23 ANNEAUX, ARITHMÉTIQUE

I. AUTRES STRUCTURES

ANNEAUX (2 LOIS)

Définition 56 *(Anneau)*

ensemble A muni de deux lois + et × tel que

1. $(A,+)$ groupe commutatif (élément neutre noté 0).
2. la loi (produit) × est interne et associative.
3. le produit est distributif à droite et à gauche par rapport à l'addition.
4. il existe un élément neutre, noté 1_A (ou 1), pour la multiplication.

Définition 57 *(Vocabulaire)*

soit $(A,+,\times)$ un anneau

→ A est *commutatif* si la loi × est commutative.
→ $a \in A$ est un *diviseur de* 0 s'il est non nul et s'il existe $b \neq 0$ tel que $a \times b = 0$.
→ A est *intègre* s'il n'a aucun diviseur de 0. Cela revient à dire que pour tout $a, b \in A$, $a \times b = 0$ si et seulement si $a = 0$ ou $b = 0$.

Définition 58 *(Sous-anneau)*

$B \subset A$ est un sous-anneau de A s'il contient 1, est stable pour les deux lois et B muni des lois induites $(+,\times)$ possède une structure d'anneau. On montre que B est un sous-anneau de A en montrant :

→ $B \subset A$ et $1_A \in B$,
→ pour tout $a, b \in B$, $a - b$ et $a \times b \in B$.

EXEMPLE

→ $(\mathbb{Z},+,\times)$ et $(\mathbb{R}[X],+,\times)$ sont des anneaux commutatifs et intègres.
→ $(\mathscr{C}^0(I,\mathbb{R}),+,\times)$ est un anneau commutatif mais il n'est pas intègre.
→ Si E est un espace vectoriel, $(\mathscr{L}(E),+,\circ)$ est un anneau non commutatif, non intègre.

Définition 59 *(Morphisme d'anneaux)*

Soit A et A' deux anneaux, $f : A \to A'$ est un morphisme d'anneaux si

→ $f(1_A) = 1_{A'}$
→ $\forall (a_1, a_2) \in A \times A, f(a_1 + a_2) = f(a_1) + f(a_2)$ et $f(a_1.a_2) = f(a_1).f(a_2)$

Propriété 98 *(Règles de calcul)*

si $a, b \in A$ commutent alors

→ $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$,
→ $a^n - b^n = (a-b)\left(\sum_{k=0}^{n-1} a^k b^{n-1-k}\right)$.

CORPS (2 LOIS)

Définition 60 *(Corps)*

On dit que $(K,+,\times)$ est un corps si

1. $(K,+,\times)$ est un anneau commutatif. On note 0 l'élément neutre pour + (appelé élément nul) et 1 l'élément neutre pour ×
2. tout $x \in K$ non nul est inversible : il existe $y \in K$ tel que $x \times y = y \times x = 1$ (on note alors $y = x^{-1}$).

on définit comme précédemment les notions de sous-corps et de morphismes de corps.

EXEMPLE

→ $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps. Dans cet ordre, ils sont des sous-corps du corps suivant.
→ Dans un corps, tous les éléments non nuls sont simplifiables, il n'y a donc pas de diviseur de zéro. Pour qu'un anneau ait une chance d'être un corps, il faut donc qu'il soit intègre (mais ce n'est pas suffisant).

ESPACES VECTORIELS (2 LOIS)

Définition 61 *(Espace vectoriel)*

Soit $(\mathbb{K}, +, .)$ un corps commutatif. On dit que $(E, +, .)$ est un espace vectoriel sur $\mathbb{K}$ si

1. la loi + est une loi interne et $(E, +)$ est un groupe commutatif.
2. la loi . est une loi externe : $\left\{ \begin{array}{ccc} \mathbb{K} \times E & \to & E \\ (\lambda, x) & \mapsto & \lambda.x \end{array} \right.$ qui vérifie
   → $(\lambda + \mu).x = \lambda.x + \mu.x$
   → $\lambda.(x + y) = \lambda.x + \lambda.y$
   → $\lambda.(\mu.x) = (\lambda.\mu).x$
   → $1.x = x$

Les éléments d'un espace vectoriel sont appelés les *vecteurs*, les éléments du corps de base $\mathbb{K}$ sont appelés *scalaires*. Le vecteur $\lambda.x$ est noté simplement λx.

Proposition 99 *(Règles de calcul)*

Soit E un $\mathbb{K}$-espace vectoriel, on a ($x, y \in E$ et $\lambda \in \mathbb{K}$)

1. $0_{\mathbb{K}}.x = 0_E$.
2. $\lambda.0_E = 0_E$.
3. $-(\lambda x) = (-\lambda)x = \lambda(-x)$
4. $\lambda(x - y) = \lambda x - \lambda y$

ALGÈBRE (3 LOIS)

Définition 62 *(Algèbre)*

Soit $\mathbb{K}$ un corps. On dit que $(A, +, \star, .)$ est une $\mathbb{K}$-algèbre si

1. $(A, +, .)$ est un $\mathbb{K}$-espace vectoriel.
2. $(A, +, \star)$ est un anneau.
3. $(\lambda.x) \star y = x \star (\lambda.y) = \lambda.(x \star y)$ pour $\lambda \in \mathbb{K}$ et $x, y \in A$.

En pratique, il y a une loi interne « additive » et deux lois « multiplicatives », l'une correspond à la multiplication par les constantes, l'autre à une multiplication interne. On peut également voir une algèbre comme un espace vectoriel muni d'une multiplication interne (avec des propriétés entre les deux multiplications).

EXEMPLE

→ $\mathscr{F}(A, \mathbb{K})$ (ensemble des applications d'un ensemble A dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) est une algèbre.
→ $\mathscr{C}^0(I, \mathbb{K}), \mathscr{C}^k(I, \mathbb{K})$ ou $\mathscr{C}^\infty(I, \mathbb{K})$ sont des algèbres.
→ $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont des algèbres.
→ $\mathbb{R}^{\mathbb{N}}$ ou $\mathbb{C}^{\mathbb{N}}$ les ensembles des suites à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$ sont des algèbres.
→ $(\mathscr{L}(E), +, \circ, .)$ l'ensemble des endomorphismes d'un espace vectoriel E est une algèbre.
→ $M_n(\mathbb{K})$ l'ensemble des matrices carrées de taille n est une algèbre.

II. IDÉAUX ET $\mathbb{K}[X]$

Définition 63 *(Idéal d'un anneau commutatif)*

Soit $(A,+,\times)$ un idéal commutatif (on notera également $\cdot$ la loi multiplicative)

→ On appelle idéal de A toute partie non vide I telle que
- $(I,+)$ est un sous-groupe de $(A,+)$ (stable par somme et opposé)
- pour tout $x \in I$ et $a \in A$, $a \times x \in I$

→ une intersection d'idéaux est un idéal, la somme de deux idéaux est un idéal. Le noyau d'un morphisme d'anneaux commutatifs est un idéal.

→ si $a \in A$, on note (a) le plus petit idéal de A contenant A - c'est $a.A = \{a \times x, x \in A\}$.

→ si $a_1,\dots,a_p$ sont des éléments de A, $I(a_1,\dots,a_p) = (a_1)+\dots+(a_p) = \left\{\sum_{i=1}^{p} a_i x_i, (x_1,\dots,x_p) \in A^p\right\}$ est le plus petit idéal de A qui contient tous les a_i.

→ Si $a,b \in A$, on dit que a divise b lorsqu'il existe $c \in A$ tel que $b = a \times c$. Cela équivaut à dire que $(b) \subset (a)$.

→ Un idéal I est principal lorsqu'il est engendré par un seul élément (il existe $a \in A$ tel que $I = (a)$). Un anneau est principal si tous ses idéaux sont principaux.

→ Les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$ sont tous principaux.

Propriété 100 *(Arithmétique dans $\mathbb{K}[X]$)*

→ Soient P et Q deux polynômes (l'un au moins non nul). Il existe un unique polynôme G unitaire tel que $(P)+(Q) = (G) = \left\{UP+VQ, (U,V) \in \mathbb{K}[X]^2\right\}$. Il est appelé pgcd de P et Q et noté $\text{pgcd}(P,Q)$ ou $P \wedge Q$.

→ P et Q sont premiers entre eux lorsque $P \wedge Q = 1$. Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, P et Q sont premiers entre-eux si et seulement si ils n'ont pas de racine complexe commune.

→ **théorème de Bézout** : P et Q sont premiers entre eux si et seulement si il existe $U,V \in \mathbb{K}[X]$ tels que $UP+VQ = 1$.

→ **lemme de Gauss** : si $A|BC$ et $A \wedge B = 1$ alors $A|C$.

→ Si A est premier avec B et C alors il est premier avec BC.

→ Généralisation à plusieurs polynômes : on appelle pgcd de $P_1,\dots,P_k$ (non tous nuls) l'unique polynôme unitaire G qui engendre l'idéal engendré par $P_1,\dots,P_k$. Les polynômes sont premiers entre eux (dans leur ensemble) lorsque leur pgcd est 1 (cela équivaut à l'existence de $U_1,\dots,U_k$ tels que $\sum_{=1}^{k} U_i P_i = 1$).

→ Un polynôme P de degré au moins 1 est irréductible lorsqu'il n'admet aucun diviseur strict (non constant et non multiple constant de P).

→ Soit $P \in \mathbb{K}[X]$ ($\mathbb{K}$ corps quelconque). On peut factoriser P par $(X-a)$ si et seulement si $P(a) = 0$. Notamment un polynôme de degré n de $\mathbb{K}[X]$ possède au maximum n racines dans K.

→ Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Ceux de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 avec un discriminant strictement négatif.

→ Tout polynôme de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ se décompose de façon unique (à l'ordre près) sous la forme $\alpha P_1 \dots P_k$ où α est scalaire et les P_i sont irréductibles unitaires.

Remarque : on n'est pas obligé d'imposer un pgcd unitaire. On parle alors d'un pgcd de P et Q

Exercice 1

Démontrer que les seuls idéaux d'un corps K sont $\{0\}$ et K.

Exercice 2

Soit $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Décomposer en produit de polynômes irréductibles dans $\mathbb{C}[X]$ puis $\mathbb{R}[X]$ le polynôme

$$P = X^{2n} - 2X^n \cos(n\theta) + 1.$$

Exercice 3

Soit $P = 2X^4 - 3X^2 + 1$ et $Q = X^3 + 3X^2 + 3X + 2$.

1. Décomposer P en facteurs premiers sur $\mathbb{C}[X]$ (calculer en 1 et -1).
2. Décomposer Q en facteurs premiers sur $\mathbb{C}[X]$ (calculer en -2).
3. Déduisez-en qu'il existe deux polynômes U et V tels que $UP+VQ = 1$. Indiquez une méthode pour déterminer deux polynômes U et V en utilisant l'algorithme d'euclide.

III. ANNEAUX $\mathbb{Z}/n\mathbb{Z}$

L'ESSENTIEL - ANNEAU $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$,
- → la relation de congruence modulo n est compatible avec l'addition et la multiplication. Cela permet de définir une structure d'anneau sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ avec $\overline{x}+\overline{y} = \overline{x+y}$ et $\overline{x}\times\overline{y} = \overline{x\times y}$.
- → un élément $a = \overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement $k \wedge n = 1$.
- → L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Proposition 101 *(Théorème chinois)*

L'application

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/(mn)\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \mapsto & (\overline{x}, \overline{x}) \end{array} \right.$$

est un isomorphisme d'anneaux si et seulement si $m \wedge n = 1$ (les classes sont prises respectivement modulo mn,m et n).

Propriété 102 *(Indicatrice d'Euler)*

- → on note $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. C'est aussi le nombre d'entier entre 1 et n qui sont premiers avec n.
- → la fonction est multiplicative : si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$.
- → Si p est premier alors $\varphi(p) = p-1$ et $\varphi(p^n) = p^n - p^{n-1} = p^n\left(1-\frac{1}{p}\right)$.
- → Si $n = \prod_{i=1}^{k} p_k^{\alpha_k}$ alors $\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$
- → Si a est un élément inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $a^{\varphi(n)} = 1$. Notamment pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ non nul, avec p premier, on a $a^{p-1} = 1$ - ou pour tout $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.

IV. EXERCICES

GROUPES

Exercice 4

Déterminer le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$. Ce groupe est-il cyclique?

Exercice 5

On dit qu'un groupe abélien G est simple lorsque ses seuls sous-groupes sont G et $\{0_G\}$.

1. À quelle condition le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est-il simple?
2. Montrer qu'un groupe abélien fini est simple si et seulement si il est cyclique d'ordre premier.

ANNEAUX, CORPS

Exercice 6 ***(Petit théorème de Fermat)***

Soit p un nombre premier.

1. Montrer que pour $k \in [\![1; p-1]\!]$, p divise $\binom{p}{k}$.
2. En déduire que, pour tout $(a,b) \in \mathbb{Z}^2$, $(a+b)^p \equiv a^p + b^p \pmod{p}$.
3. Montrer par récurrence que, pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$, et que si p ne divise pas a, alors $a^{p-1} \equiv 1 \pmod{p}$.

Exercice 7

Un nombre complexe α est dit algébrique lorsqu'il est racine d'un polynôme non nul a coefficients entiers. Soit α un nombre algébrique.

1. Montrer qu'il existe un unique polynôme $\Pi \in \mathbb{Q}[X]$, unitaire et irréductible sur $\mathbb{Q}$, tel que $\Pi(\alpha) = 0$. On note d le degré de Π.
2. On pose $\mathbb{Q}_{d-1}[\alpha] = \{P(\alpha); P \in \mathbb{Q}_{d-1}[X]\}$ et $\mathbb{Q}[\alpha] = \{P(\alpha), P \in \mathbb{Q}[X]\}$. Montrer que $\mathbb{Q}[\alpha] = \mathbb{Q}_{d-1}[\alpha]$
3. Montrer que $\mathbb{Q}_{d-1}[\alpha]$ est un corps.

Exercice 8

Montrer que $K = \{a + b\sqrt{2}\}, (a,b) \in \mathbb{Q}^2\}$ est un corps. Déterminer les morphismes d'anneaux de K dans K.

Exercice 9

Calculer $473 \wedge 220$. Donner les solutions dans $\mathbb{Z}^2$ de $473x + 220y = k$ où $k = 1, 11, 22$.

Exercice 10

Quel est le dernier chiffre de l'écriture décimale de 3^{7^5} ?

Exercice 11

Résoudre le système $3x + 7y = 3, 6x - 7y = 0$ dans $\mathbb{Z}/36\mathbb{Z}$ puis dans $\mathbb{Z}/37\mathbb{Z}$.

Exercice 12

Soit G un groupe cyclique engendré par a, de cardinal n.

1. Montrer que tout sous-groupe de G est cyclique, de cardinal divisant n.
2. Soit d un diviseur de n. Montrer que G possède un unique sous-groupe de cardinal d.
3. Démontrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d. En déduire $n = \sum_{d|n} \varphi(d)$.

Exercice 13 ***(Mines MP 2011)***

1. Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tel que $a \wedge n = 1$. Montrer que $a^{\varphi(n)} \equiv 1\,[n]$.
2. Si p est premier et $a \in \mathbb{Z}$, montrer que $a^p \equiv a\,[p]$.
3. Si m et n sont dans $\mathbb{Z}$, montrer que $m^{19}n \equiv n^{19}m\,[798]$.
4. Soient $n \geqslant 2$, $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1\,[n]$ et tel que, pour tout diviseur m de $n-1$ dans $\mathbb{N}^*$ autre que $n-1$, on ait $a^m \not\equiv 1\,[n]$. Montrer que n est premier.

Exercice 14 ***(Radical d'un idéal)***

Soit I un idéal d'un anneau commutatif A. On appelle radical de I l'ensemble $\sqrt{I}$ défini par $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}^*,\ x^n \in I\}$.

1. Montrer que le radical d'un idéal est un idéal.
2. Déterminer le radical d'un idéal de $\mathbb{Z}$.

Exercice 15

Soit p un nombre premier. On pose $Z_p = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}^*,\ p \text{ ne divise pas } b\right\}$, et $J_p = \left\{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{N}^*,\ p \text{ divise } a \text{ et ne divise pas } b\right\}$.

1. Montrer que Z_p est un sous-anneau de $\mathbb{Q}$.
2. 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.
3. Déterminer les idéaux de Z_p.

Exercice 16 ☆

Soit A un anneau commutatif et I un idéal strict de A (distinct de A).

1. Montrer que I est maximal pour l'inclusion parmi les idéaux stricts de A si, et seulement si $\forall a \in A \setminus I,\ I + aA = A$. On dit que I est principal lorsqu'il existe $a \in A$ tel que $I = aA$. On dit que I est premier lorsque $\forall (a,b) \in (A \setminus I)^2,\ ab \in A \setminus I$.
2. Montrer que tout idéal maximal est premier.
3. Etudier la situation dans $\mathbb{Z}$ et dans $K[X]$.
4. Montrer que si A est un anneau principal (c'est-à-dire intègre tel que tout idéal est principal), alors les idéaux premiers et maximaux de A sont les mêmes.
5. Soit $A = \mathscr{C}^\infty(\mathbb{R}, \mathbb{R})$ et $I = \{f \in A \mid f(0) = 0\}$. L'idéal I est-il principal? premier? maximal?
6. Soit $J = \{f \in A \mid \forall k \in \mathbb{N},\ f^{(k)}(0) = 0\}$. Montrer que J est un idéal. Est-il principal? premier? maximal?

Exercice 17 ***(Mines MP 2011)***

Soit A un anneau commutatif. Un idéal de A est dit premier si, pour tout $(x,y)\in A$, $xy\in I\Rightarrow x\in I$ ou $y\in I$.

1. Donner un exemple d'un idéal premier de $\mathbb{Z}$.
2. Si f est un morphisme d'anneau de A dans un corps K, $\ker f$ est-il premier?
3. Que peut-on dire de l'intersection de deux idéaux premiers?
4. On suppose que tous les idéaux de A sont premiers. Montrer que A est intègre. Soit $x\neq 0$. En comparant les idéaux engendrés par x et x^2, montrer que x est inversible.

Exercice 18

1. Montrer que $K=\mathbb{Q}[\sqrt{2}]$ est un corps.
2. Déterminer $\mathrm{Aut}(K)$, l'ensemble des morphismes bijectifs de K sur K (on pourra montrer que $\sqrt{2}$ n'a que deux images possibles).

Exercice 19 ***(Centrale MP 2011)*** ☆

Soit p premier impair.

1. Montrer que le nombre de carrés de $\mathbb{Z}/p\mathbb{Z}$ est $\dfrac{p+1}{2}$ (*indic* : considérer l'application $x\mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$)
2. Montrer que $x\in\mathbb{Z}/p\mathbb{Z}$ est un carré si, et seulement si, $x^{(p+1)/2}=x$ (*Indic :* on pourra s'interesser au polynôme $X^{\frac{p+1}{2}}-X$).
3. Pour quels p la classe de -1 modulo p est-elle un carré de $\mathbb{Z}/p\mathbb{Z}$?
4. Déterminer le cardinal de l'ensemble $S=\{(x,y)\in(\mathbb{Z}/p\mathbb{Z})^2, x^2+y^2=1\}$.

Exercice 20 ***(Centrale MP 2012)***

Soit $\mathbb{Z}[i]=\{a+ib,(a,b)\in\mathbb{Z}^2\}$ et $\nu:\mathbb{Z}[i]\to\mathbb{N}$ définie par $\nu(a+ib)=a^2+b^2$ si $(a,b)\in\mathbb{Z}^2$.

1. Montrer que, pour tout $z_1,z_2\in\mathbb{Z}[i]$, $\nu(z_1z_2)=\nu(z_1)\nu(z_2)$.
2. Déterminer les inversibles de $\mathbb{Z}[i]$.
3. Montrer que 2 est irréductible dans $\mathbb{Z}[i]$.
4. Soit $(z,w)\in\mathbb{Z}[i]\times\mathbb{Z}[i]\setminus\{0\}$. Montrer qu'il existe $(q,r)\in\mathbb{Z}[i]^2$ tels que $z=wq+r$ avec $\nu(r)<\nu(w)$. Ce couple est-il nécessairement unique?
5. Montrer que les idéaux de $\mathbb{Z}[i]$ sont principaux.

Exercice 21 ***(Centrale MP 2013)*** ☆

Soit G un groupe abélien fini. Si $x\in G$, on note $o(x)$ l'ordre de x et $e(G)$ le maximum des $o(x)$ pour $x\in G$.

1. Si $\mathrm{pgcd}(o(x),o(y))=1$, montrer que $o(xy)=o(x)o(y)$.
2. Montrer que $e(G)=ppcm_{x\in G}\,o(x)$.
3. Montrer que $e(G)$ divise $|G|$.
4. Montrer que G est cyclique si et seulement si $e(G)=|G|$.
5. Montrer que $e(G)=\min\{k\in\mathbb{N}^*,\forall x\in G, x^k=1\}$.
6. Déterminer $e(\mathbb{Z}/p\mathbb{Z}^*)$ lorsque p est premier (*indication :* regarder les racines de X^k-1 avec $k=e(G)$). Que peut-on en déduire sur $\mathbb{Z}/p\mathbb{Z}^*$ lorsque p est premier? Déterminer $e(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z})$.
7. Soit G un sous-groupe fini de $(\mathbb{C}^*,\cdot)$. Montrer que G est cyclique.

Exercice 22 ***(Centrale MP 2017)***

Soit $(G,\cdot)$ un groupe fini de cardinal n. On note $\hat{G}$ l'ensemble des morphismes de $(G,\cdot)$ vers $(\mathbb{C}^*,\cdot)$.

1. Dans cette question, on suppose que n est premier. Montrer que G est cyclique, puis que $|\hat{G}|=n$.

   Dans les trois questions suivantes, le groupe G est supposé abélien et sa loi de groupe est notée additivement (le groupe est alors $(G,+)$). On appelle E l'ensemble des fonctions de G vers $\mathbb{C}$.

2. Munir E d'une structure de $\mathbb{C}$-espace vectoriel et préciser sa dimension.
3. Soit $a\in G$. On définit $T_a\in\mathscr{L}(E)$ par $T_a(f)(x)=f(x+a)$ si $f\in E$ et $x\in G$. Montrer qu'il existe une base de E formée de vecteurs propres communs à tous les T_a.
4. En déduire que $|\hat{G}|=n$.
5. Montrer par un exemple que ce résultat tombe en défaut lorsque G n'est plus supposé abélien.

Exercice 23 ***(Mines MP 2021)***

Pour $s \in]1,+\infty[$, soit $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$.

1. Si $n \in \mathbb{N}^*$, soit $d(n)$ le nombre de diviseurs de n dans $\mathbb{N}^*$. Montrer que, si $s > 1$, $\sum_{n=1}^{+\infty} \frac{d(n)}{n^s} = \zeta(s)^2$
2. Pour $s > 2$, montrer que $\sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$

Exercice 24 ***(Mines MP 2019)***

Pour $n \in \mathbb{N}^*$, soit $\sigma(n)$ la somme des diviseurs de n dans $\mathbb{N}^*$. Donner un équivalent de $U_n = \sum_{k=1}^{n} \sigma(k)$.

POLYNÔMES

Exercice 25

Déterminer les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathcal{U}) \subset \mathcal{U}$ où $\mathcal{U} = \{z \in \mathbb{C}, |z| = 1\}$.

Exercice 26 ***(Mines MP 2012)***

Soit $P \in \mathbb{R}[X]$, non nul, tel que $P(X^2) = P(X)P(X-1)$.

1. Montrer que les racines de P sont de module 1.
2. Trouver ces racines.
3. Trouver P.

Exercice 27 ***(Mines MP 2021)***

Soit $P = a_0 + \cdots + a_n X^n \in \mathbb{R}[X]$ un polynôme non constant, scindé à racines simples sur $\mathbb{R}$.

1. Montrer que pour tout $x \in \mathbb{R}$, $P''(x)P(x) - P'(x)^2 < 0$.
2. Soit $k \in \{1,\dots,n-1\}$, montrer que $a_{k-1}a_{k+1} \leqslant a_k^2$.

Exercice 28 ***(Mines MP 2021)***

Soient $n \in \mathbb{N}^*$, $z_1,\dots,z_n$ les racines de X^n+1.
On pose, pour $k \in \{0,\dots,n\}$, $F_k = \frac{X^k}{X^n+1}$.

1. Décomposer F_k en éléments simples.
2. Soit $P \in \mathbb{C}_n[X]$. Montrer : $XP'(X) = \frac{n}{2}P(X) + \frac{2}{n}\sum_{k=1}^{n} \frac{z_k P(z_k X)}{(z_k-1)^2}$.
3. Si $Q \in \mathbb{C}_n[X]$, on pose $\|Q\|_\infty = \max_{|z|\leqslant 1} |Q(z)|$.
4. Montrer que, pour $P \in \mathbb{C}_n[X]$, $\|P'\|_\infty \leqslant n\|P\|_\infty$.

Exercice 29 ***(Mines MP 2019)***

Soit $P \in \mathbb{R}[X]$ de degré n tel que, pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$. On pose $Q = \sum_{k=0}^{n} P^{(k)}$. Montrer que $\forall x \in \mathbb{R}, Q(x) \geqslant 0$.