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 $\mathbb{Z}\big/37\mathbb{Z}$.

(c) L'entier $1\,035 \mod 1\,665$ est-il inversible dans $\mathbb{Z}\big/1\,665\mathbb{Z}$ 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 $m \in \mathbb{Z}$:

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

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 :

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

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 :

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

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 $\mathbb{Z}\big/37\mathbb{Z}$.

(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 :

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

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

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

Ainsi, on calcule les carrés de ces 8 éléments$\big/$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 :

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

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 :

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

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 :

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

(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 :

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

(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 $\mathbb{R}[x]$:

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

(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 :

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

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

Exercice 2. Soit l'ensemble $E := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. 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 :

$$\sigma \,:=\, \Big(\ a_1 \longrightarrow a_2 \longrightarrow a_3 \ \Big) \,=\, (a_1\ a_2\ a_3)$$

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

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

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

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

on écrit son inverse :

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

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 :

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

(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 :

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

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 :

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

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 :

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

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 :

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

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 :

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

(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 2×2 = 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 :

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

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

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

(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 :

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

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

(e) D'après un théorème du cours, ce groupe $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ 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 $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ 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 :

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

En définitive, *tous* les 8 éléments de $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ sont d'ordre égal à 4 ou divisant 4, et donc, aucun ne peut être d'ordre 8. Ceci démontre que $\big(\mathbb{Z}/15\mathbb{Z}\big)^\times$ 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 :

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

(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 :

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

de telle sorte que :

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

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 $\ell\equiv 0 \mod p$.

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 :

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

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 :

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

[Question **(e)**]

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 :

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

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 :

$$\sigma(i) \,:=\, i + 1 \;\; \mathsf{mod}\; n.$$

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 :

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

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

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

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

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

Montrer que :

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

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 $\big\{1, 2, \dots, n\big\}$ à $n \geqslant 1$ éléments, l'ordre d'un p-cycle quelconque :

$$c_p = \Big(a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \Big),$$

avec $a_1, a_2, \dots, a_{p-1}, a_p \in \{1, \dots, n\}$ 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 $p = o(\sigma)$, 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 :

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

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 :

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

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

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

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 :

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

(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 :

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

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 :

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

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 :

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

nous avons :

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

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

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

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 :

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

(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 $n \geqslant 2$.