Anneaux euclidiens, principaux, factoriels.

Exercice 1.

Soient K un corps, P un polynôme en une variable à coefficients dans K, α un élément de K et m un entier supérieur ou égal à 1.

1. On suppose que α est racine de P de multiplicité supérieure ou égal à m. Montrer que α annule les dérivées de P jusqu'à l'ordre $m-1$.
2. Montrer que la réciproque n'est pas forcément vraie, et trouver une condition nécessaire et suffisante sur K pour que la réciproque soit toujours vraie.

Exercice 2.

Soit A un anneau intègre.

1. Montrer que si A est fini, alors A est un corps.
2. Montrer que si k est un corps tel que A est muni d'une structure de k-espace vectoriel de dimension finie, compatible avec la multiplication dans A, alors A est un corps.
3. Montrer que si $A[X]$ est principal, alors A est un corps.

Exercice 3.

1. Montrer que les anneaux $\mathbb{Z}[\mathrm{i}]$, $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ et $\mathbb{Z}[\sqrt{2}]$ sont euclidiens. *Indication : choisir un stathme qui est multiplicatif.*
2. Montrer que ce n'est pas le cas de $\mathbb{Z}[\mathrm{i}\sqrt{5}]$.

Exercice 4.

Soit K un corps. Déterminer le PGCD de X^n-1 et X^m-1 dans $K[X]$.

Exercice 5.

En utilisant l'algorithme d'Euclide, calculer le PGCD des polynômes $P(X) = X^4+2X^3-X-2$ et $Q(X) = X^5-5X^3-9X^2-8X-3$ dans $\mathbb{R}[X]$, et en déduire des polynômes U et V de $\mathbb{R}[X]$ tels que $UP+VQ = \mathrm{PGCD}(P,Q)$.

Exercice 6.

Donner un exemple d'anneau...

1. ...intègre mais pas factoriel.
2. ...factoriel mais pas principal.

Remarque : l'exercice 7 décrit un exemple d'anneau principal mais pas euclidien.

Exercice 7.

Soit $\alpha := \frac{1+i\sqrt{19}}{2}$. L'objectif de cet exercice est de prouver que l'anneau $\mathbb{Z}[\alpha]$ est principal mais non euclidien.

1. Montrer que l'anneau $\mathbb{Z}[\alpha]$ est isomorphe à l'anneau quotient $\mathbb{Z}[X]/(X^2-X+5)$.
2. On note N l'application envoyant un élément de $\mathbb{Z}[\alpha] \subset \mathbb{C}$ sur le carré de son module complexe.
   (a) A l'aide de l'application N, déterminer l'ensemble des éléments inversibles de $\mathbb{Z}[\alpha]$.

(b) Montrer que si B est un anneau euclidien, il contient un élément b non inversible tel que la restriction à $B^\times \cup \{0\}$ de la projection naturelle $B \to B/(b)$ soit encore surjective.
(*Indication : Lorsque B n'est pas un corps, on pourra considérer un élément de stathme minimal.*)

(c) Montrer qu'il n'existe pas de morphisme d'anneaux de $\mathbb{Z}[\alpha]$ vers $\mathbb{Z}/n\mathbb{Z}$ lorsque n vaut 2 ou 3.

(d) En conclure que $\mathbb{Z}[\alpha]$ n'est pas euclidien.

3. Montrer que pour tous éléments $a, b \in \mathbb{Z}[\alpha]$ avec $b \neq 0$, il existe alors une paire (q, r) d'éléments de $\mathbb{Z}[\alpha]$ telle que :
— $r = 0$ ou $N(r) < N(b)$;
— ou bien $a = bq + r$, ou bien $2a = bq + r$.
4. Montrer que l'idéal de $\mathbb{Z}[\alpha]$ engendré par 2 est maximal.
5. Montrer que $\mathbb{Z}[\alpha]$ est principal.
(*Indication : On pourra s'inspirer de la démonstration donnée pour les anneaux euclidiens.*)

Exercice 8.

Le but de cet exercice est de montrer que, si A est un anneau euclidien dans lequel la division euclidienne est unique, alors A est un corps ou A est de la forme $k[X]$ avec k un corps. Soit donc A un anneau euclidien, de stathme N'

1. On définit $N : A\backslash\{0\} \to \mathbb{N}$ en posant $N(x)$ la plus petite valeur des $N'(y)$, pour y parcourant les multiples non nuls de x.
   (a) Montrer que N est un stathme euclidien sur A.
   (b) Montrer qu'on a $N(ab) \geqslant N(a)$ pour tous $a, b \in A\backslash\{0\}$.
2. Montrer qu'on a unicité de la division euclidienne si et seulement si $N(a+b) \leqslant \max(N(a), N(b))$ pour tous $a, b \in A$.
3. Montrer qu'on ne perd pas de généralité à supposer que $N(1) = 0$.
   On suppose à présent qu'on a unicité de la division euclidienne.
4. Montrer que $A^\times \cup \{0\}$ est un corps (on pourra commencer par montrer que x est inversible dans A si et seulement si $N(x) = 0$).
5. On suppose que $F := A^\times \cup \{0\}$ est différent de A, et on prend $a \in A$ tel que $N(a)$ est minimal pour les éléments x de A tels que $N(x) \neq 0$. Montrer que tout élément b non nul de A s'écrit de façon unique sous la forme
$$b = q_k a^k + \cdots + q_0,$$
   avec $q_k \neq 0$ et avec pour tout $i \in \{0, \ldots, k\}$, $q_i \in F$.
6. Conclure.