19 ANNEAUX, ARITHMÉTIQUE

I. IDÉAUX ET $\mathbb{K}[X]$

Définition 61 *(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 $(P)+(Q) = (G) = \{UP+VQ, (U,V) \in \mathbb{K}[X]^2\}$. 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.

II. EXERCICES

GROUPES

ANNEAUX, CORPS

Exercice 4

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 $\mathbb{Q}_{d-1}[\alpha] = \left\{P(\alpha); P \in \mathbb{Q}_{d-1}[X]\right\}$ 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 5

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 6

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

Exercice 7

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

Exercice 8

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

Exercice 9 ***(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 10 ***(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 11

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 12 ***(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 13

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 14 ***(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 15 ***(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 16 ***(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 17 ***(Mines MP 2021)***

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

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

POLYNÔMES

Exercice 18

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 19 ***(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 20 ***(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 21 ***(Mines MP 2021)***

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

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

Exercice 22 ***(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 $Q = \displaystyle\sum_{k=0}^{n} P^{(k)}$. Montrer que $\forall x \in \mathbb{R}, Q(x) \geqslant 0$.