Université de Rennes 1 — Année universitaire 2020-2021
Licence de mathématiques
Module Anneaux et arithmétique

**Feuille de TD n°5**

**Exercice 5.1**

Soit $\mathbf{K}$ un corps. Rappelons que si $P = \sum_{n\geqslant 0} a_n T^n$ est un élément non nul de $\mathbf{K}[[T]]$, on pose

$$\nu(P) := \mathrm{Min}\{n \in \mathbf{N}, \quad a_n \neq 0\}.$$

Montrer que $\nu$ est un stathme euclidien sur $\mathbf{K}[[T]]$. Démontrer directement que $\mathbf{K}[[T]]$ est un anneau factoriel (expliciter la liste des irréductibles de $\mathbf{K}[[T]]$ à association près et la décompostion en produits d'irréductibles d'un élément non nul de $\mathbf{K}[[T]]$ ; on pourra comparer avec l'exercice 2.6).

**Exercice 5.2**

Pour chacun des couples $(a, b)$ d'éléments de $\mathbf{Z}[i]$ donnés ci-dessous, calculer un pgcd $\delta$ de $a$ et $b$ et déterminer un couple $(u, v)$ d'éléments de $\mathbf{Z}[i]$ tel que $\delta = a\,u + b\,v$ :

$$(6 + 3\,i, -1 + 7\,i), (35, 9 + 6\,i), (10, 14).$$

**Exercice 5.3**

Montrer que les anneaux suivants sont euclidiens :

1. $\mathbf{Z}[i\sqrt{2}]$ (on pourra s'inspirer de la démonstration de la proposition 6.12 du cours) ;
2. $\mathbf{Z}[\sqrt{2}]$ (on pourra considérer $N\colon a + b\sqrt{2} \mapsto a^2 - 2b^2$) ;
3. $\mathbf{Z}[\sqrt{3}]$.

**Exercice 5.4**

Soit $r$ un entier strictement positif, $p_1, \ldots, p_r$ des nombres premiers et $d$ un entier supérieur à 2.

1. Montrer qu'il existe une infinité de polynômes unitaires irréductibles de degré $d$ de $\mathbf{Z}[X]$ qui sont réductibles modulo tous les $p_i$ (*indication :* lemme chinois).
2. Montrer qu'il existe une infinité de polynômes unitaires irréductibles de degré $d$ de $\mathbf{Z}[X]$ qui sont réductibles modulo tous les $p_i$ et tels que le critère d'Eisenstein ne s'applique pour aucun des $p_i$.

**Exercice 5.5**

Soit $P \in \mathbf{Z}[X]$ et $p$ un nombre premier. On suppose que $P$ est irréductible modulo $p$. $P$ est-il nécessairement irréductible ?

**Exercice 5.6**

Soit $P = X^4 + 1$.

1. Montrer que $P$ est un élément irréductible de $\mathbf{Z}[X]$ (*cf.* l'exercice 3.3).

2. Soit $p$ un nombre premier. En utilisant des identités remarquables, montrer que $P$ est réductible modulo $p$ si l'une des propriétés suivantes est vraie :
   (a) $-1$ est un carré modulo $p$ ;
   (b) $2$ est un carré modulo $p$ ;
   (c) $-2$ est un carré modulo $p$.
3. Soit $\mathbf{K}$ un corps fini. Soit $\alpha, \beta \in \mathbf{K}$ des éléments qui ne sont pas des carrés dans $\mathbf{K}$. Montrer qu'alors $\alpha\beta$ est un carré dans $\mathbf{K}$.
4. En déduire que pour tout nombre premier $p$, $X^4 + 1$ est réductible modulo $p$.

**Exercice 5.7**

1. Soit $A$ un anneau factoriel, $d$ un entier, $P = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme de degré au plus $d$. Soit $x \in \operatorname{Frac}(A)$ une racine de $P$ dans $\operatorname{Frac}(A)$. Montrer qu'on peut écrire $x = \frac{\alpha}{\beta}$, où $\alpha \in A$ et $\beta \in A \setminus \{0\}$ sont premiers entre eux. Montrer que $\alpha$ divise $a_0$ et que $\beta$ divise $a_d$.
2. Le polynôme $7\,X^3 - 5\,X^2 - 9\,X + 4$ a-t-il des racines rationnelles ? et le polynôme $X^4 - 2X^2 - 3$ ?
3. Montrer, par au moins trois méthodes différentes, que les polynômes $X^2 + 3X - 15$ et $X^3 - 7X^2 + 14X - 7$ sont des éléments irréductibles de $\mathbf{Z}[X]$.
4. Montrer, par au moins deux méthodes différentes, que le polynôme $X^4 + 5X^3 - 15X^2 + 25X + 15$ est un élément irréductible de $\mathbf{Z}[X]$.

**Exercice 5.8**

1. Soit $A$ un anneau intègre, $P \in A[X]$ et $a \in A$. Montrer que $P$ est irréductible si et seulement si $P(X + a)$ est irréductible.
2. Soit $p$ un nombre premier. Montrer que le polynôme $\frac{X^p - 1}{X - 1} \in \mathbf{Z}[X]$ est irréductible
3. Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et $\alpha \in \mathbf{K}^{\times}$. Montrer que $X^2 + Y^2 - \alpha^2$ est un élément irréductible de $\mathbf{K}[X, Y]$. En déduire que pour tout entier $n \geqslant 2$, $\sum_{i=1}^{n} X_i^2 - \alpha^2$ est un élément irréductible de $\mathbf{K}[X_1, \ldots, X_n]$. (on pourra considérer le morphisme de $\mathbf{K}[X_1, \ldots, X_{n-1}]$-algèbres $\mathbf{K}[X_1, \ldots, X_n] \to \mathbf{K}[X_1, \ldots, X_{n-1}]$ qui envoie $X_n$ sur 0).

**Exercice 5.9**

Dans le critère d'Eisenstein, pourquoi est-il important de supposer $\pi$ irréductible ? (question posée à l'oral de l'agrégation externe).

**Exercice 5.10**

Soit $A$ un anneau intègre.

1. Soit $a$ et $b$ des éléments de $A$ premiers entre eux. Montrer que l'ensemble des pgcd de $a$ et $b$ est $A^{\times}$.
2. Soit $a$ et $b$ des éléments associés de $A$. Montrer que l'ensemble des pgcd de $a$ et $b$ est l'ensemble des éléments de $A$ associés à $a$.
3. Soit $a \in A$. Montrer que l'ensemble des pgcd de $a$ et $0$ est l'ensemble des éléments de $A$ associés à $a$.

4. Soit $a, b \in A$. Montrer que $a$ et $b$ admettent un ppcm si et seulement si l'idéal $aA \cap bA$ est principal, et qu'alors l'ensemble des ppcm de $a$ et $b$ est l'ensemble $\{c \in A, \quad cA = aA \cap bA\}$.
5. Soit $a, b \in A$. On suppose que $a$ et $b$ admettent un pgcd $\delta$ (respectivement un ppcm $\mu$).
   (a) Soit $c \in A$. Montrer que $c$ est un pgcd (respectivement un ppcm) de $a$ et $b$ si et seulement si $c$ est associé à $\delta$ (respectivement à $\mu$).
   (b) Soit $\alpha \in A$. Montrer que $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de $\alpha\, a$ et $\alpha\, b$.
   (c) Soit $\alpha \in A \setminus \{0\}$ un diviseur commun à $a$ et $b$. Montrer que $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de $\frac{a}{\alpha}$ et $\frac{b}{\alpha}$.
   En déduire que $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux.
6. Soit $a, b \in A$. On suppose que $a$ et $b$ admettent un ppcm $\mu$. Montrer qu'alors $a$ et $b$ admettent un pgcd $\delta$, et que $\delta\mu$ est associé à $ab$.
7. Montrer que dans l'anneau $\mathbf{Z}[i\sqrt{5}]$, les éléments 2 et $1 + i\sqrt{5}$ sont premiers entre eux mais n'ont pas de ppcm, et que les éléments 9 et $2 + i\sqrt{5}$ n'ont pas de pgcd (donc pas de ppcm).

**Exercice 5.11**

En utilisant par exemple l'identité $2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ dans $\mathbf{Z}[i\sqrt{3}]$ et l'exercice 3.5, montrer qu'en général dans un anneau intègre un produit d'éléments premiers entre eux et qui ne sont pas des carrés peut néanmoins être un carré.

**Exercice 5.12**

Soit $\mathbf{K}$ un corps. Montrer que les anneaux suivants sont intègres mais ne sont pas factoriels :
1. $\mathbf{K}[X, Y]/\langle X^2 - Y^3 \rangle$ ;
2. le sous-$\mathbf{K}$ espace vectoriel de la $\mathbf{K}$-algèbre $\mathbf{K}[X, Y]$ engendré par les éléments de la forme $X^i Y^j$ où $i, j \in \mathbf{N}$ et $i + j$ est pair ;
3. $\mathbf{Z}[i\sqrt{5}]$ (*cf.* exercice 5.10.7).

**Exercice 5.13**

Soit $A$ est un anneau intègre. Montrer que l'anneau $A[X]$ est principal si et seulement si $A$ est un corps.

**Exercice 5.14**

Soit $A$ un anneau factoriel. Montrer que l'ensemble des éléments irréductibles de $A[X]$ est la réunion disjointes des deux ensembles suivants :
1. l'ensemble des polynômes constants qui sont des éléments irréductibles de $A$ ;
2. l'ensemble des polynômes qui sont primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

**Exercice 5.15**

Soit $A$ un anneau intègre et $S$ une partie multiplicative de $A$ ne contenant pas $0_A$.
1. On suppose $A$ principal ; montrer qu'alors $S^{-1}A$ est principal.
2. On suppose $A$ factoriel ; montrer qu'alors $S^{-1}A$ est factoriel.