Examens corrigés

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Examen 1

Exercice 1. **(a)** Déterminer le reste dans la division euclidienne de 2^{100} par 63.

Exercice 2. **(a)** Résoudre complètement l'équation linéaire :

$$1\,665\,x + 1\,035\,y \;=\; 45,$$

d'inconnues $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Indication: Diviser $1\,665$ par 45, puis $1\,035$ par 45 aussi.

(b) Déterminer l'inverse multiplicatif de $23 \mod 37$ dans $\mathbb{Z}/37\mathbb{Z}$.

(c) L'entier $1\,035 \mod 1\,665$ est-il inversible dans $\mathbb{Z}/1\,665\mathbb{Z}$ muni du produit ?

Exercice 3. **(a)** Montrer que le reste de la division euclidienne par 8 du carré de tout nombre impair vaut 1, et que tout nombre pair $x \in 2\,\mathbb{Z}$ vérifie $x^2 \equiv 0 \mod 8$, ou $x^2 \equiv 4 \mod 8$.

(b) Soient x, y, z trois nombres entiers *impairs*. Montrer que :

$$2\,\big(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\big),$$

ne peut jamais être égal au carré n^2 d'un entier $n \in \mathbb{Z}$.

Exercice 4. **(a)** Sur l'ensemble $\mathbb{R}$, on définit la loi de composition interne commutative $*$ par :

$$x * y \;:=\; x + y + 1.$$

Est-ce que $\big(\mathbb{R}, *\big)$ est un groupe ?

Exercice 5. Dans le groupe additif des entiers $m \mod 18$, notés $\overline{m}$ pour $m \in \mathbb{Z}$:

$$G \;:=\; \mathbb{Z}/18\mathbb{Z} \;=\; \Big\{\overline{0},\, \overline{1},\, \overline{2},\, \overline{3},\, \overline{4},\, \overline{5},\, \overline{6},\, \overline{7},\, \overline{8},\, \overline{9},\, \overline{10},\, \overline{11},\, \overline{12},\, \overline{13},\, \overline{14},\, \overline{15},\, \overline{16},\, \overline{17}\Big\},$$

on considère le sous-ensemble :

$$H \;:=\; \big\{\overline{m} \in G\colon\; 6\,\overline{m} = \overline{0}\big\}.$$

On rappelle que l'égalité $\overline{0} = 6\,\overline{m} = \overline{6\,m}$ signifie $6\,m \equiv 0 \mod 18$.

(a) Montrer que H est un sous-groupe de G.

(b) Déterminer tous les éléments distincts de H. Par la suite, on notera $d \;:=\; \mathsf{Card}\,H$ le nombre de ces éléments.

(c) Soit K un sous-groupe de G de même cardinal d. Montrer que $K = H$ nécessairement.

(d) Combien H contient-il d'éléments d'ordre 6 ?

Exercice 6. **(a)** Décomposer 561 en facteurs premiers. Indication: Cet entier est divisible par 17.

(b) Soit une indéterminée a. Pour tout entier $n \geqslant 1$, justifier la formule :

$$a^n - 1 \;=\; (a-1)\left(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1\right).$$

(c) Justifier, pour tout entier $\kappa \geqslant 1$ et tout entier $n \geqslant 1$, la formule :

$$a^{\kappa\, n} - 1 \;=\; \left(a^{\kappa} - 1\right)\left(a^{(n-1)\kappa} + a^{(n-2)\kappa} + \cdots + a^{2\kappa} + a^{\kappa} + 1\right).$$

(d) Soit un entier quelconque $a \in \mathbb{Z}$. Justifier que $a^{561} - a = a\left(a^{2\cdot 280} - 1\right) = a\left(a^2 - 1\right)\boldsymbol{k}$ avec un certain entier $\boldsymbol{k} \in \mathbb{Z}$.

(e) Pour $a \in \mathbb{Z}$ quelconque, montrer que $a(a-1)(a+1)$ est toujours divisible par 3.

(f) Montrer que $a^{561} - a$ est multiple de 3.

(g) Montrer que $a^{561} - a$ est multiple de 17. Indication: Observer que $560 = 16 \cdot 35$. Ensuite, penser au théorème de Fermat.

(h) Montrer que $a^{561} - a$ est multiple de 11.

(i) Montrer que $a^{561} \;\equiv\; a \mod 561$, pour tout entier $a \in \mathbb{Z}$.

(j) Interpréter ce résultat.

(k) Que vous inspire le nombre $1\,105$?

Exercice 7. **(a)*** Déterminer le nombre de diviseurs de $3\,528$.

2. Corrigé de l'examen 1

Exercice 1. (a) En calculant les puissances successives de 2 on constate que :

$$2^6 \;=\; 64 \;\equiv\; 1 \mod 63,$$

ce qui donne, puisque $100 = 6 \cdot 16 + 4$:

$$2^{100} \;=\; (2^6)^{16} \cdot 2^4 \;\equiv\; 1^{16} \cdot 16 \;\equiv\; 16 \mod 63.$$

Puisqu'on a $0 \leqslant 16 < 63$, on en déduit que le reste dans la division euclidienne de 2^{100} par 63 est 16.

Exercice 2. (a) Effectivement, on constate que :

$$1\,665 \;=\; 45 \cdot 37, \qquad\qquad 1\,035 \;=\; 45 \cdot 23,$$

et donc, l'équation à résoudre est équivalente à :

$$37\,x + 23\,y \;=\; 1.$$

Ici, 37 et 23 sont deux nombres *premiers* distincts, donc premiers entre eux. On reconnaît donc ici une relation de Bézout $a\,u + b\,v = 1$, qui existe toujours lorsque $1 = a \wedge b$. Mais il faut en trouver une !

Pour cela, comme on le sait, on procède avec l'algorithme d'Euclide :

$$\begin{aligned}
37 \;&=\; 1 \cdot 23 \;+\; 14 \\
23 \;&=\; 1 \cdot 14 \;+\; 9 \\
14 \;&=\; 1 \cdot 9 \;+\; 5 \\
9 \;&=\; 1 \cdot 5 \;+\; 4 \\
5 \;&=\; 4 \cdot 1 \;+\; \boxed{\mathbf{1}} \\
1 \;&=\; 1 \cdot 1 \;+\; \mathbf{0},
\end{aligned}$$

puis en remontant depuis l'avant-dernière ligne, on calcule :

$$\begin{aligned}
1 \;&=\; 5 - \underline{4}_{\text{rpl}} \\
&=\; 5 - \big(9 - 5\big) \\
&=\; -9 + 2 \cdot \underline{5}_{\text{rpl}} \\
&=\; -9 + 2\,\big(14 - 9\big) \\
&=\; 2 \cdot 14 - 3 \cdot \underline{9}_{\text{rpl}} \\
&=\; 2 \cdot 14 - 3\,\big(23 - 14\big) \\
&=\; -3 \cdot 23 + 5 \cdot \underline{14}_{\text{rpl}} \\
&=\; -3 \cdot 23 + 5\,\big(37 - 23\big) \\
&=\; 5 \cdot 37 - 8 \cdot 23 \\
&=\; \mathbf{185 - 184} \;=\; \mathbf{1} \qquad \text{OUI},
\end{aligned}$$

et donc une solution particulière (x_0, y_0) de notre équation est :

$$1 \;=\; 37\,x_0 + 23\,y_0 \;\;=\;\; 37 \cdot 5 + 23 \cdot (-8).$$

D'après un théorème du cours, l'espace des solutions complètes est alors :

$$\mathsf{Sol} \;=\; \Big\{(x,y) \in \mathbb{Z} \times \mathbb{Z}\colon\;\; x = 5 - 23\,k,\;\; y = -8 + 37\,k \\ \text{avec } k \in \mathbb{Z} \text{ quelconque}\Big\},$$

ce que l'on peut retrouver en soustrayant notre solution particulière à une solution quelconque :

$$\begin{Bmatrix} 37\,x + 23\,y \;=\; 1 \\ 37\,x_0 + 23\,y_0 \;=\; 1 \end{Bmatrix} \qquad \text{impliquent} \qquad 37\,\big(x - x_0\big) \;=\; 23\,\big(y - y_0\big) \;=\; 0,$$

d'où, comme $37 \wedge 23 = 1$:

$$x - x_0 \;=\; -23\,k, \qquad\qquad y - y_0 \;=\; 37\,k,$$

avec $k \in \mathbb{Z}$ quelconque.

(b) Grâce à la relation de Bézout que nous avons obtenue plus haut :

$$37 \cdot 5 + 23 \cdot (-8) \;=\; 1,$$

qui devient après réduction modulo 37 :

$$23 \cdot (-8) \;\equiv\; 1 \;\mod 37,$$

il est clair que l'inverse de $23 \mod 37$ est $-8 \equiv 29 \mod 37$ dans $\mathbb{Z}/37\mathbb{Z}$.

(c) Certainement pas ! Car l'existence d'un entier z qui satisferait :

$$1\,035 \cdot z \;\equiv\; 1 \;\mod 1\,665,$$

ce qui équivaudrait à :

$$1\,305\,z \;=\; 1 + 1\,665\,k,$$

avec un entier k, impliquerait, après réduction modulo 5, l'absurdité fatale :

$$0 \;\equiv\; 1 \;\mod 5.$$

Exercice 3. (a) Nous allons donc raisonner modulo 8, dans l'anneau additif :

$$\mathbb{Z}/8\mathbb{Z} \;=\; \big\{0,\,1,\,2,\,3,\,4,\,5,\,6,\,7\big\} \;\mod 8,$$

et calculer tous les carrés possibles. Comme 8 est pair, on a :

$$x \;=\; 2\,y \;\in\; 2\,\mathbb{Z} \qquad\qquad \Longleftrightarrow \qquad\qquad x \;\equiv\; 0,\;2,\;4,\;6 \;\mod 8,$$
$$x \;=\; 2\,y + 1 \;\in\; 2\,\mathbb{Z} + 1 \qquad\qquad \Longleftrightarrow \qquad\qquad x \;\equiv\; 1,\;3,\;5,\;7 \;\mod 8.$$

Ainsi, on calcule les carrés de ces 8 éléments/représentants, et on les réduit modulo 8 :

x	0	1	2	3	4	5	6	7
x^2	0	1	4	9	16	25	36	49
$x^2 \mod 8$	0	1	4	1	0	1	4	1.

Effectivement, il est maintenant transparent que tous les carrés de nombres impairs sont congrus à 1 modulo 8, et que les carrés de nombres pairs peuvent valoir 0 ou 4 modulo 8.

(b) Puisque :

$$x^2 \;\equiv\; 1 \;\mod 8, \qquad\qquad y^2 \;\equiv\; 1 \;\mod 8, \qquad\qquad z^2 \;\equiv\; 1 \;\mod 8,$$

il vient, en prenant les produits deux à deux :

$$x^2\,y^2 \;\equiv\; 1\cdot 1 \mod 8, \qquad x^2\,z^2 \;\equiv\; 1\cdot 1 \mod 8, \qquad y^2\,z^2 \;\equiv\; 1\cdot 1 \mod 8,$$

et donc :

$$\begin{aligned} 2\left(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\right) &\equiv 2\left(1+1+1\right) \mod 8 \\ &\equiv 6 \mod 8. \end{aligned}$$

Or d'après la Question **(a)** qui précède, un carrré quelconque n^2 avec $n \in \mathbb{Z}$ ne peut être congru qu'aux trois valeurs :

$$n^2 \;\equiv\; 0,\; 1,\; 4 \mod 8,$$

toutes distinctes de ce 6 *intempestif!* En conclusion, une égalité du type :

$$2\left(x^2\,y^2 + x^2\,z^2 + y^2\,z^2\right) \;=\; n^2, \qquad \text{avec} \qquad \begin{cases} x,\, y,\, z \;\in\; 2\,\mathbb{Z}+1, \\ \qquad n \;\in\; \mathbb{Z}, \end{cases}$$

est *impossible*.

Exercice 4. (a) Tout d'abord, vérifions que cette loi $*$ (un peu spéciale) est associative :

$$\begin{aligned} x * \left(y * z\right) &= x + \left(y * z\right) + 1 \\ &= x + \left(y + z + 1\right) + 1 \\ &= x + y + z + 2 \\ &= \left(x + y + 1\right) + z + 1 \\ &= \left(x * y\right) * z, \end{aligned}$$

ce, pour tous $x, y, z \in \mathbb{R}$. Super, l'associativité passe !

Observons au passage que cette loi est *commutative*, tout autant que l'est l'addition dans $\mathbb{R}$:

$$x * y \;=\; x + y + 1 \;=\; y + x + 1 \;=\; y * x.$$

Ensuite, après une réflexion rapide sur une feuille de brouillon, on devine *qui* doit être l'élément neutre de cette loi :

$$x * (-1) \;=\; x + (-1) + 1 \;=\; x,$$

sachant que $(-1) * x \;=\; x$ vient tout seul grâce à la commutativité. Ça commence à se confirmer, que $*$ est une loi de groupe !

Il reste à trouver l'*inverse* d'un élément quelconque $x \in \mathbb{R}$ pour cette loi interne $*$. Après une réflexion personnelle, on le devine aisément, puis on vérifie sur sa copie que :

$$\begin{aligned} x * \left(-\,x - 2\right) &= x + \left(-\,x - 2\right) + 1 \\ &= -\,1, \end{aligned}$$

où on doit retrouver l'élément neutre en question. L'autre égalité, requise pour satisfaire l'axiome d'inverse $(-x-2) * x = -1$, est alors ou bien offerte par la commutativité, ou bien vérifiable de manière analogue (et fort élémentaire).

En conclusion :

$$\left(\mathbb{R},\, *\right)$$

est bien un groupe — il n'y avait pas de piège !

Mais une question subsididaire surgit : ce groupe est-il « équivalent [1] », en un certain sens, au groupe $\big(\mathbb{R},+\big)$. Réponse : oui ! Le lecteur de ce corrigé pourra y réfléchir, en s'inspirant de :

$$x+y+1 \,=\, x+\tfrac{1}{2}+y+\tfrac{1}{2}.$$

Exercice 5. (a) Tout d'abord, on a $\overline{0}\in H$, car $6\cdot 0=0$, d'où $6\cdot\overline{0}=\overline{6\cdot 0}=\overline{0}$.

Ensuite, pour tous $\overline{m},\overline{n}\in H$, comme on sait d'après un théorème du cours que $\overline{m}+\overline{n}=\overline{m+n}$, et comme on sait aussi que :

$$\Big(\,6\,m\,\equiv\,0\ \mathsf{mod}\,18\quad\text{et}\quad 6\,n\,\equiv\,0\ \mathsf{mod}\,18\,\Big)\qquad\Longrightarrow\qquad 6\,\big(m{+}n\big)\,\equiv\,0\ \mathsf{mod}\,18,$$

il est clair que l'on a aussi $\overline{m}+\overline{n}\in H$ aussi.

Enfin, si $\overline{m}$ appartient à H, son élément opposé (pour l'addition) $\overline{-\,m}$ appartient aussi à H, puisque :

$$6\,m\,\equiv\,0\ \mathsf{mod}\,18\qquad\Longrightarrow\qquad 6\,\big(-\,m\big)\,=\,-\,6\,m\,\equiv\,-\,0\ \mathsf{mod}\,18.$$

Ces trois vérifications démontrent donc bien que $H\subset G$ est un *sous-groupe* de G.

(b) On a $\overline{m}\in H$ avec $m\in\mathbb{Z}$ si et seulement si :

$$6\,m\,\equiv\,0\ \mathsf{mod}\,18.$$

Or, comme $18=6\cdot 3$ (révision de CP), $6\,m$ est multiple de 18 *si et seulement si* m est multiple de 3. Par conséquent, nous obtenons :

$$H\,=\,\Big\{\overline{0},\ \overline{3},\ \overline{6},\ \overline{9},\ \overline{12},\ \overline{15}\Big\}.$$

Visiblement, le cardinal d de H est égal à 6.

(c) Soit donc $K\subset G$ un sous-groupe de cardinal $|K|=6$. Comme K est un groupe en lui-même, un théorème vu en cours qui est une conséquence directe du théorème de Lagrange a montré que *tout* élément $\overline{m}\in K$ a un ordre qui *divise* le cardinal du groupe ambiant :

$$o\big(\overline{m}\big)\ \Big|\ 6\,=\,|K|,$$

d'où nous avons déduit que :

$$\overline{m}^{\,6}\,=\,1_K\,=\,1_G,$$

et comme notre groupe $G=\mathbb{Z}\big/18\mathbb{Z}$ est additif-commutatif, d'élément neutre [2] $1_G=\overline{0}$, ceci veut en fait dire que :

$$6\,\overline{m}\,=\,\overline{0},$$

exactement comme dans la définition de H ! Ainsi, $K\subset H$, et comme K et H ont même cardinal $d=6$, ils doivent effectivement coïncider : $K=H$.

(d) D'après un théorème vu en cours, tout élément $\overline{m}\in\mathbb{Z}\big/18\mathbb{Z}$ est d'ordre :

$$o\,\big(\overline{m}\big)\,=\,\frac{18}{\mathsf{pgcd}\,(18,m)}.$$

1. En Théorie des groupes, le *problème d'équivalence* est l'un des problèmes les plus centraux, les plus importants, et les plus difficiles.

2. Aïe ! Éh ! Oh ? Vous êtes sérieux, Messieurs les professeurs ? Vous avez écrit $1=0$? N'avez-vous pas conscience que tout le langage informatique disparaîtrait, englouti à jamais dans un trou noir de contradictions intergalactiques ?

Grâce à cette belle petite formule élémentaire qui nous montre combien le *sang* de l'arithmétique irrigue les canaux fructifères de la théorie des groupes, nous sommes maintenant ramenés à des calculs directs de niveau CE1.

En effet, une petite vérification rapide sur du papier de brouillon nous convainc alors aisément que, parmi les six éléments $\overline{m} = \overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}$ de H, seuls deux ont un représentant $m \in \mathbb{Z}$ qui a un pgcd égal à 3 avec 18, d'où nous concluons qu'il y a exactement *deux* éléments d'ordre 6 dans H :

$$\overline{3} \qquad \text{et} \qquad \overline{15}.$$

Exercice 6. **(a)** Heureusement qu'il y a une indication ! En divisant 561 par 17, on trouve :

$$561 \;=\; 17 \cdot 33 \;=\; 17 \cdot 11 \cdot 3,$$

ce qui est la décomposition de 561 en ses *trois* facteurs premiers.

(b) Effectivement, quand on développe le produit à droite en disposant le résultat sur deux lignes décalées astucieusement :

$$\begin{aligned} a^n - 1 &\overset{?}{=} (a-1)\left(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1\right) \\ &= a^n + a^{n-1} + \cdots + a^3 + a^2 + a \\ &\qquad - a^{n-1} - a^{n-2} - \cdots - a^2 - a - 1 \\ &= a^n + 0 + \cdots\cdots\cdots\cdots + 0 + 0 - 1 \qquad \text{OUI,} \end{aligned}$$

on constate un grand nombre d'annulations par paires, qui offrent le résultat.

(c) Il suffit de remplacer a par a^κ dans la formule précédente.

(d) En appliquant les questions qui précèdent, on peut effectivement factoriser :

$$\begin{aligned} a^{561} - a &= a\left(a^{560} - 1\right) \\ &= a\left(a^{2\cdot 280} - 1\right) \\ &= a\left(a^2 - 1\right)\Big(\underbrace{a^{2\cdot 279} + a^{2\cdot 278} + \cdots + a^{2\cdot 2} + a^{2\cdot 1} + 1}_{=:\, k}\Big) \\ &=: a\left(a^2 - 1\right) k. \end{aligned}$$

(e) Modulo 3, trois cas seulement sont possibles :

$$a \equiv 0 \mod 3, \qquad a \equiv 1 \mod 3, \qquad a \equiv 2 \mod 3.$$

Dans chacun de ces trois cas, le produit $a(a-1)(a+1)$:

$$0\cdot(0-1)\cdot(0+1) \equiv 0 \mod 3, \quad 1\cdot(1-1)\cdot(1+1) \equiv 0 \mod 3, \quad 2\cdot(2-1)\cdot(2+1) \equiv 0 \mod 3,$$

est toujours congru à 0 modulo 3, oui.

(f) D'après ce qui précède, on a bien :

$$\begin{aligned} a^{561} - a &= a\left(a-1\right)\left(a+1\right) k \\ &\equiv 0 \cdot k \mod 3 \\ &\equiv 0 \mod 3. \end{aligned}$$

(g) Grâce à la factorisation indiquée $560 = 16 \cdot 35$ que l'on vérifie aisément en développant ce produit, on peut factoriser de manière analogue :

$$\begin{aligned} a^{561} - a &= a\left(a^{560} - 1\right) \\ &= a\left(a^{16\cdot 35} - 1\right) \\ &= a\left(a^{16} - 1\right)\big(\underbrace{a^{16\cdot 34} + a^{16\cdot 33} + \cdots + a^{16\cdot 2} + a^{16\cdot 1} + 1}_{=:\, l}\big) \\ &=: a\left(a^{16} - 1\right) l. \end{aligned}$$

Mais alors, plutôt que de procéder laborieusement comme dans la Question **(e)** plus haut, on redéveloppe ce produit :

$$a^{561} - a = \left(a^{17} - a\right) l,$$

et on reconnaît alors ce dont la deuxième formulation du Théorème de Fermat-bis parlait — tout en vérifiant mentalement que 17 est bien premier !

Ainsi, une simple application dudit Théorème de Fermat-bis offre la réponse :

$$\begin{aligned} a^{561} - a &\equiv 0 \cdot l \mod 17 \\ &= 0 \mod 17. \end{aligned}$$

(h) Évidemment, il faut procéder de manière similaire, mais l'énoncé laissait l'étudiant chercher la factorisation appropriée de 560 :

$$\begin{aligned} a^{561} - a &= a\left(a^{560} - 1\right) \\ &= a\left(a^{10\cdot 56} - 1\right) \\ &= a\left(a^{10} - 1\right)\big(\underbrace{a^{10\cdot 55} + a^{10\cdot 54} + \cdots + a^{10\cdot 2} + a^{10\cdot 1} + 1}_{=:\, m}\big) \\ &=: a\left(a^{10} - 1\right) m, \end{aligned}$$

et comme 11 est premier, Fermat vient encore à la rescousse :

$$\begin{aligned} a^{561} - a &= \left(a^{11} - a\right) m \\ &= 0 \cdot m \mod 11 \\ &\equiv 0 \mod 11. \end{aligned}$$

(i) Ah, tiens ? Mais oui ! On re-dirait Fermat, encore…

En tout cas, puisque 3, 11, 17 sont premiers entre eux, les trois Questions **(f)**, **(g)**, **(h)**, qui disaient que le nombre $a^{561} - a$ est congru à 0 modulo 3, 11, 17, impliquent, grâce au Théorème de Gauss [3], que ce nombre est *aussi* congru à 0 modulo le *produit* $3 \cdot 11 \cdot 17 = 561$.

Nous avons donc bien démontré, puisque $a \in \mathbb{Z}$ était arbitraire au départ, que l'on a :

$$a^{561} - a \equiv 0 \mod 561 \qquad (\forall\, a \in \mathbb{Z}).$$

(j) Cette conclusion est exactement la même que le Théorème de Fermat-bis — sauf que Fermat, lui, il demandait que le nombre p dans :

$$a^{p} - a \equiv 0 \mod p \qquad (\forall\, a \in \mathbb{Z}),$$

soit un nombre premier, ce qui n'est pas le cas ici, car notre petit Toto $561 = 3 \cdot 11 \cdot 17$ n'est *pas premier*.

3. — argument que l'on a d'ailleurs aussi employé pour démontrer le Théorème des restes chinois —

Ainsi, à cause du *Diable de l'Arithmétique*, les nombres premiers p ne sont pas les seuls nombres n qui vérifient le Théorème de Fermat-bis, énoncé sous la forme :

$$a^n \equiv a \bmod n \qquad (\forall\, a \in \mathbb{Z}).$$

Un nombre $n \geqslant 2$ est appelé *nombre de Carmichael* s'il n'est *pas* premier, *i.e.* s'il est *composé*, et s'il satisfait :

$$a^n \equiv a \bmod n,$$

pour tout entier $0 \leqslant a \leqslant n-1$, donc pour tout entier $a \in \mathbb{Z}$.

Les trois premiers nombres de Carmichael sont :

$$561,$$
$$1105,$$
$$1729.$$

(k) L'idée de le décomposer en facteurs premiers $5 \cdot 13 \cdot 17 = 1\,105$, et de tenter de raisonner avec lui comme nous avons raisonné avec 561. Pas le temps !

Exercice 7. (a)* Commençons par déterminer la *décomposition en facteurs premiers* de ce 'gros' nombre $3\,528$.

Le dernier chiffre est 8, donc 2 est un facteur premier. Mieux : les deux derniers chiffres sont $28 = 4 \cdot 7$, donc 4 divise $3\,528$. Encore mieux : les trois derniers chiffres sont $528 = 400 + 80 + 4$, qui est divisble par 8, donc $3\,528$ est divisible par 8. On fait alors le quotient et on obtient $3\,528 = 8 \cdot 441$.

Ensuite, la somme des chiffres de 441 étant égale à 9, on déduit que 441 est divisible par 9, on fait le quotient et on obtient $441 = 9 \cdot 49$. En définitive :

$$3\,528 = 2^3 \cdot 3^2 \cdot 7^2.$$

Ensuite, un diviseur quelconque de $3\,528$ est de la forme $2^a \cdot 3^b \cdot 7^c$, avec $0 \leqslant a \leqslant 3$, avec $0 \leqslant b \leqslant 2$, et avec $0 \leqslant c \leqslant 2$. Un triplet (a, b, c) satisfaisant ces inégalités détermine de manière unique un diviseur correspondant, et ces trois entiers a, b, c peuvent être choisis indépendamment les uns des autres.

Puisqu'il y a 4 choix possibles pour a, puis 3 choix pour b, puis 3 choix pour c, le nombre $3\,528$ possède au total exactement :

$$4 \cdot 3 \cdot 3 = 36$$

diviseurs mutuellement distincts.

3. Examen 2

Exercice 1. Soient les deux polynômes de $\mathbb{R}[x]$:

$$a \,:=\, x^3 - 9\,x^2 + 26\,x - 24 \qquad\qquad \text{et} \qquad\qquad b \,:=\, x^3 - 7\,x^2 + 7\,x + 15.$$

(a) Trouver pgcd (a, b). Indication: Il est de degré 1, de la forme $x - \alpha$ avec $\alpha \in \mathbb{Z}$, et on doit rencontrer $135 = 3 \cdot 45$ dans les calculs.

(b) Vérifier que le $\alpha \in \mathbb{Z}$ trouvé est bien racine de $a(\alpha) = 0 = b(\alpha)$.

(c) Trouver deux polynômes unitaires $a' \in \mathbb{R}[x]_1$ et $b' \in \mathbb{R}[x]_1$ tels que :

$$a \,=\, (x - \alpha)\, a' \qquad\qquad \text{et} \qquad\qquad b \,=\, (x - \alpha)\, b'.$$

(d) Décomposer a et b en facteurs irréductibles dans $\mathbb{R}[x]$.

Exercice 2. Soit l'ensemble $E \,:=\, \big\{1, 2, 3, 4, 5, 6, 7, 8, 9\big\}$. Soient les trois permutations composées de 3-cycles :

$$\begin{aligned} u \,&:=\, (1\ 2\ 3) \circ (4\ 5\ 6) \circ (7\ 8\ 9), \\ v \,&:=\, (4\ 5\ 6) \circ (7\ 8\ 9), \\ w \,&:=\, (1\ 4\ 7) \circ (2\ 5\ 8) \circ (3\ 6\ 9). \end{aligned}$$

(a) Pour trois entiers distincts $1 \leqslant a_1 < a_2 < a_3 \leqslant 9$, montrer que la permutation circulaire :

$$\sigma \,:=\, \Big(\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & a_3 \arrow[ll, bend left] \end{tikzcd} \Big) \,=\, \big(a_1\ a_2\ a_3\big)$$

satisfait $\sigma^3 = \mathsf{Id}$, tandis que $\sigma \neq \mathsf{Id} \neq \sigma^2$.

(b) Exprimer σ^{-1} en fonction de σ.

(c) Montrer que l'on a :

$$u^3 \,=\, v^3 \,=\, w^3 \,=\, \mathsf{Id}.$$

(d) Montrer que l'on a :

$$w \circ v \circ w^{-1} \,=\, (1\ 2\ 3) \circ (7\ 8\ 9).$$

Indication: Calculer l'image de chaque élément de $E = \big\{1, 2, 3, 4, 5, 6, 7, 8, 9\big\}$ par $w \circ v \circ w^{-1}$, en commençant par déterminer w^{-1}.

(e) Avec soin et sans erreur, décomposer $w^{-1} \circ v \circ w$ en composée de cycles à supports disjoints.

(f) En déduire les égalités :

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

(g) Montrer que u est une puissance négative de $w \circ v$, que l'on déterminera.

Exercice 3. **(a)** Décomposer en éléments simples, dans $F_{\mathbb{R}}[x]$, la fraction :

$$\frac{x}{x^4 + x^2 + 1}.$$

Indication: Au dénominateur, faire apparaître une différence entre deux carrés.

(b) Sur un corps commutatif $\mathbb{K}$, soit un polynôme unitaire du second degré $p := x^2 + \lambda\, x + \mu$. Montrer que p est réductible sur $\mathbb{K}$ si et seulement si il a une racine dans $\mathbb{K}$.

(c) Soit le corps $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}$ des classes résiduelles modulo 5. Décomposer en facteurs irréductibles le polynôme :

$$(x^2 + \overline{4})\,(x^2 + \overline{3}).$$

(d) Toujours avec $\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$, décomposer en éléments simples dans $F_{\mathbb{K}}[x]$ la fraction :

$$\frac{x - \overline{2}}{(x^2 + \overline{4})\,(x^2 + \overline{3})}.$$

4. Corrigé de l'examen 2

Exercice 1. (a) Appliquons l'algorithme d'Euclide en divisant a par b avec reste, et en poursuivant les divisions jusqu'à « capturer » le dernier reste non nul :

$$\begin{aligned} x^3 - 9\,x^2 + 26\,x - 24 &= 1 \cdot \big(x^3 - 7\,x^2 + 7\,x + 15\big) - 2\,x^2 + 19\,x - 39, \\ x^3 - 7\,x^2 + 7\,x + 15 &= \big(-\tfrac{1}{2}\,x - \tfrac{5}{4}\big)\big(-2\,x^2 + 19\,x - 39\big) + \boxed{\tfrac{45}{4}\,x - \tfrac{135}{4}}, \\ -2\,x^2 + 19\,x - 39 &= \big(-\tfrac{8}{45}\,x + \tfrac{52}{45}\big)\big(\boxed{\tfrac{45}{4}\,x - \tfrac{135}{4}}\big) + \mathbf{0}. \end{aligned}$$

Ainsi, pgcd (a, b) est le renormalisé unitaire :

$$\tfrac{4}{45}\big(\tfrac{45}{4}\,x - \tfrac{135}{4}\big) = x - 3.$$

et donc, $\alpha = 3$.

(b) Effectivement :

$$\begin{aligned} 3^3 - 9 \cdot 3^2 + 26 \cdot 3 - 24 &= 27 - 81 + 78 - 24 = 0, \\ 3^3 - 7 \cdot 3^2 + 7 \cdot 3 + 15 &= 27 - 63 + 21 + 15 = 0. \end{aligned}$$

(c) Ainsi, a et b sont divisibles par $x - 3$. On divise alors a et b par $x - 3$, et on trouve aisément — avec des restes nuls ! — :

$$a = (x-3)\,(x^2 - 6\,x + 8) \qquad \text{et} \qquad b = (x-3)\,(x^2 - 4\,x - 5).$$

(d) Comme les deux facteurs restants sont de degré 2, on applique la formule connue :

$$\frac{-\boldsymbol{b} \pm \sqrt{\boldsymbol{b}^2 - 4\,\boldsymbol{a}\,\boldsymbol{c}}}{2\,\boldsymbol{a}}$$

pour les racines (dans $\mathbb{C}$) d'un trinôme du second degré $\boldsymbol{a}\,x^2 + \boldsymbol{b}\,x + \boldsymbol{c}$ avec $\boldsymbol{a} \neq 0$, ce qui donne les deux couples de racines :

$$\frac{6 \pm \sqrt{6^2 - 4 \cdot 8}}{2} \qquad \text{et} \qquad \frac{4 \pm \sqrt{4^2 + 4 \cdot 5}}{2},$$

c'est-à-dire :

$$\frac{6 \pm \sqrt{4}}{2} = 3 \pm 1 \qquad \text{et} \qquad \frac{4 \pm \sqrt{36}}{2} = 2 \pm 3,$$

d'où en conclusion :

$$a = (x-3)\,(x-4)\,(x-2) \qquad \text{et} \qquad b = (x-3)\,(x-5)\,(x+1).$$

Exercice 2. (a) Cela a été vu en cours, mais re-faisons-le. Pour tout $a \neq a_1, a_2, a_3$, on a $\sigma(a) = a$, c'est-à-dire :

$$\sigma\Big|_{E\setminus\{a_1,a_2,a_3\}} = \mathsf{Id},$$

donc nous pouvons nous restreindre à considérer seulement l'action de σ sur $\{a_1, a_2, a_3\}$.

Alors par définition d'une permutation circulaire, on a :

$$\begin{aligned}\sigma(a_1) &= a_2 \neq a_1,\\ \sigma^2(a_1) &= \sigma(a_2) = a_3 \neq a_1,\end{aligned}$$

donc $\sigma \neq \mathsf{Id} \neq \sigma^2$, tandis que :

$$\begin{aligned}\sigma^3(a_1) &= \sigma(a_3) = a_1,\\ \sigma^3(a_2) &= \sigma^{3+1}(a_1) = \sigma\big(\sigma^3(a_1)\big) = \sigma(a_1) = a_2,\\ \sigma^3(a_3) &= \sigma^{3+2}(a_1) = \sigma^2\big(\sigma^3(a_1)\big) = \sigma^2(a_1) = a_3,\end{aligned}$$

et donc, $\sigma^3 = \mathsf{Id}$, comme demandé. Ainsi, σ est d'ordre 3 dans le groupe $\mathfrak{S}(E)$, lequel est d'ordre — de cardinal — $9! = 362\,880$.

(b) Comme $\mathsf{Id} = \sigma^3 = \sigma^2 \circ \sigma$, il est clair que $\sigma^{-1} = \sigma^2$.

(c) Comme chacune des trois permutations u, v, w est produit de 3-cycles à supports *disjoints :*

$$\begin{aligned}u &= u_1 \circ u_2 \circ u_3,\\ v &= v_1 \circ v_2,\\ w &= w_1 \circ w_2 \circ w_3,\end{aligned}$$

les 3-cycles de chacune de ces trois lignes commutent entre eux, et donc, pour tout entier $m \in \mathbb{Z}$, on a, grâce à une proposition connue démontrée en cours :

$$\begin{aligned}u^m &= u_1^m \circ u_2^m \circ u_3^m,\\ v^m &= v_1^m \circ v_2^m,\\ w^m &= w_1^m \circ w_2^m \circ w_3^m.\end{aligned}$$

Enfin les u_i, v_i, w_i étant *tous* des 3-cycles, la Question **(a)** donne :

$$\begin{aligned}u^3 &= u_1^3 \circ u_2^3 \circ u_3^3 = \mathsf{Id} \circ \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id},\\ v^3 &= v_1^3 \circ v_2^3 = \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id},\\ w^3 &= w_1^3 \circ w_2^3 \circ w_3^3 = \mathsf{Id} \circ \mathsf{Id} \circ \mathsf{Id} = \mathsf{Id}.\end{aligned}$$

(d) En lisant du bas vers le haut la permutation :

$$w \quad \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\ 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \end{array}$$

on écrit son inverse :

$$w^{-1} \quad \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\ 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

Puis, en écrivant :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 2 & 3 & 5 & 6 & 4 & 8 & 9 & 7 \end{array}$$

on peut composer :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ w^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 7 & 8 & 9 & 1 & 2 & 3 & 4 & 5 & 6 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 8 & 9 & 7 & 1 & 2 & 3 & 5 & 6 & 4 \\ w & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 4 & 5 & 6 & 8 & 9 & 7 \end{array}$$

ce qui montre bien que :

$$w \circ v \circ w^{-1} \;=\; (1\ 2\ 3) \circ (7\ 8\ 9).$$

(e) Grâce au fait qu'on a déjà fait le travail de détermination de w^{-1}, et qu'on a déjà explicité v, w, il suffit d'élaborer le tableau de composition :

$$\begin{array}{cccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ w & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 5 & 6 & 7 & 8 & 9 & 1 & 2 & 3 \\ v & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 6 & 4 & 8 & 9 & 7 & 1 & 2 & 3 \\ w^{-1} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 5 & 6 & 4 & 7 & 8 & 9 \end{array}$$

ce qui donne :

$$w^{-1} \circ v \circ w \;=\; (1\ 2\ 3) \circ (4\ 5\ 6).$$

(f) L'idée-clé, suggérée ici, était de remplacer w au centre par w^{-2}, ce que la Question **(b)** suggérait à l'avance :

$$\begin{aligned} \big(w \circ v\big)^2 \circ w \;&=\; w \circ v \circ \underline{w}_{\text{rpl}} \circ v \circ w \\ &=\; w \circ v \circ w^{-2} \circ v \circ w \\ &=\; \big(w \circ v \circ w^{-1}\big) \circ \big(w^{-1} \circ v \circ w\big) \\ \text{[Questions (d) et (e)]} \qquad &=\; (1\ 2\ 3) \circ (7\ 8\ 9) \circ (1\ 2\ 3) \circ (4\ 5\ 6) \\ \text{[Commutation disjointe]} \qquad &=\; (1\ 2\ 3)^2 \circ (4\ 5\ 6) \circ (7\ 8\ 9) \\ \text{[Commutation disjointe]} \qquad &=\; \Big((1\ 2\ 3) \circ (4\ 5\ 6) \circ (7\ 8\ 9)\Big)^2 \circ \Big((4\ 5\ 6) \circ (7\ 8\ 9)\Big)^{-1} \\ \text{[Reconnaître]} \qquad &=\; u^2 \circ v^{-1} \qquad\qquad \text{OUI !} \end{aligned}$$

(g) On déduit de la Question **(f)**, en utilisant $u^2 = u^{-1}$, que :

$$\begin{aligned} \big(w \circ v\big)^3 \;&=\; u^2 \\ &=\; u^{-1}, \end{aligned}$$

donc :

$$\big(w \circ v\big)^{-3} \;=\; u.$$

Exercice 3. **(a)** Écrivons, puis factorisons :

$$\begin{aligned} x^4 + x^2 + 1 &= \left(x^2+1\right)^2 - x^2 \\ &= \left(x^2+1-x\right)\left(x^2+1+x\right). \end{aligned}$$

Les discriminants de ces deux trinômes du second degré étant < 0, ils sont tous deux irréductibles.

D'après un théorème du cours, il existe des inconnues $a, b, c, d \in \mathbb{R}$, telles que :

$$\frac{x}{(x^2-x+1)\,(x^2+x+1)} = \frac{a\,x+b}{x^2-x+1} + \frac{c\,x+d}{x^2+x+1}.$$

Après élimination des dénominateurs, il vient :

$$\begin{aligned} x &= (a\,x+b)\,(x^2+x+1) + (c\,x+d)\,(x^2-x+1) \\ &= a\,x^3 + a\,x^2 + a\,x \qquad\qquad + c\,x^3 - c\,x^2 + c\,x \\ &\qquad + b\,x^2 + b\,x + b \qquad\qquad + d\,x^2 - d\,x + d \\ &= (a+c)\,x^3 + (a+b-c+d)\,x^2 + (a+b+c-d)\,x + b + d. \end{aligned}$$

Il s'agit donc d'un système linéaire :

$$\begin{aligned} 0 &= a+c, \\ 0 &= a+b-c+d, \\ 1 &= a+b+c-d, \\ 0 &= b+d. \end{aligned}$$

Résolvons $a = -c$ et $d = -b$ depuis les équations 1 et 4, puis, remplaçons ces valeurs dans les équations 2 et 3 :

$$\begin{array}{llllll} 0 = -c+b-c-b = -2\,c, & \text{d'où} & 0 = c, & \text{puis} & 0 = a \\ 1 = -c+b+c+b = 2\,b, & \text{d'où} & \frac{1}{2} = b, & \text{puis} & -\frac{1}{2} = d. \end{array}$$

En conclusion :

$$\frac{x}{x^4+x^2+1} = \frac{1/2}{x^2-x+1} + \frac{-1/2}{x^2+x+1}.$$

(b) Si p est réductible, puisque $2 = 1+1$ est la seule possibilité au niveau des degrés, il se factorise :

$$p(x) = (x-\alpha)\,(x-\beta),$$

en un produit de deux polynômes unitaires de degré 1, à coefficients dans $\mathbb{K}$. Mais alors, α et β sont des racines dans $\mathbb{K}$ de p.

S'il existe $\alpha \in \mathbb{K}$ tel que $p(\alpha) = 0$, on a vu dans le cours que le polynôme se factorise par $(x-\alpha)$:

$$p(x) = (x-\alpha)\,q(x),$$

avec un polynôme $q(x)$ de degré 1, unitaire, à coefficients dans $\mathbb{K}$, donc de la forme $x-\beta$. Ainsi, $p(x) = (x-\alpha)\,(x-\beta)$ se décompose en produit de deux polynômes de degré 1 à coefficients dans $\mathbb{K}$, et on sait que tout polynôme de degré 1 est irréductible.

(c) Comme :

$$x^2 + \overline{4} = x^2 - \overline{1} = (x+\overline{1})\,(x-\overline{1}),$$

le premier facteur au numérateur est réductible en deux facteurs de degré 1.

Par ailleurs, modulo 5, les carrés des éléments $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ de $\mathbb{Z}/5\mathbb{Z}$ sont égaux à $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{4}$, $\overline{1}$. Aucun n'est égal à $-\,\overline{3} = \overline{2}$. Donc le polynôme $x^2 + \overline{3}$ n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$.

L'équivalence contraposée de la Question **(a)** nous permet de conclure que $p(x)$ est irréductible.

(d) D'après un théorème du cours, comme le degré du numérateur est $<$ le degré du dénominateur, on doit avoir une décomposition en éléments simples du type :

$$\frac{x+\overline{3}}{(x+\overline{1})\,(x+\overline{4})\,(x^2+\overline{3})} \;=\; \frac{a\,x+b}{x^2+\overline{3}} + \frac{c}{x+\overline{1}} + \frac{d}{x+\overline{4}},$$

avec certaines constantes inconnues $a, b, c, d \in \mathbb{Z}/5\mathbb{Z}$.

Éliminons les dénominateurs :

$$\begin{aligned} x+\overline{3} \;&=\; (a\,x+b)\,(x+\overline{1})\,(x+\overline{4}) + c\,(x^2+\overline{3})\,(x+\overline{4}) + d\,(x^2+\overline{3})\,(x+\overline{1}) \\ &=\; (a\,x+b)\,(x^2+\overline{4}) + c\,\big(x^3+\overline{4}\,x^2+\overline{3}\,x+\overline{2}\big) + d\,\big(x^3+x^2+\overline{3}\,x+\overline{3}\big) \\ &=\; (a+c+d)\,x^3 + (b+\overline{4}\,c+d)\,x^2 + (\overline{4}\,a+\overline{3}\,c+\overline{3}\,d)\,x + \overline{4}\,b+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Par identification, il s'agit donc de résoudre le système linéaire suivant, à coefficients dans $\mathbb{Z}/5\mathbb{Z}$:

$$\begin{aligned} \overline{0} \;&=\; a+c+d, \\ \overline{0} \;&=\; b+\overline{4}\,c+d, \\ \overline{1} \;&=\; \overline{4}\,a+\overline{3}\,c+\overline{3}\,d, \\ \overline{3} \;&=\; \overline{4}\,b+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Remplaçons $a = -\,c - d$ depuis l'équation 1 dans les équations 2, 3, 4 :

$$\begin{aligned} \overline{0} \;&=\; b+\overline{4}\,c+d, \\ \overline{1} \;&=\; -\,\overline{4}\,c-\overline{4}\,d+\overline{3}\,c+\overline{3}\,d \;=\; \overline{4}\,c+\overline{4}\,d, \\ \overline{3} \;&=\; \overline{4}\,d+\overline{2}\,c+\overline{3}\,d. \end{aligned}$$

Remplaçons $d = -\,b - \overline{4}\,c = \overline{4}\,b + c$:

$$\begin{aligned} \overline{1} \;&=\; \overline{4}\,c+\overline{16}\,b+\overline{4}\,c \;=\; \overline{3}\,c+b, \\ \overline{3} \;&=\; \overline{4}\,b+\overline{2}\,c+\overline{12}\,b+\overline{3}\,c \;=\; b, \end{aligned}$$

puis résolvons :

$$b \;=\; \overline{3}, \qquad\qquad c \;=\; \overline{1},$$

et enfin :

$$d \;=\; \overline{3}, \qquad\qquad a \;=\; \overline{1}.$$

En conclusion, nous avons trouvé la décomposition en éléments simples :

$$\frac{x+\overline{3}}{(x+\overline{1})\,(x+\overline{4})\,(x^2+\overline{3})} \;=\; \frac{x+\overline{3}}{x^2+\overline{3}} + \frac{\overline{1}}{x+\overline{1}} + \frac{\overline{3}}{x+\overline{4}}.$$

5. Examen 3

Exercice 1. Dans le groupe $\mathfrak{S}_7$ des permutations de l'ensemble $\{1,2,3,4,5,6,7\}$, on considère :

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 6 & 3 & 1 & 2 \end{pmatrix}.$$

(a) Décomposer σ en produit de cycles à supports disjoints.

(b) Déterminer l'ordre de σ.

(c) Calculer $\tau := \sigma^{425}$.

(d) Calculer la signature de σ, puis celle de τ.

Exercice 2. On rappelle que l'on note $\varphi(n)$ le nombre d'entiers $1 \leqslant k \leqslant n$ qui sont premiers avec un entier donné $n \geqslant 1$, où par convention $\varphi(1) = 1$ car 1 est premier avec lui-même.

(a) Calculer $\varphi(135)$.

(b) Déterminer le reste de la division euclidienne de 7^{7202} par 135.

(c) Déterminer le cardinal de l'ensemble $\big(\mathbb{Z}/15\,\mathbb{Z}\big)^{\times}$ des éléments inversibles pour la multiplication $\times$ de l'anneau $\big(\mathbb{Z}/15\,\mathbb{Z},\ +,\times\big)$.

(d) Déterminer les ordres des deux éléments $\overline{2}$ et $\overline{7}$ dans le groupe abélien $\big((\mathbb{Z}/15\,\mathbb{Z})^{\times},\ \times\big)$.

(e) Ce groupe $\big((\mathbb{Z}/15\,\mathbb{Z})^{\times},\ \times\big)$ est-il cyclique ?

Exercice 3. Soit $\big(A,+,\times\big)$ un anneau commutatif dans lequel $a+a = 0_A$ pour tout élément $a \in A$.

(a) Montrer que pour tous a et b dans A, on a l'identité $(a+b)^2 = a^2 + b^2$.

(b) Montrer que l'application $\psi\colon A \longrightarrow A$ définie par $\psi(a) := a^2$ est un morphisme d'anneaux.

(c) On suppose dorénavant que A est intègre. Montrer que ψ est une application injective.

(d) En supposant de plus que A est de cardinal fini, montrer que pour tout $a \in A$, il existe $b \in A$ tel que $b^2 = a$.

Exercice 4. **(a)** Calculer le quotient et le reste de la division euclidienne de $X^4 + 5\,X^3 + 12\,X^2 + 20\,X - 6$ par $X^2 + 3\,X - 1$.

(b) Déterminer le pgcd entre $X^4 + 5\,X^3 + 12\,X^2 + 20\,X - 6$ et $X^2 + 3\,X - 1$.

Exercice 5. **(a)** Factoriser le polynôme $X^2 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$, puis décomposer en éléments simples $\frac{1}{X^2-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(b) Factoriser le polynôme $X^4 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(c) Décomposer en éléments simples $\frac{1}{X^4-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(d) Factoriser le polynôme $X^4 + 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(e) Décomposer en éléments simples $\frac{1}{X^4+1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

(f) Vérifier que :

$$\frac{1}{X^8-1} = \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{1/2}{X^4+1}.$$

(g) Factoriser le polynôme X^8-1 en produit de polynômes irréductibles dans $\mathbb{R}[X]$.

(h) Décomposer en éléments simples $\frac{1}{X^8-1}$ sur $\mathsf{Frac}\,\mathbb{R}[X]$.

6. Corrigé de l'examen 3

Exercice 1. (a) Comme on a :

$$\begin{aligned} 1 &\longmapsto 4 \longmapsto 6 \longmapsto 1, \\ 2 &\longmapsto 7 \longmapsto 2, \\ 3 &\longmapsto 5 \longmapsto 3, \end{aligned}$$

la décomposition de Σ en produit de cycles à supports disjoints est :

$$\sigma \,=\, \big(1\ 4\ 6\big)\,\big(2\ 7\big)\,\big(3\ 5\big).$$

(b) Ainsi, la permutation σ est le produit d'un 3-cycle et de deux 2-cycles [4] (transpositions), à supports disjoints. D'après le cours, son ordre vaut donc :

$$\boldsymbol{o}(\sigma) \,=\, \mathsf{ppcm}\,(3,2,2) \,=\, 6.$$

(c) Puisque $\sigma^6 = \mathsf{Id}$, effectuons la division de 425 par 6 :

$$425 \,=\, 6\cdot 70 + 5,$$

d'où :

$$\begin{aligned} \tau \,=\, \sigma^{425} \,=\, \big(\sigma^6\big)^{70}\circ\sigma^5 \,=\, \sigma^5 \,&=\, \sigma^{-1} \\ &=\, \big(1\ 6\ 4\big)\,\big(2\ 7\big)\,\big(3\ 5\big). \end{aligned}$$

(d) Rappelons que la signature $\varepsilon(\bullet)$ est un morphisme de groupes du groupe $\mathfrak{S}_n$ des permutations d'un ensemble à $n \geqslant 1$ éléments à valeurs dans $\big(\{\pm 1\},\times\big)$.

Rappelons aussi que la signature d'un cycle de longueur $p \geqslant 2$ vaut $(-1)^p$. Par conséquent :

$$\begin{aligned} \varepsilon(\sigma) \,&=\, \varepsilon\big((1\,4\,6)\,(2\,7)\,(3\,5)\big) \,=\, (-1)^{3-1}\,(-1)^{2-1}\,(-1)^{2-1} \,=\, 1, \\ \varepsilon(\tau) \,&=\, \varepsilon\big((1\,6\,4)\,(2\,7)\,(3\,5)\big) \,=\, 1. \end{aligned}$$

D'ailleurs, on sait généralement que la multiplicativité $\varepsilon\big(\sigma_1\sigma_2\big) \,=\, \varepsilon(\sigma_1)\,\varepsilon(\sigma_2)$ dans $\mathfrak{S}_n$ implique que $\varepsilon\big(\sigma^{-1}\big) = \frac{1}{\varepsilon(\sigma)}$ pour toute permutation $\sigma \in \mathfrak{S}_n$, et ici, $\frac{1}{1} = 1$.

Exercice 2. (a) D'après un théorème du cours, la fonction indicatrice d'Euler $\varphi(\bullet)$ est multiplicative sur les nombres premiers entre eux, et si un entier $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ est décomposé en facteurs premiers, on a :

$$\begin{aligned} \varphi(n) \,&=\, \varphi\big(p_1^{\alpha_1}\big)\cdots\varphi\big(p_r^{\alpha_r}\big) \\ &=\, \big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\big)\cdots\big(p_r^{\alpha_r} - p_r^{\alpha_r-1}\big). \end{aligned}$$

Ici, comme :

$$135 \,=\, 3^3\cdot 5,$$

il vient :

$$\varphi(135) \,=\, \big(3^3 - 3^2\big)\,\big(5^1 - 5^0\big) \,=\, 18\cdot 4 \,=\, 72.$$

4. — un $2\times 2 =$ quadricyle ! ? —

(b) Heureusement que 7 est premier avec $135 = 3^3\,5$, car un théorème d'Euler (qui généralise le Petit Théorème de Fermat) peut être appliqué :

$$7^{\varphi(135)} \equiv 1 \mod 135, \qquad \text{c'est-à-dire :} \qquad 7^{72} \equiv 1 \mod 135.$$

On peut vérifier sur ordinateur que 36 est l'exposant minimal $\geqslant 1$ satisfaisant $7^{36} \equiv 1 \mod 135$, mais cela n'était pas demandé, et d'ailleurs, il vaut mieux faire notre petite affaire légère avec 72, puisque l'observation aisée $7200 = 72 \cdot 100$ nous permet de déterminer le reste de la division euclidienne de 7^{7202} par 135 :

$$7^{7202} = \left(7^{72}\right)^{100} \cdot 7^2 \equiv 1 \cdot 7^2 \mod 135 \equiv 49 \mod 135.$$

(c) D'après le théorème du cours susmentionné :

$$\mathsf{Card}\left(\mathbb{Z}/15\mathbb{Z}\right)^\times = \varphi(15) = \varphi(3^1 \cdot 5^1) = \left(3^1 - 3^0\right)\left(5^1 - 5^0\right) = 8.$$

(d) Puisque modulo 15 :

$$\overline{2}^2 \equiv \overline{4} \not\equiv \overline{1}, \qquad \overline{2}^3 \equiv \overline{8} \not\equiv \overline{1}, \qquad \overline{2}^4 \equiv \overline{16} \equiv \overline{1},$$

l'ordre de $\overline{2}$ vaut 4.

De même, puisque modulo 15 :

$$\overline{7}^2 \equiv \overline{49} \equiv \overline{4} \not\equiv \overline{1}, \qquad \overline{7}^3 \equiv \overline{4}\cdot\overline{7} \equiv \overline{28} \equiv -\overline{2} \not\equiv \overline{1}, \qquad \overline{7}^4 \equiv \left(-\overline{2}\right)\cdot\overline{7} = -\overline{14} \equiv \overline{1},$$

l'ordre de $\overline{7}$ vaut 4, aussi !

(e) D'après un théorème du cours, ce groupe $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$ est cyclique si et seulement si l'un au moins de ses 8 éléments est d'ordre égal à son cardinal, 8.

On vérifie manuellement que les 8 éléments en question de $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$ sont :

$$\overline{1}, \quad \overline{2}, \quad \overline{4}, \quad \overline{7}, \quad \overline{8}, \quad \overline{11}, \quad \overline{13}, \quad \overline{14},$$

puisque, dans $\mathbb{Z}/15\mathbb{Z}$:

$$\overline{1} = \overline{1}\cdot\overline{1} = \overline{2}\cdot\overline{8} = \overline{4}\cdot\overline{4} = \overline{7}\cdot\overline{13} = \overline{8}\cdot\overline{2} = \overline{11}\cdot\overline{11} = \overline{13}\cdot\overline{7} = \overline{14}\cdot\overline{14}.$$

Parmi ces 8 éléments, on vient de voir que $\overline{2}$ et $\overline{7}$ ne peuvent pas convenir, car il sont tous deux d'ordre $4 < 8$. Évidemment, $\overline{1}$ d'ordre 1 et $\overline{14} = -\overline{1}$ d'ordre 2 ne peuvent pas convenir non plus.

Restent encore $\overline{4}$, $\overline{8}$, $\overline{11}$, $\overline{13}$: l'un d'entre eux est-il d'ordre 8 ? Hélas non, car avec un peu d'astuce pour utiliser la Question **(d)**, on calcule :

$$\begin{aligned}
\overline{4}^4 &= \left(\overline{2}^2\right)^4 = \left(\overline{2}^4\right)^2 = \overline{1}, \\
\overline{8}^4 &= \left(\overline{2}^3\right)^4 = \left(\overline{2}^4\right)^3 = \overline{1}, \\
\overline{11}^4 &= \left(-\overline{4}\right)^4 = \left(\overline{4}\right)^4 = \overline{1}, \\
\overline{13}^4 &= \left(-\overline{2}\right)^4 = \left(\overline{2}\right)^4 = \overline{1}.
\end{aligned}$$

En définitive, *tous* les 8 éléments de $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$ sont d'ordre égal à 4 ou divisant 4, et donc, aucun ne peut être d'ordre 8. Ceci démontre que $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$ n'est *pas* cyclique. Quelle déception !

Exercice 3. **(a)** C'est très simple :

$$\big(a+b\big)^2 \;=\; a^2+ab+ba+b^2 \;=\; a^2+\underline{ab+ab}_{\circ}+b^2 \;=\; a^2+0_A+b^2 \;=\; a^2+b^2.$$

(b) Cela est aisé, avec $a, b \in A$ quelconques :

$$\begin{aligned}\psi(a+b) \;&=\; \big(a+b\big)^2 \;=\; a^2+b^2 \;=\; \psi(a)+\psi(b),\\ \psi\big(a\,b\big) \;&=\; (ab)^2 \;=\; ab\,ab \;=\; aa\,bb \;=\; a^2\,b^2 \;=\; \psi(a)\,\psi(b),\\ \psi(1_A) \;&=\; 1_A^2 \;=\; 1_A.\end{aligned}$$

(c) Avec $a, b \in A$ satisfaisant $\psi(a) = \psi(b)$:

$$a^2 \;=\; b^2 \qquad\qquad \Longleftrightarrow \qquad\qquad (a-b)\,(a+b) \;=\; 0_A,$$

l'hypothèse d'intégrité de A donne $a = b$ — super ! c'est ce qu'on veut pour l'injectivité de ψ ! —, ou $a = -\,b$, mais comme on peut ajouter à droite $0_A = b + b$, il vient aussi dans ce deuxième cas :

$$a \;=\; -\,b \;=\; -\,b+b+b \;=\; b.$$

(d) Notre morphisme ψ est donc une application *injective* de l'anneau *fini* A dans lui-même. D'après la théorie élémentaire des ensembles, ceci implique automatiquement que ψ est surjective (et bijective).

Autrement dit, tout $a \in A$, possède un antécédant $b \in A$ tel que $a = \psi(b) = b^2$.

Exercice 4. **(a)** On trouve :

$$X^4+5\,X^3+12\,X^2+20\,X-6 \;=\; \big(X^2+3\,X-1\big)\,\big[X^2+2\,X+7\big]+X+1.$$

(b) D'après l'algorithme d'Euclide, il faut continuer à diviser par le reste obtenu :

$$X^3+3\,X-1 \;=\; (X+1)\,[X+2]-3.$$

En une seule étape supplémentaire, nous trouvons alors un reste non nul -3 de degré zéro. Par conséquent, le pgcd recherché vaut 1 : ces deux polynômes sont premiers entre eux.

Exercice 5. **(a)** Il est clair que $X^2-1 = (X-1)(X+1)$, et on trouve aisément :

$$\frac{1}{X^2-1} \;=\; \frac{1/2}{X-1}-\frac{1/2}{X+1},$$

ce qui se vérifie en réduisant visuellement le membre de droite au même dénominateur.

(b) Dans $\mathbb{R}[x]$, on factorise facilement :

$$X^4-1 \;=\; (X-1)\,(X+1)\,(X^2+1).$$

(c) Ensuite, avec la méthode des coefficients indéterminés :

$$\frac{1}{X^4-1} \;=\; \frac{a}{X-1}+\frac{b}{X+1}+\frac{c\,X+d}{X^2+1},$$

où a, b, c, d sont des inconnues, après multication globale par X^4-1, on obtient un système linéaire que l'on résout, pour trouver :

$$\frac{1}{X^4-1} \;=\; \frac{1/4}{X-1}-\frac{1/4}{X+1}-\frac{1/2}{X^2+1}.$$

(d) Attention ! Ce n'est pas parce que la fonction réelle $x \longmapsto x^4+1$ ne prend que des valeurs $\geqslant 1$ sur $\mathbb{R}$ et donc n'a aucune racine sur $\mathbb{R}$ que le polynôme X^4+1 ne se décompose pas en facteurs irréductibles de degrés < 4 !

Et d'ailleurs, on est certain que ce polynôme de degré *doit* se décomposer en facteurs irréductibles non triviaux, car un théorème du cours stipule que dans $\mathbb{R}[X]$, les polynômes irréductibles sont tous de degré égal à $1 < 4$, ou à $2 < 4$.

Par une astuce vue dans le polycopié, faisons apparaître une différence entre deux carrés :

$$\begin{aligned} X^4+1 &= (X^2+1)^2 - 2\,X^2 \\ &= \big(X^2+1-\sqrt{2}\,X\big)\big(X^2+1+\sqrt{2}\,X\big), \end{aligned}$$

et observons que les discriminants des deux facteurs trouvés :

$$\big(\mp\sqrt{2}\big)^2 - 4 = -2 < 0,$$

sont strictement négatifs, ce qui garantit que ces deux facteurs sont irréductibles sur $\mathbb{R}$.

(e) Ensuite, avec la méthode des coefficients indéterminés :

$$\frac{1}{X^4+1} = \frac{a\,X+b}{X^2-\sqrt{2}\,X+1} + \frac{c\,X+d}{X^2+\sqrt{2}\,X+1},$$

où a, b, c, d sont des inconnues, on trouve :

$$\frac{1}{X^4+1} = \frac{-\frac{1}{2\sqrt{2}}\,X+\frac{1}{2}}{X^2-\sqrt{2}\,X+1} + \frac{\frac{1}{2\sqrt{2}}\,X+\frac{1}{2}}{X^2+\sqrt{2}\,X+1}.$$

(f) Cela s'effectue par un calcul direct.

(g) Grâce à ce qui précède :

$$\begin{aligned} X^8-1 &= \big(X^4-1\big)\big(X^4+1\big) \\ &= (X-1)(X+1)(X^2+1)\big(X^2+1-\sqrt{2}\,X\big)\big(X^2+1+\sqrt{2}\,X\big). \end{aligned}$$

(h) On procède comme suit :

$$\begin{aligned} \frac{1}{X^8-1} &= \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{1/2}{X^4+1} \\ &= \frac{1/8}{X-1} - \frac{1/8}{X+1} - \frac{1/4}{X^2+1} - \frac{-\frac{1}{4\sqrt{2}}\,X+\frac{1}{4}}{X^2-\sqrt{2}\,X+1} - \frac{\frac{1}{4\sqrt{2}}\,X+\frac{1}{4}}{X^2+\sqrt{2}\,X+1}. \end{aligned}$$

7. Examen 4

Exercice 1. On travaille dans l'anneau commutatif $\big(\mathbb{Z}/p\mathbb{Z}, +, \times\big)$ avec le nombre (magique) $p := 17$.

(a) Calculer le reste de la division euclidienne de $16 \cdot 15 \cdot 14$ par 17.

(b) Dans $\mathbb{Z}\big/17\mathbb{Z}$, calculer $\overline{2}^1$, $\overline{2}^2$, $\overline{2}^3$, $\overline{2}^4$, $\overline{2}^5$, $\overline{2}^6$, $\overline{2}^7$, $\overline{2}^8$.

(c) Déterminer le reste de la division euclidienne du nombre (magique) 2^{2222} par 17.

Exercice 2. On s'intéresse à des systèmes linéaires à coefficients entiers, dont on recherche les solutions entières, exclusivement.

(a) Résoudre dans $\mathbb{Z}^2$ l'équation :

$$-15\,x + 6\,y + 9 \;=\; 0.$$

(b) En déduire les solutions dans $\mathbb{Z}^3$ du système :

$$\begin{cases} 0 \;=\; -3\,x + 8\,y - 2\,z - 11, \\ 0 \;=\; 6\,x + y - z - 10. \end{cases}$$

Exercice 3. Soient deux groupes G et H, et soit $f\colon G \longrightarrow H$ un morphisme de groupes.

(a) Montrer que si un élément $x \in G$ est d'ordre fini égal à un certain entier $1 \leqslant m$, alors son image $f(x) \in H$ est aussi un élément d'ordre fini, que l'on notera $1 \leqslant n$.

(b) Justifier que $n \,|\, m$.

(c) Déterminer tous les morphismes de groupes additifs, de $G := \mathbb{Z}\big/11\mathbb{Z}$ à valeurs dans $H := \mathbb{Z}\big/23\mathbb{Z}$.

Exercice 4. **(a)** Montrer que le groupe $\big(\mathbb{Z}/14\mathbb{Z}\big)^\times$ des éléments inversibles pour la multiplication $\times$ dans l'anneau $\big(\mathbb{Z}/14\mathbb{Z}, +, \times\big)$ a pour éléments :

$$\big(\mathbb{Z}/14\mathbb{Z}\big)^\times \;=\; \big\{\overline{1},\, \overline{3},\, \overline{5},\, \overline{9},\, \overline{11},\, \overline{13}\big\}.$$

(b) Calculer, dans $\mathbb{Z}/14\mathbb{Z}$:

$$\overline{5}^0, \quad \overline{5}^1, \quad \overline{5}^2, \quad \overline{5}^3, \quad \overline{5}^4, \quad \overline{5}^5, \quad \overline{5}^6.$$

(c) Montrer que l'application :

$$\begin{array}{rccc} \varphi\colon & \big(\mathbb{Z}/6\mathbb{Z}, +\big) & \longrightarrow & \big((\mathbb{Z}/14\mathbb{Z})^\times, \times\big) \\ & \overline{c} \;=\; c \mod 6 & \longmapsto & \overline{5}^c, \end{array}$$

est bien définie, et est un *isomorphisme* de groupes.

(d) Montrer que $(\mathbb{Z}/14\mathbb{Z})^\times$ est un groupe cyclique.

(e) Le groupe $(\mathbb{Z}/12\mathbb{Z})^\times$ est-il cyclique ?

Exercice 5. On fixe un entier premier $p \geqslant 2$, on prend un entier relatif $a \in \mathbb{Z}$ qui n'est *pas* divisible par p, on introduit l'entier :

$$\mathrm{N} := 1\,a \cdot 2\,a \cdot 3\,a \cdots (p-1)\,a,$$

et on se propose d'évaluer $\mathrm{N} \bmod p$ de deux manières différentes afin de redémontrer le Petit Théorème de Fermat.

(a) Vérifier que :

$$\mathrm{N} \equiv (p-1)!\,a^{p-1} \mod p.$$

(b) Pour k entier avec $1 \leqslant k \leqslant p-1$, on note r_k le reste de la division euclidienne de $k\,a$ par p, c'est-à-dire $k\,a = q_k\,p + r_k$ avec $0 \leqslant r_k \leqslant p-1$. Montrer qu'aucun reste r_k ne peut être nul.

(c) Montrer que les deux restes r_{k_1} et r_{k_2} associés à deux entiers quelconques $1 \leqslant k_1, k_2 \leqslant p-1$ satisfont :

$$0 \leqslant \left|r_{k_1} - r_{k_2}\right| \leqslant p-1.$$

(d) Établir qu'à deux entiers distincts $1 \leqslant k_1 \neq k_2 \leqslant p-1$ sont associés deux restes $r_{k_1} \neq r_{k_2}$ eux aussi *distincts*.

(e) En déduire que :

$$r_1 \cdots r_{p-1} = (p-1)!.$$

(f) Établir que :

$$a^{p-1} \equiv 1 \mod p.$$

Exercice 6. On rappelle que l'on note $\varphi(n)$ le nombre d'entiers $1 \leqslant k \leqslant n$ qui sont premiers avec un entier donné $n \geqslant 1$, où par convention $\varphi(1) = 1$ car 1 est premier avec lui-même.

(a) Avec $p \geqslant 2$ premier, et avec un exposant $r \geqslant 1$, que vaut $\varphi\big(p^r\big)$? Indication: Il suffit d'écrire la réponse sans la justifier, car c'est une question de cours. En cas d'oubli, il est évidemment autorisé de raisonner pour retrouver la valeur de $\varphi\big(p^r\big)$.

(b) Soient trois nombres premiers $2 < p_1 < p_2 < p_3$. On pose $m := p_1^3\,p_2^5$ et $n := p_2^7\,p_3$. Montrer que :

$$\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} = \frac{p_2}{\varphi(p_2)}.$$

(c) Généralement, soient deux nombres entiers quelconques $m, n \geqslant 1$ écrits sous la forme :

$$m = \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i} \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k},$$
$$n = \prod_{1 \leqslant i \leqslant r} p_i^{\beta_i} \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell},$$

avec des nombres premiers deux à deux distincts $p_1, \ldots, p_r$, $P_1, \ldots, P_{\mathrm{K}}$, $Q_1, \ldots, Q_{\mathrm{L}}$, avec des exposants strictement positifs :

$$\alpha_1, \ldots, \alpha_r \geqslant 1, \qquad a_1, \ldots, a_{\mathrm{K}} \geqslant 1,$$
$$\beta_1, \ldots, \beta_r \geqslant 1, \qquad b_1, \ldots, b_{\mathrm{L}} \geqslant 1,$$

de telle sorte que :

$$\mathsf{pgcd}\,(m,\,n) = \prod_{1 \leqslant i \leqslant r} p_i^{\min(\alpha_i, \beta_i)}.$$

Montrer que :

$$\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} = \frac{p_1 \cdots p_r}{(p_1 - 1) \cdots (p_r - 1)}.$$

Indication: Chercher à imiter le raisonnement de la question qui précède.

Exercice 7. (a) Soit $n = a\,b$ un entier composé, *i.e.* avec $1 < a < n$ et $1 < b < n$. On exclut $n = 4$, *i.e.* on suppose que $n \geqslant 5$. Montrer que $(n-1)!$ est divisible par n. Indication: On pourra par exemple observer (et justifier) que $n > a + b$, puis utiliser le fait que $\frac{(a+b)!}{a!\,b!} \in \mathbb{N}$ est entier.

8. Corrigé de l'examen 4

Exercice 1. (a) Il s'agit seulement de lire ce produit modulo 17, et il vaut :

$$16 \cdot 15 \cdot 14 \equiv (-1) \cdot (-2) \cdot (-3) \equiv -6 \equiv 11 \mod 17.$$

(b) Il vient :

$$\begin{aligned}
\overline{2}^1 &= \overline{2}, \\
\overline{2}^2 &= \overline{4}, \\
\overline{2}^3 &= \overline{8}, \\
\overline{2}^4 &= \overline{16} = -\overline{1}, \\
\overline{2}^5 &= -\overline{1} \cdot \overline{2} = -\overline{2} = \overline{15}, \\
\overline{2}^6 &= -\overline{2} \cdot \overline{2} = -\overline{4} = \overline{13}, \\
\overline{2}^7 &= -\overline{4} \cdot \overline{2} = -\overline{8} = \overline{9}, \\
\overline{2}^8 &= -\overline{8} \cdot \overline{2} = -\overline{16} = \overline{1}.
\end{aligned}$$

(c) Ah, super ! On vient de constater que $2^8 \equiv 1 \mod 17$, donc divisons 2222 par 8 :

$$2222 = 277 \cdot 8 + 6,$$

pour engranger rapidement les points :

$$\overline{2}^{2222} = \left(\overline{2}^8\right)^{277} \overline{2}^6 = \overline{1}^{277}\, \overline{13} = \overline{13}.$$

Exercice 2. (a) Après division par 3, cette équation équivaut à :

$$-5\,x + 2\,y + 3 = 0.$$

Comme -5 et 2 sont premiers entre eux, un théorème du cours garantit qu'il existe une infinité de solutions, et d'ailleurs, ledit théorème décrit *toutes* les solutions.

L'idée de la démonstration est de deviner tout d'abord une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$. « *Au doigt et à l'œil* », on trouve :

$$-5 \cdot 1 + 2 \cdot 1 + 3 = 0.$$

Ensuite, on soustrait la solution particulière d'une solution générale éventuelle, afin de faire disparaître la constante 3, ce qui donne :

$$-5\,(x-1) + 2\,(y-1) = 0.$$

Comme $5 \wedge 2 = 1$, et comme ces deux nombres sont premiers, grâce au théorème d'Euclide, on trouve la solution générale :

$$x - 1 = 2\,\boldsymbol{k} \qquad \text{et} \qquad y - 1 = 5\,\boldsymbol{k},$$

avec $\boldsymbol{k} \in \mathbb{Z}$ arbitraire.

Par acquit de conscience, il est avisé de vérifier que la solution trouvée est bien solution de l'équation initiale :

$$\begin{aligned} 0 &\overset{?}{=} -15\big(1+2\boldsymbol{k}\big)+6\big(1+5\boldsymbol{k}\big)+9 \\ &= -15+6+9-15\cdot 2\boldsymbol{k}+6\cdot 5\boldsymbol{k} \qquad\qquad \text{OUI !} \end{aligned}$$

(b) Depuis la deuxième équation, résolvons :

$$z := 6\,x+y-10,$$

puis remplaçons cette valeur de z dans la première équation :

$$\begin{aligned} 0 &= -3\,x+8\,y-12\,x-2\,y+20-11 \\ &= -15\,x+6\,y+9. \end{aligned}$$

Eurêka ! C'est la Question **(a)** !

Ainsi, la solution générale est :

$$\begin{aligned} x &= 1+2\boldsymbol{k}, \\ y &= 1+5\boldsymbol{k}, \\ z &= 6\big(1+2\boldsymbol{k}\big)+1+5\boldsymbol{k}-10 \\ &= -3+17\boldsymbol{k}, \end{aligned}$$

toujours avec $\boldsymbol{k}\in\mathbb{Z}$ arbitraire.

Comme toujours, mieux vaut vérifier tout cela en injectant dans le système initial :

$$0 \overset{?}{=} -3\big(1+2\boldsymbol{k}\big)+8\big(1+5\boldsymbol{k}\big)-2\big(-3+17\boldsymbol{k}\big)-11 \qquad \text{OUI !}$$

$$0 \overset{?}{=} 6\big(1+2\boldsymbol{k}\big)+1\big(1+5\boldsymbol{k}\big)-1\big(-3+17\boldsymbol{k}\big)-10 \qquad \text{OUI !}$$

Exercice 3. (a) Comme $e_G=x^m$, comme le morphisme f envoie l'élément neutre e_G sur l'élément neutre e_H, et comme f respecte les lois de groupes, il est clair que l'on a :

$$e_H = f(e_G) = f\big(x^m\big) = \big(f(x)\big)^m$$

Par définition même, cette identité signifie que l'élément $y:=f(x)$ de H est d'ordre fini — mais pas forcément égal à m, éventuellement plus petit que m.

(b) Un théorème du cours a clairement fait voir, grâce à la division euclidienne standard dans $\mathbb{N}_{\geqslant 1}$, que si un élément $y\in H$ satisfait $y^m=e_H$, alors son ordre $o(y)$ — à savoir le plus petit exposant $\ell\geqslant 1$ tel que $y^\ell=e_H$ — *divise* m.

(c) Observons que $11\wedge 23=1$ sont premiers entre eux, ne serait-ce que parce que ce sont deux nombres premiers distincts !

Dans $\mathbb{Z}/p\,\mathbb{Z}$ avec p premier, nous savons que l'ordre de tout élément $\overline{a}$ non nul est exactement égal à p (tandis que $\overline{0}$ est trivialement d'ordre 1), parce que $\overline{a}$ additionné $\ell\geqslant 1$ fois avec lui-même donne $\ell\,\overline{a}$, avec $a\in\{1,2,\ldots,p-1\}$ premier avec p, donc $\overline{\ell\,a}$ vaut $\overline{0}$ si et seulement si $\ell\equiv 0 \bmod p$.

Attention ! Nous parlons d'un morphisme entre groupes *additifs*. Donc l'hypothèse est que $f(\overline{0})=\overline{0}$. et nous n'avons pas forcément $f(\overline{1})=\overline{1}$, puisque nous ne parlons pas de morphismes entre groupes *multiplicatifs*.

Étant donné un morphisme $f\colon \mathbb{Z}/11\mathbb{Z}\longrightarrow\mathbb{Z}/23\mathbb{Z}$, que peut valoir l'image $f(\overline{1})$? L'ordre de $\overline{1}$ vaut 11. Nous venons de dire que l'ordre de $f(\overline{1})$ doit alors diviser 11. Or

à moins que $f(\overline{1})$ ne soit égal à $\overline{0}$ dans $\mathbb{Z}/23\mathbb{Z}$, son ordre doit être égal à 23. Mais 23 ne divise pas 11 ! Donc :

$$f(\overline{1}) = \overline{0},$$

puis $f\big(\overline{1}+\overline{1}\big) = \overline{0}$, et ainsi de suite, pour conclure que :

$$f\big(\mathbb{Z}/11\mathbb{Z}\big) = \overline{0}.$$

Le morphisme est obligatoirement trivial !

Exercice 4. (a) D'après le cours, un élément non nul $\overline{a}$ de $\mathbb{Z}/14\mathbb{Z}$ avec $a \in \{1, 2, \ldots, 13\}$ est inversible pour la multiplication si et seulement si $a \wedge 14 = 1$. Comme $14 = 2 \cdot 7$, on élimine tous les multiples de 2 et/ou de 7, et il reste six éléments :

$$\mathbb{Z}/14\mathbb{Z} = \big\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\big\}.$$

(b) On trouve :

$$\overline{5}^0 = \overline{1}, \quad \overline{5}^1 = \overline{5}, \quad \overline{5}^2 = \overline{11}, \quad \overline{5}^3 = \overline{13}, \quad \overline{5}^4 = \overline{9}, \quad \overline{5}^5 = \overline{3}, \quad \overline{5}^6 = \overline{1},$$

et on constate qu'à la puissance sixième, on revient au point de départ.

(c) Il est clair que :

$$\overline{5}^0 = \overline{1},$$
$$\overline{5}^{c \bmod 6} \times \overline{5}^{c' \bmod 6} = \overline{5}^{c+c' \bmod 6},$$

puisque nous venons de voir que $\overline{5}^6 = \overline{1}$. Cette application φ est donc bien définie, et est un morphisme de groupes.

Qui plus est, φ est surjective grâce à la Question **(b)**. Comme les deux groupes $\mathbb{Z}/6\mathbb{Z}$ et $(\mathbb{Z}/14\mathbb{Z})^\times$ sont tous deux de cardinal égal à 6, ceci implique que φ est *bijective*. Ainsi, φ est bien un *isomorphisme de groupes*.

(d) Nous savons que les groupes additifs $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ sont cycliques, engendrés par $\overline{1}$, puisque $\overline{1}$ additionné k fois avec lui-même fournit l'élément $\overline{k}$ de $\mathbb{Z}/n\mathbb{Z}$, pour $k = 1, 2, \ldots, n-1$.

En particulier, $\big(\mathbb{Z}/6\mathbb{Z}, +\big)$ est cyclique.

Et comme φ est un *isomorphisme* de groupes, φ transmet instantanément cette propriété d'être cyclique à $(\mathbb{Z}/14\mathbb{Z})^\times$.

(e) Reprenons pas à pas les raisonnements que nous venons d'effectuer pour $(\mathbb{Z}/14\mathbb{Z})^\times$. Tout d'abord :

$$\big(\mathbb{Z}/12\mathbb{Z}\big)^\times = \big\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\big\}.$$

Ensuite, si $(\mathbb{Z}/12\mathbb{Z})^\times$ était cyclique, il existerait, parmi ses quatre éléments, un certain élément $\overline{a}$ dont les quatre puissances $\overline{a}^0$, $\overline{a}^1$, $\overline{a}^2$, $\overline{a}^3$ serait distinctes et décriraient tous les quatre éléments $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

Évidemment, $\overline{a} = \overline{1}$ ne marche pas, et les trois autres non plus, d'ailleurs, puisque :

$$\begin{aligned}
\overline{5}^0 &= \overline{1}, & \overline{5}^1 &= \overline{5}, & \overline{5}^2 &= \overline{1}, & \overline{5}^3 &= \overline{5},\\
\overline{7}^0 &= \overline{1}, & \overline{7}^1 &= \overline{7}, & \overline{7}^2 &= \overline{1}, & \overline{7}^3 &= \overline{7},\\
\overline{11}^0 &= \overline{1}, & \overline{11}^1 &= \overline{11}, & \overline{11}^2 &= \overline{1}, & \overline{11}^3 &= \overline{11}.
\end{aligned}$$

En conclusion, $(\mathbb{Z}/12\mathbb{Z})^\times$ n'est *pas* cyclique — *snif!*

Exercice 5. (a) C'est instantané, grâce à la commutativité de la multiplication dans $\mathbb{Z}$, cette relation étant d'ailleurs une égalité $\mathrm{N} = (p-1)!\, a^{p-1}$, que l'on « projette » ensuite modulo p.

(b) Par l'absurde, si un reste $r_k = 0$ était nul, on aurait $k\,a = q_k\,p + 0$, ce qui impliquerait que p divise $k\,a$. Or comme tous les entiers $k \in \{1, 2, \ldots, p-1\}$ sont premiers avec l'entier premier p car strictement inférieurs à p, le Théorème d'Euclide forcerait alors p à diviser a, ce qui contredirait l'hypothèse que a n'est *pas* divisible par p.

(c) Par définition du reste de la division euclidienne par p, avec deux entiers $k_1, k_2 \in \{1, \ldots, n\}$, nous avons :

$$\begin{aligned} 0 \leqslant r_{k_1} &\leqslant p-1, \\ 0 \leqslant r_{k_2} &\leqslant p-1, \end{aligned}$$

d'où par soustractions croisées — comme nous l'avons fait plusieurs fois en cours — :

$$0 - (p-1) \leqslant r_{k_1} - r_{k_2} \leqslant p - 1 - 0,$$

c'est-à-dire comme indiqué :

$$0 \leqslant \big|r_{k_1} - r_{k_2}\big| \leqslant p-1.$$

(d) Avec deux entiers distincts quelconques $1 \leqslant k_1 \neq k_2 \leqslant p-1$, écrivons modulo p :

$$\begin{aligned} k_1\,a &\equiv r_{k_1}, \\ k_2\,a &\equiv r_{k_2}, \end{aligned}$$

puis soustrayons :

$$\big(k_1 - k_2\big)\,a \equiv r_{k_1} - r_{k_2}.$$

Ensuite, observons par soustractions croisées entre :

$$\begin{aligned} 1 \leqslant k_1 &\leqslant p-1, \\ 1 \leqslant k_2 &\leqslant p-1, \end{aligned}$$

que :

$$1 - (p-1) \leqslant \underbrace{k_1 - k_2}_{\neq 0} \leqslant (p-1) - 1,$$

c'est-à-dire :

$$1 \leqslant \big|k_1 - k_2\big| \leqslant p-2,$$

et donc manifestement, $k_1 - k_2$ ne peut pas être divisible par p.

Comme $p \nmid a$ aussi, nous voyons que le membre de gauche ci-dessus $(k_1 - k_2)\,a$ n'est *pas* congru à zéro modulo p.

Donc le membre de droite $r_{k_1} - r_{k_2}$ n'est *pas* non plus congru à zéro modulo p. Autrement dit, $r_{k_1} - r_{k_2} \neq \ell\,p$ pour tout entier $\ell \in \mathbb{Z}$.

Enfin, comme $\big|r_{k_1} - r_{k_2}\big| \leqslant p-1$, nous concluons que $r_{k_1} - r_{k_2} \neq 0$, comme désiré.

(e) Comme les $p-1$ restes $r_1, \ldots, r_{p-1}$, qui appartiennent à l'ensemble $\{1, \ldots, p-1\}$ de cardinal $p-1$, sont mutuellement distincts, il est clair qu'ils décrivent tout cet ensemble :

$$\big\{r_1, r_2, \ldots, r_{p-1}\big\} = \big\{1, 2, \ldots, p-1\big\},$$

et donc :

$$r_1 \cdot r_2 \cdots r_{p-1} = 1 \cdot 2 \cdots (p-1).$$

(f) Comme promis, en utilisant $k\,a \equiv r_k \bmod p$, calculons d'une deuxième manière l'entier-produit N modulo p :

$$\begin{aligned}
\mathrm{N} \bmod p &\equiv 1\,a \cdot 2\,a \cdots (p-1)\,a \\
&\equiv r_1 \cdot r_2 \cdots r_{p-1} \bmod p \\
\text{[Question (e)]} \qquad &\equiv 1 \cdot 2 \cdots (p-1) \bmod p \\
&\equiv (p-1)! \bmod p.
\end{aligned}$$

Une comparaison avec la Question **(a)** donne alors :

$$(p-1)!\,a^{p-1} \equiv (p-1)! \bmod p,$$

et comme $(p-1)!$ est premier avec p, on peut éliminer $(p-1)!$ dans cette relation de congruence pour atteindre le Petit Théorème de Fermat :

$$a^{p-1} \equiv 1 \bmod p \qquad (p \text{ premier},\ a \wedge p = 1).$$

Exercice 6. (a) D'après le cours :

$$\varphi\big(p^r\big) = p^r - p^{r-1}.$$

(b) Le cours a établi que pour deux entiers $r, s \geqslant 1$ premiers entre eux $1 = r \wedge s$, on a la multiplicativité $\varphi(r\,s) = \varphi(r)\,\varphi(s)$. Toutefois ici, m et n ne sont pas premiers entre eux, puisque $\mathsf{pgcd}(m, n) = p_2^5$.

En tout cas, nous pouvons calculer :

$$\begin{aligned}
\varphi(m) &= \varphi\big(p_1^3\,p_2^5\big) = \varphi\big(p_1^3\big)\,\varphi\big(p_2^5\big) = \big(p_1^3 - p_1^2\big)\,\big(p_2^5 - p_2^4\big), \\
\varphi(n) &= \varphi\big(p_2^7\,p_3\big) = \varphi\big(p_2^7\big)\,\varphi\big(p_3\big) = \big(p_2^7 - p_2^6\big)\,\big(p_3 - 1\big),
\end{aligned}$$

ainsi que :

$$\varphi\big(m\,n\big) = \varphi\big(p_1^3\,p_2^{12}\,p_3\big) = \big(p_1^3 - p_1^2\big)\,\big(p_2^{12} - p_2^{11}\big)\,\big(p_3 - 1\big).$$

Par conséquent, nous avons bien :

$$\begin{aligned}
\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} &= \frac{(p_1^3 - p_1^2)\,(p_2^{12} - p_2^{11})\,(p_3 - 1)}{(p_1^3 - p_1^2)(p_2^5 - p_2^4) \cdot (p_2^7 - p_2^6)\,(p_3 - 1)} \\
&= \frac{p_2^{11}\,(p_2 - 1)}{p_2^4\,(p_2 - 1)\,p_2^6\,(p_2 - 1)} \\
&= \frac{p_2}{(p_2 - 1)} \\
&= \frac{p_2}{\varphi(p_2)}.
\end{aligned}$$

(c) La formule connue donne :

$$\begin{aligned}
\varphi(m) &= \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k - 1}\,\big(P_k - 1\big), \\
\varphi(n) &= \prod_{1 \leqslant i \leqslant r} p_i^{\beta_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell - 1}\,\big(Q_\ell - 1\big), \\
\varphi\big(m\,n\big) &= \prod_{1 \leqslant i \leqslant r} p_i^{\alpha_i + \beta_i - 1}\,\big(p_i - 1\big) \prod_{1 \leqslant k \leqslant \mathrm{K}} P_k^{a_k - 1}\,\big(P_k - 1\big) \prod_{1 \leqslant \ell \leqslant \mathrm{L}} Q_\ell^{b_\ell - 1}\,\big(Q_\ell - 1\big),
\end{aligned}$$

d'où le résultat demandé :

$$\begin{aligned}\frac{\varphi(m\,n)}{\varphi(m)\,\varphi(n)} &= \frac{\prod_i p_i^{\alpha_i+\beta_i-1}\,(p_i-1)}{\prod_i p_i^{\alpha_i-1}\,(p_i-1)\ \prod_i p_i^{\beta_i-1}\,(p_i-1)}\\ &= \frac{\prod_{1\leqslant i\leqslant r} p_i}{\prod_{1\leqslant i\leqslant r}(p_i-1)}\\ &= \frac{p_1\cdots p_r}{(p_1-1)\cdots(p_r-1)}.\end{aligned}$$

Exercice 7. (a) On peut supposer $2 \leqslant a \leqslant b$. Comme $n \geqslant 5$, au moins une de ces deux inégalités est stricte, sinon $2 = a = b$ donnerait $n = a\,b = 4$.

On en déduit :

$$n \;=\; a\,b \;\geqslant\; 2\,b \;\geqslant\; a+b,$$

avec à nouveau encore au moins une inégalité stricte, car $a\,b = 2\,b = a+b$ forcerait $b = 2 = a$. Donc $n > a+b$, c'est-à-dire $n-1 \geqslant a+b$, et comme le quotient $\frac{(a+b)!}{a!\,b!} \in \mathbb{N}$ est toujours entier puisque c'est un nombre binomial, on conclut grâce à la transitivité de la relation de divisibilité :

$$(n-1)\,!\ \text{divisible par}\ (a+b)\,!\ \text{divisible par}\ a!\,b!\ \text{divisible par}\ a\,b.$$

9. Examen 5

Exercice 1. Soit la permutation suivante d'un ensemble à 13 éléments :

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 12 & 13 & 1 & 2 & 11 & 7 & 9 & 3 & 5 & 6 & 10 & 4 \end{pmatrix}.$$

(a) Décomposer σ en produit de cycles à supports disjoints.

(b) Déterminer l'ordre $o(\sigma)$ de σ.

(c) Déterminer la décomposition explicite de σ^{2023} en cycles disjoints.

Exercice 2. **(a)** Déterminer le reste de la division de $X^{96} - X^{25}$ par $X^2 + 1$.

(b) Déterminer les entiers $n \geqslant 1$ tels que :

$$X^3 - X^2 + X - 1 \,\Big|\, \big(X^2 - X + 1\big)^n - X^{2n} + X^n - 1.$$

Indication: On pourra factoriser $X^3 - X^2 + X - 1$ afin d'en déterminer les trois racines complexes.

Exercice 3. Soit un nombre premier $p \geqslant 2$ quelconque. On considère le groupe $\mathfrak{S}_p$ des permutations de l'ensemble $\{1, 2, \ldots, p\}$.

(a) Montrer qu'un élément arbitraire σ du groupe $\mathfrak{S}_p$ est un p-cycle si et seulement si son ordre vaut $p = o(\sigma)$.

(b) Trouver un nombre $n \geqslant 4$ non premier tel que, dans le groupe $\mathfrak{S}_n$ des permutations de $\{1, 2, \ldots, n\}$, il existe un exemple d'élément $\sigma \in \mathfrak{S}_n$ d'ordre égal à n qui n'est *pas* un n-cycle.

Exercice 4. **(a)** Sur un corps commutatif $\mathbb{K}$, soit un polynôme unitaire du troisième degré $p := x^3 + \lambda\, x^2 + \mu\, x + \nu$. Montrer que p est réductible sur $\mathbb{K}$ si et seulement si il possède une racine dans $\mathbb{K}$.

(b) Soit le corps $\mathbb{K} := \mathbb{Z}/7\mathbb{Z}$ des classes résiduelles modulo 7. Montrer que le polynôme :

$$x^3 + x^2 + \overline{2}\, x + \overline{5}$$

est réductible, en exhibant une factorisation par deux polynômes de degrés 1 et 2.

(c) Montrer que le polynôme $x^2 + \overline{3}\, x + \overline{1}$ est *irréductible* sur $\mathbb{K}[x]$ où $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$.

(d) Dans $\mathbb{K}[x]$ avec $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$, effectuer la division euclidienne de $x^3 + \overline{2}\, x^2 + \overline{3}\, x + \overline{4}$ par $x^3 + x^2 + \overline{2}\, x + \overline{5}$.

(e) Toujours dans $\mathbb{K}[x]$ avec $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$, décomposer en éléments simples la fraction rationnelle :

$$\frac{x^3 + \overline{2}\, x^2 + \overline{3}\, x + \overline{4}}{x^3 + x^2 + \overline{2}\, x + \overline{5}}.$$

Exercice 5. Dans $\mathbb{Q}[x]$, on introduit les trois polynômes :

$$\begin{aligned} D &:= x^2 + 2\,x + 5, \\ Q &:= x^5 + x^4 + 4\,x^3 - 4\,x^2 + 3\,x - 5, \\ P &:= x^6 + 4\,x^5 + 12\,x^4 + 15\,x^3 + 17\,x^2 + 3\,x + 20. \end{aligned}$$

(a) Effectuer la division euclidienne de Q par D, constater que le reste est nul, et enfin, vérifier que le résultat obtenu est correct.

(b) Diviser P par D. Ensuite, vérifier le résultat obtenu.

(c) L'objectif, maintenant, est de déterminer le pgcd entre les deux polynômes de $\mathbb{Q}[x]$:

$$\begin{aligned} B &:= x^3 - x^2 + x - 1, \\ A &:= x^4 + 2\,x^3 + 3\,x^2 - x + 4. \end{aligned}$$

En appliquant l'algorithme d'Euclide sans faire d'erreur de calcul, démontrer que :

$$\mathsf{pgcd}\,\big(A,\,B\big) \;=\; \frac{2925}{256}.$$

(d) Déterminer $\mathsf{pgcd}\,(P, Q)$. Indication: On rappelle que le pgcd est défini à une constante non nulle près.

Exercice 6. Soit $P(X) = a_0 + a_1\,X + \cdots + a_n\,X^n \in \mathbb{R}[X]$ un polynôme à coefficients réels, de degré $n \geqslant 1$, avec $a_n \neq 0$. On suppose qu'il ne prend que des valeurs positives sur $\mathbb{R}$:

$$P(x) \;\geqslant\; 0 \qquad (\forall\, x \in \mathbb{R}).$$

(a) Montrer que $a_n > 0$.

(b) Montrer que $n \in 2\,\mathbb{N}^*$ est pair.

(c) Montrer que les racines réelles $\alpha \in \mathbb{R}$ de $P(X)$ sont de multiplicité paire. Indication: Considérer le comportement de $(x - \alpha)^m$ pour $x \sim \alpha$ proche de α.

(d) Justifier l'écriture :

$$P(X) \;=\; a_n \prod_{i=1}^{s} \big(X - \alpha_i\big)^{2m_i} \prod_{j=1}^{t} \big(X^2 + c_j\,X + d_j\big)^{q_j},$$

et donner des informations sur les c_j, d_j.

(e) Montrer qu'il existe un polynôme $C \in \mathbb{C}[X]$ tel que :

$$P \;=\; C\,\overline{C}.$$

(f) En déduire qu'il existe A et B dans $\mathbb{R}[X]$ tels que :

$$P \;=\; A^2 + B^2.$$

Exercice 7. Soit un polynôme dans $\mathbb{C}[X]$ à coefficients complexes de degré $n \geqslant 1$:

$$P(X) \;:=\; \sum_{k=0}^{n} a_k\,X^k \qquad (a_n \neq 0).$$

L'objectif est de le diviser avec reste par $X^\ell - 1$, où $\ell \geqslant 1$ est un entier fixé quelconque.

(a) Factoriser $X^{q\,\ell} - 1$ par $X^\ell - 1$, où $q \geqslant 0$ est un entier arbitraire. Indication: Factoriser d'abord $Y^q - 1$ par $Y - 1$.

(b) Pour chaque entier $k \in \{0, 1, \ldots, n\}$, on note r_k le reste de la division euclidenne de k par ℓ. Montrer que le reste de la division euclidienne de $P(X)$ par $X^\ell - 1$ est le polynôme :

$$R(X) := \sum_{k=0}^{n} a_k \, X^{r_k}.$$

Exercice 8. Soit $\mathrm{N} \geqslant 1$, soit $\mathfrak{S}_\mathrm{N}$ le groupe des permutations de $\big\{1, 2, \ldots, \mathrm{N}\big\}$, et soit $\sigma \in \mathfrak{S}_\mathrm{N}$ un *cycle*, de longueur n avec $2 \leqslant n \leqslant \mathrm{N}$.

L'objectif est d'établir que pour tout entier $m \geqslant 1$, la permutation :

$$\tau := \sigma^m,$$

se décompose en $\mathsf{pgcd}\,(n, m)$ cycles de longueur $\frac{n}{\mathsf{pgcd}(n,m)}$. Par convention dans cet exercice, un *cycle de longueur* 1 dans la décomposition d'une permutation est un *point fixe* sous l'action de cette permutation.

(a) Montrer qu'il suffit d'établir le résultat pour $\mathrm{N} = n$ et pour la permutation circulaire $\sigma = \big(1 \; 2 \; \cdots \; n\big)$.

(b) On suppose donc que σ est le n-cycle $\sigma = \big(1 \; 2 \; \cdots \; n\big)$ appartenant à $\mathfrak{S}_n$, avec $n \geqslant 2$, c'est-à-dire que :

$$\sigma(i) := i + 1 \mod n.$$

On écrit $m = d\,m'$, puis $n = d\,n'$, où $d := \mathsf{pgcd}\,(m, n)$, avec bien sûr $1 = m' \wedge n'$.

Pour un élément arbitraire fixé $i \in \big\{1, 2, \ldots, n\big\}$, montrer que l'orbite de i par τ :

$$\mathsf{Orb}_\tau(i) = \big\{\tau^\ell(i) \colon \; \ell \in \mathbb{Z}\big\},$$

est constituée des n' éléments *distincts* suivants :

$$\big\{i, \; i + m, \; i + 2\,m, \; \ldots, \; i + (n' - 1)\,m\big\} \mod n.$$

Indication: En appliquant un résultat du cours, il suffit de déterminer :

$$v := \min\big\{\ell \in \mathbb{N}_{\geqslant 1} \colon \; \tau^\ell(i) = i\big\}.$$

(c) Soient deux orbites avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$:

$$\begin{aligned} \mathsf{Orb}_\tau(i) &= \big\{i, \; i + m, \; \ldots, \; i + (n' - 1)\,m\big\} \mod n, \\ \mathsf{Orb}_\tau(j) &= \big\{j, \; j + m, \; \ldots, \; j + (n' - 1)\,m\big\} \mod n. \end{aligned}$$

Montrer que :

$$\mathsf{Orb}_\tau(i) = \mathsf{Orb}_\tau(j) \qquad \Longrightarrow \qquad i \equiv j \mod d.$$

Indication: Deux orbites sont égales si et seulement si elles ont un élément en commun.

(d) Montrer qu'on a la réunion disjointe :

$$\big\{1, \; 2, \; \ldots, \; n\big\} = \mathsf{Orb}_\tau(1) \cup \cdots \cup \mathsf{Orb}_\tau(d).$$

(e) Si $\sigma \in \mathfrak{S}_\mathrm{N}$ est un n-cycle, avec $n \geqslant 2$, et si $m \geqslant 1$ est un entier, en déduire les deux cas particuliers suivants :

• lorsque $m \,|\, n$, la permutation $\tau = \sigma^m$ se décompose en m cycles de longueur $\frac{n}{m}$, à supports disjoints ;

• lorsque $m \wedge n = 1$ sont premiers entre eux, σ^m est aussi un n-cycle de même longueur que σ.

(f) Le résultat subsiste-t-il si l'on remplace $\mathfrak{S}_{\mathrm{N}}$ par $\mathfrak{S}(E)$, où E est un ensemble fini vraiment quelconque à $\mathrm{N} \geqslant 1$ éléments ?

(g) Soit $\sigma \in \mathfrak{S}_{25}$ de type $\big(12, 8, 6, 1\big)$. Calculer le type de σ^4.

10. Corrigé de l'examen 5

Exercice 1. **(a)** Une lecture directe montre que :

$$\begin{aligned}
&1 \longmapsto 8 \longmapsto 9 \longmapsto 3 \longmapsto 13 \longmapsto 4 \longmapsto 1,\\
&2 \longmapsto 12 \longmapsto 10 \longmapsto 5 \longmapsto 2,\\
&6 \longmapsto 11,\\
&7 \longmapsto 7.
\end{aligned}$$

Ainsi, σ se décompose en produit de trois cycles à supports disjoints, plus un point fixe :

$$\begin{aligned}
\sigma &= \big(1\ 8\ 9\ 3\ 13\ 4\big) \circ \big(2\ 12\ 10\ 5\big) \circ \big(6\ 11\big) \circ \big(7\big)\\
&=: c_6 \circ c_4 \circ c_2 \circ c_1.
\end{aligned}$$

(b) Rappelons que, dans le groupe $\mathfrak{S}_n$ des permutations de l'ensemble $\big\{1, 2, \ldots, n\big\}$ à $n \geqslant 1$ éléments, l'ordre d'un p-cycle quelconque :

$$c_p = \Big(\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_{p-1} \arrow[r] & a_p \arrow[lllll, bend left] \end{tikzcd} \Big),$$

avec $a_1, a_2, \ldots, a_{p-1}, a_p \in \{1, \ldots, n\}$ distincts, vaut :

$$p = \boldsymbol{o}(c_p).$$

Rappelons aussi que les points fixes, tels que (7) ci-dessus, peuvent par léger abus de pensée, être considérés comme des 1-cycles.

Alors d'après un théorème vu en cours :

$$\begin{aligned}
\boldsymbol{o}(\sigma) &= \boldsymbol{o}\big(c_6 \circ c_4 \circ c_2 \circ c_1\big)\\
&= \mathsf{ppcm}\Big(\boldsymbol{o}\big(c_6\big), \boldsymbol{o}\big(c_4\big), \boldsymbol{o}\big(c_2\big), \boldsymbol{o}\big(c_1\big), \Big)\\
&= \mathsf{ppcm}\big(6,\ 4,\ 2,\ 1\big)\\
&= 12.
\end{aligned}$$

(c) Comme $\sigma^{12} = \mathsf{Id}$, d'où pour tout entier $r \in \mathbb{Z}$:

$$\sigma^r = \sigma^{r \bmod 12},$$

il est avisé de diviser 2023 par 12 :

$$2023 = 7 + 168 \cdot 12,$$

d'où puisque les cycles à supports disjoints commutent entre eux et puisque $(c_p)^p = \mathsf{Id}$ pour tout p-cycle c_p :

$$\begin{aligned}\sigma^{2023} &= \sigma^7\\ &= \Big(c_6 \circ c_4 \circ c_2 \circ c_1\Big)^7\\ &= (c_6)^7 \circ (c_4)^7 \circ (c_2)^7 \circ \mathsf{Id}\\ &= c_6 \circ c_4^{-1} \circ c_2.\end{aligned}$$

Mais l'inverse c_4^{-1} de :

$$c_4 = \Big(\ 2 \longrightarrow 12 \longrightarrow 10 \longrightarrow 5\ \Big),$$

se calcule simplement en renversant les flèches :

$$c_4^{-1} = \Big(\ 2 \longleftarrow 12 \longleftarrow 10 \longleftarrow 5\ \Big),$$

c'est-à-dire :

$$c_4^{-1} = \big(2\ \ 5\ \ 10\ \ 12\big).$$

En conclusion :

$$\begin{aligned}\sigma^{2023} &= \big(1\ \ 8\ \ 9\ \ 3\ \ 13\ \ 4\big) \circ \big(2\ \ 5\ \ 10\ \ 12\big) \circ \big(6\ \ 11\big) \circ \big(7\big)\\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13\\ 8 & 5 & 13 & 1 & 10 & 11 & 7 & 9 & 3 & 12 & 6 & 2 & 4\end{pmatrix}.\end{aligned}$$

Exercice 2. **(a)** Il suffit de raisonner astucieusement modulo X^2+1, sans avoir à calculer le quotient $Q(X)$ dans la division euclidienne :

$$X^{96} - X^{25} = Q(X)\,(X^2+1) + R(X).$$

En effet, modulo X^2+1, on a $X^2 \equiv -1$. Donc modulo X^2+1, il est clair que :

$$X^{96} \equiv (-1)^{48} \equiv 1 \qquad \text{et} \qquad -X^{25} \equiv -X\,X^{24} \equiv -X\,(-1)^{12} \equiv -X,$$

d'où la réponse :

$$R(X) = -X+1.$$

(b) Factorisons donc :

$$X^3 - X^2 + X - 1 = (X-1)\,\big(X^2+1\big).$$

Les trois racines, distinctes, sont 1, i, $-i$.

Ensuite, avec $n \geqslant 1$ entier, pour que le polynôme $\big(X^2-X+1\big)^n - X^{2n} + X^n - 1$ soit divisible par $(X-1)(X-i)(X+i)$, il faut et il suffit qu'il ait 1, i, $-i$ pour racines.

Clairement, 1 est toujours racine, quel que soit $n \geqslant 1$. De plus, i et $-i$ sont racines si et seulement si :

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

ces deux équations étant identiques, éuivalentes à l'équation factorisée :

$$0 = \big((-1)^n + 1\big)\,\big(i^n - 1\big).$$

On voit aisément que cette équation est satisfaite si et seulement si $n \neq 2 + 4\,m$, avec $m \geqslant 0$ entier.

Exercice 3. (a) Tout d'abord, on sait que l'ordre d'un cycle est égal à sa longueur, donc l'implication $\Longrightarrow$ est immédiate.

Réciproquement, soit $\sigma \in \mathfrak{S}_p$ d'ordre $p = \mathsf{o}(\sigma)$, donc d'ordre $\geqslant 2$, car tout nombre premier p est $\geqslant 2$. En particulier, $\sigma \neq \mathsf{Id}$. Nous devons démontrer que σ est un p-cycle.

D'après un théorème du cours, $\sigma \in \mathfrak{S}_p$ se décompose en produit :

$$\sigma \,=\, c_1 \circ \cdots \circ c_k,$$

d'un certain nombre $k \geqslant 1$ de cycles c_i à supports disjoints ayant une certaine longueur $\ell_i \geqslant 2$, cela, pour $i = 1, \ldots, k$.

D'après un autre théorème du cours, nous savons aussi que :

$$\begin{aligned} p \,=\, \mathsf{o}(\sigma) \,&=\, \mathsf{ppcm}\Big(\mathsf{o}\big(c_1\big),\, \ldots,\, \mathsf{o}\big(c_k\big)\Big) \\ &=\, \mathsf{ppcm}\,\big(\ell_1, \ldots, \ell_k\big). \end{aligned}$$

Comme les cycles sont à supports disjoints dans l'ensemble $\{1, \ldots, p\}$ de longueur p, nous avons l'inégalité :

$$p \,\geqslant\, \ell_1 + \cdots + \ell_k.$$

Si l'une des longueurs ℓ_i était $\leqslant p - 1$, le ppcm à droite ci-dessus serait divisible par ℓ_i, et alors, ℓ_i diviserait p à gauche, en contradiction avec l'hypothèse que p est premier.

Donc $\ell_i = p$ nécessairement, et enfin, $k = 1$ à cause de l'inégalité ci-dessus. En définitive, σ se décompose bien en un unique cycle de longueur p.

(b) Après réflexion au brouillon, on se rend compte que ni $n = 4$ ni $n = 5$ ne peuvent produire d'exemple.

Mais avec :

$$n \,:=\, 6 \,=\, 2 \cdot 3 \,=\, \mathsf{ppcm}\,(2, 3),$$

il suffit de prendre pour σ un produit de deux cycles à supports disjoints de longueurs égales à 2 et à 3, par exemple :

$$\sigma \,:=\, \big(1\ 2\big) \circ \big(4\ 5\ 6\big) \qquad {\scriptstyle (\sigma(3)=3).}$$

Clairement, σ n'est *pas* un 6-cycle, et son ordre vaut bien :

$$\mathsf{o}(\sigma) \,=\, \mathsf{ppcm}\Big(\mathsf{o}\big(1\ 2\big),\ \mathsf{o}\big(4\ 5\ 6\big)\Big) \,=\, \mathsf{ppcm}\,(2,\,3) \,=\, 6 \,=\, n.$$

Exercice 4. (a) Si p est réductible, puisque $3 = 1 + 2$ est la seule possibilité au niveau des degrés, il se factorise :

$$p(x) \,=\, (x - \alpha)\,(x^2 + \beta\, x + \gamma),$$

en un produit de deux polynômes unitaires de degré 1, à coefficients dans $\mathbb{K}$. Mais alors, α est une racine de $p(x)$ dans $\mathbb{K}$.

Inversement, s'il existe $\alpha \in \mathbb{K}$ tel que $p(\alpha) = 0$, on a vu dans le cours que le polynôme se factorise par $(x - \alpha)$:

$$p(x) \,=\, (x - \alpha)\, q(x),$$

avec un polynôme $q(x)$ de degré 2, unitaire, à coefficients dans $\mathbb{K}$, donc de la forme $x^2 + \beta\, x + \gamma$. Ainsi, $p(x) = (x - \alpha)\,(x^2 + \beta\, x + \gamma)$ se décompose en produit de deux polynômes de degrés 1 et 2 à coefficients dans $\mathbb{K}$, ce qui montre que p est bien réductible.

(b) Pour $x = \overline{a} \in \mathbb{Z}/7\mathbb{Z}$, calculons les valeurs que prend ce polynôme :

$$\begin{aligned}
\overline{0}^3 + \overline{0}^2 + \overline{2}\cdot\overline{0} + \overline{5} &= \overline{5} = \overline{5}\\
\overline{1}^3 + \overline{1}^2 + \overline{2}\cdot\overline{1} + \overline{5} &= \overline{9} = \overline{2}\\
\overline{2}^3 + \overline{2}^2 + \overline{2}\cdot\overline{2} + \overline{5} &= \overline{21} = \overline{0}\\
\overline{3}^3 + \overline{3}^2 + \overline{2}\cdot\overline{3} + \overline{5} &= \overline{47} = \overline{5}\\
\overline{4}^3 + \overline{4}^2 + \overline{2}\cdot\overline{4} + \overline{5} &= \overline{93} = \overline{2}\\
\overline{5}^3 + \overline{5}^2 + \overline{2}\cdot\overline{5} + \overline{5} &= \overline{165} = \overline{4}\\
\overline{6}^3 + \overline{6}^2 + \overline{2}\cdot\overline{6} + \overline{5} &= \overline{269} = \overline{3}.
\end{aligned}$$

Ainsi, $\overline{2}$ est une racine. Grâce à la Question **(a)** qui précède, notre polynôme cubique est réductible, factorisable par :

$$x - \overline{2} = x + \overline{5}.$$

Une division euclidienne donne alors :

$$x^3 + x^2 + \overline{2}\,x + \overline{5} = \big(x + \overline{5}\big)\big(x^2 + \overline{3}\,x + \overline{1}\big).$$

(c) Un raisonnement tout à fait similaire à celui qui a été conduit en **(a)** montre qu'un polynôme quadratique monique $x^2 + \lambda\,x + \mu$ à coefficients dans un corps $\mathbb{K}$ est irréductible si et seulement si il n'admet aucune racine dans $\mathbb{K}$.

Calculons alors les valeurs que prend la fonction $x \longmapsto x^2 + \overline{3}\,x + \overline{1}$ sur les sept éléments de $\mathbb{Z}/7\mathbb{Z}$:

$$\begin{aligned}
\overline{0}^2 + \overline{3}\cdot\overline{0} + \overline{1} &= \overline{1} = \overline{1},\\
\overline{1}^2 + \overline{3}\cdot\overline{1} + \overline{1} &= \overline{5} = \overline{5},\\
\overline{2}^2 + \overline{3}\cdot\overline{2} + \overline{1} &= \overline{11} = \overline{4},\\
\overline{3}^2 + \overline{3}\cdot\overline{3} + \overline{1} &= \overline{19} = \overline{5},\\
\overline{4}^2 + \overline{3}\cdot\overline{4} + \overline{1} &= \overline{29} = \overline{1},\\
\overline{5}^2 + \overline{3}\cdot\overline{5} + \overline{1} &= \overline{41} = \overline{6},\\
\overline{6}^2 + \overline{3}\cdot\overline{6} + \overline{1} &= \overline{55} = \overline{6}.
\end{aligned}$$

Aucune de ces valeurs n'étant nulle, nous concluons que $x^2 + \overline{3}\,x + \overline{1}$ est bien irréductible.

(d) On trouve :

$$x^3 + \overline{2}\,x^2 + \overline{3}\,x + \overline{4} = \big(x^3 + x^2 + \overline{2}\,x + \overline{5}\big)\cdot\overline{1} + x^2 + x + \overline{6}.$$

(e) Tout d'abord, grâce à la division euclidienne :

$$\frac{x^3 + \overline{2}\,x^2 + \overline{3}\,x + \overline{4}}{x^3 + x^2 + \overline{2}\,x + \overline{5}} = \overline{1} + \frac{x^2 + x + \overline{6}}{x^3 + x^2 + \overline{2}\,x + \overline{5}}.$$

Nous sommes alors dans la situation où le degré du numérateur est strictement inférieur à celui du dénominateur, situation où nous pouvons rechercher une décomposition en éléments simples.

Pour commencer, il faut décomposer en facteurs irréductibles le dénominateur. Mais ce travail a déjà été préparé par les questions qui précèdent :

$$\text{Dénominateur} \;=\; \big(x+\overline{5}\big)\,\big(x^2+\overline{3}\,x+\overline{1}\big).$$

D'après un théorème du cours, il s'agit maintenant de déterminer trois constantes inconnues $\overline{a}$, $\overline{b}$, $\overline{c}$ telles que :

$$\frac{x^2+x+\overline{6}}{(x+\overline{5})\,(x^2+\overline{3}\,x+\overline{1})} \;=\; \frac{\overline{a}}{x+\overline{5}}+\frac{\overline{b}\,x+\overline{c}}{x^2+\overline{3}\,x+\overline{1}}.$$

Après élimination du dénominateur, nous avons :

$$x^2+x+\overline{6} \;=\; \overline{a}\,\big(x^2+\overline{3}\,x+\overline{1}\big)+\big(\overline{b}\,x+\overline{c}\big)\,\big(x+\overline{5}\big).$$

En posant $x := -\,\overline{5}=\overline{2}$, il vient :

$$\begin{aligned} & \overline{2}^2+\overline{2}+\overline{6} \;=\; \overline{a}\,\big(\overline{2}^2+\overline{3}\cdot\overline{2}+\overline{1}\big)+\overline{0} \\ \longleftrightarrow \qquad & \overline{5} \;=\; \overline{a}\cdot\overline{4} \end{aligned}$$

d'où puisque dans le corps $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{4}\cdot\overline{2}=\overline{1}$:

$$\overline{5}\cdot\overline{2} \;=\; \overline{3} \;=\; \overline{a}.$$

Ensuite, après soustraction :

$$\begin{aligned} x^2+x+\overline{6}-\overline{3}\,x^2-\overline{9}\,x-\overline{3} \;&=\; \overline{5}\,x^2+\overline{6}\,x+\overline{3} \\ &=\; \overline{b}\,x^2+\big(\overline{b}\cdot\overline{5}+\overline{c}\big)+\overline{c}\cdot\overline{5}. \end{aligned}$$

Par identification, le système linéaire de trois équations à deux inconnues :

$$\begin{aligned} \overline{5} \;&=\; \overline{b}, \\ \overline{6} \;&=\; \overline{5}\,\overline{b}+\overline{c}, \\ \overline{3} \;&=\; \overline{5}\,\overline{c}, \end{aligned}$$

admet pour solution unique :

$$\overline{b} \;:=\; \overline{5}, \qquad\qquad \overline{c} \;:=\; \overline{2}.$$

En conclusion :

$$\frac{x^3+\overline{2}\,x^2+\overline{3}\,x+\overline{4}}{x^3+x^2+\overline{2}\,x+\overline{5}} \;=\; \overline{1}+\frac{\overline{3}}{x+\overline{5}}+\frac{\overline{5}\,x+\overline{2}}{x^2+\overline{3}\,x+\overline{1}}. \qquad \square$$

Exercice 5. **(a)** On trouve, sans reste :

$$x^5+x^4+4\,x^3-4\,x^2+3\,x-5 \;=\; \big(x^2+2\,x+5\big)\,\big(x^3-x^2+x-1\big).$$

En développant le produit à droite, on retrouve bien le polynôme à gauche.

(b) On trouve, à nouveau sans reste :

$$x^6+4\,x^5+12\,x^4+15\,x^3+17\,x^2+3\,x+20 \;=\; \big(x^2+2\,x+5\big)\,\big(x^4+2\,x^3+3\,x^2-x+4\big).$$

En développant le produit à droite, on retrouve bien le polynôme à gauche.

(c) Divisons avec reste A par B :

$$x^4+2\,x^3+3\,x^2-x+4 \;=\; \big(x^3-x^2+x-1\big)\,(x+3)+5\,x^2-3\,x+7.$$

Ensuite, divisons B par le reste obtenu, ce qui crée des nombres rationnels :

$$x^3 - x^2 + x - 1 \;=\; \big(5\,x^2 - 3\,x + 7\big)\,\big(\tfrac{1}{5}\,x - \tfrac{2}{25}\big) - \tfrac{16}{25}\,x - \tfrac{11}{25}.$$

Enfin, divisons l'avant-dernier reste par le dernier :

$$5\,x^2 - 3\,x + 7 \;=\; \big(-\,\tfrac{16}{25} - \tfrac{11}{25}\big)\,\big(-\,\tfrac{125}{16}\,x + \tfrac{2575}{256}\big) + \tfrac{2925}{256}.$$

Le dernier reste non nul est bien égal à la constante non nulle :

$$\frac{2925}{256} \;=\; \mathsf{pgcd}\,\big(A, B\big),$$

ce qui montre que les deux polynômes A et B sont premiers entre eux.

(d) Après multiplication par une constante, on a :

$$1 \;=\; \mathsf{pgcd}\,\big(A,\, B\big),$$

d'où en conclusion :

$$\begin{aligned}\mathsf{pgcd}\,\big(P,\, Q\big) \;&=\; \mathsf{pgcd}\,\big(D\,A,\;\; D\,B\big)\\ &=\; D\,\mathsf{pgcd}\,\big(A,\, B\big)\\ &=\; D.\end{aligned}$$

Exercice 6. (a) Lorsque $-\infty \longleftarrow x$, et lorsque $x \longrightarrow \infty$, on sait que le monôme $a_n\,x^n$ domine tous les autres, d'où :

$$\lim_{-\infty \leftarrow x} a_n\,x^n \;=\; \lim_{-\infty \leftarrow x} P(x) \qquad\qquad \text{et} \qquad\qquad \lim_{x \to \infty} P(x) \;=\; \lim_{x \to \infty} a_n\,x^n.$$

Si $a_n < 0$ était (strictement) négatif, cette dernière limite vaudrait $-\,\infty$, ce qui contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(b) Sinon, si $n = 2\,n' + 1$ était *impair*, avec $a_n > 0$ grâce à la Question **(a)**, la limite :

$$-\,\infty \;=\; \lim_{-\infty \leftarrow x} a_n\,x^{2n'+1} \;=\; \lim_{-\infty \leftarrow x} P(x),$$

contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(c) Soit donc $\alpha \in \mathbb{R}$ une racine de $P(X)$, et soit $m \geqslant 1$ sa multiplicité :

$$P(X) \;=\; (X - \alpha)^m\,Q(X),$$

avec $Q(X)$ un polynôme de degré $n - m$ satisfaisant $0 \neq Q(\alpha)$.

Si $m = 2\,m' + 1$ était impair, comme au voisinage de $X = \alpha$ on a l'équivalent :

$$P(X) \;\sim\; \big(X - \alpha\big)^{2m'+1}\,Q(\alpha),$$

et comme la fonction réelle $x \longmapsto (x - \alpha)^{2m'+1}$ change de signe pour $x < \alpha$ et pour $x > \alpha$, ceci contredirait l'hypothèse de positivité $P \geqslant 0$ sur $\mathbb{R}$.

(d) Il s'agit de la décomposition de $P(X)$ en facteurs irréductibles, avec chaque racine réelle α_i de multiplicité *paire* $2\,m_i$, grâce à la Question **(c)**, et avec chaque trinôme du second degré, pour $1 \leqslant j \leqslant t$, n'ayant pas de racine réelle :

$$c_j^2 - 4\,d_j \;<\; 0 \qquad\qquad (1 \leqslant j \leqslant t).$$

Le degré total de $P(X)$ est visiblement *pair :*

$$n \;=\; 2\,m_1 + \cdots + 2\,m_s + 2\,q_1 + \cdots + 2\,q_t.$$

(e) Grâce à cette représentation de $P(X)$, et grâce à la connaissance des racines *complexes :*

$$\begin{aligned}\mu_j^+ &:= \frac{-c_j + \sqrt{-1}\sqrt{-c_j^2 + 4\,d_j}}{2},\\ \mu_j^- &:= \frac{-c_j - \sqrt{-1}\sqrt{-c_j^2 + 4\,d_j}}{2},\end{aligned}$$

qui sont, comme on le sait, manifestement conjuguées par paires :

$$\mu_j := \mu_j^+ = \overline{\mu_j^-} =: \overline{\mu_j} \qquad (1 \leqslant j \leqslant t),$$

il vient, sachant que les racines $\overline{\alpha_i} = \alpha_i$ sont réelles :

$$\begin{aligned}P(X) &= \sqrt{a_n} \prod_{i=1}^{s} \big(X - \alpha_i\big)^{m_i} \prod_{j=1}^{t} \big(X - \mu_j\big)^{q_j}\\ &\cdot \sqrt{a_n} \prod_{i=1}^{s} \big(X - \alpha_i\big)^{m_i} \prod_{j=1}^{t} \big(X - \overline{\mu_j}\big)^{q_j}\\ &=: C(X)\\ &\quad\cdot \overline{C(X)}.\end{aligned}$$

(f) Il suffit de décomposer $C(X)$ en parties réelle et imaginaire :

$$C(X) = A(X) + \sqrt{-1}\,B(X) \qquad \text{où} \qquad \begin{aligned}A(X) &:= \frac{C(X) + \overline{C(X)}}{2},\\ B(X) &:= \frac{C(X) - \overline{C(X)}}{2\sqrt{-1}},\end{aligned}$$

pour obtenir en conclusion :

$$\begin{aligned}P &= C\,\overline{C}\\ &= \big(A + \sqrt{-1}\,B\big)\big(A - \sqrt{-1}\,B\big)\\ &= A^2 + B^2.\end{aligned}$$

Exercice 7. (a) En posant $Y := X^\ell$ dans la factorisation connue :

$$Y^q - 1 = (Y - 1)\big(Y^{q-1} + Y^{q-2} + \cdots + Y + 1\big),$$

on trouve :

$$X^{q\,\ell} - 1 = (X^\ell - 1)\big(X^{(q-1)\,\ell} + X^{(q-2)\,\ell} + \cdots + X^\ell + 1\big).$$

(b) Montrons que $X^\ell - 1$ divise $P(X) - R(X)$, ce qui conclura, car comme dans chaque division euclidienne sur $\mathbb{Z}$ on a :

$$0 \leqslant r_k \leqslant \ell - 1 \qquad (0 \leqslant k \leqslant n),$$

le degré de $R(X)$ est strictemnt inférieur à ℓ, et donc $R(X)$ sera bien le reste dans la division euclidienne de $P(X)$ par $X^\ell - 1$.

Écrivons alors la différence :

$$P(X) - R(X) \,=\, \sum_{k=0}^{n} a_k \left(X^k - X^{r_k}\right).$$

Par linéarité, il suffit de faire voir que $X^\ell - 1$ divise chaque $X^k - X^{r_k}$. À cet effet, écrivons les divisions euclidiennes en question :

$$k \,=\, q_k\,\ell + r_k \qquad\qquad (q_k \in \mathbb{N},\ 0 \leqslant r_k \leqslant \ell{-}1,\ k{=}0{,}1{,}\ldots{,}n),$$

et calculons/factorisons :

$$\begin{aligned} X^k - X^{r_k} \,&=\, X^{q_k\ell + r_k} - X^{r_k} \\ &=\, X^{r_k}\left(X^{q_k\ell} - 1\right) \\ &=\, X^{r_k}\left(X^\ell - 1\right)\Big(X^{(q_k-1)\,\ell} + X^{(q_k-2)\,\ell} + \cdots + X^\ell + 1\Big), \end{aligned}$$

ce qui montre bien que $X^\ell - 1$ divise $P(X) - R(X)$.

Exercice 8. (a) Le support $\mathsf{Supp}\,\sigma \,=\, \big\{a_1, a_2, \ldots, a_n\big\}$ de σ est constitué de n éléments distincts, qui sont envoyés par σ sur leur voisin situé juste à droite, avec à la fin $\sigma(a_n) := a_1$.

Il est alors clair — ce qui a d'ailleurs été vu en cours — que les autres éléments du complémentaire :

$$\big\{1, 2, 3, \ldots, \mathrm{N}-1, \mathrm{N}\big\} \Big\backslash \big\{a_1, a_2, \ldots, a_n\big\},$$

restent fixés un à un par σ et par chaque puissance σ^m avec $m \in \mathbb{Z}$. Par conséquent :

$$\mathsf{Supp}\,\sigma^m \,\subset\, \big\{a_1,\ a_2,\ \ldots,\ a_n\big\} \qquad\qquad (\forall\, m \in \mathbb{Z}),$$

et donc, nous pouvons considérer que σ ainsi que ses puissances σ^m n'agissent que sur ces n éléments $a_1, a_2, \ldots, a_n$.

Autrement dit, c'est seulement la restriction de σ à $\{a_1, a_2, \ldots, a_n\}$ qui nous intéresse, et après une renumérotation éventuelle, nous pouvons supposer que $\{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, n\}$.

(b) D'après un résultat du cours, on sait que l'on a en fait :

$$\mathsf{Orb}_\tau(i) \,=\, \big\{i,\ \tau(i),\ \tau^2(i),\ \ldots,\ \tau^{v-1}(i)\big\}.$$

Il s'agit donc de déterminer l'entier minimal v tel que $\tau^v(i) = i$, et de démontrer qu'il vaut $v = n'$.

En partant de :

$$\begin{aligned} \tau(i) \,&=\, \underbrace{\sigma \circ \cdots \circ \sigma \circ \sigma}_{m \text{ fois}}(i) \\ &=\, \underbrace{\sigma \circ \cdots \circ \sigma}_{m-1 \text{ fois}}\big(i + 1 \mod n\big) \\ &=\, \cdots\cdots\cdots\cdots\cdots\cdots \\ &=\, i + m \mod n, \end{aligned}$$

nous avons :

$$\tau^\ell(i) \,=\, i + \ell\, m \mod n,$$

Ainsi $\tau^\ell(i) = i$ s'exprime par :

$$\begin{array}{rrrl} & & i + \ell m & \equiv i \mod n \\ \iff & & \ell m & \equiv 0 \mod n \\ \iff & & \ell d m' & \equiv 0 \mod d n' \\ \iff & \exists \mathrm{K} \in \mathbb{N}^* & \ell d m' & = d n' \mathrm{K} \\ \iff & \exists \mathrm{K} \in \mathbb{N}^* & \ell m' & = n' \mathrm{K}, \end{array}$$

et enfin, le théorème de Gauss avec la primalité relative $1 = n' \wedge m'$ montrent que cela est satisfait si et seulement si ℓ est divisible par n' :

$$\ell = n' \cdot \ell' \qquad \text{avec } \ell' \geqslant 1 \text{ arbitraire.}$$

En conclusion, la valeur minimale v de tels ℓ est atteinte pour $\ell' := 1$, et elle vaut bien $v = n' \cdot 1 = n'$.

(c) Supposons donc que deux éléments de chacune de ces deux orbites coïncident, et déduisons la conséquence voulue :

$$\begin{array}{rrl} & i + \ell m & \equiv j + h m \mod n \\ \iff & i + \ell d m' & \equiv j + h d m' \mod d n' \\ \iff & i - j & \equiv (-\ell + h) d m' \mod d n' \\ \implies & i - j & \equiv 0 \mod d \end{array}$$

(d) Les entiers $\{1, 2, \ldots, d\}$ sont deux à deux distincts modulo d, et donc, la Question **(c)** qui précède garantit, par contraposition, que ces d orbites sont mutuellement disjointes.

Comme elles sont toutes de même cardinal n', d'après la Question **(b)**, et comme $d n' = n$, leur réunion partitionne bien $\{1, 2, \ldots, n\}$.

(e) Ce sont vraiment des corollaires directs et immédiats.

(f) *Oh Yes Elizabeth*, car d'après le cours, toute numérotation des N éléments de E ramène (par isomorphisme) $\mathfrak{S}(E)$ à $\mathfrak{S}_{\mathrm{N}}$. Encore un demi-point sur 20 qui était « donné » !

(g) Par application du résultat qui vient d'être démontré :

n	12	8	6	1	
$\mathsf{pgcd}(4, n)$	4	4	2	1	nombre de cycles
$\frac{n}{\mathsf{pgcd}(4,n)}$	3	2	3	1	longueurs des cycles

et donc le type de σ^4 est :

$$\Big(3,\ 3,\ 3,\ 3,\quad 2,\ 2,\ 2,\ 2,\quad 3,\ 3,\quad 1\Big) = \big(3,\ 3,\ 3,\ 3,\ 3,\ 3,\quad 2,\ 2,\ 2,\ 2,\quad 1\big).$$

11. Examen 6

Exercice 1. Dire si les assertions suivantes sont vraies ou fausses. Démontrer celles qui sont vraies et donner un contre-exemple pour celles qui sont fausses.

(a) Soient a et b deux éléments de $\mathbb{Z}$. Si a est divisible par b, alors a^2 est divisible par b^2.

(b) Soient p un nombre premier et a un entier naturel non nul. Si x et y sont deux entiers vérifiant $a\,x \equiv a\,y \bmod p$, alors on a $x \equiv y \bmod p$.

(c) Soit $n \in \mathbb{N}$ un entier naturel au moins égal à 4. Si n n'est pas premier, alors il existe des entiers a, b avec $a \geqslant 2$ et $b \geqslant 2$ tels que $n = a\,b$.

(d) Soit $n \in \mathbb{N}$ un entier naturel au moins égal à 4. Si n n'est pas premier, alors il existe des entiers a, b premiers entre eux avec $a \geqslant 2$ et $b \geqslant 2$ tels que $n = ab$.

Exercice 2. Le but de cet exercice est de trouver l'ensemble des solutions entières n de l'équation

$$\mathsf{pgcd}\big(2n+8,\, 3n+15\big) \;=\; 6.$$

(a) Montrer que si n est une solution, alors $n \equiv 2 \bmod 3$ et $n \equiv 1 \bmod 2$.

(b) Déduire de la question précédente un entier k tel que si n est une solution alors $n \equiv k \bmod 6$.

(c) Montrer que pour tout entier a les nombres $2a+3$ et $3a+5$ sont premiers entre eux (On pourra par exemple trouver une relation de Bézout).

(d) Vérifier que si $n \equiv k \bmod 6$ alors n est une solution.

Exercice 3. Soit G un ensemble muni d'une loi associative notée $*$. On suppose de plus que $(G, *)$ satisfait les deux propriétés suivantes :

(N) $\exists\, e \in G, \forall\, x \in G,\, e * x = x$: Existence d'un « élément neutre à gauche ».

(I) $\forall x \in G, \exists\, y \in G,\, y * x = e$: Tout élément a un « inverse à gauche ».

(a) Montrer qu'un inverse à gauche est aussi un inverse à droite, *i.e.* :

$$\forall\, x, y \in G \qquad y * x \;=\; e \implies x * y \;=\; e.$$

Indication: On pourra considérer un inverse à gauche z de y et calculer $e * (x * y) \;=\; (z * y) * (x * y)$.

(b) Montrer que e est aussi un élément neutre à droite, *i.e.* :

$$\forall\, x \in G \qquad x * e \;=\; x.$$

Indication: On pourra calculer de deux manières $x * (y * x)$, où y est un inverse à gauche de x.

(c) Montrer que $(G, *)$ est un groupe.

Exercice 4. Soit la permutation suivante d'un ensemble à 12 éléments :

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

(a) Décomposer σ en produit de cycles à supports deux à deux disjoints.

(b) Déterminer l'ordre $o(\sigma)$ de σ.

(c) Décomposer σ^{6666} en produit explicite de cycles à supports disjoints.

(d) Rappeler comment on décompose, dans le groupe $\mathfrak{S}_n$ des permutations de $\{1, 2, 3, \ldots, n\}$, un p-cycle $(a_1 \ a_2 \ \cdots \ a_p)$ quelconque en un produit de transpositions (*i.e.* de 2-cycles).

(e) Décomposer σ en produit de transpositions.

(f) Déterminer la signature de σ.

(g) Déterminer la signature de σ^{6666}.

Exercice 5. **(a)** Décomposer en éléments simples dans $F_{\mathbb{R}}[x]$ la fraction réelle :

$$\frac{x^2 + x + 1}{(x^2 - 1)(x^2 + 1)}.$$

(b) Sur $\mathbb{K} := \mathbb{Z}/5\mathbb{Z}$, décomposer en éléments simples dans $F_{\mathbb{K}}[x]$ la fraction :

$$\frac{x - \overline{1}}{(x + \overline{1})^2 (x + \overline{2})}.$$

Exercice 6. **(a)** Dans $(\mathbb{Z}/9\mathbb{Z}, +)$, déterminer les ordres des éléments suivants, et dire lesquels sont des générateurs : $\overline{5}$, $\overline{6}$, $\overline{7}$.

Exercice 7. En justifiant votre réponse, donner la liste des sous-groupes de G dans chacun des trois cas suivants :

(a) $G = \mathbb{Z}/4\mathbb{Z}$.

(b) $G = \mathbb{Z}/6\mathbb{Z}$.

(c) (Question subsidiaire, à aborder seulement si vous pensez avoir correctement traité tout le reste du sujet.) $G = \mathbb{Z}/n\mathbb{Z}$ avec $n \geqslant 2$.

12. Corrigé de l'examen 6

Exercice 1. **(a)** Vrai ! En effet, a divisible pas b signifie qu'il existe $c \in \mathbb{Z}$ tel que $a = b\,c$, ce qui entraîne que $a^2 = b^2\,c^2$, et donc que b^2 divise a^2.

(b) Faux ! Il ne faut pas se laisser prendre par $a \neq 0$ qui n'est pas suffisant. La bonne hypothèse pour rendre vraie cette affirmation serait a premier à p.

En effet, pour tout $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ et tout $k \in \mathbb{Z}$, on a :

$$k\,p\,x \;\equiv\; k\,p\,y \mod p.$$

Plus concrètement encore, 1 et 2 ne sont par congrus modulo 2, tandis que $2 \cdot 1$ et $2 \cdot 3$ le sont.

(c) Vrai ! Et c'est quasiment la définition !

(d) Faux, Toto ! Un contre-exemple hyper-simple est $n = 4 = 2 \cdot 2$, avec $2 = a = b$.

Exercice 2. Le but de cet exercice est de trouver l'ensemble des solutions entières n de l'équation

$$\mathsf{pgcd}\big(2n + 8,\, 3n + 15\big) \;=\; 6.$$

(a) Si $n \in \mathbb{N}$ est solution de l'équation ci-dessus, on a la suite d'implications :

$$\begin{cases} 6 \,\big|\, 2n + 8 \\ 6 \,\big|\, 3n + 15 \end{cases} \implies \begin{cases} 3 \,\big|\, n + 4 \\ 2 \,\big|\, n + 5 \end{cases} \implies \begin{cases} n + 4 \;\equiv\; 0 \mod 3 \\ n + 5 \;\equiv\; 0 \mod 2 \end{cases} \implies \begin{cases} n \;\equiv\; 2 \mod 3 \\ n \;\equiv\; 1 \mod 2. \end{cases}$$

(b) On sait, d'après le théorème chinois des restes, que l'ensemble des solutions du système de congruences :

$$n \;\equiv\; 2 \mod 3,$$
$$n \;\equiv\; 1 \mod 2,$$

est une classe d'entiers modulo $2 \cdot 3 = 6$, puisque 2 et 3 sont premiers entre eux. On constate alors que $k = 5$ convient.

(c) On constate immédiatement que

$$2 \cdot (3a + 5) - 3 \cdot (2a + 3) \;=\; 6a + 10 - 6a - 9 \;=\; 1\,;$$

si bien que, d'après le théorème de Bézout, $2a + 3$ et $3a + 5$ sont premiers entre eux.

(d) Pour $n \in \mathbb{N}$ supposons que $n \equiv k \mod 6$, il existe $a \in \mathbb{N}$ tel que $n = 6a + k$.

Cherchons alors à déterminer le pgcd de $2n + 8$ et $3n + 15$, *i.e.* le pgcd de :

$$2(6a + k) + 8 \quad \text{et} \quad 3(6a + k) + 15,$$

i.e. puisqu'on peut prendre $k = 5$, le pgcd de :

$$12a + 18 \quad \text{et} \quad 18a + 30.$$

Ce dernier est 6 fois le pgcd de $2a + 3$ et $3a + 5$ dont on a montré dans la Question **(c)** qu'il vaut 1, ce qui répond à la question.

Exercice 3. (a) Pour tout $x \in G$ il existe $y \in G$ tel que $y * x = e$ et $z \in G$ tel que $z * y = e$. Alors :

$$\begin{aligned} x * y &= e * (x * y) \\ &= (z * y) * (x * y) \\ &= ((z * y) * x) * y \\ &= (z * (y * x)) * y \\ &= (z * e) * y \\ &= z * (e * y) \\ &= z * y \\ &= e. \end{aligned}$$

(b) Pour tout $x \in G$, il existe $y \in G$ tel que $y * x = e$. Mais, d'après la Question **(a)**, on a aussi $x * y = e$. Alors :

$$\begin{aligned} x * e &= x * (y * x) \\ &= (x * y) * x \\ &= e * x \\ &= x. \end{aligned}$$

(c) Grâce aux Questions **(a)** et **(b)**, les axiomes de la définition de groupe sont satisfaits.

Exercice 4. (a) On trouve :

$$\sigma = (3\,5\,6)\,(1\,7\,9\,2)\,(4\,12\,10\,11\,8).$$

(b) Lorsque σ est décomposé en produit de cycles à supports deux à deux disjoints comme ci-dessus, l'ordre de σ est le ppcm des ordres de ces cycles. L'ordre d'un cycle est aussi la longueur du cycle. Ainsi :

$$\mathsf{o}(\sigma) = 3 \cdot 4 \cdot 5 = 60.$$

(c) Écrivons $6666 = 60 * 111 + 6$, c'est-à-dire faisons la division euclidienne de 6666 par 60. Il vient alors :

$$\sigma^{6666} = \sigma^{60 \cdot 111 + 6} = (\sigma^{60})^{111}\sigma^6 = \mathsf{Id}^{111}\sigma^6 = \sigma^6,$$

puisque l'on vient de voir que $\sigma^{60} = \mathsf{Id}$.

Notons :

$$\gamma_3 := (3\,5\,6), \qquad \gamma_4 := (1\,7\,9\,2), \qquad \gamma_5 := (4\,12\,10\,11\,8),$$

les cycles qui décomposent σ et sont d'ordres respectifs 3, 4, 5. Par ailleurs, comme ces cycles sont à supports deux à deux disjoints, ils commutent :

$$\forall\, i, j \in \{3, 4, 5\}, \qquad \gamma_i\gamma_j = \gamma_j\gamma_i.$$

Il en résulte que :

$$\begin{aligned} \sigma^{6666} &= \sigma^6 \\ &= \gamma_3^6\gamma_4^6\gamma_5^6 \\ &= \gamma_4^2\gamma_5 \\ &= (1\,9)(7\,2)(4\,12\,10\,11\,8). \end{aligned}$$

(d) On a :

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_p \end{pmatrix} \;=\; (a_1\, a_2)\,(a_2\, a_3)\cdots(a_{p-1}\, a_p),$$

ce qui correspond à un produit de $p-1$ transpositions.

(e) D'après les Questions **(a)** et **(d)**, on a :

$$\begin{aligned} \sigma &= (3\,5\,6)\,(1\,7\,9\,2)\,(4\,12\,10\,11\,8) \\ &= (3\,5)(5\,6)(1\,7)(7\,9)(9\,2)(4\,12)(12\,10)(10\,11)(11\,8). \end{aligned}$$

Noter que, contrairement à la décomposition en cycles donnée à la Question **(a)**, cette décomposition en produit de transpositions n'est pas unique.

(f) La signature d'une transposition vaut -1. De plus, la signature est multiplicative (autrement dit c'est un morphisme de groupes). Ainsi si σ est un produit de r transpositions, la signature de σ est $(-1)^r$. À la Question **(e)**, on a trouvé $r = 9$; si bien que la signature de σ vaut $(-1)^9 \;=\; -1$.

(g) La propriété de multiplicativité de la signature permet de déterminer

$$\varepsilon(\sigma^{6666}) \;=\; \varepsilon(\sigma)^{6666} \;=\; (-1)^{6666} \;=\; 1.$$

On pourrait aussi appliquer les arguments des Questions **(d)** et **(e)** à la décomposition de σ^{6666} trouvée en **(c)**.

Exercice 5. (a) Cherchons $a, b, c, d \in \mathbb{R}$ tels que :

$$\frac{x^2+x+1}{(x^2-1)\,(x^2+1)} \;=\; \frac{a}{x-1} + \frac{b}{x+1} + \frac{cx+d}{x^2+1}.$$

Cette équation donne lieu à la suite d'équivalences :

$$\begin{aligned} & \frac{x^2+x+1}{(x^2-1)\,(x^2+1)} \;=\; \frac{a}{x-1} + \frac{b}{x+1} + \frac{cx+d}{x^2+1} \\ \Longleftrightarrow \quad & x^2+x+1 \;=\; a(x+1)(x^2+1) + b(x-1)(x^2+1) + (cx+d)(x^2-1) \\ \Longleftrightarrow \quad & x^2+x+1 \;=\; (a+b+c)x^3 + (a-b+d)x^2 + (a+b-c)x + (a-b-d). \end{aligned}$$

Cette dernière égalité équivaut aux systèmes linéaires équivalents suivants :

$$\begin{aligned}
& \left\{\begin{array}{rcl} a+b+c & = & 0 \\ a-b+d & = & 1 \\ a+b-c & = & 1 \\ a-b-d & = & 1 \end{array}\right\} \\
\Leftrightarrow \quad & \left\{\begin{array}{rcl} a+b+c & = & 0 \\ a-b+d & = & 1 \\ 2a+2b & = & 1 \\ 2a-2b & = & 2 \end{array}\right\} \\
\Leftrightarrow \quad & \left\{\begin{array}{rcl} a+b+c & = & 0 \\ a-b+d & = & 1 \\ 2a+2b & = & 1 \\ 4a & = & 3 \end{array}\right\} \\
\Leftrightarrow \quad & \left\{\begin{array}{rcl} a & = & \frac{3}{4} \\ b & = & -\frac{1}{4} \\ c & = & -\frac{1}{2} \\ d & = & 0 \end{array}\right\},
\end{aligned}$$

si bien que :

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

(b) Pour $a, b, c \in \mathbb{K}$ on a (en omettant les barres pour alléger les notations) :

$$\begin{aligned}
\frac{x-1}{(x+1)^2(x+2)} &= \frac{ax+b}{(x+1)^2} + \frac{c}{x+2} \\
\Longleftrightarrow \qquad x-1 &= (ax+b)(x+2) + c(x+1)^2 \\
\Longleftrightarrow \qquad x-1 &= (a+c)x^2 + (2a+b+2c)x + 2b + c.
\end{aligned}$$

D'où le système linéaire :

$$\begin{aligned}
\Longleftrightarrow \quad & \left\{\begin{array}{rcl} a+c & = & 0 \\ 2a+b+2c & = & 1 \\ 2b+c & = & -1 \end{array}\right\} \\
\Longleftrightarrow \quad & \left\{\begin{array}{rcl} a+c & = & 0 \\ b & = & 1 \\ 2b+c & = & -1 \end{array}\right\} \\
\Longleftrightarrow \quad & \left\{\begin{array}{rcl} a & = & 3 \\ b & = & 1 \\ c & = & -3 \end{array}\right\}
\end{aligned}$$

On a donc dans $\mathbb{Z}/5\mathbb{Z}$ la décomposition :

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

Exercice 6. (a) Pour tout $a \in \mathbb{Z}$, l'ordre de $\overline{a}$ dans $\mathbb{Z}/9\mathbb{Z}$ est $\frac{9}{\mathsf{pgcd}\,(9,a)}$. Cela montre que $\overline{5}$ et $\overline{7}$ sont d'ordre 9, c'est-à-dire sont des générateurs de $\mathbb{Z}/9\mathbb{Z}$, et que $\overline{6}$ est d'ordre 3.

Plutôt que d'utiliser que l'ordre vaut $\frac{9}{\mathsf{pgcd}\,(9,a)}$, on pouvait aussi faire la liste des restes dans la division euclidienne par 9 des multiples de a, jusqu'à tomber sur 0. L'ordre de $\overline{a}$ est alors le nombre d'éléments de cette liste. Par exemple pour $a = 6$ on obtient $\overline{a} = \overline{6}$, $2\overline{a} = \overline{12} = \overline{3}$ et $3\overline{a} = \overline{18} = \overline{0}$, donc l'ordre de $\overline{a}$ est 3.

Exercice 7. (a) Il est clair que $\{\overline{0}\}$, $\{\overline{0}, \overline{2}\}$ et $\mathbb{Z}/4\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}/4\mathbb{Z}$: montrons que ce sont les seuls. Soit H un sous-groupe de $\mathbb{Z}/4\mathbb{Z}$. Alors son cardinal divise 4 donc c'est 1, 2 ou 4. Si c'est 1 ou 4 alors H est égal à $\{\overline{0}\}$ ou à $\mathbb{Z}/4\mathbb{Z}$. Supposons désormais que H est de cardinal 2, c'est-à-dire de la forme $\{\overline{0}, \overline{a}\}$ avec $\overline{a} \neq \overline{0}$. Si $\overline{a}$ est égal à $\overline{1}$ ou à $\overline{3}$ alors $2\overline{a} = \overline{2} \in H$ ce qui est contradictoire. Donc $\overline{a} = \overline{2}$ et $H = \{\overline{0}, \overline{2}\}$.

(b) Clairement $\{\overline{0}\}$, $\{\overline{0}, \overline{3}\}$, $\{\overline{0}, \overline{2}, \overline{4}\}$ et $\mathbb{Z}/6\mathbb{Z}$ conviennent. Si H est un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$, son cardinal est 2, 3, 6 ou 1. Les deux derniers cas se traitent comme en **(a)**. Si H est de cardinal 2 alors $H = \{\overline{0}, \overline{a}\}$ avec $\overline{a} \neq \overline{0}$ et $2\overline{a} \in H$. Comme $2\overline{a} = \overline{a}$ imposerait $\overline{a} = \overline{0}$, on a donc $2\overline{a} = \overline{0}$ d'où $\overline{a} = \overline{3}$. Reste à traiter le cas où H est de cardinal 3. Il existe alors $a \in \mathbb{Z}$ tel que $\overline{a} \neq \overline{0}$ et $\overline{a} \in H$. L'ordre de $\overline{a}$ divise 3 et n'est pas 1 donc c'est 3, et $H = \{\overline{0}, \overline{a}, 2\overline{a}\}$ avec $\overline{a} = \overline{2}$ ou $\overline{a} = \overline{4}$ (qui conduisent au même sous-groupe).

(c) Toute partie de la forme $\left\{\overline{d}, 2\overline{d}, \ldots, \frac{n}{d}\overline{d} = \overline{n} = \overline{0}\right\}$, où $d \geqslant 1$ divise n, est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ noté H_d (en effet c'est le sous-groupe engendré par $\overline{d}$). Soit H un sous-groupe quelconque de $\mathbb{Z}/n\mathbb{Z}$; notons δ son cardinal. Alors δ divise n ; posons $d = n/\delta$. Soit $a \in \mathbb{Z}$ tel que $\overline{a} \in H$. L'ordre de $\overline{a}$ divise celui de H donc $\delta\overline{a} = \overline{0}$, c'est-à-dire $n|\delta a$. Comme $n = \delta d$ cela donne $d|a$ d'où $\overline{a} \in H_d$. On a donc $H \subset H_d$; comme ces deux ensembles ont même cardinal, ils sont égaux.

13. Examen 7

Exercice 1. Soient $a \geqslant 1$ et $b \geqslant 1$ deux nombres entiers premiers entre eux, *i.e.* $a \wedge b = 1$. On pose :

$$c := (a-b)^2 \qquad \text{et} \qquad d := a^2 - a\,b + b^2.$$

L'objectif est d'établir que pgcd $(c, d) = 1$. On raisonne par contradiction.

(a) Soit p un nombre premier (donc $p \geqslant 2$) qui divise à la fois c et d :

$$p \mid c \qquad \text{et} \qquad p \mid d.$$

Montrer que $p \,\big|\, a\,b$.

(b) Montrer que $p \,\big|\, (a-b)$.

(c) Montrer que $p \mid a^2$.

(d) Montrer que $p \mid b^2$.

(e) Déterminer pgcd (c, d).

Exercice 2. Soient deux entiers $m \geqslant 2$ et $n \geqslant 2$. Soient C_m un groupe cyclique à m éléments, et C_n un groupe cyclique à n éléments.

(a) À quels groupes connus C_m et C_n sont-ils isomorphes ? Justifier la réponse en invoquant un théorème du cours.

(b) Lorsque $m \wedge n = 1$ sont premiers entre eux, montrer que le groupe produit $C_m \times C_n$ est aussi cyclique. Indication: Appliquer le cours.

(c) Lorsque $m \wedge n > 1$ ne sont *pas* premiers entre eux, établir que $C_m \times C_n$ n'est *pas* cyclique. Indication: On pourra raisonner par l'absurde, et se servir de ppcm (m, n).

Exercice 3. L'objectif est de montrer que l'ensemble $\mathbb{R}^3$, muni de la loi interne $*$ définie par :

$$(a, b, c) * (a', b', c') := \big(a + a',\ b + b' + a\,c',\ c + c'\big),$$

est un *groupe*.

(a) Montrer que cette loi est associative.

(b) Vérifier que $(0, 0, 0)$ est élément neutre.

(c) Trouver l'inverse (a', b', c') d'un élément quelconque (a, b, c), et vérifier qu'il est effectivement inverse. Indication: Deux conditions doivent être satistaites par un inverse.

(d) Ce groupe $(\mathbb{R}^3, *)$ est-il commutatif ?

Exercice 4. L'objectif est de démontrer qu'il n'existe *pas* d'entiers $x, y, z \in \mathbb{Z}$ non tous nuls, *i.e.* $(x, y, z) \neq (0, 0, 0)$, satisfaisant l'équation diophantienne :

$$(\mathsf{ED}) \qquad 5\,x^3 + 11\,y^3 + 13\,z^3 = 0.$$

(a) Dans $\mathbb{Z}/13\mathbb{Z}$, calculer $\overline{1}^3$, $\overline{2}^3$, $\overline{3}^3$, $\overline{4}^3$, $\overline{5}^3$, $\overline{6}^3$, comme éléments de $\big\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{11}, \overline{12}\big\}$. Indication: Bien vérifier ses calculs avant de poursuivre.

(b) En déduire les valeurs de $\overline{12}^3$, $\overline{11}^3$, $\overline{10}^3$, $\overline{9}^3$, $\overline{8}^3$, $\overline{7}^3$. Indication: L'ensemble $\{\overline{1}^3, \overline{2}^3, \ldots, \overline{11}^3, \overline{12}^3\}$ contient exactement 4 éléments distincts.

(c) Trouver deux entiers :

$$-12 \leqslant \alpha \leqslant -1 \qquad \text{et} \qquad 1 \leqslant \beta \leqslant 5,$$

qui satisfont :

$$5\,\alpha + 13\,\beta = 1.$$

(d) Montrer que l'équation diophantienne (ED) implique $x^3 \equiv 3\,y^3 \mod 13$.

(e) Quels sont les cinq éléments distincts de l'ensemble :

$$E := \{\overline{0}^3, \overline{1}^3, \overline{2}^3, \ldots, \overline{11}^3, \overline{12}^3\} \textbf{ ?}$$

Déterminer ensuite les éléments distincts de l'ensemble :

$$F := \{\overline{3}\cdot\overline{0}^3,\ \overline{3}\cdot\overline{1}^3,\ \overline{3}\cdot\overline{2}^3,\ \ldots,\ \overline{3}\cdot\overline{11}^3,\ \overline{3}\cdot\overline{12}^3\}.$$

(f) Montrer, pour toute solution $(x, y, z) \neq (0, 0, 0)$ de l'équation (ED), que :

$$x \equiv 0 \mod 13 \qquad \text{et} \qquad y \equiv 0 \mod 13.$$

(g) Toujours avec $(x, y, z) \neq (0, 0, 0)$ solution de (ED), montrer que :

$$z \equiv 0 \mod 13.$$

(h) Montrer que si l'on connaît une solution entière $(x, y, z) \neq (0, 0, 0)$ de l'équation $5\,x^3 + 11\,y^3 + 13\,z^3 = 0$, on peut trouver une solution entière $(x', y', z') \neq (0, 0, 0)$ telle que x', y', z' soient *mutuellement premiers entre eux*, c'est-à-dire avec $1 = \mathrm{pgcd}\,(x', y', z')$.

(i) Conclure.

Exercice 5. L'objectif est de démontrer que le groupe des inversibles $\big(\mathbb{Z}/17\mathbb{Z}\big)^\times$ de l'anneau $\big(\mathbb{Z}/17\mathbb{Z}, +\times\big)$ est *cyclique*, l'une des découvertes de Gauss lorsqu'il était adolescent. Le point-clé, c'est que $17 - 1 = 2^4$ est une puissance de 2, donc a pour diviseurs 1, 2, 4, 8, 16.

(a) Dans $\mathbb{Z}/17\mathbb{Z}$, en partant de $\overline{3}^1 = \overline{3}$, vérifier que $\overline{3}^2 = -\,\overline{8}$, que $\overline{3}^4 = -\,\overline{4}$, que $\overline{3}^8 = -\,\overline{1}$, et enfin calculer $\overline{3}^{16}$.

(b) Soit $n \in \mathbb{N}_{\geqslant 1}$ l'ordre multiplicatif de $\overline{3}$ dans $\big(\mathbb{Z}/17\mathbb{Z}\big)^\times$, c'est-à-dire le plus petit entier strictement positif tel que $\overline{3}^n = \overline{1}$ dans $\mathbb{Z}/17\mathbb{Z}$. Montrer que :

$$n \,\big|\, 16.$$

(c) Montrer que $n \nmid 8$. Indication: On pourra raisonner par l'absurde.

(d) En déduire que $n = 16$.

(e) Justifier que l'ordre (le nombre d'éléments) du groupe multiplicatif $\big(\mathbb{Z}/17\mathbb{Z}\big)^\times$ est égal à 16.

(f) On introduit le morphisme de groupes :

$$\begin{aligned} f\colon \quad (\mathbb{Z}, +) &\longrightarrow \Big(\big(\mathbb{Z}/17\mathbb{Z}\big)^\times, \times\Big) \\ k &\longmapsto \overline{3}^k =: f(k). \end{aligned}$$

Établir que f est surjectif. Indication: Montrer que $\overline{3}^1, \overline{3}^2, \ldots, \overline{3}^{16}$ sont distincts deux à deux modulo 17.

(g) Montrer que $\mathsf{Ker}\, f = 16\,\mathbb{Z}$.

(h) En déduire l'existence d'un isomorphisme de groupes :

$$\mathbb{Z}/16\mathbb{Z} \xrightarrow{\sim} \big(\mathbb{Z}/17\mathbb{Z}\big)^{\times},$$

les lois étant l'addition à gauche, et la multiplication à droite.

Exercice 6. **(a)** Montrer que pour tout entier $n \in \mathbb{N}$, on a :

$$3^{n+3} - 4^{4\,n+2} \equiv 0 \mod 11.$$

Exercice 7. Soit un groupe *fini* G, avec $2 \leqslant \mathsf{Card}\, G < \infty$, dont la loi $*$ est notée multiplicativement, et soit $e := 1_G \in G$ son élément neutre. On fait l'hypothèse forte :

$$\forall\, g \in G, \qquad g^2 = e.$$

(a) Montrer que G est en fait *commutatif*. Indication: Que vaut l'inverse g^{-1} ?

(b) Pour un élément quelconque $g \in G \backslash \{e\}$, montrer que le sous-groupe $\langle g \rangle \subset G$ engendré par g est *isomorphe* à $\mathbb{Z}/2\mathbb{Z}$.

(c) Établir que G est *isomorphe* à un groupe produit :

$$\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z},$$

constitué d'un certain nombre $r \geqslant 1$ de facteurs.

14. Corrigé de l'examen 7

Exercice 1. (a) Rappelons la propriété générale, valable pour $m, n, \lambda, \mu \in \mathbb{Z}$ quelconques, dans laquelle $p \in \mathbb{Z}^*$ n'est pas forcément premier :

$$\Big(p \,|\, m \quad \text{et} \quad p \,|\, n\Big) \qquad \Longrightarrow \qquad p \,\Big|\, \big(\lambda\, m + \mu\, n\big).$$

Ainsi, puisque :

$$\begin{aligned} -\,c + d \;&=\; -\,\big(a^2 - 2\,a\,b + b^2\big) + a^2 - a\,b + b^2 \\ &=\; a\,b, \end{aligned}$$

il vient bien :

$$\Big(p \,|\, c \quad \text{et} \quad p \,|\, d\Big) \qquad \Longrightarrow \qquad p \,\Big|\, a\,b.$$

(b) D'après le théorème d'Euclide, si un nombre premier p divise un produit quelconque $n_1 \cdots n_i \cdots n_r$ de nombres entiers, alors il divise un des facteurs n_i. Donc quand les facteurs sont tous les mêmes, on a bien :

$$p \,\Big|\, (a-b)(a-b) \qquad \Longrightarrow \qquad p \,\Big|\, (a-b).$$

(c) Trivialement :

$$\begin{aligned} p \,\Big|\, (a-b) \qquad &\Longrightarrow \qquad p \,\Big|\, (a-b)\,b \\ &\qquad\;\; \text{c.-à-d.} \qquad p \,\Big|\, a\,b - b^2, \end{aligned}$$

et ensuite :

$$\Big(p \,\Big|\, a^2 - a\,b + b^2 \quad \text{et} \quad p \,\Big|\, a\,b - b^2\Big) \qquad \Longrightarrow \qquad p \,|\, a^2.$$

(d) Comme toutes les hypothèses de cet exercice sont symétriques à travers l'échange $a \longleftrightarrow b$, nous obtenons sans effort aussi :

$$p \,|\, b^2.$$

(e) Ainsi, si on avait $\mathsf{pgcd}\,(c, d) > 1$, tout diviseur premier p de $\mathsf{pgcd}\,(c, d)$ diviserait à la fois a^2 et b^2, donc grâce au théorème d'Euclide, diviserait à la fois a et b. Mais comme par hypothèse $a \wedge b = 1$, c'est une contradiction. En conclusion :

$$\mathsf{pgcd}\,(c, d) \;=\; 1.$$

Exercice 2. (a) D'après un théorème du cours, tout groupe cyclique G d'ordre (*i.e.* de cardinal) un entier $p \geqslant 2$, est isomorphe à $\big(\mathbb{Z}/p\mathbb{Z}, +\big)$. Ainsi :

$$C_m \simeq \mathbb{Z}/m\mathbb{Z} \qquad \text{et} \qquad C_n \simeq \mathbb{Z}/n\mathbb{Z}.$$

(b) Encore d'après un (autre) théorème du cours, essentiellement équivalent au théorème des restes chinois, lorsque $m \wedge n = 1$ sont premiers entre eux, on a un *isomorphisme d'anneaux* (donc un isomorphisme de groupes additifs sous-jacents) :

$$\begin{aligned} \mathbb{Z}/mn\,\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x \bmod mn &\longmapsto \big(x \bmod m,\ x \bmod n\big). \end{aligned}$$

Comme $\mathbb{Z}/mn\mathbb{Z}$ est cyclique, engendré par $\overline{1}$, et comme les isomorphismes entre groupes préservent les propriétés structurelles telles que *e.g.* la cyclicité, il est clair que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique, et qu'il en va de même pour $C_m \times C_n$.

(c) Maintenant, si $d := \mathsf{pgcd}\,(m, n)$ est > 1, écrivons :

$$m = d\,m' \qquad \text{et} \qquad n = d\,n',$$

d'où :

$$\mathsf{ppcm}\,(m, n) = d\,m'\,n' < d\,m'\,d\,n' = m\,n.$$

Par l'absurde, supposons que le groupe produit $C_m \times C_n$, de cardinal $m\,n$, soit cyclique. Alors il serait isomorphe à $\mathbb{Z}/mn\,\mathbb{Z}$, grâce au rappel de cours de la Question **(a)**.

Nécessairement, il devrait exister un élément dans ce groupe $C_m \times C_n$ qui *l'engendrerait* (additivement). On noterait alors (x, y) un tel élément.

Ensuite, les mn itérés additifs successifs de cet élément :

$$(0,0), \quad (x,y), \quad (2x,\,2y), \quad \ldots, \quad (kx, ky), \quad \ldots, \quad \big((mn-1)x,\,(mn-1)y\big),$$

devraient donc être distincts deux à deux, afin de décrire tous les mn éléments de $\mathbb{Z}/mn\mathbb{Z}$.

Mais ceci est radicalement impossible !

En effet, déjà pour :

$$k := d\,m'\,n' \leqslant m\,n - 1,$$

il est clair que l'on a :

$$\big(k\,x,\ k\,y\big) = \big(n'\,m\,x,\ m'\,n\,x\big) = (0,0) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

et donc les $m\,n$ éléments en question ne sont *pas* distincts deux à deux.

Cette (lamentable !) contradiction montre bien que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est *jamais* cyclique dès que $m \wedge n > 1$. Éh oui, la vie est dure !

Exercice 3. L'objectif est de montrer que l'ensemble $\mathbb{R}^3$, muni de la loi interne $*$ définie par :

$$(a, b, c) * (a', b', c') := \big(a + a',\ b + b' + a\,c',\ c + c'\big),$$

est un *groupe*.

(a) En effet, calculons avec soin :

$$\begin{aligned}
\Big((a,b,c)*(a',b',c')\Big)*(a'',b'',c'') &= \Big(a+a',\ b+b'+a\,c',\ c+c'\Big)*(a'',b'',c'') \\
&= \Big((a+a')+a'',\ \ (b+b'+a\,c')+b''+(a+a')\,c'',\ \ (c+c')+c''\Big) \\
&= \Big(a+(a'+a''),\ \ b+\big(b'+b''+a'c''\big)+a\,(c'+c''),\ \ c+(c'+c'')\Big) \\
&= (a,b,c)*\Big(a'+a'',\ \ b'+b''+a'c'',\ \ c'+c''\Big) \\
&= (a,b,c)*\Big((a',b',c')*(a'',b'',c'')\Big),
\end{aligned}$$

ce qui est l'associativité.

(b) En effet :

$$\begin{aligned}
(a,b,c)*(0,0,0) &= \big(a+0,\ b+0+a\cdot 0,\ c+0\big) = (a,b,c), \\
(0,0,0)*(a,b,c) &= \big(0+a,\ 0+b+0\cdot c,\ 0+c\big) = (a,b,c).
\end{aligned}$$

(c) Puisque l'on connaît l'élément neutre, l'inverse (a',b',c') de (a,b,c) doit satisfaire :

$$\begin{aligned}
(0,0,0) &= (a,b,c)*(a',b',c') \\
&= \big(a+a',\ b+b'+a\,c',\ c+c'\big),
\end{aligned}$$

d'où nécessairement :

$$a' := -a, \qquad c' := -c, \qquad b' := -b+a\,c.$$

Il reste encore à vérifier qu'en multpliant dans l'autre sens, on retrouve bien l'élément neutre :

$$\begin{aligned}
(a',b',c')*(a,b,c) &= \big(-\,a,\ -b+a\,c,\ -c\big)*(a,b,c) \\
&= \Big(-\,a+a,\ -b+a\,c+b+(-a)\cdot c,\ -c+c\Big) \\
&= (0,0,0).
\end{aligned}$$

Ainsi, $(\mathbb{R}^3,*)$ est bien un groupe.

(d) Non, $(\mathbb{R}^3,*)$ n'est pas commutatif, parce que :

$$(1,0,0)*(0,0,1) = (1,1,1),$$

est différent de :

$$(0,0,1)*(1,0,0) = (1,0,1).$$

Exercice 4. (a) On calcule modulo 13 :

$$\overline{1}^3 = \overline{1}, \qquad \overline{2}^3 = \overline{8}, \qquad \overline{3}^3 = \overline{27} = \overline{1},$$

puis :

$$\begin{aligned}
\overline{4}^3 &= \overline{4}\cdot\overline{16} = \overline{4}\cdot\overline{3} = \overline{12}, \\
\overline{5}^3 &= \overline{5}\cdot\overline{25} = \overline{5}\cdot(-\overline{1}) = \overline{8}, \\
\overline{6}^3 &= \overline{6}\cdot\overline{36} = \overline{6}\cdot(-\overline{3}) = -\,\overline{18} = -\,\overline{5} = \overline{8}.
\end{aligned}$$

(b) Comme on a modulo 13 :

$$\overline{12} = -\,\overline{1}, \qquad \overline{11} = -\,\overline{2}, \qquad \overline{10} = -\,\overline{3}, \qquad \overline{9} = -\,\overline{4}, \qquad \overline{8} = -\,\overline{5}, \qquad \overline{7} = -\,\overline{6},$$

il vient en utilisant la Question **(a)** qui précède :

$$\begin{aligned}\overline{12}^3 &= -\overline{1}^3, & \overline{11}^3 &= -\overline{2}^3, & \overline{10}^3 &= -\overline{3}^3, & \overline{9}^3 &= -\overline{4}^3, & \overline{8}^3 &= -\overline{5}^3, & \overline{7}^3 &= -\overline{6}^3,\\ &= \overline{12}, & &= \overline{5}, & &= \overline{12}, & &= \overline{1}, & &= \overline{5}, & &= \overline{5}.\end{aligned}$$

(c) Euclidivisons :

$$\begin{aligned}13 &= 2\cdot 5 + 3\\ 5 &= 1\cdot 3 + 2\\ 3 &= 1\cdot 2 + \boxed{1}\\ 2 &= 2\cdot 1 + \mathbf{0},\end{aligned}$$

et saumons-remontons :

$$\begin{aligned}-5\cdot 5 + 2\cdot 13 &= -1\cdot 5 + 2\cdot\big(13 - 2\cdot 5\big) =\\ &= -1\cdot 5 + 2\cdot \underline{3}_{\text{rpl}} = 3 - 1\cdot\big(5 - 1\cdot 3\big) =\\ &= 3 - 1\cdot \underline{2}_{\text{rpl}} = \mathbf{1},\end{aligned}$$

pour obtenir :

$$\underbrace{(-5)}_{\alpha}\cdot 5 + \underset{\beta}{2}\cdot 13 = 1.$$

(d) Modulo 13, le terme $13\cdot z^3$ disparaît, d'où :

$$(-5)\cdot\Big(\ 5\,x^3 \equiv -11\,y^3 \mod 13\ \Big),$$

et après multiplication par -5 qui est l'inverse de 5 dans $\big(\mathbb{Z}/13\mathbb{Z}\big)^\times$ grâce à la Question **(c)**, nous obtenons :

$$\begin{aligned}x^3 &\equiv 55\,y^3 \mod 13\\ &\equiv 3\,y^3 \mod 13.\end{aligned}$$

(e) Nous avons déjà implicitement constaté que :

$$E = \big\{\overline{0},\ \overline{1},\ \overline{5},\ \overline{8},\ \overline{12}\big\},$$

d'où en multipliant ces cinq éléments par $\overline{3}$ dans $\mathbb{Z}/13\mathbb{Z}$:

$$F = \big\{\overline{0},\ \overline{3},\ \overline{2},\ \overline{11},\ \overline{10}\big\}.$$

(f) Comme $x^3 \equiv 3\,y^3 \mod 13$, les seules valeurs communes possibles de $\overline{x}^3 = \overline{3}\,\overline{y}^3$ appartiennent à l'intersection :

$$E\cap F = \big\{\overline{0}\big\}.$$

Et comme cette unique valeur possible $\overline{0}$ provient seulement de $\overline{x} = \overline{0}$ et de $\overline{y} = \overline{0}$, nous avons bien :

$$x \equiv 0 \mod 13 \qquad \text{et} \qquad y \equiv 0 \mod 13.$$

(g) Nous savons que :

$$x = 13\,x' \qquad \text{et} \qquad y = 13\,y' \qquad (x', y' \in \mathbb{Z}),$$

d'où en revenant à (ED) :

$$13\,z^3 = 13^3\big(-5\,x'^{13} - 11\,y'^{13}\big),$$

puis après division par 13 :

$$z^3 \,=\, 13^2\, u,$$

pour un certain entier $u \in \mathbb{Z}$. Ainsi, z^3 est divisible par 13, et comme 13 est un nombre premier, z lui-même est divisible par 13, c'est-à-dire que $z \equiv 0 \mod 13$.

(h) Soit donc $(x, y, z) \neq (0, 0, 0)$ solution de (ED). Posons :

$$d \,:=\, \mathsf{pgcd}\,(x, y, z),$$

puis :

$$x \,=:\, d\,x', \qquad\qquad y \,=:\, d\,y', \qquad\qquad z \,=:\, d\,z'.$$

Comme x, y, z sont tous à la puissance 3 dans (ED), nous pouvons factoriser puis simplifier par d^3 :

$$\begin{aligned} 0 \,&=\, 5\,(d\,x')^3 + 11\,(d\,y')^3 + 13\,(d\,z')^3 \\ &=\, \underline{d^3}_{\circ}\,\big[5\,x'^3 + 11\,y'^3 + 13\,z'^3,\big], \end{aligned}$$

donc $(x', y', z') \neq (0, 0, 0)$ est (bien) aussi solution, sans facteur commun, de (ED).

(i) Par l'absurde, si l'équation diophantienne (ED) possédait une solution $(x, y, z) \neq (0, 0, 0)$, alors elle posséderait *aussi* une solution $(x, y, z) \neq (0, 0, 0)$ telle que x, y, z n'aient aucun facteur en commun, grâce à la Question **(h)** vue à l'instant, en contradiction flagrante avec les raisonnements qui nous ont conduits à constater que *toute* solution a ses *trois* coordonnées x, y, z multiples de 13 (facteur commun).

Exercice 5. (a) Il suffit de prendre le carré, modulo 17, du résultat précédent, en admettant des résultats négatifs afin de faciliter les calculs :

$$\overline{3}^1 \,=\, \overline{3}, \qquad \overline{3}^2 \,=\, \overline{9} \,=\, -\,\overline{8}, \qquad \begin{aligned} \overline{3}^4 \,&=\, \big(-\,\overline{8}\big)^2 \,=\, \overline{64} \,=\, -\,\overline{4}, \\ \overline{3}^8 \,&=\, \big(-\,\overline{4}\big)^2 \,=\, \overline{16} \,=\, -\,\overline{1}, \\ \overline{3}^{16} \,&=\, \big(-\,\overline{1}\big)^2 \,=\, \overline{1}. \end{aligned}$$

(b) Puisque nous venons de voir que $\overline{3}^{16} = \overline{1}$, un théorème du cours donne bien $n \,\big|\, 16$.

On peut redémontrer ce fait dans ce cas précis comme suit. Effectuons la division euclidienne de 16 par n :

$$16 \,=\, n\,q + r,$$

avec $q \in \mathbb{N}$ et $r \in \{0, 1, \ldots, n-1\}$. On a alors :

$$\overline{1} \,=\, \overline{3}^{16} \,=\, \overline{3}^{n\,q+r} \,=\, \big(\overline{3}^n\big)^q \cdot \overline{3}^r \,=\, \overline{1}^q \cdot \overline{3}^r \,=\, \overline{3}^r,$$

et comme par définition de l'ordre n, aucune puissances $\overline{3}^1, \ldots, \overline{3}^{n-1}$ ne peut être égale à $\overline{1}$, nécessairement $r = 0$, d'où :

$$16 \,=\, n\,q,$$

ce qui exprime bien que n divise 16 !

(c) Par l'absurde, supposons que $n \,|\, 8$. Autrement dit :

$$8 \,=\, n\,k \qquad\qquad (\exists\, k \in \mathbb{N}_{\geqslant 1}).$$

Alors par un calcul similaire à celui qui précède, on en déduit que :

$$\overline{3}^8 \,=\, \overline{3}^{n\,k} \,=\, \big(\overline{3}^n\big)^k \,=\, \overline{1}^k \,=\, \overline{1},$$

ce qui est une contradiction, puisque nous venons de voir dans la Question **(a)** que $\overline{3}^8 = \overline{16} = -\overline{1}$. Donc $n \nmid 8$.

(d) Par la Question **(b)**, nous savons que $n \mid 16 = 2^4$, d'où :

$$n \in \{1,\, 2^1,\, 2^2,\, 2^3,\, 2^4\},$$

et comme nous venons aussi de voir que $n \nmid 8 = 2^3$, il est clair que :

$$n = 2^4.$$

(e) Pour tout entier premier $p \in \mathscr{P}$, on a vu en cours, que le groupe multiplicatif :

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^\times = \{\overline{1}, \ldots, \overline{p-1}\},$$

de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est constitué de tous les nombres modulo p à l'exception d'un seul, $\overline{0}$, ceci, parce que tous les entiers $1 \leqslant i \leqslant p-1$ sont premiers avec p, de telle sorte que le théorème de Bézout :

$$u\,i + v\,p = 1 \qquad (\exists\, u \in \mathbb{Z}, \exists\, v \in \mathbb{Z}),$$

lu (réduit) modulo p, permet d'obtenir l'inverse multiplicatif $\overline{u}$ de $\overline{i}$ dans $\mathbb{Z}/p\mathbb{Z}$:

$$\overline{u}\,\overline{i} + \overline{0} = \overline{1}.$$

Ainsi :

$$p - 1 = \Big|\big(\mathbb{Z}/p\mathbb{Z}\big)^\times\Big|,$$

et ici avec l'entier $p = 17$ qui est bien premier, nous avons donc justifié que :

$$16 = 17 - 1 = \Big|\big(\mathbb{Z}/17\mathbb{Z}\big)^\times\Big|.$$

(f) Par l'absurde, s'il existait deux entiers $1 \leqslant i < j \leqslant 16$ tels que :

$$\overline{3}^j = \overline{3}^i \mod 17,$$

on en déduirait :

$$\overline{3}^{j-i} \equiv \overline{1} \mod 17,$$

et comme :

$$1 \leqslant j - i \leqslant 15,$$

ceci contredirait le fait, établi à la Question **(d)**, que l'entier minimal n tel que $\overline{3}^n = \overline{1}$ vaut $n = 16$, lequel est … strictement supérieur à 15 !

Ainsi, nous avons trouvé 16 éléments distincts $\overline{3}^1$, $\overline{3}^2$, …, $\overline{3}^{16}$ dans l'image de notre morphisme f, et comme le cardinal (l'ordre) de $\big(\mathbb{Z}/17\mathbb{Z}\big)^\times$ est égal à 16, c'est terminé, f est bien surjectif !

(g) Effectivement, un élément $k \in \mathsf{Ker}\, f$ qui satisfait par définition :

$$\overline{3}^k = \overline{1} \mod 17,$$

doit, d'après le résultat de la Question **(d)** et grâce à un théorème vu en cours, être multiple de l'ordre $16 = n$ de $\overline{3}$, ce qui veut bien dire que $k \in 16\,\mathbb{Z}$.

On peut redémontrer ici dans cette circonstance numérique spécifique le théorème vu en cours comme suit. Effectuons la division euclidienne :

$$k = 16\,q + r,$$

avec $q \in \mathbb{Z}$ et $r \in \{0, 1, \ldots, 15\}$. Alors :

$$\overline{1} \,=\, \overline{3}^k \,=\, \overline{3}^{16\,q+r} \,=\, \big(\overline{3}^{16}\big)^q \cdot \overline{3}^r \,=\, \overline{1}^q \cdot \overline{3}^r \,=\, \overline{3}^r,$$

et comme 16 est l'ordre de $\overline{3}$, cette équation force $r = 0$, ce qui veut bien dire que :

$$k \,=\, 16\,q \;\in\; 16\,\mathbb{N},$$

vu que l'on sait déjà que $\overline{3}^{16} = \overline{1}$.

(h) En partant du morphisme :

$$\mathbb{Z} \xrightarrow{\;f\;} \big(\mathbb{Z}/17\mathbb{Z}\big)^\times$$

dont on connaît le noyau $\mathsf{Ker}\, f = 16\,\mathbb{Z}$, le *Théorème de factorisation* vu en cours s'applique et nous donne le diagramme suivant :

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "f"] \arrow[d, "\pi"'] & \big(\mathbb{Z}/17\mathbb{Z}\big)^\times \\
\mathbb{Z}/16\mathbb{Z} \arrow[ur, "\sim", "\overline{f}"'] &
\end{tikzcd}$$

qui est *commutatif*, au sens où :

$$f \,=\, \overline{f} \circ \pi,$$

avec un morphisme $\overline{f}$ qui est un *isomorphisme*, puisqu'on s'est « débarassé du noyau ».

Exercice 6. (a) Calculons astucieusement :

$$\begin{aligned}
3^{n+3} - 4^{4\,n+2} \,&=\, 3^3 \cdot 3^n - 4^2 \cdot (4^4)^n \\
&=\, 27 \cdot 3^n - 16 \cdot \big(16 \cdot 16\big)^n \\
&\equiv\, 5 \cdot 3^n - 5 \cdot (5 \cdot 5)^n \mod 11 \\
&=\, \underline{5 \cdot 3^n}_{\circ} - \underline{5 \cdot 3^n}_{\circ} \mod 11 \\
&\equiv\, 0 \mod 11.
\end{aligned}$$

Exercice 7. (a) Pour $g, h \in G$ quelconques, puisque $g^{-1} = g$ et $h^{-1} = h$, interrogeons-nous sur la commutation :

$$\begin{aligned}
g\,h \overset{?}{=} h\,g \qquad &\Longleftrightarrow \qquad (h\,g)^{-1}\,g\,h \overset{?}{=} e \\
&\Longleftrightarrow \qquad g^{-1}h^{-1}\,g\,h \overset{?}{=} e \\
&\Longleftrightarrow \qquad g\,h\,g\,h \overset{?}{=} e \\
&\Longleftrightarrow \qquad \big(g\,h\big)^2 \overset{\text{OUI}}{=} e
\end{aligned}$$

(b) Introduisons l'application :

$$\begin{aligned}
\varphi\colon \quad \mathbb{Z} \,&\longrightarrow\, G \\
k \,&\longmapsto\, g^k,
\end{aligned}$$

avec $\varphi(0) = e \neq g = \varphi(1)$. D'après l'hypothèse forte, $\varphi(2) = e$.

Le noyau $\mathsf{Ker}\,\varphi$ de φ est un sous-groupe de $\mathbb{Z}$, comme on l'a vu en cours, de la forme $\mu\,\mathbb{Z}$ avec $\mu \in \mathbb{N}_{\geqslant 1}$. Clairement, $\mathsf{Ker}\,\varphi = 2\,\mathbb{Z}$.

Enfin, grâce au théorème de factorisation :

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\varphi"] \arrow[d] & G \\ \mathbb{Z}/2\mathbb{Z} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

nous obtenons bien un isomorphisme $\overline{\varphi}\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow G$.

(c) Soit $g_1 \neq e$. Soit $\langle g_1 \rangle$ le sous-groupe engendré, isomorphe à $\mathbb{Z}/2\mathbb{Z}$, donc. Si $\langle g_1 \rangle = G$, on s'arrête.

Sinon, soit un élément $g_2 \notin \langle g_1 \rangle$. Soit $\langle g_1, g_2 \rangle$ le groupe engendré. Si $\langle g_1, g_2 \rangle = G$, on s'arrête.

Et ainsi de suite.

Par récurrence, et parce que $\mathsf{Card}\, G < \infty$, il existe un entier $r \geqslant 1$ et un élément $g_r \notin \langle g_1, \ldots, g_{r-1} \rangle$ tel que $G = \langle g_1, \ldots, g_{r-1}, g_r \rangle$.

Comme G est commutatif, on a vu en cours que :

$$G = \big\{ g_1^{i_1} \cdots g_r^{i_r} \colon\ i_1, \ldots, i_r \in \mathbb{Z} \big\}.$$

Mais comme $g_i^{-1} = g_i$, et comme $g_i^2 = e$, on a en fait :

$$G = \big\{ g_1^{i_1} \cdots g_r^{i_r} \colon\ i_1, \ldots, i_r \in \{0, 1\} \big\}.$$

Introduisons l'application :

$$\begin{aligned} \psi\colon \quad \mathbb{Z} \times \cdots \times \mathbb{Z} &\longrightarrow G \\ (i_1, \ldots, i_r) &\longmapsto g_1^{i_1} \cdots g_r^{i_r}. \end{aligned}$$

Il est clair que :

$$\mathsf{Ker}\, \psi = 2\mathbb{Z} \times \cdots \times 2\mathbb{Z} = \big(\mathbb{Z}/2\mathbb{Z}\big)^r.$$

Enfin, grâce au théorème de factorisation :

$$\begin{tikzcd} \mathbb{Z}^r \arrow[r, "\psi"] \arrow[d] & G \\ (\mathbb{Z}/2\mathbb{Z})^r \arrow[ur, "\overline{\psi}"'] & \end{tikzcd}$$

nous obtenons bien un isomorphisme $\overline{\psi}\colon (\mathbb{Z}/2\mathbb{Z})^r \longrightarrow G$.

15. Examen 8

Exercice 1. Dans $\mathbb{R}[X]$, soient les deux polynômes :

$$A := X^5 - 2\,X^4 + X^3 + X^2 - 2\,X + 1 \qquad \text{et} \qquad B := X^4 - 2\,X^3 + 2\,X^2 - 2\,X + 1.$$

(a) Déterminer $D := \mathsf{pgcd}\,(A, B)$. Indication: Ce polynôme *unitaire* $D \in \mathbb{R}[X]_1$ est de degré $2 = \mathsf{deg}\,D$.

(b) Déterminer les deux polynômes A_1 et B_1 de $\mathbb{R}[X]$ tels que :

$$A \;=\; D\,A_1 \qquad\qquad \text{et} \qquad\qquad B \;=\; D\,B_1.$$

(c) Sous forme d'un produit, déterminer explicitement le polynôme :

$$M \;:=\; \mathsf{ppcm}\,(A, B).$$

(d) Factoriser M dans $\mathbb{R}[X]$ en facteurs *irréductibles*.

Exercice 2. Soit un entier quelconque $n \geqslant 2$. Soit le groupe $\mathfrak{S}_n$ des permutations (bijections) de $\{1, 2, \ldots, n\}$, muni de la loi interne de composition (des bijections).

Un premier objectif est de démontrer, par récurrence sur l'entier n, que les $n-1$ transpositions :

$$\big(1\;\;2\big),\;\; \big(2\;\;3\big),\;\; \ldots,\;\; \big(n-1\;\;n\big),$$

engendrent $\mathfrak{S}_n$.

(a) Que dire (rapidement) pour $n = 2$?

(b) Avec $n \geqslant 2$ fixé, on suppose par récurrence que $(1\;\;2)$, $(2\;\;3)$, …, $\big(n-1\;\;n\big)$ engendrent $\mathfrak{S}_n$. Justifier que, pour tous $1 \leqslant i < j \leqslant n$, la transposition :

$$\big(i\;\;j\big) \;\in\; \Big\langle \big(1\;\;2\big),\, \big(2\;\;3\big),\, \ldots,\, \big(n-1\;\;n\big) \Big\rangle,$$

où la notation $\langle \bullet \rangle$ signifie *groupe engendré par une partie*.

(c) Avec $1 \leqslant k \leqslant n-1$ quelconque, montrer que l'on a dans $\mathfrak{S}_{n+1}$:

$$\big(n\;\;n+1\big) \circ \big(k\;\;n\big) \circ \big(n\;\;n+1\big) \;=\; \big(k\;\;n+1\big).$$

(d) Établir que $(1\;\;2)$, $(2\;\;3)$, …, $(n-1\;\;n)$, $(n\;\;n+1)$ engendrent $\mathfrak{S}_{n+1}$, puis, conclure le premier objectif. Indication: Le cours a démontré que l'ensemble de *toutes* les transpositions possibles engendre $\mathfrak{S}_{n+1}$.

(e) Un deuxième objectif est de démontrer, par récurrence sur $n \geqslant 3$, que les deux (seulement !) permutations :

$$t \;:=\; \big(1\;\;2\big) \qquad\qquad \text{et} \qquad\qquad c \;:=\; \big(1\;\;2\;\;\cdots\;\;n\big),$$

engendrent $\mathfrak{S}_n$.

Montrer que, pour $n \geqslant 3$:

$$c\,t\,c^{-1} \;=\; \big(2\;\;3\big).$$

(f) Pour tout entier $1 \leqslant i \leqslant n-2$, montrer que :

$$c^i\, t\, c^{-i} \;=\; \big(i+1 \;\; i+2\big).$$

(g) Montrer que $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$ engendrent $\mathfrak{S}_n$.

Exercice 3. L'objectif est de décomposer en éléments simples, sur $\mathbb{R}[x]$, la fraction rationnelle :

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

(a) Justifier l'égalité :

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

avec des inconnues réelles a, b, c, b', c', b'', c''.

(b) En comparant $B(-x)$ avec $B(x)$, montrer que $c = c' = c'' = 0$.

(c) Montrer que $a = 1$. Indication: On pourra commencer par multiplier l'égalité par un facteur approprié.

(d) Montrer que $b = -4$. Indication: On pourra commencer par multiplier l'égalité par un facteur approprié.

(e) On introduit la *fonction* rationnelle définie sur $\mathbb{R}\backslash\{0\}$ par :

$$f(x) \;:=\; \frac{(x^2-1)^2}{x\,(x^2+1)^3}.$$

Déterminer b'' en calculant $\lim\limits_{x\to+\infty} x\,f(x)$.

(f) Déterminer b', puis, conclure.

(g) Trouver la décomposition en éléments simples de :

$$A(x) \;:=\; \frac{x^4-2\,x^2-x+1}{x\,(x^2+1)^3}.$$

Exercice 4. Avec un entier $n \geqslant 2$, soit $\mathfrak{S}_n$ le groupe des permutations de $\{1,2,\ldots,n\}$. Soit le cycle de longueur n :

$$\sigma \;:=\; \big(1\ \ 2\ \ \cdots\ \ n\big).$$

(a) Avec $n = 4$ et $\sigma = (1\ 2\ 3\ 4)$, décomposer en cycles à supports disjoints les quatre puissances σ, σ^2, σ^3, σ^4. Pour quelles valeurs de $1 \leqslant k \leqslant 4$ la permutation σ^k est-elle constituée d'un et d'un seul cycle ?

(b) Avec $n = 6$ et $\sigma = (1\ 2\ 3\ 4\ 5\ 6)$, décomposer en cycles à supports disjoints les six puissances σ, σ^2, σ^3, σ^4, σ^5, σ^6. Pour quelles valeurs de $1 \leqslant k \leqslant 6$ la permutation σ^k est-elle constituée d'un et d'un seul cycle ?

(c) On revient au cas général. On fixe un entier $1 \leqslant k \leqslant n$. L'objectif est de déterminer si la décomposition de :

$$\tau \;:=\; \sigma^k \;=\; \big(1\ 2\ \cdots\ n\big) \circ \cdots \circ \big(1\ 2\ \cdots\ n\big) \qquad (k\,\text{fois}),$$

en cycles à supports disjoints est, ou n'est pas, constituée d'un et d'un seul cycle.

Pour un entier $a \in \mathbb{Z}$, on notera $a\ [n]$ l'unique représentant de $a \bmod n$ dans l'ensemble $\{1,2,\ldots,n\}$ — et non pas dans l'ensemble $\big\{\overline{0},\overline{1},\ldots,\overline{n-1}\big\}$.

Commencer par vérifier, pour tout $i \in \{1, 2, \ldots, n\}$ fixé, que :

$$\sigma(i) \;=\; i + 1 \;\; [n],$$

puis, pour tout exposant $m \geqslant 1$, que :

$$\sigma^m(i) \;=\; i + m \;\; [n],$$

et enfin, pour tout exposant $\ell \geqslant 1$, que :

$$\tau^\ell(i) \;=\; i + k\,\ell \;\; [n].$$

(d) On suppose maintenant que $k \wedge n = 1$ sont premiers entre eux. Après avoir justifié que $\tau^n = \mathsf{Id}$, montrer que les n éléments de l'ensemble :

$$\big\{\tau^\ell(i)\big\}_{0 \leqslant \ell \leqslant n-1} \qquad (i \in \{1,2,\ldots,n\}),$$

sont distincts deux à deux, puis, en déduire que la décomposition de σ^k en cycles à supports disjoints est constituée d'un et d'un seul cycle.

(e) On suppose à l'inverse que :

$$1 \;<\; d \;:=\; \mathsf{pgcd}\,(k, n),$$

et on note $k = d\,k'$ et $n = d\,n'$, avec $1 = k' \wedge n'$. Vérifier que $\tau^{n'} = \mathsf{Id}$, puis, montrer que les τ-orbites sont toutes de cardinal $\leqslant n'$.

(f) Toujours sous l'hypothèse $1 < k \wedge n$, montrer que la décomposition en cycles à supports disjoints de τ contient *au moins* deux cycles distincts. Indication: On pourra exhiber deux éléments de $\{1, 2, \ldots, n\}$ dont les τ-orbites sont *distinctes*.

Exercice 5. L'objectif est d'exhiber un exemple d'anneau dans lequel la factorisation en facteurs irréductibles n'est pas nécessairement unique. Dans $\mathbb{C}$, on note $\alpha := i\sqrt{5}$. On a alors $\alpha^2 = -5$.

(a) On introduit :

$$\mathbb{Z}\big[i\sqrt{5}\big] \;:=\; \big\{z \in \mathbb{C}\colon\; \exists\, a, b \in \mathbb{Z},\; z = a + b\,i\sqrt{5}\big\}.$$

Montrer que $\mathbb{Z}\big[i\sqrt{5}\big]$ est un sous-anneau de $\mathbb{C}$. Indication: Vérifier que $\mathbb{Z}\big[i\sqrt{5}\big]$ contient $0, 1 \in \mathbb{C}$, et est stable par soustraction et par multiplication.

(b) Pour tout $z = a + b\alpha \in \mathbb{Z}\big[i\sqrt{5}\big]$ (où $a, b \in \mathbb{Z}$), on définit sa *norme :*

$$N(z) \;:=\; a^2 + 5\,b^2.$$

Vérifier que $N(z) = |z|^2$, puis que $N(zw) = N(z)N(w)$, pour tous $z, w \in \mathbb{Z}\big[i\sqrt{5}\big]$.

Dans les questions suivantes, on profitera de cette « multiplicativité » de la norme.

(c) Montrer que les *seuls* éléments $z \in \mathbb{Z}\big[i\sqrt{5}\big]$ de norme $N(z) = 1$ sont $+1$ et -1.

(d) On dit qu'un élément $z \in \mathbb{Z}\big[i\sqrt{5}\big]$ est *inversible* s'il existe $w \in \mathbb{Z}\big[i\sqrt{5}\big]$ tel que $1 = z\,w\,(= w\,z)$. Montrer que les seuls éléments inversibles de $\mathbb{Z}\big[i\sqrt{5}\big]$ sont $+1$ et -1.

(e) Montrer qu'il n'existe pas d'élément de norme 2 ou 3 dans $\mathbb{Z}\big[i\sqrt{5}\big]$.

(f) Un élément $z \in \mathbb{Z}\big[i\sqrt{5}\big]$ est dit *irréductible* s'il est non nul, non inversible et ne peut pas s'écrire comme produit $z = x\,y$ de deux éléments $x, y \in \mathbb{Z}\big[i\sqrt{5}\big]$ non inversibles. Montrer que les quatre éléments suivants de $\mathbb{Z}\big[i\sqrt{5}\big]$ sont irréductibles :

$$2, \quad 3, \quad 1 + i\sqrt{5}, \quad 1 - i\sqrt{5}.$$

Indication: On pourra commencer par observer que les quatre normes respectives valent 4, 9, 6, 6.

(g) Conclure l'objectif visé, à savoir, montrer que dans $\mathbb{Z}\left[i\sqrt{5}\right]$, la factorisation en facteurs irréductibles n'est *pas unique à un facteur* ± 1 *près*.

16. Corrigé de l'examen 8

Exercice 1. **(a)** Euclidivisons :

$$X^5-2\,X^4+X^3+X^2-2\,X+1 \;=\; \big(X\big)\,\big(X^4-2\,X^3+2\,X^2-2\,X+1\big)-X^3+3\,X^2-3\,X+1,$$

re-euclidivisons :

$$X^4-2\,X^3+2\,X^2-2\,X+1 \;=\; \big(-\,X-1\big)\,\big(-X^3+3\,X^2-3\,X+1\big)+2\,X^2-4\,X+2,$$

et re-re-euclidivisons :

$$-X^3+3\,X^2-3\,X+1 \;=\; \big(-\,\tfrac{1}{2}\,X+\tfrac{1}{2}\big)\,\big(2\,X^2-4\,X+2\big)+\mathbf{0},$$

ce dernier reste étant nul.

Ainsi, comme le pgcd est le dernier reste non nul *renormalisé afin d'être unitaire*, nous trouvons :

$$D \;=\; \mathsf{pgcd}\,(A,B) \;=\; X^2-2\,X+1 \;=\; \big(X-1\big)^2.$$

(b) Il suffit de diviser A par D et de diviser B par D ; on trouve :

$$A \;=\; \big(X-1\big)^2\,\big(X^3+1\big) \qquad \text{et} \qquad B \;=\; \big(X-1\big)^2\,\big(X^2+1\big),$$

d'où :

$$A_1 \;=\; X^3+1 \qquad \text{et} \qquad B_1 \;=\; X^2+1.$$

(c) D'après le cours :

$$\begin{aligned} M \;=\; \frac{A\,B}{D} \;&=\; A_1\,D\,B_1 \\ &=\; \big(X^3+1\big)\,\big(X-1\big)^2\,\big(X^2+1\big). \end{aligned}$$

(d) On sait que X^2+1, de degré 2, est irréductible parce qu'il n'a aucune racine réelle. On sait aussi que -1 est racine de X^3+1, d'où la factorisation :

$$X^3+1 \;=\; \big(X+1\big)\,\big(X^2-X+1\big).$$

Enfin, X^2-X+1, de degré 2 et de discriminant $(-1)^2-4<0$ strictement négatif, n'a pas de racine réelle, donc est irréductible.

En, conclusion, la factorisation de M en facteurs irréductibles dans $\mathbb{R}[X]$ est :

$$M \;=\; \big(X+1\big)\,\big(X^2-X+1\big)\,\big(X-1\big)^2\,\big(X^2+1\big).$$

Exercice 2. **(a)** Que puisque $\mathfrak{S}_n = \big\{\mathsf{Id}, (1\ 2)\big\}$, l'objectif est atteint hyper-rapidement !

(b) C'est clair, et pas seulement ces tranpositions $(i\ j)$, mais aussi *toutes* les permutations appartenant à $\mathfrak{S}_n$ sont dans ce groupe engendré par les $n-1$ transpositions $(1\ 2)$, $(2\ 3)$, …, $\big(n-1\ \ n\big)$.

(c) En effet, en écrivant seulement les images successives des trois éléments du triplet $\big\{k, n, n+1\big\}$ puisque les $n+1-3$ autres éléments restent imperturbablement fixés :

$$\begin{array}{ccccc}
 & k & n & n+1 \\
(n\ n+1) & \downarrow & \downarrow & \downarrow \\
 & k & n+1 & n \\
(k\ n) & \downarrow & \downarrow & \downarrow \\
 & n & n+1 & k \\
(n\ n+1) & \downarrow & \downarrow & \downarrow \\
 & n+1 & n & k
\end{array}$$

nous voyons que n est fixé, et nous constatons bien que cette composition est égale à la transposition $\big(k\ \ n+1\big)$.

(d) D'après la Question **(b)**, l'hypothèse de récurrence donne toutes les transpositions $(i\ j)$ avec $1 \leqslant i < j \leqslant n$ quelconques.

Comme par hypothèse, on dispose de la transposition $(n\ \ n+1)$, la Question **(c)** nous a fait obtenir toutes les transpositions $(k\ \ n+1)$ avec $1 \leqslant k \leqslant n$ quelconque.

En définitive, nous disposons de toutes les transpositions de la forme $(k\ \ell)$ avec $1 \leqslant k < \ell \leqslant n+1$ quelconques.

Et cet ensemble engendre $\mathfrak{S}_{n+1}$, d'après un théorème du cours.

(e) Il s'agit de se demander si :

$$\begin{aligned}
& c\,t\,c^{-1} \overset{?}{=} \big(2\ \ 3\big) \\
\Longleftrightarrow \qquad & c \circ t \overset{?}{=} \big(2\ \ 3\big) \circ c.
\end{aligned}$$

Effectivement

$$\begin{array}{ccccccccc}
 & 1 & 2 & 3 & 4 & \cdots & n-1 & n \\
t & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 2 & 1 & 3 & 4 & \cdots & n-1 & n \\
c & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 3 & 2 & 4 & 5 & \cdots & n & 1
\end{array}
\quad = \quad
\begin{array}{ccccccccc}
 & 1 & 2 & 3 & 4 & \cdots & n-1 & n \\
c & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 2 & 3 & 4 & 5 & \cdots & n & 1 \\
(2\ 3) & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 3 & 2 & 4 & 5 & \cdots & n & 1
\end{array}$$

(f) Nous venons de constater que cela est vrai lorsque $i = 1$. Par récurrence, supposons donc que pour un indice $1 \leqslant i \leqslant n-3$, on ait :

$$c^i\,t\,c^{-i} = \big(i+1\ \ i+2\big).$$

Alors :

$$\begin{aligned}
c^{i+1}\,t\,c^{-i-1} &= c\,c^i\,t\,c^{-i}\,c^{-1} \\
&= c\,\big(i+1\ \ i+2\big)\,c^{-1},
\end{aligned}$$

et il s'agit de se demander si :

$$\begin{aligned}
& c\,\big(i+1\ \ i+2\big)\,c^{-1} \overset{?}{=} \big(i+2\ \ i+3\big) \\
\Longleftrightarrow \qquad & c \circ \big(i+1\ \ i+2\big) \overset{?}{=} \big(i+2\ \ i+3\big) \circ c.
\end{aligned}$$

Effectivement, la composition de gauche :

$$\begin{array}{cccccccccccc}
 & 1 & 2 & \cdots & i & i+1 & i+2 & i+3 & \cdots & n-1 & n \\
(i+1\ \ i+2) & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\
 & 1 & 2 & \cdots & i & i+2 & i+1 & i+3 & \cdots & n-1 & n \\
c & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\
 & 2 & 3 & \cdots & i+1 & i+3 & i+2 & i+4 & \cdots & n & 1
\end{array}$$

est bien égale à la composition de droite :

$$\begin{array}{cccccccccccc}
 & 1 & 2 & \cdots & i & i+1 & i+2 & i+3 & \cdots & n-1 & n \\
c & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\
 & 2 & 3 & \cdots & i+1 & i+2 & i+3 & i+4 & \cdots & n & 1 \\
(i+2\ \ i+3) & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\
 & 2 & 3 & \cdots & i+1 & i+3 & i+2 & i+4 & \cdots & n & 1
\end{array}$$

(g) Dans le sous-groupe engendré par $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$, nous venons de constater qu'il y avait toutes les transpositions :

$$\big(1\ \ 2\big), \quad \big(2\ \ 3\big) \,=\, c\,t\,c^{-1}, \quad \big(3\ \ 4\big) \,=\, c^2\,t\,c^{-2}, \quad \ldots, \quad \big(n-1\ \ n\big) \,=\, c^{n-2}\,t\,c^{-n+2},$$

qui engendrent $\mathfrak{S}_n$, grâce au premier objectif, atteint à la fin de la Question **(d)**.

Exercice 3. (a) Le dénominateur étant décomposé en facteurs irréductibles, et ayant un degré strictement supérieur à celui du numérateur, un théorème du cours s'applique directement pour nous dire que la décomposition attendue de $B(x)$ en éléments simples est bien de cette forme-là.

(b) Clairement, d'après l'expression originale, on a l'imparité :

$$B(-x) \,=\, -\,B(x),$$

d'où au niveau des décompositions en éléments simples :

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

puis après simplifications :

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

L'*unicité* de la décomposition en éléments simples, établie en cours, entraîne alors les égalités :

$$c \,=\, -\,c, \qquad\qquad c' \,=\, -\,c', \qquad\qquad c'' \,=\, -\,c'',$$

c'est-à-dire :

$$0 \,=\, c \,=\, c' \,=\, c''.$$

(c) Multiplions par x l'égalité :

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

ce qui donne :

$$\frac{(x^2-1)^2}{(x^2+1)^3} \,=\, a+x\,\big(\cdots\big),$$

puis, attribuons à x la note $x := 0$ (sur 20 ?) pour obtenir :

$$\frac{(0^2-1)^2}{(0^2+1)^3} \;=\; a+0,$$

c'est-à-dire :

$$1 \;=\; a.$$

(d) De manière similaire, multiplions la même égalité par $(x^2+1)^3$, ce qui donne :

$$\frac{(x^2-1)^2}{x} \;=\; b\,x + (x^2+1)^3\,\big(\cdots\big),$$

puis, attribuons à x la belle note imaginaire $x := i$ (sur $\sqrt{-20}$), pour obtenir :

$$\frac{(i^2-1)^2}{i} \;=\; b\,i+0,$$

c'est-à-dire :

$$-4 \;=\; b.$$

(e) Clairement :

$$\begin{aligned}\lim_{x\to+\infty} x\,f(x) \;&=\; \lim_{x\to+\infty} \frac{\underline{x_\circ}\,(x^2-1)^2}{\underline{x_\circ}\,(x^2+1)^3}\\ &=\; \lim_{x\to+\infty} \frac{x^4+\cdots}{x^6+\cdots}\\ &=\; 0.\end{aligned}$$

Ensuite, pour tout $x \neq 0$, on a grâce à ce qui précède :

$$f(x) \;=\; \frac{1}{x} - \frac{4\,x}{(x^2+1)^3} + \frac{b'\,x}{(x^2+1)^2} + \frac{b''\,x}{x^2+1},$$

d'où :

$$\begin{aligned}0 \;&=\; \lim_{x\to+\infty} x\left(\frac{1}{x} - \frac{4\,x}{(x^2+1)^3} + \frac{b'\,x}{(x^2+1)^2} + \frac{b''\,x}{x^2+1},\right)\\ &=\; 1-0+0+b'',\end{aligned}$$

c'est-à-dire :

$$-1 \;=\; b''.$$

(f) Il suffit par exemple de prendre la valeur en $x=1$ de l'égalité :

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

ce qui donne :

$$0 \;=\; 1 - \frac{4}{8} + \frac{b'}{4} - \frac{1}{2},$$

c'est-à-dire :

$$0 \;=\; b'.$$

En conclusion, nous avons complètement déterminé la décomposition en éléments simples de :

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

(g) Astucieusement :

$$\begin{aligned} A(x) &= \frac{(x^2-1)^2 - x}{x\,(x^2+1)^3} \\ &= B(x) - \frac{\underline{x}_\circ}{\underline{x}_\circ\,(x^2+1)^3} \\ &= \frac{1}{x} - \frac{4\,x}{(x^2+1)^3} - \frac{x}{x^2+1} - \frac{1}{(x^2+1)^3} \\ &= \frac{1}{x} - \frac{4\,x+1}{(x^2+1)^3} - \frac{x}{x^2+1}. \end{aligned}$$

Exercice 4. **(a)** On trouve :

$$\begin{aligned} \sigma^1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \big(1\ 2\ 3\ 4\big), \\ \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \big(1\ 3\big)\big(2\ 4\big), \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \big(1\ 4\ 3\ 2\big) = \sigma^{-1}, \\ \sigma^4 &= \mathsf{Id}, \end{aligned}$$

puisque σ est d'ordre égal à sa longueur, 4.

Visiblement, ce sont σ^1 et σ^3 qui sont constituées d'un unique cycle.

(b) On trouve :

$$\begin{aligned} \sigma^1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = \big(1\ 2\ 3\ 4\ 5\ 6\big), \\ \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = \big(1\ 3\ 5\big)\big(2\ 4\ 6\big), \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = \big(1\ 4\big)\big(2\ 5\big)\big(3\ 6\big), \\ \sigma^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = \big(1\ 5\ 3\big)\big(2\ 6\ 4\big), \\ \sigma^5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \big(1\ 6\ 5\ 4\ 3\ 2\big) = \sigma^{-1}, \\ \sigma^6 &= \mathsf{Id}, \end{aligned}$$

puisque σ est d'ordre égal à sa longueur, 6.

Visiblement, ce sont σ^1 et σ^5 qui sont constituées d'un unique cycle.

(c) La première identité $\sigma(i) = i+1\ [n]$ est précisément la définition de la permutation circulaire $\sigma = (1\ 2\ \cdots\ n)$.

Ensuite :

$$\sigma^2(i) = \sigma\big(\sigma(i)\big) = \sigma\big(i+1\ [n]\big) = i+2\ [n],$$

et une récurrence immédiate donne alors bien $\sigma^m(i) = i+m\ [n]$.

Enfin :

$$\tau^\ell(i) = \big(\sigma^k\big)^\ell(i) = \sigma^{k\ell}(i) = i + k\,\ell\ \ [n].$$

(d) Comme σ est d'ordre égal à sa longueur n, il est clair que :

$$\tau^n \;=\; \big(\sigma^n\big)^k \;=\; \mathsf{Id}^k \;=\; \mathsf{Id}.$$

L'argument concernant le cardinal de l'ensemble $\big\{\tau^\ell(i)\big\}_{0\leqslant\ell\leqslant n-1}$ a été plusieurs fois vu en cours et en annales d'examens, sous diverses formes parfois légèrement modifiées.

Pour deux entiers quelconques $0 \leqslant \ell_1, \ell_2 \leqslant n-1$:

$$\begin{aligned}
& & \tau^{\ell_1}(i) \;&=\; \tau^{\ell_2}(i) \\
&\Longleftrightarrow & \sigma^{k\ell_1}(i) \;&=\; \sigma^{k\ell_2}(i) \\
&\Longleftrightarrow & k\ell_1 + i \;\; [n] \;&=\; k\ell_2 + i \;\; [n] \\
&\Longrightarrow & k\,(\ell_1 - \ell_2) \;&\equiv\; 0 \;\; \mathsf{mod}\, n,
\end{aligned}$$

c'est-à-dire pour un certain entier $\lambda \in \mathbb{Z}$:

$$k\,(\ell_1 - \ell_2) \;=\; \lambda\, n,$$

et comme $k \wedge n = 1$, le théorème de Gauss force n à diviser $\ell_1 - \ell_2$, ce qui n'est possible que si $\ell_1 - \ell_2 = 0$, parce que l'on sait, on a vu en cours, ou on voit aisément, que :

$$0 \;\leqslant\; \big|\ell_1 - \ell_2\big| \;\leqslant\; n-1.$$

Donc les valeurs $\tau^\ell(i)$ sont bien distinctes deux à deux, pour $\ell = 0, 1, \ldots, n-1$.

Ainsi, toujours avec $k \wedge n = 1$, l'orbite d'un élément quelconque $i \in \{1, 2, \ldots, n\}$ est constituée du nombre maximal possible, n, d'éléments, ce qui montre que $\tau = \sigma^k$ est un (unique) cycle de longueur n. En définitive, la décomposition en cycles de σ^k ne peut comporter que ce cycle-là, puisque la somme des longueurs de cycles de n'importe quelle décomposition dans $\mathfrak{S}_n$ est toujours $\leqslant n$.

(e) Clairement :

$$\tau^{n'} \;=\; \sigma^{kn'} \;=\; \sigma^{k'dn'} \;=\; \big(\sigma^{dn'}\big)^{k'} \;=\; \big(\sigma^n\big)^{k'} \;=\; \big(\mathsf{Id}\big)^{k'} \;=\; \mathsf{Id}.$$

Ainsi, la τ-orbite d'un élément quelconque $i \in \{1, 2, \ldots, n\}$, qui se réduit à :

$$\big\{\tau^\ell(i)\big\}_{\ell\in\mathbb{Z}} \;=\; \big\{\tau^\ell(i)\big\}_{\ell\in\mathbb{N}} \;=\; \big\{\tau^\ell(i)\big\}_{0\leqslant\ell\leqslant n'-1},$$

est bien de cardinal $\leqslant n'$.

(f) Considérons les deux τ-orbites des éléments $i = 1$ et $i = 2$, qui constituent chacune un cycle dans la décomposition de τ :

$$\big\{\tau^\ell(1)\big\}_{0\leqslant\ell\leqslant n'-1} \qquad \text{et} \qquad \big\{\tau^\ell(2)\big\}_{0\leqslant\ell\leqslant n'-1}.$$

Mais au fait, ces deux τ-orbites sont-elles distinctes ?

Le cours a démontré que deux classes d'équivalences, en particulier deux orbites de n'importe quel type, sont distinctes si et seulement si elles n'ont aucun élément en commun.

Supposons donc par l'absurde qu'il existe deux entiers $0 \leqslant \ell_1 \leqslant n'-1$ et $0 \leqslant \ell_2 \leqslant n'-1$ pour lesquels on aurait la coïncidence (malencontreuse) :

$$\tau^{\ell_1}(1) \;=\; \tau^{\ell_2}(2),$$

c'est-à-dire grâce à ce qui précède :

$$\begin{aligned}
& & k\ell_1 + 1 \;\; [n] \;&=\; k\ell_2 + 2 \;\; [n] \\
&\Longrightarrow & k\,(\ell_1 - \ell_2) \;&=\; 2 - 1 \;\; \mathsf{mod}\, n,
\end{aligned}$$

c'est-à-dire pour un certain entier $\lambda \in \mathbb{Z}$:

$$k\,(\ell_1 - \ell_2) \;=\; 1 + \lambda\, n.$$

Mais comme $k = d\,k'$ ainsi que $n = d\,n'$, l'égalité :

$$d\,k'\,(\ell_1 - \ell_2) \;=\; 1 + \lambda\, d\, n',$$

impliquerait en lisant (en réduisant) cette égalité modulo d :

$$0 \;\equiv\; 1 \;\; \mathsf{mod}\, d,$$

une contradiction manifeste, qui est conclusive.

Exercice 5. (a) On abrège $\alpha = i\sqrt{5}$. On a $0 = 0 + 0\,\alpha$, donc $0 \in \mathbb{Z}\big[i\sqrt{5}\big]$.

Soient $z, w \in \mathbb{Z}\big[i\sqrt{5}\big]$ *quelconques*. Alors il existe $a, b, c, d \in \mathbb{Z}$ tels que $z = a + b\,\alpha$ et $w = c + d\,\alpha$.

On a $z - w = (a - c) + (b - d)\alpha$, d'où $z - w \in \mathbb{Z}\big[i\sqrt{5}\big]$ puisque $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$. On conclut que $\mathbb{Z}\big[i\sqrt{5}\big]$ est un sous-groupe de $(\mathbb{C}, +)$.

Ensuite :

$$\begin{aligned} zw \;&=\; ac + (ad + bc)\alpha + bd\,\alpha^2 \\ &=\; (ac - 5bd) + (ad + bc)\alpha, \end{aligned}$$

d'où $zw \in \mathbb{Z}\big[i\sqrt{5}\big]$ puisque $ac - 5bd \in \mathbb{Z}$ et $ad + bc \in \mathbb{Z}$.

Finalement, $1 = 1 + 0\alpha$, donc $1 \in \mathbb{Z}\big[i\sqrt{5}\big]$. On conclut que $\mathbb{Z}\big[i\sqrt{5}\big]$ est bien un sous-anneau de $\mathbb{C}$.

(b) Notons que $\overline{\alpha} = -\alpha$ puisque α est purement imaginaire. On a alors $\overline{z} = a - b\alpha$ et donc :

$$N(z) \;=\; a^2 + 5\,b^2 \;=\; a^2 - b^2\alpha^2 \;=\; (a + b\alpha)(a - b\alpha) \;=\; z\bar{z} \;=\; |z|^2.$$

Il s'ensuit que $N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$.

(c) Soit $z = a + b\alpha \in \mathbb{Z}\big[i\sqrt{5}\big]$, où $a, b \in \mathbb{Z}$, et supposons $a^2 + 5b^2 = N(z) = 1$. Si $b \neq 0$, alors $|b| \geqslant 1$ et donc $a^2 + 5b^2 \geqslant 5b^2 \geqslant 5 > 1$, ce qui est une contradiction. D'où $b = 0$, puis $a^2 = 1$, et enfin $z = a = \pm 1$.

(d) Notons que la norme de n'importe quel élément de $\mathbb{Z}\big[i\sqrt{5}\big]$ est un entier. Soit $z \in \mathbb{Z}\big[i\sqrt{5}\big]$ inversible, alors il existe $w \in \mathbb{Z}\big[i\sqrt{5}\big]$ tel que $zw = 1$. D'où $N(z)N(w) = N(1) = 1^2 = 1$. On en déduit que $N(z) = N(w) = 1$, vu que $N(z), N(w) \in \mathbb{N}$. Mais alors $z \in \{1, -1\}$ par le calcul ci-dessus.

Inversement, les éléments 1 et -1 sont manifestement inversibles dans $\mathbb{Z}\big[i\sqrt{5}\big]$: chacun d'eux est égal à son propre inverse !

(e) Soit $z = a + b\,i\sqrt{5}$, où $a, b \in \mathbb{Z}$, et supposons $N(z) \in \{2, 3\}$, c'est-à-dire $a^2 + 5b^2 \in \{2, 3\}$. Avec le même argument que celui de la question précédente, on ne peut pas avoir $b^2 \geqslant 1$, donc cela force $b = 0$. Ainsi, $a^2 \in \{2, 3\}$, mais ceci est impossible avec $a \in \mathbb{Z}$!

Donc, il n'existe pas d'élément de norme 2 ou 3 dans $\mathbb{Z}\big[i\sqrt{5}\big]$. Snif !

(f) Oui, les quatre normes respectives, modules au carré de ces nombres complexes, valent bien :

$$2 \cdot 2, \qquad 3 \cdot 3, \qquad 2 \cdot 3, \qquad 2 \cdot 3.$$

Soit z l'un de ces quatre nombres complexes. Si $z = x\,y$ avec $x, y \in \mathbb{Z}\big[i\sqrt{5}\big]$, alors :

$$N(z) \;=\; 6 \;=\; N(x)\,N(y).$$

Supposons par l'absurde que x et y sont non-inversibles. Alors $N(x) > 1$ et $N(y) > 1$, car sinon, la Question **(c)** forcerait $x = \pm 1$ ou $y = \pm 1$, qui seraient trivialement inversibles.

Comme $6 = 2 \cdot 3$ est la décomposition en facteurs premiers de $N(z) = N(x)\,N(y)$, et comme $N(x)$, $N(y)$ sont des entiers > 1, nécessairement :

$$N(x) \in \{2, 3\} \qquad \text{et} \qquad N(y) \in \{2, 3\}.$$

Mais la Question **(e)** a déjà fait voir qu'*aucun* élément de $\mathbb{Z}\big[i\sqrt{5}\big]$ ne peut avoir une telle norme !

Donc z ne peut *pas* s'écrire sous cette forme $z = x\,y$, donc z est bien irréductible.

(g) Tout d'abord, la factorisation $6 = (-2) \cdot (-3)$ est la même que la factorisation triviale $6 = 2 \cdot 3$ à un facteur ± 1 près. Donc elle ne convient pas.

Pour trouver une autre factorisation vraiment exotique de 6 dans $\mathbb{Z}\big[i\sqrt{5}\big]$, il suffit de constater que dans les deux factorisations *distinctes :*

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= \big(1 + i\sqrt{5}\big) \cdot \big(1 - i\,\sqrt{5}\big), \end{aligned}$$

les quatre éléments écrits sont irréductibles, d'après la Question **(f)** qui précède, et qu'ils sont visiblement non égaux l'un à l'autre à un facteur ± 1 près.

17. Examen 9

Exercice 1. **(a)** Pour $n = 1, 2, 3, 4$, déterminer le reste de la division euclidienne de :

$$7\,n + 15 \qquad \text{par} \qquad 3\,n + 2.$$

(b) Pour $n \geqslant 5$, déterminer le reste de la division euclidienne de :

$$7\,n + 15 \qquad \text{par} \qquad 3\,n + 2.$$

(c) Montrer que, pour tout $n \in \mathbb{N}$, l'entier $2^{5n+1} + 3^{n+3}$ est multiple de 29. Indication: On pourra raisonner par récurrence sur n, en supposant que $2^{5n+1} + 3^{n+3} = 29\,k$ avec $k \in \mathbb{N}$.

Exercice 2. **(a)** En appliquant l'algorithme d'Euclide, calculer :

$$\mathsf{pgcd}\,\big(87,\,24\big) \;=\; \textbf{?}.$$

(b) Montrer que l'équation en nombres entiers d'inconnues $x, y \in \mathbb{Z}$:

$$24\,x + 87\,y \;=\; c,$$

n'a aucune solution lorsque c n'est pas multiple de 3, et surtout, en trouver au moins une solution explicite lorsque $c = 3\,c'$ est multiple de 3, avec $c' \in \mathbb{Z}$.

(c) Dans cette circonstance, montrer que l'ensemble des solutions est :

$$\mathsf{Sol} \;:=\; \big\{\big(11\,c' + 29\,k,\;\; -3\,c' - 8\,k\big):\;\; k \in \mathbb{Z} \text{ quelconque}\big\}.$$

Exercice 3. Soit G un groupe, pas forcément commutatif, d'élément neutre $e \in G$ dont la loi $\cdot$ est notée multiplicativement (sans symbole), l'inverse d'un élément arbitraire $z \in G$ étant noté z^{-1}.

On fixe un élément $a \in G$, d'inverse a^{-1}. On introduit une loi de composition interne $*$ sur G :

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & x * y, \end{array}$$

définie par :

$$x * y \;:=\; x\,a\,y.$$

(a) Montrer que $(G, *)$ est un groupe, d'élément neutre $e' := a^{-1}$. Indication: Après avoir vérifié l'associativité de la loi $*$, on pourra vérifier que l'inverse x' pour la loi $*$ d'un élément quelconque $x \in G$ est $a^{-1}x^{-1}a^{-1} =: x'$. Attention ! Comme G n'est pas supposé commutatif, il faut vérifier « des deux côtés » !

(b) Soit $H \subset G$ un sous-groupe de G pour la loi initiale. Rappeler la propriété caractéristique exprimant, au moyen de deux éléments quelconques $x, y \in H$, que H est un sous-groupe de G.

(c) Vérifier que l'inverse, pour la loi $*$, de $a^{-1}\,y$, est :

$$\big(a^{-1}\,y\big)' \;=\; a^{-1}\,y^{-1}.$$

(d) On pose :

$$K := a^{-1} H = \big\{a^{-1} x \colon \ x \in H\big\}.$$

Montrer que K est un sous-groupe de G pour la loi $*$.

(e) Montrer que l'application :

$$\begin{array}{rccc} f\colon & (G,\cdot) & \longrightarrow & (G,*) \\ & x & \longmapsto & x\,a^{-1}, \end{array}$$

est un *isomorphisme* de groupes.

Exercice 4. **(a)** Soient $q, r \in \mathbb{Z}$. On s'intéresse à l'équation :

$$q^4 \equiv 2 + r^2 \mod 3.$$

Montrer que $q^4 \equiv 0 \mod 3$ nécessairement. Indication: Calculer toutes les puissances 4ièmes et 2ièmes possibles modulo 3, *i.e.* $q^4 \mod 3$ et $r^2 \mod 3$ pour $q, r \in \mathbb{Z}/3\,\mathbb{Z}$ quelconques.

(b) Soient $p, r \in \mathbb{Z}$. On s'intéresse à l'équation :

$$3\,p^4 \equiv 1 + 4\,r^2 \mod 5.$$

Montrer que $3\,p^4 \equiv 0 \mod 5$ nécessairement. Indication: Calculer toutes les puissances 4ièmes et 2ièmes possibles modulo 5.

(c) On s'intéresse maintenant à l'équation diophantienne à 3 variables entières :

$$3\,p^4 - 5\,q^4 - 4\,r^2 = 26, \tag{ED}$$

et on cherche les solutions $p, q, r \in \mathscr{P}$ qui sont tous des nombres *premiers*. Montrer que $q = 3$. Indication: Réduire l'équation diophantienne (ED) modulo 3.

(d) Montrer que $p = 5$. Indication: Réduire l'équation diophantienne (ED) modulo 5.

(e) Déterminer toutes les solutions de l'équation diophantienne (ED)

Exercice 5. On dit qu'un groupe $(G, *)$ est *divisible* si :

$$\forall\, x \in G, \quad \forall\, n \in \mathbb{N}^*, \quad \exists\, y \in G, \quad \text{t.q.} \quad y^n = x.$$

(a) Les groupes suivants sont-ils divisibles ?

(i) $(\mathbb{R}^*, \times)$?

(ii) $(\mathbb{Q}_+^*, \times)$?

(iii) $(\mathbb{R}, +)$?

(iv) $(\mathbb{Z}, +)$?

(b) Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. Montrer que $G_1 \times G_2$ (muni de la loi produit) est divisible si, et seulement si, G_1 et G_2 sont divisibles.

(c) On suppose que G_1 et G_2 sont isomorphes, c'est-à-dire, on suppose qu'il existe un isomorphisme de groupes $\psi\colon G_1 \longrightarrow G_2$. Montrer que G_1 est divisible si, et seulement si, G_2 est divisible.

(d) En déduire que $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ne sont *pas* isomorphes.

Exercice 6. Soit $\mathscr{P} := \{2, 3, 5, 7, \ldots, \}$ l'ensemble des nombres premiers. Soit :

$$3 + 4\,\mathbb{N} \,=\, \big\{3 + 4\,k\colon\ k \in \mathbb{N}\big\}.$$

(a) Tous les nombres entiers de la forme $3 + 4\,k$ sont-ils premiers ?

(b) Déterminer l'ensemble intersection :

$$\mathscr{P} \cap \big\{3 + 4\,k\colon\ 0 \leqslant k \leqslant 10\big\}.$$

(c) Justifier qu'au-delà du premier nombre premier $2 \in \mathscr{P}$, tous les nombres premiers $q \in \mathscr{P}$ sont de la forme :

$$q \,=\, 1 + 4\,\ell \qquad\qquad \text{ou} \qquad\qquad q \,=\, 3 + 4\,k.$$

(d) Montrer que le produit de deux nombres de la forme $1 + 4\,\ell$ avec $\ell \in \mathbb{N}$, est encore de la même forme $1 + 4\,\mathrm{L}$.

(e) En déduire que le produit d'un nombre fini d'entiers de la forme $1 + 4\,\ell$ est encore de cette forme.

(f) On introduit l'ensemble :

$$X \,:=\, \mathscr{P} \cap \big(3 + 4\,\mathbb{N}\big).$$

L'objectif est de montrer que $\mathsf{Card}\, X \,=\, \infty$ (de même que l'on sait que $\infty \,=\, \mathsf{Card}\, \mathscr{P}$), autrement dit, qu'il existe une infinité de nombres *premiers* de la forme $3 + 4\,k$ avec $k \in \mathbb{N}$.

En raisonnant par l'absurde, on suppose la finitude de $\mathsf{Card}\, X =: r < \infty$, et on écrit :

$$X \,=\, \big\{p_1,\, p_2,\, p_3,\, \ldots, p_r\big\},$$

avec, comme à la Question **(a)**, $p_1 = 3$, $p_2 = 7$, $p_3 = 11, \ldots$ On pose :

$$A \,:=\, -1 + 4\,p_1 p_2 p_3 \cdots p_r.$$

Établir que la décomposition en facteurs premiers de A incorpore alors au moins un nombre premier de la forme $q = 3 + 4\,k$.

(g) Conclure.

Exercice 7. On rappelle que l'*ordre* d'un élément $x \in G$ d'un groupe G est :

$$o(x) \,:=\, \mathsf{min}\,\big\{m \geqslant 1\colon\ x^m = 1_G\big\}.$$

Soient H et K deux groupes, dont les lois respectives sont notées multiplicativement (sans symbole), et dont les éléments neutres sont notés simplement 1 et 1. On considère le *groupe produit :*

$$H \times K \,:=\, \big\{(h, k)\colon\ h \in H,\ k \in K\big\},$$

muni de la loi produit, agissant composante par composante, avec $(1, 1)$ pour élément neutre.

(a) Montrer que si h est un élément d'ordre $p \geqslant 1$ de H et si k est un élément d'ordre $q \geqslant 1$ de K, alors (h, k) est un élément d'ordre :

$$r \,:=\, \mathsf{ppcm}\,\big(p, q\big),$$

dans $H \times K$.

(b) On rappelle qu'un groupe G est dit *cyclique* s'il existe un élément $x \in G$ et un entier $n \geqslant 1$ tels que :

$$G \,=\, \big\{1_G,\, x,\, \ldots,\, x^{n-1}\big\} \qquad\qquad \text{avec} \qquad\qquad x^n \,=\, 1_G.$$

On suppose dorénavant que H et K sont tous les deux des groupes cycliques. On note :

$$r := \mathsf{Card}\, H \qquad \text{et} \qquad s := \mathsf{Card}\, K.$$

Montrer que :

$$r \wedge s = 1 \qquad \Longrightarrow \qquad H \times K \text{ est cyclique.}$$

(c) En supposant toujours H et K cycliques, montrer l'implication inverse :

$$r \wedge s = 1 \qquad \Longleftarrow \qquad H \times K \text{ est cyclique.}$$

18. Corrigé de l'examen 9

Exercice 1. **(a)** Pour $n = 1$:

$$22 \;=\; 4 \cdot 5 + \boxed{2},$$

pour $n = 2$:

$$29 \;=\; 3 \cdot 8 + \boxed{5},$$

pour $n = 3$:

$$36 \;=\; 3 \cdot 11 + \boxed{3},$$

pour $n = 4$:

$$43 \;=\; 3 \cdot 14 + \boxed{1},$$

les restes demandés étant encadrés.

(b) Une unique observation suffit :

$$7\,n + 15 \;=\; 2\,(3\,n + 2) + \boxed{n + 11},$$

puisque alors, le reste encadré est bien strictement inférieur à ce par quoi l'on divise :

$$n + 11 \;\overset{?}{<}\; 3\,n + 2 \qquad\qquad \Longleftrightarrow \qquad\qquad 9 \;\overset{?}{<}\; 2\,n \quad \text{OUI},$$

car par hypothèse, $n \geqslant 5$.

(c) Pour $n = 0$, on a bien :

$$2^{0+1} + 3^{0+3} \;=\; 29 \;\equiv\; 0 \mod 29.$$

Supposons à un certain niveau n que $2^{3n+1} + 3^{n+3}$ est multiple de 29, à savoir, supposons qu'il existe un entier $k \in \mathbb{N}$ tel que :

$$2^{5n+1} + 3^{n+3} \;=\; 29\,k.$$

Alors un calcul astucieux :

$$\begin{aligned}
2^{5(n+1)+1} + 3^{n+1+3} &= 2^5 \cdot 2^{5n+1} + 3 \cdot \underline{3^{n+3}}_{\text{rpl}} \\
\text{[Hyp-Réc]} \qquad &= 2^5 \cdot 2^{5n+1} + 3 \cdot \left(29\,k - 2^{5n+1}\right) \\
&= \left(2^5 - 3\right) 2^{5n+1} + 29 \cdot 3\,k \\
&= 29 \cdot \Big(\underbrace{2^{5n+1} + 3\,k}_{=:\,\ell \in N}\Big),
\end{aligned}$$

montre que la divisibilité par 29 est encore vraie à l'étage $n + 1$ au-dessus, donc est vraie pour tout entier $n \geqslant 0$, grâce au principe d'induction complète.

Exercice 2. (a) Descendons l'échelle d'Euclide :

$$\begin{aligned} 87 &= 3 \cdot 24 + 15 \\ 24 &= 1 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + \boxed{3} \\ 6 &= 2 \cdot 3 + \mathbf{0}, \end{aligned}$$

et empoignons par le col le dernier reste non nul qui frétille comme un gardon :

$$\boxed{3} = \mathsf{pgcd}\,\big(87, 24\big).$$

(b) Cette équation :

$$3 \cdot 8\,x + 3 \cdot 29\,y = c,$$

dont le membre de gauche est multiple de 3, ne peut clairement avoir de solution que si $c = 3\,c'$ avec $c' \in \mathbb{Z}$ est aussi multiple de 3.

Dans cette circonstance, après division par 3, l'équation à résoudre est équivalente à :

$$8\,x + 29\,y = c'.$$

Comme $8 \wedge 29 = 1$ sont premiers entre eux, le théorème de Bézout fournit en principe deux entiers u et v qui satisfont :

$$8\,u + 29\,v = 1,$$

et puisque la Question **(c)** que nous n'avons pas hésité à lire à l'avance fournissait implicitement une réponse, nous devinons — en nous épargnant d'avoir à effectuer le calcul parfois difficile de remontée salmonique de la cascade d'Euclide — que :

$$8 \cdot 11 + 29 \cdot (-3) = 1,$$

ce qui est vrai !

Enfin, en multipliant cette identité de Bézout par c', puis par 3 :

$$\begin{aligned} 8 \cdot 11\,c' - 29 \cdot 3\,c' &= c', \\ 3 \cdot 8 \cdot 11c' - 3 \cdot 29 \cdot 3\,c' &= 3\,c' \end{aligned}$$

nous obtenons au moins une solution de l'équation proposée :

$$24 \cdot \underbrace{11\,c'}_{x} - 87 \cdot \underbrace{3\,c'}_{y} = c.$$

(c) Un résultat du cours, basé sur le théorème de Gauss, donne alors directement l'ensemble complet des solutions, tel qu'il est écrit.

Exercice 3. (a) Tout d'abord, vérifions l'*associativité* de la loi $*$. Pour $x, y, z \in G$ quelconques, on a bien, grâce à l'associativité de la loi (non écrite) du groupe original G :

$$\begin{aligned} (x * y) * z &= \big(x\,a\,y\big)\,a\,z \\ &= x\,a\,\big(y\,a\,z\big) \\ &= x * (y * z). \end{aligned}$$

Ensuite, avec $x \in G$ quelconque, vérifions que l'élément neutre pour la loi $*$ est $e' := a^{-1}$. Les *deux* identités qui doivent être satisfaites (et non pas une seule, car le groupe n'est pas forcément commutatif) :

$$\begin{aligned} x * e' &= x * a^{-1} = x\,\underline{a\,a^{-1}}_{\circ} = x, \\ e' * x &= a^{-1} * x = \underline{a^{-1}\,a}_{\circ}\,x = x, \end{aligned}$$

le sont effectivement, ce qui est charmant.

Enfin — merci à l'indic de service ! —, vérifions que $x' := a^{-1}x^{-1}a^{-1}$ est bien l'inverse, pour la loi $*$, de x, ce qui, à nouveau en vertu de la définition mathématique rigoureuse d'une structure de groupe, exige *deux* calculs *non équivalents* (bien que similaires) :

$$\begin{aligned} x * a^{-1}x^{-1}a^{-1} &= \underline{x\,\underline{a\,a^{-1}}_{\circ}\,x^{-1}}_{\circ\circ}\,a^{-1} = e\,a^{-1} = e', \\ a^{-1}x^{-1}a^{-1} * x &= a^{-1}\underline{x^{-1}\underline{a^{-1}\,a}_{\circ}\,x}_{\circ\circ} = a^{-1}\,e = e'. \end{aligned}$$

(b) D'après le cours, un sous-ensemble (non vide) $H \subset G$ est un sous-groupe (pour la loi originale) si et seulement si :

$$\text{pour tout } x \in H \text{ et pour tout } y \in H \text{ d'inverse } y^{-1} \in G \quad \text{on a } x\,y^{-1} \in H \text{ aussi.}$$

(c) Effectivement :

$$\begin{aligned} a^{-1}\,y * a^{-1}\,y^{-1} &= a^{-1}\,\underline{y\,\underline{a\,a^{-1}}_{\circ}\,y^{-1}}_{\circ\circ} = a^{-1} = e', \\ a^{-1}\,y^{-1} * a^{-1}\,y &= a^{-1}\,\underline{y^{-1}\,\underline{a\,a^{-1}}_{\circ}\,y}_{\circ\circ} = a^{-1} = e'. \end{aligned}$$

(d) D'après le critère rappelé à la Question **(b)**, il s'agit de montrer que pour tous :

$$u = a^{-1}\,x \in K \qquad \text{et} \qquad v = a^{-1}\,y \in K,$$

avec :

$$x \in H \text{ quelconque} \qquad \text{et} \qquad y \in H \text{ quelconque,}$$

— d'où en vertu de l'hypothèse que H est un sous-groupe :

$$x\,y^{-1} \in H \text{ —,}$$

nous avons encore :

$$u * v' \overset{?}{\in} K.$$

Or comme grâce la Question **(c)** nous connaissons l'inverse :

$$v' = \left(a^{-1}\,y\right)' = a^{-1}\,y^{-1},$$

tous ces préliminaires nous permettent de calculer soigneusement :

$$\begin{aligned} u * v' &= a^{-1}\,x * \left(a^{-1}\,y\right)' \\ &= a^{-1}\,x * a^{-1}\,y^{-1} \\ &= a^{-1}\,x\,\underline{a\,a^{-1}}_{\circ}\,y^{-1} \\ &= \underbrace{a^{-1}\,\underbrace{x\,y^{-1}}_{\in H}}_{\in K}, \end{aligned}$$

et de constater que le produit $u * v'$ appartient bien encore à K.

(e) Pour $x, y \in G$ arbitraires, nous avons :

$$\begin{aligned} f(x\,y) &= x\,y\,a^{-1} \\ &= x\,a^{-1}\,a\,y\,a^{-1} \\ &= x\,a^{-1} * y\,a^{-1} \\ &= f(x) * f(y), \end{aligned}$$

ce qui montre que f est un morphisme (de groupes).

Ce morphisme est *bijectif*, car l'application inverse évidente :

$$\begin{array}{ccccc} (G,\cdot) & \longleftarrow & (G,*) & : & g \\ y\,a & \longleftarrow\!\shortmid & y, & & \end{array}$$

satisfait visiblement :

$$g \circ f \;=\; \mathsf{Id} \;=\; f \circ g.$$

Exercice 4. **(a)** Pour $q = \overline{0}, \overline{1}, \overline{2}$ dans $\mathbb{Z}/3\,\mathbb{Z}$ et pour $r = \overline{0}, \overline{1}, \overline{2}$, on a :

$$\begin{array}{ccccc} & \overline{0} & \overline{1} & \overline{2} \\ \overline{x}^2 & \overline{0} & \overline{1} & \overline{1} \\ \overline{x}^4 & \overline{0} & \overline{1} & \overline{1} \end{array} \qquad \text{et} \qquad \begin{array}{ccccc} & \overline{0} & \overline{1} & \overline{2} \\ \overline{r}^2 & \overline{0} & \overline{1} & \overline{1} \\ 2+\overline{r}^2 & \overline{2} & \overline{0} & \overline{0} \end{array}$$

donc :

$$\big\{\overline{0},\,\overline{1}\big\} \;\ni\; q^4 \;=\; 2 + r^2 \;\in\; \big\{\overline{0},\,\overline{2}\big\},$$

la seule valeur possible dans l'intersection étant :

$$\overline{0} \;=\; q^4 \;=\; 2 + r^2 \;=\; \overline{0}.$$

(b) Pour $p = \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ dans $\mathbb{Z}/5\,\mathbb{Z}$ et pour $r = \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$, on a :

$$\begin{array}{ccccc} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{p}^4 & \overline{0} & \overline{1} & \overline{1} & \overline{1} & \overline{1} \\ 3\,\overline{p}^4 & \overline{0} & \overline{3} & \overline{3} & \overline{3} & \overline{3} \end{array} \qquad \text{et} \qquad \begin{array}{ccccc} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{r}^2 & \overline{0} & \overline{1} & -\overline{1} & -\overline{1} & \overline{1} \\ 1+4\,\overline{r}^2 & \overline{1} & \overline{0} & \overline{2} & \overline{2} & \overline{0} \end{array}$$

donc :

$$\big\{\overline{0},\,\overline{3}\big\} \;\ni\; 3\,p^4 \;=\; 1 + 4\,r^2 \;\in\; \big\{\overline{0},\,\overline{1},\,\overline{2}\big\},$$

la seule valeur possible dans l'intersection étant :

$$\overline{0} \;=\; 3\,p^4 \;=\; 1 + 4\,r^2 \;=\; \overline{0}.$$

(c) Après réduction modulo 3, l'équation devient :

$$0 - 2\,q^4 - 1\,r^2 \;\equiv\; 2 \;\mod 3,$$

c'est-à-dire :

$$q^4 \;\equiv\; 2 + r^2 \;\mod 3,$$

et on reconnaît ce qui a été déjà préparé par la Question **(a)**.

Ainsi, nous savons que $q^4 \equiv 0 \mod 3$, *i.e.* que (iy-heu-queu) :

$$3 \,\big|\, q\,q\,q\,q,$$

et le théorème d'Euclide donne $3 \,|\, q$, et enfin, comme par hypothèse $q \in \mathscr{P}$, il est incontournable que $q = 3$.

(d) Puisque nous savons dorénavant que $q = 3$, remplaçons cette valeur dans (ED) :

$$\begin{aligned} 3\,p^4 - 4\,r^2 &= 26 + 5 \cdot 3^4 \\ &= 26 + 5 \cdot 81 \\ &= 431, \end{aligned}$$

puis, gaillardement, réduisons modulo nos 5 doigts :

$$3\,p^4 \equiv 1 + 4\,r^2 \mod 5.$$

Eurêka ! Nous reconnaissons l'équation traitée à la Question **(b)** ! Donc nous savons que :

$$3\,p^4 \equiv 0 \mod 5,$$

c'est-à-dire :

$$5 \,\big|\, 3\,p\,p\,p\,p,$$

et le théorème de Gauss-Euclide donne :

$$5 \,\big|\, p,$$

et comme $p \in \mathscr{P}$ est premier, il est incontournable que $p = 5$.

(e) Comme $p = 5$, nous pouvons remplacer cette valeur dans l'équation diophantienne réduite que nous avons écrite dans notre réponse à la Question **(d)**, ce qui nous donne :

$$\begin{aligned} 3 \cdot 5^4 - 4\,r^2 &= 431 \\ 3 \cdot 625 - 431 &= 4\,r^2 \\ 1\,444 &= 4\,r^2 \\ 361 &= r^2, \end{aligned}$$

et comme la sélection à l'entrée de la L2-DéDé exigeait de connaître par cœur toutes ses tables de multiplications jusqu'à $25 \cdot 25 = 625$, l'étudiant bien à l'aise dans ses bottes arithmétiques reconnaît instantanément le *carré* d'une excellente note sur 20 :

$$19 = r.$$

En conclusion, l'équation diophantienne (ED) possède une *unique* solution entière constituée de nombres premiers, à savoir :

$$\big(p,\, q,\, r\big) = \big(5,\, 3,\, 19\big).$$

Exercice 5. (a) (i) $(\mathbb{R}^*, \times)$ est bien un groupe, mais il n'est pas divisible, car pour $x = -1 \in \mathbb{R}^*$ et $n = 2 \in \mathbb{N}^*$, on sait que $\forall\, y \in \mathbb{R}^*$, on a $y^2 > 0$, donc $y^2 \neq x$.

(ii) $(\mathbb{Q}_+^*, \times)$ est bien un groupe, mais il n'est pas divisible, car pour $x = 2 \in \mathbb{Q}_+^*$ et $n = 2 \in \mathbb{N}^*$, on sait depuis la Préhistoire que $y^2 = 2$ n'a pas de solution dans $\mathbb{Q}$, donc pas dans $\mathbb{Q}_+^*$.

(iii) $(\mathbb{R}, +)$ *est bien un groupe divisible* — n'en voilà enfin un ! —, car si $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$, en posant $y = \frac{x}{n} \in \mathbb{R}$, on a :

$$y^n = \left(\tfrac{x}{n}\right) + \cdots + \left(\tfrac{x}{n}\right) = x.$$

(iv) $(\mathbb{Z}, +)$ est bien un groupe, mais hélas, il n'est pas divisible — match perdu 1 à 3 —, car pour $x = 1 \in \mathbb{Z}$ et $n = 2 \in \mathbb{N}^*$, l'équation $2\,y = 1$ n'a pas de solution dans $\mathbb{Z}$ puisque $\frac{1}{2} \notin \mathbb{Z}$.

(b) Supposons que $G_1 \times G_2$ est divisible. Soient $x_1 \in G_1$, $x_2 \in G_2$ et $n \in \mathbb{N}^*$. Donc il existe $(y_1, y_2) \in G_1 \times G_2$ tel que $(y_1, y_2)^n = (x_1, x_2)$. Donc $y_1^n = x_1$ et $y_2^n = x_2$, donc G_1 et G_2 sont divisibles car $y_1 \in G_1$ et $y_2 \in G_2$.

Réciproquement, supposons que G_1 et G_2 sont divisibles. Soient $(x_1, x_2) \in G_1 \times G_2$ et $n \in \mathbb{N}^*$. Donc il existe $y_1 \in G_1$ et $y_2 \in G_2$ tels que $y_1^n = x_1$ et $y_2^n = x_2$ (puisque $x_1 \in G_1$ et $x_2 \in G_2$). Donc $(y_1, y_2) \in G_1 \times G_2$ et $(y_1, y_2)^n = (x_1, x_2)$. Donc $G_1 \times G_2$ est divisible.

(c) Supposons que G_1 est divisible. Soient $x_2 \in G_2$ et $n \in \mathbb{N}^*$. Comme ψ est bijective, il existe $x_1 \in G$ tel que $x_2 = \psi(x_1)$. De plus, comme G_1 est divisible, il existe $y_1 \in G_1$ tel que $y_1^n = x_1$. Donc $\psi(y_1^n) = \psi(x_1) = x_2$. En posant $y_2 = \psi(y_1) \in G_2$, on a :

$$\begin{aligned} x_2 = \psi(y_1^n) &= (\psi(y_1))^n \qquad \text{car } \psi \text{ est un morphisme} \\ &= y_2^n, \end{aligned}$$

d'où $x_2 = y_2^n$, donc G_2 est divisible.

Par symétrie, la réciproque se démontre de même au moyen de l'isomorphisme *inverse* $G_1 \longleftarrow G_2 \colon\ \psi^{-1}$.

(d) La Question **(a)** nous a appris que $(\mathbb{R}, +)$ est divisible, tandis que $(\mathbb{R}^*, \times)$ ne l'est *pas*. Donc à cause de la Question **(c)**, il ne peuvent certainement pas être isomorphes !

Exercice 6. (a) Éh non, Cunégonde ! Car avec $k = 3$:

$$3 + 4 \cdot 3 \;=\; 15 \;=\; 3 \cdot 5,$$

n'est pas premier !

(b) Écrivons, mon bon Gédéon, pour $k = 0, 1, 2, \ldots, 9, 10$, ces onze nombres $3 + 4\,k$, et sélectionnons seulement les perles premières :

$$\boxed{3}, \quad \boxed{7}, \quad \boxed{11}, \quad 15, \quad \boxed{19}, \quad \boxed{23}, \quad 27, \quad \boxed{31}, \quad 35, \quad 39, \quad \boxed{43}.$$

(c) Après $2, 3 \in \mathscr{P}$, aucun entier $n \geqslant 4$ qui est *pair*, donc de la forme $n = 2\,m$ avec $m \geqslant 2$, ne pourrait être premier, car il admettrait 2 comme diviseur strict.

Donc chaque nombre premier $p \geqslant 3$ est impair, c'est-à-dire de la forme $q = 1 + 2\,m$ avec $m \geqslant 1$. Suivant que $m = 2\,\ell$ est *pair*, ou que $m = 1 + 2\,k$ est *impair*, on trouve :

$$q \;=\; 1 + 4\,\ell \qquad\qquad \text{ou} \qquad\qquad q \;=\; 3 + 4\,k.$$

(d) Même avec $\ell \in \mathbb{Z}$ de signe quelconque, cela est vrai, puisqu'on a vu en cours que :

$$\left.\begin{aligned} n_1 &\equiv 1 \mod 4 \\ n_2 &\equiv 1 \mod 4 \end{aligned}\right\} \qquad \Longrightarrow \qquad n_1\, n_2 \;\equiv\; 1 \cdot 1 \mod 4.$$

(e) Pareil avec un nombre quelconque $r \geqslant 1$ de facteurs :

$$\left.\begin{aligned} n_1 &\equiv 1 \mod 4 \\ &\cdots\cdots\cdots\cdots \\ n_r &\equiv 1 \mod 4 \end{aligned}\right\} \qquad \Longrightarrow \qquad n_1 \cdots n_r \;\equiv\; 1 \cdots 1 \mod 4,$$

car quand on a compris comment multiplier 1 par 1, on ne se met plus aucune limite !

(f) Évidemment, le nombre premier 2 n'apparaît pas comme facteur premier dans la décomposition de :

$$A \;=\; -1 + 4\,p_1 \cdots p_r,$$

qui est impair. Donc grâce à la Question **(c)**, tous les facteurs premiers q de A sont de la forme :

$$q \,=\, 1 + 4\,\ell \qquad\qquad \text{ou} \qquad\qquad q \,=\, 3 + 4\,k.$$

Mais si *tous* (sans exception) les facteurs premiers de A étaient de la forme $1+4\,\ell$, donc $\equiv\, 1 \bmod 4$, alors d'après la Question **(e)**, l'entier A serait lui aussi $\equiv\, 1 \bmod 4$, ce qui n'est pas le cas puisque :

$$\begin{aligned} A \,&=\, -1 + 4\,p_1 \cdots p_r \\ &\equiv\, -1 \mod 4 \\ &\equiv\, 3 \mod 4. \end{aligned}$$

Par conséquent, il est nécessaire que, dans la décomposition en facteurs premiers de A, il existe au moins un nombre premier q de la forme $q = 3 + 4\,k$.

(g) Rappelons que nous cherchons à atteindre une contradiction après avoir supposé (en raisonnant par l'absurde) que l'ensemble X de tous les nombres premiers de la forme $3+4\,k$ était *fini*, $X = \big\{p_1, \ldots, p_r\big\}$.

Forcément, le facteur premier $q = 3 + 4\,k$ de A dont nous venons d'affirmer l'existence devrait donc appartenir à cette liste, donc être égal $q = p_i$ à l'un d'entre eux pour un certain indice $1 \leqslant i \leqslant r$.

Mézalor, en réduisant notre grand A modulo ce petit p_i :

$$A \,=\, p_i\,\big(\cdots\big) \qquad\qquad \text{et} \qquad\qquad A \,=\, -1 + p_1 \cdots p_i \cdots p_r,$$

nous aboutissons à une contradiction manifeste :

$$A \,\equiv\, 0 \mod p_i \qquad\qquad \text{et} \qquad\qquad A \,\equiv\, -1 \mod p_i,$$

qui est conclusive.

La force grandiose (*sic !*) du raisonnement par l'absurde nous permet ainsi d'affirmer qu'il existe une infinité de nombres premiers de la forme $3 + 4\,k$.

« *Mézalor*, en prenant les normes, 6 diviserait 4 ou 9, ce qui n'est pas. »
Pierre Samuel, Théorie algébrique des nombres, Éditions Hermann, Paris, 1997.

Exercice 7. (a) Par définition, pour tout entier $i \geqslant 1$, on a :

$$(h,k)^i \,=\, \underbrace{(h,k)\,(h,k)\,\cdots(h,k)}_{\text{composé } i \text{ fois}} \,=\, \big(h^i, k^i\big).$$

D'après un théorème du cours, valable dans n'importe quel groupe, l'ordre d'un élément se repère en prenant ses puissances successives jusqu'à retomber au point neutre :

$$\begin{aligned} o\,\big(h,k\big) \,&=\, \min\Big\{i \in \mathbb{N}_{\geqslant 1} \colon\ (h,k)^i = (1,1)\Big\} \\ &=\, \min\Big\{i \in \mathbb{N}_{\geqslant 1} \colon\ h^i = 1 \text{ et } k^i = 1\Big\}. \end{aligned}$$

Or, toujours d'après le cours, $h^i = 1$ est satisfait si et seulement si i est multiple entier de $p = o(h)$; de même $k^i = 1$ est satisfait si et seulement si i est multiple entier de $q = o(k)$.

Ainsi, i doit être multiple à la fois de p et de q, et puisque c'est le i *minimal* qui nous intéresse, il est clair, d'après la définition arithmétique du pipicm — oui, il y a deux i ici, minimaux —, que :

$$\begin{aligned} o\,\big(h,k\big) \,&=\, \mathsf{ppcm}\,\big(p,q\big) \\ &=\, \mathsf{ppcm}\,\big(o(h),\, o(k)\big). \end{aligned}$$

(b) Par hypothèse, il existe deux éléments $h \in H$ et $k \in K$ qui *engendrent* H et K au sens où :

$$H = \{1, h, \ldots, h^{r-1}\} \qquad \text{et} \qquad K = \{1, k, \ldots, k^{s-1}\},$$

les éléments écrits dans les accolades étant mutuellement distincts.

Rappelons que :

$$\mathsf{Card}\, H \times K = \mathsf{Card}\, H \cdot \mathsf{Card}\, K = r\, s.$$

Maintenant, nous affirmons que les puissances successives de l'élément :

$$(h, k) \in H \times K$$

engendrent $H \times K$ en totalité, et, plus précisément, nous affirmons que :

$$H \times K = \Big\{(1,1),\ (h,k),\ \big(h^2,\ k^2\big),\ \ldots,\ \big(h^{rs-1},\ k^{rs-1}\big)\Big\},$$

avec $r\, s$ éléments écrits dans les accolades que nous affirmons mutuellement distincts.

En effet, comme $o(h) = r$, comme $o(k) = s$, et comme l'hypothèse que $r \wedge s = 1$ sont premiers entre eux implique :

$$\mathsf{ppcm}\,(r, s) = r\, s,$$

il suffit d'appliquer la Question **(a)**, qui nous donne :

$$o\,(h, k) = r\, s,$$

ce qui garantit, d'après un raisonnement (basé sur la division euclidienne) qui a été plusieurs fois vu en cours dans divers contextes, que les $r\, s$ éléments :

$$\Big\{\big(h^i,\ k^i\big)\Big\}_{0 \leqslant i \leqslant r\, s - 1}$$

sont bien mutuellement distincts, et donc, « remplissent bien » le produit $H \times K$, qui est de cardinal égal à ce même nombre $r\, s$.

(c) Par hypothèse, il existe un certain élément $(h, k) \in H \times K$ qui est générateur :

$$\begin{aligned} \big\{(x, y)\colon\ x \in H,\ k \in K\big\} &= H \times K \\ &= \Big\{\big(h^i,\ k^i\big)\Big\}_{0 \leqslant i \leqslant r\, s - 1}. \end{aligned}$$

Autrement dit :

$$o\,(h, k) = r\, s.$$

En particulier, en prenant toutes les premières composantes h^i de ces $\big(h^i, k^i\big)$, on doit trouver tous les éléments possibles $x \in H$. Donc — et de même pour les secondes composantes — :

$$\begin{aligned} H &= \big\{h^i\colon\ 0 \leqslant i \leqslant r\, s - 1\big\}, \\ K &= \big\{k^i\colon\ 0 \leqslant i \leqslant r\, s - 1\big\}, \end{aligned}$$

ce qui signifie que h et k sont chacun générateurs de leurs groupes respectifs (lesquels étaient supposés cycliques depuis le début, donc ne serions-nous pas en train de « tourner en rond » ?).

Mais non, nous ne tournons pas en rond ! Un heureux dénouement nous attend ! Car comme :

$$\begin{aligned} o\,(h) &= r, \\ o\,(k) &= s, \end{aligned}$$

et puisque, d'après la Question **(a)**, l'élément (h, k) est d'ordre $\mathsf{ppcm}\,(r, s)$, nous concluons que :

$$r\,s \;=\; \boldsymbol{o}\,(h, k) \;=\; \mathsf{ppcm}\,(r, s),$$

ce qui n'est possible que si :

$$r \wedge s \;=\; 1.$$

19. Examen 10

Exercice 1. **(a)** Effectuer la division euclidienne de A par B, où :

$$A := 3X^5 + 4X^2 + 1, \qquad B := X^2 + 2X + 3.$$

(b) À quelles conditions sur $a, b, c \in \mathbb{R}$ le polynôme $E := X^4 + aX^2 + bX + c$ est-il divisible par le polynôme $F := X^2 + X + 1$?

Exercice 2. **(a)** Avec $n \in \mathbb{N}_{\geqslant 1}$, effectuer la divsion euclidienne de P_n par Q_n, où :

$$P_n := nX^{n+1} - (n+1)X^n + 1 \qquad Q_n := X^n - nX + n - 1.$$

(b) Pour $n = 1$, déterminer pgcd (P_1, Q_1).

(c) Pour $n \geqslant 2$, déterminer pgcd (P_n, Q_n). Indication: Le pgcd est le même que pour $n = 1$.

Exercice 3. Avec $n \geqslant 4$ entier, soit $\mathfrak{S}_n$ le groupe des permutations de $\{1, 2, \ldots, n\}$.

(a) Soient trois entiers $1 \leqslant i, j, k \leqslant n$ qui sont distincts deux à deux. Montrer que le produit des deux transpositions :

$$\big(i\ j\big) \circ \big(j\ k\big),$$

est égal à un 3-cycle, que l'on déterminera.

(b) Soient quatre entiers $1 \leqslant i, j, k, l \leqslant n$ qui sont distincts deux à deux. Montrer que le produit des deux 3-cycles :

$$\big(i\ j\ k\big) \circ \big(i\ l\ k\big)$$

est égal à un produit de deux transpositions, que l'on déterminera.

(c) On considère maintenant un produit :

$$s = t_1 \circ t_2 \circ \cdots \circ t_{2\nu-1} \circ t_{2\nu},$$

d'un nombre *pair* de transpositions $t_\kappa \in \mathfrak{S}_n$. Justifier que l'on peut supposer que $t_\kappa \neq t_{\kappa+1}$, pour tout $\kappa = 1, \ldots, 2\nu - 1$.

(d) Établir que la permutation $s = t_1 \circ t_2 \circ \cdots \circ t_{2\nu-1} \circ t_{2\nu}$ est aussi égale à un produit de 3-cycles.

Exercice 4. **(a)** Soient les deux permutations de l'ensemble $\big\{1, 2, 3, \ldots, 11\big\}$:

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

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

Montrer sans calculs que σ et τ commutent.

(b) Vérifier par un calcul direct que $\sigma \circ \tau = \tau \circ \sigma$.

(c) Décomposer σ et τ en cycles à supports disjoints.

(d) Décomposer en produit de cycles à supports disjoints le produit suivant de trois permutations de $\{1, 2, 3, \ldots, 10\}$:

$$\big(1\ \ 8\ \ 6\ \ 7\big)\,\big(8\ \ 6\ \ 7\ \ 5\big)\,\big(6\ \ 7\ \ 5\ \ 1\big).$$

(e) Soit la permutation de $\{1, 2, 3, 4, 5\}$:

$$\theta \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}.$$

Calculer θ^{2023}.

(f) Soit la permutation des entiers de 1 à 12 définie par :

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

Décomposer ω en produit de transpositions, en appliquant l'algorithme suivant, qui consiste, pour une permutation donnée de $\{1, \ldots, n\}$, à remettre les éléments $1, \ldots, n$ de la deuxième ligne *dans l'ordre*, en en mettant (au moins) un à sa « place » à chaque étape, comme cela est illustré, pour la permutation :

$$\theta \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 5 & 1 & 4 & 6 \end{pmatrix},$$

ci-dessous :

$$\begin{aligned}
1\ 2\ 3\ 4\ 5\ 6\ 7 \;&\xrightarrow{\ \theta\ }\; 3\ 7\ 2\ 5\ 1\ 4\ 6 \\
&\xrightarrow{\ \tau_{1,3}\ }\; 1\ 7\ 2\ 5\ 3\ 4\ 6 \\
&\xrightarrow{\ \tau_{2,7}\ }\; 1\ 2\ 7\ 5\ 3\ 4\ 6 \\
&\xrightarrow{\ \tau_{3,7}\ }\; 1\ 2\ 3\ 5\ 7\ 4\ 6 \\
&\xrightarrow{\ \tau_{5,4}\ }\; 1\ 2\ 3\ 4\ 7\ 5\ 6 \\
&\xrightarrow{\ \tau_{5,7}\ }\; 1\ 2\ 3\ 4\ 5\ 7\ 6 \\
&\xrightarrow{\ \tau_{6,7}\ }\; 1\ 2\ 3\ 4\ 5\ 6\ 7,
\end{aligned}$$

d'où :

$$\tau_{6,7} \circ \tau_{5,7} \circ \tau_{5,4} \circ \tau_{3,7} \circ \tau_{2,7} \circ \tau_{1,3} \circ \theta \;=\; \mathsf{Id}.$$

(g) En déduire la signature $\varepsilon(\theta)$ de θ, puis celle $\varepsilon(\omega)$ de ω. Indication: Elles sont différentes.

Exercice 5. L'objectif est de décomposer en éléments simples, dans $\mathbb{R}[x]$, puis dans $\mathbb{C}[x]$, la fraction rationnelle :

$$A(x) \;:=\; \frac{(x^2+1)^2}{(x+1)^2\,(3\,x^2-2\,x+1)}.$$

(a) Justifier et montrer l'égalité :

$$A(x) \;=\; \frac{1}{3} + \frac{a}{(x+1)^2} + \frac{a'}{x+1} + \frac{b\,x+c}{3\,x^2-2\,x+1},$$

avec des inconnues réelles $a, a', b, c \in \mathbb{R}$.

(b) Déterminer la valeur de la constante $a \in \mathbb{R}$.

(c) On pose :

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

Établir que :

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

(d) Décomposer $B(x)$ en éléments simples dans $\mathbb{R}[x]$, et ensuite, en déduire la décomposition de $A(x)$ en éléments simples dans $\mathbb{R}[x]$.

(e) Trouver la décomposition en éléments simples de $A(x)$ sur $\mathbb{C}[x]$.

Exercice 6. Soit un groupe abstrait G noté multiplicativement, et soient deux sous-groupes $H \subset G$ et $K \subset G$. L'objectif est de montrer que $H \cup K$ est aussi un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

(a) Lorsque $H \subset K$, que dire ?

(b) On suppose dorénavant que $H \not\subset K$, et on se propose d'établir que $K \subset H$, ce qui remplira l'objectif.

Soit $h \in H \backslash K$. Montrer que :

$$\forall\, y \;\in\; K, \qquad h\,y \;\notin\; K.$$

(c) En supposant de plus que $H \cup K$ est un sous-groupe de G, montrer que $K \subset H$.

(d) Conclure.

Exercice 7. Soit A un anneau *pas forcément commutatif* dans lequel $a^2 = a$ pour tout $a \in A$.

(a) Montrer que $a + a = 0$, pour tout $a \in A$. Indication: On pourra développer $(a+1)\,(a+1)$.

(b) Montrer que $a\,b = -\,b\,a$, puis que $a\,b = b\,a$, pour tous $a, b \in A$, c'est-à-dire que A est, en fait, commutatif.

(c) Montrer que $a\,b\,(a+b) = 0$, pour tous $a, b \in A$.

(d) Montrer que si A contient au moins trois éléments distincts, alors A n'est pas un anneau intègre.

20. Corrigé de l'examen 10

Exercice 1. **(a)** Il fallait trouver :

$$3\,X^5 + 4\,X^2 + 1 \;=\; \big(X^2 + 2\,X + 3\big)\,\big(3\,X^3 - 6\,X^2 + 3\,X + 16\big) - 41\,X - 47.$$

(b) Si nous euclidivisons E par F :

$$X^4 + a\,X^2 + b\,X + c \;=\; \big(X^2 + X + 1\big)\,\big(X^2 - X + a\big) + (b - a + 1)\,X + c - a,$$

il est clair que $F \mid E$ si et seulement si le reste obtenu est le polynôme nul, c'est-à-dire ssi :

$$\left.\begin{aligned} 0 &= b - a + 1 \\ 0 &= c - a \end{aligned}\right\} \qquad \Longleftrightarrow \qquad \left\{\begin{aligned} b &= a - 1, \\ c &= a. \end{aligned}\right.$$

Exercice 2. **(a)** On trouve :

$$n\,X^{n+1} - (n+1)\,X^n + 1 \;=\; \big(X^n - n\,X + n - 1\big)\,\big(n\,X - (n+1)\big) + n^2\,(X-1)^2.$$

(b) Puisque, pour $n = 1$:

$$P_1 \;=\; X^2 - 2\,X + 1, \qquad\qquad Q_1 \;=\; 0,$$

il est clair que :

$$\mathsf{pgcd}\,(P_1, Q_1) \;=\; \mathsf{pgcd}\,(P_1, 0) \;=\; P_1 \;=\; (X-1)^2.$$

(c) Nous n'allons pas re-diviser Q_n par $n^2\,(X-1)^2$ comme le ferait tout élève stupide d'Euclide ! Mieux, nous allons vérifier que Q_n est divisible par $(X-1)^2$, comme suit :

- 1 est racine de Q_n, car $1^n - n \cdot 1 + n - 1 = 0$;
- 1 est aussi racine du polynôme dérivé :

$$Q_n' \;=\; n\,X^{n-1} - n,$$

car $n \cdot 1^{n-1} - n = 0$;

donc un théorème du cours assure que Q_n est divisible par $(X-1)^2$, et l'on peut écrire $Q_n = (X-1)^2\,R_n$ pour un certain polynôme R_n.

Enfin, en repartant de l'équation :

$$P_n \;=\; Q_n\,(\cdots) + n^2\,(X-1)^2,$$

il vient :

$$\begin{aligned} \mathsf{pgcd}\,(P_n, Q_n) \;&=\; \mathsf{pgcd}\,\big(Q_n,\; n^2(X-1)^2\big) \\ &=\; \mathsf{pgcd}\,\big((X-1)^2\,R_n,\; n^2(X-1)^2\big) \\ &=\; (X-1)^2. \end{aligned}$$

Sinon, les étudiants scrupuleux d'Euclide qui auront re-divisé Q_n par $n^2\,(X-1)^2$ devraient être parvenus à trouver le résultat :

$$Q_n \;=\; n^2\,(X-1)^2\left(\frac{1}{n^2}\sum_{1 \leqslant i \leqslant n-1} i\;X^{n-1-i}\right) + \mathbf{0},$$

avec un reste nul, ce qui leur montrerait d'une manière alternative que le pgcd demandé est bien égal à $(X-1)^2$.

Exercice 3. **(a)** En effet, calculons cette composition :

$$\begin{array}{cccc} & i & j & k \\ (j\ k) & \downarrow & \downarrow & \downarrow \\ & i & k & j \\ (i\ j) & \downarrow & \downarrow & \downarrow \\ & j & k & i \end{array},$$

et constatons qu'elle est bien égale à une permutation circulaire :

$$\big(i\ j\big) \circ \big(j\ k\big) \;=\; \big(i\ j\ k\big).$$

(b) En effet, calculons cette composition :

$$\begin{array}{cccc} & i & j & k & l \\ (i\ l\ k) & \downarrow & \downarrow & \downarrow & \downarrow \\ & l & j & i & k \\ (i\ j\ k) & \downarrow & \downarrow & \downarrow & \downarrow \\ & l & k & j & i \end{array},$$

et constatons qu'elle est bien égale à la composition de deux transpositions :

$$\big(i\ j\ k\big) \circ \big(i\ l\ k\big) \;=\; \big(i\ l\big) \circ \big(j\ k\big),$$

qui, d'ailleurs, commutent, puisqu'elles sont à supports disjoints.

(c) Effectivement, il est bien connu que toute transposition est d'ordre 2 :

$$t_\kappa \circ t_\kappa \;=\; \mathsf{Id} \qquad (1 \leqslant \kappa \leqslant 2\,\nu).$$

Par conséquent, dans le produit proposé de 2ν transpositions :

$$s \;=\; t_1 \circ \cdots\cdots t_\kappa \circ \underbrace{t_{\kappa+1}}_{=\,t_\kappa} \circ \cdots \circ t_{2\nu},$$

quand il se produit que deux transpositions immédiatement voisines sont *égales*, on peut naturellement les *supprimer :*

$$\begin{aligned} s \;&=\; t_1 \circ \cdots \circ t_{\kappa-1} \circ \underbrace{t_\kappa \circ t_\kappa}_{=\,\mathsf{Id}} \circ t_{\kappa+2} \circ \cdots \circ t_{2\nu} \\ &=\; t_1 \circ \cdots \circ t_{\kappa-1} \circ \mathsf{Id} \circ t_{\kappa+2} \circ \cdots \circ t_{2\nu} \\ &=\; t_1 \circ \cdots \circ t_{\kappa-1} \circ t_{\kappa+2} \circ \cdots \circ t_{2\nu}. \end{aligned}$$

Une fois cette opération effectuée, il est possible que $t_{\kappa-1}$ soit égale à $t_{\kappa+2}$, et alors, on recommence. On répète ce procédé jusqu'à épuisement, c'est-à-dire jusqu'à ce qu'il ne reste, dans s, *aucune* paire de deux transpositions successives qui soient égales. On dit alors que s est sous forme réduite.

Évidemment, comme le nombre initial $2\,\nu$ de transposition qui constituait s était pair, et comme on supprime à chaque fois 2 (un nombre pair !) de transpositions, à la fin, la forme réduite de s comporte toujours un nombre *pair* de transpositions.

(d) Sans perte de généralité, nous pouvons donc supposer que s est sous forme réduite, à savoir que s ne comporte aucun couple de transpositions successives qui soient égales.

En particulier, si nous regroupons les transpositions par paires :

$$s \,=\, t_1 \circ t_2 \circ \cdots \circ t_{2\lambda-1} \circ t_{2\lambda} \circ \cdots \circ t_{2\nu-1} \circ t_{2\nu},$$

pour tout $\lambda = 1, \ldots, \nu$, nous avons :

$$t_{2\lambda-1} \,\neq\, t_{2\lambda}.$$

Comme chacune de ces deux transpositions $t_{2\lambda-1}$ et $t_{2\lambda}$ implique un doubleton d'entiers appartenant à $\{1, \ldots, n\}$, et comme ces deux doubletons d'entiers ne sont pas égaux, exactement deux cas peuvent se produire concernant les $2 + 2 = 4$ entiers impliqués :

(**Cas 1**) $\quad t_{2\lambda-1} \,=\, \big(i\ j\big) \qquad t_{2\lambda} \,=\, \big(j\ k\big), \qquad$ avec $i,\ j,\ k$ distincts;

(**Cas 2**) $\quad t_{2\lambda-1} \,=\, \big(i\ j\big) \qquad t_{2\lambda} \,=\, \big(k\ l\big), \qquad$ avec $i,\ j,\ k,\ l$ distincts.

Dans le premier cas, la Question **(a)** nous permet de remplacer la composition des deux permutations circulaires considérées par un 3-cycle :

$$t_{2\lambda-1} \circ t_{2\lambda} \,=\, \big(i\ j\big) \circ \big(j\ k\big) \,=\, \big(i\ j\ k\big).$$

Dans le deuxième cas, la Question **(b)** nous permet de remplacer la composition des deux permutations circulaires considérées par la compositions de deux 3-cycles :

$$\begin{aligned} t_{2\lambda-1} \circ t_{2\lambda} \,&=\, \big(i\ j\big) \circ \big(k\ l\big) \\ &=\, \big(i\ k\ l\big) \circ \big(i\ j\ l\big), \end{aligned}$$

en faisant attention aux changements de lettres.

Après avoir effectué ces opérations de remplacement pour tous les couples successifs $t_{2\lambda-1} \circ t_{2\lambda}$ de transpositions, c'est-à-dire pour tout $\lambda = 1, \ldots, \nu$, nous avons bien démontré, au final, que toute composition $s = t_1 \circ t_2 \circ \cdots \circ t_{2\nu-1} \circ t_{2\nu}$ d'un nombre 2ν pair de 2-cycles est aussi égale à un certain produit de 3-cycles.

Exercice 4. **(a)** Il suffit d'observer que les deux supports :

$$\begin{aligned} \mathsf{Supp}\,\sigma \,&=\, \big\{1,\ 3,\ 5,\ 6,\ 8,\ 11\big\}, \\ \mathsf{Supp}\,\tau \,&=\, \big\{2,\ 7,\ 9,\ 10\big\}, \end{aligned}$$

sont disjoints !

(b) En effet :

$$\begin{array}{cccccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 9 & 3 & 4 & 5 & 6 & 2 & 8 & 10 & 7 & 11 \\ \sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 9 & 6 & 4 & 1 & 5 & 2 & 11 & 10 & 7 & 8 \end{array} \;=\; \begin{array}{cccccccccccc} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \sigma & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 2 & 6 & 4 & 1 & 5 & 7 & 11 & 9 & 10 & 8 \\ \tau & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 9 & 6 & 4 & 1 & 5 & 2 & 11 & 10 & 7 & 8 \end{array}$$

(c) D'un seul coup d'œil comme Guy l'Éclair :

$$\begin{aligned} \sigma \,&=\, \big(1\ \ 3\ \ 6\ \ 5\big)\,\big(8\ \ 11\big), \\ \tau \,&=\, \big(2\ \ 9\ \ 10\ \ 7\big). \end{aligned}$$

(d) Comme les cinq éléments de l'ensemble $\big\{2, 3, 4, 9, 10\big\}$ du complémentaire de la réunion des trois supports concernés sont toujours fixés, nous pouvons nous contenter

d'écrire cette composition sous la forme :

$$\begin{array}{ccccc} 1 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 1 & 7 & 5 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 5 & 8 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 8 & 5 & 6 & 7 \end{array}$$

et donc 1 est fixé aussi, et enfin :

$$\big(1\ \ 8\ \ 6\ \ 7\big)\big(8\ \ 6\ \ 7\ \ 5\big)\big(6\ \ 7\ \ 5\ \ 1\big) \,=\, \big(5\ \ 8\ \ 7\ \ 6\big)$$

.

(e) Comme θ admet la décomposition :

$$\theta \,=\, \big(1\ \ 2\ \ 4\big)\big(3\ \ 5\big),$$

en deux cycles d'ordres égaux à leurs longueurs respectives, un théorème du cours donne :

$$o(\sigma) \,=\, \mathsf{ppcm}\,(3,2) \,=\, 6,$$

et donc :

$$\sigma^{2023} \,=\, \big(\sigma^6\big)^{337}\,\sigma \,=\, \sigma.$$

(f) De manière analogue :

$$\begin{array}{rcl} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12 & \xrightarrow{\omega} & 7\ 1\ 5\ 12\ 6\ 3\ 9\ 4\ 2\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{1,7}} & 1\ 7\ 5\ 12\ 6\ 3\ 9\ 4\ 2\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{2,7}} & 1\ 2\ 5\ 12\ 6\ 3\ 9\ 4\ 7\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{3,5}} & 1\ 2\ 3\ 12\ 6\ 5\ 9\ 4\ 7\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{4,12}} & 1\ 2\ 3\ 4\ 6\ 5\ 9\ 12\ 7\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{5,6}} & 1\ 2\ 3\ 4\ 5\ 6\ 9\ 12\ 7\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{7,9}} & 1\ 2\ 3\ 4\ 5\ 6\ 7\ 12\ 9\ 11\ 8\ 10 \\ & \xrightarrow{\tau_{8,12}} & 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 11\ 12\ 10 \\ & \xrightarrow{\tau_{10,11}} & 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 12\ 11 \\ & \xrightarrow{\tau_{11,12}} & 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12, \end{array}$$

d'où :

$$\tau_{11,12} \circ \tau_{10,11} \circ \tau_{8,12} \circ \tau_{7,9} \circ \tau_{5,6} \circ \tau_{4,12} \circ \tau_{3,5} \circ \tau_{2,7} \circ \tau_{1,7} \circ \omega \,=\, \mathsf{Id}.$$

(g) Comme le cours nous l'a appris, la signature d'une permutation vaut (-1) à la puissance le nombre de transpositions en lesquelles on peut la décomposer, la *parité* de ce nombre étant indépendante de la décomposition.

Comme pour :

$$\begin{aligned} \theta \,&=\, \tau_{1,3}^{-1} \circ \tau_{2,7}^{-1} \circ \tau_{3,7}^{-1} \circ \tau_{5,4}^{-1} \circ \tau_{5,7}^{-1} \circ \tau_{6,7}^{-1} \\ &=\, \tau_{1,3} \circ \tau_{2,7} \circ \tau_{3,7} \circ \tau_{5,4} \circ \tau_{5,7} \circ \tau_{6,7}, \end{aligned}$$

il y a 6 transpositions, nous trouvons $\varepsilon(\theta) = (-1)^6 = 1$.

Et comme, pour :

$$\begin{aligned}\omega &= \tau_{1,7}^{-1} \circ \tau_{2,7}^{-1} \circ \tau_{3,5}^{-1} \circ \tau_{4,12}^{-1} \circ \tau_{5,6}^{-1} \circ \tau_{7,9}^{-1} \circ \tau_{8,12}^{-1} \circ \tau_{10,11}^{-1} \circ \tau_{11,12}^{-1} \\ &= \tau_{1,7} \circ \tau_{2,7} \circ \tau_{3,5} \circ \tau_{4,12} \circ \tau_{5,6} \circ \tau_{7,9} \circ \tau_{8,12} \circ \tau_{10,11} \circ \tau_{11,12},\end{aligned}$$

il y a 9 transpositions, nous trouvons $\varepsilon(\omega) = (-1)^9 = -1$.

Exercice 5. (a) Tout d'abord, au dénominateur, le polynôme du second degré :

$$3\,x^2 - 2\,x + 1,$$

a un discriminant égal à :

$$(-2)^2 - 4 \cdot 3 \cdot 1 \;=\; -8 \;<\; 0,$$

strictement négatif, donc ce polynôme est irréductible sur $\mathbb{R}[x]$.

Si $r(x)$ désigne le *reste* de la division euclidienne du numérateur de $A(x)$ par son dénominateur, un théorème du cours garantit que l'on peut décomposer $A(x)$ sous la forme :

$$A(x) \;=\; r(x) + \frac{a}{(x+1)^2} + \frac{a'}{x+1} + \frac{b\,x + c}{3\,x^2 - 2\,x + 1},$$

avec constantes réelles $a, a', b, c \in \mathbb{R}$ qu'il faudra déterminer plus tard.

En tout cas, pour l'instant, puisque :

$$A(x) \;=\; \frac{x^4 + \cdots}{x^2\,3\,x^2 + \cdots},$$

les points de suspension désignant des termes de degrés inférieurs, on trouve que $r(x)$ est de degré 0, égale à la constante :

$$r(x) \;=\; \lim_{x \to \infty} \frac{x^4 + \cdots}{3\,x^4 + \cdots} \;=\; \frac{1}{3},$$

d'où comme demandé :

$$A(x) \;=\; \frac{1}{3} + \frac{a}{(x+1)^2} + \frac{a'}{x+1} + \frac{b\,x + c}{3\,x^2 - 2\,x + 1},$$

(b) Multiplions l'égalité de la Question **(a)** par $(x+1)^2$ pour obtenir :

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

d'où après simplifications :

$$\frac{(x^2+1)^2}{3\,x^2 - 2\,x + 1} \;=\; (x+1)^2\,\frac{1}{3} + a + a'\,(x+1) + (x+1)^2\,\frac{b\,x + c}{3\,x^2 - 2\,x + 1}.$$

En posant $x := -1$, *tous* les termes à droite sauf a s'évanouissent (deviennent égaux à 0), et donc, nous obtenons :

$$\frac{((-1)^2+1)^2}{3\,(-1)^2 - 2\,(-1) + 1} \;=\; \frac{4}{6} \;=\; 0 + a + 0 + 0,$$

c'est-à-dire :

$$\frac{2}{3} \;=\; a.$$

(c) Maintenant que nous connaissons les valeurs de $r(x)$ et de a, il suffit de soustraire et de calculer — sans erreur ! — en commençant par réduire au même dénominateur :

$$\begin{aligned} B(x) &= \frac{(x^2+1)^2}{(x+1)^2\,(3\,x^2-2\,x+1)} - \frac{1}{3} - \frac{2}{3\,(x+1)^2} \\ &= \frac{3\,(x^2+1)^2 - (x+1)^2\,(3\,x^2-2\,x+1) - 2\,(3\,x^2-2\,x+1)}{3\,(x+1)^2\,(3\,x^2-2\,x+1)} \\ &= \frac{3\,x^4+6\,x^2+3-(x^2+2\,x+1)\,(3\,x^2-2\,x+1)-6\,x^2+4\,x-2}{3\,(x+1)^2\,(3\,x^2-2\,x+1)}, \end{aligned}$$

en développant le produit au centre :

$$\begin{aligned} \big(x^2+2\,x+1\big)\,\big(3\,x^2-2\,x+1\big) &= 3\,x^4-2\,x^3+x^2+6\,x^3-4\,x^2+2\,x+3\,x^2-2\,x+1 \\ &= 3\,x^4+4\,x^3+1 \end{aligned}$$

et en sommant le tout :

$$\begin{aligned} B(x) &= \frac{3\,x^4+6\,x^2+3-3\,x^4-4\,x^3-1-6\,x^2+4\,x-2}{3\,(x+1)^2\,(3\,x^2-2\,x+1)} \\ &= \frac{-4\,x^3+4\,x}{3\,(x+1)^2\,(3\,x^2-2\,x+1)}, \end{aligned}$$

en observant astucieusement que le numérateur se factorise :

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

et en concluant finalement que le tout se simplifie :

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

(d) D'après la Question **(a)**, quand on a retranché les deux premiers termes, il reste :

$$\begin{aligned} B(x) &= \frac{a'}{x+1} + \frac{b\,x+c}{3\,x^2-2\,x+1} \\ \text{[Question (c)]} \qquad &= -\frac{4}{3}\,\frac{x\,(x-1)}{(x+1)\,(3\,x^2-2\,x+1)}, \end{aligned}$$

toujours avec des constantes inconnues $a, b, c \in \mathbb{R}$. Il s'agit donc ici de déterminer la décomposition en éléments simples de $B(x)$.

Pour ce faire, réduisons au même dénominateur à gauche et à droite :

$$\frac{3\,(3\,x^2-2\,x+1)\,a' + 3\,(x+1)\,(b\,x+c)}{3\,(x+1)\,(3\,x^2-2\,x+1)} = \frac{-4\,x\,(x-1)}{3\,(x+1)\,(3\,x^2-2\,x+1)},$$

identifions les deux numérateurs :

$$3\,(3\,x^2-2\,x+1)\,a' + 3\,(x+1)\,(b\,x+c) = -4\,x\,(x-1),$$

développons-les et plaçons tous les termes à gauche :

$$\big(9\,a'+3\,b+4\big)\,x^2 + \big(-\,6\,a'+3\,b+3\,c-4\big)\,x + 3\,a'+3\,c = 0.$$

Ce trinôme en x devant être identiquement nul, nous obtenons le système linéaire suivant :

$$\begin{aligned} 9\,a' + 3\,b \qquad &= -\,4 \\ -\,6\,a' + 3\,b + 3\,c &= \quad 4 \\ 3\,a' + \qquad 3\,c &= \quad 0 \end{aligned}$$

La combinaison linéaire des trois lignes L_1, L_2, L_3 :

$$0 \;=\; L_1 + L_2 - L_3 \;=\; 6\,b$$

permet de résoudre rapidement ce système linéaire :

$$b \;:=\; 0, \qquad\qquad a' \;:=\; -\,\frac{4}{9}, \qquad\qquad c \;:=\; \frac{4}{9}.$$

Ainsi :

$$B(x) \;=\; -\,\frac{4}{9}\,\frac{1}{x+1} + \frac{4}{9}\,\frac{1}{3\,x^2 - 2\,x + 1},$$

et en conclusion, nous obtenons la décomposition en élément simple de la proposée :

$$A(x) \;=\; \frac{1}{3} + \frac{2}{3}\,\frac{1}{(x+1)^2} - \frac{4}{9}\,\frac{1}{x+1} + \frac{4}{9}\,\frac{1}{3\,x^2 - 2\,x + 1}.$$

(e) Sachant que les deux racines complexes conjuguées de $3\,x^2 - 2\,x + 1$ sont :

$$\frac{2 \pm \sqrt{-\,8}}{2 \cdot 3} \;=\; \frac{1 \pm i\,\sqrt{2}}{3},$$

il reste, en oubliant temporairement le coefficient $\frac{4}{9}$, à décomposer :

$$\frac{1}{3\,x^2 - 2\,x + 1} \;=\; \frac{1}{3\,\big(x - (\frac{1}{3} + i\,\frac{\sqrt{2}}{3})\big)\,\big(x - (\frac{1}{3} - i\,\frac{\sqrt{2}}{3})\big)}.$$

Or comme pour toute constante complexe non réelle $\alpha \in \mathbb{C}\backslash\mathbb{R}$, on a :

$$\frac{1}{3}\,\frac{1}{(x-\alpha)\,(x-\overline{\alpha})} \;=\; \frac{1}{3}\,\frac{1}{\alpha - \overline{\alpha}}\left\{\frac{1}{(x-\alpha)} - \frac{1}{(x-\overline{\alpha})}\right\},$$

avec :

$$\alpha \;:=\; \frac{1}{3} + i\,\frac{\sqrt{2}}{3},$$

d'où :

$$\alpha - \overline{\alpha} \;=\; \frac{1}{3} + i\,\frac{\sqrt{2}}{3} - \left(\frac{1}{3} - i\,\frac{\sqrt{2}}{3}\right) \;=\; i\,2\,\tfrac{\sqrt{2}}{3},$$

nous avons :

$$\begin{aligned} \frac{1}{3\,x^2 - 2\,x + 1} \;&=\; \frac{1}{3}\,\frac{1}{\big(x - (\frac{1}{3} + i\,\frac{\sqrt{2}}{3})\big)\,\big(x - (\frac{1}{3} - i\,\frac{\sqrt{2}}{3})\big)} \\ &=\; \frac{1}{3}\,\frac{1}{i\,2\,\frac{\sqrt{2}}{3}}\left\{\frac{1}{x - \frac{1}{3} - i\,\frac{\sqrt{2}}{3}} - \frac{1}{x - \frac{1}{3} + i\,\frac{\sqrt{2}}{3}}\right\} \\ &=\; -\,i\,\frac{1}{2\,\sqrt{2}}\,\frac{1}{x - \frac{1}{3} - i\,\frac{\sqrt{2}}{3}} + i\,\frac{1}{2\,\sqrt{2}}\,\frac{1}{x - \frac{1}{3} + i\,\frac{\sqrt{2}}{3}} \\ &=\; -\,i\,\frac{\sqrt{2}}{4}\,\frac{1}{x - \frac{1}{3} - i\,\frac{\sqrt{2}}{3}} + i\,\frac{\sqrt{2}}{4}\,\frac{1}{x - \frac{1}{3} + i\,\frac{\sqrt{2}}{3}}, \end{aligned}$$

et enfin, en re-multipliant par $\frac{4}{9}$:

$$\begin{aligned}\frac{4}{9}\,\frac{1}{3\,x^2-2\,x+1} &= \frac{4}{9}\left(-\,i\,\frac{\sqrt{2}}{4}\,\frac{1}{x-\frac{1}{3}-i\,\frac{\sqrt{2}}{3}}+i\,\frac{\sqrt{2}}{4}\,\frac{1}{x-\frac{1}{3}+i\,\frac{\sqrt{2}}{3}}\right)\\ &= -\,i\,\frac{\sqrt{2}}{9}\,\frac{1}{x-\frac{1}{3}-i\,\frac{\sqrt{2}}{3}}+i\,\frac{\sqrt{2}}{9}\,\frac{1}{x-\frac{1}{3}+i\,\frac{\sqrt{2}}{3}}.\end{aligned}$$

En conclusion, la décomposition en éléments simples sur $\mathbb{C}[x]$ de la fraction rationnelle $A(x)$ est :

$$A(x) \;=\; \frac{1}{3}+\frac{2}{3}\,\frac{1}{(x+1)^2}-\frac{4}{9}\,\frac{1}{x+1}-i\,\frac{\sqrt{2}}{9}\,\frac{1}{x-\frac{1}{3}-i\,\frac{\sqrt{2}}{3}}+i\,\frac{\sqrt{2}}{9}\,\frac{1}{x-\frac{1}{3}+i\,\frac{\sqrt{2}}{3}}.$$

Exercice 6. **(a)** Trivial, Charlie ! $H\cup K=K$ est un sous-groupe, gratuitement !

(b) Par l'absurde, si, pour un $y\in K$, on avait $h\,y\in K$, alors on déduirait que :

$$\underbrace{h\,y}_{\in K}\cdot\underbrace{y^{-1}}_{\in K} \;=\; h \;\in\; K,$$

serait aussi un élément de K, contrairement à l'hypothèse qui a été faite sur h.

(c) Comme $h\in H\subset H\cup K$, comme $y\in K\subset H\cup K$, et comme on suppose que $H\cup K$ est un sous-groupe, il est clair que :

$$h\,y \;\in\; H\cup K \qquad\qquad (h\in H\backslash K \text{ fixé}, \forall\, y\in K).$$

Mais $h\,y\notin K$ d'après la Question **(b)**, donc nécessairement :

$$\begin{aligned} h\,y \;&\in\; H\\ \Longrightarrow\qquad y \;&\in\; h^{-1}H \;=\; H,\end{aligned}$$

c'est-à-dire que $\forall\, y\in K$ on a $y\in H$, ce qui fait bien voir que $K\subset H$.

(d) Ainsi nous avons démontré que :

$$\Big(H\;\not\subset\;K \quad \text{et} \quad H\cup K \text{ sous-groupe}\Big) \qquad\Longrightarrow\qquad K\;\subset\;H,$$

ce qui remplit l'objectif qui nous était assigné.

Exercice 7. **(a)** Par hypothèse, pour tous $a,b\in A$, on a :

$(a+1)\,(a+1) \;=\; a+1,$ c'est-à-dire : $a^2+a\,1+1\,a+1^2 \;=\; a+1,$

d'où :

$$a+a \;=\; 0 \qquad\qquad (\forall\, a\in A).$$

(b) Par hypothèse, pour tous $a,b\in A$, on a :

$$a^2 \;=\; a, \qquad b^2 \;=\; b, \qquad (a+b)\,(a+b) \;=\; a+b,$$

$$\begin{aligned}\underline{a^2}_{\circ}+a\,b+b\,a+\underline{b^2}_{\circ\circ} \;&=\; \underline{a}_{\circ}+\underline{b}_{\circ\circ},\\ a\,b+b\,a \;&=\; 0,\end{aligned}$$

d'où :

$$a\,b \;=\; -\,b\,a \;=\; b\,a,$$

puisque $-\,c=c$, pour tout $c\in A$.

(c) Grâce au fait que nous savons dorénavant que A est commutatif, nous pouvons développer aisément $a\,b\,(a+b)$, ré-utiliser l'hypothèse de départ, et appliquer le résultat des Questions **(a)**, **(b)** qui précèdent :

$$\begin{aligned} a\,b\,(a+b) &= a\,b\,a + a\,b\,b \\ &= a^2\,b + a\,b^2 \\ &= a\,b + b\,a \\ &= 0. \end{aligned}$$

(d) Puisque A contient 0 et (au moins) trois éléments deux à deux distincts, il est clair qu'il existe $a \in A$ avec $a \neq 0$ et il existe $b \in A$ avec $b \neq 0$ tel que $b \neq a$. Autrement dit, $\big\{0, a, b\big\}$ est un triplet d'éléments de A *mutuellement distincts*.

Si on avait $a\,b = 0$, ce serait terminé, nous verrions immédiatement que A n'est pas intègre. Donc nous pouvons supposer que $a\,b \neq 0$.

D'après la Question **(c)** qui précède, il est toujours vrai que :

$$0 = a\,b\,\big(a+b\big).$$

Maintenant, nous aimerions savoir si $a + b \neq 0$ ici.

Or, pour tous $a, b \in A$ l'annulation $a + b = 0$ entraînerait, grâce à la Question **(a)** :

$$a = -b = -b + 0 = -b + b + b = b,$$

c'est-à-dire $a = b$, ce qui contredirait notre hypothèse $a \neq b$. Donc nous avons bien $a + b \neq 0$ ici.

En définitive, dans notre produit nul $a\,b\,(a+b) = 0$, nous savons que $a\,b \neq 0$ et que $a + b \neq 0$, ce qui montre que A n'est pas intègre.