Feuille 1 : Valuations, anneaux de Dedekind

Exercice 1. Une valeur absolue $|\cdot|$ est dite *non-archimédienne* si elle vérifie l'inégalité ultramétrique

$$|x+y| \leq \max(|x|, |y|).$$

Montrer que $|\cdot|$ est non-archimédienne si et seulement si la restriction de $|\cdot|$ à $\mathbb{Z}$ est bornée.

Exercice 2. Soit K un corps et soient $|\cdot|_1$ et $|\cdot|_1$ deux valeurs absolues de K. On suppose que $|\cdot|_1$ et $|\cdot|_2$ définissent la même topologie. Montrer qu'elles sont équivalentes, c'est-à-dire qu'il existe $e > 0$ tel que $|\cdot|_2 = |\cdot|_1^e$.

Exercice 3. Soit K un corps et soit $|\cdot|$ une valeur absolue non triviale de K. Notons A l'ensemble des suites de Cauchy de K et I le sous-ensemble de A formé par les suites qui convergent vers 0.

1. Montrer que A est un anneau, que I est un idéal de A et que les suites constantes identifient K à un sous-anneau de A.
2. Montrer que la topologie de K s'étend à A, que I est fermé dans A et que A/I est un corps qui étend K. On peut montrer que le corps A/I est le complété de K pour $|\cdot|$.
3. Soit $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ des valeurs absolues non triviales de K deux à deux non équivalentes. Montrer qu'il existe $\theta \in K$ tel que $|\theta|_1 > 1$ et $|\theta|_i < 1$ pour $i \neq 1$.
4. Montrer que, pour tout $\delta > 0$, il existe $\theta \in K$ tel que $|\theta - 1|_1 < \delta$ et $|\theta|_j < \delta$ si $j \neq 1$.
5. Notons $K_1, \ldots, K_2$ les complétés respectifs de K pour $|\cdot|_1, \ldots, |\cdot|_n$. Considérons l'application diagonale

   $$K \to K_1 \times K_2 \times \cdots \times K_n.$$

   Montrer que son image est dense.

Exercice 4. Soit A un anneau commutatif. Pour $\mathfrak{p}$ un idéal premier de A, on note $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$ et $A_{(\mathfrak{p})} = S_{\mathfrak{p}}^{-1}A$ le localisé de A en $\mathfrak{p}$. Cette définition s'étend à tout A-module M : on pose $M_{(\mathfrak{p})}$ l'ensemble des fractions $\frac{m}{s}$ pour $(m, s) \in M \times S_{\mathfrak{p}}$, modulo l'identification $\frac{m}{s} = \frac{n}{t}$ s'il existe $u \in S_{\mathfrak{p}}$ tel que $u(tm - sn) = 0$.

1. Vérifier que $M_{(\mathfrak{p})}$ est un $A_{(\mathfrak{p})}$-module.
2. Montrer que $M \to M_{(\mathfrak{p})}$ qui envoie m vers $\frac{m}{1}$ est injective si et seulement si la multiplication $M \to^{\times s} M$ est injective pour tout $s \in S_{\mathfrak{p}}$. Cette condition est vérifiée si A est inclus dans un corps K et M dans un K-espace vectoriel (très souvent dans ce cours).

3. Montrer que sous cette condition, $M = \bigcap_{\mathfrak{p}} M_{(\mathfrak{p})}$.

Exercice 5. 1. Montrer qu'un anneau factoriel est intégralement clos.

2. Montrer que $\mathbb{Z}[\sqrt{5}]$ n'est pas factoriel.

Exercice 6. 1. Soit B un anneau et A un sous-anneau. Pour $a \in B$, montrer l'équivalence entre

   (a) a est racine d'un polynôme unitaire $P(x) \in A[x]$.

   (b) $A[a]$ est un A-module de type fini.

   (c) Il existe un A-module de type fini $M \subseteq B$ tel que $A \subseteq M$ et $aM \subseteq M$.

2. En déduire que la somme et le produit de deux entiers algébriques sont algébriques.

Exercice 7. Soit A un anneau de Dedekind. Montrer que pour tous idéaux fractionnaires I, J, on a $I \cap J = I \cdot J \cdot (I+J)^{-1}$.

Exercice 8. Soit A un anneau de Dedekind. Montrer que tout idéal fractionnaire de A est engendré par au plus deux éléments, le premier pouvant être choisi arbitrairement parmi les éléments non nuls de l'idéal.

Exercice 9. Soit A un anneau de Dedekind, K son corps des fractions et $\mathfrak{p}$ un idéal premier de A.

1. Soit $x \in \mathfrak{p}$. Montrer qu'il existe $y \notin xA$ tel que $y\mathfrak{p} \subseteq xA$.
2. Montrer qu'avec ces conditions on a $\mathfrak{p}^{-1} = A + (\frac{y}{x})A$.
3. Soit I un idéal entier et $k \geq 0$. Montrer que $I \subseteq \mathfrak{p}^k$ si et seulement si $\left(\frac{y}{x}\right)^k I \subseteq A$.
4. Soit $\alpha = \sqrt[3]{5}$. On admet que $\mathbb{Z}[\alpha]$ est de Dedekind. Calculer l'inverse de l'idéal $(3, 1+\alpha)$.

Exercice 10. Soit K un corps de nombres de degré n.

1. Montrer que tout idéal entier non nul contient une infinité d'entiers naturels.
2. Réciproquement, montrer que l'entier $b > 0$ est contenu dans au plus b^n idéaux entiers.

Exercice 11 (Critère de Dedekind I)**.** Soit $K = \mathbb{Q}(\theta)$ un corps de nombres, où θ est un entier algébrique annulé par $f(x) \in \mathbb{Z}[x]$ irréductible unitaire. Soit p un nombre premier ne divisant pas $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ et

$$f(x) = \prod_{i=1}^{r} f_i(x)^{e_i} \bmod p$$

la factorisation en irréductibles de f modulo p, où l'on considère $f_i(x) \in \mathbb{Z}[x]$ unitaire. On définit, pour $1 \leq i \leq r$, l'idéal $\mathfrak{p}_i = p\mathcal{O}_K + f_i(\theta)\mathcal{O}_K$.

1. Montrer que $\mathcal{O}_K = \mathbb{Z}[\theta] + \mathfrak{p}_i$.

2. Montrer que $\mathfrak{p}_i$ est un idéal premier de degré d'inertie $\deg(f_i)$.
3. Montrer l'égalité $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$.

Exercice 12 (Critère de Dedekind II)**.** On reprend les notations de l'exercice précédent, sauf qu'on ne suppose plus que $\mathbb{Z}[\theta]$ est p-maximal, c'est-à-dire que l'indice $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ est premier à p. Le but de cet exercice est de donner un critère effectif de p-maximalité. On définit $g(x) = \prod_i f_i(x)$ le radical de f modulo p, et

$$R_p = \{x \in \mathbb{Z}[\theta],\ \exists m \geq 0,\ x^m \in p\mathbb{Z}[\theta]\}$$

le radical de (p) dans $\mathbb{Z}[\theta]$.

1. Montrer que $R_p = p\mathbb{Z}[\theta] + g(\theta)\mathbb{Z}[\theta]$ (c'est-à-dire que $a(\theta) \in R_p$ si et seulement si $g \mid a(x) \bmod p$).
2. On suppose que $p \mid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Montrer qu'il existe $a \in \mathcal{O}_K$ tel que $a \notin \mathbb{Z}[\theta]$ mais $pa \in \mathbb{Z}[\theta]$. Montrer qu'il existe $b \in \mathcal{O}_K$ tel que $b \notin \mathbb{Z}[\theta]$ mais $pb \in \mathbb{Z}[\theta]$ et $g(\theta)b \in \mathbb{Z}[\theta]$.
3. Montrer qu'on a dans ce cas $pb \in R_p$ et $g(\theta)b \in R_p$.
4. On suppose de plus que $h(x) = \prod_i f_i^{e_i - 1}$ et $r(x) = \frac{f(x) - g(x)h(x)}{p} \in \mathbb{Z}[x]$ sont premiers entre eux modulo p. En écrivant les éléments de R_p sous la forme $a(x) = g(x)U(x) + pV(x)$, montrer que les conditions $pb \in R_p$ et $g(\theta)b \in R_p$ impliquent $b \in \mathbb{Z}[\theta]$.
5. Réciproquement, supposons $e_i \geq 2$ et $f_i(x) \mid r(x) \bmod p$. En posant $R(x) = f_i(x)^{e_i - 1} \prod_{j \neq i} f_j(x)^{e_j}$, montrer que $\alpha = \frac{R(\theta)}{p}$ est un entier algébrique.
6. En déduire le critère : $\mathbb{Z}[\theta]$ est p-maximal si et seulement si g et r sont premiers entre eux modulo p.
7. Montrer que le critère d'Eisenstein est un cas particulier de ce critère.