Université de Paris **16 septembre 2021**
M2 – Théorie des nombres

Feuille 1 : Valuations, anneaux de Dedekind

1 Valuations, localisation

Exercice 1 :

Une valeur absolue est dite *non-archimédienne* si elle vérifie l'inégalité ultramétrique

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

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

Il suffit de montrer le sens réciproque, supposons donc $|n| \leqslant B$ pour tout $n \in \mathbb{Z}$. Alors pour x, y, on a $|x+y|^n \leqslant \sum \left|\binom{n}{k} x^{n-j} y^j\right| \leqslant nB \max(|x|, |y|)^n$. On obtient le résultat en prenant la racine n-ième et en faisant tendre $n \to \infty$.

Exercice 2 :

On suppose que les valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ définissent la même topologie sur K. Montrer qu'elles sont équivalentes, c'est-à-dire qu'il existe $e > 0$ tel que $|\cdot|_2 = |\cdot|_1^e$.

Si les topologies sont équivalentes, on a $\{x, |x|_1 < 1\} = \{x, |x|_2 < 1\}$ puisque $x^n \to 0$ selon chaque valeur absolue.
On a donc pour tous x, y, et tous exposants $m, n \in \mathbb{Z}$ $|x^m/y^n|_1 < 1 \Leftrightarrow |x^m/y^n|_2 < 1$.
Supposons $|x|_1 > 1$ et $n > 0$, en prenant le logarithme on obtient $\frac{n}{m} < \frac{\log|y|_1}{\log|x|_1} \Leftrightarrow \frac{n}{m} < \frac{\log|y|_2}{\log|x|_2}$, si bien que les fractions à droite sont égales (comme bornes supérieures de rationnels). En faisant varier y, on a bien $|\cdot|_1 = |\cdot|_2^e$, où $e = \frac{\log|x|_1}{\log|x|_2}$.
Cela conclut, car soit les valeurs absolues sont triviales soit il existe x tel que $|x|_1 \neq 1$, quitte à prendre l'inverse on peut supposer $|x|_1 > 1$.

Exercice 3 :

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. Montrer que $M \to M_{(\mathfrak{p})}$ est injective si et seulement si la multiplication $M \to^{\times s} M$ est injective pour tout $s \in S_\mathfrak{p}$.

Clair.

Cette condition est vérifiée si A est inclus dans un corps K et M dans un K-espace vectoriel (très souvent dans ce cours).

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

L'inclusion $\subset$ est vérifiée par hypothèse, réciproquement soit $x \in \bigcap M_{(\mathfrak{p})}$. On introduit l'idéal $I = \{a \in A, ax \in M\} \subset A$. Par hypothèse, $x = \frac{m}{s}$ pour donc A contient un élément non nul de chaque $S_\mathfrak{p}$, donc il n'est contenu dans aucun idéal premier. Donc $I = A$, et $x \in M$.

2 ENTIERS ALGÉBRIQUES

Exercice 4 :

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

Soit A un anneau factoriel et $r/s \in \mathrm{Frac}(A)$ entier sur A, avec r, s premiers entre eux. Il existe une équation à coefficients $a_i \in A$

$$(\tfrac{r}{s})^n + a_{n-1}(\tfrac{r}{s})^{n-1} + \cdots + a_0 = 0$$

En chassant les dénominateurs on obtient

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0$$

, donc $s \mid r^n$ donc s est une unité, ainsi $r/s \in A$.

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

Le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ est racine de $x^2 - x - 1$, donc entier.

Exercice 5 :

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

1. a est racine d'un polynôme unitaire $P(x) \in A[x]$.
2. $A[a]$ est un A-module de type fini
3. il existe un A-module de type fini $M \subset B$ contenant A tel que $aM \subset M$.

Il suffit de montrer $3 \Rightarrow 1$, c'est une conséquence de Cayley-Hamilton. Puisque M est de type fini, on peut écrire sur une famille génératrice (m_i) des relations $am_i = \sum a_{i,j}m_j$, de sorte que (m_i) est dans le noyau de la matrice $aId - (a_{i,j})$. Son déterminant est alors nul : c'est clair si A est intègre, en général la formule de la commatrice montre que c'est un annulateur de tous les m_i, donc de $1 \in A \subset M$. En développant ce déterminant, on obtient un polynôme unitaire en a.

2. Montrer que la somme et le produit de deux entiers algébriques sont algébriques (on pourra donner deux démonstrations, utilisant respectivement les points 1 et 3).

— Si a et b sont entiers, $a + b$ et ab stabilisent $A[a]A[b]$ qui est de type fini.
— (via le résultant) Si $P(a) = Q(b) = 0$, alors $P(x)$ et $Q(z - x)$ s'annulent tous deux en $x = a$ pour $z = x + b$. Ainsi, $a + b$ est racine du résultant $R(z) = \mathrm{Res}_x(P(x), Q(z - x))$, qui est unitaire.
De même, $S(t) = \mathrm{Res}_x(P(x), x^n Q(t/x))$ est un polynôme unitaire qui s'annule en $t = xy$.

3 ANNEAUX DE DEDEKIND

Exercice 6 :

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

C'est vrai localement, en vérifiant les valuations.

Exercice 7 :

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.

Soit $x \in I$ non nul, on a localement $v_{\mathfrak{p}}(x) \geqslant v_{\mathfrak{p}}(I)$ pour tout idéal premier $\mathfrak{p}$. Il suffit de prendre un élément y tel qu'en tout $\mathfrak{p}$ on ait $\min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)) = v_{\mathfrak{p}}(I)$, c'est possible par approximation faible. Explicitement, cela revient à prendre via le lemme chinois un élément $y = (y_1, \dots y_n) \in A/(x) = \prod_i A/\mathfrak{p}_i^{v_{\mathfrak{p}_i}(x)}$ tel que $y_i \in \mathfrak{p}^{v_{\mathfrak{p}}(I)} \setminus \mathfrak{p}^{v_{\mathfrak{p}}(I)+1}$.

Exercice 8 : Inverse, valuation

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 $y\mathfrak{p} \subset xA$.

Prendre un élément y tel que $v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(x) - 1$ et $v_{\mathfrak{q}}(y) \geqslant v_{\mathfrak{q}}(x)$ en $\mathfrak{q} \neq \mathfrak{q}$.

2. Montrer qu'avec ces valeurs on a $\mathfrak{p}^{-1} = A + (\frac{y}{x})A$.

C'est bien un idéal fractionnaire, et on vérifie localement les valuations.

3. Soit I un idéal entier et $k \geqslant 0$, montrer que $I \subset \mathfrak{p}^k$ si et seulement si $(\frac{y}{x})^k I \subset A$.

Il suffit de le voir pour $k = 1$, et $\mathfrak{p} \mid I$ ssi $I \subset \mathfrak{p}$ ssi $\mathfrak{p}^{-1} I \subset A$.

4. Soit $\alpha = \sqrt[3]{5}$, on admet que $\mathbb{Z}[\sqrt[3]{5}]$ est de Dedekind. Calculer l'inverse de l'idéal $\mathfrak{p} = (3, 1 + \alpha)$.

L'idéal est bien premier puisque le quotient est $\mathbb{Z}/3\mathbb{Z}$ On prend $x = 3$, en posant $y = y_0 + y_1\alpha + y_2\alpha^2$. on a $y(1 + \alpha) = (y_0 + 5) + (y_0 + y_1)\alpha + (y_1 + y_2)\alpha^2$, d'où un zéro modulo 3 non trivial $y = 1 - \alpha + \alpha^2$. L'inverse est donc $(1, \frac{1-\alpha+\alpha^2}{3})$.

Exercice 9 :

Soit K un corps de nombres de degré n.

1. Montrer que tout idéal entier non nul contient une infinité d'entiers naturels.

Soit $\mathfrak{a}$ un idéal, on a par exemple $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$, ainsi que tous ses multiples.

2. Réciproquement, montrer que l'entier $b > 0$ est contenu dans au plus b^n idéaux entiers.

Soit $\mathfrak{a}$ un idéal contenant b, on écrit $\mathfrak{a} = b\mathbb{Z}_K + \beta\mathbb{Z}_K$, où β peut être pris dans $\mathbb{Z}_K/(b)$, qui est de cardinal b^n.

Exercice 10 : Critère de Dedekind I

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

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

une factorisation en irréductibles de $f(x)$ modulo p, où l'on considère des relevés $f_i(x) \in \mathbb{Z}[x]$ de même degré.
On définit pour $1 \leqslant i \leqslant r$ l'idéal $\mathfrak{p}_i = p\mathbb{Z}_K + f_i(\theta)\mathbb{Z}_K$.

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

On calcule l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta] + \mathfrak{p}_i]$. Puisque $\mathbb{Z}[\theta] \subset \mathbb{Z}[\theta] + \mathfrak{p}_i$ et $p\mathbb{Z}_K \subset \mathbb{Z}[\theta] + \mathfrak{p}_i$, cet indice est un diviseur commun à $[\mathbb{Z}_K : \mathbb{Z}[\theta]$ et $[\mathbb{Z}_K : p\mathbb{Z}_K] = p^n$, c'est donc 1.

2. Montrer que $\mathfrak{p}_i$ est un idéal premier de degré résiduel $\deg(f_i)$.

D'après la question précédente, le morphisme d'évaluation en θ $\mathbb{Z}[x] \to \mathbb{Z}_K/\mathfrak{p}$ est surjectif.
Son noyau contient l'idéal $p\mathbb{Z}[\theta] + f_i(\theta)\mathbb{Z}[\theta]$. Or cet idéal est maximal de quotient $\mathbb{F}_p[x]/(f_i) = \mathbb{F}_{p^{\deg f_i}}$.
Ainsi, si $\mathfrak{p}$ n'est pas égal à $\mathbb{Z}_K$ tout entier, le noyau est exactement $p\mathbb{Z}[\theta] + f_i(\theta)\mathbb{Z}[\theta]$, on a un isomorphisme et $\mathfrak{p}$ est un idéal premier de degré résiduel $\deg(f_i)$.
La question suivante montrera que l'on ne peut avoir $\mathfrak{p} = \mathbb{Z}_k$.

3. Montrer l'égalité $p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i}$.

Il suffit de montrer que $p\mathbb{Z}_K \mid \prod_i \mathfrak{p}_i^{e_i}$, en utilisant l'existence de la factorisation et l'égalité $n = \sum_i e_i f_i$ (qui prouve au passage qu'aucun des $\mathfrak{p}_i$ n'est trivial).
Or en développant $\prod_i \mathfrak{p}_i^{e_i} = (p, \prod_i f_i(\theta)_i^e)$, et $\prod_i f_i(\theta)_i^e = f(\theta) + pQ(\theta) \in p\mathbb{Z}_K$. On a donc bien $\prod_i \mathfrak{p}_i^{e_i} \subset p\mathbb{Z}_K$.

Pour cet exercice, une méthode plus simple pour arriver au résultat est de montrer directement l'isomorphisme $\mathbb{Z}_K/(p) = \mathbb{Z}[\theta]/(p)$. (surjectivité grâce à l'hypothèse sur l'indice, et égalité des cardinaux). Le quotient de droite est $\mathbb{F}_p[x]/(f) = \prod_i \mathbb{F}_p[x]/f_i^{e_i}$, ses idéaux premiers sont les (p, f_i), donc les idéaux premiers de $\mathbb{Z}_K$ contenant (p) sont également les $(p, f_i(\theta))$.

Exercice 11 : 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 $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ 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 $R_p = \{x \in \mathbb{Z}[\theta], \exists m \geqslant 0, x^m \in p\mathbb{Z}[\theta]\}$ 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 $a(\theta) \in R_p \Leftrightarrow g \mid a(x) \bmod p$).

Soit $A(\theta) \in R_p$, par hypothèse il existe $m \geqslant 0$ tel que $A(x)^m = f(x)u(x) + pv(x)$, d'où en réduisant modulo p $g(x) \mid A(x) \mod p$. L'inclusion réciproque est évidente, puisque R_p est un idéal et que p et $g(\theta)^n = 0$.

2. On suppose que $p \mid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, montrer qu'il existe $a \in \mathbb{Z}_K$ tel que $a \notin \mathbb{Z}[\theta]$ mais $pa \in \mathbb{Z}[\theta]$.

Un élément a d'ordre p dans le quotient convient.

Montrer qu'il existe $b \in \mathbb{Z}_K$ tel que $b \notin \mathbb{Z}[\theta]$ mais $pb \in \mathbb{Z}[\theta]$ et $g(\theta)b \in \mathbb{Z}[\theta]$

On a $ag(\theta)^n = a(f(\theta) + pm(\theta)) \in \mathbb{Z}[\theta]$, donc on a existence de k tel que $b = ag(\theta)^k$ vérifie la condition.

3. Montrer qu'on a dans ce cas $pb \in R_p$ et $g(\theta)b \in R_p$.

L'ordre de b^k dans $\mathbb{Z}_K/\mathbb{Z}[\theta]$ est un diviseur commun de $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ et p^k, donc en notant $v = v_p([\mathbb{Z}_K : \mathbb{Z}[\theta]])$ on a $p^v b^k \in \mathbb{Z}[\theta]$, et pour $k > v$ $(pb)^k \in p\mathbb{Z}[\theta]$, donc $pb \in R_p$. De même, $g(\theta)^n \in p\mathbb{Z}[\theta]$ donc $g(\theta)b)^{n(v+1)} \in p^{v+1}\mathbb{Z}[\theta]$ et $(g(\theta)b)^{n(v+1)} \in p\mathbb{Z}[\theta]$, ce qu'on voulait.
Démonstration alternative : le radical R_p est l'intersection des idéaux premiers de $\mathbb{Z}[\theta]$ contenant p, on doit donc montrer qu'un tel idéal $\mathfrak{p}$ contient aussi pb. Soit $\mathfrak{P}$ un idéal de $\mathbb{Z}_K$ au dessus de $\mathfrak{p}$, il contient p donc pb puisque $b \in \mathbb{Z}_K$, donc $pb \in \mathfrak{P} \cap \mathbb{Z}[\theta] = \mathfrak{p}$. Idem avec $g(\theta)b$, l'idéal $\mathfrak{P}$ au dessus contient une puissance $g(\theta)^n$, donc $g(\theta)$, donc $g(\theta)b$.

4. On suppose de plus que $h(x) = \prod f_i^{e_i - 1}$ 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 $a(x) = g(x)U(x) + pV(x)$ (question 1), montrer que les conditions $pb \in R_p$ et $g(\theta)b \in R_p$ impliquent $b \in \mathbb{Z}[\theta]$.

On écrit

$$\begin{cases} pb & = g(x)U(x) + pV(x) \\ g(\theta)b & = g(x)R(x) + pS(x) \end{cases},$$

le but est de montrer que $pb \in p\mathbb{Z}[\theta]$, c'est-à-dire que $gU \equiv 0 \mod p, f(x)$, c'est-à-dire que pour tout i tel que $e_i > 1$, $f_i^{e_i - 1} \mid U(x) \mod p$.
En multipliant chaque ligne on a deux écritures de $pg(\theta)b$, qui diffèrent donc d'un multiple de $f(x) = gh + pr(x)$.
On obtient donc

$$g^2U + pgV = pgR + p^2S + (gh + pr)Q.$$

En réduisant modulo p on obtient $g^2U = ghQ$ soit $gU = hQ \mod p$.
En réduisant modulo $f_i(x)$ on obtient $f_i \mid p^2S + prQ$ donc $f_i \mid rQ \mod p$. Par hypothèse f_i ne divise pas r si $e_i > 1$, donc $f_i \mid Q \mod p$ et $f_i^{e_i} \mid gU \mod p$.
On a bien $pb \in p\mathbb{Z}[\theta]$.

5. Réciproquement, supposons $e_i \geqslant 2$ et $f_i(x) \mid r(x) \mod p$. 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 de degré 2.

On écrit $R = f_i S$, $f_i R = gh = f - pr$, et $r = f_i T + pV$, alors

$$R^2 = f_i RS = (f - pr)S = fS - p(f_i T + pV)S = fS - pTR - p^2 VS$$

de sorte que

$$\alpha^2 + T(\theta)\alpha + V(\theta)S(\theta) = 0,$$

d'où $\alpha \in \mathbb{Z}_K$.

6. En déduire le critère : $\mathbb{Z}[\theta]$ est p-maximal si et seulement si h et r sont premiers entre eux modulo p.

C'est ce que montrent les deux questions précédentes, avec en prime la construction d'un élément permettant d'étendre $\mathbb{Z}[\theta]$ quand il n'est pas p-maximal.

7. Montrer que le critère d'Eisenstein est un cas particulier de ce critère.

Sous les hypothèses du critère d'Eisenstein on écrit $f(x) = x \cdot x^{n-1} + pr(x)$ avec $x \nmid r(x) \bmod p$, donc $Z[\theta]$ est p-maximal, et il y a un unique premier $\mathfrak{p}$ au-dessus de p, qui est ramifié de degré de ramification n. Par formule des degrés, on en déduit $[K : \mathbb{Q}] = n$ et l'irréductibilité de f.