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.

Indications 1. Il suffit de montrer le sens réciproque, supposons donc $|n| \leq B$ pour tout $n \in \mathbb{Z}$. Alors pour x, y, on a :

$$|x+y|^n \leq \sum \left(\binom{n}{k} x^{n-k} y^k \right) \leq (n+1)B \max(|x|,|y|)^n.$$

On obtient le résultat en prenant la racine n-ème et en faisant tendre $n \to \infty$.

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 $|\cdot|_2 = |\cdot|_1^e$.

Indications 2. On a que $|\cdot|_1$ est trivial si et seulement si $|\cdot|_2$ l'est, donc on peut supposer que $|\cdot|_1$ soit non trivial. Il existe en particulier θ tel que $|\theta|_1 \neq 1$. Quitte à remplacer θ par θ^{-1}, on peut supposer $|\theta|_1 < 1$.

Si les topologies sont équivalentes, on a

$$\{x, |x|_1 < 1\} = \{x, |x|_2 < 1\}$$

puisque $x^n \to 0$ selon chaque valeur absolue. En particulier, $|\theta|_2 < 1$. De plus, pour tout x, y et tous exposants $m, n \in \mathbb{Z}$,

$$\left|\frac{x^m}{y^n}\right|_1 < 1 \iff \left|\frac{x^m}{y^n}\right|_2 < 1$$

En particulier, si $n > 0$ on a, en prenant le logarithme de l'équivalence ci-dessus avec $x = \theta$,

$$\frac{m}{n} > \frac{\log|y|_1}{\log|\theta|_1} \iff \frac{m}{n} > \frac{\log|y|_2}{\log|\theta|_2}$$

pour tout y. Donc, par densité de $\mathbb{Q}$, les fractions à droite sont égales. En faisant varier y on termine avec $e = \frac{\log|\theta|_1}{\log|\theta|_2}$.

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.

Indications 3. On définit une fonction $|\cdot|_A \colon A \to \mathbb{R}$ par

$$|(x_n)|_A = \lim_{n\to\infty} |x_n|$$

1. Le fait que A est un anneau et est clair par continuité de la somme et du produit. Le produit d'une suite de Cauchy avec une suite qui tend vers 0 tend vers 0 (exercice), donc I est bien un idéal de A. L'application φ qui envoie x sur la suite constante égale à x identifie K à un sous-anneau de A.
2. La fonction $|\cdot|_A$ est presque une valeur absolue (la seule chose qui manque est $|(x_n)|_A = 0 \Rightarrow (x_n) = 0$) qui muni A d'une *pseudo-distance* (voir ici) et donc d'une topologie qui étend celle de K, et sa continuité implique que I est un idéal fermé. L'inverse d'une suite de Cauchy qui ne tend pas vers 0 est encore une suite de Cauchy (utiliser le fait que pour une telle suite (x_n) il existe un réel strictement positif C tel que $|x_n| > C$ pour tout n assez grand), donc I est maximal et A/I est un corps. L'application φ passe au quotient et identifie K à un sous-corps de A/I. La valeur absolue passe aussi au quotient, et A/I est donc un corps muni d'une valeur absolue. Il est immédiat de vérifier que K est dense dans A/I donc pour vérifier que A/I est complet il suffit de vérifier que toute suite de Cauchy à valeurs dans K converge dans A/I (utiliser un argument diagonal), ce qui est facile.
3. Par induction sur n.
Supposons $n = 2$. Par hypothèse les deux valeurs absolues ne sont pas équivalentes, donc, par l'exercice précèdent, les deux boules ouvertes unitaire ne sont pas égales. Supposons qu'on peut trouver x tel que $|x|_1 < 1$ et $|x|_2 \geq 1$ et soit y tel que $|y|_2 > 1$ (il existe parce que $|\cdot|_2$ est non trivial). Si n est très grand on a $|x^n y|_1 = |x|_1^n |y|_1 < 1$ et $|x^n y|_2 = |x|_2^n |y|_2 > 1$

et donc on peut prendre $\theta = (x^n y)^{-1}$. Si d'autre part il existe x tel que $|x|_2 < 1$ et $|x|_1 \geq 1$ on choisit y tel que $|y|_1 > 1$ et on pose $\theta = x^n y$ pour n très grand.
Supposons maintenant le résultat vrai pour $n-1$ valeur absolue. Soit donc $x \in K$ tel que $|x|_1 > 1$ et $|x|_i < 1$ pour $i = 2, \ldots, n-1$. En utilisant le cas $n = 2$, soit y tel que $|y|_1 > 1$ et $|y|_n < 1$.

— Dans le cas $|x|_n \leq 1$ on pose $\theta = yx^m$ pour m très grand. On a

$$|\theta|_1 = |y|_1 |x|_1^m > 1$$

De plus

$$|\theta|_n = |y|_n |x|_n^m \leq |y|_n < 1$$

Si $i = 2, \ldots, n-1$ on a

$$|\theta|_i = |y|_i |x|_i^m < 1$$

car $|x|_i^m \to 0$ quand $m \to \infty$.

— Dans le cas $|x|_n > 1$ on pose, pour $m \in \mathbb{N}$

$$\theta_m = \frac{yx^m}{1 + x^m}$$

Si $i = 1$ ou $i = n$, on a

$$|\theta_m - y|_i = \left| y \frac{x^m - (1 + x^m)}{1 + x^m} \right|_i = \frac{|y|_i}{|1 + x^m|_i}.$$

Or, $|x^m|_i \to \infty$ donc $|1 + x^m|_i \geq |x^m| - 1 \to \infty$ et $|\theta_m - y|_i \to 0$, c'est-à-dire que $\theta_m \to y$ et en particulier, si m est assez grand, $|\theta_m|_1 > 1$ et $|\theta_m|_n < 1$.
Si $i = 2, \ldots, n-1$ on a $|x^m|_i \to 0$ donc $x^m \to 0$ (pour la topologie induite par $|\cdot|_i$) et $1 + x^m \to 1$. En particulier, $\theta_m \to 0$ et donc $|\theta_m|_i < 1$ pour m assez grand. On voit donc que θ_m, pour m très grand, a les propriétés demandées.

4. Soit x comme dans la question précédente. On pose

$$\theta_m = \frac{x^m}{1 + x^m}$$

On a

$$|\theta_m - 1|_1 = \frac{1}{|1 + x^m|_1} \to 0$$

De plus, si $j \neq 1$, on a $x^m \to 0$ pour la topologie induite par $|\cdot|_j$ et donc $\theta_m \to 0$. En particulier, θ_m pour m assez grand convient.

5. Il suffit de démontrer l'affirmation suivante : pour tout $\varepsilon > 0$ et pour tout $x_1, \ldots, x_n \in K$ il existe $x \in K$ tel que $|x - x_i|_i < \varepsilon$.

Soit donc $x_1, \ldots, x_n \in K$ et $\varepsilon > 0$. On pose $\delta = \frac{\varepsilon}{nM}$ ou $M = \max_{i,j} |x_i|_j$. La question précédente implique que, pour tout i, il existe $a_i \in K$ tel que $|a_i - 1|_i < \delta$ et $|a_i|_j < \delta$ si $j \neq i$. On pose

$$x = a_1 x_1 + \cdots a_n x_n \in K$$

On a

$$|x - x_i|_i \leq |x_i|_i |a_i - 1|_i + \left| \sum_{j \neq i}^{n} a_j x_j \right|_i \leq M\delta + (n-1)M\delta = \varepsilon$$

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, $M = \bigcap_\mathfrak{p} M_{(\mathfrak{p})}$.

Indications 4.
1. Évident.
2. Aussi Clair.
3. L'inclusion $M \subseteq \bigcap_\mathfrak{p} M_{(\mathfrak{p})}$ est vérifiée par hypothèse. Réciproquement, soit $x \in \bigcap_\mathfrak{p} M_{(\mathfrak{p})}$. On introduit l'idéal $I = \{a \in A \mid ax \in M\} \subseteq A$. Par hypothèse, $x = \frac{m}{s}$ pour un élément non nul de chaque $S_{(\mathfrak{p})}$, donc I n'est contenu dans aucun idéal premier. Par conséquent, $I = A$ et $x \in M$.

Exercice 5.
1. Montrer qu'un anneau factoriel est intégralement clos.
2. Montrer que $\mathbb{Z}[\sqrt{5}]$ n'est pas factoriel.

Indications 5.
1. Soit A un anneau factoriel et $\frac{r}{s} \in \mathrm{Frac}(A)$ entier sur A, avec r et s premiers entre eux. Il existe une équation à coefficients $a_i \in A$:

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

En chassant les dénominateurs, on obtient :

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

Donc $s \mid r^n$, et ainsi s est une unité, donc $\frac{r}{s} \in A$.

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

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.

Indications 6. 1. Il suffit de montrer que (c) implique (a), ce qui 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 $a\mathrm{Id} - (a_{i,j})$. Son déterminant est alors nul : c'est clair si A est intègre, et en général, la formule de la comatrice montre que c'est un annulateur de tous les m_i, donc de $1 \in A \subseteq M$. En développant ce déterminant, on obtient un polynôme unitaire en a.
2. Si a et b sont entiers, alors $a+b$ et ab stabilisent $A[a]A[b]$ qui est de type fini.

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

Indications 7. C'est vrai localement, en vérifiant les valuations.

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.

Indications 8. Soit $x \in I$ non nul, on a localement $v_p(x) > v_p(I)$ pour tout idéal premier p. Il suffit de prendre un élément y tel qu'en tout p on ait $\min(v_p(x), v_p(y)) = v_p(I)$, c'est possible par approximation faible.

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 $(3, 1+\alpha)$.

Indications 9. 1. Prendre y tel que $v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(x) - 1$ et $v_{\mathfrak{q}}(y) \geq v_{\mathfrak{q}}(x)$ si $\mathfrak{q} \neq \mathfrak{p}$.
2. On vérifie localement les valuations.
3. Il suffit de le faire pour $k = 1$, et ce cas suit parce que $\mathfrak{p} \mid I$ si et seulement si $I \subseteq \mathfrak{p}$ si et seulement si $\mathfrak{p}^{-1} I \subseteq A$.

4. L'idéal est premier parce que le quotient est $\mathbb{Z}/3\mathbb{Z}$. On applique les autres questions avec $x = 3$: en posant $y = y_0 + y_1\alpha + y_2\alpha^2$ on a $y(1+\alpha) = y_0 + 5 + (y_0+y_1)\alpha + (y_1+y_2)\alpha^2$ et donc $y = 1 - \alpha + \alpha^2$ marche. L'inverse est donc
$$(3, 1+\alpha)^{-1} = \left(1, \frac{1-\alpha+\alpha^2}{3}\right).$$

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.

Indications 10.
1. Soit a un idéal, on a par exemple $\mathrm{Norm}_{K/\mathbb{Q}}(a) \in a \cap \mathbb{Z}$, ainsi que tous ses multiples. Donc l'idéal a contient une infinité d'entiers naturels.
2. Soit I un idéal contenant b. On peut écrire $I = b\mathcal{O}_K + \beta\mathcal{O}_K$, où β peut être pris dans $\mathcal{O}_K/(b)$, qui est de cardinalité b^n. Donc l'entier b 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 $1 \le i \le r$, 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 $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$.

Indications 11.
1. On calcule l'indice $[\mathcal{O}_K : \mathbb{Z}[\theta] + \mathfrak{p}_i]$. Puisque $\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\theta]+\mathfrak{p}_i$ et $p\mathcal{O}_K \subseteq \mathbb{Z}[\theta]+\mathfrak{p}_i$, cet indice est un diviseur commun à $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ et $[\mathcal{O}_K : p\mathcal{O}_K] = p^n$, c'est donc 1.
2. D'après la question précédente, le morphisme d'évaluation en θ, $\mathbb{Z}[x] \to \mathcal{O}_K/\mathfrak{p}_i$ est surjectif. Son noyau contient l'idéal $p\mathbb{Z}[\theta] + f_i(\theta)\mathbb{Z}[\theta]$, et lui est égal puisque cet idéal est maximal de quotient $\mathbb{F}_p[x]/(f_i) \cong \mathbb{F}_{p^{\deg(f_i)}}$. Ainsi, $\mathfrak{p}_i$ est un idéal premier de degré résiduel $\deg(f_i)$.
3. En utilisant l'existence de la factorisation et l'égalité $n = \sum_i e_i f_i$, il suffit de montrer que $p\mathcal{O}_K \mid \prod_i \mathfrak{p}_i^{e_i}$, c'est-à-dire $\prod_i \mathfrak{p}_i^{e_i} \subseteq p\mathcal{O}_K$. Or, en développant, on voit qu'il suffit de montrer que $\prod_i f_i(\theta)^{e_i} \subseteq p\mathcal{O}_K$. On a $\prod_i f_i(\theta)^{e_i} = f(\theta) + pQ(\theta) \in p\mathcal{O}_K$ et donc $\prod_i \mathfrak{p}_i^{e_i} \subseteq p\mathcal{O}_K$.

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.

Indications 12.

1. Soit $A(\theta) \in R_p$. Par hypothèse il existe $m > 0$ tel que $A(x)^m = f(x)u(x) + pv(x)$, d'où en réduisant modulo p, on obtient $g(x) \mid A(x) \bmod p$. L'inclusion réciproque est évidente puisque R_p est un idéal et que p et $g(\theta)^n = 0$.
2. Un élément a d'ordre p dans le quotient $\mathcal{O}_K/\mathcal{O}_K[\theta]$ convient. On a $ag(\theta)^n = a(f(\theta) + pm(\theta)) \in \mathbb{Z}[\theta]$, donc il existe un entier k tel que $b = ag(\theta)^k$ vérifie la condition.
3. L'ordre de b^k dans $\mathcal{O}_K/\mathbb{Z}[\theta]$ est un diviseur commun de $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ et de p^k, donc en notant $v = v_p([\mathcal{O}_K : \mathbb{Z}[\theta]])$ on a $p^v b^k \in \mathbb{Z}[\theta]$ et si $k > v$ alors $(pb)^k \in p\mathbb{Z}[\theta]$. Donc $pb \in R_p$. De même, $g(\theta)^n \in p\mathbb{Z}[\theta]$ donc $(g(\theta)b)^{n(v+1)} \in p^{n+1}\mathbb{Z}[\theta]$ et $(g(\theta)b)^{n(v+1)} \in p\mathbb{Z}[\theta]$, ce qu'on voulait.
4. On écrit :
$$pb = g(x)U(x) + pV(x)$$
et
$$g(\theta)b = g(x)R(x) + pS(x).$$
Le but est de montrer que $pb \in p\mathbb{Z}[\theta]$, c'est-à-dire que $gU \equiv 0 \bmod p$, et que pour tout i tel que $e_i > 1$ on a $f_i^{e_i-1} \mid U(x) \bmod p$. 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 que $gU = hQ \mod p$. En réduisant modulo $f_i(x)$ on obtient $f_i \mid p^2S + prQ$ donc $f_i \mid rQ \mod p$. Par hypothèse, $f_i(x)$ 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. On écrit $R = f_iS$, $f_iR = gh = f - pr$ et $r = f_iT + pV$. Donc

$$R^2 = f_iRS = (f - pr)S = fS - p(f_iT + pV)S = fS - pTR - p^2VS$$

de sorte que

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

d'où α est un entier algébrique.

6. C'est une conséquence des questions précédentes.

7. Sous les hypothèses du critère d'Eisenstein on écrit $f(x) = x \cdot x^{n-1} + pr(x)$ avec $p \nmid r(x) \mod p$. Soit θ une racine du polynôme P, donc $\mathbb{Z}[\theta]$ est p-maximal et il y a un unique premier $\mathfrak{p}$ au-dessus de p qui est ramifié de degré de ramification e. Par la formule des degrés, on en déduit $e = [K : \mathbb{Q}] \leq n$. soit $P = X^n + c_{n-1}X^{n-1} + ... + c_0$. On sait que p est totalement ramifié dans $\mathcal{O}_K$, où $K = \mathbb{Q}(\theta)$. On écrit $p = P^e$ pour P un idéal premier de $\mathcal{O}_K$ et on a $e \leq n$. Il faut montrer que $e = n$. On a

$$\theta^n + c_{n-1}\theta^{n-1} + ... + c_0 = 0$$

et en réduisant modulo p on trouve $\theta^n \equiv 0 \mod p$ et donc $\theta^n \equiv 0 \mod P$ (parce que $p \in P$). Car P est premier, on en déduit $\theta \equiv 0 \mod P$. Tous les c_i sont divisible par p, donc par P^e, donc $c_i\theta^i \equiv 0 \mod P^{e+1}$ si $i \neq 0$ et en regardant $P(\theta) = 0$ on trouve $\theta^n + c_0 \equiv 0 \mod P^{e+1}$. Or, c_0 est divisible par p une seule fois et donc il n'est pas divisible par P^{e+1} et donc $\theta^n \not\equiv 0 \mod P^{e+1}$. On sait que θ est divisible par P, du coup $\theta^n \not\equiv 0 \mod P^{e+1}$ implique que $n < e + 1$, c'est-à-dire $n \leq e$ comme on veut.