Exercices du CH03 : Structures algébriques usuelles

Exercices de la banque INP à étudier : ex 84 (racines n-ièmes de l'unité), 85 (factorisation de polynômes), 86 (démonstration petit théorème de Fermat), 89 (nombres complexes), 94 (système de congruences).

I Généralités sur les groupes

Sauf mention du contraire, les lois de groupe seront notées multiplicativement.

Exercice 1 (*Noyau)
Soient $(G, *)$ et $(G', \bullet)$, deux groupes, et $f : G \to G'$ un morphisme de groupes. Soient $x \in G$ et $y \in \ker f$. Montrer que $x * y * x^{-1} \in \ker f$.

Corrigé de l'exercice 1
Puisque f est un morphisme, on a

$$f(x * y * x^{-1}) = f(x) \bullet \underbrace{f(y)}_{=e_{G'}} \bullet f(x^{-1}) = f(x) \bullet f(x^{-1}) = f(x * x^{-1}) = f(e_G) = e_{G'},$$

donc $x * y * x^{-1} \in \ker(f)$.

Exercice 2 (*Exemples de morphismes de groupes)
Montrer que chacune des applications suivantes est un morphisme de groupes (en précisant les lois considérées). Déterminer leurs noyaux et images respectifs. Sont-ils injectifs ? surjectifs ? bijectifs ?

$$\begin{array}{rcl} f : \mathbb{C} & \to & \mathbb{C}, \\ z & \mapsto & \overline{z} \end{array} \qquad \begin{array}{rcl} g : \mathbb{C} & \to & \mathbb{C}^*, \\ z & \mapsto & e^z \end{array} \qquad \begin{array}{rcl} h_n : \mathbb{C}^* & \to & \mathbb{C}^*, \ n \in \mathbb{N}^* \\ z & \mapsto & z^n \end{array}$$

Corrigé de l'exercice 2

- $(\mathbb{C}, +)$ est un groupe et pour tout $(z, z') \in \mathbb{C}^2$:

  $$f(z + z') = \overline{z + z'} = \overline{z} + \overline{z'} = f(z) + f(z'),$$

  donc f est un morphisme de groupes.
  Puisque $f \circ f = Id$, f est bijectif, donc $Ker(f) = \{0\}$ et $Im(f) = \mathbb{C}$.
- $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ sont des groupes et pour tout $(z, z') \in \mathbb{C}^2$:

  $$g(z + z') = e^{z+z'} = e^z e^{z'} = g(z)g(z'),$$

  donc g est un morphisme de groupes.
  $Ker(g) = \{z \in \mathbb{C},\ e^z = 1\} = 2i\pi\mathbb{Z} \neq \{0\}$, donc g n'est pas injectif.
  $Im(g) = \mathbb{C}^*$ (car si $w \neq 0$, il existe $(\rho, \theta) \in]0, +\infty[\times\mathbb{R}$ tel que $w = \rho e^{i\theta} = e^{\ln(\rho)+i\theta}$), donc g est surjectif.
- Fixons $n \in \mathbb{N}^*$. $(\mathbb{C}^*, \times)$ est un groupe et pour tout $(z, z') \in (\mathbb{C}^*)^2$:

  $$h_n(zz') = (zz')^n = z^n(z')^n = h_n(z)h_n(z'),$$

  donc h_n est un morphisme de groupes.
  Si $n = 1$, $h_n = Id$, donc h_n est bijectif, $Ker(h_n) = \{1\}$ et $Im(h_n) = \mathbb{C}^*$.
  Si $n \geq 2$, alors $Ker(h_n) = \{z \in \mathbb{C}^*,\ z^n = 1\} = \mathbb{U}_n = \langle e^{2i\pi/n} \rangle \neq \{1\}$, donc h_n n'est pas injectif.
  En outre $Im(h_n) = \mathbb{C}^*$ car si $w \in \mathbb{C}^*$, il existe $(\rho, \theta) \in]0, +\infty[\times\mathbb{R}$ tel que $w = \rho e^{i\theta}$, et donc $w = h_n(\rho^{1/n} e^{i\theta/n})$, ce qui montre que h_n est surjectif.

Exercice 3 (Exemples de groupes isomorphes ou non)**

1. Les groupes $(\mathbb{Z}/6\mathbb{Z})$ et $\mathbb{U}_6$ sont-ils isomorphes ? Et les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{U}_6$?
   On justifiera soigneusement.
2. Les groupes $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ sont-ils isomorphes ?

Corrigé de l'exercice 3

1. $\mathbb{U}_6 = \langle e^{i\pi/3} \rangle = \{e^{ik\pi/3},\ k \in [\![0,5]\!]\}$, donc $\mathbb{U}_6$ est monogène et de cardinal 6.
   D'après le cours, $(\mathbb{U}_6, \times)$ est donc isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$. On a même un isomorphisme explicite :

$$\left\{ \begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \longrightarrow & \mathbb{U}_6 \\ \overline{k} & \longmapsto & e^{ik\pi/3} \end{array} \right. .$$

   De même façon, le groupe additif produit

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(\overline{0},\dot{0}), (\overline{0},\dot{1}), (\overline{0},\dot{2}), (\overline{1},\dot{0}), (\overline{1},\dot{1}), (\overline{1},\dot{2})\}$$

   est monogène de cardinal 6 car il est engendré par $(\overline{1},\dot{1})$ (les ordres possibles de cet élément sont $1, 2, 3, 6$ et $3 \times (\overline{1},\dot{1}) = (\overline{1},\dot{0}) \neq (\overline{0},\dot{0})$, donc cet élément est d'ordre 6).
   D'où $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$, et donc également à $(\mathbb{U}_6, \times)$.

   Remarque
   On peut aussi utiliser le théorème chinois : 2 étant premier avec 3, les anneaux $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +, \times)$ *et* $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ *sont isomorphes, et donc a fortiori les groupes additifs sous-jacents le sont.*

2. Non, $((\mathbb{Z}/2\mathbb{Z})^2, +)$ et $(\mathbb{Z}/4\mathbb{Z}, +)$ ne sont pas isomorphes, car $((\mathbb{Z}/2\mathbb{Z})^2, +)$ ne possède que des éléments d'ordre 1 ou 2 (facile à vérifier), alors que $(\mathbb{Z}/4\mathbb{Z}, +)$ est cyclique, donc possède un élément d'ordre 4 (on rappelle qu'un isomorphisme de groupes conserve les ordres des éléments).

Exercice 4 (*Groupe de matrices)

Par un argument rapide, établir que l'ensemble $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},\ n \in \mathbb{Z} \right\}$ est un sous-groupe de $GL_2(\mathbb{R})$, et qu'il est monogène.

Corrigé de l'exercice 4

L'application $\varphi : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \longrightarrow & (GL_2(\mathbb{R}), \times) \\ n & \longmapsto & \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \end{array} \right.$ est bien définie ($\det \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = 1 \neq 0$ pour tout $n \in \mathbb{Z}$) et c'est un morphisme de groupes car pour tout $(n, m) \in \mathbb{Z}^2$, $\varphi(n+m) = \varphi(n)\varphi(m)$. Donc son image H est un sous-groupe de $GL_2(\mathbb{R})$, et on a

$$H = \varphi(\mathbb{Z}) = \varphi(\langle 1 \rangle) = \langle \varphi(1) \rangle = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle,$$

donc H est monogène.

Exercice 5 (Ordres et sous-groupes)**

1. Que dire de l'ordre des éléments dans un groupe fini de cardinal p premier ?
   Par conséquent, quels sont les sous-groupes d'un groupe fini G de cardinal p premier ?
2. Déterminer tous les sous-groupes de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.
   Indication : On raisonnera sur les ordres possibles des éléments, compte tenu du cardinal du groupe...
3. Sans effort, déterminer tous les sous-groupes de $\mathbb{U}_4$, $\mathbb{U}_5$ et $\mathbb{U}_6$.

Corrigé de l'exercice 5

1. Si $Card(G) = p$ est premier, alors les ordres possibles des éléments de G sont 1 (pour le neutre) et p (pour les autres), puisque ce sont les diviseurs de p dans $\mathbb{N}$. On en déduit que G ne possède que deux sous-groupes : $\{e\}$ et G. En effet, tout sous-groupe H différent de $\{e\}$ contient un élément x d'ordre p, donc H contient $\langle x\rangle = G$.

   Remarque
   En particulier, tout groupe de cardinal premier est cyclique, et donc commutatif.

2. - Dans $\mathbb{Z}/4\mathbb{Z}$, il y a exactement deux éléments d'ordre 4 (les deux générateurs $\overline{1}$ et $\overline{3}$) et un d'ordre 2 (la classe $\overline{2}$). Donc les sous-groupes sont $\{\overline{0}\}$, $\{\overline{0},\overline{2}\} = \langle\overline{2}\rangle$ et $\mathbb{Z}/4\mathbb{Z}$.
     En effet, un sous-groupe H différent de $\{\overline{0}\}$ et de $\mathbb{Z}/4\mathbb{Z}$ contient au moins deux éléments mais aucun d'ordre 4, donc il ne reste que les deux autres.
   - $\mathbb{Z}/5\mathbb{Z}$ étant de cardinal premier, il ne contient que deux sous-groupes : $\{\overline{0}\}$ et $\mathbb{Z}/5\mathbb{Z}$.
   - Dans $\mathbb{Z}/6\mathbb{Z}$, il y a exactement deux éléments d'ordre 6 (les deux générateurs $\overline{1}$ et $\overline{5}$), deux éléments d'ordre 3 ($\overline{2}$ et $\overline{4}$), et un élément d'ordre 2 ($\overline{3}$).
     Soit H un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$ différent de $\{\overline{0}\}$ et $\mathbb{Z}/6\mathbb{Z}$. Alors H ne contient aucun élément d'ordre 6, donc $\{\overline{0}\} \subsetneq H \subset \{\overline{0},\overline{2},\overline{3},\overline{4}\}$. Raisonnons alors en fonction du cardinal de H :
     — si $Card(H) = 2$, alors H contient nécessairement (en plus du neutre) un élément d'ordre 2, donc $H = \{\overline{0},\overline{3}\} = \langle\overline{3}\rangle$.
     — si $Card(H) = 3$, alors H contient nécessairement (en plus du neutre) deux éléments d'ordre 3, donc $H = \{\overline{0},\overline{2},\overline{4}\} = \langle\overline{2}\rangle$.
     — si $Card(H) = 4$, alors $H = \{\overline{0},\overline{2},\overline{3},\overline{4}\}$ mais ce n'est pas un sous-groupe (il n'est pas stable par somme).
     Donc $\mathbb{Z}/6\mathbb{Z}$ possède exactement 4 sous-groupes : $\{\overline{0}\}, \{\overline{0},\overline{3}\}, \{\overline{0},\overline{2},\overline{4}\}, \mathbb{Z}/6\mathbb{Z}$.

   Remarque
   Bien sûr, si on utilisait le théorème de Lagrange (hors programme), alors les cas $Card(H) \in \{4,5\}$ *seraient d'emblée éliminés.*

3. On sait que pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{U}_n, \times)$ est cyclique (engendré par $e^{2i\pi/n}$), donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ via l'application :

$$\theta : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ \overline{k} & \longmapsto & (e^{2i\pi/n})^k \end{array} \right. .$$

   Les sous-groupes de $\mathbb{U}_n$ sont donc les images par θ des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. Ainsi, en utilisant la question précédente :
   - Les sous-groupes de $\mathbb{U}_4$ sont $\{1\}$, $\{-1,1\}$, $\mathbb{U}_4$.
   - Les sous-groupes de $\mathbb{U}_5$ sont $\{1\}$, $\mathbb{U}_5$.
   - Les sous-groupes de $\mathbb{U}_6$ sont $\{1\}$, $\{-1,1\}$, $\{1,j,j^2\}$, $\mathbb{U}_6$ où $j = e^{2i\pi/3}$.

Exercice 6 (Conjugaison)**

Soit G un groupe. Pour $a \in G$, on note $f_a : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1} \end{array} \right.$.

Cette application est appelée *morphisme de conjugaison.*

1. Justement, montrer que pour tout $a \in G$, f_a est un automorphisme de G.
2. Montrer que $\varphi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & f_a \end{array} \right.$ est un morphisme de groupes, où $Aut(G)$ désigne l'ensemble des automorphismes du groupe G.
3. Est-ce que φ est injective ?

Corrigé de l'exercice 6

1. Soit $a \in G$. Pour tout $(x,y) \in G^2$, on a

$$f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y),$$

donc f_a est un morphisme de groupes. Et on voit facilement que f_a est bijectif, d'inverse

$$g_a = f_{a^{-1}} : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ y & \longmapsto & a^{-1}ya \end{array} \right. ,$$

(vérifier en explicitant $f_a \circ g_a$ et $g_a \circ f_a$) donc f_a est un automorphisme du groupe G.

2. Signalons déjà que $(Aut(G), \circ)$ est un groupe, en tant que sous-groupe du groupe des permutations $S(G) = \{\text{bijections } G \to G\}$. Ensuite, pour tout $(a, b) \in G^2$ et pour tout $x \in G$, on a

$$\varphi(ab)(x) = f_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = f_a(f_b(x)) = (f_a \circ f_b)(x) = (\varphi(a) \circ \varphi(b))(x),$$

ce qui montre que $\varphi(ab) = \varphi(a) \circ \varphi(b)$ dans $Aut(G)$, et donc que $\varphi : G \to Aut(G)$ est un morphisme de groupes.

3. $Ker(\varphi) = \{a \in G,\ f_a = Id\} = \{a \in G,\ \forall x \in G,\ ax = xa\}$. C'est le **centre de** G (éléments du groupe qui commutent avec tous les autres), noté $Z(G)$ en général.
On n'a pas toujours $Ker(\varphi) = \{e\}$. Par exemple :
   - En algèbre linéaire, si $G = GL(E)$ (groupe des automorphismes d'un espace vectoriel E), alors $Ker(\varphi) = Z(GL(E)) = \{\lambda Id,\ \lambda \in \mathbb{K}^*\}$, puisque les automorphismes linéaires qui commutent avec tous les autres sont les homothéties non nulles. Donc φ n'est pas injective.
   - Pire, si G est commutatif, alors dans ce cas $f_a = Id$ pour tout $a \in G$, donc φ est non injective (elle est constante !).

Exercice 7 (Morphismes entre groupes additifs)**

1. Déterminer tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$. *Regarder l'image de* $1\ldots$
2. Démontrer que les groupes additifs $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes.
3. Montrer que le seul morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ est le morphisme nul.

Corrigé de l'exercice 7

1. Soit $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ un morphisme de groupes. Pour tout $n \in \mathbb{N}$ on a

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = n\varphi(1),$$

(par récurrence immédiate), et la formule reste vraie pour les $n \in \mathbb{Z}$ puisque si $n < 0$, on a

$$\varphi(n) = \varphi(-|n|) = -\varphi(|n|) = -|n|\varphi(1) = n\varphi(1).$$

donc la valeur de $\varphi(1)$ détermine entièrement φ. Réciproquement, pour tout entier $n_0 \in \mathbb{Z}$, l'application $n \mapsto n_0 n$ est un morphisme de groupes de $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$.
Donc les morphismes cherchés sont les applications du type $n \mapsto n_0 n$ avec $n_0 \in \mathbb{Z}$.

2. Soit $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}^2, +)$ un morphisme de groupes. Alors :

$$Im(\varphi) = \varphi(\mathbb{Z}) = \varphi(\langle 1 \rangle) = \langle \varphi(1) \rangle.$$

En notant $\varphi(1) = (a, b) \in \mathbb{Z}^2$, on a donc

$$Im(\varphi) = \{(ka, kb),\ k \in \mathbb{Z}\}.$$

Si $a = 0$, alors $(1, 0) \notin Im(\varphi)$ et si $a \neq 0$, alors $(0, 1) \notin Im(\varphi)$. Donc φ n'est pas surjective, ce qui montre qu'il n'existe pas d'isomorphisme de groupes entre $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$.

3. Soit $\varphi : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ un morphisme de groupes. D'après la question 1., la restriction de φ à $\mathbb{Z}$ (qui est un morphisme de groupes $\mathbb{Z} \to \mathbb{Z}$), est de la forme $n \to n_0 n$, où $n_0 = \varphi(1) \in \mathbb{Z}$.
Si $\varphi(1) \neq 0$, alors

$$n_0 = \varphi(1) = \varphi(1/|n_0| + \cdots + 1/|n_0|) = |n_0|\varphi(1/|n_0|) = n_0\varphi(1/n_0),$$

donc nécessairement $\varphi(1/n_0) = 1$, ce qui entraîne par exemple :

$$2\varphi(1/2n_0) = \varphi(1/2n_0 + 1/2n_0) = \varphi(1/n_0) = 1$$

c'est-à-dire $\varphi(1/2n_0) = 1/2$, et cela contredit le fait que $\varphi(\mathbb{Q}) \subset \mathbb{Z}$.
Donc $\varphi(1) = 0$, ce qui entraîne pour tout $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$:

$$0 = \varphi(a) = \varphi(b \times a/b) = b \times \varphi(a/b)$$

et donc $\varphi(a/b) = 0$. Finalement, φ est le morphisme nul, et ce dernier est bien un morphisme de groupes. Donc il n'y a qu'un morphisme de groupes $(\mathbb{Q}, +) \to (\mathbb{Z}, +)$: le morphisme nul.

Exercice 8 (*Groupe fini et dénombrement)**
Soient A et B deux parties d'un groupe fini $(G, *)$ vérifiant : $Card(A) + Card(B) > Card(G)$.
Montrer que pour tout élément x de G, il existe $(a, b) \in A \times B$ tel que $x = a * b$.

Corrigé de l'exercice 8
Soit $x \in G$. On veut montrer qu'il existe $a \in A$ tel que $a^{-1} * x \in B$.
On considère donc l'application $\varphi_x : \left\{ \begin{array}{ccc} A & \longrightarrow & G \\ a & \longmapsto & a^{-1} * x \end{array} \right.$. Elle est injective (facile à vérifier), donc $Card(\varphi_x(A)) = Card(A)$. Il s'ensuit :

$$Card(\varphi_x(A) \cap B) = Card(\varphi_x(A)) + Card(B) - Card(\varphi_x(A) \cup B) = Card(A) + Card(B) - Card(\varphi_x(A) \cup B).$$

Mais $\varphi_x(A) \cup B \subset G$ donc

$$Card(\varphi_x(A) \cap B) \geq Card(A) + Card(B) - Card(G) > 0.$$

On en déduit que $\varphi_x(A) \cap B$ est non vide, ce qu'il fallait montrer.

Exercice 9 (*Théorème de Lagrange et ordre d'un élément dans un groupe fini)**
Soit G un groupe fini et H un sous-groupe de G.

1. Montrer que la relation définie par $x\mathcal{R}y \iff x^{-1}y \in H$ est une relation d'équivalence sur G, puis que toutes les classes d'équivalence de cette relation ont même cardinal.
2. En déduire que $Card(H)$ divise $Card(G)$ (c'est le *théorème de Lagrange*).
3. Application : en déduire que tout élément $x \in G$ vérifie $x^{Card(G)} = e$.
   On a donc ainsi démontré le théorème correspondant du cours.

Corrigé de l'exercice 9

1. La relation est réflexive car pour tout $x \in G$, $x^{-1}x = e \in H$, donc $x\mathcal{R}x$.
   Elle est symétrique car si $x\mathcal{R}y$, alors $x^{-1}y \in H$, donc (puisque H est stable par inverse) : $(x^{-1}y)^{-1} = y^{-1}x \in H$, c'est-à-dire $y\mathcal{R}x$.
   Enfin, elle est transitive car si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x^{-1}y \in H$ et $y^{-1}z \in H$, donc (puisque H est stable par produit) : $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$, c'est-à-dire $x\mathcal{R}z$.
   Examinons maintenant les classes d'équivalence. Pour $x \in G$ fixé, on a

   $$cl(x) = \{y \in G,\ x\mathcal{R}y\} = \{y \in G,\ x^{-1}y \in H\} = \{xh,\ h \in H\} = xH.$$

   L'application $h \mapsto xh$ étant une bijection de H sur xH (d'inverse $k \to x^{-1}k$), on en déduit que $cl(x)$ est en bijection avec H, donc toutes les classes d'équivalence de $\mathcal{R}$ ont même cardinal : celui de H.
2. G est fini et les classes $cl(x)$ partitionnent G (**comme dans toute relation d'équivalence**), donc il y a un nombre fini de classes, noté $N \in \mathbb{N}^*$, et il existe $x_1, \cdots, x_N$ dans G tel que $G = \bigcup_{i=1}^{N} cl(x_i)$ (réunion disjointe).
   On en déduit $Card(G) = \sum_{i=1}^{N} Card(cl(x_i)) = \sum_{i=1}^{N} Card(H) = NCard(H)$, donc $Card(H)$ divise $Card(G)$.
3. Fixons $x \in G$. Déjà, x est d'ordre fini car le sous-groupe engendré $H = \langle x \rangle$ est fini (G étant fini). En appliquant le théorème de Lagrange, on obtient que $ordre(x) = Card\langle x \rangle$ divise $Card(G)$, et donc $x^{Card(G)} = e$.

II Groupe symétrique

Exercice 10 (*Un exemple)
Décomposer la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 7 & 8 & 2 & 6 & 3 & 4 & 5 \end{pmatrix} \in S_9$ en produit de cycles disjoints et déterminer sa signature.

Corrigé de l'exercice 10
La décomposition est $\sigma = \begin{pmatrix} 1 & 9 & 5 & 2 \end{pmatrix}\begin{pmatrix} 3 & 7 \end{pmatrix}\begin{pmatrix} 4 & 8 \end{pmatrix}$.
Pour la signature :

- soit on utilise la décomposition précédente, que ε est un morphisme de groupes, et que la signature d'un p-cycle est $(-1)^{p-1}$:

$$\varepsilon(\sigma) = \varepsilon\begin{pmatrix} 1 & 9 & 5 & 2 \end{pmatrix}\varepsilon\begin{pmatrix} 3 & 7 \end{pmatrix}\varepsilon\begin{pmatrix} 4 & 8 \end{pmatrix} = (-1)^3(-1)^1(-1)^1 = -1.$$

- soit on compte les couples (i,j) avec $i<j$ présentant une inversion (i.e. $\sigma(i)>\sigma(j)$) :

$$(1,2),\cdots,(1,9),(3,5),\cdots,(3,9),(4,5),\cdots,(4,9),(6,7),(6,8),(6,9),$$

donc $I(\sigma)=21$, ce qui donne $\varepsilon(\sigma) = (-1)^{I(\sigma)} = (-1)^{21} = -1$.

Exercice 11 (Conjugaison d'un cycle)**
Soit $p \in \{1,\dots,n\}$ et $\sigma = (a_1\ \dots\ a_p)$ un p-cycle de S_n. Étant donné un élément quelconque $\rho \in S_n$, déterminer $\rho\circ\sigma\circ\rho^{-1}$ (élément dit « conjugué de σ par ρ »).

Corrigé de l'exercice 11
Soit $x \in \{1,\cdots,n\}$. Calculons $\rho\circ\sigma\circ\rho^{-1}(x)$.
On distingue deux cas :

- S'il existe $i \in \{1,\dots,p\}$ tel que $x = \rho(a_i)$, alors $\rho\circ\sigma\circ\rho^{-1}(x) = \rho\circ\sigma\circ\rho^{-1}\big(\rho(a_i)\big) = \rho\big(\sigma(a_i)\big) = \rho(a_{i+1})$, quitte à poser $a_{p+1}=a_0$ par commodité d'écriture.
- Sinon, c'est donc que, pour tout $i\in\{1,\dots,p\}$, $x\neq\rho(a_i)$. Par injectivité de ρ^{-1} (c'est une permutation donc une bijection), on a donc $\rho^{-1}(x)\neq\rho^{-1}\big(\rho(a_i)\big)=a_i$. Et donc $\rho^{-1}(x)$ n'appartenant pas au support du cycle σ, on a $\sigma\big(\rho^{-1}(x)\big)=\rho^{-1}(x)$. Puis $\rho\circ\sigma\circ\rho^{-1}(x)=\rho\big(\rho^{-1}(x)\big)=x$.

Et on reconnaît finalement que $\rho\circ\sigma\circ\rho^{-1}$ est le p-cycle $\big(\rho(a_1)\ \dots\ \rho(a_p)\big)$.

Exercice 12 (*Générateurs de S_n)**
Soit un entier $n\geq 2$. Montrer que le groupe symétrique S_n est engendré par :

1. les transpositions $\tau_{i,j} = (i\ j)$ avec $1\leq i<j\leq n$;
2. les transpositions $\tau_{i,i+1}$ avec $1\leq i\leq n-1$;
3. la paire $\{\tau_{1,2},\ (1\ 2\ \cdots\ n)\}$.
4. les transpositions $\tau_{1,k}$ avec $2\leq k\leq n$.

Corrigé de l'exercice 12

1. On sait d'après le cours (cf. MP2I) que toute permutation $\sigma\in S_n$ s'écrit comme produit commutatif de cycles de supports disjoints. Il suffit donc de montrer qu'un p-cycle quelconque $(a_1\ \cdots\ a_p)$ s'ecrit comme produit de transpositions. Cela résulte de la décomposition :

$$(a_1\ \cdots\ a_p) = (a_1\ a_2)\circ(a_2\ a_3)\circ\cdots\circ(a_{p-1}\ a_p) = \tau_{a_1,a_2}\circ\tau_{a_2,a_3}\circ\cdots\circ\tau_{a_{p-1},a_p}.$$

(vérifier l'image de chaque élément mais attention, ce produit est non commutatif !).
En définitive, toute permutation σ peut s'écrire comme produit de transpositions. En notant G le sous-groupe de S_n engendré par les transpositions, on a donc $S_n\subset G$, mais l'inclusion $G\subset S_n$ est automatique, donc $G=S_n$.

2. D'après la question précédente, il suffit de montrer que toute transposition $\tau_{i,j}$ s'écrit comme produit de transpositions du type $\tau_{i,i+1}$. Pour cela, on utilise le **principe de conjugaison** (vu dans un exercice précédent) : pour tout cycle $\sigma = (a_1 \ \cdots \ a_p)$ et pour toute permutation $\rho \in S_n$, la composée $\rho \circ \sigma \circ \rho^{-1}$ est le cycle $(\rho(a_1) \ \cdots \ \rho(a_p))$.
   Appliqué à des transpositions, ce principe donne

$$\tau \circ \tau_{i,i+1} \circ \tau^{-1} = \tau \circ \tau_{i,i+1} \circ \tau = (\tau(i) \ \ \tau(i+1)),$$

   donc en choisissant $\tau = \tau_{i+1,i+2}$, on obtient

$$\tau_{i+1,i+2} \circ \tau_{i,i+1} \circ \tau_{i+1,i+2} = \tau_{i,i+2}.$$

   En itérant ce procédé, on peut ainsi reconstruire toute transposition $\tau_{i,j}$: pour tout (i,j) tel que $1 \leq i < j \leq n$, on a :

$$\tau_{i,j} = \tau_{j-1,j} \circ \cdots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \cdots \circ \tau_{j-1,j},$$

   ce qui montre le résultat
3. Encore le même principe : en notant $\sigma = (1 \ 2 \ \cdots \ n)$, on a

$$\sigma \circ \tau_{1,2} \circ \sigma^{-1} = (\sigma(1) \ \ \sigma(2)) = (2 \ \ 3) = \tau_{2,3},$$

   et en itérant :

$$\forall k \in [\![0, n-2]\!], \quad \sigma^k \circ \tau_{1,2} \circ \sigma^{-k} = (k+1 \ \ k+2) = \tau_{k+1,k+2},$$

   ce qui permet d'engendrer les $n-1$ transpositions de la question précédente, suffisant ainsi à engendrer S_n.
4. Toujours par conjugaison : pour tout $1 < i < k \leq n$, on a

$$\tau_{1,i} \circ \tau_{1,k} \circ \tau_{1,i}^{-1} = \tau_{1,i} \circ \tau_{1,k} \circ \tau_{1,i} = (\tau_{1,i}(1) \ \ \tau_{1,i}(k)) = (i \ \ k) = \tau_{i,k},$$

   ce qui montre que les transpositions $(\tau_{1,k})_{2 \leq k \leq n}$ engendrent toutes les transpositions, et donc le groupe S_n en entier.

Exercice 13 (Générateurs de A_n)**
Soit $n \in \mathbb{N}^*$. On note A_n le *groupe alterné d'ordre n*, c'est-à-dire l'ensemble des permutations paires (de signature 1) de S_n.

1. Montrer que A_n est un sous-groupe de S_n. Quel est son cardinal ?
2. Montrer que pour $n \geq 3$, A_n est engendré par les 3-cycles.

Corrigé de l'exercice 13

1. La signature $\varepsilon : (S_n, \circ) \to (\{-1,1\}, \times)$ est un morphisme de groupes (surjectif lorsque $n \geq 2$), et $A_n = Ker(\varepsilon)$, donc A_n est un sous-groupe de S_n.
   Au niveau du cardinal :
   - Si $n = 1$, alors $A_1 = S_1 = \{Id\}$, donc $Card(A_1) = 1$.
   - Si $n \geq 2$, alors l'application

$$\theta_1 : \left\{ \begin{array}{ccc} A_n & \longrightarrow & S_n \setminus A_n \\ \sigma & \longmapsto & \sigma \circ \tau_{1,2} \end{array} \right.$$

     est une bijection d'inverse

$$\theta_2 : \left\{ \begin{array}{ccc} S_n \setminus A_n & \longrightarrow & A_n \\ \rho & \longmapsto & \rho \circ \tau_{1,2} \end{array} \right. ,$$

     (c'est facile à vérifier) donc $Card(A_n) = Card(S_n \setminus A_n)$.
     Or, $Card(A_n) + Card(S_n \setminus A_n) = Card(S_n) = n!$, donc $Card(A_n) = n!/2$.

2. Supposons $n \geq 3$. On sait que tout élément de A_n, donc toute permutation paire, se décompose en un produit d'un nombre pair de transpositions (puisque chacune de signature -1). Il suffit donc de montrer que tout produit de deux transpositions peut s'écrire comme un produit (éventuellement vide) de 3-cycles.
   - Si les deux transpositions sont identiques, il n'y a rien à faire puisque $\tau_{a,b} \circ \tau_{a,b} = Id$.
   - Si les deux transpositions ont un élément commun dans leurs supports :
   $$\tau_{a,c} \circ \tau_{a,b} = (a\ c) \circ (a\ b) = (a\ b\ c).$$
   - Si les deux transpositions ont des supports disjoints (ce qui peut se produire lorsque $n \geq 4$) :
   $$\tau_{a,b} \circ \tau_{c,d} = (a\ b) \circ (c\ d) = (a\ d\ c) \circ (a\ b\ c).$$

   Ceci montre bien que tout élément de A_n se décompose comme produit de 3-cycles (mais attention, les supports des cycles ne seront pas nécessairement disjoints !). En notant G le sous-groupe de S_n engendré par les 3-cycles, on a donc $A_n \subset G$. D'autre part, chaque 3-cycle est bien un élément de A_n donc on a aussi $G \subset A_n$ (**ne pas oublier de le vérifier ! A la différence de l'exercice précédent, on cherche à engendrer un sous-groupe de S_n, et non pas S_n tout entier, donc l'inclusion $G \subset A_n$ n'est pas automatique**). Finalement $G = A_n$.

Exercice 14 (*Orbite et stabilisateur)**
Soient $n \geq 2$ et G un sous-groupe de S_n. Pour tout $x \in \{1, \dots, n\}$, on note $\Omega(x) = \{\sigma(x),\ \sigma \in G\}$ (cet ensemble est appelé *l'orbite de x sous l'action de G*).

1. Démontrer : $\forall (x, y) \in \{1, \dots, n\}^2$, $\Omega(x) \cap \Omega(y) = \emptyset$ ou $\Omega(x) = \Omega(y)$.
2. Démontrer que l'ensemble $G_x = \{\sigma \in G,\ \sigma(x) = x\}$ est un sous-groupe de G.
   On l'appelle *stabilisateur de x*.
3. À l'aide de l'application $f : \begin{cases} G & \longrightarrow & \Omega(x) \\ \sigma & \longmapsto & \sigma(x) \end{cases}$, en déduire : $Card\ \Omega(x) = \dfrac{Card\ G}{Card\ G_x}$.
4. Soit G un sous-groupe de S_n de cardinal p^k, avec $k \geq 1$ et p un nombre premier ne divisant pas n. Montrer qu'il existe $x \in \{1, \dots, n\}$ tel que : $\forall \sigma \in G$, $\sigma(x) = x$.

Corrigé de l'exercice 14

1. On donne deux méthodes :
   - **"A la main"** : Soit $(x, y) \in \{1, \cdots, n\}^2$. Si $\Omega(x) \cap \Omega(y) \neq \emptyset$, alors il existe $z \in \Omega(x) \cap \Omega(y)$, donc il existe deux permutations σ, σ' dans G telles que $z = \sigma(x) = \sigma'(y)$.
   On a alors $\Omega(x) \subset \Omega(y)$ car si $t \in \Omega(x)$, alors il existe $\sigma'' \in G$ telle que
   $$t = \sigma''(x) = \sigma''(\sigma^{-1}(z)) = \sigma''(\sigma^{-1}(\sigma'(y))) = (\sigma'' \circ \sigma^{-1} \circ \sigma')(y),$$
   et comme G est un sous-groupe de S_n, on a $\sigma'' \circ \sigma^{-1} \circ \sigma' \in G$, et donc $t \in \Omega(y)$.
   Vu que x et y jouent des rôles symétriques, on a aussi $\Omega(y) \subset \Omega(x)$, donc $\Omega(x) = \Omega(y)$.
   - **En utilisant les relations d'équivalence** : la relation sur $\{1, \cdots, n\}$ définie par
   $$x \mathcal{R} y \iff \exists \sigma \in G,\ y = \sigma(x)$$
   est une relation d'équivalence (facile à vérifier). Pour tout $x \in \{1, \cdots, n\}$ la classe de x est :
   $$cl(x) = \{y \in \{1, \cdots, n\},\ \exists \sigma \in G,\ y = \sigma(x)\} = \Omega(x).$$
   On utilise alors le résultat général suivant : les classes d'une relation d'équivalence sur un ensemble X forment toujours une partition de X. Ici, on obtient donc que les $\Omega(x)$ forment une partition de $\{1, \cdots, n\}$, et en particulier, deux classes sont soit égales soit disjointes, ce qu'il fallait montrer.
2. Fixons $x \in \{1, \cdots, n\}$. L'ensemble $G_x = \{\sigma \in G,\ \sigma(x) = x\}$ est un sous-groupe de G car :
   - $Id \in G_x$ puisque $Id \in G$ et $Id(x) = x$;

- Si σ, σ' sont dans G_x, alors $\sigma^{-1} \circ \sigma'$ aussi car

$$(\sigma^{-1} \circ \sigma')(x) = \sigma^{-1}(\sigma'(x)) = \sigma^{-1}(x) = x,$$

puisque $\sigma(x) = \sigma'(x) = x$.

3. Considérons l'application $f : \left\{ \begin{array}{ccc} G & \longrightarrow & \Omega(x) \\ \sigma & \longmapsto & \sigma(x) \end{array} \right.$.
Cette application est surjective par définition de l'ensemble $\Omega(x)$. Donc pour tout $y \in \Omega(x)$, l'ensemble $f^{-1}(\{y\})$ est non vide, et on a :

$$G = \bigcup_{y \in \Omega(x)} f^{-1}(\{y\})$$

(cette réunion étant disjointe).
Vu que S_n est fini, G aussi et on a

$$Card(G) = \sum_{y \in \Omega(x)} Card\left(f^{-1}(\{y\})\right).$$

Or, chaque ensemble $f^{-1}(\{y\})$ est de même cardinal que G_x, car si on fixe $\sigma_0 \in f^{-1}(\{y\})$, l'application

$$\left\{ \begin{array}{ccc} G_x & \longrightarrow & f^{-1}(\{y\}) \\ \sigma & \longmapsto & \sigma_0 \circ \sigma \end{array} \right.$$

est une bijection d'inverse $\varphi \mapsto \sigma_0^{-1} \circ \varphi$, vu que :

$$\sigma \in G_x \iff \sigma(x) = x \iff (\sigma_0 \circ \sigma)(x) = \sigma_0(x) = y \iff \sigma_0 \circ \sigma \in f^{-1}(\{y\}).$$

Donc finalement :

$$Card(G) = \sum_{y \in \Omega(x)} Card(G_x) = Card(\Omega(x)) \times Card(G_x).$$

4. On veut montrer que sous les hypothèses, il existe $x \in \{1, \cdots, n\}$ tel que $G_x = G$.
D'après la question précédente, on a

$$\forall x \in \{1, \cdots, n\}, \qquad p^k = Card(\Omega(x)) \times Card(G_x),$$

donc $Card(\Omega(x))$ divise p^k, c'est-à-dire $Card(\Omega(x)) = 1$ ou p divise $Card(\Omega(x))$.
En outre, les classes $\Omega(x)$ partitionnent $\{1, \cdots, n\}$ (voir question 1.), donc en notant $\Omega(x_1), \cdots, \Omega(x_q)$ les classes distinctes, on a

$$n = \sum_{i=1}^{q} Card(\Omega(x_i)).$$

Si jamais aucun des $Card(\Omega(x_i))$ ne vaut 1, alors ils sont tous multiples de p, et donc par somme p divise n, ce qui est exclu par hypothèse. Donc il existe une classe $\Omega(x)$ de cardinal 1, ce qui entraîne :

$$Card(G) = Card(G_x),$$

et donc (puisque G_x est un sous-groupe de G), $G_x = G$, ce qui fallait montrer.

Remarque
Un exemple de cette situation avec $n = 4$ et $p = 3$.
Dans S_4, si on considère le sous-groupe

$$G = < (1\ 2\ 3) > = \{Id, (1\ 2\ 3), (1\ 3\ 2)\},$$

alors l'élément $x = 4$ est bien fixé par tous les éléments de G.

III Anneaux et corps

Exercice 15 (*Sous-corps de $\mathbb{Q}$)
Soit K un sous-corps de $\mathbb{Q}$.

1. Montrer qu'on a $\mathbb{Z} \subset K$.
2. En déduire qu'on a $K = \mathbb{Q}$. *Ainsi $\mathbb{Q}$ n'admet pas d'autre sous-corps que lui-même.*

Corrigé de l'exercice 15

1. En tant que sous-anneau de $\mathbb{Q}$, K contient 1, et il est stable par somme et opposé, donc par récurrence évidente, K contient tous les $n \in \mathbb{Z}$.
2. Pour tout $n \in \mathbb{N}^*$, $n \in K$ donc $1/n \in K$ puisque K est un sous-corps de $\mathbb{Q}$. Vu que K est également stable par produit on en déduit que pour tout $(m, n) \in \mathbb{Z} \times \mathbb{N}^*$, $m/n = m \times (1/n) \in K$, donc $\mathbb{Q} \subset K$. L'autre inclusion est vraie par hypothèse, donc $K = \mathbb{Q}$.

Exercice 16 (Injectivité d'un morphisme de corps)**
Montrer que tout morphisme de corps est injectif.

Corrigé de l'exercice 16
Soit $\varphi : K \to L$ un morphisme de corps. Si $x \neq 0_K$, alors x est inversible et

$$1_L = \varphi(1_K) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}),$$

donc $\varphi(x) \neq 0_L$ (puisque $0_L \neq 1_L$). Ceci montre que $Ker(\varphi) = \{0_K\}$ et donc φ est injectif.
Variante : Avec les mêmes notations, φ étant un morphisme d'anneaux, $Ker(\varphi)$ est un idéal du corps K. Si $Ker(\varphi)$ était non nul, alors il contiendrait un élément inversible x, donc par absorption, $Ker(\varphi)$ contiendrait $1_K = x^{-1}x$, ce qui est impossible car $\varphi(1_K) = 1_L$.

Remarque
Au passage, ce raisonnement montre qu'un corps K n'a que deux idéaux : $\{0_K\}$ et K (un idéal non nul contient alors 1_K, et donc par absorption, il est égal à tout le corps).

Exercice 17 (Anneau intègre fini)**

1. Soit A un anneau intègre et soit $a \neq 0$.
   On définit les applications $\gamma_a : A \to A$ et $\delta_a : A \to A$ par : $\forall x \in A,\ \gamma_a(x) = ax$ et $\delta_a(x) = xa$.
   Montrer que γ_a et δ_a sont injectives.
2. En déduire que dans un anneau intègre fini, tout élément non nul est inversible.
   Ainsi, si l'on suppose A de plus commutatif, on obtient le résultat suivant : tout anneau intègre fini et commutatif est un corps.
   *En fait on peut même prouver que tout anneau intègre fini est un corps, sans supposer la commutativité, mais cela fait appel à un résultat connu sous le nom de **théorème de Wedderburn**.*

Corrigé de l'exercice 17

1. Prouvons que, pour tout $a \in A \setminus \{0\}$, γ_a est injective :
   On fixe donc $a \in A \setminus \{0\}$.
   Soit $(x, y) \in A^2$ tel que $\gamma_a(x) = \gamma_a(y)$. On a donc $ax = ay$, d'où $a(y - x) = 0$. Par intégrité, on a donc $y - x = 0$ vu que $a \neq 0$. Et donc $x = y$.
   Ceci prouve l'injectivité de γ_a. On obtient celle de δ_a par le même procédé.
2. Supposons A de plus fini.
   Alors pour tout $a \neq 0$, $\gamma_a : A \to A$ est une injection entre deux ensembles de même cardinaux donc est une bijection ! En particulier 1 admet un unique antécédent par cette application, i.e. :

$$\exists! y \in A,\ \gamma_a(y) = ay = 1.$$

Ce raisonnement étant valable pour n'importe quel $a \neq 0$, on a ainsi démontré que tout élément non nul de A est inversible à droite.
Par le même argument, δ_a est bijective pour tout $a \neq 0$ et donc :

$$\exists! z \in A,\ \delta_a(z) = za = 1.$$

Tout élément non nul de A est donc aussi inversible à gauche.
Il faut faire attention : l'inverse à gauche est-il égal à l'inverse à droite ? C'est-à-dire, pour un $a \neq 0$ fixé, le y et le z obtenus coïncident-ils ?
La réponse est oui et on le démontre ainsi : si pour $a \neq 0$, on a trouvé $(y, z) \in A^2$ tel que $ay = 1$ et $za = 1$, alors :

$$y = 1y = (za)y = z(ay) = z1 = z.$$

Conclusion : tout élément non nul de A possède un inverse.
Ainsi, si l'on suppose de plus A commutatif, on obtient que A est un corps. On a par conséquent démontré que tout anneau commutatif intègre et fini est un corps.

Exercice 18 (Sous-corps classiques de $\mathbb{C}$)**

1. Soient K un sous-corps de $\mathbb{C}$ et $n \in \mathbb{N}$ tel que $\sqrt{n} \notin K$.
   On note $K[\sqrt{n}] = \left\{a + b\sqrt{n},\ (a, b) \in K^2\right\}$. Montrer que $K[\sqrt{n}]$ est un sous-corps de $\mathbb{C}$.
2. En déduire que $L = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ (a, b, c, d) \in \mathbb{Q}^4\right\}$, muni de l'addition et de la multiplication usuelles, est un corps.

Corrigé de l'exercice 18

1. Il est facile de voir que $1 = 1 + 0\sqrt{n} \in K[\sqrt{n}]$, et que $K[\sqrt{n}]$ est stable par différence et par produit, c'est donc un sous-anneau de $\mathbb{C}$. De plus, si $x = a + b\sqrt{n} \in K \setminus \{0\}$, alors l'inverse $1/x$ (qui existe dans le corps $\mathbb{C}$) est en fait dans $K[\sqrt{n}]$ puisque

$$\frac{1}{x} = \frac{a - b\sqrt{n}}{a^2 - nb^2} = \underbrace{\left(\frac{a}{a^2 - nb^2}\right)}_{\in K} + \underbrace{\left(\frac{-b}{a^2 - nb^2}\right)}_{\in K}\sqrt{n}.$$

   Donc $K[\sqrt{n}]$ est un sous-corps de $\mathbb{C}$.
2. Par la question précédente, $\mathbb{K}_1 = \mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{C}$ car $\sqrt{2} \notin \mathbb{Q}$.
   En itérant ce raisonnement, on obtient que $\mathbb{K}_2 = \mathbb{K}_1[\sqrt{3}]$ est aussi un sous-corps de $\mathbb{C}$ car $\sqrt{3} \notin \mathbb{K}_1$: sinon, on aurait $\sqrt{3} = a + b\sqrt{2}$ avec $(a, b) \in \mathbb{Q}^2$, et donc $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, ce qui oblige $ab = 0$ (sinon $\sqrt{2} \in \mathbb{Q}$, absurde), et donc $3 = a^2$ ou $3 = 2b^2$, ce qui est impossible dans les deux cas (écrire a et b comme fractions irréductibles, passer dans $\mathbb{Z}$ et raisonner avec les valuations 2-adiques et 3-adiques, classiquement).
   Or, $\mathbb{K}_2 = \{x + y\sqrt{3},\ (x, y) \in \mathbb{K}_1^2\} = \{a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3},\ (a, b, c, d) \in \mathbb{Q}^4\} = L$, ce qui montre que L est un sous-corps de $\mathbb{C}$, et donc un corps.

Exercice 19 (Sous-anneaux de $\mathbb{Z}^2$)**
Pour $d \in \mathbb{N}$, on note $A_d = \{(x, y) \in \mathbb{Z}^2,\ y \equiv x\ [d]\}$.

1. Montrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de $\mathbb{Z}^2$.
2. (a) Réciproquement, soit A un sous-anneau de $\mathbb{Z}^2$.
   Démontrer que $H = \{x \in \mathbb{Z},\ (x, 0) \in A\}$ est un sous-groupe de $\mathbb{Z}$.
   (b) En déduire qu'il existe $d \in \mathbb{N}$ tel que $A = A_d$.

Corrigé de l'exercice 19

1. Soit $d \in \mathbb{N}$. Rappelons que $(0, 0)$ est l'élément nul de l'anneau produit $\mathbb{Z}^2$ et que $(1, 1)$ est son élément unité. Comme $1 \equiv 1\ [d]$, on a $(1, 1) \in A_d$.
   Soient (x, y) et (x', y') dans A_d. On a donc $y \equiv x\ [d]$ et $y' \equiv x'\ [d]$. Or $(x, y) - (x', y') = (x - x', y - y')$, où $(y - y') - (x - x') = (y - x) - (y' - x')$ est divisible par d donc $y - y' \equiv x - x'\ [d]$

et donc $(x,y)-(x',y') \in A_d$.
$(x,y)\times(x',y') = (xx',yy')$ et on sait que $y \equiv x\ [d]$ et $y' \equiv x'\ [d]$ impliquent $yy' \equiv xx'\ [d]$ donc $(xx',yy') \in A_d$.
On a ainsi prouvé que A_d est un sous-anneau de $\mathbb{Z}^2$.

2. (a) Soit A un sous-anneau de $\mathbb{Z}^2$.
On a $(0,0) \in A$ donc $0 \in H$.
Soit $(x,y) \in H^2$. On a donc $(x,0) \in A$ et $(y,0) \in A$. On en déduit $(x,0)-(y,0) \in A$, c'est-à-dire $(x-y,0) \in A$ et donc $x-y \in H$.
On a donc prouvé que H est un sous-groupe de $\mathbb{Z}$.

   (b) H est un sous-groupe de $\mathbb{Z}$ donc il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$. Ce d est notre candidat, on veut montrer que $A = A_d$.
   — Soit $(x,y) \in A_d$. Il existe $k \in \mathbb{Z}$ tel que $y = x + kd$. Ainsi $(x,y) = (y,y) + (kd,0) = y(1,1) + k(d,0)$ avec $(d,0) \in A$ car $d \in H$, et bien sûr $(1,1) \in A$, d'où $(x,y) \in A$. Ainsi $A_d \subset A$.
   — Soit $(x,y) \in A$. Par division euclidienne, il existe r et r' dans $\{0,\dots,d-1\}$ tels que $x = kd + r$ et $y = k'd + r'$.
   Comme $A_d \subset A$, on a $(kd,k'd) \in A$ donc $(x,y)-(kd,k'd) \in A$, c'est-à-dire $(r,r') \in A$. Puis $(r,r')-r'(1,1) = (r-r',0) \in A$ donc $r-r' \in H$ puis d divise $r-r'$. Or $-d < r-r' < d$ donc cela implique $r-r' = 0$ donc $r = r'$. Ainsi $y-x = (k'-k)d$ donc $y \equiv x\ [d]$ et on a prouvé que $(x,y) \in A_d$.
   Ainsi $A \subset A_d$.
   Et donc $A = A_d$.

IV Idéaux

Exercice 20 (Eléments nilpotents)**
Soit $(A,+,\times)$ un anneau commutatif.
On dit d'un élément a de A qu'il est **nilpotent** lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.
Montrer que l'ensemble des éléments nilpotents de A est un idéal de A.

Corrigé de l'exercice 20
Notons I l'ensemble des éléments nilpotents de A.
Tout d'abord, $0_A \in I$ car $0_A^1 = 0_A$.
Ensuite, I vérifie la propriété d'absorption car pour tout $x \in I$ et $a \in A$, il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$, et donc $(ax)^n = a^n x^n$ (par commutativité de A), ce qui amène $(ax)^n = 0_A$, et donc $ax \in I$.
Enfin, I est stable par somme car pour tout $(x,y) \in I^2$, il existe $(n_1,n_2) \in (\mathbb{N}^*)^2$ tel que $x^{n_1} = y^{n_2} = 0_A$, donc puisque $xy = yx$:

$$(x+y)^{n_1+n_2} = \sum_{k=0}^{n_1-1} \binom{n_1+n_2}{k} x^k y^{n_1+n_2-k} + \sum_{k=n_1}^{n_1+n_2} \binom{n_1+n_2}{k} x^k y^{n_1+n_2-k},$$

et cette somme est nulle, car dans la première somme $n_1+n_2-k \geq n_2$ donc $y^{n_1+n_2-k} = 0_A$, et dans la seconde $k \geq n_1$ donc $x^k = 0_A$. Finalement, I est bien un idéal de A.

Exercice 21 (Idéal de fonctions)**
Soit $A = \mathbb{R}^{\mathbb{R}}$ l'anneau des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, muni des lois $+$ et $\times$ usuelles.
Pour $x \in \mathbb{R}$, on note $I_x = \{f \in A,\ f(x) = 0\}$.

1. Montrer que, pour tout $x \in \mathbb{R}$, I_x est un idéal de A.
2. Montrer que, si x_1 et x_2 sont deux éléments distincts de $\mathbb{R}$, alors $I_{x_1} + I_{x_2} = A$.

Corrigé de l'exercice 21

1. Très simple : la fonction nulle est clairement dans I_x, I_x est stable par somme, et si $f \in I_x$ et $g \in A$, la fonction produit fg est dans I_x (en effet $f(x) = 0$ donc $(fg)(x) = 0$).

Variante : I_x est le noyau du morphisme d'anneaux $\varphi_x : \left\{ \begin{array}{ccc} A & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(x) \end{array} \right.$ donc c'est un idéal de A.

2. Soit $x_1 \neq x_2$ dans $\mathbb{R}$.
L'inclusion $I_{x_1} + I_{x_2} \subset A$ est immédiate, puisque I_{x_1} et I_{x_2} sont deux idéaux de A.
Réciproquement, étant donnée $f \in A$ (fonction $\mathbb{R} \to \mathbb{R}$), on peut écrire f comme la somme d'une fonction nulle en x_1 et d'une fonction nulle en x_2 via l'écriture :

$$\forall x \in \mathbb{R}, \qquad f(x) = \frac{(x - x_1)f(x)}{x_2 - x_1} + \frac{(x_2 - x)f(x)}{x_2 - x_1}.$$

D'où l'inclusion $A \subset I_{x_1} + I_{x_2}$,

Exercice 22 (Produit de deux idéaux)**
Soit A un anneau commutatif et I et J deux idéaux de A.

1. On note $IJ = \left\{ \sum_{k=1}^{n} a_k b_k,\ n \in \mathbb{N}^* \text{ et } \forall k \in \mathbb{N},\ a_k \in I \text{ et } b_k \in J \right\}$.
Montrer que IJ est un idéal de A (dit autrement, c'est l'idéal engendré par les produits d'éléments de I et de J).
2. On suppose qu'on a $I + J = A$. Montrer que $IJ = I \cap J$.
3. Soit $(m, n) \in \mathbb{N}^2$. On se place dans $A = \mathbb{Z}$ avec $I = m\mathbb{Z}$ et $J = n\mathbb{Z}$. Déterminer IJ.

Corrigé de l'exercice 22

1. Tout d'abord $0_A = 0_A \times 0_A$ et 0_A est à la fois dans I et J, donc $0_A \in IJ$.
Ensuite, si $x = \sum_{k=1}^{n} a_k b_k$ et $y = \sum_{k=1}^{m} a'_k b'_k$ avec les a_k, a'_k dans I et les b_k, b'_k dans J, alors

$$x + y = \sum_{k=1}^{m+n} a''_k b''_k,$$

avec $a''_k = \left\{ \begin{array}{l} a_k \text{ si } k \leq n \\ a'_{k-n} \text{ si } k > n \end{array} \right. \in I$ et $b''_k = \left\{ \begin{array}{l} b_k \text{ si } k \leq n \\ b'_{k-n} \text{ si } k > n \end{array} \right. \in J$, ce qui montre que $x + y \in IJ$.
Enfin, si $x = \sum_{k=1}^{n} a_k b_k$ avec les a_k dans I, les b_k dans J et si $a \in A$, alors

$$xa = \sum_{k=1}^{n} \underbrace{a_k}_{\in I} \underbrace{(b_k a)}_{\in J},$$

donc $xa \in IJ$.

2. L'inclusion $IJ \subset I \cap J$ est toujours vraie car si $x = \sum_{k=1}^{n} a_k b_k \in IJ$, alors par absorption, chaque terme $a_k b_k$ est dans I (puisque a_k est dans I), donc la somme x est dans I (puisque I est stable par somme). Idem pour J, donc $x \in I \cap J$.
Réciproquement, soit $x \in I \cap J$. L'hypothèse $I + J = A$ permet de décomposer notamment le neutre 1 sous la forme

$$1 = i + j, \qquad (i, j) \in I \times J$$

(sorte de "relation de Bézout"). Donc

$$x = x(i + j) = xi + xj = ix + xj,$$

avec $(i, x) \in I \times J$ et $(x, j) \in I \times J$, donc $x \in IJ$.

3. Dans cet exemple, si $x \in IJ = (m\mathbb{Z})(n\mathbb{Z})$, alors x s'écrit comme une somme de produits $a_k b_k$, avec $m | a_k$ et $n | b_k$. Donc $mn | a_k b_k$ pour tout k, et par somme $mn | x$.
Ceci montre que $(m\mathbb{Z})(n\mathbb{Z}) \subset (mn\mathbb{Z})$.
Réciproquement, si $x \in mn\mathbb{Z}$, alors $x = (mn)u = m(nu)$ avec $u \in \mathbb{Z}$, donc $x \in (m\mathbb{Z})(n\mathbb{Z})$.
Finalement on a $(m\mathbb{Z})(n\mathbb{Z}) = (mn\mathbb{Z})$.

Exercice 23 (Idéaux maximaux)**
Soit A un anneau. Un idéal I de A est dit maximal lorsqu'il est distinct de A et que les deux seuls idéaux de A contenant I sont I et A.

1. Déterminer les idéaux maximaux de $\mathbb{Z}$.
2. Montrer que $I = \{f \in C(\mathbb{R}, \mathbb{R}),\ f(0) = 0\}$ est un idéal maximal de $C(\mathbb{R}, \mathbb{R})$.

Corrigé de l'exercice 23

1. On sait que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$. Ainsi un idéal $I = n\mathbb{Z}$ de $\mathbb{Z}$ est non maximal ssi il existe $m \in \mathbb{Z} \setminus \{1, n\}$ tel que $n\mathbb{Z} \subset m\mathbb{Z}$. Comme $n\mathbb{Z} \subset m\mathbb{Z} \iff m \mid n$, $n\mathbb{Z}$ est non maximal ssi n possède un diviseur m non trivial (i.e. différent de 1 et n) ssi n est non premier.
   Ainsi les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.
2. On veut montrer que $I = \{f \in C(\mathbb{R}, \mathbb{R}),\ f(0) = 0\}$ est un idéal maximal de $C(\mathbb{R}, \mathbb{R})$.
   Soit J un idéal de $C(\mathbb{R}, \mathbb{R})$ contenant strictement I. Il existe donc $f \in J$ tel que $f(0) \neq 0$. Notons g la fonction constante égale à $f(0)$ et $h = f - g$. On a $h(0) = f(0) - f(0) = 0$ donc $h \in I$ puis $h \in J$ et ainsi $g = f - h \in J$ car J, en tant qu'idéal, est un sous-groupe additif de $C(\mathbb{R}, \mathbb{R})$.
   Comme on a $f(0) \neq 0$, on peut aussi définir la fonction c constante égale à $\frac{1}{f(0)}$. Comme J est un idéal, on a $cg \in J$. Or cg est la fonction constante égale à 1, c'est-à-dire que $cg = 1_{C(\mathbb{R},\mathbb{R})}$, d'où $J = C(\mathbb{R}, \mathbb{R})$ (un idéal qui contient 1_A est automatiquement égal à A par absorption).
   On a ainsi prouvé que I est maximal.

Exercice 24 (Suite croissante d'idéaux)**
Soit A un anneau commutatif intègre et $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A.
On pose $I = \bigcup_{n\in\mathbb{N}} I_n$.

1. Montrer que I est un idéal de A.
2. Montrer que si A est principal (c'est-à-dire que tout idéal de A est monogène), alors la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire.

Corrigé de l'exercice 24

1. — On a I_0 qui est un idéal donc $0_A \in I_0$. Ainsi $0_A \in I$.
   — Soit $(x, y) \in I^2$. Il existe $m \in \mathbb{N}$ tel que $x \in I_m$ et il existe $n \in \mathbb{N}$ tel que $y \in I_n$. Supposons par exemple $m \geq n$. Alors, comme on a $I_n \subset I_m$, on a $y \in I_m$ aussi. Vu que I_m est un sous-groupe additif de A, on en déduit $x - y \in I_m$ donc $x - y \in I$.
   On a ainsi prouvé que I est un sous-groupe additif de A.
   — Soit aussi $a \in A$. Comme I_m est un idéal de A, on a $ax \in I_m$ donc $ax \in I$.
   Ainsi I est un idéal de A.
2. Comme A est supposé principal, on en déduit qu'il existe $\alpha \in A$ tel que $I = \alpha A$. Mais alors $\alpha \in I$ donc il existe $N \in \mathbb{N}$ tel que $\alpha \in I_N$. Il s'ensuit facilement $I = I_N$. Et donc la suite $(I_n)_{n\in\mathbb{N}}$ stationne à partir du rang N.

V Révisions d'arithmétique

Exercice 25 (*Triplets pythagoriciens)
Soient 3 entiers non nuls a, b et c tels que $a^2 + b^2 = c^2$.

1. Montrer que a et b ne peuvent pas être tous deux impairs.
2. Si c est pair, que dire de a et b ? Illustrer ce cas par un exemple.

Corrigé de l'exercice 25

1. On obtient facilement que si a est pair, alors $a^2 \equiv 0$ [4] et si a est impair, alors $a^2 \equiv 1$ [4].
   Si a et b sont impairs, on a donc $c^2 \equiv a^2 + b^2 \equiv 2$ [4], ce qui est impossible (quel que soit la parité de c). Donc a ou b est pair.

2. Si a est pair et b impair, ou l'inverse, on a alors $c^2 \equiv a^2 + b^2 \equiv 1$ [4], ce qui contredit la parité de c. Donc a et b sont pairs.
   Exemple numérique : $(a, b, c) = (6, 8, 10)$.

Exercice 26 (Critère de divisibilité par 11)**

1. Pour $k \in \mathbb{N}$, déterminer le reste de la division euclidienne de 10^k par 11.
2. En déduire le critère de divisibilité par 11 d'un entier.

Corrigé de l'exercice 26

1. Puisque $10 \equiv -1$ [11], on a pour tout $k \in \mathbb{N}$, $10^k \equiv (-1)^k$ [11], donc le reste de la division euclidienne de 10^k par 11 est 1 si k est pair, -1 si k est impair.
2. Notons $x = \pm \sum_{k=0}^{n} a_k 10^k$ l'écriture décimale de $x \in \mathbb{Z}$, avec $n \in \mathbb{N}$ et les $a_k \in \{0, \cdots, 9\}$.
   Alors $x \equiv \pm \sum_{k=0}^{n} (-1)^k a_k$, donc x est multiple de 11 ssi la somme alternée de ses chiffres donne un multiple de 11.

Exercice 27 (Carré parfait)**
Montrer, sans utiliser la calculatrice, que 1842377 n'est pas un carré parfait.

Corrigé de l'exercice 27
Posons $n = 1842377$ et supposons qu'il existe $k \in \mathbb{Z}$ tel que $n = k^2$. Pour exhiber une contradiction, il suffit d'étudier le chiffre des unités de n, en regardant ce qui se passe modulo 10 : on a $k^2 \equiv 7$ [10], et on voit que ceci est impossible en passant en revue tous les cas :

$k \equiv ?$ [10]	0	± 1	± 2	± 3	± 4	5
$k^2 \equiv ?$ [10]	0	1	4	9	6	5

Exercice 28 (PGCD, PPCM)**
On rappelle que $a \wedge b$ désigne le PGCD de a et b, et $a \vee b$ le PPCM de a et b.

1. Montrer que $(a + b) \wedge (a \vee b) = a \wedge b$ pour tout $(a, b) \in (\mathbb{N}^*)^2$.
2. Déterminer les $(a, b) \in \mathbb{N}^2$ tels que $\begin{cases} a + b = 144 \\ a \vee b = 420 \end{cases}$.

Corrigé de l'exercice 28
Notons $d = a \wedge b = pgcd(a, b)$ et $m = a \vee b = ppcm(a, b)$.

1. Montrons que $(a + b) \wedge m = d$.
   L'idée est de factoriser $a + b$ et m par d : en notant $a' = d/a$ et $b' = d/b$, on a $a' \wedge b' = 1$, et

$$m = \frac{ab}{d} = (a'b')d, \qquad a + b = (a' + b')d.$$

   Or, $a' + b'$ et $a'b'$ sont premiers entre eux. On peut le voir de deux manières :

   - soit avec Bézout : par hypothèse, il existe $(u, v) \in \mathbb{Z}^2$ tels que $a'u + b'v = 1$ donc

$$1 = (a'u + b'v)^2 = (a' + b')(a'u^2 + b'v^2) - a'b'(u^2 + v^2) + 2a'b'uv$$
$$= (a' + b')(a'u^2 + b'v^2) - a'b'(u - v)^2,$$

     ce qui montre le résultat ;
   - soit en considérant un diviseur premier de $a' + b'$ et $a'b'$, noté p. Puisque p divise $a'b'$, on obtient par le lemme de Gauss que p divise a' ou p divise b' (car si p ne divise par a', alors $p \wedge a' = 1$ donc p divise b'). Mais p divise aussi $a' + b'$, donc facilement, on obtient que p divise a' et b', ce qui est impossible car a' et b' sont premiers entre eux. Il n'existe donc pas de diviseur premier commun à $a' + b'$ et $a'b'$: ils sont donc premiers entre eux.

On en déduit :

$$(a+b)\wedge m = (a'+b')d \ \wedge \ (a'b')d = d((a'+b')\wedge a'b') = d.$$

2. Résolvons maintenant le système proposé : si $a+b=144$ et $m=420$, alors $d=(a+b)\wedge m = 144\wedge 420 = 12$. Il s'ensuit :
$$ab = dm = 12\times 420 = 5040,$$
donc on connaît la somme et le produit de a et b. Les entiers a et b sont donc les solutions de :
$$(x-a)(x-b)=0 \iff x^2-(a+b)x+ab=0 \iff x^2-144x+5040=0.$$
On en déduit $(a,b)=(84,60)$ ou $(a,b)=(60,84)$, et on vérifie facilement que ces deux couples sont bien solutions.

Exercice 29 (Nombres de Mersenne)**
Soient a et p deux entiers strictement supérieurs à 1. Montrer que si a^p-1 est un nombre premier, alors $a=2$ et p est premier.

Corrigé de l'exercice 29
La clef est la factorisation suivante :

$$a^p-1 = (a-1)(a^{p-1}+\cdots+a+1).$$

Tous les facteurs sont dans $\mathbb{N}$, donc puisque a^p-1 est supposé premier, on en déduit que $a-1=1$ ou $a^{p-1}+\cdots+a+1=1$. Mais $p\geq 2$ et $a\geq 2$ donc $a^{p-1}+\cdots+a+1\geq 1+a>1$. D'où $a=2$.
Ensuite, décomposons $p=p_1p_2$ avec p_1,p_2 dans $\mathbb{N}^*$. On a alors

$$2^p-1 = (2^{p_1})^{p_2}-1.$$

Si $p_2>1$, alors en appliquant ce qui précède à $a=2^{p_1}>1$, on obtient que $2^{p_1}=2$, donc $p_1=1$. Ceci montre que les seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p, donc p est un nombre premier.

Remarque
Les $(2^p-1)_{p\in\mathcal{P}}$ s'appellent les nombres de Mersenne. Mais ils ne sont pas tous premiers, par ex : $2^{11}-1=2047=23\times 89$ n'est pas premier.

Exercice 30 (*Carré parfait 2)**
Soient a, b et c des entiers strictement positifs et premiers entre eux dans leur ensemble tels que : $\frac{1}{a}+\frac{1}{b}=\frac{1}{c}$. Démontrer que $a+b$ est un carré parfait.

Corrigé de l'exercice 30
Considérons un diviseur premier de $a+b$, noté p (il en existe car $a+b\geq 1+1=2$). Par hypothèse :

$$ab = c(a+b),$$

donc p divise ab. Par le lemme d'Euclide (qui vient du lemme de Gauss), on en déduit que p divise a ou p divise b. Mais p divise $a+b$, donc p divise a et p divise b.
Notons $\alpha\geq 1$ et $\beta\geq 1$ les valuations p-adiques respectives de a et b. On peut alors écrire :

$$a=p^\alpha a', \qquad b=p^\beta b',$$

où $a'\wedge p = b'\wedge p = 1$.
Montrons alors que $\alpha=\beta$:

- si on avait $\alpha<\beta$, alors en remplaçant dans l'égalité $ab=c(a+b)$, on obtiendrait :
$$p^{\alpha+\beta}a'b' = cp^\alpha(a'+p^{\beta-\alpha}b'),$$
c'est-à-dire
$$ca' = p^\beta a'b' - cp^{\beta-\alpha}b'.$$
Donc p divise ca', mais p est premier avec a', donc par le lemme de Gauss, p divise c, ce qui est impossible puisque p divise déjà a et b, et a,b,c sont premiers entre eux par hypothèse.

- de même si $\beta < \alpha$.

Donc $\alpha = \beta$. Finalement, $c(a+b) = ab = p^{2\alpha}a'b'$, donc en notant $\gamma \geq 1$ la valuation p-adique de $a+b$, on a

$$cp^{\gamma}u = p^{2\alpha}a'b',$$

avec p qui ne divise ni c, ni u, ni a', ni b'. Par unicité de la valuation p-adique, on en déduit que $\gamma = 2\alpha$.
Ainsi, tous les diviseurs premiers de $a+b$ ont une valuation paire, ce qui prouve que $a+b$ est un carré parfait.

Exercice 31 (Nombres premiers congrus à 3 modulo 4)**
En s'inspirant de la preuve de l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Corrigé de l'exercice 31
Notons $\mathcal{P}_3$ l'ensemble des nombres premiers congrus à 3 modulo 4. Ils sont tous impairs.
Si on suppose $\mathcal{P}_3$ fini, on peut considérer l'entier

$$N = 4\left(\prod_{p\in\mathcal{P}_3} p\right) - 1.$$

N est impair et strictement supérieur à 1, donc N possède des diviseurs premiers, tous impairs.
Ces diviseurs premiers ne sont pas tous congrus à 1 modulo 4, sinon on aurait $N \equiv 1$ [4], ce qui est faux car $N \equiv 3$ [4]. Il existe donc $p_0 \in \mathcal{P}_3$ qui divise N.
Ceci entraîne que p_0 divise $4\left(\prod_{p\in\mathcal{P}_3} p\right) - N = 1$, ce qui est impossible. L'ensemble $\mathcal{P}_3$ est donc infini.

VI Anneaux $\mathbb{Z}/n\mathbb{Z}$ et arithmétique

Exercice 32 (*Calculs d'inverses modulo n)
Déterminer, selon s'il existe ou pas, l'inverse de :

- 6 modulo 17.
- 12 modulo 30.
- 11 modulo 25.

Corrigé de l'exercice 32

- 6 est premier avec 17, donc $\overline{6}$ est inversible dans $\mathbb{Z}/17\mathbb{Z}$.
  Puisque $\overline{6} \times \overline{3} = \overline{18} = \overline{1}$, on a $\overline{6}^{-1} = \overline{3}$ dans $\mathbb{Z}/17\mathbb{Z}$.
- 12 n'est pas premier avec 30 (leur pgcd vaut 6), donc $\overline{12}$ n'est pas inversible dans $\mathbb{Z}/30\mathbb{Z}$.
- 11 est premier avec 25, donc $\overline{11}$ est inversible dans $\mathbb{Z}/25\mathbb{Z}$.
  Pour trouver l'inverse, on cherche une identité de Bézout entre 11 et 25 en remontant l'algorithme d'Euclide :

$$25 = 11 \times 2 + 3$$

$$11 = 3 \times 3 + 2$$

$$3 = 2 \times 1 + 1,$$

  d'où :

$$1 = 3 - 2 \times 1$$

$$1 = 3 - (11 - 3 \times 3) \times 1 = -11 + 3 \times 4,$$

$$1 = -11 + (25 - 11 \times 2) \times 4 = 11 \times (-9) + 25 \times 4.$$

  En prenant la congruence modulo 25, on obtient $\overline{11} \times \overline{-9} = \overline{1}$ dans $\mathbb{Z}/25\mathbb{Z}$, donc $\overline{11}^{-1} = \overline{-9} = \overline{16}$.

Exercice 33 (*Equations linéaires modulo n)

1. Résoudre l'équation $9x \equiv 3\ [16]$.
2. Résoudre l'équation $10x \equiv 4\ [78]$.

Corrigé de l'exercice 33

1. Dans $\mathbb{Z}/16\mathbb{Z}$, cette équation se réécrit $\overline{9}\overline{x} = \overline{3}$.
   Puisque 9 est premier avec 16, $\overline{9} \in (\mathbb{Z}/16\mathbb{Z})^\times$ et $\overline{9}^2 = \overline{81} = \overline{1}$, donc
   $$9x \equiv 3\ [16] \iff \overline{9}\overline{x} = \overline{3} \iff \overline{x} = \overline{9} \times \overline{3} = \overline{27} = \overline{11} \iff x \equiv 11\ [16].$$
2. En divisant par 2 les congruences, on a :
   $$10x \equiv 4\ [78] \iff 5x \equiv 2\ [39]$$
   Puisque 5 est premier avec 39, $\overline{5} \in (\mathbb{Z}/39\mathbb{Z})^\times$ et $\overline{8} \times \overline{5} = \overline{1}$, donc
   $$10x \equiv 4\ [78] \iff \overline{5}\overline{x} = \overline{2} \iff \overline{x} = \overline{8} \times \overline{2} = \overline{16} \iff x \equiv 16\ [39].$$

Exercice 34 (*Système dans $\mathbb{Z}/n\mathbb{Z}$)

Résoudre dans $\mathbb{Z}/37\mathbb{Z}$ le système $\begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases}$.

Corrigé de l'exercice 34

37 étant premier, $\mathbb{Z}/37\mathbb{Z}$ est un corps, ce qui va faciliter la résolution du système, puisque tout élément non nul est inversible. Déjà on a (en additionnant les deux équations, ce qui est une opération aisément réversible) :
$$\begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases} \iff \begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{9}x = \overline{20} \end{cases}.$$
Pour résoudre la seconde équation, déterminons l'inverse de $\overline{9}$: puisque $\overline{9} \times \overline{-4} = \overline{-36} = \overline{1}$, on a $\overline{9}^{-1} = \overline{-4}$, donc
$$\overline{9}x = \overline{20} \iff x = \overline{-4} \times \overline{20} = -\overline{80} = -\overline{6}.$$
Finalement
$$\begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases} \iff \begin{cases} x = -\overline{6} \\ \overline{6}x + \overline{7}y = \overline{20} \end{cases} \iff \begin{cases} x = -\overline{6} \\ -\overline{36} + \overline{7}y = \overline{20} \end{cases} \iff \begin{cases} x = -\overline{6} \\ \overline{7}y = \overline{19} \end{cases}.$$
Reste à trouver l'inverse de $\overline{7}$: grâce à l'algorithme d'Euclide, on obtient l'identité de Bézout :
$$7 \times 16 + 37 \times (-3) = 1,$$
ce qui montre que $\overline{7}^{-1} = \overline{16}$. Donc finalement :
$$\begin{cases} \overline{6}x + \overline{7}y = \overline{20} \\ \overline{3}x - \overline{7}y = \overline{0} \end{cases} \iff \begin{cases} x = -\overline{6} \\ y = \overline{16} \times \overline{19} = \overline{8} \times \overline{38} = \overline{8} \end{cases}.$$
Le système linéaire proposé admet donc une unique solution dans $\mathbb{Z}/37\mathbb{Z}$: le couple $(\overline{-6}, \overline{8})$.

Exercice 35 (Exemple d'un groupe d'inversibles)**

Déterminer le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ et trouver un groupe additif qui lui soit isomorphe.
Indication : une fois calculé le cardinal de $(\mathbb{Z}/8\mathbb{Z})^\times$, on cherchera parmi les groupes additifs connus celui ou ceux de même cardinal. On aura ainsi les groupes candidats.

Corrigé de l'exercice 35

Les inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont les $\overline{k}$ avec $0 \leq k < 8$ et $k \wedge 8 = 1$. Donc $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Dans ce groupe multiplicatif de cardinal 4, les trois éléments non neutres sont d'ordre 2 (facile à vérifier). Donc $((\mathbb{Z}/8\mathbb{Z})^\times, \times)$ ne peut être isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ qui est cyclique. Examinons plutôt le groupe connu

$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$: lui aussi possède trois éléments d'ordre 2 (en plus du neutre). Il suffit alors de faire correspondre les neutres et les éléments d'ordre 2 pour obtenir un isomorphisme explicite entre ces deux groupes. Par exemple :

$$\theta : \left\{ \begin{array}{ccc} (\mathbb{Z}/8\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ x & \longmapsto & \theta(x) = \left\{ \begin{array}{l} (\dot{0},\dot{0}) \text{ si } x = \overline{1} \\ (\dot{0},\dot{1}) \text{ si } x = \overline{3} \\ (\dot{1},\dot{0}) \text{ si } x = \overline{5} \\ (\dot{1},\dot{1}) \text{ si } x = \overline{7} \end{array} \right. \end{array} \right.$$

On a bien $\theta(xy) = \theta(x) + \theta(y)$ pour tous les éléments x, y (vérifier rapidement) et θ est clairement bijective.

Exercice 36 (Equation du second degré dans $\mathbb{Z}/n\mathbb{Z}$)**
Résoudre l'équation $x^2 + \overline{2}x - \overline{3} = \overline{0}$ dans $\mathbb{Z}/7\mathbb{Z}$ et dans $\mathbb{Z}/91\mathbb{Z}$.

Corrigé de l'exercice 36
Déjà, remarquons la factorisation :

$$x^2 + \overline{2}x - \overline{3} = (x - \overline{1})(x + \overline{3}),$$

valable dans tout anneau $\mathbb{Z}/n\mathbb{Z}$.

- **Résolution dans $\mathbb{Z}/7\mathbb{Z}$** : vu que 7 est premier, $\mathbb{Z}/7\mathbb{Z}$ est un corps, donc *a fortiori* un anneau intègre. D'où :

  $$x^2 + \overline{2}x - \overline{3} = \overline{0} \iff (x - \overline{1})(x + \overline{3}) = \overline{0} \iff x \in \{\overline{1}, -\overline{3}\}.$$

  Il y a donc deux solutions dans $\mathbb{Z}/7\mathbb{Z}$: $\overline{1}$ et $\overline{4}$.
- **Résolution dans $\mathbb{Z}/91\mathbb{Z}$** : on ne peut pas procéder de manière identique car $\mathbb{Z}/91\mathbb{Z}$ n'est pas un anneau intègre ($\overline{7} \times \overline{13} = \overline{0}$ alors que $\overline{7}$ et $\overline{13}$ sont non nuls). Vu que $91 = 7 \times 13$ et $7 \wedge 13 = 1$, on a un isomorphisme d'anneaux donné par le théorème chinois :

  $$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}/91\mathbb{Z} & \longrightarrow & \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}, \hat{x}) \end{array} \right. .$$

  On en déduit les équivalences :

  $$x^2 + \overline{2}x - \overline{3} = \overline{0} \iff \overline{x^2 - 2x - 3} = \overline{0} \iff \left\{ \begin{array}{l} x^2 + \dot{2}x - \dot{3} = \dot{0} \\ x^2 + \hat{2}x - \hat{3} = \hat{0} \end{array} \right. \iff \left\{ \begin{array}{l} \dot{x} \in \{\dot{1}, \dot{-3}\} \\ \hat{x} \in \{\hat{1}, \hat{-3}\} \end{array} \right. ,$$

  (la résolution dans $\mathbb{Z}/13\mathbb{Z}$ se fait comme dans $\mathbb{Z}/7\mathbb{Z}$, puisqu'on a aussi un corps), c'est-à-dire

  $$x^2 + \overline{2}x - \overline{3} = \overline{0} \iff \psi(\overline{x}) \in \{(\dot{1},\hat{1}), (\dot{1},\hat{-3}), (\dot{-3},\hat{1}), (\dot{-3},\hat{-3})\}.$$

  Reste à calculer les antécédents par ψ des quatres couples : pour $(\dot{1},\hat{1})$ et $(\dot{-3},\hat{-3})$, c'est facile puisque

  $$(\dot{1},\hat{1}) = \psi(\overline{1}), \qquad (\dot{-3},\hat{-3}) = \psi(\overline{-3}) = \psi(\overline{88}).$$

  Pour les deux autres, on utilise l'identité de Bézout :

  $$7 \times 2 + 13 \times (-1) = 1,$$

  qui donne

  $$(\dot{1},\hat{-3}) = \psi(\overline{(-3) \times 7 \times 2 + 1 \times 13 \times (-1)}) = \psi(\overline{-55}) = \psi(\overline{36}),$$
  $$(\dot{-3},\hat{1}) = \psi(\overline{1 \times 7 \times 2 + (-3) \times 13 \times (-1)}) = \psi(\overline{53}).$$

  Finalement l'équation du second degré à 4 solutions dans $\mathbb{Z}/91\mathbb{Z}$: $\overline{1}, \overline{36}, \overline{53}, \overline{88}$.

Remarque
Ceci montre qu'un polynôme à coefficients dans un anneau non intègre peut avoir plus de racines que son degré.

Exercice 37 (Diviseur premier d'un nombre de Mersenne)**
Soient p premier impair et k un diviseur premier de $2^p - 1$. Montrer que $k \equiv 1\ [2p]$.
Indication : examiner l'ordre de $\overline{2}$ *dans* $(\mathbb{Z}/k\mathbb{Z})^\times$.

Corrigé de l'exercice 37
Par hypothèse, $\overline{2}^p = \overline{1}$ dans $\mathbb{Z}/k\mathbb{Z}$, qui est un corps puisque k est un nombre premier. Ceci montre que $\overline{2} \in (\mathbb{Z}/k\mathbb{Z})^\times$ et $ord(\overline{2})$ divise p. Mais p est premier et $\overline{2} \neq \overline{1}$ (puisque $k > 1$), donc $ord(\overline{2}) = p$.
Par ailleurs, $ord(\overline{2})$ divise $Card((\mathbb{Z}/k\mathbb{Z})^\times) = \varphi(k) = k - 1$ donc p divise $k - 1$.
Enfin, $k - 1$ est pair (puisque k est impair, en tant que diviseur premier du nombre impair $2^p - 1$), donc 2 divise $k-1$. Finalement, puisque $2 \wedge p = 1$ (p étant impair), on obtient que le produit $2p$ divise $k - 1$ et donc $k \equiv 1\ [2p]$.

Exercice 38 (Théorème de Wilson)**
1. Soit p un nombre premier. Combien l'équation $x^2 = 1$ possède-t-elle de solutions dans $\mathbb{Z}/p\mathbb{Z}$?
2. Montrer qu'un nombre p est premier si et seulement si on a $(p-1)! \equiv -1\ [p]$.
   C'est le théorème de Wilson.
3. *Application* : calculer le reste de la division euclidienne de $(103!)^{109}$ par 107.

Corrigé de l'exercice 38
Le cas $p = 2$ est évident. On suppose donc $p \geq 3$ dans ce qui suit.

1. Soit $x \in \mathbb{Z}/p\mathbb{Z}$. On a $x^2 = \overline{1} \iff x^2 - \overline{1} = 0 \iff (x-\overline{1})(x+\overline{1}) = 0 \iff x - \overline{1} = 0$ ou $x + \overline{1} = 0$ car $\mathbb{Z}/p\mathbb{Z}$ est intègre (en tant que corps).
   Donc les solutions de l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ sont $-\overline{1}$ et $\overline{1}$ (on notera que si on a $p = 2$, alors $-\overline{1}$ et $\overline{1}$ sont confondus).

   Remarque
   Comme cela arrive parfois dans les livres ou sujets de concours, l'énoncé a confondu -1 *et* 1 *avec leurs classes modulo p. Il vaut mieux éviter en pratique, au moins les premiers temps...*

2. $\boxed{\Leftarrow}$: Soit $p \geq 3$. On suppose $(p-1)! \equiv -1\ [p]$. Notons que $(p-1)! = \prod_{k=1}^{p-1} k$ et donc la relation $(p-1)! \equiv -1\ [p]$ donne en passant dans $\mathbb{Z}/p\mathbb{Z}$:
$$\prod_{k=1}^{p-1} \overline{k} = -\overline{1} \neq \overline{0}.$$
   En particulier, un élément quelconque $\overline{k} \in \{\overline{1}, \ldots, \overline{p-1}\}$ vérifie :
$$\overline{k} \times \left(- \prod_{1 \leq j \leq p-1,\ j \neq k} \overline{j} \right) = \overline{1},$$
   donc est inversible.
   Or on sait qu'un élément $\overline{k}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ ssi $p \wedge k = 1$, donc on vient de prouver que tout élément $k \in \{1, \ldots, p-1\}$ est premier avec p, c'est-à-dire que p est premier.

   $\boxed{\Rightarrow}$: On suppose p premier. On cherche à établir (dans le corps $\mathbb{Z}/p\mathbb{Z}$) :
$$\prod_{k=1}^{p-1} \overline{k} = -\overline{1}.$$
   Dans le produit $\prod_{k=1}^{p-1} \overline{k}$ n'apparaissent que des éléments inversibles car on sait que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible lorsque p est premier. Si on met de côté les éléments qui ont

pour inverse eux-mêmes, on peut regrouper dans ce produit (grâce à la commutativité de $\times$ dans $\mathbb{Z}/p\mathbb{Z}$) chaque élément avec son inverse, et chaque couple ainsi obtenu donnera $\overline{1}$ en se multipliant.
Que sont les élements égaux à leurs inverses ? Ceux vérifiant $x = x^{-1}$, c'est-à-dire $x^2 = \overline{1}$, et la question précédente nous dit qu'il s'agit de $\overline{1}$ et de $-\overline{1}$.
Le produit $\prod_{k=1}^{p-1} \overline{k}$ se résume donc après arrangement et simplification en un produit dont tous les facteurs valent $\overline{1}$ sauf un facteur qui vaut $-\overline{1}$. D'où : $\prod_{k=1}^{p-1} \overline{k} = -\overline{1}$.

3. 107 est un nombre premier donc d'après le théorème de Wilson, $(106)! \equiv -1$ [107].
Or $(106)! = 104 \times 105 \times 106 \times (103)!$ et $106 \equiv -1$ [107], $105 \equiv -2$ [107] et $104 \equiv -3$ [107]. Donc $(106)! \equiv -1$ [107] se réécrit $-6 \times (103)! \equiv -1$ [107].
Or $6 \times 18 = 108$ donc $6 \times 18 \equiv 1$ [107]. Ainsi $-6 \times (103)! \equiv -1$ [107] donne $(103)! \equiv 18$ [107]. Puis $(103!)^{109} \equiv 18^{109}$ [107]. Or $1 \leq 18 < 107$ et 107 est premier donc, par le petit théorème de Fermat (ou celui d'Euler qui est plus général), $18^{106} \equiv 1$ [107], donc $18^{109} = 18^{106} \times 18^3 \equiv 18^3$ [107]. Enfin $18^2 = 324 \equiv 3$ [107] et finalement, vu que $18 \times 3 = 54$, on obtient : $(103!)^{109} \equiv 54$ [107].

VII Polynômes

Exercice 39 (*Factorisation)
Factoriser au maximum les polynômes $X^4 + X^2 + 1$ et $X^6 + 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Corrigé de l'exercice 39

1. Dans $\mathbb{R}[X]$, on a
$$X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 + X + 1)(X^2 - X + 1),$$
et les facteurs sont irréductibles.
Dans $\mathbb{C}[X]$, on a également
$$X^2 + X + 1 = (X - j)(X - \overline{j}), \qquad (X^2 - X + 1) = (X + j)(X + \overline{j}),$$
avec $j = e^{2i\pi/3}$. Donc
$$X^4 + X^2 + 1 = (X - j)(X - \overline{j})(X + j)(X + \overline{j}).$$

2. Les racines complexes de $X^6 + 1$ sont les racines sixièmes de $-1 = e^{i\pi}$, donc les $e^{i\left(\frac{\pi}{6} + \frac{2k\pi}{6}\right)}$ pour $k \in [\![0, 5]\!]$. On a donc la factorisation suivante dans $\mathbb{C}[X]$:
$$X^6 + 1 = (X - e^{i\pi/6})(X - i)(X - e^{i5\pi/6})(X - e^{-i5\pi/6})(X + i)(X - e^{-i\pi/6}).$$
En regroupant les facteurs correspondants aux racines complexes conjuguées, on obtient la factorisation suivante dans $\mathbb{R}[X]$:
$$X^6 + 1 = (X^2 - \sqrt{3}X + 1)(X^2 + 1)(X^2 + \sqrt{3}X + 1),$$
et les trois facteurs sont bien irréductibles.

Exercice 40 (*CNS pour que deux polynômes soient premiers entre eux)
Soient A et B dans $\mathbb{C}[X]$. Montrer que A et B sont premiers entre eux si et seulement si ils n'ont pas de racine commune dans $\mathbb{C}$. Est-ce vrai dans $\mathbb{R}$?

Corrigé de l'exercice 40

$\boxed{\Rightarrow}$ S'il existe $\alpha \in \mathbb{C}$ tel que $A(\alpha) = B(\alpha) = 0$, alors $(X - \alpha)$ divise A et B dans $\mathbb{C}[X]$. Ainsi, A et B possèdent un diviseur commun non inversible, donc ne sont pas premiers entre eux.
Variante : Puisqu'il existe une identité de Bézout $AU + BV = 1$ par hypothèse, alors A et B ne peuvent posséder une racine commune dans $\mathbb{C}$, car cela entraînerait $0 = 1$ (en évaluant la relation de Bézout.

$\boxed{\Leftarrow}$ Si A et B ne sont pas premiers entre eux, alors ils possèdent un diviseur commun non inversible, noté D. Ce polynôme D étant non constant, il possède par le théorème de d'Alembert-Gauss au moins une racine complexe α, qui est racine de A et B par divisibilité.

• C'est faux dans $\mathbb{R}$: par exemple, les polynômes $(X-1)(X^2+1)$ et $(X-2)(X^2+1)$ ne sont pas premiers entre eux (puisque tous deux divisibles par X^2+1 non constant), et ils n'ont pas de racine commune dans $\mathbb{R}$.

Exercice 41 (Polynômes sans racine entière)**
Soit $P \in \mathbb{Z}[X]$. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $P(0), P(1), \dots, P(n-1)$ ne soient pas divisibles par n. Montrer qu'aucune racine de P n'est entière.

Corrigé de l'exercice 41
L'hypothèse implique déjà que P est non nul. Si P est constant, il n'a aucune racine dans $\mathbb{C}$, donc dans $\mathbb{Z}$. On suppose donc que P est non constant et qu'il existe $\alpha \in \mathbb{Z}$ tel que $P(\alpha) = 0$.
En notant $P = \sum_{k=0}^{d} a_k X^k$ (avec $d \in \mathbb{N}^*$ et les a_k dans $\mathbb{Z}$), et $r \in [\![0, n-1]\!]$ le reste de α dans la division euclidienne par n, on a :

$$0 \equiv P(\alpha) \equiv \sum_{k=0}^{d} a_k \alpha^k \equiv \sum_{k=0}^{d} a_k r^k \equiv P(r) \ [n],$$

c'est-à-dire que n divise $P(r)$, ce qui contredit l'hypothèse.

Exercice 42 (Existence de racine entière)**
Soient $P \in \mathbb{Z}[X] \setminus \{0\}$ unitaire et $r \in \mathbb{Q}$ tel que $P(r) = 0$. Montrer qu'on a en fait $r \in \mathbb{Z}$.

Corrigé de l'exercice 42

Notons $r = a/b$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $a \wedge b = 1$ et $P = X^n + \sum_{k=0}^{n-1} c_k X^k$ avec $n \in \mathbb{N}^*$ (P est non constant car il est non nul et possède une racine) et les $c_k \in \mathbb{Z}$. Par hypothèse, on a $P(r) = 0$ donc

$$a^n = -\sum_{k=0}^{n-1} c_k a^k b^{n-k},$$

donc b divise a^n. Puisque $a \wedge b = 1$, une application répétée du lemme de Gauss montre que b divise a, et donc $b = 1$. D'où $r \in \mathbb{Z}$.

Exercice 43 (*Polynômes cyclotomiques)**
Pour un entier $n \geq 1$, on dit qu'une racine n-ième de l'unité z est primitive lorsque $z^d \neq 1$ pour tout entier d tel que $1 \leq d < n$. On note $\mathbb{P}_n$ l'ensemble des racines primitives n-ièmes de 1.
On définit $\Phi_n \in \mathbb{C}[X]$ par $\Phi_n = \prod_{z \in \mathbb{P}_n} (X - z)$.

1. Déterminer $\mathbb{P}_1$, $\mathbb{P}_2$, $\mathbb{P}_3$ et $\mathbb{P}_4$.
   Quel est le degré de Φ_n ?
2. Montrer que pour tout $n \geq 1$, on a $X^n - 1 = \prod_{d \geq 1,\ d|n} \Phi_d$.
3. Montrer que si p est un nombre premier et si k est un entier ≥ 1, alors :
$$\Phi_{p^k} = X^{(p-1)p^{k-1}} + X^{(p-2)p^{k-1}} + \cdots + X^{p^{k-1}} + 1.$$
4. Calculer Φ_n pour $n = 1, 2, 3, 4, 5, 6$.
5. Montrer que $\Phi_n \in \mathbb{Z}[X]$.

Corrigé de l'exercice 43

1. Pour déterminer $\mathbb{P}_n$ on ne conserve que les éléments d'ordre n du groupe cyclique $(\mathbb{U}_n, \times)$.
   Puisque $\mathbb{U}_1 = \{1\}$, on a $\mathbb{P}_1 = \{1\}$.

Puisque $\mathbb{U}_2 = \{-1, 1\}$, on a $\mathbb{P}_2 = \{-1\}$.
Puisque $\mathbb{U}_3 = \{1, j, j^2\}$ avec $j = e^{2i\pi/3}$, on a $\mathbb{P}_3 = \{j, j^2\}$.
Puisque $\mathbb{U}_4 = \{-1, 1, -i, i\}$ on a $\mathbb{P}_4 = \{i, -i\}$.
Le degré de Φ_n est exactement le cardinal de $\mathbb{P}_n$, c'est-à-dire le nombre de générateurs de $(\mathbb{U}_n, \times)$. Or, en tant que groupe cyclique de cardinal n, $(\mathbb{U}_n, \times)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$, et puisqu'un isomorphisme de groupes conserve l'ordre des éléments, $(\mathbb{U}_n, \times)$ possède autant de générateurs que $(\mathbb{Z}/n\mathbb{Z}, +)$, c'est-à-dire $\varphi(n)$ (on rappelle que les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ avec $1 \leq k \leq n$ et $k \wedge n$). Ceci montre que $\deg(\Phi_n) = \varphi(n)$.

2. Puisque dans un groupe fini, tout élément a un ordre qui divise le cardinal du groupe, on peut partitionner $\mathbb{U}_n$ selon l'ordre de ses éléments :

$$\mathbb{U}_n = \bigcup_{d \geq 1,\ d|n} \Omega_{n,d},$$

où $\Omega_{n,d} = \{z \in \mathbb{U}_n,\ ord(z) = d\}$. Cette réunion étant disjointe, on en déduit

$$X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{d \geq 1,\ d|n} \left(\prod_{z \in \Omega_{n,d}} (X - z) \right).$$

Or, pour tout diviseur positif d de n, on a $\Omega_{n,d} = \mathbb{P}_d$: en effet, les éléments de $\mathbb{P}_d$ sont les éléments de $\mathbb{U}_d$ d'ordre d, mais puisque $d|n$, cela coïncide avec les éléments de $\mathbb{U}_n$ d'ordre d, c'est-à-dire $\Omega_{n,d}$, parce que $\mathbb{U}_d \subset \mathbb{U}_n$ (**c'est le point subtil**). Donc

$$X^n - 1 = \prod_{d \geq 1,\ d|n} \left(\prod_{z \in \mathbb{P}_d} (X - z) \right) = \prod_{d \geq 1,\ d|n} \Phi_d.$$

3. Si p est premier et si $k \geq 1$, alors les diviseurs positifs de p^k sont les p^l avec $l \in [\![0, k]\!]$ donc d'après la question précédente :

$$\frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = \frac{\prod_{l=0}^{k} \Phi_{p^l}}{\prod_{l=0}^{k-1} \Phi_{p^l}} = \Phi_{p^k}.$$

On a donc en posant $Y = X^{p^{k-1}}$:

$$\Phi_{p^k} = \frac{Y^p - 1}{Y - 1} = 1 + Y + \cdots + Y^{p-1} = 1 + X^{p^{k-1}} + \cdots + X^{(p-1)p^{k-1}},$$

ce qui montre le résultat voulu.

4. D'après les calculs faits à la question 1., on a

$$\Phi_1 = X - 1,\ \Phi_2 = X + 1,\ \Phi_3 = (X - j)(X - j^2) = X^2 + X + 1,\ \Phi_4 = (X - i)(X + i) = X^2 + 1.$$

En outre, 5 étant premier, on a d'après la question précédente :

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1.$$

Enfin, d'après la formule de la question 2. :

$$X^6 - 1 = \Phi_1\Phi_2\Phi_3\Phi_6 = (X^2 - 1)(X^2 + X + 1)\Phi_6 = (X^4 + X^3 - X - 1)\Phi_6,$$

donc

$$\Phi_6 = \frac{X^6 - 1}{X^4 + X^3 - X - 1} = X^2 - X + 1.$$

5. Montrons par récurrence forte que pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$:
   - C'est vrai pour $n = 1$ car $\Phi_1 = X - 1$.

- Soit $n \geq 2$. Supposons que $\Phi_d \in \mathbb{Z}[X]$ pour tout $1 \leq d < n$ et montrons que $\Phi_n \in \mathbb{Z}[X]$. D'après la question 2., on a
$$X^n - 1 = \Phi_n \times Q,$$
avec $Q = \prod_{d|n,\ 1\leq d<n} \Phi_d$.
Par hypothèse de récurrence, $Q \in \mathbb{Z}[X]$ (comme produit de polynômes à coefficients entiers). Par ailleurs, tous les polynômes cyclotomiques sont unitaires, donc Φ_n et Q sont unitaires. Notons $q = \varphi(n) = \deg(\Phi_n) \in [\![1, n-1]\!]$. On peut alors écrire :
$$\Phi_n = \sum_{k=0}^{q} a_k X^k,$$
$$Q = \sum_{k=0}^{n-q} b_k X^k,$$
et donc
$$X^n - 1 = \sum_{k=0}^{n} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) X^k,$$
avec les $a_k \in \mathbb{C}$, les $b_k \in \mathbb{Z}$ et les conventions $a_q = b_{n-q} = 1$, $a_l = 0$ si $l > q$ et $b_l = 0$ si $l > n - q$. Montrons alors que $a_0, a_1, \cdots, a_{q-1}$ sont entiers.
En identifiant les coefficients de $X^n - 1$, on obtient
$$\forall k \in [\![1, n-1]\!], \qquad \sum_{l=0}^{k} a_l b_{k-l} = 0.$$
L'idée est de procéder par récurrence descendante, en exprimant à chaque fois le a_j d'indice minimal en fonction des a_l avec $l > j$, et ceci est possible car $b_{n-q} = 1$.
Le coefficient b_{n-q} est dans le terme de la somme d'indice $l = k + q - n$, il apparaît ssi $0 \leq k + q - n \leq k$, c'est-à-dire $k \geq n - q$. En isolant ce terme, on a donc
$$\forall k \in [\![n-q, n-1]\!], \qquad a_{k+q-n} = - \sum_{l=k+q-n+1}^{k} a_l b_{k-l}.$$
Puisque $a_q = 1$, on en déduit successivement que $a_{q-1}, a_{q-2}, \cdots, a_0 \in \mathbb{Z}$ et donc $\Phi_n \in \mathbb{Z}[X]$.