Feuille 11 – Anneaux de Dedekind

Dans tous les exercices de cette feuille, A désigne un anneau de Dedekind.

Exercice 1.

1. Soit K un corps. L'anneau $K[X,Y]$ est-il de Dedekind ? Déterminer $(X,Y)^{-1}$.
2. Soit $P \in \mathbb{C}[X,Y]$. Montrer que $\mathbb{C}[X,Y]/(P)$ est un anneau de Dedekind si, et seulement si $\left(P, \frac{dP}{dX}, \frac{dP}{dY}\right) = \mathbb{C}[X,Y]$.

Exercice 2. Démontrer qu'un anneau de Dedekind est factoriel si, et seulement s'il est principal.

Exercice 3. Soient $I, J \subseteq A$ deux idéaux. Montrer que l'application bilinéaire $(i,j) \in I \times J \mapsto ij \in IJ$ induit un isomorphisme $I \otimes_A J \simeq IJ$. Et si A n'est pas de Dedekind ?

Exercice 4. Montrer qu'un anneau intègre tel que tout idéal non nul s'écrive comme produit d'idéaux premiers est de Dedekind.

Exercice 5. Montrer que tout idéal d'un anneau de Dedekind est engendré par au plus deux éléments.

Exercice 6. Soit $\mathfrak{p}$ un idéal premier non nul de A, et soit $i \in \mathbb{N}$ un entier naturel.

1. Expliquer comment munir l'espace $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ d'une structure naturelle d'espace vectoriel sur $A/\mathfrak{p}$.
2. Fixons un élément $a \in \mathfrak{p}^i$ n'appartenant pas à $\mathfrak{p}^{i+1}$ et posons, pour tout $x \in A$, $\varphi_i(x) := ax + \mathfrak{p}^{i+1}$. Montrer que l'application $\varphi_i : A \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ ainsi définie induit un isomorphisme de $A/\mathfrak{p}$-espaces vectoriels entre $A/\mathfrak{p}$ et $\mathfrak{p}^i/\mathfrak{p}^{i+1}$.

Exercice 7. (Modules sans torsion sur un anneau de Dedekind) Soit M un A-module de type fini sans torsion.

1. Notons K le corps de fractions de A ; on note M_K le localisé de M en l'idéal premier (0). Pour $m \in M$ et $x \in K$, on a *a priori* $xm \in M_K$; on note $J_m = \{x \in K \mid xm \in M\} \subseteq K$ et $M_m = \{xm \mid x \in J\} \subseteq M$.
   (a) Montrer que J_m est un idéal fractionnaire contenant A.
   (b) Montrer que J_m est un A-module projectif de type fini.
   (c) Montrer que M/M_m est un A-module de type fini sans torsion.
2. Montrer que $M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$, où les $\mathfrak{a}_k$ sont des idéaux non nuls de A.
3. Soit M un A-module de type fini. Montrer que les conditions suivantes sont équivalentes :
   – M est un A-module projectif ;
   – M est un A-module sans torsion ;
   – $M \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ où les $\mathfrak{a}_k$ sont des idéaux non nuls de A.
4. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls de A, montrer qu'il existe un isomorphisme de A-modules $\mathfrak{a} \oplus \mathfrak{b} \simeq A \oplus \mathfrak{a}\mathfrak{b}$, en commençant par le cas particulier où $\mathfrak{a}$ et $\mathfrak{b}$ sont étrangers.
5. Montrer que tout A-module projectif de type fini (et non nul) est isomorphe à un module de la forme $A^{n-1} \oplus \mathfrak{a}$, où $\mathfrak{a}$ est un idéal non nul de A ; on précisera la forme de $\mathfrak{a}$ quand le module est de la forme $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ comme ci-dessus.
6. Montrer que si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls de A tels que $A^{n-1} \oplus \mathfrak{a} \simeq A^{n-1} \oplus \mathfrak{b}$ alors $\mathfrak{a}$ et $\mathfrak{b}$ sont dans la même classe d'équivalence d'idéaux fractionnaires (on pourra considérer la puissance extérieure n-ième de ces A-modules).

Exercice 8. (Théorème d'approximation forte) Soit K le corps des fractions de A. Nous allons démontrer ce théorème : soit $n \geqslant 1$ un entier et soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ des idéaux premiers non nuls de A deux à deux distincts. Fixons des éléments $x_1, \ldots, x_n$ de K (non nécessairement distincts) et des entiers relatifs $v_1, \ldots, v_n$. Il existe alors un élément $x \in K$ vérifiant les conditions suivantes :

- pour tout $i \in [\![1, n]\!]$, $v_{\mathfrak{p}_i}(x - x_i) \geqslant v_i$;
- pour tout idéal premier non nul $\mathfrak{p}$ de A distinct de $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, on a $v_p(x) \geqslant 0$.

1. Soient $I_1, \ldots, I_r$ des idéaux non nuls de A deux à deux étrangers. Démontrer que l'application naturelle de projection $A \to \prod_{k=1}^{r} A/I_k$ est un morphisme d'anneaux surjectif.
2. Démontrer que pour tous idéaux premiers non nuls distincts $\mathfrak{p}$ et $\mathfrak{q}$ de A, et pour tous entiers naturels $m_1, m_2 \in \mathbb{N}^*$, les idéaux $\mathfrak{p}^{m_1}$ et $\mathfrak{q}^{m_2}$ sont étrangers dans A.
3. En déduire que le théorème est vrai lorsque les éléments $x_1, \ldots, x_n$ sont choisis dans A.
4. Compléter ce qui précède pour obtenir une preuve générale du théorème d'approximation forte.
5. Déduire de ce théorème qu'un anneau de Dedekind n'ayant qu'un nombre fini d'idéaux premiers est principal.

Exercice 9. Soit K le corps des fractions de A. Notons $\mathrm{Spm}(A)$ l'ensemble des idéaux premiers non nuls de A.

1. Démontrer l'équivalence des assertions suivantes pour I idéal entier non nul de A et $\mathfrak{p} \in \mathrm{Spm}(A)$:
   - la valuation $\mathfrak{p}$-adique de I est non nulle ;
   - l'idéal $\mathfrak{p}$ apparaît dans la décomposition en idéaux maximaux de l'idéal I ;
   - l'idéal I est inclus dans $\mathfrak{p}$.
2. Démontrer que pour tout idéal fractionnaire non nul J de A et pour tout idéal premier non nul $\mathfrak{p} \subseteq A$, on a $v_{\mathfrak{p}}(J) = \inf\{v_{\mathfrak{p}}(x) \mid x \in J\}$.
3. Démontrer que pour tout élément x de K et pour tout idéal premier non nul $\mathfrak{p} \subseteq A$, on a $v_{\mathfrak{p}}(x) = \max\{n \in \mathbb{N} \mid x \in \mathfrak{p}^n\}$.
4. Démontrer qu'on a également $A = \{x \in K \mid \forall \mathfrak{p} \in \mathrm{Spm}(A), v_{\mathfrak{p}}(x) \geqslant 0\}$.
5. Montrer que pour tout élément non nul x de K, l'ensemble $\{\mathfrak{p} \in \mathrm{Spm}(A) \mid v_{\mathfrak{p}}(x) \neq 0\}$ est fini.

On sait que l'ensemble $I(A)$ des idéaux fractionnaires de A forme un groupe. Soit $P(A)$ l'ensemble de ses idéaux (fractionnaires) principaux, on note $\mathrm{Cl}(A) = I(A)/P(A)$ le groupe des classes des idéaux de A. On admet qu'il s'agit d'un groupe fini si A est l'anneau des entiers d'un corps de nombres.

Exercice 10. Soit p un nombre premier impair qui ne divise pas le cardinal de $\mathrm{Cl}(\mathbb{Z}[\zeta_p])$, pour $\zeta_p = \exp\left(\frac{2i\pi}{p}\right)$ (par exemple tout nombre premier $p < 37$ convient). Soit $(x, y, z) \in \mathbb{Z}^3$ une solution de l'équation $x^p + y^p = z^p$, telle que x, y et z soient premiers entre eux dans leur ensemble, et telle que p ne divise pas xyz.

1. Montrer que si $p = 3$, alors une telle solution ne peut pas exister (raisonner modulo 3 et 9).
2. On suppose $p > 3$. Justifier que $x + \zeta_p^i y$ et $x + \zeta_p^j y$ sont premiers entre eux pour $i \not\equiv j \bmod p$. En déduire que l'idéal engendré par $x + \zeta_p y$ égale I^p pour I un idéal de $\mathbb{Z}[\zeta_p]$.
3. En déduire que $x + \zeta_p y = \varepsilon \alpha^p$, où $\alpha \in \mathbb{Z}[\zeta_p]$ et ε est inversible dans $\mathbb{Z}[\zeta_p]$.
4. Montrer qu'une unité de $\mathbb{Z}[\zeta_p]$ est de la forme $\zeta_p^s \eta$, où $\eta \in \mathbb{Z}[\zeta_p] \cap \mathbb{R}$. En déduire la congruence : $\zeta_p^{-s} x + \zeta_p^{1-s} y \equiv \zeta_p^s x + \zeta_p^{s-1} y \bmod p\mathbb{Z}[\zeta_p]$.
5. Montrer que $x \equiv y \equiv -z \bmod p$. En déduire que l'équation $x^p + y^p = z^p$ n'admet pas de solutions telles que p ne divise pas xyz.