

Quelques remarques sur le polygone de Newton

David A. Madore

15 avril 2020

CVS:\$Id: valuation.tex,v 1.19 2006-06-24 11:34:00 david Exp \$

Introduction

0.1. Le but de cette note est de présenter de façon assez élémentaire la notion de polygone de Newton d'un polynôme et d'expliquer comment, notamment, on peut en déduire un critère d'irréductibilité des polynômes à coefficients rationnels (ou, en réalité, p -adiques).

0.2. Nous commençons par des considérations très générales sur les valuations sur un anneau commutatif afin d'éclaircir la signification de ce terme. En réalité, on n'aura usage que de la valuation p -adique sur les rationnels et de valuations qui seront explicitement construites à partir d'elles ci-dessous (le lecteur peut donc omettre cette première partie sauf quand il y est explicitement fait référence, et lire directement à partir de 2.1 ci-dessous).

0.3. Si p est un nombre premier, on définit $v_p: \mathbb{Z} \rightarrow \mathbb{Z} \sqcup \{\infty\}$ qui à un entier n non nul associe l'exposant de la plus grande puissance de p qui divise n (c'est-à-dire l'exposant de p dans la décomposition de n en facteurs premiers), et $v_p(0) = \infty$. Cette fonction s'étend à $\mathbb{Q}$ par $v_p(a/b) = v_p(a) - v_p(b)$: les propriétés usuelles de la décomposition en facteurs premiers montrent qu'il s'agit d'une valuation au sens de la définition 1.4 plus bas, et on l'appelle la *valuation p -adique* (sur $\mathbb{Z}$ ou sur $\mathbb{Q}$).

0.4. Exemples : Si n est un entier, on a $v_2(n) = 0$ si et seulement si n est impair, $v_2(n) \geq 1$ si et seulement si n est pair, $v_2(n) \geq 2$ si et seulement si n est multiple de 4, etc. Pour x rationnel, $v_2(x) \geq 0$ signifie exactement que le dénominateur

réduit de x est impair. Pour $x = \frac{35}{88}$, on a $v_2(x) = -3$, $v_5(x) = 1$, $v_7(x) = 1$, $v_{11}(x) = -1$, et $v_p(x) = 0$ pour tout $p \neq \{2, 5, 7, 11\}$. Un résultat classique d'arithmétique affirme que pour tout $n \in \mathbb{N}$ on a $v_p(n!) = \sum_{r=1}^{+\infty} \lfloor \frac{n}{p^r} \rfloor$, où $\lfloor \cdot \rfloor$ désigne la partie entière.

0.5. Tous les anneaux considérés ici seront implicitement supposés commutatifs (et unitaires).

1 Généralités sur les valuations

Définition 1.1. On appelle *groupe abélien totalement ordonné* un groupe abélien Γ muni d'un ordre total $<$ vérifiant la propriété suivante de compatibilité entre la structure algébrique et la structure d'ordre : si $\alpha < \beta$ et γ sont dans Γ alors $\alpha + \gamma < \beta + \gamma$.

1.2. Exemples : Tout sous-groupe de $\mathbb{R}$, et notamment $\mathbb{Z}$ ou $\mathbb{Q}$ ou $\mathbb{R}$ lui-même, hérite d'une structure de groupe abélien totalement ordonné. S'agissant d'un sous-groupe de $\mathbb{Q}$, cette structure est d'ailleurs uniquement définie par la condition $1 \geq 0$.

1.3. On peut par ailleurs remarquer que dans un groupe abélien totalement ordonné Γ on a $x > 0$ si et seulement si $(-x) < 0$, et que Γ est nécessairement *sans torsion* comme groupe abélien, c'est-à-dire que si $x \neq 0$ alors $nx \neq 0$ pour tout $n \neq 0$ entier (c'est évident pour $x > 0$ comme pour $x < 0$).

Définition 1.4. Soit A un anneau non nul. On appelle *valuation* sur l'anneau A une application $v : A \rightarrow \Gamma \uplus \{\infty\}$, où Γ est un groupe abélien totalement ordonné (et $\uplus$ désigne la réunion disjointe), qui vérifie les propriétés suivantes (pour $x, y \in A$ quelconques) :

- (o) $v(x) = \infty$ si et seulement si $x = 0$,
- (i) $v(xy) = v(x) + v(y)$ avec la convention $\alpha + \infty = \infty$ pour tout $\alpha \in \Gamma \uplus \{\infty\}$,
- (ii) $v(x + y) \geq \min(v(x), v(y))$ avec la convention $\infty \geq \alpha$ pour tout $\alpha \in \Gamma \uplus \{\infty\}$.

Le groupe (ordonné) engendré par $v(A \setminus \{0\})$ dans Γ sera appelé *groupe de valuations*.

Faits 1.5. Soit A un anneau muni d'une valuation v . Alors on a $v(1) = v(-1) = 0$ et $v(x - y) \geq \min(v(x), v(y))$. Si $(x_i)_{i \in I}$ est une famille finie d'éléments de A alors (i) $v(\prod_{i \in I} x_i) = \sum_{i \in I} v(x_i)$ et (ii) $v(\sum_{i \in I} x_i) \geq \min_{i \in I} v(x_i)$.

Démonstration. Immédiat. $\square$

Fait 1.6. Soit A un anneau muni d'une valuation v . Si $(x_i)_{i \in I}$ est une famille finie d'éléments de A et si, pour un certain $i_0 \in I$, on a $v(x_{i_0}) < v(x_i)$ pour tout $i \neq i_0$, alors $v(\sum_{i \in I} v(x_i)) = v(x_{i_0})$ (autrement dit, on a égalité dans le (ii) de 1.5).

Démonstration. Soit $y = \sum_{i \in I} x_i$ et $z = \sum_{i \neq i_0} x_i$. Le (ii) de 1.5) montre $v(y) \geq \min_{i \in I}(v(x_i)) = v(x_{i_0})$ mais également $v(z) > v(x_{i_0})$. Comme par ailleurs $x_{i_0} = y - z$ donc $v(x_{i_0}) \geq \min(v(y), v(z))$, on a prouvé $v(y) = v(x_{i_0})$. $\square$

Proposition 1.7. Si un anneau A est muni d'une valuation v , alors A est un anneau intègre, et la valuation v se prolonge de façon unique en une valuation sur le corps des fractions K de A . La partie $R = \{x \in K : v(x) \geq 0\}$ de K est alors également un anneau intègre, et pour tout $x \in K^\times$ on a soit $x \in R$ soit $x^{-1} \in R$ (notamment, R a encore K pour corps des fractions).

Démonstration. Dans $\Gamma \uplus \{\infty\}$, on a $\alpha + \beta = \infty$ si et seulement si l'un de α et de β est ∞ . Les conditions (o) et (i) de la définition 1.4 montrent donc que $xy = 0$ si et seulement si $x = 0$ ou $y = 0$, c'est-à-dire que A est intègre. Il est donc légitime de considérer $K = \text{Frac}(A)$ le corps des fractions de A . On prolonge $v : A \rightarrow \Gamma \uplus \{\infty\}$ en une application $K \rightarrow \Gamma \uplus \{\infty\}$ en posant $v(x/y) = v(x) - v(y)$: la condition (i) de la définition 1.4 montre que ce prolongement est bien défini, et il est facile de vérifier qu'il s'agit encore d'une valuation (sur le corps K), qui est bien entendu l'unique valuation sur K prolongeant la valuation donnée sur A (puisque la relation $v(x/y) = v(x) - v(y)$ était nécessaire).

Le fait que $R = \{x \in K : v(x) \geq 0\}$ soit un sous-anneau de K est une conséquence immédiate des propriétés définissant une valuation (R est stable par addition et par multiplication, et $v(1) = 0$ a été vu en 1.5). Cet anneau est bien entendu intègre (étant un sous-anneau d'un corps). Et si $x \in K^\times$, comme $v(x^{-1}) = -v(x)$ (puisque on a déjà remarqué $v(1) = 0$), on a soit $v(x) \geq 0$ soit $v(x^{-1}) \geq 0$. $\square$

Définition 1.8. On appelle *anneau de valuation* un anneau intègre R tel que pour tout élément non nul x du corps des fractions K de R on ait soit $x \in R$ soit $x^{-1} \in R$.

Proposition 1.9. Si R est un anneau de valuation, il existe une et (à isomorphisme croissant près sur le groupe de valuations) une seule valuation v sur le corps des fractions K de R telle que $R = \{x \in K : v(x) \geq 0\}$. L'anneau R est un anneau local, c'est-à-dire qu'il a un unique idéal maximal, qui est donné exactement comme $\{x \in R : v(x) > 0\}$.

Démonstration. Si v est une valuation sur K telle que $x \in R$ si et seulement si $v(x) \geq 0$, alors clairement $v(x) = 0$ si et seulement si x est dans l'ensemble $R^\times$ des inversibles de R : ceci prouve que v définit un isomorphisme entre le groupe $K^\times/R^\times$ et le groupe de valuations $v(K^\times)$, et il s'agit d'un isomorphisme croissant si on ordonne totalement $K^\times/R^\times$ en imposant $x \succeq y$ si et seulement si $x/y \in R$ (il s'agit d'un ordre total précisément car R est un anneau de valuation). Ceci prouve l'unicité. Mais si on pose précisément $\Gamma = K^\times/R^\times$ avec l'ordre qu'on vient d'expliquer, la surjection canonique $K^\times \rightarrow K^\times/R^\times$ construit alors justement une valuation $v: K \rightarrow \Gamma \sqcup \{\infty\}$ dont on a prouvé l'unicité sujette à la condition que $R = \{x \in K : v(x) \geq 0\}$.

Le fait que $\mathfrak{m} = \{x \in R : v(x) > 0\}$ soit un idéal (propre) de R est clair. Comme tout élément de R qui n'est pas dans $\mathfrak{m}$ est inversible, il est clair que cet idéal est maximal, et que c'est l'unique idéal maximal de R . $\square$

Scholie 1.10. On peut donc identifier les valuations sur un anneau intègre aux valuations sur son corps des fractions : la donnée d'une valuation sur A (anneau intègre) est exactement équivalente à celle d'une valuation sur K son corps des fractions.

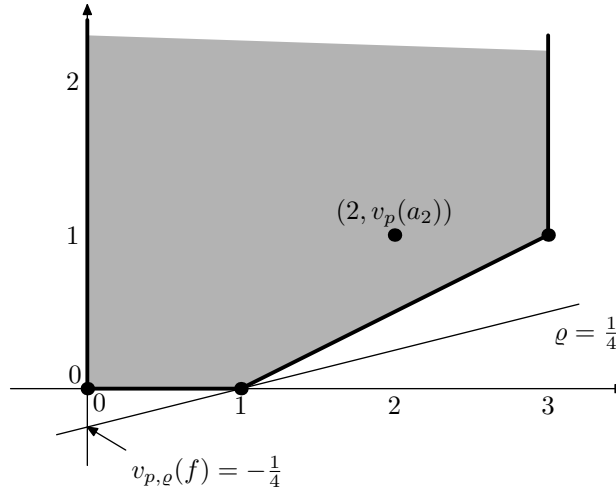
De plus, les valuations sur un corps s'identifient aux anneaux de valuation ayant ce corps pour corps des fractions : toute valuation v sur un corps K détermine un anneau de valuation $R = \{x \in K : v(x) \geq 0\}$ ayant K pour corps des fractions, et réciproquement tout anneau de valuation R ayant K pour corps des fractions détermine une unique valuation sur K qui est positive sur R .

1.11. Exemples : Si k est un corps, la fonction $v_0 = \text{ord} : k[t] \rightarrow \mathbb{Z} \cup \{\infty\}$ qui à un polynôme $f = \sum a_i t^i \in k[t]$ non nul associe le plus petit i tel que $a_i \neq 0$ (c'est-à-dire l'ordre d'annulation de f en 0, et $v_0(0) = \infty$) est une valuation sur $k[t]$ (donc s'étend de façon unique en une valuation sur $k(t)$, pour laquelle $v_0(f)$ mesure soit l'ordre d'annulation de f en 0 lorsque $v_0(f) \geq 0$ soit l'opposé de l'ordre du pôle lorsque $v_0(f) < 0$); l'anneau de valuation associé est l'ensemble des fractions rationnelles qui n'ont pas de pôle en 0. Plus généralement, on peut définir $v_a(f) = v_0(f(t-a))$ la valuation au point a pour tout $a \in k$ (ou même $a \in \bar{k}$ si k n'est pas algébriquement clos). On définit également $v_\infty(f) = -\deg f$ pour tout $f \in k[t]$ non nul (et par extension $v_\infty(f/g) = \deg g - \deg f$, et naturellement $v_\infty(0) = \infty$) : ceci fournit également une valuation sur $k[t]$ ou $k(t)$. On peut montrer que toute valuation sur $k(t)$ qui s'annule sur $k^\times$ et qui n'est pas la valuation triviale (soit $v(f) = 0$ pour tout $f \neq 0$) est de la forme v_a pour un $a \in \bar{k}$ ou bien v_∞ (à isomorphisme croissant près du groupe de valuations).

2 Pentas du polygone de Newton

2.1. Supposons maintenant que p soit un nombre premier (pour lequel on considérera la valuation p -adique v_p définie en 0.3), et ϱ un réel quelconque (que l'on appellera la *pente* dans ce qui suit). On définit une fonction $v_{p,\varrho}: \mathbb{Q}[t] \rightarrow \mathbb{R} \cup \{\infty\}$ ou *valuation penchée* p -adique de pente ϱ sur $\mathbb{Q}[t]$, de la façon suivante : si $f = \sum a_i t^i \in \mathbb{Q}[t]$ est un polynôme non nul, on pose $v_{p,\varrho}(f) = \min\{v_p(a_i) - \varrho i : a_i \neq 0\}$ (et bien entendu $v_{p,\varrho}(0) = \infty$).

2.2. Exemples : Pour tout $\varrho \in \mathbb{R}$, si $a \in \mathbb{Q}$ (considéré comme polynôme constant), alors $v_{p,\varrho}(a) = v_p(a)$. Par ailleurs, $v_{p,\varrho}(t) = -\varrho$ (et plus généralement $v_{p,\varrho}(t^i) = -\varrho i$). Si $f(t) = 1 + t + pt^2 + pt^3$, alors $v_{p,\varrho}(f)$ vaut 0 si $\varrho \leq 0$, vaut $-\varrho$ si $0 \leq \varrho \leq \frac{1}{2}$ et $1 - 3\varrho$ si $\varrho \geq \frac{1}{2}$ (cf. illustration suivante).



2.3. Remarques : On peut se figurer $v_{p,\varrho}(f)$ de la façon suivante : on trace dans le plan $\mathbb{R}^2$ l'ensemble des couples $(i, v_p(a_i))$ — alors $v_{p,\varrho}(f)$ est la plus grande ordonnée z telle que tous ces points soient au-dessus de la droite d'équation $\xi \mapsto \varrho \xi + z$. Remarquons que la construction des valuations penchées peut se faire en partant non de v_p mais de n'importe quel anneau muni d'une valuation à valeurs entières (voire rationnelles) : nous avons préféré nous restreindre au cas particulier de v_p sur $\mathbb{Q}$ pour plus de clarté.

Le résultat clé qui nous intéresse maintenant est le fait que les $v_{p,\varrho}$ sont effectivement des valuations : ceci fera l'objet de la proposition 2.6 ci-dessous ; l'inégalité $v_{p,\varrho}(fg) \geq v_{p,\varrho}(f) + v_{p,\varrho}(g)$ est assez claire, mais pour prouver l'inégalité dans l'autre sens nous allons introduire une notion intermédiaire, à savoir les abscisses extrêmes auxquelles la droite d'équation $\xi \mapsto \varrho \xi + v_{p,\varrho}(f)$ rencontre les points

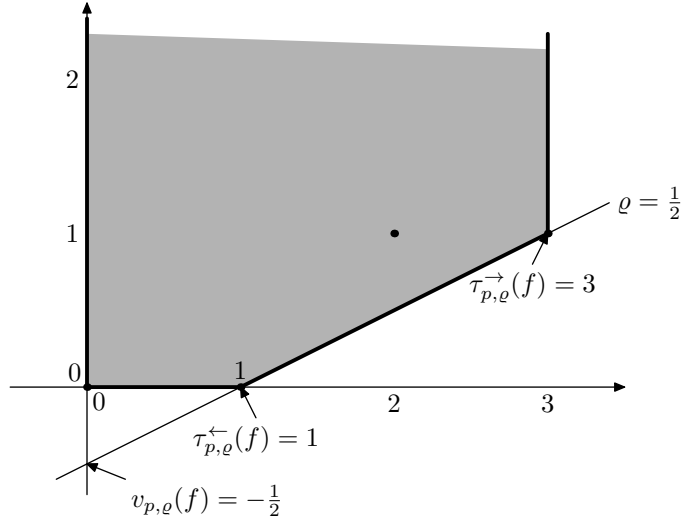
$(i, v_p(a_i))$ (certaines notions seront plus claires compte tenu de la définition 2.19, plus loin, du polygone de Newton — pour l’instant nous nous contentons de manipuler ses pentes) :

2.4. Si p est un nombre premier, et ϱ un réel quelconque, on définit pour tout polynôme $f = \sum a_i t^i \in \mathbb{Q}[t]$ non nul l’entier $\tau_{p,\varrho}^{\leftarrow}(f)$ comme le plus petit j pour lequel $v_p(a_j) = \varrho j + v_{p,\varrho}(f)$ (autrement dit, le plus petit j tel que le minimum $v_p(a_j) - \varrho j$ soit atteint) et $\tau_{p,\varrho}^{\rightarrow}(f)$ comme le plus grand tel j . On a trivialement $\text{ord } f \leq \tau_{p,\varrho}^{\leftarrow}(f) \leq \tau_{p,\varrho}^{\rightarrow}(f) \leq \deg f$.

Lorsque ϱ est irrationnel, il est évident que $\tau_{p,\varrho}^{\leftarrow}(f) = \tau_{p,\varrho}^{\rightarrow}(f)$ (la droite $\xi \mapsto \varrho \xi + z$, de pente ϱ , ne peut pas rencontrer deux points $(i, v_p(a_i))$ distincts à coefficients rationnels). Lorsque, à l’inverse, $\tau_{p,\varrho}^{\leftarrow}(f) < \tau_{p,\varrho}^{\rightarrow}(f)$, on dit que ϱ (rationnel, comme on vient de l’expliquer) est une *pente du polygone de Newton (p -adique)* de f . L’ensemble des pentes en question est fini, puisque chaque pente doit pouvoir s’écrire $\frac{v_p(a_s) - v_p(a_r)}{s - r}$ pour certains $r < s$ (à savoir $r = \tau_{p,\varrho}^{\leftarrow}(f)$ et $s = \tau_{p,\varrho}^{\rightarrow}(f)$), or il n’y a qu’un nombre fini de i avec $a_i \neq 0$.

La quantité $\tau_{p,\varrho}^{\rightarrow}(f) - \tau_{p,\varrho}^{\leftarrow}(f)$ s’appelle *largeur* de la pente ϱ (dans le polygone de Newton p -adique de f) — elle est inférieure ou égale à $\deg f - \text{ord } f$.

2.5. Exemple : Pour continuer l’exemple de 2.2, les pentes du polygone de Newton de $f(t) = 1 + t + pt^2 + pt^3$ sont $\varrho = 0$ (pour laquelle $\tau^{\leftarrow} = 0$ et $\tau^{\rightarrow} = 1$: elle est donc de largeur 1) et $\varrho = \frac{1}{2}$ (pour laquelle $\tau^{\leftarrow} = 1$ et $\tau^{\rightarrow} = 3$: elle est donc de largeur 2). Pour tout autre ϱ , on a soit $\tau^{\leftarrow} = \tau^{\rightarrow} = 0$ (lorsque $\varrho < 0$) soit $\tau^{\leftarrow} = \tau^{\rightarrow} = 1$ (lorsque $0 < \varrho < \frac{1}{2}$) soit $\tau^{\leftarrow} = \tau^{\rightarrow} = 3$ (lorsque $\varrho > \frac{1}{2}$).



Proposition 2.6. Pour tout premier p et tout $\varrho \in \mathbb{R}$, la fonction $v_{p,\varrho}$ définie en 2.1 est une valuation sur $\mathbb{Q}[t]$, au sens de la définition 1.4. De plus, lorsque $f, g \in \mathbb{Q}[t]$ sont non nuls, on a $\tau_{p,\varrho}^{\leftarrow}(fg) = \tau_{p,\varrho}^{\leftarrow}(f) + \tau_{p,\varrho}^{\leftarrow}(g)$ et l'égalité analogue pour $\tau^{\rightarrow}$.

Démonstration. Les conditions (o) et (ii) sont immédiates d'après la définition (et le fait que v_p lui-même soit une valuation). La condition restant à prouver est donc (i). Soient $f, g \in \mathbb{Q}[t]$ avec $f = \sum a_i t^i$ et $g = \sum b_i t^i$, et fixons p et ϱ . Si $h = fg$ alors $h = \sum c_i t^i$ où $c_i = \sum_{j=0}^{j=i} a_j b_{i-j}$: comme $v_p(c_i) \geq \min_{j=0}^{j=i} (v_p(a_j) + v_p(b_{i-j}))$, on a également $v_p(c_i) - \varrho i \geq \min_{j=0}^{j=i} ((v_p(a_j) - \varrho j) + (v_p(b_{i-j}) - \varrho(i-j)))$ ce qui prouve $v_{p,\varrho}(h) \geq v_{p,\varrho}(f) + v_{p,\varrho}(g)$.

On va montrer l'inégalité dans l'autre sens en même temps que l'affirmation sur $\tau^{\leftarrow}$. Soit $r = \tau_{p,\varrho}^{\leftarrow}(f)$, et $s = \tau_{p,\varrho}^{\leftarrow}(g)$. Dans la somme $c_{r+s} = \sum_{j=0}^{j=r+s} a_j b_{r+s-j}$, le terme pour lequel $j = r$ est alors de valuation p -adique $\varrho(r+s) + v_{p,\varrho}(f) + v_{p,\varrho}(g)$, et tous les autres termes sont de valuation p -adique strictement supérieure (par exemple, si $j < r$ alors $v_p(a_j) > \varrho j + v_{p,\varrho}(f)$ par minimalité de r , et $v_p(b_{r+s-j}) \geq \varrho(r+s-j) + v_{p,\varrho}(g)$ de toute manière). D'après le fait 1.6, on a prouvé $v_p(c_{r+s}) = \varrho(r+s) + v_{p,\varrho}(f) + v_{p,\varrho}(g)$, et ceci montre $v_{p,\varrho}(h) \leq v_{p,\varrho}(f) + v_{p,\varrho}(g)$ donc il y a égalité. Enfin, si $i < r+s$ alors chaque terme de $\sum_{j=0}^{j=i} a_j b_{i-j}$ est de valuation strictement supérieure à $\varrho i + v_{p,\varrho}(f) + v_{p,\varrho}(g)$, donc on a bien montré que $\tau_{p,\varrho}^{\leftarrow}(h) = r + s$. L'égalité sur $\tau^{\rightarrow}$ est entièrement analogue. $\square$

Corollaire 2.7. Si $f, g \in \mathbb{Q}[t]$ sont non nuls, les pentes du polygone de Newton (à p premier fixé) de fg sont exactement les pentes de celui de f et de celui de g . Plus précisément : la largeur d'une pente ϱ de fg est égale à la somme de ses largeurs comme pente de f et comme pente de g .

Démonstration. Le fait que, à p et ϱ fixés, $\tau_{p,\varrho}^{\leftarrow}(fg) = \tau_{p,\varrho}^{\leftarrow}(f) + \tau_{p,\varrho}^{\leftarrow}(g)$ et de même pour $\tau^{\rightarrow}$, donc aussi pour $\tau^{\rightarrow} - \tau^{\leftarrow}$ (la largeur), montre que cette dernière quantité est strictement positive pour fg (i.e., que ϱ est une pente de son polygone de Newton) si et seulement si elle l'est pour f ou pour g . $\square$

Observation 2.8. Si (pour un certain nombre premier p) une pente ϱ d'un polynôme $h \in \mathbb{Q}[t]$ a pour largeur $\deg h - \text{ord } h$ (la plus grande largeur possible), c'est qu'on a $\tau_{p,\varrho}^{\leftarrow}(h) = \text{ord } h$ et $\tau_{p,\varrho}^{\rightarrow}(h) = \deg h$.

Observation 2.9. Soit ϱ un rationnel. Alors son dénominateur réduit est le plus petit naturel non nul q tel que ϱq soit entier (i.e., que ϱ admette q pour dénominateur). Si z est un entier quelconque, deux entiers i et j tels que $\varrho i + z$ et $\varrho j + z$ soient tous les deux entiers sont donc distincts d'au moins ce dénominateur réduit.

Corollaire 2.10 (critère de Dumas). Si $h \in \mathbb{Q}[t]$ avec $\text{ord } h = 0$ (i.e., $h(0) \neq 0$) a (pour un certain premier p) une pente ϱ de son polygone de Newton (on verra plus loin que c'est la seule), dont la largeur est $\deg h$ et est égale au dénominateur réduit de ϱ (c'est-à-dire que la droite $\xi \mapsto \varrho\xi + v_{p,\varrho}(h)$ ne rencontre pas d'autre point de $\mathbb{Z}^2$ entre celui d'abscisse $\tau_{p,\varrho}^{\leftarrow}(h) = 0$ et celui d'abscisse $\tau_{p,\varrho}^{\rightarrow}(h) = \deg h$) alors h est irréductible.

Démonstration. On a $\tau_{p,\varrho}^{\leftarrow}(h) = 0$ et $\tau_{p,\varrho}^{\rightarrow}(h) = \deg h$ comme observé en 2.8. Supposons maintenant $h = fg$; notamment, $\text{ord } f = \text{ord } g = 0$ et $\deg h = \deg f + \deg g$. Comme la largeur de la pente ϱ dans h , qui vaut $\deg h$, doit être (d'après la proposition 2.6) la somme de celles de celle-ci dans f et dans g , qui sont au plus $\deg f$ et $\deg g$ respectivement, ces inégalités sont des égalités. Notamment, $\tau_{p,\varrho}^{\leftarrow}(f) = 0$ et $\tau_{p,\varrho}^{\rightarrow}(f) = \deg f$. Mais ceci impose que $\deg f$ soit multiple du dénominateur réduit de ϱ , dont on a supposé que c'était $\deg h$. L'écriture $h = fg$ est donc triviale (soit f soit g est constant). $\square$

Corollaire 2.11 (critère d'Eisenstein). Si $h = \sum a_i t^i \in \mathbb{Q}[t]$ de degré $d = \deg h$ vérifie (pour un certain premier p) $v_p(a_0) = 1$ et $v_p(a_d) = 0$ (ou le contraire) et de plus $v_p(a_i) \geq 1$ pour tout $0 < i < d$, alors h est irréductible.

Démonstration. Pour fixer les idées, on suppose $v_p(a_0) = 1$ et $v_p(a_d) = 0$. Alors pour $\varrho = -\frac{1}{d}$, les hypothèses assurent qu'il y a exactement deux points $(i, v_p(a_i))$ sur la droite $\xi \mapsto \varrho\xi$, tous les autres étant strictement au-dessus, et comme ces deux-points ont pour abscisses $\tau_{p,\varrho}^{\leftarrow}(h) = 0$ et $\tau_{p,\varrho}^{\rightarrow}(h) = d$, c'est-à-dire que ϱ est une pente de largeur maximale d . Manifestement son dénominateur réduit est d . Comme $h(0) \neq 0$ puisque $v_p(a_0)$ est fini, le corollaire 2.10 s'applique. $\square$

2.12. Note : (Voir 2.21 pour des exemples d'application de ces critères.) Tels que nous les avons énoncés, les critères de Dumas et d'Eisenstein sont simples à prouver, mais ils ont ceci d'insatisfaisant qu'ils ne cherchent pas à savoir si la pente ϱ de largeur maximale est la seule pente du polygone de Newton ou si, réciproquement, le fait d'avoir une seule pente impose qu'elle soit de largeur maximale. Nous allons donc maintenant prouver des résultats de comparaison des pentes entre elles dont l'essence, géométriquement « évidente », peut se résumer en disant que la somme des largeurs des différentes pentes p -adiques d'un polynôme $f \in \mathbb{Q}[t]$ non nul est précisément $\deg f - \text{ord } f$ (notamment, tout polynôme qui n'est pas un monôme a au moins une pente dans son polygone de Newton, et un polynôme a une seule pente si et seulement si la largeur de celle-ci est la largeur maximale $\deg f - \text{ord } f$).

2.13. Le lemme technique 2.14 a l'interprétation géométrique simple suivante : si on augmente la pente d'une droite (de l'enveloppe inférieure du polygone de Newton), tout point à gauche du point de contact droit ($\tau^{\rightarrow}$) ne peut que baisser en ordonnée. Le lemme 2.15, lui, étudie la situation à droite du point de contact droit.

Lemme 2.14. Soient $f \in \mathbb{Q}[t]$ non nul, p un nombre premier fixé et $\varrho < \varsigma$ deux réels. (a) Si $\xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$ alors $\varrho\xi + v_{p,\varrho}(f) \geq \varsigma\xi + v_{p,\varsigma}(f)$, avec inégalité stricte si $\xi < \tau_{p,\varrho}^{\rightarrow}(f)$. (b) Dualelement, si $\xi \geq \tau_{p,\varsigma}^{\leftarrow}(f)$ alors $\varrho\xi + v_{p,\varrho}(f) \leq \varsigma\xi + v_{p,\varsigma}(f)$, avec inégalité stricte si $\xi > \tau_{p,\varsigma}^{\leftarrow}(f)$.

Démonstration. Prouvons le (a). Écrivons comme d'habitude $f = \sum a_i t^i$. Soit $r = \tau_{p,\varrho}^{\rightarrow}(f)$, de sorte que $v_{p,\varrho}(f) = v_p(a_r) - \varrho r$. Si $\xi \leq r$ alors $\varrho\xi + v_{p,\varrho}(f) = \varrho(\xi - r) + v_p(a_r) \geq \varsigma(\xi - r) + v_p(a_r) \geq \varsigma\xi + v_{p,\varsigma}(f)$, et si $\xi < r$ alors il y a inégalité stricte ($\varrho(\xi - r) + v_p(a_r) > \varsigma(\xi - r) + v_p(a_r)$). Le résultat (b) est rigoureusement analogue. $\square$

Lemme 2.15. Soient $f = \sum a_i t^i \in \mathbb{Q}[t]$ non nul, p un nombre premier fixé et $\varrho \in \mathbb{R}$. Posons $r = \tau_{p,\varrho}^{\rightarrow}(f)$. Si $\varsigma \geq \varrho$ est suffisamment proche de ϱ , alors on a $v_p(a_j) - \varsigma j > v_p(a_r) - \varsigma r$ pour tout $j > r$ (pour lequel $a_j \neq 0$); on a alors $\tau_{p,\varsigma}^{\rightarrow}(f) = r$.

Démonstration. Pour ce qui est de la première affirmation : si $j > r$ alors $v_p(a_j) - \varrho j > v_p(a_r) - \varrho r$ (puisque r est le plus grand entier réalisant le minimum de $v(a_i) - \varrho i$) donc cette inégalité — stricte — vaut encore si on remplace ϱ par un $\varsigma \geq \varrho$ suffisamment proche (vu qu'il n'y a qu'un nombre fini de j). Mais pour un tel ς , il est alors vrai que le plus grand j pour lequel $v_p(a_j) - \varsigma j$ atteint son minimum est précisément $j = r$, i.e., $\tau_{p,\varsigma}^{\rightarrow}(f) = r$. $\square$

Proposition 2.16. Si $f \in \mathbb{Q}[t]$ est non nul et p est un premier fixé alors :

- lorsque $\varrho < \varsigma$ on a $v_{p,\varrho}(f) \geq v_{p,\varsigma}(f)$ et $\tau_{p,\varrho}^{\rightarrow}(f) \leq \tau_{p,\varsigma}^{\leftarrow}(f)$,
- pour $\varrho \in \mathbb{R}$ fixé, si $\varsigma > \varrho$ est suffisamment proche de ϱ alors $\tau_{p,\varrho}^{\rightarrow}(f) = \tau_{p,\varsigma}^{\leftarrow}(f) = \tau_{p,\varsigma}^{\leftarrow}(f)$
- pour tout réel $\text{ord } f < \xi < \deg f$, il existe au moins un ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$,
- mieux : pour tout réel $\text{ord } f \leq \xi < \deg f$, il existe un unique ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$ (naturellement, ceci vaut encore si on échange l'emplacement de l'inégalité stricte et de l'inégalité large aussi bien dans l'hypothèse que dans la conclusion),

- si f n'est pas un monôme, il existe au moins un ϱ qui soit une pente du polygone de Newton de f .

Démonstration. Écrivons comme d'habitude $f = \sum a_i t^i$.

- Si $\varrho < \varsigma$, le lemme 2.14 (a) (appliqué à $\xi = 0$, puisque $0 \leq \tau_{p,\varrho}^{\rightarrow}(f)$) prouve $v_{p,\varrho}(f) \geq v_{p,\varsigma}(f)$. D'autre part, toujours le lemme 2.14 (a) montre que si $j < \tau_{p,\varrho}^{\rightarrow}(f)$ alors $v_p(a_j) \geq \varrho j + v_{p,\varrho}(f) > \varsigma j + v_{p,\varsigma}(f)$ donc nécessairement $\tau_{p,\varsigma}^{\leftarrow}(f) \geq \tau_{p,\varrho}^{\rightarrow}(f)$.
- Si $\varsigma > \varrho$ est suffisamment proche de ϱ alors le lemme 2.15 montre que $\tau_{p,\varrho}^{\rightarrow}(f) = \tau_{p,\varsigma}^{\rightarrow}(f)$. Mais le point précédent montre que $\tau_{p,\varrho}^{\rightarrow}(f) \leq \tau_{p,\varsigma}^{\leftarrow}(f) \leq \tau_{p,\varsigma}^{\rightarrow}(f)$. Il y a donc des égalités partout.
- Fixons $\text{ord } f < \xi < \deg f$. La fonction $\varphi: \varrho \mapsto (\varrho \xi + v_{p,\varrho}(f)) = \min\{\varrho(\xi - i) + v_p(a_i) : a_i \neq 0\}$ est continue, étant le minimum d'un nombre fini de fonctions continues. Lorsque $\varrho \rightarrow +\infty$, l'hypothèse $\xi < \deg f$ (donc $\xi - i < 0$ pour au moins un i avec $a_i \neq 0$) assure qu'au moins une de ces fonctions tend vers $-\infty$ donc $\varphi(\varrho) \rightarrow -\infty$; de même, $\varphi(\varrho) \rightarrow -\infty$ lorsque $\varrho \rightarrow -\infty$. Soit alors ϱ tel que $\varphi(\varrho)$ atteigne son maximum. Si on avait $\xi > \tau_{p,\varrho}^{\rightarrow}(f)$ alors pour $\varsigma > \varrho$ suffisamment proche de ϱ le point précédent montre que $\xi > \tau_{p,\varsigma}^{\leftarrow}(f)$ et par le lemme 2.14 (b), on a $\varphi(\varrho) < \varphi(\varsigma)$, ce qui contredit le fait que φ devait atteindre son maximum en ϱ ; c'est donc que $\xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$. De même $\xi \geq \tau_{p,\varrho}^{\leftarrow}(f)$.
- Si on avait $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$ et $\tau_{p,\varsigma}^{\leftarrow}(f) \leq \xi < \tau_{p,\varsigma}^{\rightarrow}(f)$ pour $\varsigma > \varrho$, ceci donnerait $\tau_{p,\varrho}^{\rightarrow}(f) > \tau_{p,\varsigma}^{\leftarrow}(f)$, contredisant le premier point de la présente proposition : on a donc prouvé que, quelle que soit ξ , la pente ϱ telle que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$, lorsqu'elle existe, est unique.
Maintenant, si $\text{ord } f \leq \xi < \deg f$, montrons qu'il existe ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$. Si ξ n'est pas entier, on a déjà prouvé qu'il existe ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$, et comme $\tau^{\leftarrow}$ et $\tau^{\rightarrow}$ sont entiers, on a ce qu'on veut. Si ξ est entier, en appliquant le même résultat à $\xi + \frac{1}{2}$ (qui vérifie $\text{ord } f < \xi + \frac{1}{2} < \deg f$), on trouve ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi + \frac{1}{2} \leq \tau_{p,\varrho}^{\rightarrow}(f)$, et comme ξ et $\tau^{\leftarrow}$ sont entiers, on a $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$.
- Si f n'est pas un monôme, on peut trouver ξ tel que $\text{ord } f \leq \xi < \deg f$, et alors le résultat précédent montre qu'il existe ϱ tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi < \tau_{p,\varrho}^{\rightarrow}(f)$.

□

Scholie 2.17. Pour $f \in \mathbb{Q}[t]$ non nul et p premier fixés,

- la fonction $\varrho \mapsto v_{p,\varrho}(f)$ est continue et décroissante,

- chacune des fonctions $\varrho \mapsto \tau_{p,\varrho}^{\leftarrow}(f)$ et $\varrho \mapsto \tau_{p,\varrho}^{\rightarrow}(f)$ est croissante, la seconde majore la première et elles ne diffèrent qu'en un nombre fini de points (les pentes du polygone de Newton p -adique de f),
- $\varrho \mapsto \tau_{p,\varrho}^{\leftarrow}(f)$ est continue à gauche et $\varrho \mapsto \tau_{p,\varrho}^{\rightarrow}(f)$ est continue à droite.

2.18. On va enfin définir ce qu'est, au juste, le polygone de Newton. Il s'agit tout simplement de l'épigraphe de la fonction continue (convexe) et affine par morceaux $\mathcal{N}$ entre les abscisses $\text{ord } f$ et $\text{deg } f$ qui a les pentes ϱ , dans l'ordre croissant, chacune sur l'intervalle $[\tau_{p,\varrho}^{\leftarrow}(f); \tau_{p,\varrho}^{\rightarrow}(f)]$ (et avec $\mathcal{N}(\text{ord } f) = v(a_{\text{ord } f})$ et $\mathcal{N}(\text{deg } f) = v(a_{\text{deg } f})$); ou, de façon équivalente, de l'enveloppe convexe supérieure de l'ensemble des points $(i, v_p(a_i))$. Plus précisément :

Définition et proposition 2.19. Soit $f \in \mathbb{Q}[t]$ non nul et soit p un nombre premier. On appelle *polygone de Newton (p -adique)* de f la région du plan $\mathbb{R}^2$ constituée des points (ξ, z) tels que $\text{ord } f \leq \xi \leq \text{deg } f$ et qu'on ait $z \geq \varrho\xi + v_{p,\varrho}(f)$ pour tout $\varrho \in \mathbb{R}$. C'est l'enveloppe convexe supérieure de l'ensemble des points $(i, v_p(a_i))$, c'est-à-dire la plus petite partie convexe et stable par toute translation de vecteur $(0, z)$ avec $z > 0$ contenant les points en question. Si $\text{ord } f \leq \xi \leq \text{deg } f$ alors (ξ, z) est dans le polygone de Newton si et seulement si $z \geq \varrho\xi + v_{p,\varrho}(f)$ où ϱ est un quelconque réel tel que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$.

Démonstration. Soit C le polygone de Newton (tel que défini par la première phrase : la région du plan $\mathbb{R}^2$ constituée des points (ξ, z) tels que $\text{ord } f \leq \xi \leq \text{deg } f$ et que pour tout $\varrho \in \mathbb{R}$ on ait $z \geq \varrho\xi + v_{p,\varrho}(f)$). Montrons d'abord la dernière affirmation : supposons que $\tau_{p,\varrho}^{\leftarrow}(f) \leq \xi \leq \tau_{p,\varrho}^{\rightarrow}(f)$ et que $z \geq \varrho\xi + v_{p,\varrho}(f)$, et soit ς un réel quelconque, mettons $\varsigma > \varrho$ pour fixer les idées : alors $z \geq \varrho\xi + v_{p,\varrho}(f) \geq \varsigma\xi + v_{p,\varsigma}(f)$ d'après le lemme 2.14. Comme ceci vaut pour tout ς , on a prouvé que (ξ, z) est bien dans C . La réciproque est triviale.

Le fait que C soit convexe est clair puisqu'il est défini comme une intersection de demi-plans (chaque inégalité $z \geq \varrho\xi + v_{p,\varrho}(f)$ définit un demi-plan, ainsi que $\xi \geq \text{ord } f$ et $\xi \leq \text{deg } f$) donc de convexes. Le fait qu'il soit stable par translations vers le haut l'est encore plus. Le fait que C contienne chaque $(i, v_p(a_i))$ est la définition même des $v_{p,\varrho}(f)$. Réciproquement, si C' est un convexe stable par translation vers le haut et qui contient chaque point $(i, v_p(a_i))$, alors pour toute pente ϱ (de largeur éventuellement nulle), C' doit contenir les points $(r, v_p(a_r))$ et $(s, v_p(a_s))$ où $r = \tau_{p,\varrho}^{\leftarrow}(f)$ et $s = \tau_{p,\varrho}^{\rightarrow}(f)$, donc tout le segment fermé qui les rejoint (qui a pour pente ϱ) et tout translaté vers le haut de ce segment, c'est-à-dire, finalement, tout point (ξ, z) avec $r \leq \xi \leq s$ et $z \geq \varrho\xi + v_{p,\varrho}(f)$; or on a vu (proposition 2.16) que tout $\text{ord } f \leq \xi \leq \text{deg } f$ vérifie $r \leq \xi \leq s$ pour de tels r

et s , et on a vu ci-dessus que ceci suffit pour assurer que (ξ, z) est dans le polygone de Newton C . Donc C' contient C , et on a bien prouvé que C était le plus petit convexe stable par translation vers le haut qui contient chaque $(i, v_p(a_i))$. $\square$

Définition et proposition 2.20. Si $f \in \mathbb{Q}[t]$ est non nul et p un nombre premier, on appelle *sommet* du polygone de Newton un point de la forme $(r, v_p(a_r))$, où $r = \tau_{p,\varrho}^{\leftarrow}(f)$ ou bien $r = \tau_{p,\varrho}^{\rightarrow}(f)$ pour un certain ϱ . Comme on l'a vu ci-dessus, le polygone de Newton est aussi l'enveloppe convexe supérieure de ses sommets, ce qui justifie cette terminologie.

On appelle *fonction* du polygone de Newton de f la fonction $\mathcal{N}$ définie sur l'intervalle $[\text{ord } f; \deg f]$ et à valeurs dans $\mathbb{R}$ par $\mathcal{N}(\xi) = \max_{\varrho \in \mathbb{R}}(\varrho\xi + v_{p,\varrho}(f))$, c'est-à-dire la fonction dont le graphe est la frontière inférieure du polygone de Newton. Cette fonction est continue, convexe et affine par morceaux sur $[\text{ord } f; \deg f]$.

Démonstration. De nouveau, tous les résultats découlent essentiellement du fait que $[\text{ord } f; \deg f]$ est la réunion des $[\tau_{p,\varrho}^{\leftarrow}(f); \tau_{p,\varrho}^{\rightarrow}(f)]$ et que sur chacun de ces intervalles $\mathcal{N}(\xi)$ vaut $\varrho\xi + v_{p,\varrho}(f)$. $\square$

2.21. Exemples : Le critère d'Eisenstein 2.11 (appliqué à $p = 3$) montre que $t^3 + 9t + 6 \in \mathbb{Q}[t]$ est irréductible.

Le critère de Dumas 2.10 (appliqué à $p = 2$) montre que $t^3 + 2t^2 + 4 \in \mathbb{Q}[t]$ est irréductible (la seule pente étant $-\frac{2}{3}$).

Bien que $t^2 - 1 \in \mathbb{Q}[t]$ n'ait (pour tout p) qu'une seule pente ($\varrho = 0$) dans son polygone de Newton, il n'est évidemment pas irréductible ($t^2 - 1 = (t - 1)(t + 1)$) : la largeur de ϱ est ici 2, qui est strictement supérieure à son dénominateur réduit (1).

Le critère de Dumas ne s'applique pas tel quel à $h = 2t^4 + 2t^3 + 3t^2 + 6 \in \mathbb{Q}[t]$. Cependant, il est tout de même irréductible, et on peut le montrer par une analyse un peu plus fine. En effet, le polygone de Newton 2-adique a les pentes $-\frac{1}{2}$ et $\frac{1}{2}$ avec largeurs respectives 2 et 2, et le polygone de Newton 3-adique a les pentes $-\frac{1}{3}$ et 0 avec largeurs respectives 3 et 1 : le premier montre donc que si h se réduit non trivialement cela doit être comme produit de deux polynômes de degré 2 (irréductibles) tandis que le second montre que cela doit être comme produit d'un polynôme de degré 1 et d'un autre de degré 3; ces deux décompositions étant incompatibles, h est irréductible.

Exercice 2.22. Soit $n \geq 1$: montrer que le polynôme de l'exponentielle tronquée, $h = 1 + t + \frac{1}{2}t^2 + \frac{1}{6}t^3 + \cdots + \frac{1}{n!}t^n$, est irréductible sur $\mathbb{Q}$. (*Indication* : Pour

chaque nombre premier p divisant n , montrer que tout facteur de h doit être de degré multiple de $p^{v_p(n)}$.)

3 Réduction modulo une pente

3.1. Les techniques exposées dans la partie précédente permettent d'expliquer, par exemple, pourquoi un polynôme tel que $t^3 + 4 \in \mathbb{Q}[t]$ est irréductible, mais elles sont impuissantes face à, disons, $t^4 + 2t^2 + 4$, dont le polygone de Newton, bien qu'il n'ait qu'une seule pente (en l'occurrence, $-\frac{1}{2}$), n'est pas simple (la largeur de cette pente, en l'occurrence 4, est un multiple strict de son dénominateur réduit, en l'occurrence 2) de sorte que le critère 2.10 ne s'applique pas.

Nous cherchons donc à développer une technique plus raffinée, celle de *réduction modulo une pente*, qui permet de traiter plus de cas. Il s'agit de généraliser simultanément les résultats déjà vus et le critère simple suivant : lorsque le polygone de Newton a pour seule pente la pente nulle $\varrho = 0$ avec valuation $v_{p,0}$ nulle et largeur maximale (c'est-à-dire, plus simplement, lorsque $v_p(a_0) = v_p(a_{\deg f}) = 0$), il suffit pour garantir l'irréductibilité que la réduction de f modulo p (qui a bien un sens puisque tous les coefficients sont de valuation $v_p(a_i) \geq 0$) soit irréductible dans $\mathbb{F}_p[t]$. Ainsi $t^2 + t + 1 \in \mathbb{Q}[t]$ est-il irréductible parce qu'il l'est dans $\mathbb{F}_2[t]$.

Commençons par quelques définitions simples (on dit qu'un rationnel $x \in \mathbb{Q}$ admet q pour dénominateur, où $q \in \mathbb{N}^{>0}$, lorsque qx est un entier) :

Définition et proposition 3.2. Soit $f \in \mathbb{Q}[t]$ et soit p un nombre premier fixé. Soit ϱ un nombre rationnel, de dénominateur réduit $q \in \mathbb{N}^{>0}$. La largeur de la pente ϱ (déjà définie en 2.4) est l'entier naturel $\ell = \tau_{p,\varrho}^{\rightarrow}(f) - \tau_{p,\varrho}^{\leftarrow}(f)$ (qui est strictement positif lorsque ϱ est effectivement une pente du polygone de Newton p -adique de f) : cette largeur est un multiple entier de q , et on appelle *degré* de ϱ le quotient $\ell/q \in \mathbb{Z}$.

Démonstration. L'affirmation est triviale eu égard au fait que ℓ est effectivement un dénominateur de ϱ (puisque $\varrho = \frac{v_p(a_s) - v_p(a_r)}{\ell}$ avec $r = \tau_{p,\varrho}^{\leftarrow}(f)$ et $s = \tau_{p,\varrho}^{\rightarrow}(f)$) de sorte que $\ell = s - r$. $\square$

Proposition 3.3. Soit p un nombre premier fixé et soit ϱ un nombre rationnel, de dénominateur réduit $q \in \mathbb{N}^{>0}$. L'ensemble $v_{p,\varrho}(\mathbb{Q}[t] \setminus \{0\}) \subseteq \mathbb{R}$ des valuations possibles des polynômes à coefficients rationnels pour la valuation penchée $v_{p,\varrho}$ est exactement l'ensemble $\frac{1}{q}\mathbb{Z}$ des rationnels qui admettent q pour dénominateur.

Démonstration. Si $f \in \mathbb{Q}[t]$ est un polynôme non nul quelconque, il est clair sur la définition même que $v_{p,\varrho}(f) \in \frac{1}{q}\mathbb{Z}$. Réciproquement, tout élément de $\frac{1}{q}\mathbb{Z}$ peut s'écrire $w + \varrho k$ avec $w \in \mathbb{Z}$ et $k \in \mathbb{N}$, et alors $p^w t^k$ a la valuation penchée voulue. $\square$

Définition 3.4. Soit p un nombre premier fixé et soit ϱ un nombre rationnel, de dénominateur réduit $q \in \mathbb{N}^{>0}$. Pour tout $f = \sum a_i t^i \in \mathbb{Q}[t]$ tel que $v_{p,\varrho}(f) \geq 0$, on appelle *réduction de f modulo $(p$ et suivant) la pente ϱ* le polynôme $\tilde{f} = \tilde{a}_j \tilde{t}^j \in \mathbb{F}_p[\tilde{t}]$, où pour tout indice j on appelle $\tilde{a}_j$ la réduction modulo p de $p^{-qj\varrho} a_{qj}$.

3.5. Remarques : Pour que la définition précédente ait un sens, il faut noter que $v_p(p^{-qj\varrho} a_{qj}) \geq 0$ (pour espérer pouvoir le réduire modulo p) : or ceci est bien le cas car $v_p(p^{-qj\varrho} a_{qj}) = v_p(a_{qj}) - qj\varrho \geq v_{p,\varrho}(f) \geq 0$. D'autre part, si i n'est pas un multiple de q , alors on a encore $v_p(a_i) - i\varrho \geq v_{p,\varrho}(f) \geq 0$, mais comme $(i\varrho \text{ donc})$ $v_p(a_i) - i\varrho$ n'est pas un entier, cette inégalité est stricte, donc il est intuitivement sensé de ne considérer dans la définition de $\tilde{f}$ que les coefficients a_{qj} (en omettant tous les autres a_i).

Proposition 3.6. Fixons p un nombre premier et ϱ un nombre rationnel. Si $f, g \in \mathbb{Q}[t]$ vérifient tous deux $v_{p,\varrho} \geq 0$ alors, en réduisant modulo la pente ϱ , on a $\widetilde{f+g} = \tilde{f} + \tilde{g}$ et $\widetilde{fg} = \tilde{f}\tilde{g}$ avec les notations introduites en 3.4.

Démonstration. Soit q le dénominateur réduit de ϱ . Écrivons $f = \sum a_i t^i$ et $g = \sum b_i t^i$ et bien sûr $\tilde{f} = \tilde{a}_j \tilde{t}^j$ et $\tilde{g} = \tilde{b}_j \tilde{t}^j$ où $\tilde{a}_j$ est la réduction modulo p de $p^{-qj\varrho} a_{qj}$ et de même pour $\tilde{b}_j$.

La première formule ne pose pas de difficulté particulière : si $c_i = a_i + b_i$ est le coefficient de degré i de $f + g$ alors $p^{-qj\varrho} c_{qj} = p^{-qj\varrho} (a_{qj} + b_{qj})$ se réduit modulo p en $\tilde{a}_j + \tilde{b}_j$, ce qui prouve la formule voulue.

Pour ce qui est de la seconde formule, soit $c_i = \sum_{l=1}^{l=i} a_l b_{i-l}$ le coefficient de degré i de fg . On a $v_p(a_l) \geq \varrho l$ — et cette inégalité est stricte si l n'est pas multiple de q car alors ϱl n'est pas entier ; de même, on a $v_p(b_{i-l}) \geq \varrho(i-l)$ avec inégalité stricte si $i-l$ n'est pas multiple de q . Posons $i = qj$: dans l'écriture de c_{qj} , tous les termes $a_l b_{qj-l}$ ont alors valuation p -adique au moins ϱqj , et ceux pour lesquels l n'est pas multiple de q ont valuation strictement plus que ϱqj ; par conséquent, dans la somme $p^{-qj\varrho} c_{qj} = \sum_{l=1}^{l=qj} p^{-qj\varrho} a_l b_{qj-l}$, tous les termes ont valuation positive et ceux pour lesquels l n'est pas multiple de q ont valuation strictement positive, donc en réduction modulo p on peut ne conserver que les termes où $l = qm$, c'est-à-dire les $p^{-qm\varrho} a_{qm} \cdot p^{-q(j-m)\varrho} b_{q(j-m)}$, et en réduisant modulo p on trouve $\tilde{c}_j = \sum_{m=1}^{m=j} \tilde{a}_m \tilde{b}_{j-m}$. C'est ce qu'il fallait démontrer. $\square$

Corollaire 3.7. Si $h \in \mathbb{Q}[t]$ avec $\text{ord } h = 0$ (i.e., $h(0) \neq 0$) n'a (pour un certain premier p) qu'une seule pente ϱ dans son polygone de Newton et que, en posant $v = v_{p,\varrho}(h)$, la réduction de $p^{-v}h$ modulo la pente ϱ (au sens de 3.4) est irréductible, alors h est irréductible.

Démonstration. La pente ϱ , étant la seule, est de largeur maximale (en vertu de la proposition 2.16), c'est-à-dire ici $\deg h$: i.e., $\tau_{p,\varrho}^{\rightarrow}(h) = \deg h$ tandis que $\tau_{p,\varrho}^{\leftarrow}(h) = 0$.

Quitte à multiplier h par p^{-v} , on peut supposer $v = 0$. Supposons maintenant $h = fg$: de même, on peut supposer $v_{p,\varrho}(f) = 0$, et alors la proposition 2.6 implique que $v_{p,\varrho}(g) = 0$, et, comme en 2.10, que $\tau_{p,\varrho}^{\rightarrow}(f) = \deg f$ et $\tau_{p,\varrho}^{\rightarrow}(g) = \deg g$ tandis que, bien entendu, $\tau_{p,\varrho}^{\leftarrow}(f) = \tau_{p,\varrho}^{\leftarrow}(g) = 0$. Notons $\tilde{f}, \tilde{g}, \tilde{h}$ les réductions de f, g, h respectivement modulo la pente ϱ : on a $\deg \tilde{f} = \frac{1}{q} \deg f$ et les résultats analogues pour g et h d'après ce qu'on vient de remarquer sur la largeur de la pente ϱ dans ces différents polynômes. Or la proposition 3.6 montre que $\tilde{h} = \tilde{f}\tilde{g}$, et comme on a supposé $\tilde{h}$ irréductible, ceci implique $\deg \tilde{f} = 0$ ou $\deg \tilde{g} = 0$, soit $\deg f = 0$ ou $\deg g = 0$. $\square$

3.8. Remarque : Le critère 2.10 n'est que le cas particulier de ce dernier corollaire lorsque $\tilde{h}$ est de degré 1 (donc certainement irréductible).

3.9. Exemples : Le polynôme $h = t^4 + 2t^2 + 4$ a pour unique pente $-\frac{1}{2}$ dans son polygone de Newton 2-adique. Quitte à multiplier par $\frac{1}{4}$ (pour avoir $v_{2,-\frac{1}{2}}(h) = 0$), on peut réduire h modulo cette pente et la réduction vaut $\tilde{h} = \tilde{t}^2 + \tilde{t} + 1$ (le dénominateur réduit de $\varrho = -\frac{1}{2}$ vaut $q = 2$, de sorte que $\tilde{h}$ est de degré deux fois plus petit que la largeur de la pente, d'où l'intérêt de la notion introduite en 3.2). La pente ϱ n'est pas de degré 1 ici (le polynôme $\tilde{h}$ n'est pas de degré 1) mais 2, mais comme le polynôme h est irréductible sur $\mathbb{F}_2$ (son corps de rupture est $\mathbb{F}_4$), on en déduit néanmoins que h est irréductible sur $\mathbb{Q}$.

De même, le polynôme $t^4 + 3t^3 - 9t^2 + 9$ est irréductible sur $\mathbb{Q}$ comme on le voit en considérant son polygone de Newton 3-adique : ce dernier a pour unique pente $-\frac{1}{2}$ avec largeur 4 (degré 2), et quitte à renormaliser la réduction modulo cette pente est $\tilde{t}^2 + 1$, qui est irréductible dans $\mathbb{F}_3$.