TD2 : Compléments sur les anneaux (3ème partie)

Exercice 1. Soit A un anneau tel que $A[X]$ est factoriel. Montrer que A est factoriel.

Exercice 2. Soit A un anneau factoriel et $K = \mathrm{Fr}(A)$ son corps des fractions. Soient $P, Q \in A[X]$ avec Q primitif.
Montrer que si $Q|P$ dans $K[X]$, alors $Q|P$ dans $A[X]$.

Exercice 3.

1. Soient $n \in \mathbb{N}$ et $p \in \mathbb{N}$ premier.
   (a) Montrer que la valuation p-adique de $n!$ est donnée par $v_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.
   (b) Soit $(n_N \dots n_0)_p$ l'écriture de n en base p, i.e. $n = \sum_{k=0}^{N} n_k p^k$ où $n_k \in \{0; \dots; p-1\}$. Montrer que
   $$v_p(n!) = \frac{n-s}{p-1}, \text{ avec } s = \sum_{k=0}^{N} n_k.$$
   (c) Utiliser les formules précédentes pour montrer que les coefficients binomiaux $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ sont des entiers.
2. Soit A un anneau factoriel et $a, b, c \in A$ tels que $a + b + c = 0$. Soit π un irréductible de A, montrer qu'au moins deux éléments parmi a, b, c ont la même valuation π-adique.
3. Résoudre dans $\mathbb{Z}^3$ l'équation $x^3 + 2y^3 + 4z^3 = 0$.

Exercice 4. Soit A un anneau factoriel et soient $a \in A \setminus \{0\}$ et $m \geq 2$.
Montrer que si $a^m = uv$ avec u et v premiers entre eux dans A, alors il existe $c, d \in A^\times$ et $\bar{u}, \bar{v} \in A$ tels que $u = c\bar{u}^m$ et $v = d\bar{v}^m$.

Exercice 5. On souhaite résoudre l'équation $y^3 - x^2 = 2$ dans $\mathbb{Z}$.

1. En utilisant la même méthode que pour les entiers gaussiens, montrer que $\mathbb{Z}[i\sqrt{2}]$ est euclidien (donc factoriel) et déterminer ses éléments inversibles.
2. Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation $y^3 - x^2 = 2$. Montrer que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$. En déduire que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont des cubes dans $\mathbb{Z}[i\sqrt{2}]$.
3. Conclure.

Exercice 6.

1. Soit $P \in k[X]$ un polynôme unitaire à coefficients dans un corps k.

(a) On suppose dans cette question que k est de caractéristique nulle. Montrer que P et P' sont premiers entre eux si et seulement P est sans facteur carré.
En déduire que P est à racine simple dans toute extension de k si et seulement si P et P' sont premiers entre eux.

(b) Si k est de caractéristique p, montrer que si $Q \in k[X]$ est de dérivée nulle, alors il existe un polynôme $S \in k[X]$ tel que $Q(X) = S(X^p)$. En déduire que l'équivalence précédente est remplacée par :

$$P \text{ et } P' \text{ premiers entre eux } \Leftrightarrow P \text{ sans facteur carré et sans facteur de la forme } S(X^p).$$

2. Soit $P \in \mathbb{Q}[X]$ irréductible. Que peut-on dire de la multiplicité de ses racines dans $\mathbb{C}$?
3. Soient $R_1, R_2 \in \mathbb{Q}[X]$ irréductibles unitaires. Montrer que s'il existe $\alpha \in \mathbb{C}$ tel que $R_1(\alpha) = R_2(\alpha)$, alors $R_1 = R_2$.
4. Soit $P = (X-a)^3(X-b)^2(X-c) \in \mathbb{Q}[X]$ avec a, b, c distincts. Montrer que $a, b, c \in \mathbb{Q}$.

Exercice 7. Soit $P \in \mathbb{R}[X]$. Montrer que

$$\forall x \in \mathbb{R}, P(x) \geq 0 \Leftrightarrow \exists A, B \in \mathbb{R}[X],\ P = A^2 + B^2.$$

Exercice 8 . La notion de factorialité généralise la propriété de décomposition unique en facteurs premiers de $\mathbb{Z}$ mais attention les anneaux factoriels ne vérifient pas toutes les propriétés de $\mathbb{Z}$.

1. Montrer que $k[X, Y]$ et $\mathbb{Z}[X]$ sont des exemples d'anneaux factoriels dans lesquels le théorème de Bézout (i.e. pour tout a, b dans l'anneau, l'idéal (a, b) est principal) n'est pas satisfait.
2. Justifier que $k[X_1, \dots, X_n, \dots]$ est un anneau. Montrer qu'il est factoriel mais pas noethérien.

Exercice 9 . Soit A un anneau intègre. On rappelle qu'un élément $x \in \mathrm{Fr}(A)$ est *entier sur* A s'il existe un polynôme unitaire $Q \in A[X] \subset \mathrm{Fr}(A)[X]$ tel que $Q(x) = 0$.
On dit que A est *intégralement clos* si tout élément de $x \in \mathrm{Fr}(A)$ entier sur A appartient à A.

1. Montrer que tout anneau factoriel est intégralement clos.
2. Soit $d \in \mathbb{Z}^*$ un entier sans facteur carré. Montrer que si $d = 1 \bmod 4$, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos (donc non factoriel). *Indication : considérer l'élément* $\frac{1+\sqrt{d}}{2}$.

Exercice 10. Montrer que $\mathbb{Z}[i\sqrt{d}]$ n'est jamais factoriel si $d \geq 3$. On montrera que le lemme d'Euclide n'est pas satisfait en remarquant que $2 | (d + i\sqrt{d})(d - i\sqrt{d})$.

Exercice 11 . Exemples d'anneaux non factoriels.

1. Dans $\mathbb{Z}[i\sqrt{3}]$, montrer que 4 et $2(1 + i\sqrt{3})$ n'ont ni ppcm ni pgcd. La fraction $4/2(1 + i\sqrt{3})$ admet-elle une unique forme irréductible dans $\mathrm{Fr}(\mathbb{Z}[i\sqrt{3}])$?
2. Dans $k[X^2, X^3]$ montrer qu'il existe trois éléments A, B, C avec A et B premiers entre eux tels que $A|C$, $B|C$ mais $AB \nmid C$.
3. Montrer que $k[X^2, XY, Y^2]$ est noethérien intègre mais pas factoriel.
4. Montrer que $A = \{P \in \mathbb{Q}[X] : P(0) \in \mathbb{Z}\}$ n'est ni factoriel ni noethérien. *Indication : montrer que* 2 *est irréductible dans* A *et utiliser que pour tout* $n \in \mathbb{N}$, $X = 2^n \left(\frac{1}{2^n} X\right) \in A$.

Exercice 12 . Montrer qu'un anneau factoriel vérifiant le théorème de Bézout est principal.

Exercice 13 . Donner toutes les implications entre les propriétés suivantes, où A est un anneau commutatif intègre :

- (P1) : A est euclidien
- (P2) : A est principal
- (P3) : A est noethérien
- (P4) : A est factoriel
- (P5) : A est un anneau de Bézout
- (P6) : A vérifie le lemme de Gauss
- (P7) : A vérifie (E)
- (P8) : A vérifie (U)

Exercice 14. Soit k un corps, étudier l'irréductibilité des polynômes ci-dessous dans $k[X,Y]$:
$Y - X^2, X^2 + Y^2 - 1, X^2 + Y^2 + 1, X^2 - Y^2 - 1, Y^2 - X^3, X^3 - Y^2 - X, XY^3 - X^2Y - Y^2 + X$.

Exercice 15.

1. Soit $p \in \mathbb{N}$ un nombre premier. Montrer que le polynôme $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}[X]$. *Indication : poser $X = Y + 1$ et appliquer Eisenstein avec p.*
2. Soit $A = \mathbb{Z}[T]$. Montrer que le polynôme $X^n - T \in A[X]$ est irréductible.

Exercice 16. Étudier l'irréducibilité des polynômes suivants sur $\mathbb{Z}$ en les réduisant modulo des petits nombres premiers : X^3+4X^2-5X+7 ; $5X^3+3X^2-4X-27$; $X^3-6X^2-4X-13$; $X^3+4X^2-4X+25$; $X^4 + 5X^3 - 3X^2 - X + 7$; $X^4 + 7X^2 + 4X + 1$; $X^6 + X^3 + 1$; $X^7 + X + 1$.

Exercice 17. Soit $P(X) = X^4 + 1 \in \mathbb{Z}[X]$.

1. Montrer que P est irréductible sur $\mathbb{Z}$. *Indication : calculer $P(X + 1)$ et appliquer Eisenstein avec $p = 2$.*
2. Montrer que P est réductible modulo 2, puis pour tout p p premier impair.