M1 MPA : Algèbre et Arithmétique 2016–2017
Feuille d'exercices n° 3

I. Soit R un anneau factoriel et $a, b, c \in R$ trois éléments non nuls. Montrer que si on a $\operatorname{pgcd}(a, b) = 1$, alors on a $\operatorname{pgcd}(ac, bc) = c$.

II. Soit R un anneau factoriel tel que pour tout $a, b \in A$ l'idéal (a, b) engendré par a et b est principal. Montrer que R est principal. (Attention. On ne suppose pas que R est noethérien.)

III. Montrer que l'anneau $\mathbf{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbf{Z}\}$ est isomorphe à $\mathbf{Z}[X]/(X^2 - 3)$. Est-il intègre ?

IV. Soit B un anneau, et $P \in B[X]$ un polynôme non nul. Trouver une condition sur les coefficients de P qui permet de conclure que pour tout $F \in B[X]$ il existe $Q, R \in B[X]$ avec $F = PQ + R$ et $R = 0$ ou $\deg R < \deg P$.

V. Soit $A = \mathbf{C}[X, Y]/(Y^2 - X^3)$. Considérons le morphisme d'anneaux

$$\begin{array}{rcl} \varphi\colon \mathbf{C}[X, Y] & \to & \mathbf{C}[T] \\ F(X, Y) & \mapsto & F(T^2, T^3). \end{array}$$

(a) Montrer qu'on a $\ker \varphi = (Y^2 - X^3)$. En déduire que A est isomorphe à un sous-anneau de $\mathbf{C}[T]$.

(b) L'anneau A est-il intègre ?

(c) Montrer que l'image de φ est $R = \mathbf{C}[T^2, T^3]$.

(d) En trouvant deux factorisations différentes de T^6 dans R, montrer que R n'est pas factoriel.

(e) Donner des $\mathbf{C}$-bases des idéaux (T^2), (T^3) et $(T^2) \cap (T^3)$ de R. Les éléments T^2 et T^3 ont-ils un ppcm dans R ?

(f) Les éléments T^5 et T^6 ont-ils un pgcd dans R ?

VI. Montrer que les anneaux $\mathbf{C}[X, Y]/(Y - X^2)$ et $\mathbf{C}[X, Y]/(XY - 1)$ sont principaux. (Trouver des anneaux plus simples auxquels ils sont isomorphes.)

VII. Soit n un entier qui n'est pas un carré. Pour $z = x + y\sqrt{n} \in \mathbf{Q}[\sqrt{n}]$ avec $x, y \in \mathbf{Q}$ on pose $\tilde{z} = x - y\sqrt{n}$ et $N(z) = z\tilde{z}$. Montrer les énoncés suivants.

(a) L'application $z \mapsto \tilde{z}$ est un automorphisme de l'anneau $\mathbf{Q}[\sqrt{n}]$.

(b) Pour tout $z \in \mathbf{Q}[\sqrt{n}]$ on a $N(z) \in \mathbf{Q}$. De plus on a $N(zz') = N(z)N(z')$, et on a $N(z) = 0$ ssi on a $z = 0$.

(c) $\mathbf{Q}[\sqrt{n}]$ est un corps.

(d) Les inversibles de $\mathbf{Z}[\sqrt{n}]$ sont les $z \in \mathbf{Z}[\sqrt{n}]$ avec $N(z) = \pm 1$.

(e) Il existe des factorisations en irréductibles dans $\mathbf{Z}[\sqrt{n}]$.

(f) Pour tout $x, y \in \mathbf{Z}[\sqrt{2}]$ avec $y \neq 0$ il existe $q, r \in \mathbf{Z}[\sqrt{2}]$ avec $x = qy + r$ et $N(r) < N(y)$.

(g) L'anneau $\mathbf{Z}[\sqrt{-3}]$ n'est pas factoriel.

(h) L'anneau $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ est euclidien.

VIII. (*Entiers de Gauss irréductibles et sommes de deux carrés*) Soit $\mathbf{Z}[i] = \{m + ni \mid m, n \in \mathbf{Z}\}$ l'anneau des entiers de Gauss. Pour $z \in \mathbf{Z}[i]$ on pose $N(z) = |z|^2 \in \mathbf{N}$. On note S l'ensemble d'entiers n qui s'écrivent sous la forme $n = a^2 + b^2$ avec $a, b \in \mathbf{N}$.

(a) Montrer que $\mathbf{Z}[i]$ est un anneau intègre isomorphe à $\mathbf{Z}[X]/(X^2 + 1)$.

(b) Quels sont les inversibles de $\mathbf{Z}[i]$? Utiliser la multiplicativité de N pour déduire l'identité de Diophantos

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

(c) Montrer que $\mathbf{Z}[i]$ est euclidien avec N un stathme euclidien.

(d) Montrer que S est la réunion de $\{0\}$ et du sous-monoïde de $(\mathbf{N} \smallsetminus \{0\}, \cdot, 1)$ engendré par les normes des irréductibles de $\mathbf{Z}[i]$.

(e) Soit p un nombre premier qui s'écrit sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbf{N}$. Montrer que $a + bi$ et $a - bi$ sont des irréductibles de $\mathbf{Z}[i]$.

(f) Soit p un nombre premier. Montrer qu'on a $p \in S$ ssi p n'est pas irréductible dans $\mathbf{Z}[i]$.

(g) Montrer qu'aux associés près les deux derniers points donnent tous les irréductibles de $\mathbf{Z}[i]$.

(h) Montrer que si on a $n \equiv 3 \pmod 4$, alors on a $n \notin S$. (Quels sont les carrés modulo 4 ?)

(i) Soit p un nombre premier avec $p \equiv 1 \pmod 4$. Montrer que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$. (Rappel : Pour F un corps commutatif, tout sous-groupe fini de $F^\times$ est cyclique.)

(j) Pour I, J des idéaux d'un anneau R, montrer qu'on a des isomorphismes d'anneaux $\frac{R/I}{(I+J)/I} \cong R/(I + J) \cong \frac{R/J}{(I+J/J}$.

(k) En déduire que p est irréductible dans $\mathbf{Z}[i]$ ssi $X^2 + 1$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$.

En déduire :

Théorème de deux carrés (Girard, Fermat, Euler)**.** *Un entier naturel non nul est la somme de deux carrés si et seulement si dans sa factorisation en premiers les premiers congrus à* 3 *modulo* 4 *figurent avec une exposante paire.*

Pour information :

Théorème de trois carrés (Legendre, 1797–1798)**.** *Un entier naturel est la somme de trois carrés si et seulement si ce n'est pas de la forme* $4^k m$ *avec* $m \equiv 7 \pmod 8$.

Théorème de quatre carrés (Lagrange, 1770)**.** *Tout entier naturel est la somme de quatre carrés.*