n + x^n - 1 \quad [x^2+1] \\
 &\equiv x^{2n}(1+(-1)^n) - (1+(-1)^n) \quad [x^2+1] \\
 &\equiv (x^{2n}-1)(1+(-1)^n) \quad [x^2+1]
 \end{aligned}$$

si n impair $Q_n \equiv 0 \quad [x^2+1]$ donc $P \mid Q_n$

si n pair $\exists n' \in \mathbb{N}$ tq $n = 2n'$

$$\begin{aligned}
 Q_n &\equiv 2(x^{2n'} - 1) \quad [x^2+1] \\
 &\equiv 2((-1)^{n'} - 1) \quad [x^2+1]
 \end{aligned}$$

si n' pair $\exists n'' \in \mathbb{N}$ tq $n' = 2n''$, $Q_n \equiv 0 \quad [x^2+1]$ donc $P \mid Q_n$

si n' impair $Q_n \equiv -4 \quad [x^2+1]$ donc $P \nmid Q_n$

finalment, $P \mid Q_n$ car n impair ou $4 | n$.

Exercice 3

Soit $\mathbb{Q}[X]$ et 3 polynômes:

$$\mathcal{D} := x^2 + 2x + 5$$

$$\mathcal{Q} := x^5 + x^4 + 4x^3 - 4x^2 + 3x - 5$$

$$\mathcal{P} := x^6 + 4x^5 + 12x^4 + 15x^3 + 17x^2 + 3x + 20$$

$$\begin{array}{r|l} a) & x^5 + x^4 + 4x^3 - 4x^2 + 3x - 5 \\ & - x^5 + 2x^4 + 5x^3 \\ \hline & -x^4 - x^3 - 4x^2 + 3x - 5 \\ & - x^4 - 2x^3 - 5x^2 \\ \hline & x^3 + x^2 + 3x - 5 \\ & - x^3 + 2x^2 + 5x \\ \hline & -x^2 - 2x - 5 \\ & - x^2 - 2x - 5 \\ \hline & 0 \end{array}$$

Vérification des calculs: $(x^3 - x^2 + x - 1)(x^2 + 2x + 5) =$

$$\begin{aligned} &= x^5 - x^4 + x^3 - x^2 \\ &\quad + 2x^4 - 2x^3 + 2x^2 - 2x \\ &\quad + 5x^3 - 5x^2 + 5x - 5 \\ &= x^5 + x^4 + 4x^3 - 4x^2 + 3x - 5 \end{aligned}$$

D'où $\mathcal{Q} : \mathcal{D} = x^3 - x^2 + x - 1$

$$\begin{array}{r|l} b) & x^6 + 4x^5 + 12x^4 + 15x^3 + 17x^2 + 3x + 20 \\ & - x^6 + 2x^5 + 5x^4 \\ \hline & 2x^5 + 7x^4 + 15x^3 + 17x^2 + 3x + 20 \\ & - 2x^5 + 4x^4 + 10x^3 \\ \hline & 3x^4 + 5x^3 + 17x^2 + 3x + 20 \\ & - 3x^4 + 6x^3 + 15x^2 \\ \hline & -x^3 + 2x^2 + 3x + 20 \\ & - x^3 - 2x^2 - 5x \\ \hline & 4x^2 + 8x + 20 \\ & - 4x^2 + 8x + 20 \\ \hline & 0 \end{array}$$

$\mathcal{P} : \mathcal{D} = x^4 + 2x^3 + 3x^2 - x + 4$

Soit $A = x^4 + 2x^3 + 3x^2 - x + 4$ et $B = x^3 - x^2 + x - 1$

$$\begin{array}{r|l}
 c) \quad x^4 + 2x^3 + 3x^2 - x + 4 & x^3 - x^2 + x - 1 \\
 \underline{-x^4 - 2x^3 + x^2 - 2} & x + 3 \\
 3x^3 + 2x^2 + 4 & \\
 \underline{3x^3 - 3x^2 + 3x - 3} & \\
 5x^2 - 3x + 7 &
 \end{array}$$

$$\begin{array}{r|l}
 x^3 - x^2 + x - 1 & 5x^2 - 3x + 7 \\
 \underline{x^3 - \frac{2}{5}x^2 + \frac{7}{5}x} & \frac{1}{5}x + \frac{-2}{25} \\
 -\frac{2}{5}x^2 - \frac{2}{5}x - 1 & \\
 \underline{-\frac{2}{5}x^2 + \frac{6}{25}x - \frac{4}{25}} & \\
 -\frac{16}{25}x - \frac{11}{25} &
 \end{array}$$

$$\begin{array}{r|l}
 5x^2 - 3x + 7 & -\frac{16}{25}x - \frac{11}{25} \\
 \underline{5x^2 + \frac{55}{16}x} & -\frac{125}{16}x + \frac{2575}{256} \\
 -\frac{103}{16}x + 7 & \\
 \underline{-\frac{103}{16}x - \frac{1191}{256}} & \\
 \frac{2925}{256} &
 \end{array}$$

$$\begin{array}{r|l}
 -\frac{16}{25}x - \frac{11}{25} & \frac{2925}{256} \\
 \underline{-\frac{16}{25}x} & -\frac{4036}{73125}x - \frac{2816}{73125} \\
 -\frac{11}{25} & \\
 \underline{-\frac{11}{25}} & \\
 0 &
 \end{array}$$

Où $\frac{2925}{256}$ est le dernier reste non nul en divisant A par B
 donc $\text{pgcd}(A, B) = \frac{2925}{256}$

d) $\text{pgcd}(P, Q)$

$$Q = D \cdot B \text{ d'après (a)}$$

$$P = D \cdot A \text{ d'après (b)}$$

$$\text{pgcd}(P, Q) = \text{pgcd}(D \cdot B, D \cdot A) = D \text{pgcd}(B, A) = D \text{ d'après (c)}$$

On multiplie par une constante et on obtient $\text{pgcd}(A, B) = 1$

$$\text{D'où } \text{pgcd}(P, Q) = D$$

Exercice 5

$$B(x) := \frac{(x^2-1)^2}{x(x^2+1)^3}$$

a) Le dénominateur est sous forme décomposée en facteurs irréductibles, de plus le degré de dénominateur est supérieur à celui de numérateur, donc le théorème du cours s'applique :

$$B(x) = \frac{a}{x} + \frac{bx+c}{(x^2+1)^3} + \frac{b'x+c'}{(x^2+1)^2} + \frac{b''x+c''}{x^2+1}$$

où $a, b, c, b', c', b'', c''$ sont des inconnues à déterminer.

b)

$$B(-x) = -\frac{(x^2-1)^2}{x(x^2+1)^3} = -B(x)$$

$$\text{Alors } B(-x) + B(x) = 0$$

$$\Rightarrow -\frac{a}{x} + \frac{-bx+c}{(x^2+1)^3} + \frac{-b'x+c'}{(x^2+1)^2} + \frac{-b''x+c''}{x^2+1} + \frac{a}{x} + \frac{bx+c}{(x^2+1)^3} + \frac{b'x+c'}{(x^2+1)^2} + \frac{b''x+c''}{x^2+1} = 0$$

$$\frac{2c}{(x^2+1)^3} + \frac{2c'}{(x^2+1)^2} + \frac{2c''}{x^2+1} = 0$$

$$\Rightarrow \frac{c}{(x^2+1)^3} + \frac{c'}{(x^2+1)^2} + \frac{c''}{x^2+1} = \frac{-c}{(x^2+1)^3} + \frac{-c'}{(x^2+1)^2} + \frac{c''}{x^2+1}$$

Mais d'après le cours, la décomposition est unique, ce qui donne
 $c = -c \quad c' = -c' \quad c'' = -c'' \Rightarrow c = c' = c'' = 0$

c) Alors on obtient :

$$B(x) = \frac{a}{x} + \frac{bx}{(x^2+1)^3} + \frac{b'x}{(x^2+1)^2} + \frac{b''x}{(x^2+1)}$$

On multiplie par x et on obtient

$$\frac{(x^2-1)^2}{(x^2+1)^3} = a + \frac{bx^2}{(x^2+1)^3} + \frac{b'x^2}{(x^2+1)^2} + \frac{b''x^2}{x^2+1}$$

Posons $x=0$:

$$\underline{1 = a}$$

d) Alors on obtient :

$$B(x) = \frac{1}{x} + \frac{bx}{(x^2+1)^3} + \frac{b'x}{(x^2+1)^2} + \frac{b''x}{(x^2+1)}$$

Multiplions par $(x^2+1)^3$

$$\frac{(x^2-1)^2}{x} = \frac{(x^2+1)^3}{x} + bx + b'x(x^2+1) + b''x(x^2+1)^2$$

On pose $x=i$

$$\begin{aligned} & \frac{(i^2+1)}{(-1+1)} = 0 \\ & = (-1+1) = 0 \end{aligned}$$

$$\frac{(-2)^2}{i} = 0 + bi$$

$$\frac{4}{i} = b = \frac{4}{-1} = -4$$

Donc $b = -4$

Donc on obtient:

$$B(x) = \frac{1}{x} - \frac{4x}{(x^2+1)^2} + \frac{\beta'x}{(x^2+1)^2} + \frac{\beta''x}{(x^2+1)}$$

e) Soit $f(x) := \frac{(x^2-1)^2}{x(x^2+1)^2}$

$$\lim_{x \rightarrow +\infty} x f(x) = \lim_{x \rightarrow +\infty} \frac{(x^2-1)^2}{(x^2+1)^2} = \lim_{x \rightarrow +\infty} \frac{x^4 - 2x^2 + 1}{x^4 + 2x^2 + 1} = 0$$

$$\lim_{x \rightarrow +\infty} x \beta(x) = \lim_{x \rightarrow +\infty} \left(1 - \frac{4x^2}{(x^2+1)^2} + \frac{\beta'x^2}{(x^2+1)^2} + \frac{\beta''x^2}{x^2+1} \right)$$

$$= \lim_{x \rightarrow +\infty} \left(1 - 0 + 0 + \frac{\beta''}{1 + \frac{1}{x^2}} \right)$$

$$= \lim_{x \rightarrow +\infty} \left(1 - 0 + 0 + \beta'' \right) = 0$$

$$\text{D'où } 1 + \beta'' = 0 \Rightarrow \beta'' = -1$$

Donc on obtient

$$B(x) = \frac{(x^2-1)^2}{x(x^2+1)^2} = \frac{1}{x} - \frac{4x}{(x^2+1)^2} + \frac{\beta'x}{(x^2+1)^2} - \frac{x}{x^2+1}$$

f)
$$\frac{(x^2-1)^2}{x(x^2+1)} = \frac{(x^2+1)^2}{x} - \frac{4x}{x^2+1} + \beta'x - (x^2+1)x$$

$$0 = 4 - 2 + \beta' - 2$$

$$0 = \beta'$$

Donc le résultat final est:

$$B(x) = \frac{(x^2-1)^2}{x(x^2+1)^2} = \frac{1}{x} - \frac{4x}{(x^2+1)^2} - \frac{x}{x^2+1}$$

$$g) \quad (x^2-1)^2 = x^4 - 2x^2 + 1$$

$$\frac{x^4 - 2x^2 - x + 1}{x(x^2+1)^3} = \frac{(x^2-1)^2 - x}{x(x^2+1)^3} = \frac{(x^2-1)^2}{x(x^2+1)^3} - \frac{x}{x(x^2+1)^3}$$

$$= \beta(x) - \frac{1}{(x^2+1)^3} =$$

D'après les questions précédentes :

$$\frac{x^4 - 2x^2 - x + 1}{x(x^2+1)^3} = \frac{1}{x} - \frac{4x}{(x^2+1)^3} - \frac{x}{x^2+1} - \frac{1}{(x^2+1)^3}$$

$$= \frac{1}{x} - \frac{4x+1}{(x^2+1)^3} - \frac{x}{x^2+1}$$

Exercice 6

$$a) \quad A(x) = \frac{x}{x^4+x^2+1} = \frac{x}{(x^2+1)^2-x^2} = \frac{x}{(x^2+x+1)(x^2-x+1)}$$

$$(2x^2+2)^4 = 4x^4 + 8x^2 + 4 - 3(x^2+1)^2$$

$$4(x^2+1)^4 - 3(x^2+1)^2 - x^2$$

$$4(x^2+1)^4 - 3(x^2+1)^2 - x^2$$

$$= (x^2+1)^2 - x^2 = (x^2+1-x)(x^2+1+x)$$

D'après le théorème du cours de décomposition

$$A(x) = \frac{x}{x^4+x^2+1} = \frac{x}{(x^2+x+1)(x^2-x+1)} = \frac{ax+b}{x^2+x+1} + \frac{cx+d}{x^2-x+1}$$

avec a, b, c, d des réels à déterminer.

Multiplications par (x^2+x+1)

$$\frac{x}{x^2-x+1} = ax+b + \frac{(cx+d)(x^2+x+1)}{x^2-x+1}$$

$$0 = b + (d)(1) = b+d \Rightarrow d = -b$$

$$A(x) = \frac{x}{x^4 + x^2 + 1} = \frac{x}{(x^2 + x + 1)(x^2 - x + 1)} = \frac{ax + b}{x^2 + x + 1} + \frac{cx + d}{x^2 - x + 1}$$

$$x = (ax + b)(x^2 - x + 1) + (cx + d)(x^2 + x + 1)$$

$$x = ax^3 + bx^2 - ax^2 - bx + ax + b + cx^3 + dx^2 + cx^2 + dx + cx + d$$

$$= (a+c)x^3 + (-a+b+cx+dx)x^2 + (a-b+c+dx)x + (b+d)$$

$$\Rightarrow \begin{cases} 0 = a+c \\ 0 = -a+b+cx+dx \\ 1 = a-b+c+dx \\ 0 = b+d \end{cases} = \begin{bmatrix} a & b & c & d & 2 \\ 1 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 1 & 0 \\ 1 & -1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{array}{l} L_2 \leftarrow (L_2 + L_1) \cdot \frac{1}{2} \\ L_3 \leftarrow (L_3 + L_4 - L_1) \cdot \frac{1}{2} \end{array}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{array}{l} L_1 \leftarrow L_1 - L_2 \\ L_4 \leftarrow L_4 - L_3 \end{array}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 1 & 0 & 0 & -\frac{1}{2} \end{bmatrix} \Rightarrow \begin{array}{l} b = -\frac{1}{2} \\ d = \frac{1}{2} \\ c = 0 \end{array}$$

$$\text{Donc : } \frac{x}{(x^2 + x + 1)(x^2 - x + 1)} = \frac{-\frac{1}{2}}{x^2 + x + 1} + \frac{\frac{1}{2}}{x^2 - x + 1} = A(x)$$

b) Il faut montrer que

$$p := x^2 + \lambda x + \mu \Leftrightarrow \exists \alpha \quad x^2 + \lambda x + \mu = 0$$

$$\exists Q(x), Q'(x) \quad p = Q(x)Q'(x)$$

\Rightarrow Soit $p := x^2 + \lambda x + \mu$ sur \mathbb{K}
 irréductible. Or $\deg(p) = 2$
 donc la seule possibilité de
 décomposition est: $\deg(Q(x)) = \deg(Q'(x)) = 1$

donc $Q(x) = (x - \alpha)$ $Q'(x) = (x - \beta)$
 où $p = (x - \alpha)(x - \beta)$ et de plus les polynômes
 de degré 1 sont irréductibles.

Si on pose $p(x) = (x - \alpha)(x - \beta) = 0$

donc par définition, α est une racine de p !

⊆ Soit $p := x^2 + \lambda x + \mu$ et on suppose que $\exists \alpha \in K$ et $\mu \alpha = 0$

D'après le cours, si α est une racine de p alors p se décompose comme $p = (x - \alpha)Q(x)$ où $Q(x)$ est un polynôme sur K

$$\text{par contre } \deg(p) = \deg(x - \alpha) + \deg(Q(x)) \\ \Leftrightarrow 2 = 1 + \deg(Q(x)) \\ \Rightarrow \deg(Q(x)) = 2 - 1 = 1$$

donc $Q(x)$ est aussi de la forme $(x - \beta) = Q(x)$ mais les polynômes de degré 1 sont irréductibles.

Donc $p = (x - \alpha)(x - \beta)$ ce qui est une décomposition. donc p réductible.

$$c) \quad (x^2 + \bar{4}) \equiv (x^2 - \bar{1}) \quad [5] \\ \equiv (x - \bar{1})(x + \bar{1}) \quad [5]$$

mais $(x^2 + \bar{3}) = (x^2 - \bar{2})$ n'a pas de racines, d'après b) cela signifie que $(x^2 + \bar{3})$ est irréductible.

$$d) \quad \text{Soit } A(x) = \frac{x - \bar{2}}{(x^2 + \bar{4})(x^2 + \bar{3})} \in F_K[x] \text{ où } K = \mathbb{Z}/5\mathbb{Z}$$

$$\text{D'après c) } A(x) = \frac{x - \bar{2}}{(x - \bar{1})(x + \bar{1})(x^2 + \bar{3})}$$

Où tous les facteurs du dénominateur et numérateur sont irréductibles (d'après c) et $\deg(1) \Rightarrow$ irréductible)

Degré de numérateur est inférieur à celui de dénominateur

ce qui, d'après le théorème du cours nous permet à décomposer ce polynôme:

$$A(x) = \frac{x - \bar{2}}{(x - \bar{1})(x + \bar{1})(x^2 + \bar{3})} = \frac{a x + b}{x^2 + \bar{3}} + \frac{c}{x - \bar{1}} + \frac{d}{x + \bar{1}}$$

avec a, b, c, d des inconnues, à déterminer

$$A(x) = \frac{x-\bar{2}}{(x-\bar{1})(x+\bar{i})(x^2+\bar{3})} = \frac{ax+\bar{b}}{x^2+\bar{3}} + \frac{c}{x-\bar{1}} + \frac{d}{x+\bar{i}}$$

$$\begin{aligned} \Rightarrow x-\bar{2} &= (ax+\bar{b})(x-\bar{1})(x+\bar{i}) + c(x^2+\bar{3})(x+\bar{1}) + d(x-\bar{1})(x^2+\bar{3}) \\ &= (ax+\bar{b})(x^2+\bar{4}) + cx^3 + cx^2 + \bar{3}cx + \bar{3}c \\ &\quad + dx^3 + \bar{3}dx - dx^2 - \bar{3}d \end{aligned}$$

$$= \underline{ax^3} + \underline{\bar{4}ax} + \underline{\bar{b}x^2} + \underline{\bar{4}b} + \underline{cx^3} + \underline{cx^2} + \underline{\bar{3}cx} + \underline{\bar{3}c} + \underline{dx^3} + \underline{\bar{3}dx} - \underline{dx^2} - \underline{\bar{3}d}$$

$$\Rightarrow x = x^3(a+c+d) + x^2(\bar{b}+c-d) + x(\bar{4}a+\bar{3}c+\bar{3}d) + (\bar{4}b+\bar{3}c-\bar{3}d+\bar{2})$$

$$\Rightarrow \begin{cases} 0 = a+c+d & \Rightarrow a = -c-d \\ 0 = \bar{b}+c-d \\ 1 = \bar{4}a+\bar{3}c+\bar{3}d = -\bar{4}c-\bar{4}d+\bar{3}c+\bar{3}d = -c-d \\ 0 = \bar{4}b+\bar{3}c-\bar{3}d+\bar{2} \end{cases}$$

$$\Rightarrow a=1$$

$$\Rightarrow \begin{cases} a=1 \\ 1 = -c-d & \Rightarrow -d = 1+c \\ 0 = \bar{b}+c-d & \Rightarrow 0 = \bar{b}+c+1+c = \bar{b}+2c+1 \Rightarrow \bar{b}+2c = -1 \\ 1 = \bar{4} + \bar{3}c + \bar{3}d \\ 0 = \bar{4}b + \bar{3}c - \bar{3}d + \bar{2} \end{cases}$$

$$1 = \bar{4}b + \bar{1}c + \bar{1} \Rightarrow \begin{cases} \bar{4}b + c = 0 & \Rightarrow -\bar{7}b = -\bar{1} \\ \bar{b} + 2c = -1 & \Rightarrow \bar{7}b = \bar{1} \\ & \Rightarrow \bar{2}b = \bar{1} = -\bar{4} \\ & \Rightarrow \bar{b} = -\bar{2} \end{cases}$$

$$\Rightarrow \begin{cases} a=1 & \bar{b} = -\bar{2} \\ 0 = \bar{4} + \bar{3}c - \bar{3}d & \Rightarrow \bar{1} = \bar{b} + \bar{6}c \\ 1 = \bar{4} + \bar{3}c + \bar{3}d & \Rightarrow \bar{1} = \bar{3} + \bar{c} \Rightarrow c = -\bar{2} = \bar{3} \\ 1 = -c-d & \Rightarrow -1-c = d \Rightarrow -\bar{1}+\bar{2} = d = \bar{1} \end{cases}$$

$$a = \bar{1} \quad \bar{b} = \bar{3} \quad c = \bar{3} \quad d = \bar{1}$$

$$A(x) = \frac{x+\bar{3}}{x+\bar{3}} + \frac{\bar{3}}{x-\bar{1}} + \frac{\bar{1}}{x+\bar{1}}$$

$$= \frac{x+\bar{3}}{x+\bar{3}} + \frac{\bar{3}}{x+\bar{9}} + \frac{\bar{1}}{x+\bar{1}}$$

~~_____~~