Feuille 6 – Anneaux de Dedekind

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

Exercice 1. Soit K un corps. L'anneau $K[X,Y]$ est-il de Dedekind ?

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

Exercice 3. Soit I un idéal fractionnaire de A. Démontrer que le A-module I peut être engendré par au plus deux éléments.

Exercice 4. Soient K le corps des fractions de A et $\mathfrak{p}$ un idéal premier non nul de A. Démontrer que le localisé en $\mathfrak{p}$ d'un idéal fractionnaire J de A est un idéal fractionnaire de $A_\mathfrak{p}$ et que l'on a de plus $v_\mathfrak{p}(J) = v_\mathfrak{p}(J_\mathfrak{p})$.

Exercice 5. 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 fractionnaire 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.

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. Soit K le corps des fractions de A. Nous allons démontrer le théorème d'approximation forte : 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 8. Soit K un corps complet pour une valuation discrète v dont on note A l'anneau de la valuation. Notons $|\cdot|$ l'application définie sur K par $|x| := e^{-v(x)}$.

1. Vérifier que $|\cdot|$ définit une valeur absolue ultramétrique sur K.
2. Considérons un polynôme $P \in A[X]$ et un élément $x_0 \in A$ vérifiant $|P(x_0)| < |P'(x_0)|^2$. Posons $c := \frac{|P(x_0)|}{|P'(x_0)|^2}$, et considérons la suite $(x_n)_{n\geqslant 0}$ définie par la relation suivante :
$$\forall n \geqslant 0, \quad x_{n+1} = x_n - P'(x_n)^{-1}P(x_n).$$
   (a) Montrer que pour tout entier $n \geqslant 0$, x_n définit bien un élément de A et qu'il vérifie $|P'(x_n)| = |P'(x_0)|$, ainsi que
$$\frac{|P(x_n)|}{|P'(x_n)|^2} \leqslant c^{2^n}.$$
   (b) En déduire que la suite $(x_n)_{n\geqslant 0}$ converge dans A vers une racine x de P vérifiant $|x-x_0| < 1$.
   (c) En conclure que si $|P'(x_0)| = 1 > |P(x_0)|$, alors P a une racine x dans A vérifiant $|x-x_0| < 1$.
3. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et soit p un entier premier. Supposons qu'il existe un élément $x \in \mathbb{Z}/p\mathbb{Z}$ vérifiant $P(x) \equiv 0 \bmod p$ et $P'(x) \not\equiv 0 \bmod p$. Démontrer que P admet une racine dans $\mathbb{Z}_p$ qui est congrue à x modulo p.

Exercice 9. Soit K un corps complet pour une valuation discrète v, dont on note A l'anneau de la valuation et $\mathfrak{m}$ l'idéal maximal. Fixons une uniformisante π de A et S un système de représentants dans A des éléments de $A/\mathfrak{m}$. Démontrer que tout élément de A s'écrit de manière unique comme une série convergente de la forme $\sum_{n\geqslant 0} s_n\pi^n$ avec $s_n \in S$ pour tout entier $n \geqslant 0$.

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 $\mathrm{Div}(A) = I(A)/P(A)$ 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. Quel est le groupe des classes d'un anneau de valuation discrète ? Et d'un anneau principal ?

Exercice 11. Soit p un nombre premier impair qui ne divise pas le cardinal de $\mathrm{Div}(\mathbb{Z}[\zeta_p])$, pour $\zeta_p = \exp\left(\frac{2i\pi}{p}\right)$ (par exemple $p = 37$ 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.