Eléments d'algèbre générale

Relation d'équivalence

Exercice 1 [02643] [correction]
Soit $\mathcal{R}$ une relation binaire sur un ensemble E à la fois réflexive et transitive.
On définit les nouvelles relations $\mathcal{S}$ et $\mathcal{T}$ par :
$x\mathcal{S}y \Leftrightarrow (x\mathcal{R}y$ et $y\mathcal{R}x)$ et $x\mathcal{T}y \Leftrightarrow (x\mathcal{R}y$ ou $y\mathcal{R}x)$.
Les relations $\mathcal{S}$ et $\mathcal{T}$ sont-elles des relations d'équivalences ?

Exercice 2 [02644] [correction]
Soit E un ensemble et A une partie de E.
On définit une relation $\mathcal{R}$ sur $\wp(E)$ par : $X\mathcal{R}Y \Leftrightarrow X \cup A = Y \cup A$.
a) Montrer que $\mathcal{R}$ est une relation d'équivalence
b) Décrire la classe d'équivalence de $X \in \wp(E)$

Exercice 3 [02983] [correction]
On considère sur $\mathcal{F}(E,E)$ la relation binaire $\mathcal{R}$ définie par :
$f\mathcal{R}g \Leftrightarrow \exists \varphi \in \mathfrak{S}(E)$ telle que $f \circ \varphi = \varphi \circ g$.
a) Montrer que $\mathcal{R}$ est une relation d'équivalence.
b) Décrire la classe d'équivalence d'une fonction donnée $f \in \mathfrak{S}(E)$.

Exercice 4 [02984] [correction]
Soit $\mathcal{R}$ une relation binaire réflexive et transitive.
On définit une relation $\mathcal{S}$ par $x\mathcal{S}y \Leftrightarrow x\mathcal{R}y$ et $y\mathcal{R}x$.
Montrer que $\mathcal{S}$ est une relation d'équivalence et que $\mathcal{R}$ permet de définir une relation d'ordre sur les classes d'équivalences de $\mathcal{S}$.

Exercice 5 [02985] [correction]
Soit $(G,\times)$ un groupe et H un sous groupe de $(G,\times)$.
On définit une relation binaire $\mathcal{R}$ sur G par :

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$$

Montrer que $\mathcal{R}$ est une relation d'équivalence et en décrire les classes d'équivalence.

Exercice 6 X MP [03243] [correction]
Soit G un groupe multiplicatif de cardinal p^α avec p premier et $\alpha \in \mathbb{N}^\star$.
Montrer que

$$Z(G) \neq \{1\}$$

Groupes

Exercice 7 [00113] [correction]
Un sous-groupe d'un groupe produit est-il nécessairement produit de deux sous-groupes ?

Exercice 8 [00114] [correction]
Soient H et K deux sous-groupes d'un groupe $(G,\star)$.
A quelle condition l'ensemble $H \cup K$ est-il un sous-groupe de $(G,\star)$?

Exercice 9 [00115] [correction]
Un élément a d'un groupe $(G,\star)$ est dit élément de torsion si, et seulement si, il existe $n \in \mathbb{N}^\star$ tel que $a^n = e$. Montrer que le sous-ensemble formé des éléments de torsion d'un groupe abélien en est un sous-groupe.

Exercice 10 [00116] [correction]
Soient $(G,\star)$ un groupe fini commutatif d'ordre n et $a \in G$.
a) Justifier que $x \mapsto a \star x$ est une permutation de G.
b) En considérant le produit des éléments de G, établir que $a^n = e$.

Exercice 11 [00117] [correction]
[Théorème de Lagrange]
Soit H un sous-groupe d'un groupe $(G,.)$ fini.
a) Montrer que les ensembles $aH = \{ax/x \in H\}$ avec $a \in G$ ont tous le cardinal de H.
b) Montrer que les ensembles aH avec $a \in G$ sont deux à deux confondus ou disjoints.
c) En déduire que le cardinal de H divise celui de G.
d) Application : Montrer que tout élément de G est d'ordre fini et que cet ordre divise le cardinal de G.

Exercice 12 [00119] [correction]
Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Déterminer les morphismes du groupe $(\mathfrak{S}_n, \circ)$ vers $(\mathbb{C}^\star, \times)$.

Exercice 13 [00120] [correction]
Soit $n \in \mathbb{N}$ tel que $n \geqslant 3$. On considère la transposition $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$ et le n-cycle $\chi = \begin{pmatrix} 1 & 2 & \dots & n \end{pmatrix}$.
a) Justifier que $\{\tau, \chi\}$ est une partie génératrice de $(\mathfrak{S}_n, \circ)$.
b) Existe-t-il une partie génératrice de $(\mathfrak{S}_n, \circ)$ formée d'un seul élément ?

Exercice 14 [00121] [correction]
Soit H l'ensemble des $\sigma \in \mathfrak{S}_n$ vérifiant $\sigma(k) + \sigma(n+1-k) = n+1$ pour tout $k \in \{1, \dots, n\}$.
Montrer que H est un sous-groupe de $(\mathfrak{S}_n, \circ)$

Exercice 15 [00122] [correction]
Les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^\star, \times)$ sont-ils isomorphes ?

Exercice 16 Centrale MP [02363] [correction]
Quel est le plus petit entier n tel qu'il existe un groupe non commutatif de cardinal n ?

Exercice 17 Centrale MP [02366] [correction]
Montrer que $\left\{x + y\sqrt{3}/x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$ est un sous-groupe de $(\mathbb{R}_+^\star, \times)$.

Exercice 18 Centrale MP [02368] [correction]
Soit n un entier naturel non nul, $(e_1, \dots, e_n)$ la base canonique de $E = \mathbb{R}^n$.
Soit S_n l'ensemble des permutations de $\{1, 2, \dots, n\}$. Soit $t_i = (1, i)$.
Pour $s \in S_n$, on définit $u_s(e_i) = e_{s(i)}$.
a) Montrer que $(t_2, t_3, \dots, t_n)$ engendre S_n.
b) Interpréter géométriquement u_s lorsque s est une transposition.
c) Soit $s = (1\ 2\ \dots\ n-1\ n)$. On suppose que s est la composée de p transpositions. Montrer que $p \geqslant n-1$.
d) Quelle est le cardinal minimal d'une famille de transpositions génératrice de S_n ?

Exercice 19 Mines-Ponts MP [02648] [correction]
Soit G un groupe, H un sous-groupe de G, A une partie non vide de G. On pose $AH = \{ah/a \in A, h \in H\}$. Montrer que $AH = H$ si, et seulement si, $A \subset H$.

Exercice 20 X MP [02948] [correction]
a) Montrer que tout sous-groupe additif de $\mathbb{R}$ qui n'est pas monogène est dense dans $\mathbb{R}$.
b) Soit $x \in \mathbb{R}\backslash\mathbb{Q}$. Montrer qu'il existe une infinité de $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ tels que

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

c) Montrer la divergence de la suite de terme général

$$u_n = \frac{1}{n \sin n}$$

Exercice 21 Centrale MP [01479] [correction]
Soit G le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ engendré par les deux matrices S et T suivantes :

$$S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, T = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

Rappelons que c'est le plus petit sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ contenant S et T.
a) Avec le logiciel de calcul formel, créer les matrices S, T. Expliciter les éléments du groupe $\langle R \rangle$ engendré par la matrice $R = ST$ et préciser le cardinal de ce sous-groupe de G.
Quelles sont les matrices SR et R^7S ?
b) Montrer que tout élément de G est soit une puissance R^k de R, soit un produit R^kS. Préciser le cardinal n de G.
Dresser la liste de tous les éléments de G et déterminer la nature géométrique des endomorphismes canoniquement associés dans l'espace euclidien $\mathbb{R}^2$.
c) La transformation $\phi_S : g \mapsto S.g$ définit une permutation de l'ensemble G.
A l'aide du logiciel de calcul formel, dresser la séquence des éléments de G et de leurs images par ϕ_S.
Quelle est la signature de la permutation de G (qu'on peut identifier à l'ensemble $\{1, 2, \dots, n\}$) ainsi définie ?

Exercice 22 Centrale MP [03199] [correction]
Soient $A(1,0)$ et $B(0,1)$. Les points $M_0(x_0,y_0)$ et $M_1(x_1,y_1)$ sont donnés.
On construit le point P_0 par les conditions :
– les droites (P_0M_0) et (Ox) sont parallèles ;
– $P_0 \in (AB)$.
On construit le point Q_0 par les conditions :
– les droites (P_0Q_0) et (M_1B) sont parallèles ;
– $Q_0 \in (AM_1)$.
Soit le point $M_2(x_2,y_2)$ tel que le quadrilatère $(M_0P_0Q_0M_2)$ soit un parallélogramme.
On pose

$$M_2 = M_0 \star M_1$$

a) Démontrer

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_0 + x_1y_0 \\ y_0y_1 \end{pmatrix}$$

b) Démontrer que la loi $\star$ est associative, admet un élément neutre et que, si $y_0 \neq 0$, le point M_0 admet un inverse.
c) On définit une suite de points $(M_n)_{n\in\mathbb{N}}$ par la donnée de M_0, de M_1 et de la relation de récurrence valable pour tout entier $n \geqslant 2$

$$M_n = M_{n-1} \star M_{n-2}$$

Déterminer y_n en fonction de y_0 et de y_1.

Exercice 23 [03256] [correction]
Soit H un sous-groupe strict d'un groupe $(G,\star)$. Déterminer le groupe engendré par le complémentaire de H dans G.

Exercice 24 [03332] [correction]
Soient a et b deux éléments d'ordre respectifs p et q d'un groupe abélien $(G,\star)$.
Existe-t-il dans G un élément d'ordre$m = \text{ppcm}(p,q)$?

Groupe cyclique

Exercice 25 [00123] [correction]
On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique.
On introduit $(G,\star)$ un groupe cyclique de générateur a et H un sous-groupe de $(G,\star)$.
a) Justifier l'existence d'un plus petit entier naturel non nul tel que $a^n \in H$.
b) Etablir que H est le groupe engendré par a^n.

Exercice 26 [00124] [correction]
Soit G un groupe cyclique de cardinal n.
Montrer, que pour tout diviseur $d \in \mathbb{N}^\star$ de n, G possède un et un seul sous-groupe de cardinal d.

Exercice 27 [00125] [correction]
Soit H et K deux groupes notés multiplicativement.
a) Montrer que si h est un élément d'ordre p de H et k un élément d'ordre q de K alors (h,k) est un élément d'ordre $\text{ppcm}(p,q)$ de $H \times K$.
b) On suppose H et K cycliques. Montrer que le groupe produit $H \times K$ est cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 28 Centrale MP [02365] [correction]
Soit p un nombre premier ; on pose

$$G_p = \left\{z \in \mathbb{C}; \exists k \in \mathbb{N}, z^{p^k} = 1\right\}$$

a) Montrer que G_p est un sous-groupe de $(\mathbb{C}^\star,\times)$.
b) Montrer que les sous-groupes propres de G_p sont cycliques et qu'aucun d'eux n'est maximal pour l'inclusion.
c) Montrer que G_p n'est pas engendré par un système fini d'éléments.

Anneaux

Exercice 29 [00126] [correction]
Soit $f : \mathbb{C} \to \mathbb{C}$ un endomorphisme de l'anneau $(\mathbb{C},+,\times)$ tel que $\forall x \in \mathbb{R}, f(x) = x$.
Montrer que f est l'identité ou la conjugaison complexe.

Exercice 30 [00127] [correction]
Soit a un élément d'un ensemble X.
Montrer l'application $E_a : \mathcal{F}(X,\mathbb{R}) \to \mathbb{R}$ définie par $E_a(f) = f(a)$ est un morphisme d'anneaux.

Exercice 31 [00128] [correction]
Pour $d \in \mathbb{N}$, on note

$$A_d = \left\{(x, y) \in \mathbb{Z}^2 / d \mid (y - x)\right\}$$

a) Montrer que A_d est un sous anneau $(\mathbb{Z}^2, +, \times)$.
b) Inversement, soit A un sous anneau de $(\mathbb{Z}^2, +, \times)$.
Montrer que $H = \{x \in \mathbb{Z} / (x, 0) \in A\}$ est un sous groupe de $(\mathbb{Z}, +)$.
c) En déduire qu'il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$ et $A = A_d$.

Corps

Exercice 32 [00129] [correction]
Soit A un anneau intègre fini. Montrer que A est un corps.
On pourra introduire l'application $x \mapsto ax$ pour $a \in A, a \neq 0$.

Exercice 33 [00130] [correction]
Soit $\mathbb{K}$ un corps fini commutatif. Calculer $\prod_{x \in \mathbb{K}^\star} x$.

Exercice 34 [00132] [correction]
Soient K, L deux corps et f un morphisme d'anneaux entre K et L.
a) Montrer que $\forall x \in K \backslash \{0\}, f(x)$ est inversible et déterminer $f(x)^{-1}$.
b) En déduire que tout morphisme de corps est injectif.

Exercice 35 [00133] [correction]
a) Montrer que si p est premier alors

$$\forall k \in \{1, \ldots, p-1\}, p \mid \binom{p}{k}$$

b) En déduire que si $\mathbb{K}$ est un corps de caractéristique $p \neq 0$ alors

$$\forall a, b \in \mathbb{K}, (a + b)^p = a^p + b^p$$

Idéaux

Exercice 36 [00134] [correction]
Quels sont les idéaux d'un corps $\mathbb{K}$?

Exercice 37 [00135] [correction]
L'ensemble

$$\mathbb{D} = \left\{\frac{p}{10^n}; p \in \mathbb{Z}, n \in \mathbb{N}\right\}$$

des nombres décimaux est évidemment un sous-anneau de $(\mathbb{Q}, +, \times)$.
Montrer que les idéaux de $\mathbb{D}$ sont principaux (c'est-à-dire de la forme $a\mathbb{D}$ avec $a \in \mathbb{D}$).

Exercice 38 [00136] [correction]
[Nilradical d'un anneau]
On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A i.e. des $x \in A$ tels qu'il existe $n \in \mathbb{N}^\star$ vérifiant $x^n = 0$.
Montrer que N est un idéal de A.

Exercice 39 [00137] [correction]
[Radical d'un idéal]
Soit I un idéal d'un anneau commutatif A. On note $R(I)$ l'ensemble des éléments x de A pour lesquels il existe un entier n non nul tel que $x^n \in I$.
a) Montrer que $R(I)$ est un idéal de A contenant I.
b) Montrer que si I et J sont deux idéaux alors

$$R(I \cap J) = R(I) \cap R(J)$$

c) On suppose que $A = \mathbb{Z}$. Montrer que l'ensemble des entiers n non nuls tels que $R(n\mathbb{Z}) = n\mathbb{Z}$ est exactement l'ensemble des entiers sans facteurs carrés.

Exercice 40 [00138] [correction]
Soient A un anneau commutatif et e un élément idempotent de A (i.e. $e^2 = e$).
a) Montrer que $J = \{x \in A / xe = 0\}$ est un idéal de A.
b) On note $I = Ae$ l'idéal principal engendré par e. Déterminer $I + J$ et $I \cap J$.
c) Etablir que pour tout idéal K de A : $(K \cap I) + (K \cap J) = K$.

Exercice 41 [00140] [correction]
[Idéaux premiers]
Un idéal I d'un anneau commutatif $(A,+,\times)$ est dit premier si, et seulement si,

$$\forall x,y\in A, xy\in I\Rightarrow x\in I \text{ ou } y\in I$$

a) Donner un exemple d'idéal premier dans $\mathbb{Z}$.
b) Soit $P\in\mathbb{K}[X]$ un polynôme irréductible. Montrer que $P.\mathbb{K}[X]$ est premier.
c) Soient J et K deux idéaux de A. Montrer que $J\cap K=I\Rightarrow (J=I \text{ ou } K=I)$.
d) Soit $(A,+,\times)$ un anneau commutatif dont tout idéal est premier. Etablir que A est intègre puis que A est un corps.

Exercice 42 [00141] [correction]
[$\mathbb{Z}$ est noethérien]
Montrer que tout suite croissante (pour l'inclusion) d'idéaux de $\mathbb{Z}$ est stationnaire.
Ce résultat se généralise-t-il aux idéaux de $\mathbb{K}[X]$?.

Exercice 43 Centrale MP [02367] [correction]
Soit A un sous-anneau de $\mathbb{Q}$.
a) Soit p un entier et q un entier strictement positif premier avec p. Montrer que si $p/q\in A$ alors $1/q\in A$.
b) Soit I un idéal de A autre que $\{0\}$. Montrer qu'il existe $n\in\mathbb{N}^\star$ tel que $I\cap\mathbb{Z}=n\mathbb{Z}$ et qu'alors $I=nA$.
c) Soit p un nombre premier. On pose

$$Z_p=\{a/b; a\in\mathbb{Z}, b\in\mathbb{N}^\star, p\wedge b=1\}$$

Montrer que si $x\in\mathbb{Q}^\star$ alors x ou $1/x$ appartient à Z_p.
d) On suppose ici que x ou $1/x$ appartient à A pour tout $x\in\mathbb{Q}^\star$. On note I l'ensemble des éléments non inversibles de A.
Montrer que I inclut tous les idéaux stricts de A. En déduire que $A=\mathbb{Q}$ ou $A=Z_p$ pour un certain nombre premier p.

Exercice 44 Mines-Ponts MP [02661] [correction]
Soit p un nombre premier. On note Z_p l'ensemble des a/b où $(a,b)\in\mathbb{Z}\times\mathbb{N}^\star$ et p ne divise pas b. On note J_p l'ensemble des a/b où $(a,b)\in\mathbb{Z}\times\mathbb{N}^\star$, p divise a et p ne divise pas b.
a) Montrer que Z_p est un sous-anneau de $\mathbb{Q}$.
b) Montrer que J_p est un idéal de Z_p et que tout idéal de Z_p autre que Z_p est inclus dans J_p.
c) Déterminer les idéaux de Z_p.

Exercice 45 [02450] [correction]
Soit A un sous-anneau d'un corps K.
On suppose :

$$\forall x\in K\backslash\{0\}, x\in A \text{ ou } x^{-1}\in A$$

et on forme I l'ensemble des éléments de l'anneau A non inversibles.
a) Montrer que I est un idéal de A.
b) Montrer que tout idéal de A autre que A est inclus dans I.

Classe de congruence

Exercice 46 [00142] [correction]
Résoudre les équations suivantes :
a) $3x+5=0$ dans $\mathbb{Z}/10\mathbb{Z}$
b) $x^2=1$ dans $\mathbb{Z}/8\mathbb{Z}$
c) $x^2+2x+2=0$ dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 47 [00143] [correction]
Résoudre les systèmes suivants :

$$\text{a) }\begin{cases} x\equiv 1 & [6] \\ x\equiv 2 & [7]\end{cases}$$

$$\text{b) }\begin{cases} 3x\equiv 2 & [5] \\ 5x\equiv 1 & [6]\end{cases}$$

$$\text{c) }\begin{cases} x+y\equiv 4 & [11] \\ xy\equiv 10 & [11]\end{cases}$$

Exercice 48 [00144] [correction]
[Petit théorème de Fermat]
Soit p un nombre premier. Montrer que $\forall a\in(\mathbb{Z}/p\mathbb{Z})^\star, a^{p-1}=1$.

Exercice 49 [00145] [correction]
Soit p un nombre premier et k un entier premier avec $p-1$.
Montrer que l'application $\varphi:\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$ définie par $\varphi(x)=x^k$ est bijective.

Exercice 50 [00146] [correction]
Soit p un entier premier. Montrer que $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1.

Exercice 51 [00147] [correction]
Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z},+)$ et $(\mathbb{Z}/m\mathbb{Z},+)$.

Exercice 52 [00148] [correction]
[Théorème de Wilson]
Soit p un nombre premier supérieur à 2.
a) Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui égaux à leurs inverses ?
b) En déduire que $p \mid (p-1)!+1$.
c) Montrer que si $n \geqslant 2$ est tel que $n \mid (n-1)!+1$ alors n est premier.

Exercice 53 [00149] [correction]
Soit p un nombre premier supérieur à 3.
a) Quel est le nombre de carré dans $\mathbb{Z}/p\mathbb{Z}$?
b) On suppose $p = 1 \quad [4]$. En calculant de deux façons $(p-1)!$, justifier que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
c) On suppose $p = 3 \quad [4]$. Montrer que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 54 Centrale MP [02364] [correction]
Soit un entier $n \geqslant 2$. Combien $\mathbb{Z}/n\mathbb{Z}$ admet-il de sous-groupes ?

Exercice 55 Mines-Ponts MP [02649] [correction]
Soit $(G,.)$ un groupe fini tel que

$$\forall g \in G, g^2 = e$$

où e est le neutre de G. On suppose G non réduit à $\{e\}$.
Montrer qu'il existe $n \in \mathbb{N}^\star$ tel que G est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n,+)$.

Exercice 56 Mines-Ponts MP [02655] [correction]
Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$?

Exercice 57 Mines-Ponts MP [02660] [correction]
Si p est un nombre premier, quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

Exercice 58 [03218] [correction]
Soit p un nombre premier. Calculer

$$\sum_{k=1}^{p} \bar{k} \text{ et } \sum_{k=1}^{p} \bar{k}^2$$

Indicatrice d'Euler

Exercice 59 [00151] [correction]
Pour $n \in \mathbb{N}^\star$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z},\times)$.
a) Calculer $\varphi(p)$ et $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}^\star$.
b) Soient m et n premiers entre eux.
On considère l'application $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ définie par $f(\bar{x}) = (\hat{x},\tilde{x})$.
Montrer que f est bien définie et réalise un isomorphisme d'anneaux.
c) En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.
d) Exprimer $\varphi(n)$ selon la décomposition primaire de n.

Exercice 60 [00152] [correction]
Pour $n \in \mathbb{N}^\star$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z},\times)$.
Montrer que

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^\star, a^{\varphi(n)} = 1$$

Exercice 61 [00153] [correction]
Pour $n \in \mathbb{N}^\star$, on note $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$.
a) Montrer que si H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$, il existe a divisant n vérifiant $H = < a >$.
b) Observer que si $d \mid n$ il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ d'ordre d.
c) Justifier que si $d \mid n$ le sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$ possède exactement $\varphi(d)$ élément d'ordre d.
d) Montrer que $\forall n \in \mathbb{N}^\star, \sum_{d\mid n} \varphi(d) = n$.

Arithmétique

Exercice 62 [00155] [correction]
Soit A un ensemble de $n+1 \geqslant 2$ entiers distincts tous inférieurs ou égaux à $2n$.
Montrer qu'il existe deux éléments de A tels que l'un divise l'autre.

Exercice 63 Centrale MP [02358] [correction]
Pour $n \in \mathbb{N}^\star$, on désigne par N le nombre de diviseurs positifs de n et par P leur produit.
Relation entre n, N et P ?

Exercice 64 Centrale MP [02359] [correction]
Soit A la somme des chiffres de 4444^{4444}, B celle de A et enfin C celle de B. Que vaut C ?

Exercice 65 Centrale MP [02361] [correction]
Soit $P \in \mathbb{Z}[X]$ et a, b deux entiers relatifs avec $b > 0$ et $\sqrt{b}$ irrationnel.
a) Exemple : montrer que $\sqrt{6}$ est irrationnel.
b) Quelle est la forme de $(a+\sqrt{b})^n$?
c) Montrer que si $a+\sqrt{b}$ est racine de P alors $a-\sqrt{b}$ aussi.
d) On suppose que $a+\sqrt{b}$ est racine double de P. Montrer que $P = RQ^2$ avec R et Q dans $\mathbb{Z}[X]$.

Exercice 66 Centrale MP [02369] [correction]
On suppose que n est un entier $\geqslant 2$ tel que $2^n - 1$ est premier.
Montrer que n est premier.

Exercice 67 Centrale MP [02370] [correction]
On note $\mathcal{P}$ l'ensemble des nombres premiers. Pour tout entier $n > 0$, on note $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. On note $\lfloor x \rfloor$ la partie entière de x. On note $\pi(x)$ le nombre de nombres premiers au plus égaux à x.
a) Montrer que $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
b) Montrer que $\binom{2n}{n}$ divise $\prod_{p \in \mathcal{P}; p \leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$.
c) Montrer que $\binom{2n}{n} \leqslant (2n)^{\pi(2n)}$.
d) Montrer que $\frac{x}{\ln x} = O(\pi(x))$ quand $x \to +\infty$

Exercice 68 Mines-Ponts MP [02654] [correction]
Montrer qu'il existe une infinité de nombres premiers de la forme $4n+3$.

Exercice 69 Mines-Ponts MP [02656] [correction]
Soit des entiers $a > 1$ et $n > 0$. Montrer que si $a^n + 1$ est premier alors n est une puissance de 2.

Exercice 70 Mines-Ponts MP [02657] [correction]
Soit, pour $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.
a) Montrer, si $(n, m) \in \mathbb{N}^2$ avec $n \neq m$, que $F_n \wedge F_m = 1$.
b) Retrouver à l'aide du a) le fait que l'ensemble des nombres premiers est infini.

Exercice 71 Mines-Ponts MP [02658] [correction]
a) Pour $(a, n) \in \mathbb{Z} \times \mathbb{N}^\star$ avec $a \wedge n = 1$, montrer que $a^{\varphi(n)} = 1 \quad [n]$.
b) Pour p premier et $k \in \{1, \dots, p-1\}$, montrer que p divise $\binom{p}{k}$.
c) Soit $(a, n) \in (\mathbb{N}^\star)^2$. On suppose que $a^{n-1} = 1 \quad [n]$. On suppose que pour tout x divisant $n-1$ et différent de $n-1$, on a $a^x \neq 1 \quad [n]$. Montrer que n est premier.

Dénombrement

Exercice 72 Centrale MP [02357] [correction]
Soit E un ensemble de cardinal n, $\mathcal{R}$ une relation d'équivalence sur E ayant k classes d'équivalence et $G = \left\{(x, y) \in E^2 / x\mathcal{R}y\right\}$ le graphe de $\mathcal{R}$ supposé de cardinal p. Prouver qu'on a $n^2 \leqslant kp$.

Exercice 73 Centrale MP [02362] [correction]
Soit E un ensemble fini de cardinal n. Calculer :

$$\sum_{X \subset E} \operatorname{Card} X, \ \sum_{X, Y \subset E} \operatorname{Card}(X \cap Y) \text{ et } \sum_{X, Y \subset E} \operatorname{Card}(X \cup Y)$$

Corrections

Exercice 1 : [énoncé]
Les relations $\mathcal{S}$ et $\mathcal{T}$ sont clairement réflexives et symétriques.
Soit $x, y, z \in E$.
Supposons $x\mathcal{S}y$ et $y\mathcal{S}z$.
On a alors $x\mathcal{R}y$ et $y\mathcal{R}z$ donc $x\mathcal{R}z$ et aussi $y\mathcal{R}x$ et $z\mathcal{R}y$ donc $z\mathcal{R}x$ puis $x\mathcal{S}z$.
Le raisonnement n'est plus valable avec $\mathcal{T}$ et on peut présumer que $\mathcal{T}$ ne sera pas une relation d'équivalence.
Prenons pour $\mathcal{R}$ la relation divise définie sur $\mathbb{N}^\star$. On a $2 \mid 6$ et $3 \mid 6$ donc $2\mathcal{T}6$ et $6\mathcal{T}3$ or $2 \not\mathcal{T} 3$.
Ici la relation $\mathcal{T}$ n'est pas transitive.

Exercice 2 : [énoncé]
a) Ras
b) $Y \in Cl(X) \Leftrightarrow Y \cup A = X \cup A$.
Soit $Y \in Cl(X)$. On a $Y \cup A = X \cup A$
$\forall x \in Y \backslash A$ on a $x \in Y \cup A = X \cup A$ et $x \notin A$ donc $x \in X \backslash A$. Ainsi $Y \backslash A \subset X \backslash A$ et inversement $X \backslash A \subset Y \backslash A$ donc $X \backslash A = Y \backslash A$.
Puisque $Y = (Y \backslash A) \cup (Y \cap A)$ on a $Y = (X \backslash A) \cup B$ avec $B \in \wp(A)$.
Inversement soit $Y = (X \backslash A) \cup B$ avec $B \in \wp(A)$.
On a $Y \cup A = (X \backslash A) \cup (B \cup A) = (X \cap \bar{A}) \cup A = X \cup A$.
Finalement $Cl(X) = \{(X \backslash A) \cup B / B \in \wp(A)\}$.

Exercice 3 : [énoncé]
a) $f \circ \mathrm{Id}_E = \mathrm{Id}_E \circ f$ donc $f\mathcal{R}f$.
Si $f\mathcal{R}g$ alors $\exists \varphi \in \mathfrak{S}(E)$ telle que $f \circ \varphi = \varphi \circ g$ mais alors $g \circ \varphi^{-1} = \varphi^{-1} \circ f$ donc $g\mathcal{R}f$.
Si $f\mathcal{R}g$ et $g\mathcal{R}h$ alors $\exists \varphi, \psi \in \mathfrak{S}(E)$ telles que $f \circ \varphi = \varphi \circ g$ et $g \circ \psi = \psi \circ h$ donc $f \circ \theta = \theta \circ h$ avec $\theta = \varphi \circ \psi \in \mathfrak{S}(E)$. Ainsi $f\mathcal{R}h$.
b) $g \in \mathcal{C}l(f) \Leftrightarrow \exists \varphi \in \mathfrak{S}(E)$ telle que $g = \varphi^{-1} \circ f \circ \varphi$.
Finalement $Cl(f) = \left\{\varphi^{-1} \circ f \circ \varphi / \varphi \in \mathfrak{S}(E)\right\}$.

Exercice 4 : [énoncé]
$\mathcal{S}$ est réflexive, symétrique et transitive sans difficultés.
On définit $Cl(x) \preccurlyeq Cl(y) \Leftrightarrow x\mathcal{R}y$. La relation $\preccurlyeq$ est bien définie, réflexive transitive.
Si $Cl(x) \preccurlyeq Cl(y)$ et $Cl(y) \preccurlyeq Cl(x)$ alors $x\mathcal{S}y$ donc $Cl(x) = Cl(y)$.

Exercice 5 : [énoncé]
Soit $x \in G$. On a $x\mathcal{R}x$ car $xx^{-1} = 1 \in H$.
Soient $x, y \in G$. Si $x\mathcal{R}y$ alors $xy^{-1} \in H$ et donc $yx^{-1} \in H$ d'où $y\mathcal{R}x$.
Soient $x, y, z \in G$. Si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $xy^{-1} \in H$ et $yz^{-1} \in H$ donc $xz^{-1} \in H$ d'où $x\mathcal{R}z$.
Finalement $\mathcal{R}$ est une relation d'équivalence.
Soit $a \in G$.

$$x \in Cl(a) \Leftrightarrow x\mathcal{R}a \Leftrightarrow xa^{-1} \in H$$

donc

$$Cl(a) = Ha = \{ha / h \in H\}$$

Exercice 6 : [énoncé]
Considérons la relation binaire $\mathcal{R}$ sur G définie par

$$y_1\mathcal{R}y_2 \Leftrightarrow \exists x \in G, xy_1 = y_2x$$

Il est immédiat de vérifier que $\mathcal{R}$ est une relation d'équivalence sur G. Les classes d'équivalence de $\mathcal{R}$ forment donc une partition de G ce qui permet d'affirmer que le cardinal de G est la somme des cardinaux des classes d'équivalence de $\mathcal{R}$.
Une classe d'équivalence d'un élément y est réduite à un singleton si, et seulement si,

$$\forall x \in G, xy = yx$$

i.e.

$$y \in Z(G)$$

En dénombrant G en fonction des classes d'équivalence de $\mathcal{R}$ et en isolant parmi celles-ci celles qui sont réduites à un singleton on a

$$\mathrm{Card} G = \mathrm{Card} Z(G) + N$$

avec N la somme des cardinaux des classes d'équivalence de $\mathcal{R}$ qui ne sont pas réduites à un singleton.
Pour poursuivre, montrons maintenant que le cardinal d'une classe d'équivalence de la relation $\mathcal{R}$ divise le cardinal de G.
Considérons une classe d'équivalence $\{y_1, \ldots, y_n\}$ pour la relation $\mathcal{R}$ et notons

$$H_i = \{x \in G / xy_1 = y_ix\}$$

Pour $i \in \{1, \ldots, n\}$, puisque $y_1\mathcal{R}y_i$, il existe $x_i \in G$ tel que

$$x_iy_1 = y_ix_i$$

Considérons alors l'application $\varphi : H_1 \to H_i$ définie par

$$\varphi(x) = x_i x$$

On vérifie que cette application est bien définie et qu'elle est bijective.
On en déduit

$$\text{Card}H_1 = \ldots = \text{Card}H_m = n$$

et puisque G est la réunion disjointes des $H_1, \ldots, H_m$

$$\text{Card}G = mn = p^\alpha$$

Ainsi toutes les classes d'équivalences qui ne sont pas réduites à 1 élément ont un cardinal multiple de p et donc $p \mid N$.
Puisque p divise $\text{Card}G = \text{Card}Z(G) + N$, on a

$$p \mid \text{Card}Z(G)$$

Sachant $Z(G) \neq \emptyset$ (car $1 \in Z(G)$) on peut affirmer

$$\text{Card}Z(G) \geqslant p$$

Exercice 7 : [énoncé]
Non. $\{(x,x)/x \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}^2, +)$ n'est pas produit de deux sous-groupes.

Exercice 8 : [énoncé]
Si $H \subset K$ ou $K \subset H$ alors $H \cup K = K$ (resp. H) et donc $H \cup K$ est un sous-groupe de $(G, \star)$
Inversement, supposons que $H \cup K$ est un sous groupe et que $H \not\subset K$. Il existe alors $h \in H$ tel que $h \notin K$.
Pour tout $k \in K$, on a $k \star h \in H \cup K$ car $H \cup K$ est stable.
Si $k \star h \in K$ alors $h = k^{-1} \star (k \star h) \in K$ ce qui est exclu.
Il reste $k \star h \in H$ qui donne $k = (k \star h) \star h^{-1} \in H$. Ainsi $K \subset H$.
Ainsi si $H \cup K$ est un sous-groupe alors $H \subset K$ ou $K \subset H$.

Exercice 9 : [énoncé]
Notons T l'ensemble des éléments de torsion d'un groupe abélien $(G, \star)$. $T \subset G$, $e \in T$, si $x, y \in T$ avec $x^n = y^m = e$ alors $(x \star y^{-1})^{mn} = x^{mn} \star y^{-mn} = e$ donc $x \star y^{-1} \in T$.

Exercice 10 : [énoncé]
a) Puisque a est inversible, a est régulier ce qui fournit l'injectivité de l'application $x \mapsto a \star x$.
Un argument de cardinalité finie donne la bijectivité de l'application.
b) Par permutation $\prod_{x \in G} x = \prod_{x \in G} a \star x = a^n \star \prod_{x \in G} x$ donc $a^n = e$.

Exercice 11 : [énoncé]
a) L'application $f : H \to aH$ définie par $f(x) = ax$ est bijective.
b) Si $aH \cap bH \neq \emptyset$ alors $b^{-1}a \in H$ et alors puisque $ax = bb^{-1}ax$ on a $aH \subset bH$.
Par symétrie $aH = bH$.
c) Notons k le nombre d'ensembles aH deux à deux distincts. La réunion de ceux-ci est égale à G donc par cardinalité $\text{Card}G = k\text{Card}H$ d'où $\text{Card}H \mid \text{Card}G$.
d) $< x >$ est un sous-groupe de $(G, .)$ de cardinal égal à l'ordre de l'élément x.

Exercice 12 : [énoncé]
Soient φ un tel morphisme et τ la transposition qui échange 1 et 2. On a $\tau^2 = \text{Id}$ donc $\varphi(\tau)^2 = 1$ d'où $\varphi(\tau) = 1$ ou -1. Soit $\tau' = \begin{pmatrix} i & j \end{pmatrix}$ une transposition quelconque de $\mathfrak{S}_n$. Il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $\tau' = \sigma \circ \tau \circ \sigma^{-1}$ et alors $\varphi(\tau') = \varphi(\tau)$. Sachant enfin que tout élément de $\mathfrak{S}_n$ est produit de transpositions on peut conclure :
Si $\varphi(\tau) = 1$ alors $\varphi : \sigma \mapsto 1$. Si $\varphi(\tau) = -1$ alors $\varphi = \varepsilon$ (morphisme signature).

Exercice 13 : [énoncé]
a) $\chi \circ \tau \circ \chi^{-1} = \begin{pmatrix} 2 & 3 \end{pmatrix}$, $\chi^2 \circ \tau \circ \chi^{-2} = \begin{pmatrix} 3 & 4 \end{pmatrix}$, etc.
Les transpositions de la forme $\begin{pmatrix} i & i+1 \end{pmatrix}$ appartiennent au sous-groupe engendré par χ et τ. Or pour $1 \leqslant i < j \leqslant n$, on observe

$$\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} i & i+1 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} j-1 & j \end{pmatrix} \circ \ldots \circ \begin{pmatrix} i & i+1 \end{pmatrix}$$

donc toutes les transpositions appartiennent au sous-groupe engendré par χ et τ.
Sachant que toute permutation est produit de transposition, on peut conclure que $\{\chi, \tau\}$ engendre le groupe $(\mathfrak{S}_n, \circ)$.
b) Le groupe $(\mathfrak{S}_n, \circ)$ n'étant pas commutatif ($n \geqslant 3$), il n'est pas monogène.

Exercice 14 : [énoncé]
$H \subset \mathfrak{S}_n$, $\text{Id} \in H$. Remarquons, $\forall k \in \{1, \ldots, n\}$, $\sigma(k) = n + 1 - \sigma(n + 1 - k)$.

$\forall \sigma, \sigma' \in H$,
$(\sigma' \circ \sigma)(k) = \sigma'(\sigma(k)) = n+1-\sigma'(n+1-\sigma(k)) = n+1-\sigma' \circ \sigma(n+1-k)$ donc $\sigma' \circ \sigma \in H$.
$\forall \sigma \in H$. Posons $\ell = \sigma^{-1}(k)$. On a $\sigma(n+1-\ell) = n+1-\sigma(\ell) = n+1-k$ donc $\sigma^{-1}(n+1-k) = n+1-\ell$ puis $\sigma^{-1}(k)+\sigma^{-1}(n+1-k) = \ell+(n+1-\ell) = n+1$.

Exercice 15 : [énoncé]
Non, l'équation $x^2 = 1$ admet deux solutions dans $(\mathbb{Q}^\star, \times)$ alors que l'équation analogue dans $(\mathbb{Q}, +)$, à savoir $2x = 0$, n'admet qu'une solution.

Exercice 16 : [énoncé]
Notons, pour $n = 6$ que $(\mathfrak{S}_3, \circ)$ est un groupe non commutatif à 6 éléments.
Un groupe à $n = 1$ élément est évidemment commutatif.
Pour $n = 2, 3$ ou 5, les éléments d'un groupe à n éléments vérifient $x^n = e$.
Puisque n est premier, un élément autre que e de ce groupe est un élément d'ordre n et le groupe est donc cyclique donc commutatif.
Pour $n = 4$, s'il y a un élément d'ordre 4 dans le groupe, celui-ci est cyclique.
Sinon, tous les éléments du groupe vérifient $x^2 = e$. Il est alors classique de justifier que le groupe est commutatif.

Exercice 17 : [énoncé]
Notons $H = \left\{x + y\sqrt{3}/x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$.
Pour $a \in H$, $a = x + y\sqrt{3}$ avec $x \in \mathbb{N}$, $y \in$ et $x^2 - 3y^2 = 1$. On a donc $x = \sqrt{1+3y^2} > \sqrt{3}\,|y|$ puis $a > 0$. Ainsi $H \subset \mathbb{R}_+^\star$.
$1 \in H$ car on peut écrire $1 = 1 + 0\sqrt{3}$ avec $1^2 - 3.0^2 = 1$.
Pour $a \in H$, on a avec des notations immédiates, $\frac{1}{a} = x - y\sqrt{3}$ avec $x \in \mathbb{N}$, $-y \in \mathbb{Z}$ et $x^2 - 3(-y)^2 = 1$. Ainsi $1/a \in H$.
Pour $a, b \in H$ et avec des notations immédiates, $ab = xx' + 3yy' + (xy' + x'y)\sqrt{3}$ avec $xx' + 3yy' \in \mathbb{Z}$, $xy' + xy' \in \mathbb{Z}$ et $(xx' + 3yy')^2 - 3(xy' + x'y)^2 = 1$. Enfin puisque $x > \sqrt{3}\,|y|$ et $x' > \sqrt{3}\,|y'|$, on a $xx' + 3yy' \geqslant 0$ et finalement $ab \in H$.

Exercice 18 : [énoncé]
a) Pour $i \neq j \in \{2, \dots, n\}$, $(i, j) = (1, i) \circ (1, j) \circ (1, j)$.
Toute transposition appartient à $\langle t_2, t_3, \dots, t_n\rangle$ et puisque celles-ci engendrent S_n, $S_n = \langle t_2, t_3, \dots, t_n\rangle$.
b) Si $s = (i, j)$, u_s est la réflexion par rapport à l'hyperplan de vecteur normal $e_i - e_j$.
c) Si s est le produit de p transpositions alors $\ker u_s$ contient l'intersection de p hyperplans. Ici $\ker u_s = \{0\}$ donc $p \geqslant n-1$.
d) $n-1$.

Exercice 19 : [énoncé]
Supposons $AH = H$. $\forall a \in A$, $a = ae \in AH = H$ donc $A \subset H$.
Supposons $A \subset H$. Pour $x \in AH$, $x = ah$ avec $a \in A$, $h \in H$. Or $a, h \in H$ donc $x = ah \in H$. Ainsi $AH \subset H$. Inversement, pour $a \in A$ (il en existe car $A \neq \emptyset$) et pour tout $h \in H$, $h = a(a^{-1}h)$ avec $a^{-1}h \in H$ donc $h \in AH$. Ainsi $H \subset AH$ puis $=$.

Exercice 20 : [énoncé]
a) Soit H un tel groupe. Nécessairement $H \neq \{0\}$ ce qui permet d'introduire

$$a = \inf\{h > 0/h \in H\}$$

Si $a \neq 0$, on montre que $a \in H$ puis par division euclidienne que tout $x \in H$ est multiple de a. Ainsi $H = a\mathbb{Z}$ ce qui est exclu. Il reste $a = 0$ et alors pour tout $\varepsilon > 0$, il existe $\alpha \in H \cap \left]0, \varepsilon\right]$. On a alors $\alpha\mathbb{Z} \subset H$ et donc pour tout $x \in \mathbb{R}$, il existe $h \in \alpha\mathbb{Z} \subset H$ vérifiant $|x - h| \leqslant \alpha \leqslant \varepsilon$. Ainsi H est dense dans $\mathbb{R}$.
b) Soit $x \in \mathbb{R}\backslash\mathbb{Q}$. Pour $N \in \mathbb{N}^\star$, considérons l'application $f : \{0, \dots, N\} \to [0, 1[$ définie par $f(kx) = kx - \lfloor kx \rfloor$. Puisque les $N+1$ valeurs prises par f sont dans les N intervalles $[i/N, (i+1)/N[$ (avec $i \in \{0, \dots, N-1\}$), il existe au moins deux valeurs prises dans le même intervalle. Ainsi, il existe $k < k' \in \{0, \dots, N\}$ tel que $|f(k') - f(k)| < 1/N$. En posant $p = \lfloor k'x \rfloor - \lfloor kx \rfloor \in \mathbb{Z}$ et $q = k' - k \in \{1, \dots, N\}$, on a $|qx - p| < 1/N$ et donc

$$\left|x - \frac{p}{q}\right| < \frac{1}{Nq} < \frac{1}{q^2}$$

En faisant varier N, on peut construire des couples (p, q) distincts et donc affirmer qu'il existe une infinité de couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^\star$ vérifiant

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^2}$$

c) Puisque π est irrationnel, il existe une suite de rationnels p_n/q_n vérifiant

$$\left|\pi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

avec $q_n \to +\infty$.

On a alors

$$|u_{p_n}| = \left|\frac{1}{p_n \sin p_n}\right| = \left|\frac{1}{p_n \sin(p_n - q_n\pi)}\right| \geqslant \frac{1}{|p_n|}\frac{1}{|p_n - q_n\pi|} \geqslant \frac{q_n}{p_n} \to \frac{1}{\pi}$$

Ainsi la suite (u_n) ne tend pas vers 0.

$$\{|\sin n| / n \in \mathbb{N}\} = \{|\sin(n + 2k\pi)| / n \in \mathbb{Z}, k \in \mathbb{Z}\} = |\sin(\mathbb{Z} + 2\pi\mathbb{Z})|$$

Puisque le sous-groupe $H = \mathbb{Z} + 2\pi\mathbb{Z}$, n'est pas monogène (car π irrationnel), H est dense dans $\mathbb{R}$ et par l'application $|\sin(.)|$ qui est une surjection continue de $\mathbb{R}$ sur $[0,1]$, on peut affirmer que $\{|\sin n| / n \in \mathbb{N}\}$ est dense dans $[0,1]$.
En particulier, il existe une infinité de n tel que $|\sin n| \geqslant 1/2$ et pour ceux-ci $|u_n| \leqslant 2/n$.
Ainsi, il existe une suite extraite de (u_n) convergeant vers 0.
Au final, la suite (u_n) diverge.

Exercice 21 : [énoncé]
a) On définit les matrices S et T puis on calcule R

```
S:=matrix(2,2,[-1,0,0,1]);
T:=matrix(2,2,[-1,1,1,1])/sqrt(2);
R:=evalm(S&*T);
```

On obtient

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

La matrice R est la matrice d'une rotation d'angle $\pi/4$ et donc vérifie $R^8 = I_2$.
On en déduit

$$\langle R\rangle = \left\{I_2, R, R^2, \dots, R^7\right\}$$

groupe cyclique de cardinal 8.
On peut visualiser les éléments de $\langle R\rangle$ en écrivant

```
seq(evalm(R&^k),k=0..7);
```

On calculer SR et R^7S

```
evalm(S&*R);
```

```
evalm(R^7&*S);
```

On constate

$$SR = R^7S = T$$

b) Considérons

$$H = \langle R\rangle \cup \langle R\rangle S$$

H est évidemment une partie de G contenant S et T.
On établit aisément $SR^\ell = R^{7\ell}S$ pour tout $\ell \in \mathbb{Z}$.
On en déduit alors que H est stable par produit.
On en déduit aussi que H est stable par passage à l'inverse car

$$(R^kS)^{-1} = S^{-1}R^{-k} = SR^{-k} = R^{-7k}S$$

Ainsi H est un sous-groupe inclus dans G contenant S et T. Or G est le plus petit sous-groupe contenant S et T donc $G = H$.
Il y a 8 éléments dans $\langle R\rangle$, l'application $M \mapsto MS$ étant injective, il y aussi 8 éléments dans $\langle R\rangle S$. Enfin les éléments $\langle R\rangle$ sont distincts de ceux de $\langle R\rangle S$ car de déterminants distincts.
On en déduit

$$G = \left\{I_2, R, R^2, \dots, R^7\right\} \cup \left\{S, RS, R^2S, \dots, R^7S\right\}$$

de cardinal $n = 16$.
La séquence de tous les éléments de G est

```
seq(evalm(R&^k),k=0..7),seq(evalm(R&^k&*S),k=0..7);
```

Les endomorphismes canoniquement associés aux éléments R^k sont des rotations, plus précisément, les rotations d'angles $k\pi/4$.
Les endomorphisme canoniquement associés aux éléments R^kS sont des réflexions. L'axe de réflexion s'obtient en recherchant un vecteur propre associé à la valeur propre 1.
c) On obtient la séquence des images respectives de la séquence précédente donnant les éléments de G en écrivant

```
seq(evalm(S&*R&^k),k=0..7),seq(evalm(S&*R&^k&*S),k=0..7);
```

La permutation de $\{1, 2, \dots, 16\}$ correspondante est

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 9 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 1 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Le nombre d'inversion de celle-ci est

$$8 + (14 + 13 + 12 + 11 + 10 + 9 + 8) + 0 + (6 + 5 + 4 + 3 + 2 + 1 + 0)$$

soit encore
$$(1+2+\cdots+14)+1=106$$
La permutation considérée est donc paire, i.e. de signature 1.
On peut aussi tenter, un calcul direct avec Maple
On définit la liste des éléments de G.

```
L:=[seq(evalm(R&^k),k=0..7),seq(evalm(R&^k&*S),k=0..7)]:
```

On définit la procédure donnant l'indice d'un élément de G

```
indice:=proc(M)
local k;
global L;
for k from 1 to 16 do
if equal(M,L[k]) then RETURN(k) fi
od
end:
```

Enfin on calcule la signature par la formule
$$\varepsilon(\sigma)=\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}$$
ce qui se traduit

```
product('product('(indice(M[j])-indice(M[i]))/(j-i)',j=i+1..16)',i=1..15);
```

Exercice 22 : [énoncé]
a) On a
$$P_0\left|\begin{matrix}1-y_0\\ y_0\end{matrix}\right. \text{ et } Q_0\left|\begin{matrix}1+y_0(x_1-1)\\ y_0y_1\end{matrix}\right.$$
(en considérant que les cas singuliers sont les prolongements du cas général)
On en déduit
$$\begin{cases}x_2=x_0+y_0x_1\\ y_2=y_0y_1\end{cases}$$
b) Avec des notations immédiates
$$(M_0\star M_1)\star M_2\left|\begin{matrix}(x_0+y_0x_1)+(y_0y_1)x_2\\ (y_0y_1)y_2\end{matrix}\right. \text{ et } M_0\star(M_1\star M_2)\left|\begin{matrix}x_0+y_0(x_1+y_1x_2)\\ y_0(y_1y_2)\end{matrix}\right.$$
et on vérifie bien l'associativité de la loi $\star$.
On remarque que
$$B\star M=M\star B=M$$
donc B est élément neutre de la loi $\star$.
Enfin si $y_0\neq 0$ alors pour
$$x_1=-x_0/y_0$$
$$y_1=1/y_0$$
on observe
$$M_0\star M_1=M_1\star M_0=B$$
et donc on peut affirmer que M_0 est inversible d'inverse M_1.
c) On a
$$y_n=y_{n-1}y_{n-2}$$
et on peut donc affirmer qu'il est possible d'écrire y_n sous la forme
$$y_n=y_0^{a_n}y_1^{b_n}$$
avec
$$\begin{cases}a_0=1,a_1=0,a_n=a_{n-1}+a_{n-2}\\ b_0=0,b_1=1,b_n=b_{n-1}+b_{n-2}\end{cases}$$
Les suites (a_n) et (b_n) sont récurrente linéaires d'ordre 2 d'équation caractéristique $r^2=r+1$ de racines
$$r_1=\frac{1+\sqrt{5}}{2} \text{ et } r_2=\frac{1-\sqrt{5}}{2}$$
On obtient après calculs
$$a_n=\frac{r_2}{r_2-r_1}r_1^n+\frac{r_1}{r_1-r_2}r_2^n \text{ et } b_n=\frac{r_2^n-r_1^n}{r_2-r_1}$$

Exercice 23 : [énoncé]
Notons K le complémentaire de H dans G et montrons $\langle K\rangle=G$.
On a évidemment $\langle K\rangle\subset G$.
Inversement, on a $K\subset\langle K\rangle$ et il suffit d'établir $H\subset\langle K\rangle$ pour conclure.
Puisque H est un sous-groupe strict de G, son complémentaire K est non vide et donc il existe $a\in K$.
Pour $x\in H$, l'élément $a\star x$ ne peut appartenir à H car sinon $a=(a\star x)\star x^{-1}$ serait élément du sous-groupe H. On en déduit que $a\star x\in K$ et donc
$$x=a^{-1}\star(a\star x)\in\langle K\rangle$$

Ainsi
$$G = H \cup K \subset \langle K \rangle$$
et on peut conclure $\langle K \rangle = G$.

Exercice 24 : [énoncé]
Posons $d = \text{pgcd}(p, q)$. On peut écrire $d = pu + qv$ avec $u, v \in \mathbb{Z}$, $p = dp'$, $q = dq'$ avec $p' \wedge q' = 1$ et $m = dp'q'$.
Considérons l'élément $x = a^v b^{-u} \in G$.
Puisque $a^m = b^m = e$, on vérifie immédiatement que $x^m = e$.
Inversement, supposons $x^r = e$.
On a $a^{vr} = b^{ur}$.
Or a^{vr} est un élément d'ordre divisant p et b^{ur} est un élément d'ordre divisant q donc $a^{vr} = b^{ur}$ est un élément d'ordre divisant $d = \text{pgcd}(p, q)$. Ainsi
$$a^{vrd} = b^{urd} = e$$
On en déduit que, d'une part, p divise vrd et donc $m = pq'$ divise $vrdq' = vrq$ et que, d'autre part $m = qp'$ divise urp. On peut alors affirmer que m divise $vrq + urp = r$
Finalement x est un élément d'ordre m.
Notons que ce résultat permet d'établir que dans un groupe abélien fini il existe un élément dont l'ordre est multiple de l'ordre de tous les éléments du groupe.

Exercice 25 : [énoncé]
a) L'ensemble des $n \in \mathbb{N}^\star$ est une partie non vide (car $a^{\text{Card}G} = e \in H$) de $\mathbb{N}$, elle possède donc un plus petit élément.
b) Posons $b = a^n$. Puisque b appartient au sous-groupe H, $< b > \subset H$.
Considérons ensuite $x \in H$. Il existe $p \in \mathbb{Z}$ tel que $x = a^p$. Soit r le reste de la division euclidienne de p par n : $p = nq + r$ avec $0 \leqslant r < n$. Comme $a^r = a^{p-nq} = xb^{-q}$, on a $a^r \in H$ et par définition de n, on obtient $r = 0$. Par suite $x = a^{nq} = b^q$ et donc $x \in < b >$. Ainsi $H =< b >$ est cyclique.

Exercice 26 : [énoncé]
Par isomorphisme, on peut supposer que $G = \mathbb{Z}/n\mathbb{Z}$ ce qui rend les choses plus concrètes.
Soient $d \in \mathbb{N}^\star$ un diviseur de n et d' son complément à n : $d' = n/d$.
$H =< \overline{d'} >= \left\{0, \bar{d'}, 2\bar{d'}, \dots, (d-1)\bar{d'}\right\}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ à d éléments.
Inversement, considérons un sous-groupe H à d éléments.
Pour tout $\bar{x}$ de H, on a $d\bar{x} = \bar{0}$ car l'ordre d'un élément divise celui du groupe.
Par suite $n \mid dx$ puis $d' \mid x$ ce qui donne $\bar{x} \in \left\{0, \bar{d'}, 2\bar{d'}, \dots, (d-1)\bar{d'}\right\}$.
Ainsi $H \subset \left\{0, \bar{d'}, 2\bar{d'}, \dots, (d-1)\bar{d'}\right\}$ puis l'égalité par cardinalité.

Exercice 27 : [énoncé]
a) $(h, k)^n = 1_{H\times K} \Leftrightarrow p \mid n$ et $q \mid n$ donc (h, k) est un élément d'ordre $\text{ppcm}(p, q)$.
b) Posons p et q les ordres de H et K.
Supposons p et q premiers entre eux.
Si h et k sont générateurs de H et K alors (h, k) est un élément d'ordre $\text{ppcm}(p, q) = pq$ de $H \times K$.
Or $\text{Card}H \times K = pq$ donc $H \times K$ est cyclique.
Inversement, supposons $H \times K$ cyclique.
Si (h, k) est générateur de $H \times K$ alors h et k sont respectivement générateurs de H et K.
On en déduit que h est un élément d'ordre p, k d'ordre q et puisque (h, k) est d'ordre $\text{ppcm}(p, q)$ et pq, on conclut que p et q sont premiers entre eux.

Exercice 28 : [énoncé]
a) $G_p \subset \mathbb{C}^\star$, $1 \in G_p$, pour $z \in G_p$, il existe $k \in \mathbb{N}$ tel que $z^{p^k} = 1$ et alors $(1/z)^{p^k} = 1$ donc $1/z \in G_p$.
Si de plus $z' \in G_p$, il existe $k' \in \mathbb{N}$ vérifiant $z'^{p^{k'}}$ et alors
$(zz')^{p^{k+k'}} = \left(z^{p^k}\right)^{p^{k'}} \left(z'^{p^{k'}}\right)^{p^k} = 1$ donc $zz' \in G_p$.
b) Notons $U_{p^k} = \left\{z \in \mathbb{C}/z^{p^k} = 1\right\}$.
Soit H un sous-groupe de G_p différent de G_p.
S'il existe une infinité de $k \in \mathbb{N}$ vérifiant $U_{p^k} \subset H$ alors $H = G_p$ car G_p est la réunion croissante de U_{p^k}.
Ceci étant exclu, on peut introduire le plus grand $k \in \mathbb{N}$ vérifiant $U_{p^k} \subset H$.
Pour $\ell > k$, tous les $U_{p^\ell} \backslash U_{p^k}$ engendrent au moins $U_{p^{k+1}}$, or $U_{p^{k+1}} \not\subset H$ donc$H \subset U_{p^k}$ puis $H = U_{p^k}$
H est donc un sous-groupe cyclique et ne peut être maximal pour l'inclusion car inclus dans le sous-groupe propre $U_{p^{k+1}}$.
c) Si G_p pouvait être engendré par un système fini d'éléments, il existerait $k \in \mathbb{N}$ tel que ses éléments sont tous racines p^kème de l'unité et alors $G_p \subset U_{p^k}$ ce qui est absurde.

Exercice 29 : [énoncé]
Posons $j = f(i)$. On a $j^2 = f(i)^2 = f(i^2) = f(-1) = -f(1) = -1$ donc $j = \pm i$.
Si $j = i$ alors $\forall a, b \in \mathbb{R}$, $f(a + ib) = f(a) + f(i)f(b) = a + ib$ donc $f = \text{Id}_{\mathbb{C}}$.
Si $j = -i$ alors $\forall a, b \in \mathbb{R}$, $f(a + ib) = f(a) + f(i)f(b) = a - ib$ donc $f : z \mapsto \bar{z}$.

Exercice 30 : [énoncé]
$E_a(x \mapsto 1) = 1$.
$\forall f, g \in \mathcal{F}(X, \mathbb{R})$, $E_a(f+g) = (f+g)(a) = f(a) + g(a) = E_a(f) + E_a(g)$ et $E_a(fg) = (fg)(a) = f(a)g(a) = E_a(f)E_a(g)$ donc E_a est un morphisme d'anneaux.

Exercice 31 : [énoncé]
a) $A_d \subset \mathbb{Z}^2$ et $1_{\mathbb{Z}^2} = (1,1) \in A_d$.
Pour $(x,y), (x',y') \in A_d$, $(x,y) - (x',y') = (x-x', y-y')$ avec $d \mid (y-y') - (x-x')$ donc $(x,y) - (x',y') \in A_d$.
Aussi $(x,y)(x',y') = (xx', yy')$ avec $d \mid (yy' - xx') = (y-x)y' + x(y'-x')$ donc $(x,y)(x',y') \in A_d$.
b) $H \neq \emptyset$ car $0 \in H$ et $\forall x, y \in H$, $x - y \in H$ car $(x-y, 0) = (x,0) - (y,0) \in A$.
c) H sous groupe de $(\mathbb{Z}, +)$ donc il existe $d \in \mathbb{N}$ tel que

$$H = d\mathbb{Z}$$

Pour tout $(x,y) \in A$, on a $(x,y) - (y,y) = (x-y, 0) \in A$ car $(y,y) \in <(1,1)> \subset A$. Par suite $x - y \in d\mathbb{Z}$.
Inversement, si $x - y \in d\mathbb{Z}$ alors $(x-y, 0) \in A$ puis $(x,y) = (x-y,0) + y.(1,1) \in A$.
Ainsi

$$(x,y) \in A \Leftrightarrow x - y \in d\mathbb{Z}$$

et donc alors

$$A = \left\{(x,y) \in \mathbb{Z}^2 / d \mid (y-x)\right\} = A_d$$

Exercice 32 : [énoncé]
Il s'agit ici de montrer que tout $a \in A$, tel que $a \neq 0$, est inversible.
L'application $x \mapsto ax$ est une injection de A vers A car A est intègre, l'élément a est régulier.
Puisque A est fini, cette application est bijective et il existe donc $b \in A$ tel que $ab = 1$.
Ainsi a est inversible.

Exercice 33 : [énoncé]
En regroupant chaque x avec son inverse, lorsqu'ils sont distincts, on simplifie $\prod_{x \in \mathbb{K}^\star} x = \prod_{x \in \mathbb{K}^\star, x = x^{-1}} x$. Or $x = x^{-1}$ équivaut à $x^2 = 1$ et a pour solutions 1 et -1.
Que celles-ci soient ou non distinctes, on obtient $\prod_{x \in \mathbb{K}^\star} x = -1$.

Exercice 34 : [énoncé]
a) Pour $x \in K \backslash \{0\}$, $f(x).f(x^{-1}) = f(x.x^{-1}) = f(1_K) = 1_L$ donc $f(x)$ est inversible et $f(x)^{-1} = f(x^{-1})$.
b) Si $f(x) = f(y)$ alors $f(x) - f(y) = f(x-y) = 0_L$. Or 0_L n'est pas inversible donc $x - y = 0_K$ i.e. $x = y$.
Ainsi f est morphisme injectif.

Exercice 35 : [énoncé]
a) $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ donc $p \mid k\binom{p}{k}$. Or $p \wedge k = 1$ car p est premier et $k \in \{1, \ldots, p-1\}$ donc $p \mid \binom{p}{k}$.
b) Par la formule du binôme, $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$.
Or pour $k \in \{1, \ldots, p-1\}$, $\binom{p}{k} = 0$ dans $\mathbb{K}$ car $p \mid \binom{p}{k}$ et $\mathbb{K}$ est de caractéristique p.
Après simplification, on obtient $\forall a, b \in \mathbb{K}, (a+b)^p = a^p + b^p$.

Exercice 36 : [énoncé]
Soit I un idéal d'un corps $\mathbb{K}$. Si $I \neq \{0\}$ alors I contient un élément x non nul. Puisque $x \in I$ et $x^{-1} \in \mathbb{K}$ on a $1 = xx^{-1} \in I$ puis pour tout $y \in \mathbb{K}$, $y = 1 \times y \in I$ et finalement $I = \mathbb{K}$. Les idéaux de $\mathbb{K}$ sont donc $\{0\}$ et $\mathbb{K}$.

Exercice 37 : [énoncé]
Soit I un idéal de $\mathbb{D}$. $I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il existe $a \in \mathbb{Z}$ vérifiant $I \cap \mathbb{Z} = a\mathbb{Z}$.
Puisque $a \in I$, on a $a\mathbb{D} \subset I$.
Inversement, soit $x \in I$. On peut écrire $x = \frac{p}{10^n}$ avec $p \in \mathbb{Z}$ et $n \in \mathbb{N}$.
On a alors $10^n x \in I$ par absorption donc $p \in I \cap \mathbb{Z}$. On en déduit $a \mid p$ puis $x \in a\mathbb{D}$.
Finalement $I = a\mathbb{D}$

Exercice 38 : [énoncé]
$N \subset A$, $0 \in N$ donc $N \neq \emptyset$. Pour $x, y \in N$, il existe $n, m \in \mathbb{N}^\star$ tel que $x^n = y^m = 0$.

Par la formule du binôme,

$$(x+y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k}$$

Pour $k \geqslant n$, $x^k = 0$ et pour $k \leqslant n-1$, $y^{n+m-1-k} = 0$. Dans les deux cas $x^k y^{n+m-1-k} = 0$ et donc $(x+y)^{n+m-1} = 0$. Par suite $x+y \in N$.
Enfin pour $a \in A$ et $x \in N$, $ax \in N$ car $(ax)^n = a^n x^n$.

Exercice 39 : [énoncé]
a) Par définition $R(I) \subset A$
$0^1 = 0 \in I$ donc $0 \in R(I)$.
Soient $x, y \in R(I)$, il existe $n, m \in \mathbb{N}^\star$ tels que $x^n, y^m \in I$.
On a alors

$$(x+y)^{n+m-1} = \sum_{k=0}^{n-1} \binom{n+m-1}{k} x^k y^{n+m-1-k} + \sum_{k=n}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k} \in I$$

car les premiers termes de la somme sont dans I puisque $y^{n+m-1-k} \in I$ et les suivants le sont aussi car $x^k \in I$
donc $x+y \in R(I)$.
Soit de plus $a \in A$. On a $(ax)^n = a^n x^n \in I$ donc $ax \in R(I)$.
Ainsi $R(I)$ est un idéal de A.
Soit $x \in I$, on a $x^1 \in I$ donc $x \in R(I)$.
b) Si $x \in R(I \cap J)$ alors il existe $n \in \mathbb{N}^\star$ tel que $x^n \in I \cap J$.
On a alors $x^n \in I$ donc $x \in R(I)$ et de même $x \in R(J)$. Ainsi

$$R(I \cap J) \subset R(I) \cap R(J)$$

Soit $x \in R(I) \cap R(J)$. Il existe $n, m \in \mathbb{N}^\star$ tel que $x^n \in I$ et $x^m \in J$.
Pour $N = \max(m, n)$, on a par absorption $x^N \in I$ et $x^N \in J$ donc $x^N \in I \cap J$.
Ainsi $x \in R(I \cap J)$ et on peut affirmer

$$R(I \cap J) \supset R(I) \cap R(J)$$

puis l'égalité.
c) Si n a un facteur carré d^2 avec $d \geqslant 2$.
Posons $k \in \mathbb{Z}$ tel que $n = d^2 k$.
On a $dk \notin n\mathbb{Z}$ et $(dk)^2 = nk \in n\mathbb{Z}$ donc $dk \in R(n\mathbb{Z})$. Ainsi $R(n\mathbb{Z}) \neq n\mathbb{Z}$.
Si n n'a pas de facteurs carrés alors n s'écrit $n = p_1 p_2 \dots p_m$ avec $p_1, \dots, p_m$ nombres premiers deux à deux distincts.
Pour tout $x \in R(n\mathbb{Z})$, il existe $k \in \mathbb{N}^\star$ tel que $x^k \in n\mathbb{Z}$.
Tous les $p_1, \dots, p_m$ sont alors facteurs premiers de x^k donc de x et par conséquent n divise x.
Finalement $R(n\mathbb{Z}) \subset n\mathbb{Z}$ puis $R(n\mathbb{Z}) = n\mathbb{Z}$ car l'autre inclusion est toujours vraie.

Exercice 40 : [énoncé]
a) sans difficultés.
b) Pour tout $x \in A$, $x = xe + x(1-e)$ avec $xe \in I$ et $x - xe \in J$. Par suite $I + J = A$.
Si $xe \in J$ alors $xe = xe^2 = 0$ donc $I \cap J = \{0\}$.
c) L'inclusion $(K \cap I) + (K \cap J) \subset K$ est immédiate. L'inclusion réciproque provient de l'écriture $x = xe + x(1-e)$.

Exercice 41 : [énoncé]
a) Pour $p \in \mathcal{P}$, $p\mathbb{Z}$ est un idéal premier. En effet on sait que $p\mathbb{Z}$ est un idéal et en vertu du lemme d'Euclide : $xy \in p\mathbb{Z} \Rightarrow x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$.
b) Même principe
c) Supposons $J \cap K = I$.
Si $J = I$ ok Sinon $\exists a \in J$ tel que $a \notin I$. $\forall b \in K$, $ab \in J \cap K$ d'où $ab \in I$ puis $b \in I$ car $a \notin I$. Ainsi $K \subset I$. D'autre part $I = J \cap K \subset K$ donc $I = K$.
d) $I = \{0\}$ est un idéal premier donc $xy = 0 \Rightarrow x = 0$ ou $y = 0$.
Soit $x \in A$ tel que $x \neq 0$. $x^2 A$ est premier et $x^2 \in x^2 A$ donc $x \in x^2 A$.
Ainsi $\exists y \in A$ tel que $x = x^2 y$ et puisque $x \neq 0$, $xy = 1$.
Ainsi A est un corps.

Exercice 42 : [énoncé]
Une suite croissante (I_n) d'idéaux de $\mathbb{Z}$ se détermine par une suite d'entiers naturels (a_n) vérifiant $I_n = a_n \mathbb{Z}$ et $a_{n+1} \mid a_n$. Si pour tout $n \in \mathbb{N}$, $I_n = \{0\}$ alors la suite (I_n) est stationnaire.
Sinon à partir d'un certain rang $I_n \neq \{0\}$ et la relation $a_{n+1} \mid a_n$ entraîne $a_{n+1} \leqslant a_n$. La suite d'entiers naturels (a_n) est décroissante et donc stationnaire. Il en est de même pour (I_n).
Ce résultat se généralise à $\mathbb{K}[X]$ en travaillant avec une suite de polynômes unitaires (P_n) vérifiant $P_{n+1} \mid P_n$ ce qui permet d'affirmer en cas de non nullité $\deg P_{n+1} \leqslant \deg P_n$ puis $(\deg P_n)$ stationnaire, puis encore (P_n) stationnaire et enfin (I_n) stationnaire.

Exercice 43 : [énoncé]
Notons qu'un sous-anneau de $\mathbb{Q}$ possédant 1 contient nécessairement $\mathbb{Z}$.
a) Par égalité de Bézout, on peut écrire $pu + qv = 1$ avec $u, v \in \mathbb{Z}$. Si $\frac{p}{q} \in A$ alors

$$\frac{1}{q} = u\frac{p}{q} + v.1 \in A$$

b) $I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
Puisque $I \neq \{0\}$, il existe $p/q \in I$ non nul et par absorption, $p = q.p/q \in I \cap \mathbb{Z}$ avec $p \neq 0$. Par suite $I \cap \mathbb{Z} \neq \{0\}$ et donc $n \in \mathbb{N}^\star$.
Puisque $n \in I$, on peut affirmer par absorption que $nA \subset I$.
Inversement, pour $p/q \in I$ avec $p \wedge q = 1$ on a $1/q \in A$ et $p \in n\mathbb{Z}$ donc $p/q \in nA$.
Ainsi $I = nA$.
c) On peut vérifier que Z_p est un sous-anneau de $\mathbb{Q}$.
Pour $x = a/b \in \mathbb{Q}^\star$ avec $a \wedge b = 1$. Si $p \not| b$ alors $p \wedge b = 1$ et $x \in Z_p$. Sinon $p \mid b$ et donc $p \not| a$ d'où l'on tire $1/x \in Z_p$.
d) Soit J un idéal strict de A. J ne contient pas d'éléments inversibles de A car sinon il devrait contenir 1 et donc être égal à A.
Ainsi J est inclus dans I. De plus, on peut montrer que I est un idéal de A.
En effet $I \subset A$ et $0 \in I$.
Soient $a \in A$ et $x \in I$.
Cas $a = 0$: $ax = 0 \in I$.
Cas $a \neq 0$: Supposons $(ax)^{-1} \in A$ alors $a^{-1}x^{-1} \in A$ et donc $x^{-1} = a(a^{-1}x^{-1}) \in A$ ce qui est exclu. Ainsi, $(ax)^{-1} \notin A$ et donc $ax \in I$.
Soient $x, y \in I$. Montrons que $x + y \in I$.
Cas $x = 0$, $y = 0$ ou $x + y = 0$: c'est immédiat.
Cas $x \neq 0$, $y \neq 0$ et $x + y \neq 0$: On a $(x + y)^{-1}(x + y) = 1$ donc

$$(x + y)^{-1}(1 + x^{-1}y) = x^{-1} \text{ et } (x + y)^{-1}(1 + xy^{-1}) = y^{-1} \text{ (*)}$$

Par l'hypothèse de départ, l'un au moins des deux éléments $x^{-1}y$ ou $xy^{-1} = (x^{-1}y)^{-1}$ appartient à A.
Par opérations dans A à l'aide des relations (*), si $(x + y)^{-1} \in A$ alors x^{-1} ou y^{-1} appartient à A ce qui est exclu. Ainsi $(x + y)^{-1} \notin A$ et donc $x + y \in I$.
Finalement I est un idéal de A.
Par suite, il existe $n \in \mathbb{N}$, vérifiant $I = nA$.
Si $n = 0$ alors $I = \{0\}$ et alors $A = \mathbb{Q}$ car pour tout $x \in \mathbb{Q}^\star$, x ou $1/x \in A$ et dans les deux cas $x \in A$ car $I = \{0\}$.
Si $n = 1$ alors $I = A$ ce qui est absurde car $1 \in A$ est inversible.
Nécessairement $n \geqslant 2$. Si $n = qr$ avec $2 \leqslant q, r \leqslant n - 1$ alors puisque $1/n \notin A$, au moins l'un des éléments $1/q$ et $1/r \notin A$. Quitte à échanger, on peut supposer $1/q \notin A$. qA est alors un idéal strict de A donc $qA \subset I$. Inversement $I \subset qA$ puisque n est multiple de q. Ainsi, si n n'est pas premier alors il existe un facteur non trivial q de n tel que $I = nA = qA$. Quitte à recommencer, on peut se ramener à un nombre premier p.
Finalement, il existe un nombre premier p vérifiant $I = pA$.
Montrons qu'alors $A = Z_p$.
Soit $x \in A$. On peut écrire $x = a/b$ avec $a \wedge b = 1$. On sait qu'alors $1/b \in A$ donc si $p \mid b$ alors $1/p \in A$ ce qui est absurde car $p \in I$. Ainsi $p \not| b$ et puisque p est premier, $p \wedge b = 1$. Ainsi $A \subset Z_p$.
Soit $x \in Z_p$, $x = a/b$ avec $b \wedge p = 1$. Si $x \notin A$ alors $x \neq 0$ et $1/x = b/a \in A$ puis $b/a \in I \in pA$ ce qui entraîne, après étude arithmétique, $p \mid b$ et est absurde.
Ainsi $Z_p \subset A$ puis finalement $Z_p = A$.

Exercice 44 : [énoncé]
a) Facile.
b) J_p idéal de Z_p : facile.
Soit I un idéal de Z_p. On suppose $I \not\subset J_p$, il existe donc un élément $a/b \in I$ vérifiant $a/b \notin J_p$. Par suite p ne divise ni a, ni b et donc et $b/a \in Z_p$ de sorte que a/b est inversible dans Z_p. Ainsi l'idéal contient un élément inversible, donc par absorption il possède 1 et enfin il est égal à Z_p.
c) Pour $k \in \mathbb{N}$, posons J_{p^k} l'ensemble des a/b où $(a, b) \in \mathbb{Z} \times \mathbb{N}^\star$, $p^k \mid a$ et p ne divise pas b. On vérifie aisément que J_{p^k} est un idéal de Z_p.
Soit I un idéal de Z_p. Posons
$k = \max\left\{\ell / \forall x \in I, \exists (a, b) \in \mathbb{Z} \times \mathbb{N}^\star, x = a/b, p^\ell \mid a, p \text{ ne divise pas } b\right\}$.
On a évidemment $I \subset J_{p^k}$.
Inversement, il existe $x = a/b \in I$ avec $p^k \mid a$, p^{k+1} ne divise pas a et p ne divise pas b.
On peut écrire $a = p^k a'$ avec p qui ne divise pas a', et donc on peut écrire $x = p^k x'$ avec $x' = a'/b$ inversible dans Z_p. Par suite tout élément de J_{p^k} peut s'écrire xy avec $y \in Z_p$ et donc appartient à I. Ainsi $J_{p^k} \subset I$ puis $=$.
Finalement les idéaux de Z_p sont les J_{p^k} avec $k \in \mathbb{N}$.

Exercice 45 : [énoncé]
a) $I \subset A$ et $0 \in I$.
Soient $a \in A$ et $x \in I$
Si $a = 0$ alors $ax = 0 \in I$.
Pour $a \neq 0$, supposons $(ax)^{-1} \in A$.
On a alors $a^{-1}x^{-1} \in A$ et donc $x^{-1} = a(a^{-1}x^{-1}) \in A$ ce qui est exclu.
Nécessairement $(ax)^{-1} \notin A$ et donc $ax \in I$.
Soient $x, y \in I$. Montrons que $x + y \in I$.
Si $x = 0$, $y = 0$ ou $x + y = 0$, c'est immédiat. Sinon :

On a $(x+y)^{-1}(x+y)=1$ donc

$$(x+y)^{-1}(1+x^{-1}y)=x^{-1} \text{ et } (x+y)^{-1}(1+xy^{-1})=y^{-1} \ (*)$$

Par l'hypothèse de départ, l'un au moins des deux éléments $x^{-1}y$ ou $xy^{-1}=(x^{-1}y)^{-1}$ appartient à A.
Par opérations dans A à l'aide des relations (*), si $(x+y)^{-1}\in A$ alors x^{-1} ou y^{-1} appartient à A ce qui est exclu. Ainsi $(x+y)^{-1}\notin A$ et donc $x+y\in I$.
Finalement I est un idéal de A.
b) Soit J un idéal de A distinct de A.
Pour tout $x\in J$, si $x^{-1}\in A$ alors par absorption $1=xx^{-1}\in J$ et donc $J=I$ ce qui est exclu.
On en déduit que $x^{-1}\notin A$ et donc $x\in I$. Ainsi $J\subset I$.

Exercice 46 : [énoncé]
a) $3x+5=0\Leftrightarrow x+5=0\Leftrightarrow x=5$ car l'inverse de 3 dans $\mathbb{Z}/10\mathbb{Z}$ est 7.
b) Il suffit de tester les entiers $0,1,2,3,4$. 1 et 3 conviennent. Les solutions sont $1,3,5,7$.
c) $x^2+2x+2=0\Leftrightarrow x^2+2x-3=0\Leftrightarrow (x-1)(x+3)=0$ donc les solutions sont 1 et -3.

Exercice 47 : [énoncé]
a) $x\equiv 1\quad [6]$ donne $x=1+6k$ qui dans la deuxième équation donne $6k=1\quad [7]$.
Or l'inverse de 6 étant 6 on parvient à $k=6\quad [7]$ i.e. $k=6+7\ell$ puis $x=37+42\ell$ avec $\ell\in\mathbb{Z}$. Inversement ok.
b) $\begin{cases} 3x\equiv 2 & [5] \\ 5x\equiv 1 & [6]\end{cases}\Leftrightarrow\begin{cases} x\equiv 4 & [5] \\ x\equiv 5 & [6]\end{cases}$, on poursuit comme ci-dessus. Les solutions sont $29+30\ell$ avec $\ell\in\mathbb{Z}$.
c) Les solutions du système sont solutions de l'équation $z^2-4z+10=0\quad [11]$.
Or $z^2-4z+10=z^2+7z+10=(z+2)(z+5)$ donc les solutions sont $-2=9$ et $-5=6$. On obtient comme solutions les couples $(9,6)$ et $(6,9)$.

Exercice 48 : [énoncé]
Pour $a\in(\mathbb{Z}/p\mathbb{Z})^\star$, l'application $x\mapsto ax$ est une permutation de $(\mathbb{Z}/p\mathbb{Z})^\star$.
Le calcul $\prod\limits_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} x=\prod\limits_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} ax=a^{p-1}\prod\limits_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} x$ donne alors $a^{p-1}=1$ car $\prod\limits_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} x\neq 0$.

Exercice 49 : [énoncé]
Par l'égalité de Bézout, $uk-(p-1)v=1$. Considérons alors l'application $\psi:\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$ définie par $\psi(x)=x^u$. On observe $\psi(\varphi(x))=x^{ku}=x\times x^{(p-1)v}$.
Si $x=0$ alors $\psi(\varphi(x))=0=x$.
Si $x\neq 0$ alors par le petit théorème de Fermat, $x^{p-1}=1$ puis $\psi(\varphi(x))=x\times 1^v=x$.
Ainsi $\psi\circ\varphi=\mathrm{Id}$ et de même $\varphi\circ\psi=\mathrm{Id}$. On peut conclure que φ est bijective.

Exercice 50 : [énoncé]
Considérons $a\in(\mathbb{Z}/p\mathbb{Z})^\star$. Il est clair que l'application $x\mapsto ax$ est une permutation de $\mathbb{Z}/p\mathbb{Z}$ donc $a^k\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}} x^k=\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}}(ax)^k=\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}} x^k$ donc $(a^k-1)\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}} x^k=0$. S'il existe $a\in(\mathbb{Z}/p\mathbb{Z})^\star$ tel que $a^k\neq 1$ alors $\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}} x^k=0$.
Sinon, $\sum\limits_{x\in\mathbb{Z}/p\mathbb{Z}} x^k=0+\sum\limits_{x\in(\mathbb{Z}/p\mathbb{Z})^\star} 1=p-1=-1$.

Exercice 51 : [énoncé]
Notons $\bar{x}$ les éléments de $\mathbb{Z}/n\mathbb{Z}$ et $\hat{x}$ ceux de $\mathbb{Z}/m\mathbb{Z}$. Posons $d=\operatorname{pgcd}(n,m)$.
$n=dn'$ et $m=dm'$ avec $n'\wedge m'=1$. Soit φ un tel morphisme.
$n.\varphi(\bar{1})=\varphi(n.\bar{1})=\varphi(\bar{n})=\varphi(\bar{0})=\hat{0}$ donc $m\mid n\varphi(\bar{1})$ d'où $m'\mid\varphi(\bar{1})$.
Ainsi $\varphi(\bar{1})=m'a$ avec $a\in\mathbb{Z}/m\mathbb{Z}$ puis $\forall x\in\mathbb{Z}/n\mathbb{Z},\varphi(x)=x.m'a$.
Inversement, s'il existe a tel que $\forall x\in\mathbb{Z}/n\mathbb{Z},\varphi(x)=x.m'a$ alors φ est bien définie car $x=y\quad [n]\Rightarrow x.m'=y.m'\quad [m]$ et c'est clairement un morphisme.

Exercice 52 : [énoncé]
a) Dans le corps $\mathbb{Z}/p\mathbb{Z}$ l'équation $x^2=1$ n'a que pour seules solutions 1 et $-1=p-1\quad [p]$ (éventuellement confondues quand $p=2$)
b) Dans le produit $(p-1)!=1\times 2\times\cdots\times p-1$ où l'on retrouve tous les éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ chaque élément, sauf 1 et $p-1$, peut être apparier à son inverse (qui lui est distincts). Par suite $(p-1)!=p-1=-1\quad [p]$.
c) Dans $(\mathbb{Z}/n\mathbb{Z},+,\times)$, $1\times 2\times\ldots\times(n-1)=-1$ donc les éléments $1,2,\ldots,n-1$ sont tous inversibles. Il en découle que $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps et donc n est premier.

Exercice 53 : [énoncé]
a) Considérons l'application $\varphi:x\mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$.
Dans le corps $\mathbb{Z}/p\mathbb{Z}$: $\varphi(x)=\varphi(y)\Leftrightarrow x=\pm y$.

Dans Imφ, seul 0 possède un seul antécédent, les autres éléments possèdent deux antécédents distincts. Par suite Card$\mathbb{Z}/p\mathbb{Z} = 1 + 2(\text{CardIm}\varphi - 1)$ donc il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.
b) D'une part, dans le produit $(p-1)!$ calculé dans $\mathbb{Z}/p\mathbb{Z}$, tous les termes qui ne sont pas égaux à leur inverse se simplifient. Il ne reste que les termes égaux à leur inverse qui sont les solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ à savoir 1 et -1.
Ainsi $(p-1)! = -1$ dans $\mathbb{Z}/p\mathbb{Z}$.
D'autre part, en posant $n = \frac{p-1}{2}$,
$(p-1)! = 1\times\ldots\times n\times(n+1)\times\ldots\times(p-1) = 1\times\ldots\times n\times(-n)\times\ldots\times(-1) = (-1)^n(n!)^2$.
Or $p = 1 \quad [4]$ donc n est pair et $-1 = (p-1)! = (n!)^2$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
c) Si -1 est un carré de $\mathbb{Z}/p\mathbb{Z}$, alors l'application $x \mapsto -x$ définit une involution sur l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$. Puisque seul 0 est point fixe de cette application, on peut affirmer qu'il y a qu'un nombre impair de carré dans $\mathbb{Z}/p\mathbb{Z}$.
Or si $p = 3 \quad [4]$, $(p+1)/2$ est un entier pair, -1 ne peut donc être un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 54 : [énoncé]
Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et $a = \min\left\{k > 0, \bar{k} \in \mathbb{Z}/n\mathbb{Z}\right\}$.
On a $<\bar{a}>\subset H$. Inversement soit $\bar{k} \in H$. Par division euclidienne de k par a, $\bar{k} = q\bar{a} + \bar{r}$ avec $r \in \{0, \ldots, a-1\}$. La minimalité de a entraîne $r = 0$ et donc $\bar{k} \in <\bar{a}>$. Ainsi $H = <\bar{a}>$.
De plus, puisque $\bar{0} \in H = <\bar{a}>$, on peut affirmer que a divise n. Inversement, chaque diviseur de n définit un sous-groupe différent de $\mathbb{Z}/n\mathbb{Z}$. Ainsi il y a autant de sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ que de diviseurs positifs de n.

Exercice 55 : [énoncé]
Il est classique d'établir que le groupe $(G, .)$ est abélien.
Pour $\bar{0}, \bar{1} \in \mathbb{Z}/2\mathbb{Z}$ et $x \in G$, posons $\bar{0}.x = e$ et $\bar{1}.x = x$. On définit ainsi un produit extérieur sur G qui munit le groupe abélien $(G, .)$ d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. De plus cet espace est de dimension finie car Card$G < +\infty$, il est donc isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +, .)$ pour un certain $n \in \mathbb{N}^\star$. En particulier $(G, .)$ est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Exercice 56 : [énoncé]
Les inversibles dans $\mathbb{Z}/78\mathbb{Z}$ sont les classes associés aux entiers de $\{1, \ldots, 78\}$ qui sont premiers avec $78 = 2 \times 3 \times 13$. Il suffit ensuite de dénombrer les multiples de $2, 3, 13$ compris entre 1 et 78. On conclut qu'il y a 24 éléments inversible dans $\mathbb{Z}/78\mathbb{Z}$. On peut aussi calculer $\varphi(78) = 1 \times 2 \times 12 = 24$.

Exercice 57 : [énoncé]
Si $p = 2$: il y a deux carrés dans $\mathbb{Z}/2\mathbb{Z}$.
Si $p \geqslant 3$, considérons l'application $\varphi : x \mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$.
Dans le corps $\mathbb{Z}/p\mathbb{Z}$: $\varphi(x) = \varphi(y) \Leftrightarrow x = \pm y$.
Dans Imφ, seul 0 possède un seul antécédent, les autres éléments possèdent deux antécédents distincts. Par suite Card$\mathbb{Z}/p\mathbb{Z} = 1 + 2(\text{CardIm}\varphi - 1)$ donc il y $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 58 : [énoncé]
On a

$$\sum_{k=1}^{p} \bar{k} = \overline{\sum_{k=1}^{p} k} = \overline{\frac{p(p+1)}{2}}$$

Si $p = 2$ alors

$$\sum_{k=1}^{p} \bar{k} = \bar{1}$$

Si $p \geqslant 3$ alors $(p+1)/2$ est un entier et donc

$$\sum_{k=1}^{p} \bar{k} = \bar{p} \times \overline{\frac{(p+1)}{2}} = \bar{0}$$

On a

$$\sum_{k=1}^{p} \bar{k}^2 = \overline{\sum_{k=1}^{p} k^2} = \overline{\frac{p(p+1)(2p+1)}{6}}$$

Si $p = 2$ alors

$$\sum_{k=1}^{p} \bar{k}^2 = \bar{1}$$

Si $p = 3$ alors

$$\sum_{k=1}^{p} \bar{k}^2 = \bar{1}^2 + \bar{2}^2 = \bar{2}$$

Si $p \geqslant 5$ alors $(p+1)(2p+1)$ est divisible par 6.
En effet, $p+1$ est pair donc $(p+1)(2p+1)$ aussi.
De plus, sur les trois nombres consécutifs

$$2p, (2p+1), (2p+2)$$

l'un est divisible par 3. Ce ne peut être $2p$et si $2p+2$ est divisible par 3 alors $p+1$ l'est aussi. Par suite $(p+1)(2p+1)$ est divisible par 3.

Ainsi

$$\sum_{k=1}^{p}\bar{k}^2=\bar{p}\times\overline{\frac{(p+1)(2p+1)}{6}}=\bar{0}$$

Exercice 59 : [énoncé]
Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z},\times)$ sont les éléments représentés par un nombre premier avec n.
a) $\varphi(p)=p-1$. Etre premier avec p^α équivaut à être premier avec p i.e. à ne pas être divisible par p puisque $p\in\mathcal{P}$. Il y a $p^{\alpha-1}$ multiples de p compris entre 1 et p^α donc $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.
b) Si $x=y\quad[mn]$ alors $x=y\quad[n]$ et $x=y\quad[m]$ donc f est bien définie.
$\varphi(\bar{1})=(\hat{1},\tilde{1})$ et si $a=x+y/xy\quad[mn]$ alors $a=x+y/xy\quad[n]$ donc φ est un morphisme d'anneaux.
Si $f(\bar{x})=f(\bar{y})$ alors $x=y\quad[m]$ et $x=y\quad[n]$ alors $m,n\mid y-x$ et puisque $m\wedge n=1$ alors $mn\mid y-x$ donc $\bar{x}=\bar{y}\quad[mn]$.
f est injective puis bijective par l'égalité des cardinaux.
c) Les inversibles de $\mathbb{Z}/mn\mathbb{Z}$ correspondent aux couples formés par un inversible de $\mathbb{Z}/n\mathbb{Z}$ et un inversible de $\mathbb{Z}/m\mathbb{Z}$. Par suite $\varphi(mn)=\varphi(m)\varphi(n)$.
d) Si $n=\prod_{i=1}^{N}p_i^{\alpha_i}$ alors $\varphi(n)=\prod_{i=1}^{N}p_i^{\alpha_i-1}(p_i-1)$.

Exercice 60 : [énoncé]
Soit $f:x\mapsto ax$ de $(\mathbb{Z}/n\mathbb{Z})^\star$ vers lui-même.
Cette application est bien définie, injective et finalement bijective par cardinalité.
Ainsi $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\star}x=\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\star}ax=a^{\varphi(n)}\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\star}x$ puis $a^{\varphi(n)}=1$ car $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\star}x$ est inversible.

Exercice 61 : [énoncé]
a) Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
Si $H=\{0\}$ alors $H=<n>$.
Sinon, on peut introduire $a=\min\left\{k\in\mathbb{N}^\star/\bar{k}\in H\right\}$.
La division euclidienne de n par a donne $n=qa+r$ d'où $\bar{r}\in H$ puis $r=0$. Ainsi $a\mid n$.
On a $<a>\subset H$ et par division euclidienne on montre $H\subset<a>$ d'où $<a>=H$.
b) Si a divise n, on observe que $<a>$ est d'ordre n/a. Ainsi $<n/d>$ est l'unique sous-groupe d'ordre d de $(\mathbb{Z}/n\mathbb{Z},+)$.
c) Un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est générateur d'un sous-groupe à d éléments donc générateur de $<n/d>$. Inversement, tout générateur de $<n/d>$ est élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Or $<n/d>$ est cyclique d'ordre d donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et possède ainsi $\varphi(d)$ générateurs. On peut donc affirmer que $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(d)$ élément d'ordre d.
d) L'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est cardinal d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et donc diviseur de n. En dénombrant $\mathbb{Z}/n\mathbb{Z}$ selon l'ordre de ses éléments, on obtient $\sum_{d\mid n}\varphi(d)=n$.

Exercice 62 : [énoncé]
Raisonnons par récurrence sur $n\geqslant 1$.
Pour $n=1$: ok
Supposons la propriété établie au rang n.
Par l'absurde supposons que A soit une partie de $n+2$ entiers distincts tous inférieurs ou égaux à $2n+2$. Indexons les éléments de A par ordre croissant : $A=\{a_0,\dots,a_n,a_{n+1}\}$ avec $a_i<a_{i+1}$.
Si $a_n\leqslant 2n$ alors l'ensemble $\{a_0,\dots,a_{2n}\}$ est contraire à l'hypothèse de récurrence.
Sinon $a_n=2n+1$ et $a_{n+1}=2n+2$. Puisque $n+1\mid a_{n+1}$, nécessairement $n+1\notin\{a_0,\dots,a_{n-1}\}$
Considérons alors $\{a_0,\dots,a_{n-1}\}\cup\{n+1\}$. C'est une partie à $n+1$ éléments tous inférieur ou égaux à $2n$. Par hypothèse de récurrence, l'un d'eux divise l'autre et il en est donc de même dans $\{a_0,\dots,a_{n-1},a_{n+1}\}$. Ceci induit une contradiction avec l'hypothèse de départ.
Récurrence établie.

Exercice 63 : [énoncé]
Si n n'est pas un carré alors, en associant dans P^2 chaque diviseur avec celui qui lui est conjugué, on obtient un produit de N termes égaux à n. Ainsi $P^2=n^N$.
Si n est un carré alors P^2 est un produit de $N-1$ termes égaux à n et donc $P^2=n^{N-1}$.

Exercice 64 : [énoncé]
Posons $x=4444^{4444}$, $4444=7\quad[9]$, $7^3=1\quad[9]$ donc $4444^{4444}=7\quad[9]$.
$x<10^{5\times 4444}$ donc $A\leqslant 9\times 5\times 4444=199980$, $B\leqslant 9\times 5+1=46$ puis $C\leqslant 4+9=13$.
Or $C=B=A=x\quad[9]$ donc $C=7$

Exercice 65 : [énoncé]
a) Supposons $\sqrt{6}=p/q$ avec $p\wedge q=1$. On a $6q^2=p^2$ donc p pair, $p=2k$. On

obtient alors $3q^2 = 2k^2$ et donc q est pair. Absurde car p et q sont premiers entre eux.
b) Par développement selon la formule du binôme de Newton
$(a+\sqrt{b})^n = \alpha_k + \beta_k\sqrt{b}$ avec $\alpha_k, \beta_k \in \mathbb{Z}$.
c) $a+\sqrt{b}$ racine de $P = \sum_{k=0}^{n} a_k X^k$ donne $\sum_{k=0}^{n} a_k\alpha_k = \left(\sum_{k=0}^{n} a_k\beta^k\right)\sqrt{b}$.
L'irrationalité de $\sqrt{b}$ entraîne $\sum_{k=0}^{n} a_k\alpha_k = \sum_{k=0}^{n} a_k\beta_k = 0$ ce qui permet de justifier $P(a-\sqrt{b}) = 0$.
d) Posons $Q = (X-a+\sqrt{b})(X-a-\sqrt{b}) = X^2 - 2aX + a^2 - b \in \mathbb{Z}[X]$.
Par division euclidienne $P = QS + T$ avec $\deg T < 2$. Or en posant cette division euclidienne, on peut affirmer que $S, T \in \mathbb{Z}[X]$ avec $P, Q \in \mathbb{Z}[X]$ et Q unitaire.
$a+\sqrt{b}, a-\sqrt{b}$ racine de P entraîne $T = 0$ et donc $P = QS$ avec $Q, S \in \mathbb{Z}[X]$. En dérivant $P' = Q'S + QS'$ et $a+\sqrt{b}$ entraîne racine de P' donne $a+\sqrt{b}$ racine de S. On peut alors comme ci-dessus justifier $S = QR$ avec $R \in \mathbb{Z}[X]$ et conclure.

Exercice 66 : [énoncé]
Si $n = ab$ avec $a, b \in \mathbb{N}^\star$ alors

$$2^n - 1 = (2^a - 1)(1 + 2^a + \cdots + 2^{a(b-1)})$$

donc $2^a - 1 \mid 2^n - 1$ d'où $2^a - 1 = 1$ ou $2^a - 1 = 2^n - 1$ ce qui implique $a = 1$ ou $a = n$.
Ainsi n ne possède que des diviseurs triviaux, il est premier.

Exercice 67 : [énoncé]
a) Pour k suffisamment grand $\lfloor n/p^k \rfloor = 0$, la somme évoquée existe donc car elle ne comporte qu'un nombre fini de termes non nuls. $n! = 1 \times 2 \times \ldots \times n$, parmi les entiers allant de 1 à n, il y en a exactement $\lfloor n/p \rfloor$ divisibles par p, $\lfloor n/p^2 \rfloor$ divisibles par p^2, etc... donc $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
b) $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Pour tout $p \in \mathcal{P}$, $v_p\left(\frac{(2n)!}{(n!)^2}\right) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor$ or
$\lfloor 2x \rfloor - 2\lfloor x \rfloor = 0$ ou 1 donc
$\sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \leqslant \operatorname{Card}\left\{k \in \mathbb{N}^\star / \lfloor 2n/p^k \rfloor > 0\right\} \leqslant \left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor$.
De plus les nombres premiers diviseurs de $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ sont diviseurs d'un entier inférieur à $2n$ (lemme d'Euclide) et sont donc eux-mêmes inférieur à $2n$. Il en découle $\binom{2n}{n} \mid \prod_{p\in\mathcal{P};p\leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$ car toutes les puissances de nombres premiers intervenant dans la décomposition de $\binom{2n}{n}$ divisent $\prod_{p\in\mathcal{P};p\leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor}$.
c) $\binom{2n}{n} \leqslant \prod_{p\in\mathcal{P};p\leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p} \right\rfloor} \leqslant \prod_{p\in\mathcal{P};p\leqslant 2n} p^{\frac{\ln(2n)}{\ln p}} \leqslant \prod_{p\in\mathcal{P};p\leqslant 2n} (2n) = (2n)^{\pi(2n)}$.
d) En passant au logarithme : $\sum_{k=1}^{2n} \ln k - 2\sum_{k=1}^{n} \ln k \leqslant \pi(2n)\ln(2n)$.
A l'aide d'une comparaison intégrale on obtient
$\int_1^n \ln(t)\mathrm{d}t \leqslant \sum_{k=1}^{n} \ln k \leqslant \int_1^{(n+1)} \ln(t)\mathrm{d}t$ donc
$n\ln n - n + 1 \leqslant \sum_{k=1}^{n} \ln k \leqslant (n+1)\ln(n+1) - n$ donc $\sum_{k=1}^{n} \ln k = n\ln n - n + O(\ln n)$.
Par suite $\sum_{k=1}^{2n} \ln k - 2\sum_{k=1}^{n} \ln k = 2n\ln(2n) - 2n - 2(n\ln n - n) + O(\ln n)$ puis
$\sum_{k=1}^{2n} \ln k - 2\sum_{k=1}^{n} \ln k \sim \ln(2)(2n)$.
On en déduit $\frac{2n}{\ln 2n} = O(\pi(2n))$.
Ajoutons $\frac{x}{\ln x} \sim \frac{2\lfloor x/2 \rfloor}{\ln 2\lfloor x/2 \rfloor}$ par calculs et $\pi(x) \sim \pi(2\lfloor x/2 \rfloor)$ car $\pi(x)$ et $\pi(2\lfloor x/2 \rfloor)$ ne diffèrent qu'au plus d'une unité et $\pi(x) \to +\infty$. Finalement, une certaine satisfaction.

Exercice 68 : [énoncé]
Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers de la forme $4n+3$. Posons N le produit de ceux-ci et considérons l'entier $4N-1$.
$4N-1$ est impair donc 2 ne le divise pas.
Si tous les facteurs premiers de $4N-1$ sont égaux à 1 modulo 4 alors
$4N - 1 \equiv 1 \quad [4]$ ce qui est absurde.
L'un au moins des facteurs premiers de $4N-1$ est alors de la forme $4n+3$ et donc celui-ci apparaît dans le produit N.
Ce facteur premier divise $4N-1$ et il divise N, il divise donc -1, c'est absurde.

Exercice 69 : [énoncé]
$n = 2^k(2p+1)$, $a^n + 1 = b^{2p+1} - (-1)^{2p+1} = (b+1)c$ avec $b = a^{2^k}$. On en déduit que $b+1 \mid a^n+1$, or a^n+1 est supposé premier et $b+1 > 1$ donc $b+1 = a^n+1$ puis $n = 2^k$.

Exercice 70 : [énoncé]
a) Quitte à échanger, supposons $n < m$.
On remarque que
$$(F_n - 1)^{2^{m-n}} = F_m - 1$$
En développant cette relation par la formule du binôme, on parvient à une relation de la forme
$$F_m + vF_n = 2$$
avec $v \in \mathbb{Z}$ car les coefficients binomiaux sont des entiers.
On en déduit que $\text{pgcd}(F_n, F_m) = 1$ ou 2.
Puisque F_n et F_m ne sont pas tous deux pairs, ils sont premiers entre eux.
b) Les F_n sont en nombre infini et possèdent des facteurs premiers distincts, il existe donc une infinité de nombres premiers.

Exercice 71 : [énoncé]
a) L'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de cardinal $\varphi(n)$.
b) $k\binom{p}{k} = p\binom{p-1}{k-1}$ donc $p \mid k\binom{p}{k}$ or $p \wedge k = 1$ donc $p \mid \binom{p}{k}$.
c) Posons $d = (n-1) \wedge \varphi(n)$. $d = (n-1)u + \varphi(n)v$ donc $a^d = 1 \quad [n]$. Or $d \mid n-1$ donc nécessairement $d = n-1$. Par suite $n-1 \mid \varphi(n)$ puis $\varphi(n) = n-1$ ce qui entraîne que n est premier.

Exercice 72 : [énoncé]
Notons $n_1, \ldots, n_k$ les cardinaux respectifs des k classes d'équivalence de $\mathcal{R}$. D'une part $n = n_1 + \cdots + n_k$, d'autre part $p = n_1^2 + \cdots + n_k^2$. Par l'inégalité de Cauchy-Schwarz : $(n_1 + \cdots + n_k)^2 \leqslant k(n_1^2 + \cdots + n_k^2)$.

Exercice 73 : [énoncé]
Pour $k \in \{0, \ldots, n\}$, il y a $\binom{n}{k}$ parties X à un k éléments dans E. Par suite

$\sum\limits_{X \subset E} \text{Card}(X) = \sum\limits_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.

Pour $k \in \{0, \ldots, n\}$, il y a $\binom{n}{k}$ parties Z à k éléments dans E.
Pour une telle partie Z, les parties X contenant Z ont $\ell \in \{k, \ldots, n\}$ éléments.
Il y a $\binom{n-k}{\ell-k}$ parties X à ℓ éléments contenant Z.
Pour une telle partie X, une partie Y telle que $X \cap Y = Z$ est une partie Y déterminée par $Z \subset Y \subset Z \cup C_E X$.
Il y a $2^{n-\ell}$ parties Y possibles.
Ainsi, il y a $\sum\limits_{\ell=k}^{n} \binom{n-k}{\ell-k} 2^{n-\ell} = (1+2)^{n-k} = 3^{n-k}$ couples (X, Y) tels que $X \cap Y = Z$.

$\sum\limits_{X, Y \subset E} \text{Card}(X \cap Y) = \sum\limits_{k=0}^{n} \sum\limits_{\text{Card} Z = k} \sum\limits_{X \cap Y = Z} \text{Card}(X \cap Y) = \sum\limits_{k=0}^{n} k\binom{n}{k} 3^{n-k}$.

Or $((3+x)^n)' = n(3+x)^{n-1} = \sum\limits_{k=0}^{n} k\binom{n}{k} 3^{n-k} x^{k-1}$ donc

$\sum\limits_{X, Y \subset E} \text{Card}(X \cap Y) = n4^{n-1}$.

Enfin $\text{Card}(X \cup Y) = \text{Card}X + \text{Card}Y - \text{Card}(X \cap Y)$ donne
$\sum\limits_{X, Y \subset E} \text{Card}(X \cup Y) = 2^n n2^{n-1} + 2^n n2^{n-1} - n4^{n-1} = 3n4^{n-1}$.