Feuille 5 – Anneaux intégralement clos

Exercice 1.

1. Montrer que tout anneau factoriel est intégralement clos.
2. Montrer que l'anneau des fonctions holomorphes sur $\mathbb{C}$ est intégralement clos, mais non factoriel.
3. Soit $A = \mathbb{C}[X,Y]/(Y^2 - X^3)$. Montrer que A est intègre, de corps de fractions isomorphe à $\mathbb{C}(T)$. En déduire que A n'est pas intégralement clos.

Exercice 2. Soit K un corps de dimension 2 sur $\mathbb{Q}$ (en tant qu'espace vectoriel).

1. Montrer qu'il existe un entier d sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$, et en déduire qu'il n'existe qu'un seul automorphisme de corps non trivial $\sigma : K \to K$.
2. Montrer que pour tout $x \in K$ entier sur $\mathbb{Z}$, l'élément $\sigma(x)$ est aussi entier sur $\mathbb{Z}$; en déduire que $x = a + b\sqrt{d}$ est entier sur $\mathbb{Z}$, si, et seulement si $2a$ et $a^2 - db^2$ sont tous les deux des entiers (rationnels, c'est-à-dire des éléments de $\mathbb{Z}$).
3. En déduire que l'anneau des entiers de K est $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2$ ou $3 \bmod 4$, et $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ sinon (remarquons que d ne peut pas être divisible par 4).
4. En particulier, $\mathbb{Z}[i\sqrt{5}]$ est intégralement clos. Montrer qu'il n'est pas factoriel.

Exercice 3. Soit A un anneau intègre de corps de fractions K, et soit L un corps de dimension n sur K. Soient $x \in L$, et x_1, ..., x_n les racines du polynômes minimal de x sur K (prises dans une clôture algébrique de K). On note $m_x : L \to L$ l'endomorphisme de multiplication par x. C'est une application K-linéaire ; sa trace et son déterminant sont donc des éléments de K.

1. Montrer que $\mathrm{Tr}(m_x) = [L : K(x)] \sum_{i=1}^{n} x_i$ et $\det(m_x) = \left(\prod_{i=1}^{n} x_i\right)^{[L:K(x)]}$. En déduire que si x est entier sur A, alors $\mathrm{Tr}(m_x)$ et $\det(m_x)$ également.
   On considère le cas $A = \mathbb{Z}$ (donc $K = \mathbb{Q}$) dans toutes les questions suivantes.
2. Montrer que la forme $\mathbb{Q}$-bilinéaire $(x,y) \mapsto \mathrm{Tr}(m_{xy})$ est non dégénérée, et en déduire que l'anneau des entiers d'un corps de nombres L est un $\mathbb{Z}$-module de rang $[L : \mathbb{Q}]$.
3. Soit $x \in L$ un entier sur $\mathbb{Z}$. Montrer que $1/x$ est entier sur $\mathbb{Z}$ si, et seulement si $|\det(m_x)| = 1$.
4. Soit p un nombre premier, et soit $\zeta_p = \exp\left(\frac{2i\pi}{p}\right)$.
   (a) Montrer que $(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}$ (on peut commencer par montrer que $p = \varepsilon(1-\zeta_p)^{p-1}$, où $\varepsilon \in \mathbb{Z}[\zeta_p]^\times$).
   (b) Montrer que si $z = \sum_{i=0}^{p-2} a_i \zeta_p^i$ est un entier algébrique, alors $\mathrm{Tr}((1-\zeta_p)z)$ est un multiple entier de p. En déduire que l'anneau des entiers de $\mathbb{Q}(\zeta_p)$ est $\mathbb{Z}[\zeta_p]$.
5. On veut montrer que l'anneau $\mathbb{Z}[\sqrt[3]{2}]$ est intégralement clos.
   (a) Montrer qu'il est entier sur $\mathbb{Z}$.
   (b) Soit $z = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$ un élément entier sur $\mathbb{Z}$. En calculant la trace de m_z, $m_{\sqrt[3]{2}z}$ et $m_{(\sqrt[3]{2})^2 z}$ (vues comme applications $\mathbb{Q}$-linéaires), montrer que $6z \in \mathbb{Z}[\sqrt[3]{2}]$.
   (c) Montrer que $6a$, $6b$ et $6c$ sont des multiples de 6, et conclure.

Exercice 4. L'objectif de cet exercice est de démontrer un cas particulier du théorème d'Ax-Grothendieck, à savoir : une $P : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale (c'est-à-dire dont toutes les coordonnées sont polynomiales) est injective si, et seulement si elle est bijective. On abrégera $(x_1, \dots, x_n)$ en $\vec{x}$, et de même pour $(y_1, \dots, y_n)$ qu'on écrira $\vec{y}$. Dans le même esprit, la lettre X désignera $(X_1, \dots, X_n)$, et Y désignera $(Y_1, \dots, Y_n)$.

1. Montrer que le théorème est vrai si l'on remplace $\mathbb{C}$ par un corps fini.
2. Notons P_i les coordonnées de P, supposée injective. À l'aide du Nullstellensatz, montrer que pour tout $j \in [\![1, n]\!]$, il existe un entier $r_j \geqslant 1$ et des polynômes $Q_{ij} \in \mathbb{C}[X, Y]$ tels que :
$$\forall (\vec{x}, \vec{y}) \in (\mathbb{C}^n)^2, \quad \sum_{i=1}^{n} (P_i(\vec{x}) - P_i(\vec{y})) \cdot Q_{ij}(\vec{x}, \vec{y}) = (x_j - y_j)^{r_j} .$$
3. Raisonnons par l'absurde, et supposons que P soit injective, sans pour autant être surjective. Soit $\vec{z_0} = (\vec{z}_{01}, \ldots, \vec{z}_{0n}) \in \mathbb{C}^n$ tel que $P(\vec{x}) = \vec{z_0}$ n'ait pas de solution sur $\mathbb{C}^n$. Montrer qu'il existe des polynômes $R_i \in \mathbb{C}[X]$ tels que : $\forall \vec{x} \in \mathbb{C}^n, \quad \sum\limits_{i=1}^{n} (P_i(\vec{x}) - \vec{z}_{0i}) \cdot R_i(\vec{x}) = 1.$
Soit $\mathbb{Z}[\mathcal{C}]$ le sous-anneau de $\mathbb{C}$ engendré par les coefficients des P_i, Q_i, R_i et $\vec{z_0}$. Considérons $\mathfrak{M}$ un idéal maximal de $\mathbb{Z}[\mathcal{C}]$. L'objectif des prochaines questions est de montrer que le quotient $k = \mathbb{Z}[\mathcal{C}]/\mathfrak{M}$ est un corps fini.
4. On suppose que k est de caractéristique nulle. Montrer que sous cette hypothèse, $\mathbb{Q}$ doit avoir un nombre fini de générateurs. En déduire que k est de caractéristique $p > 0$. On peut alors écrire $\mathbb{Z}/p\mathbb{Z} \subseteq k$.
5. Posons $\mathbb{Z}[\mathcal{C}] = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$, où les α_m sont des nombres complexes. Soit J le noyau du morphisme surjectif $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \ldots, X_m] \to \overline{k}$, défini par $X_i \mapsto \alpha_i \bmod \mathfrak{M}$. Montrer que $\overline{\mathbb{Z}/p\mathbb{Z}}[X_1, \ldots, X_m]/J$ est un corps isomorphe à $\overline{\mathbb{Z}/p\mathbb{Z}}$.
6. En déduire que les $\alpha_i \bmod \mathfrak{M}$ sont algébriques sur $\mathbb{Z}/p\mathbb{Z}$, puis que k est un corps fini. Conclure.