Polygones de Newton et groupes de Galois

Huan CHEN, Hongzhou LIN
Sous la direction de
Tony LY

22 juin 2011

Table des matières

1 Introduction

Dans notre exposé, on étudie les groupes de Galois sur $\mathbb{Q}$ des polynômes de Taylor de l'exponentielle et des polynômes de Laguerre généralisés. On va utiliser un outil puissant : le polygone de Newton. Le polygone de Newton d'un polynôme est défini comme l'enveloppe convexe supérieure dans $\mathbb{R}^2$ d'un nombre fini de points à coordonnées rationnelles associées à ce polynôme. Pour établir la théorie du polygone de Newton, on a besoin de considérer le corps $\mathbb{Q}_p$ (p est un nombre premier), la complétion de $\mathbb{Q}$ muni d'une nouvelle valeur absolue $|\quad|_p$. Dans $\mathbb{Q}_p$, il y a des analogues du corps des nombres réels $\mathbb{R}$. Par exemple, on peut développer les éléments dans $\mathbb{Q}_p$ en base p comme le développement décimal dans $\mathbb{R}$. Dans $\mathbb{Q}_p$, on a le lemme de Hensel qui nous donne un moyen de trouver des racines d'un polynôme sous certaine condition. La technique d'approximation pour le lemme de Hesnsel est essentiellement la même que celle de méthode de Newton pour faire un calcul approchée d'une racine réelle d'un polynôme. De plus, on va aussi voir comment étendre cette valeur absolue sur les extensions algébriques de $\mathbb{Q}_p$. C'est dans cette procédure qu'un phénomène intéressant appelé la ramification se produit.

Nous tenons à remercier Tony LY qui, en tant que directeur de mémoire, nous donne beaucoup de conseils précieux sur l'exposé et la rédaction. Nous remercions aussi Yichao HUANG qui lit notre mémoire soigneusement et nous aide à éviter beaucoup de fautes.

2 Valeurs absolues et nombres p-adiques

Dans cette partie, on commence par définir une famille de nouvelles valeurs absolues $|\quad|_p$ sur $\mathbb{Q}$. Elles nous donneront d'autres critères pour juger si deux points sont proches ou non. Elles ont la propriété ultramétrique et comportent très différemment de celle qu'on a vue il y a longtemps. En effet, par le théorème 2.7 suivant, on voit qu'avec la valeur absolue usuelle, elles sont toutes les valeurs absolues possibles sur $\mathbb{Q}$. Comme $\mathbb{Q}$ est dénombrable, par le théorème de Baire, $(\mathbb{Q}, |\quad|_p)$ n'est pas complet. On va aussi étudier sa complétion $\mathbb{Q}_p$, l'ensemble des nombres p-adiques. C'est sur ce corps et ses extensions algébriques qu'on va établir la théorie du polygone de Newton.

2.1 Les valeurs absolues sur $\mathbb{Q}$

Définition 2.1.

1 Une valeur absolue sur un corps F est une application $|\quad| : F \to \mathbb{R}_+$ qui vérifie :
- $|x| = 0$ si et seulement si $x = 0$;
- $|x \cdot y| = |x| \cdot |y|$;
- $|x + y| \leq |x| + |y|$.

Il y a une distance naturelle associée à une valeur absolue qui est définie par $d(x, y) = |x - y|$.

2 Une distance est dite non archimédienne (ou ultramétrique) si $d(x, y) \leq \max(d(x, z), d(z, y))$. Une valeur absolue est dite non archimédienne (ou ultramétrique) si la distance associée l'est. Sinon, elle est dite archimédienne.

Définition 2.2. Soient p un nombre premier et a un nombre entier non nul. On définit

$$\mathrm{ord}_p a = \max\{m \in \mathbb{N} \mid a \equiv 0 \pmod{p^m}\}.$$

Et on definit aussi $\mathrm{ord}_p 0 = +\infty$. Pour un nombre $x = \frac{a}{b} \in \mathbb{Q}$, $\mathrm{ord}_p x \overset{\text{def}}{=} \mathrm{ord}_p a - \mathrm{ord}_p b$.

Remarque 2.3. Il est facile de voir que la définition de $\mathrm{ord}_p x$ ne dépend pas de l'écriture $\frac{a}{b}$.

Définition 2.4. Soit p un nombre premier. On définit une application $|\quad|_p$ de $\mathbb{Q}$ dans $\mathbb{R}_+$ comme suit :

$$|x|_p = p^{-\mathrm{ord}_p x}.$$

Proposition 2.5. *L'application $|\quad|_p$ est une valeur absolue non archimédienne sur $\mathbb{Q}$.*

Remarque 2.6. On appelle $|\quad|_p$ la valeur absolue p-adique.

Démonstration. Il est évident de voir :
- $|x|_p = 0 \quad$ si et seulement si $x = 0$;
- $|x|_p \cdot |y|_p = |x \cdot y|_p$, pour tout $x, y \in \mathbb{Q}$.

Il reste à montrer l'inégalité ultramétrique. On suppose $x = \frac{a}{b}, y = \frac{c}{d}$ où $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(c,d) = 1$. On a $x + y = \dfrac{ad+bc}{bd}$,

$$\begin{aligned}
\mathrm{ord}_p(x+y) &= \mathrm{ord}_p(ad+bc) - \mathrm{ord}_p b - \mathrm{ord}_p d \\
&\geq \min(\mathrm{ord}_p ad, \mathrm{ord}_p bc) - \mathrm{ord}_p b - \mathrm{ord}_p d \\
&= \min(\mathrm{ord}_p a + \mathrm{ord}_p d, \mathrm{ord}_p b + \mathrm{ord}_p c) - \mathrm{ord}_p b - \mathrm{ord}_p d \\
&= \min(\mathrm{ord}_p a - \mathrm{ord}_p b, \mathrm{ord}_p b - \mathrm{ord}_p d) \\
&= \min(\mathrm{ord}_p x, \mathrm{ord}_p y).
\end{aligned}$$

Donc $|x+y|_p = p^{-\mathrm{ord}_p(x+y)} \leq \max(p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}) = \max(|x|_p, |y|_p)$. □

On dit que deux valeurs absolues $|\quad|_1$, $|\quad|_2$ sur un corps sont équivalentes s'il existe $\alpha \in \mathbb{R}_+^*$ vérifiant $|\quad|_1 = |\quad|_2^\alpha$. Il est aussi équivalent de dire qu'elles définissent la même notion des suites de Cauchy sur ce corps. Donc si on remplace p dans la définition de $|\quad|_p$ par une constante $\rho \in]0,1[$ quelconque, (i.e $|x|'_p = \rho^{-\mathrm{ord}_p x}$ pour $x \in \mathbb{Q}$) la valeur absolue qu'on obtiendra est équivalente à celle qu'on a définie avant. Parfois, on note aussi la valeur absolue usuelle sur $\mathbb{Q}$ par $|\quad|_\infty$. Par convention, la valeur absolue triviale signifie la valeur absolue qui prend la valeur 0 en 0 et 1 sur les autres points.

Théorème 2.7 (Ostrowski)**.** *Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à l'une des $|\quad|_p$ où p est premier ou $p = \infty$.*

Démonstration. On note cette valeur absolue $|\quad|$. On va distinguer deux cas différents.

Cas 1. Supposons qu'il existe un nombre entier positif m tel que $|m| > 1$. Soit n_0 le plus petit nombre entier positif qui satisfait cette condition. Comme $|n_0| > 1$, il existe un réel $\alpha > 0$ tel que $|n_0| = n_0^\alpha$. Soit $n \in \mathbb{N}^*$, on le développe en base n_0, i.e

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_s n_0^s, \text{ où } a_i \in \mathbb{Z} \quad \text{et } 0 \leq a_i < n_0\,, a_s \neq 0.$$

Donc

$$\begin{aligned}
|n| &\leq |a_0| + |a_1 n_0| + |a_2 n_0^2| + \cdots + |a_s n_0^s| \\
&= |a_0| + |a_1| \cdot n_0^\alpha + |a_2| \cdot n_0^{2\alpha} + \cdots + |a_s| \cdot n_0^{s\alpha}.
\end{aligned}$$

Comme tous les a_i sont $< n_0$, par notre choix de n_0, nous avons $|a_i| \leq 1$. Donc

$$\begin{aligned} |n| &\leq 1 + n_0^{\alpha} + n_0^{2\alpha} + \cdots + n_0^{s\alpha} \\ &= n_0^{s\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-s\alpha}) \\ &\leq n^{\alpha} \sum_{i=0}^{\infty} n_0^{-i\alpha}, \quad \text{car } n \geq n_0^s. \end{aligned}$$

On note C la somme infinie dans le terme de droite. Donc

$$|n| \leq Cn^{\alpha} \quad \text{pour tout } n \in \mathbb{N}^*. \tag{1}$$

Maintenant, prenons n et N quelconques, remplaçons n par n^N dans l'équation (1) et prenons la racine $N^{\text{ième}}$:

$$|n| \leq \sqrt[N]{C} n^{\alpha}.$$

Quand N tend vers ∞ pour n fixé, on obtient

$$|n| \leq n^{\alpha}. \tag{2}$$

On montre l'inégalité dans l'autre sens. On suppose que n s'écrit en base n_0 comme avant, alors on a $n_0^{s+1} > n \geq n_0^s$. Comme $|n_0^{s+1}| = |n + n_0^{s+1} - n| \leq |n| + |n_0^{s+1} - n|$, on a

$$\begin{aligned} |n| &\geq |n_0^{s+1}| - |n_0^{s+1} - n| \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha} \quad \text{(par l'équation (2))} \\ &\geq n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^{\alpha} \quad \text{(car } n \geq n_0^s\text{)} \\ &= n_0^{(s+1)\alpha} \Big[1 - (1 - \frac{1}{n_0})^{\alpha}\Big] \\ &\geq C' n^{\alpha}, \end{aligned}$$

pour une constante C' qui ne dépend que de n_0 et α. On utilise cette inégalité pour n^N, et prend la racine $N^{\text{ième}}$, puis on fait tendre $N \to \infty$. On obtient : $|n| \geq n^{\alpha}$. Donc

$$|n| = n^{\alpha} \quad \text{pour } n \in \mathbb{N}.$$

À cause de l'égalité $|-1| = 1$ (puisque $|-1|^2 = |1| = 1$) et parce que tout rationnel $x = \frac{a}{b}$ vérifie $|x| = \frac{|a|}{|b|}$, on a

$$|x| = |x|_{\infty}^{\alpha} \quad \text{pour } x \in \mathbb{Q}.$$

Donc par définition précédente, $|\quad|$ est équivalente à la valeur absolue usuelle $|\quad|_{\infty}$.

Cas 2. Supposons $|n| \leq 1$ pour tout nombre entier n. Soit n_0 le plus petit n positif tel que $|n| < 1$. Un tel n_0 existe car on a supposé que cette valeur absolue n'est pas triviale.

D'abord, n_0 est nécessairement premier. Sinon, on aurait $n = n_1 \cdot n_2$ avec n_1 et n_2 tous les deux $< n$, donc $|n_1| = |n_2| = 1$, $|n| = |n_1| \cdot |n_2| = 1$; c'est absurde. On note p ce nombre premier.

On affirme que $|q| = 1$ si p et q sont premiers entre eux. Sinon, pour N suffisamment grand, on a $|q^N| = |q|^N < \frac{1}{2}$. Aussi, pour M suffisamment grand, on aurait $|p^M| < \frac{1}{2}$. Puisque p^M et q^N sont premiers entre eux, on peut trouver deux nombres entiers m et n, tels que $mp^M + nq^N = 1$. Mais, on aurait

$$1 = |1| = |mp^M + nq^N| \leq |mp^M| + |nq^N| = |m| \cdot |p^M| + |n| \cdot |q^N|.$$

Mais $|m|, |n| \leq 1$, donc

$$1 \leq |p^M| + |q^N| < \frac{1}{2} + \frac{1}{2} = 1.$$

C'est absurde. Donc $|q| = 1$ pour tout q premier à p.

Pour tout nombre entier $a = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r}$. On a $|a| = |p_1|^{b_1} |p_2|^{b2} \dots |p_r|^{b_r}$. Si on note $\rho = |p| < 1$, on a bien

$$|a| = \rho^{\mathrm{ord}_p a}. \tag{3}$$

Aussi, l'équation (3) est vraie pour tous les nombres rationnels. Donc elle est équivalente à $|\quad|_p$. □

Remarque 2.8. En fait, que ce soit p premier ou $p = \infty$, $\mathbb{Q}$ muni de la valeur absolue $|\quad|_p$ n'est pas complet. Comme $\mathbb{Q}$ est dénombrable, on note ses éléments $\{a_i\}_{i=0}^{\infty}$, alors

$$\mathbb{Q} = \bigcup_{i=0}^{\infty} \{a_i\}.$$

Tout singleton $\{a_i\}$ est d'intérieur vide. Par le théorème de Baire, $(\mathbb{Q}, |\quad|_p)$ n'est pas complet.

2.2 La complétion de $(\mathbb{Q}, |\quad|_p)$

Soit p un nombre premier. Dans la section précédente, on a vu que $(\mathbb{Q}, |\quad|_p)$ n'est pas complet. On note $\mathbb{Q}_p$ sa complétion et on prolonge $|\quad|_p$ à $\mathbb{Q}_p$ par continuité. On note $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | \, |a|_p \leq 1\}$ qui est un anneau. Les éléments de $\mathbb{Z}_p$ s'appellent les entiers p-adiques. Le théorème suivant nous donne une expression explicite des nombres p-adiques.

Remarque 2.9. Le corps des rationnels $\mathbb{Q}$ s'injecte dans $\mathbb{Q}_p$ car $(\mathbb{Q}, |\quad|_p)$ est séparé. De plus, $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$. Pour plus d'information sur la procédure de la complétion, on peut voir la polycopie du cours topologie par Frédéric Paulin.

Théorème 2.10 (Le développement p-adique)**.** *Tout élément a non nul de $\mathbb{Q}_p$ s'écrit de manière unique comme :*

$$a = a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \dots + a_m p^m + \dots,$$

où $n \in \mathbb{Z}$, $0 \leq a_i < p, a_n \neq 0$.

Démonstration. D'abord, cette expression converge dans $\mathbb{Q}_p$. Si on note

$$S_r = \sum_{i=0}^{r} a_{n+i} p^{n+i},$$

alors on a

$$|S_r - S_{r+s}|_p \leq \max_{i=1,2\dots s} |a_{r+i} p^{r+i}|_p \leq p^{-r}.$$

Elle est une suite de Cauchy dans $\mathbb{Q}_p$, donc elle converge dans $\mathbb{Q}_p$.

Puis, on montre l'unicité. Soient deux expressions S et $\widetilde{S}$ différentes. Quitte à multiplier par un p^N avec N assez grand, on peut supposer

$$S = \sum_{i=0}^{\infty} a_i p^i, \quad \widetilde{S} = \sum_{i=0}^{\infty} b_i p^i,$$

où $a_i, b_i \in \mathbb{Z}$ et $0 \leq a_i, b_i < p$. On pose $n_0 = \min\{i \geq 0 | a_i \neq b_i\}$ qui existe parce que S et $\tilde{S}$ sont différents. Alors, on a

$$|S - \widetilde{S}|_p = |a_{n_0} - b_{n_0}|_p \cdot p^{-n_0} > 0.$$

Enfin, on montre que tout élément a non nul dans $\mathbb{Q}_p$ peut s'écrire sous la forme ci-dessus. À une constante multiplicative d'une puissance de p près, on peut supposer $|a|_p \leq 1$. Comme a est non nul, il existe une suite dans $\mathbb{Q}$ non nulle (b_n) telle que $b_n \to a$ quand $n \to \infty$ et $b_n \neq 0$. Pour un $\epsilon < \frac{1}{p}|a|_p$ fixé, il existe un nombre entier N, tel que pour tout $m, n \geq N$, on ait $|b_m - b_n|_p < \epsilon$. On suppose $b_N = \frac{s}{t}$, où s, t sont premiers entre eux. Comme on a

$$|b_N - a|_p = \lim_{n \to \infty} |b_N - b_n|_p \leq \epsilon,$$

on déduit que $|b_N|_p = |a|_p \leq 1$ et on note $M = -\log_p |a|_p \in \mathbb{Z}$. Donc $p \nmid t$ et $s = p^M \cdot s'$ avec $p \nmid s'$. Pour $i > 1$ fixé, on peut trouver deux entiers m, n vérifiant $mt + np^i = 1$. Prenons $\alpha = sm \in \mathbb{Z}$. Alors, on a

$$|b_N - \alpha|_p = |\frac{s}{t} - sm|_p = |\frac{s}{t}|_p |1 - mt|_p = |\frac{s}{t}|_p \cdot |-np^i|_p \leq |a|_p p^{-i}$$

donc $|\alpha|_p \leq |a|_p$. Posons $\alpha = a_0 p^M + a' p^{M+1}$, où $a' \in \mathbb{Z}$ et $0 \leq a_0 < p$ entier. Alors on a

$$|a - a_0 p^M|_p \leq \max(|a - b_N|_p, |b_N - \alpha|_p, |\alpha - a_0 p^M|_p) \leq p^{-(M+1)} = p^{-1}|a|_p.$$

De la même façon, on montre qu'il y a $a_1 \in \{0, 1, \ldots, p-1\}$ avec $|a - a_0 p^M - a_1 p^{M_1}|_p \leq p^{-1}|a - a_0 p^M|_p \leq p^{-2}|a|_p$, où $M_1 = -\log_p |a - a_0 p^M|_p \geq M + 1$. Par récurrence, on finit la démonstration. □

On a aussi un résultat de compacité.

Proposition 2.11. *L'anneau $\mathbb{Z}_p$ est compact pour $|\quad|_p$.*

Démonstration. Comme $\mathbb{Z}_p$ est muni d'une distance, il suffit de montrer que pour toute suite bornée (x_n) de $\mathbb{Z}_p$, on peut en extraire une sous-suite qui converge. On peut les écrire :

$$x_n = a_0^{(n)} + a_1^{(n)} p + \cdots + a_i^{(n)} p^i + \cdots \quad \text{où } a_i^{(n)} \in \{0, 1, \ldots, p-1\}.$$

D'abord, on peut en extraire une sous-suite $(x_n^{(1)})$ dont les premiers chiffres sont égaux. Après, on peut extraire de $(x_n^{(1)})$ une sous-sous-suite $(x_n^{(2)})$ dont les deuxièmes chiffres sont égaux, etc. Prenant $y_n = x_n^{(n)}$, on trouve une sous-suite de (x_n) qui converge, d'où la compacité de $(\mathbb{Z}_p, |\quad|_p)$. □

3 Outils supplémentaires sur les corps p-adiques

Comme $\mathbb{Q}$ s'injecte dans $\mathbb{Q}_p$, les extensions algébriques de $\mathbb{Q}$ s'injectent naturellement dans la clôture algébrique de $\mathbb{Q}_p$. Pour étudier les groupes de Galois des polynômes sur $\mathbb{Q}$, il est naturel de considérer les extensions algébriques de $\mathbb{Q}_p$. On va voir comment on peut étendre $|\quad|_p$ sur ces extensions de $\mathbb{Q}_p$. Dans la procédure d'extension, un phénomène appelé la ramification apparaît.

3.1 L'extension de la valeur absolue sur une extension algébrique de $\mathbb{Q}_p$

Dans toute la suite, on fixe une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$; et toute extension algébrique de $\mathbb{Q}_p$ sera donc vue comme un sous-corps de $\overline{\mathbb{Q}}_p$. Dans cette partie, on montre qu'on peut étendre $|\quad|_p$ sur une extension algébrique de $\mathbb{Q}_p$, et que cette extension est unique.

Définition 3.1. Soit K un espace vectoriel sur un corps F muni d'une valeur absolue $|\quad|$. Une norme $\|\quad\|$ sur K est une application de K dans $\mathbb{R}_+$, qui vérifie :

1. $\|x\| = 0$ si et seulement si $x = 0$;
2. $\|\lambda x\| = |\lambda| \cdot \|x\|$ pour $\lambda \in F$, $x \in K$;
3. $\|x + y\| \leq \|x\| + \|y\|$, pour $x, y \in K$.

Proposition 3.2 (L'unicité)**.** *Soit K une extension algébrique de $\mathbb{Q}_p$. Il existe au plus une valeur absolue sur K qui étend $|\quad|_p$.*

Démonstration. D'abord, on traite le cas où $n = [K : \mathbb{Q}_p] < \infty$. Supposons qu'il y a deux valeurs absolues $|\quad|_1$ et $|\quad|_2$ définies sur K qui étendent $|\quad|_p$. K peut aussi être vu comme un espace vectoriel sur $\mathbb{Q}_p$ de dimension finie. Fixons une base $\{v_i\}_{i=1}^n$. On définit une norme sur K.

$$\|a_1v_1 + a_2v_2 + \cdots + a_nv_n\|_{\sup} \stackrel{\text{def}}{=} \max_{1\leq i\leq n} |a_i|_p.$$

Si $x = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, on a

$$\begin{aligned} |x|_1 &\leq |a_1|_p\,|v_1|_1 + |a_2|_p\,|v_2|_1 + \cdots + |a_n|_p\,|v_n|_1 \\ &\leq n \cdot \max |v_i|_1 \cdot \|x\|_{\sup}. \end{aligned}$$

Donc

$$|\quad|_1 \leq c\|\quad\|_{\sup}, \quad \text{où } c \text{ est une constante positive.} \tag{4}$$

On montre l'inégalité dans l'autre sens. Considérons $U = \{x \in K \mid \|x\|_{\sup} = 1\}$ muni de la distance associée à la norme $\|\quad\|_{\sup}$. L'ensemble U est compact car $\mathbb{Z}_p$ est compact. L'application ϕ de U dans $\mathbb{R}$ qui à un élément x de U associe $|x|_1$ est continue par l'inégalité (4). Donc il existe $x_0 \in U$ en lequel ϕ atteint son minimum, noté c'. Comme $0 \notin U$, on a $c' > 0$. Ça implique $|\quad|_1 \geq c'\|\quad\|_{\sup}$.

On a le même résultat pour $|\quad|_2$. Donc on conclut qu'il existe c_1 tel que $|\quad|_1 \leq c_1|\quad|_2$. Si $|\quad|_1 \neq |\quad|_2$, il existe $x \in K$ tel que $|x|_1 > |x|_2$. Mais pour tout $n \in \mathbb{Z}_+$, on a $|x^n|_1 \leq c_1|x^n|_2$, d'où une contradiction. On a fini la démonstration pour le cas où l'extension est finie.

Pour le cas général, on peut restreindre les deux valeurs absolues sur toutes les sous-extensions de degré fini et ainsi on obtient le même résultat. □

Il reste à résoudre le problème d'existence.

Définition 3.3 (Norme)**.** Pour simplifier, ici on se restreint au cas où le corps de base F est de caractéristique 0. Soit $K = F(\alpha)$ une extension de degré fini de F. Le polynôme minimal de α sur F est $f = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$. Les trois valeurs suivantes sont égales.

1. On voit K comme un espace vectoriel sur F. La multiplication par α est un endomorphisme A_α de K dans K. On note $\mathbb{N}_1(\alpha) = \det(A_\alpha)$;
2. $\mathbb{N}_2(\alpha) = (-1)^n a_n$;
3. $\mathbb{N}_3(\alpha) = \prod_{i=1}^n \alpha_i$, où les α_i sont tous les conjugués de α dans une clôture normale sur F.

On l'appelle la norme de α dans K sur F et on la note $\mathbb{N}_{K/F}(\alpha)$.

Proposition 3.4 (L'existence)**.** *Soit K une extension de degré fini de $\mathbb{Q}_p$. Il existe une valeur absolue sur K qui étend $|\quad|_p$.*

Démonstration. Soient $n = [K : \mathbb{Q}_p]$ et $\alpha \in K$. On pose

$$|\alpha|_p \stackrel{\text{def}}{=} |\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}.$$

Il est facile de voir que

1. $|\quad|_p$ coïncide avec la valeur absolue p-adique sur $\mathbb{Q}_p$;
2. $|\quad|_p$ est multiplicative ;
3. $|\alpha|_p = 0$ si et seulement si $\alpha = 0$.

Il reste à montrer que $|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p)$. Supposons $|\beta|_p = \max(|\alpha|_p, |\beta|_p)$. Puis, posons $\gamma = \alpha/\beta$. Il est équivalent de montrer

$$|1 + \gamma|_p \leq 1 \quad \text{si } |\gamma|_p \leq 1.$$

Dans un premier temps, on suppose $K = \mathbb{Q}_p(\gamma)$. Prenons $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ comme base de l'espace vectoriel K sur $\mathbb{Q}_p$. Soit A la matrice de multiplication par γ sous cette base, alors A^i est la matrice associée à la multiplication par γ^i. $|\gamma|_p = |\det(A)|_p^{1/n}$ et $|1+\gamma|_p^{1/n} = |\det(I_n + A)|_p^{1/n}$. Posons $\|\quad\|_{\sup}$ la norme supérieure sur le $\mathbb{Q}_p$-espace vectoriel des $n \times n$ matrices à coefficients dans $\mathbb{Q}_p$.

On affirme que $\{\|A^i\|\}$ est bornée. Sinon, soit i_j une suite strictement croissante avec $\|A^{i_j}\|_{\sup} = b_j > j$. Soit β_j le coefficient dans A^{i_j} vérifiant $|\beta_j|_p = \|A^{i_j}\|_{\sup}$. Considérons la suite de matrices

$$B_j \stackrel{\text{def}}{=} A^{i_j}/\beta j. \tag{5}$$

Il est clair que l'on a $\|B_j\|_{\sup} = 1$. Comme la boule unité de la norme supérieure est compacte, on peut trouver une sous-suite (B_{j_k}) qui converge vers un certain B. Puisque $\det B_j = \det A^{i_j}/\beta_j^n$, on a

$$|\det B_j|_p \leq |\det A^{i_j}|_p / j^n = |\gamma|_p^{n i_j}/j^n \leq 1/j^n.$$

Comme $B_{j_k} \to B$ au sens où le maximum des coefficients des $B_{j_k} - B$ tend vers 0, $\det B_{j_k}$ tend vers $\det B$. Donc $\det B = 0$.

Donc il y a un élément $l \in K$ non nul avec $B(l) = 0$. On montre que ça entraîne $B = 0$. Il suffit de voir que $B(\gamma^i l) = 0$ pour tout i car $\{\gamma^i l\}_{i=0}^{n-1}$ est une base de K. Par la définition 5 $\beta_j B_j$ est une multiplication par γ^{i_j} et on a alors

$$\begin{aligned} B(\gamma^i l) &= \lim_{k\to\infty} B_{j_k}(\gamma^i l) = \lim_{k\to\infty} \gamma^i B_{j_k}(l) \\ &= \gamma^i \lim_{k\to\infty} B_{j_k}(l) = \gamma^i B(l) = 0. \end{aligned}$$

On a $B = 0$. Mais en même temps, on a $\|B\|_{\sup} = 1$. C'est une contradiction. Donc $\{\|A^i\|_{\sup}\}$ est majorée par une constante C.

Remarquons que pour une matrice $n \times n : A = (a_{i,j})$, on a toujours

$$|\det A|_p \leq (\max_{i,j} |a_{i,j}|_p)^n = \|A\|_{\sup}^n.$$

Pour $N \in \mathbb{N}$ quelconque, on a

$$\begin{aligned} |1+\gamma|_p^N &= |\det(1+A)^N|_p^{1/n} \leq \|(1+A)^N\|_{\sup} \\ &\leq \max_{0\leq i\leq N} \|\binom{N}{i} A^i\|_{\sup} \leq \max_{0\leq i\leq N} \|A^i\|_{\sup} \\ &\leq C. \end{aligned}$$

Donc $|1+\gamma|_p \leq \sqrt[N]{C}$. Quand $N \to \infty$, on obtient $|1+\gamma|_p \leq 1$.

Si γ n'est pas un élément primitif, on peut obtenir le résultat pour $\mathbb{Q}_p(\gamma)$. Puis, on a

$$1 \geq |\mathbb{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1+\gamma)|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]} = |\mathbb{N}_{K/\mathbb{Q}_p}(1+\gamma)|_p^{1/n} = |1+\gamma|_p.$$

On a achevé la démonstration. □

Remarque 3.5. Par les deux propositions précédentes, on conclut que $|\quad|_p$ a une unique extension sur une extension de degré fini de $\mathbb{Q}_p$. Comme tout élément de $\overline{\mathbb{Q}}_p$ est en fait dans une extension finie de $\mathbb{Q}_p$, il y a une unique extension de $|\quad|_p$ sur la clôture algébrique de $\mathbb{Q}_p$. Parce que la proposition 3.2 a été établie sous hypothèse de finitude, cette extension est en fait unique sur $\overline{\mathbb{Q}}_p$, et on la note encore $|\quad|_p$.

3.2 Un peu de théorie de la ramification

Proposition 3.6. *Soit K une extension de degré fini de $\mathbb{Q}_p$. Posons*

$$\mathfrak{O}_K = \{x \in K \,|\, |x|_p \leq 1\}, \quad \mathfrak{M}_K = \{x \in K \,|\, |x|_p < 1\}.$$

Alors l'anneau $\mathfrak{O}_K$ est la clôture intégrale de $\mathbb{Z}_p$ et il possède un unique idéal maximal, $\mathfrak{M}_K$. De plus, $\mathfrak{O}_K/\mathfrak{M}_K$ est une extension de $\mathbb{F}_p$ de degré au plus $[K : \mathbb{Q}_p]$.

Remarque 3.7. Ceci est en particulier vrai pour $K = \mathbb{Q}_p$. On dit que l'anneau $\mathbb{Z}_p$ (resp. $\mathfrak{O}_K$) est local.

Démonstration. Il est évident que $\mathfrak{O}_K$ est un anneau.

Soit $\alpha \in K$ un entier algébrique sur $\mathbb{Z}_p$, alors il existe des $a_i \in \mathbb{Z}_p$ tels que l'égalité suivante soit satisfaite :

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0.$$

On a

$$\begin{aligned} |\alpha|_p^m = |\alpha^m|_p &= |a_1\alpha^{m-1} + \cdots + a_m|_p \leq \max_{1\leq i\leq m} |a_i\alpha^{m-i}|_p \\ &\leq \max_{1\leq i\leq m} |\alpha^{m-i}|_p = \max(|\alpha|_p^{m-1}, 1). \end{aligned}$$

Il s'ensuit $|\alpha|_p \leq 1$.

Réciproquement, supposons $|\alpha|_p \leq 1$, alors tous les conjugués de α sur $\mathbb{Q}_p$ est aussi de valeur absolue ≤ 1 par définition. Le polynôme minimal unitaire de α a des coefficients

obtenus par l'addition et la multiplication des conjugués de α, donc aussi de valeur absolue ≤ 1. Comme ils sont dans $\mathbb{Q}_p$, ils sont dans $\mathbb{Z}_p$.

Soit $a \in \mathfrak{O}_K \smallsetminus \mathfrak{M}_K$. Comme K est un corps, a admet un inverse dans K, de plus $|a|_p = 1$, on a ainsi $|a^{-1}|_p = 1$, donc $a^{-1} \in \mathfrak{O}_K \smallsetminus \mathfrak{M}_K \subseteq \mathfrak{O}_K$. Donc a est inversible dans $\mathfrak{O}_K$.

D'autre part, si un élément b$\in \mathfrak{O}_K$ est inversible dans $\mathfrak{O}_K$, on a

$$1 \geqslant |b^{-1}|_p = \frac{1}{|b|_p} \geqslant 1.$$

On a nécessairement que $|b|_p$=1, donc $b \in \mathfrak{O}_K - \mathfrak{M}_K$.

Donc le complémentaire de $\mathfrak{M}_K$ dans $\mathfrak{O}_K$ est l'ensemble de toutes les unités de $\mathfrak{O}_K$. Donc $\mathfrak{M}_K$ est l'unique idéal maximal de $\mathfrak{O}_K$.

Remarquons l'égalité $\mathfrak{M}_K \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Considérons le corps $\mathfrak{O}_K/\mathfrak{M}_K$ dont les éléments sont sous la forme $a + \mathfrak{M}_K$. Si $a, b \in \mathbb{Z}_p$, alors $a + \mathfrak{M}_p = b + \mathfrak{M}_p$ si et seulement si $a - b \in \mathfrak{M}_K \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Donc il y a une inclusion naturelle de $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$ dans $\mathfrak{O}_K/\mathfrak{M}_K$. Donc $\mathfrak{O}_K/\mathfrak{M}_K$ est une extension de $\mathbb{F}_p$.

Il reste à voir que $\mathfrak{O}_K/\mathfrak{M}_K$ est de dimension $\leq n \overset{\text{def}}{=} [K : \mathbb{Q}_p]$ sur $\mathbb{F}_p$. Il suffit de voir que tout $(n+1)$-uplet $(\overline{a_1}, \ldots, \overline{a_{n+1}})$ dans $\mathfrak{O}_K/\mathfrak{M}_K$ vérifie une relation de dépendance linéaire sur $\mathbb{F}_p$. Comme $[K : \mathbb{Q}_p] = n$, il existe des $b_i \in \mathbb{Q}_p$ non tous nuls vérifiant

$$a_1 b_1 + a_2 b_2 + \cdots + a_{n+1} b_{n+1} = 0.$$

À une constante multiplicative d'une puissance de p près, on peut supposer que b_i est un élément de $\mathbb{Z}_p$ pour tout i et qu'il existe un i_0 avec $b_{i_0} \notin p\mathbb{Z}_p$. L'image de cette équation dans $\mathfrak{O}_K/\mathfrak{M}_K$ est

$$\overline{a_1}\overline{b_1} + \overline{a_2}\overline{b_2} + \cdots + \overline{a_{n+1}}\overline{b_{n+1}} = 0.$$

où $\overline{b_i}$ est l'image de b_i dans $\mathfrak{O}_K/\mathfrak{M}_K$. Puisque $b_{i_0} \notin p\mathbb{Z}_p$, on a $\overline{b_{i_0}} \neq 0$. Donc $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{n+1}}$ ne sont pas libres. □

Le corps $\mathfrak{O}_K/\mathfrak{M}_K$ s'appelle le corps résiduel de K qui est une extension de degré fini de $\mathbb{F}_p$. En particulier, le corps résiduel de $\mathbb{Q}_p$ est $\mathbb{F}_p$. On note souvent $[\mathfrak{O}_K/\mathfrak{M}_K : \mathbb{F}_p]$ par f.

Soit K une extension de $\mathbb{Q}_p$ de degré n, pour $\alpha \in K$, on définit

$$\operatorname{ord}_p \alpha \overset{\text{def}}{=} -\log_p |\alpha|_p = -\log_p |\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n} = -\frac{1}{n} \log_p |\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p.$$

Cette définition coïncide avec celle qu'on a déjà définie quand $\alpha \in \mathbb{Q}_p$. Évidemment, elle satisfait la propriété : $\operatorname{ord}_p \alpha\beta = \operatorname{ord}_p \alpha + \operatorname{ord}_p \beta$. L'image de K par l'application ord_p est contenue dans $\frac{1}{n}\mathbb{Z}$. Comme l'image est un sous-groupe de $\frac{1}{n}\mathbb{Z}$, elle est nécessairement de la forme $\frac{1}{e}\mathbb{Z}$ pour un nombre entier positif e qui divise n. L'entier e est appelé l'indice de ramification de K sur $\mathbb{Q}_p$. Si $e = 1$, l'extension $\mathbb{Q}_p \hookrightarrow K$ est dite une extension non ramifiée. Si $e = n$, cette extension est dite totalement ramifiée.

Proposition 3.8. *Soit K une extension de degré n de $\mathbb{Q}_p$. Soient e son indice de ramification et f la dimension de son corps résiduel sur $\mathbb{F}_p$. Alors on a l'identité :*

$$n = ef.$$

Démonstration. L'espace $\mathfrak{O}_K/\mathfrak{M}_K$ est de dimension f sur $\mathbb{F}_p$: on peut choisir $\{y_i\}_{i=1}^f \subseteq K$ tel que $\{\overline{y_i}\}_{i=1}^f$ forme une base de $\mathfrak{O}_K/\mathfrak{M}_K$. Puis, comme $\mathrm{ord}_p(K) = \frac{1}{e}\mathbb{Z}$, il existe $\pi \in K$ avec $\mathrm{ord}_p\pi = \frac{1}{e}$. On va montrer que $\{\pi^i y_j\}_{i=0,\ldots,e-1,j=1,\ldots,f}$ forme une base de K sur $\mathbb{Q}_p$.

D'abord, on montre qu'ils sont linéairement indépendants. Sinon, il existe des $\lambda_{i,j} \in \mathbb{Q}_p$ non tous nuls vérifiant $\sum_{i,j} \lambda_{i,j}\pi^i y_j = 0$. Comme $\overline{y_j} \neq 0$, on a $|y_j|_p = 1$. À une constante multiplicative d'une puissance de p près, on suppose $\lambda_{i,j} \in \mathbb{Z}_p$. Puisqu'on a

$$\sum_i \pi^i \sum_j \lambda_{i,j} y_j = 0. \tag{6}$$

Passons au quotient,

$$\sum_j \overline{\lambda_{0,j}}\,\overline{y_j} = 0. \tag{7}$$

Donc $\lambda_{0,j} \in p\mathbb{Z}_p$ et on peut les écrire : $\lambda_{0,j} = \pi^e \lambda_{0,j}^{(1)}$, où $\lambda_{0,j}^{(1)} \in \mathbb{Z}_p$. Si on divise l'équation (6) par π, de la même preuve, on obtient $\lambda_{1,j} \in p\mathbb{Z}_p$. Par récurrence, quelque soit n, on a $\lambda_{i,j} \in p^n\mathbb{Z}_p$. Donc $\lambda_{i,j} = 0$ pour tous i, j. C'est une contradiction. Donc les $\pi^i y_j$ (pour $0 \leq i \leq e-1, 1 \leq j \leq f$) sont linéairement indépendants.

On montre que tous les éléments de K peuvent s'écrire comme une combinaison linéaire des $\pi^i y_j$ à coefficients dans $\mathbb{Q}_p$. Sans perte de généralité, on peut ne considérer que les éléments dans $\mathfrak{O}_K$. Soit $\alpha \in \mathfrak{O}_K$. Alors, il existe $\lambda_{0,j}^{(0)} \in \mathbb{Z}_p$ tel que on ait

$$\overline{\alpha} = \sum_{j=1}^{f} \overline{\lambda_{0,j}^{(0)}}\,\overline{y_j}.$$

Alors, on a $\alpha - \sum_{j=1}^f \lambda_{0,j}^{(0)} y_j \in \pi\mathfrak{O}_K$, donc $\alpha - \sum_{j=1}^f \lambda_{0,j}^{(0)} y_j = \pi\alpha_1$, où $\alpha_1 \in \mathfrak{O}_K$. Par récurrence, il existe $\{\lambda_{i,j}^{(l)}\} \subseteq \mathbb{Z}_p$, tel qu'on ait

$$\alpha - \sum_{i,j} \pi^i y_j \sum_{l=0}^{k-1} \lambda_{i,j}^{(l)} \in p^k \mathfrak{O}_K$$

Posons $\lambda_{i,j} = \sum_{k=0}^{\infty} \lambda_{i,j}^{(k)} p^k$ qui est bien défini. On a $\alpha = \sum_{i,j} \lambda_{i,j}\pi^i y_j$. Donc on a trouvé une base de cardinal ef de K sur $\mathbb{Q}_p$, d'où $n = ef$. □

3.3 Lemme de Hensel

Dans cette section, on va présenter le lemme de Hensel qui nous donne un moyen de trouver des racines parmi les entiers p-adiques d'un polynôme à coefficients entiers p-adiques sous certaine condition. La technique d'approximation pour le lemme de Hesnsel est essentiellement la même que celle de méthode de Newton pour faire un calcul approchée d'une racine réelle d'un polynôme. Dans cette section, on se place dans $\mathbb{Q}_p$.

Lemme 3.9 (Lemme de Hensel)**.** *Soient $F = c_0 + c_1X + \cdots + c_nX^n$ un polynôme à coefficients entiers p-adiques (i.e $ord_p(c_i) \geq 0$) et F' sa dérivé. Soit a_0 un entier p-adique tel que $F(a_0) \equiv 0 \pmod p$ et $F'(a_0) \not\equiv 0 \pmod p$. Alors il existe un unique entier p-adique tel que*

$$a \equiv a_0 \pmod p \quad \text{et} \quad F(a) = 0.$$

Démonstration. On va montrer qu'il existe une unique suite de nombres entiers (a_n) telle que pour tout $n \geq 1$:

1. $F(a_n) \equiv 0 \pmod{p^{n+1}}$;
2. $a_n \equiv a_{n+1} \pmod{p^n}$;
3. $0 \leq a_n < p^{n+1}$.

On montre par récurrence l'existence et l'unicité de a_n.

Pour $n = 1$, soit b_0 l'unique entier dans $\{0, 1, \ldots, p-1\}$ qui à a_0 modulo p. On cherche a_1 sous la forme $b_0 + xp$ avec $0 \leq x \leq p-1$. Pour tout x, ce nombre vérifie les condition 2 et 3. Maintenant on développe $F(b_0 + xp)$:

$$\begin{aligned} F(b_0 + xp) &= \sum_{i=0}^{n} c_i (b_0 + xp)^i \\ &\equiv \sum_{i=0}^{n} c_i b_0^i + (\sum_{i=0}^{n} i c_i b_0^{i-1}) xp \pmod{p^2} \\ &\equiv F(b_0) + F'(b_0) xp \pmod{p^2}. \end{aligned}$$

Comme $F(a_0) \equiv 0 \pmod{p}$ et $b_0 \equiv a_0 \pmod{p}$, on peut écrire $F(a_0) \equiv \alpha p \pmod{p^2}$ avec $\alpha \in \{0, 1, \ldots p-1\}$. Donc pour avoir $F(a_1) \equiv 0 \pmod{p^2}$, il faut $\alpha p + F'(b_0) xp \equiv 0 \pmod{p^2}$, ainsi $\alpha + F'(b_0) x \equiv 0 \pmod{p}$. Puisque par hypothèse $F'(a_0) \not\equiv 0 \pmod{p}$, cette équation a une unique solution dans $\{0, 1, \ldots, p-1\}$ qu'on note b_1. Donc on prend $a_1 = b_0 + b_1 p$ qui vérifie les trois conditions ci-dessus.

Maintenant, supposons les $a_1, a_2, \ldots, a_{n-1}$ sont construits, on cherche a_n sous la forme $a_n = a_{n-1} + xp^n$ avec $x \in \{0, 1, \ldots, p-1\}$. On développe $F(a_{n-1} + xp^n)$ comme dans le cas $n = 1$ et on passe au modulo p^{n+1} :

$$F(a_{n-1} + xp^n) \equiv F(a_{n-1}) + F'(a_{n-1}) xp^n \pmod{p^{n+1}}.$$

Par hypothèse de récurrence, $F(a_{n-1}) \equiv 0 \pmod{p^n}$, on peut ainsi écrire $F(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$. Pour avoir $F(a_{n-1} + xp^n) \equiv 0 \pmod{p^{n+1}}$, il faut que

$$\alpha' p^n + F'(a_{n-1}) xp^n \equiv 0 \pmod{p^{n+1}} \quad \text{ainsi} \quad \alpha' + F'(a_{n-1}) x \equiv 0 \pmod{p}.$$

Comme $a_{n-1} \equiv a_0 \pmod{p}$, on a $F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 \pmod{p}$. Donc on peut trouver un unique $b_n \in \{0, 1, \ldots, p-1\}$ tel que l'équation précédente soit vérifiée. Donc on prend $a_n = a_{n-1} + b_n p^n$ qui vérifie les trois conditions de récurrence.

Donc la suite (a_n) est bien construite, et on pose $a = b_0 + b_1 p + b_2 p^2 + \ldots$. Pour tout n, on a $F(a) \equiv F(a_n) \equiv 0 \pmod{p^{n+1}}$, donc le nombre p-adique $F(a)$ doit être 0. Réciproquement, si on se donne un a$=d_0 + d_1 p + d_2 p^2 + \ldots$ tel que $F(a) = 0$ et $a \equiv a_0 \pmod{p}$, alors on prendre $a'_n = d_0 + d_1 p + \cdots + d_n p^n$, la suite (a'_n) vérifie la condition de la suite (a_n) et par unicité de la suite (a_n), a est ainsi unique. Donc on a montré l'existence et l'unicité de a. □

On compare ici le lemme de Hensel avec la méthode de calcul approchée de Newton. Dans la méthode de Newton pour les polynômes réels, si $f'(a_{n-1}) \neq 0$, on pose

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

Le terme de correction $-f(a_{n-1})/f'(a_{n-1})$ resemble au terme $b_n p^n$ dans le lemme de Hensel qui est :

$$b_n p^n \equiv -\frac{\alpha' p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

C'est comme un point de vue p-adique de la méthode de Newton, mais dans le cas réel la suite (a_n) construite ne sont pas toujours convergente. Or dans le cas p-adique, on a toujours une convergence ce qui est beaucoup meilleur que dans le cas réel. Par exemple si on prend $f(x) = x^3 - x$ et on fait un mauvais choix $a_0 = 1/\sqrt{5}$, on a

$$\begin{aligned} a_1 &= \frac{1}{\sqrt{5}} - \frac{\frac{1}{5\sqrt{5}} - \frac{1}{\sqrt{5}}}{\frac{3}{5} - 1} = \frac{1}{\sqrt{5}}\Big(1 - \frac{\frac{1}{5} - 1}{\frac{3}{5} - 1}\Big) = -\frac{1}{\sqrt{5}} \\ a_2 &= \frac{1}{\sqrt{5}}; \quad a_3 = -\frac{1}{\sqrt{5}} \ldots . \end{aligned}$$

Mais dans les corps p-adiques, ce genre de non convergence ne produit pas, c'est ainsi d'avantage de travailler dans les corps p-adiques.

4 Polygone de Newton

Dans ce chapitre [1], on considère une extension algébrique K de $\mathbb{Q}_p$ munie de la valeur absolue $|\quad|_p$. On établira la théorie du polygone de Newton dans ce corps.

4.1 La définition du polygone de Newton et le théorème principal

Soit $P = a_0 + a_1 X + ... + a_n X^n \in K[X]$. On suppose que n est le degré de P et que P n'est divisible par X, c'est-à-dire que $a_0 \neq 0$ et $a_n \neq 0$. Pour obtenir le polygone de Newton $\Pi(P)$, on regarde l'ensemble des points dans $\mathbb{R}^2$ qui sont définis par

$$A(j) = (j, -\mathrm{ord}_p a_j) \quad (a_j \neq 0).$$

On définit $\Pi(P)$ comme l'enveloppe convexe supérieure de ces points $A(j)$. Il contient l'ensemble des segments σ_s $(1 \leq s \leq r)$, où σ_s joint $A(m_{s-1}), A(m_s)$ où les $A(m_i)$ sont les sommets de $\Pi(P)$ et que

$$0 = m_0 < m_1 < ... < m_r = n.$$

On note γ_s la pente de σ_s, on a ainsi

$$\gamma_s = \frac{-\mathrm{ord}_p a_{m_s} + \mathrm{ord}_p a_{m_{s-1}}}{m_s - m_{s-1}}.$$

Par convexité, on a alors les inégalités $\gamma_1 > \gamma_2 > ... > \gamma_r$ et le fait que tout point $A(j)$ se situe sur ou en dessous de $\Pi(P)$.

Définition 4.1. Avec les notations ci-dessus, on dit qu'un polynôme P est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r)$ avec $l_s = m_s - m_{s-1}$ $(1 \leq s \leq r)$. Si de plus $r = 1$, on dit que P est pur.

On se propose de montrer le théorème principal.

1. La théorie des polygones de Newton est identique pour un corps complet muni d'une valeur absolue ultramétrique.

Théorème 4.2. *Soit $P \in K[X]$ de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r)$. Alors*

$$P = g_1 \cdots g_r$$

avec g_s pur et de type (l_s, γ_s) $(1 \leq s \leq r)$.

Remarque 4.3. Il n'est pas nécessaire que les g_s soient irréductibles.

4.2 La démonstration du théorème principal

Pour montrer le théorème principal, on a besion d'une famille des valeurs absolues sur le corps des fractions rationnelles $K(X)$.

Définition 4.4. Soit $c > 0$. Pour $P = a_0 + a_1X + ... + a_nX^n \in K[X]$, on définit

$$\|P\|_c = \max_{j \in [0,n]} c^j |a_j|_p.$$

Pour $H \in K(X)$, on définit

$$\|H\|_c = \frac{\|P\|_c}{\|Q\|_c} \quad \text{si } H = \frac{P}{Q}.$$

Proposition 4.5. *L'application $\| \quad \|_c$ est une valeur absolue non archimédienne sur $K(X)$ qui coïncide avec $| \quad |_p$ sur K.*

Démonstration. Soient $P, Q \in K[X]$, $P = a_0 + a_1X + ... + a_nX^n \in K[X]$ et $Q = b_0 + b_1X + ... + b_mX^m$. D'après la propriété de la valeur absolue ultramétrique, on a clairement que

$$\|P + Q\|_c \leq \max(\|P\|_c, \|Q\|_c)$$

et

$$\|PQ\|_c \leq \|P\|_c \|Q\|_c. \tag{8}$$

On montre maintenant qu'il y a en fait l'égalité pour (8). Supposons $P, Q \neq 0$. Soit I l'unique entier vérifiant

$$\|P\|_c = \|a_I X^I\|_c \quad \text{et } \|a_i X^i\|_c < \|P\|_c \quad \text{pour } i < I.$$

On définit de la même manière J vérifiant

$$\|Q\|_c = \|b_J X^J\|_c \quad \text{et } \|a_j X^j\|_c < \|Q\|_c \quad \text{pour } j < J.$$

Alors le coefficient de X^{I+J} de PQ est

$$\sum_{i+j=I+J} a_i b_j.$$

On distingue trois cas différents :

1. Dans le cas $i < I$, on a $\|a_i X^i\|_c < \|P\|_c$, c'est-à-dire que $|a_i|_p < c^{-i}\|P\|_c$. De plus $|b_j|_p \leq c^{-j}\|Q\|_c$; on a ainsi

$$|a_i b_j|_p < c^{-i-j}\|P\|_c\|Q\|_c = c^{-I-J}\|P\|_c\|Q\|_c. \tag{9}$$

2. Dans le cas $j < J$, on a la même inégalité (9).
3. Enfin, $i = I, j = J$, on a $|a_I b_J| = c^{-I-J}\|P\|_c\|Q\|_c$. Alors

$$|\sum_{i+j=I+J} a_i b_j|_p = c^{-I-J}\|P\|_c\|Q\|_c.$$

On a donc par définition de $\| \ \|_c$ que $\|PQ\|_c \geqslant \|P\|_c\|Q\|_c$. Avec (8) on a l'égalité $\|PQ\|_c = \|P\|_c\|Q\|_c$.

Maintenant, soit $H \in K(X)$. On suppose

$$H = \frac{P}{Q} = \frac{p}{q} \quad \text{avec } p, q, P, Q \in K[X].$$

Alors on a $pQ = qP$, d'où $\|p\|_c\|Q\|_c = \|q\|_c\|P\|_c$.
Donc la définition de $\|H\|_c$ est bien indépendante du choix de P, Q.

On a ainsi que $\| \ \|_c$ est une valeur absolue non archimédienne sur $K(X)$. □

Le lemme suivant donne les liens entre les valeurs absolues définies ci-dessus et le polygone de Newton.

Lemme 4.6. *Soient $P = a_0 + a_1X + ... + a_nX^n \in K[X]$, $\gamma \in \mathbb{R}$ et c avec $\log_p c = -\gamma$. Soient $i \in [1, n]$ et $A(i) = (i, -\mathrm{ord}_p a_i)$. Considérons la droite D_i passant par $A(i)$ et de pente γ.*

1. *Un point $A(j)$ se situe sur la droite D_i si et seulement si $\|a_jX^j\|_c = \|a_iX^i\|_c$;*
2. *Un point $A(j)$ se situe en dessous de la droite D_i si et seulement si $\|a_jX^j\|_c < \|a_iX^i\|_c$;*
3. *Un point $A(j)$ se situe en dessus de la droite D_i si et seulement si $\|a_jX^j\|_c > \|a_iX^i\|_c$.*

Démonstration. La droite D_i a comme l'équation $y = \gamma(x - i) - \mathrm{ord}_p a_i$, un point $A(j)$ est sur la droite si et seulement si

$$-\mathrm{ord}_p a_j = -(j - i)\log_p c - \mathrm{ord}_p a_i.$$

L'égalité ci-dessus est équivalente à $\|a_jX^j\|_c = \|a_iX^i\|_c$. Les deux autres inégalités s'obtiennent de la même façon. □

Lemme 4.7. *Soient $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r)$, $s \in [1, r]$ et $c \in \mathbb{R}$ avec $\log_p c = -\gamma_s$. Alors on a*

$$\|a_jX^j\|_c = \|P\|_c \quad \textit{si } j = m_{s-1}, m_s$$

et

$$\|P - \sum_{m_{s-1} \leq j \leq m_s} a_jX^j\|_c < \|P\|_c.$$

Démonstration. On a déjà

$$\log_p c = -\gamma_s = \frac{-\mathrm{ord}_p a_{m_s} + \mathrm{ord}_p a_{m_{s-1}}}{m_s - m_{s-1}}.$$

Par définition du polygone de Newton, on a que la droite passant par $A(m_{s-1})$ et $A(m_s)$ est de pente γ_s et que tous les autres points se situent en dessous de cette droite. Donc par lemme 4.6, on a pour tout $j \in [0, n]$,

$$\|a_j X^j\|_c \leq \|a_{m_s} X^{m_s}\|_c = \|a_{m_{s-1}} X^{m_{s-1}}\|_c.$$

On a donc

$$\|P\|_c = \max_{0 \leq i \geq n} \|a_i X^i\|_c = \|a_{m_{s-1}} X^{m_{s-1}}\|_c = \|a_{m_s} X^{m_s}\|_c.$$

De plus, les points en dehors de $[m_{s-1}, m_s]$ sont strictement en dessous de cette droite. Une autre application du lemme 4.6 donne la deuxième inégalité. □

Les deux lemmes suivants disent que la multiplication des polynômes correspond à la composition des polygones de Newton.

Lemme 4.8. *Supposons que $P, Q \in K[X]$ sont purs avec la même pente γ. Alors PQ est aussi pur et de pente γ.*

Démonstration. Soit c vérifiant $\log_p c = -\gamma$, on écrit $P = a_0 + a_1 X + ... + a_n X^n$ et $Q = b_0 + b_1 X + ... + b_m X^m$, d'après le lemme 4.6, on a

$$\|P\|_c = \|a_0\|_c = \|a_n X^n\|_c \quad \text{et } \|Q\|_c = \|b_0\|_c = \|b_m X^m\|_c.$$

On note $PQ = d_0 + d_1 X + ... + d_{n+m} X^{n+m}$; on a alors

$$\|PQ\|_c = \|a_0 b_0\|_c = \|d_0\|_c = \|a_n b_m X^{n+m}\|_c = \|d_{n+m} X^{n+m}\|_c.$$

Donc par lemme 4.6, les points se situent tous en dessous ou sur la droite passant par $A(0) = (0, -\mathrm{ord}_p(a_0 b_0))$ et $A(n+m) = (n+m, -\mathrm{ord}_p(a_n b_m))$. Comme la pente de ce segment est exactement γ, on a que PQ est pur et de type γ. □

Lemme 4.9. *Supposons $P \in K[X]$ est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots; l_r, \gamma_r)$ et que Q est pur de type (N, γ) avec $\gamma < \gamma_r$. Alors PQ est de type $(l_1, \gamma_1; l_2, \gamma_2; \ldots l_r, \gamma_r; N, \gamma)$.*

Démonstration. On écrit $P = a_0 + a_1 X + \cdots + a_n X^n$ et $Q = b_0 + b_1 X + \cdots + b_m X^m$. Soit $s \in [1, r]$, soit c tel que $\log_p c = -\gamma_s$. Comme on a $\gamma_s \geqslant \gamma_r > \gamma$, on a par convexité que tous les points associés à Q sauf $A(0)$ se situent strictement en dessous de la droite passant par $A(0)$ de pente γ_s, alors d'après lemme 4.6,

$$\|Q - b_0\|_c < \|Q\|_c.$$

Et donc on a

$$\|PQ - b_0 \sum_{m_{s-1} \leq j \leq m_s} a_j X^j\|_c < \|PQ\|_c.$$

De la même manière, si on pose $\log_p c = -\gamma$, on a

$$\|PQ - a_n X^n Q\|_c < \|PQ\|_c.$$

Donc avec toutes ces inégalités et le fait que Q est pur, on obtient que le polygone de Newton de PQ est bien sous la forme demandée. □

Lemme 4.10. *Soient $c > 0$ et $P = a_0 + a_1X + \cdots a_nX^n \in K[X]$. Supposons*

$$Q = b_0 + b_1X + ... + b_NX^N \in K[X] \quad \textit{avec } \|Q\|_c = \|b_nX^n\|_c.$$

On fait la division euclidienne de P par Q

$$P = LQ + R; \quad \deg R < N.$$

Alors on a

$$\|L\|_c \, \|Q\|_c \leq \|P\|_c \quad \textit{et } \|R\|_c \leq \|P\|_c.$$

Démonstration. Soient $P \neq 0$ et n le degré de P. Si $n > N$, on a gagné. Donc on suppose que $n \leq N$. Alors L est de degré $n - N$. Les coefficients L_{n-N}, $L_{n-N-1}, \ldots,$ L_0 de L sont déterminés par les équations

$$b_NL_{n-N-j} + b_{N-1}L_{n-N-j+1} + .. + b_{N-j}L_{n-N} = a_{n-j}.$$

Donc par la propriété ultra-métrqiue, on a $|b_NL_{n-N-j}|_p \leq |a_{n-j}|_p$, on a ainsi

$$\|P\|_c \geqslant |a_{n-j}c^{n-j}|_p \geqslant |b_Nc^NL_{n-N-j}c^{n-N-j}|_p = \|Q\|_c \, |L_{n-N-j}c^{n-N-j}|_p.$$

Ceci est vrai pour tout $j \in \{0, 1, \ldots, n - N\}$, donc on a $\|L\|_c \, \|Q\|_c \leq \|P\|_c$. De plus $R = P - LQ$, donc par l'inégalité ultramétrique on a $\|R\|_c \leq \|P\|_c$. □

Enfin, la décomposition du polygone de Newton correspond à la décomposition du polynôme.

Lemme 4.11. *Soient $c > 0$, $P = a_0 + a_1X + ... + a_nX^n \in K[X]$. Soit N vérifiant*

$$\|a_NX^N\|_c = \|P\|_c \quad \textit{et } \|a_jX^j\|_c < \|P\|_c \quad \textit{pour } j > N.$$

Alors $P = QR$ avec $Q, R \in K[X]$ de degré N, $n - N$ respectivement.

Démonstration. Soit Δ vérifiant

$$\|P - \sum_{i=0}^{N} a_iX^i\|_c = \Delta\|P\|_c.$$

On a par hypothèse $\Delta < 1$. On construit maintenant par récurrence deux suites de polynômes (Q_m),(R_m) avec $\deg Q_m = N$ et $\deg R_m \leq n - N$. Pour tout m, ils vérifient les propriétés suivantes :

1. $\|P - Q_m\|_c \leq \Delta\|P\|_c$ et $\|R_m - 1\|_c \leq \Delta$;
2. $\|Q_m\|_c = \|P\|_c$ est atteint par le monôme de degré N de Q_m ;
3. $\|P - Q_mR_m\|_c \leq \Delta^m\|P\|_c$.

On pose

$$Q_0 = \sum_{i=0}^{N} a_iX^i \quad \text{et } R_0 = 1.$$

On vérifie aisément que les propriétés sont satisfaites par Q_0 et R_0. Supposons que Q_m et R_m sont construits. Pour $m + 1$, on pose δ tel que $\|P - Q_mR_m\|_c = \delta\|P\|_c$. Alors, $\delta \leq \Delta^m$. On fait la division euclidienne de $P - Q_mR_m$ par Q_m :

$$P - Q_mR_m = L_mQ_m + S_m \quad \text{avec } \deg L_m \leq n - N, \deg S_m < N.$$

Par le lemme 4.10, on a $\|L_m\|_c \leq \delta$, $\|S_m\|_c \leq \delta\|P\|_c$. On pose $Q_{m+1} = Q_m + S_m$, $R_{m+1} = R_m + L_m$. Alors

$$\|P - Q_{m+1}\|_c \leq \max(\|P - Q_m\|_c, \|S_m\|_c) \leq \max(\Delta\|P\|_c, \delta\|P\|_c) = \Delta\|P\|_c,$$

$$\|R_{m+1} - 1\|_c \leq \max(\|R_m - 1\|_c, \|L_m\|_c) \leq \max(\Delta, \delta) \leq \Delta.$$

On a $\|Q_{m+1}\|_c = \|Q_m + S_m\|_c$. Comme $\|Q_m\|_c = \|P\|_c > \delta\|P\|_c = \|S_m\|_c$, on a $\|Q_{m+1}\|_c = \|Q_m\|_c = \|P\|_c$. Puisque $\deg(S_m) < N$, le coefficient de X^N ne change pas. On a par l'hypothèse de récurrence que $\|Q_{m+1}\|_c$ est aussi atteint par le monôme de degré N.

$$\begin{aligned}
\|P - Q_{m+1}R_{m+1}\|_c &= \|P - Q_mR_m - Q_mL_m - R_mS_m - L_mS_m\|_c \\
&= \|(R_m - 1)S_m + S_mL_m\|_c \\
&\leq \max(\|R_m - 1\|_c \, \|S_m\|_c, \|S_m\|_c \, \|L_m\|_c) \\
&\leq \Delta\delta\|P\|_c \leq \Delta^{m+1}\|P\|_c.
\end{aligned}$$

Donc les suites (Q_m) et (R_m) sont bien définies.

De plus, par la construction, on voit que $\|Q_{m+1} - Q_m\|_c = \|S_m\|_c \leq \Delta^m\|P\|_c$, donc la suite de $k^{\text{ième}}$ coefficients de (Q_m) $(0 \leq k \leq N)$ est de Cauchy. Donc (Q_m) converge vers un certain Q qui est aussi de degré N. De la même manière, la suite (R_m) admet une limite R qui est de degré $\leq n - N$. On a ainsi $\|P - QR\|_c$=0, d'où $P = QR$. □

Corollaire 4.12. *Supposons que $P \in K[X]$ est irréductible. Alors P est pur.*

Démonstration. Si P n'est pas pur, alors on peut trouver un c et un N tel que $0 < N < \deg P$ qui vérifient la condition du lemme 4.11, ce qui est contradictoire avec P soit irréductible. □

On montre maintenant le théorème principal.

Démonstration. On décompose P en produit de polynômes irréductibles. D'après le corollaire 4.12, ces facteurs irréductibles sont purs. En utilisant le lemme 4.8, on regroupe ceux qui ont la même pente, donc on écrit alors P comme produit de polynômes purs P_i $(1 \leq i \leq N)$ avec P_i de type (n_i, δ_i) et que $\delta_1 > \delta_2 > \cdots > \delta_N$. Donc d'après le lemme 4.9, on a que le type de $\prod P_i$ est $(n_1, \delta_1; n_2, \delta_2; \ldots; n_N, \delta_N)$ qui est aussi le type de P, on a ainsi que $n_s = l_s, \delta_s = \gamma_s$ $(1 \leq s \leq r)$, d'où le résultat. □

5 Application à la détermination de groupes de Galois

Dans cette partie, on utilise l'outil qu'on a établi pour étudier les groupes de Galois des polynômes de Taylor de l'exponnetielle et les polynômes de Laguerre généralisés. Avant de le faire, on donne quelques prélimilaires.

5.1 Préliminaires

Lemme 5.1. *Soient $f \in \mathbb{Q}[X]$ unitaire irréductible de degré n et Δ le discriminant de f. Soit G le groupe de Galois de f sur $\mathbb{Q}$. Alors $G \subseteq A_n$ si et seulement si Δ est un carré dans $\mathbb{Q}$.*

Démonstration. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ les racines de f dans $\overline{\mathbb{Q}}$. Par définition,

$$\sqrt{\Delta} = \pm \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Soit $\sigma \in S_n$, on a

$$\sigma \cdot \sqrt{\Delta} = (-1)^{\mathrm{sign}(\sigma)} \sqrt{\Delta}.$$

Comme tout élément dans G fixe $\mathbb{Q}$, par la théorie de Galois, on a que $G \subseteq A_n$ si et seulement si Δ est un carré dans $\mathbb{Q}$. □

Lemme 5.2. *Soient p un nombre premier, $R \in \mathbb{Q}_p[X]$ un polynôme pur de type (n, γ) pour $|\quad|_p$. Soit α une racine de R dans $\overline{\mathbb{Q}}_p$, alors* $\mathrm{ord}_p(\alpha) = \gamma$.

Démonstration. On peut supposer R unitaire : en effet, la renormalisation revient juste à faire une translation verticale du polygone de Newton. Dans $\overline{\mathbb{Q}}_p$, R est scindé. On écrit $R = X^n + b_{n-1}X^{n-1} + ... + b_0 = (X - x_1)(X - x_2)\ldots(X - x_n)$. Les $X - x_i$ sont de type $(1, \mathrm{ord}_p(x_i))$. Par le lemme 4.8 et le lemme 4.9, on a $\mathrm{ord}_p(x_i) = \gamma$ pour tout i. □

On fixe un nombre premier p.

Lemme 5.3. *On se place dans $(\mathbb{Q}_p, |\quad|_p)$. Soient $d \in \mathbb{N}$, $R \in \mathbb{Q}_p[X]$. On suppose d divise tous les dénominateurs des pentes du polygone de Newton de R. Alors d divise le degré de tous les facteurs de R dans $\mathbb{Q}_p[X]$.*

Démonstration. Il suffit de le faire pour les facteurs irréductibles de R dans $\mathbb{Q}_p[X]$, car tous les facteurs de R dans $\mathbb{Q}_p[X]$ s'écrivent comme produit de facteurs irréductibles. Soient f un facteur irréductible de R dans $\mathbb{Q}_p[X]$ et α une racine de f dans la clôture de $\mathbb{Q}_p$. Par le corollaire 4.12, f est pur. Comme $R = fg$ où $g = R/f \in \mathbb{Q}_p[X]$, d divise le dénominateur de la pente du polygone de Newton de f. Par lemme 5.2, d divise l'indice de ramification de $\mathbb{Q}_p(\alpha)$. Par la proposition 3.8, d divise $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = \deg f$. □

Remarque 5.4. Soient $R \in \mathbb{Q}[X]$ et d un nombre entier. S'il existe un nombre premier p tel que d divise tous les dénominateurs des pentes du polygone de Newton de R dans $\mathbb{Q}_p$, alors d divise le degré de tous les facteurs de R dans $\mathbb{Q}[X]$.

Lemme 5.5. *Soit $k \in \mathbb{N}$ et*

$$k = a_0 + a_1 p + ... + a_s p^s$$

avec $0 \leq a_i < p$. Alors

$$\mathrm{ord}_p(k!) = \frac{k - (a_0 + a_1 + ... + a_s)}{p - 1}.$$

C'est un résultat facile à obtenir.

5.2 Le groupe de Galois sur $\mathbb{Q}$ des polynômes de Taylor de l'exponentielle

Définition 5.6. Pour $n \in \mathbb{N}$, on définit le $n^{\text{ième}}$ polynôme de Taylor de la fonction exponentielle :

$$f_n = 1 + X + \frac{X^2}{2!} + ... + \frac{X^n}{n!}.$$

Dans cette partie, on se propose de montrer le théorème suivant.

Théorème 5.7 (Schur)**.** *Soit $n \geq 8$ un entier. Le groupe de Galois G_n du polynôme f_n sur $\mathbb{Q}$ est le groupe alterné A_n si n est divisible par 4, et le groupe symétrique S_n sinon.*

Remarque 5.8. C'est encore vrai pour $n \leq 7$, mais il s'agit alors de vérifier à la main que G_n contient A_n.

On va le faire en trois étapes :

1. On montre que f_n est irréductible.
2. On montre que G_n contient un p-cycle où p est un nombre premier dans $]\frac{n}{2}, n[$ pour $n \geq 8$.
3. On calcule le discriminant D_n de f_n et détermine quand il est un carré.

Soit $n \in \mathbb{N}$. On écrit

$$n = b_1 p^{n_1} + b_2 p^{n_2} + ... + b_s p^{n_s}$$

avec $n_1 > n_2 > ...n_s \geq 0$ et $0 < b_i < p$; puis on pose

$$x_i = b_1 p^{n_1} + ... + b_i p^{n_i}.$$

On commence par expliciter le polygone de Newton de f_n.

Lemme 5.9. *Les sommets de polygone du Newton de f_n sont exactement $(0,0)$ et les*

$$(x_i, -\mathrm{ord}_p(\frac{1}{x_i!})) = (x_i, \mathrm{ord}_p(x_i!)), \quad 1 \leq i \leq s.$$

Démonstration. On montre par récurrence que les x_i sont les sommets du polygone de Newton de f_n. Pour $i = 1$, comme le premier sommet est $(0,0)$, le deuxième est le point qui a la pente maximale. Cela correspond à l'entier k tel que $\frac{\mathrm{ord}_p(k!)}{k}$ est maximal. Soit $k = a_0 + a_1 p + ... + a_t p^t$ avec $0 \leq a_i < p$, on a que

$$\frac{\mathrm{ord}_p(k!)}{k} = \frac{1}{p-1} - \frac{a_0 + a_1 + ... + a_t}{k(p-1)}.$$

De plus, on a

$$\frac{a_0 + a_1 + ... + a_t}{k} = \frac{a_0 + a_1 + ... + a_t}{a_0 + a_1 p + ... + a_t p^t} \geqslant \frac{1}{p^t} \geqslant \frac{1}{p^{n_1}}.$$

On a l'égalité si et seulement si $a_0 = a_1 = ... = a_{t-1} = 0$ et $t = n_1$, donc la pente maximale est atteinte pour tout $l p^{n_1}$ avec $l \leq b_1$. Donc le deuxième sommet est $x_1 = b_1 p^{n_1}$ qui est le plus grand nombre de pente maximale.

On suppose le résultat vrai pour i. Pour $i+1$, on cherche les $y > x_i$ qui a pour pente maximale

$$\frac{\mathrm{ord}_p(y!) - \mathrm{ord}_p(x_i!)}{y - x_i}.$$

Comme $x_i < y \leq n$, on a nécessairement que $y - x_i \leq b_{i+1} p^{n_{i+1}}$ et que le développement de y coïncide avec x pour le degré plus grand que n_{i+1}. Par un calcul direct et le lemme 5.5, on voit que

$$\frac{\mathrm{ord}_p(y!) - \mathrm{ord}_p(x_i!)}{y - x} = \frac{\mathrm{ord}_p((y - x_i)!)}{y - x_i} \quad \text{avec } y - x_i \leq b_{i+1} p^{n_{i+1}}.$$

Donc par le résultat pour $i = 1$, on a que le maximum est atteint pour $l p^{n_{i+1}}$. Ainsi le sommet suivant vérifie $y - x_i = b_{i+1} p^{n_{i+1}}$, donc c'est le x_{i+1}. Donc on a le résultat par récurrence. □

On a donc que les sommets de f_n sont les x_i et les pentes associées sont

$$\gamma_i = \frac{\mathrm{ord}_p(x_i!) - \mathrm{ord}_p(x_{i-1}!)}{x_i - x_{i-1}} = \frac{p^{n_i} - 1}{p^{n_i}(p-1)}.$$

On en déduit quelques résultats utiles pour étudier l'irréductibilité de f_n.

Lemme 5.10. *On suppose que p^m divise n. Alors p^m divise le degré de chaque facteur irréductible de f_n dans $\mathbb{Q}$.*

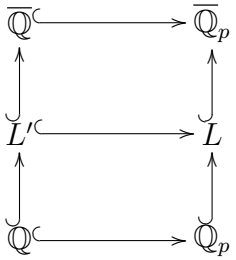
Démonstration. Comme p^m divise n, on a $m \leq n_s < n_{s-1} < \cdots < n_1$. Donc p^m divise les dénominateurs de toutes les pentes d'après le calcul précédent. Donc par le lemme 5.3, on a que p^m divise le degré de chaque facteur irréductible de f_n dans $\mathbb{Q}$. □

Lemme 5.11. *On suppose que $p^k \leq n$. Alors p^k divise le degré du corps de décomposition de f_n sur $\mathbb{Q}$.*

Démonstration. Comme $p^k \leq n$, on a que $k \leq n_1$. Alors p^k divise le dénominateur de γ_1. Si on note g le polynôme correspondant à ce segment et α une racine de g, par le lemme 5.2, p^k divise le dénominateur de $\mathrm{ord}_p\alpha$, donc p^k divise l'indice de ramification de $\mathbb{Q}_p(\alpha)$. Par la proposition 3.8, p^k divise $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$. Si on note L le corps de décomposition de f_n sur $\mathbb{Q}_p$, et L' le corps de décompostion de f_n sur $\mathbb{Q}$, on a

$$L \cap \overline{\mathbb{Q}} = L'.$$

Et on a le graphe suivant :



On considère l'application ϕ de $\mathrm{Gal}(L|\mathbb{Q}_p)$ dans $\mathrm{Gal}(L'|\mathbb{Q})$ par restriction. On montre qu'elle est injective. Soient $\sigma_1, \sigma_2 \in \mathrm{Gal}(L|\mathbb{Q}_p)$ vérifiant $\sigma_1 \circ \sigma_2^{-1}|L' = \mathrm{id}$. Alors $\sigma_1 \circ \sigma_2^{-1}$ fixe toutes les racines de f_n. Comme L est le corps de décomposition de f_n sur $\mathbb{Q}_p$, on a $\sigma_1 \circ \sigma_2^{-1} = \mathrm{id}$. Donc $\sigma_1 = \sigma_2$. Donc on a $|\mathrm{Gal}(L|\mathbb{Q}_p)| \mid |\mathrm{Gal}(L'|\mathbb{Q})|$. Comme $\mathbb{Q}_p(\alpha)$ est un sous-corps de L, on a $p^k \mid [L' : \mathbb{Q}]$. □

Proposition 5.12. *Soit $n \in \mathbb{N}^*$. Le polynôme f_n est irréductible.*

Démonstration. On fait la décomposition en facteurs premiers de n

$$n = \prod_p p^{\alpha_p}.$$

Le lemme 5.10 implique que pour tout p, p^{α_p} divise le degré de chaque facteur irréductible dans $\mathbb{Q}[X]$ de f_n. Donc le degré d'un facteur irréductible est supérieur à n, ainsi f_n est irréductible. □

Lemme 5.13. *Le groupe de Galois G_n de $f_n (n \geqslant 8)$ contient un p-cycle, où p est un nombre premier dans $]n/2, n-2[$.*

Démonstration. Pour $n \geq 8$, par théorème B.1, il existe un nombre premier p entre $n/2$ et $n-2$. Par le lemme 5.11, p divise le degré du corps de décomposition de f_n. Donc p divise l'ordre de G_n. Par le théorème de Cauchy, G_n contient un élément d'ordre p et que les seuls éléments d'ordre p dans S_n sont des p-cycles, donc on a le résultat. □

La démonstration du théorème 5.7. Comme f_n est irréductible sur $\mathbb{Q}$ de caractéristique nulle, il est scindé à racines simples dans son corps de décomposition. On écrit ainsi

$$f_n = \frac{1}{n!}(X-\alpha_1)\cdots(X-\alpha_n).$$

Alors,

$$\begin{aligned}
\Delta_n &= (\frac{1}{n!})^{2n-2}\prod_{i<j}(\alpha_i-\alpha_j)^2 \\
&= (-1)^{\binom{n}{2}}(\frac{1}{n!})^{2n-2}\prod_{i=1}^{n}(n!f_n'(\alpha_i)) \\
&= (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2}\prod_{i=1}^{n}f_n'(\alpha_i) \\
&= (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2}\prod_{i=1}^{n}f_{n-1}(\alpha_i) \\
&= (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2}\prod_{i=1}^{n}\frac{(-\alpha_i^n)}{n!} \quad (\text{car } f_{n-1} = f_n - \frac{X^n}{n!}) \\
&= (-1)^{\binom{n}{2}+n}(\frac{1}{n!})^{n-2}(-1)^n(\frac{\prod_{i=1}^{n}\alpha_i}{n!})^n \\
&= (-1)^{\binom{n}{2}}(\frac{1}{n!})^{n-2}.
\end{aligned}$$

Si $n>1$ est impair, il existe p un nombre premier tel que

$$\mathrm{ord}_p(n!) = 1.$$

En effet, ceci est vrai pour $n = 3, 5, 7$, et pour $n \geq 8$, il existe un premier dans $]n/2, n-2[$. Donc dans ce cas Δ_n ne peut pas être un carré car $\mathrm{ord}_p(\Delta_n) = n$ est impair. Si $n \equiv 2 \pmod 4$, $\Delta_n < 0$ n'est pas un carré et si 4 divise n, on a clairement que Δ_n est un carré. Pour le cas $n \geq 8$, par le théorème A.3, on a $A_n \subseteq G_n$. Cela complète la preuve du théorème en utilisant le lemme 5.1. □

5.3 Le groupe de Galois sur $\mathbb{Q}$ des polynômes de Laguerre généralisés

Dans cette section, on s'intéresse aux groupes de Galois des polynômes de Laguerre généralisés en utilisant les résultats sur le polygone de Newton.

Définition 5.14. Soit $\alpha \in \mathbb{Q} \setminus \mathbb{Z}^-$, on définit les polynômes de Laguerre généralisés par

$$L_n^{(\alpha)} = \sum_{j=0}^{n}\binom{n+\alpha}{n-j}\frac{(-X)^j}{j!}.$$

Ici, on a posé

$$\binom{n+\alpha}{n-j} = \frac{(n+\alpha)(n+\alpha-1)\dots(\alpha+1+j)}{(n-j)!} \quad \text{pour } \alpha \in \mathbb{Q} \quad \text{et } n, j \in \mathbb{N}, n-j \geq 0.$$

5.3.1 L'irréductibilité des polynômes de Laguerre généralisés pour n assez grand

Pour étudier le groupe de Galois de ces polynômes, on va encore utiliser les mêmes méthodes que pour les polynômes de Taylor de l'exponentielle. Mais on remarque que les $L_n^{(\alpha)}$ ne sont pas toujours irréductibles, par exemple $L_2^{(2)} = \frac{1}{2}(X-2)(X-6)$. On commence par montrer le théorème suivant.

Théorème 5.15 (Filaseta et Lam)**.** *On suppose α est un nombre rationnel qui n'est pas un entier négatif. Alors pour tout sauf un nombre fini d'entiers n, $L_n^{(\alpha)}$ est irréductible sur $\mathbb{Q}$.*

D'après ce théorème, on voit que pour α fixé, pour n assez grand, les $L_n^{(\alpha)}$ sont irréductibles. L'étape d'après est de montrer que pour n assez grand, le groupe de Galois de $L_n^{(\alpha)}$ contient un p-cycle comme pour les polynômes de Taylor de l'exponentielle, où $p \in]\frac{n}{2}, n[$. On conclura à l'aide du théorème de Jordan.

On commence par étudier l'irréductibilité des polynômes de Laguerre généralisés. On a besoin du lemme suivant :

Lemme 5.16. *Soient un entier $1 \leq k \leq n$ et p un nombre premier. On suppose $g = b_0 + b_1 X + ... + b_n X^n \in \mathbb{Z}[X]$ et $p \nmid b_n$, $p | b_j$ pour tout $j \in \{0, 1..., n-k\}$ et $\mathrm{ord}_p(b_j) > \mathrm{ord}_p(b_0) - j/k$ pour tout $1 \leq j \leq n$. Alors pour tous entiers $a_0, a_1, ..., a_n$ avec $|a_0|_p = |a_n|_p = 1$, le polynôme $f = \sum_{j=0}^n a_j b_j X^j$ n'a pas de facteur de degré k dans $\mathbb{Z}[X]$.*

Remarque 5.17. On peut appliquer ce lemme à $n! f_n$ à la place de 5.10 pour obtenir l'irréductibilité de f_n.

Démonstration. Soient $a_0, a_1, ..., a_n$ des entiers avec $|a_0|_p = |a_n|_p = 1$. On se place dans $\mathbb{Q}_p$. On suppose par l'absurde que (H) : il existe u et v dans $\mathbb{Z}[X]$ tel que $f = uv$ et deg $u = k$. Mais alors la même décomposition subsiste dans $\mathbb{Q}_p$, et c'est donc dans $\mathbb{Q}_p$ que l'on travaille à l'aide de la théorie des polygones de Newton. On considère le polygone de Newton de f associé à $|\quad|_p$; on suppose qu'il est de type $(l_1, \gamma_1, ; l_2, \gamma_2; \dots ; l_r, \gamma_r)$. Par hypothèse, on a

$$\begin{aligned} \mathrm{ord}_p(a_j b_j) &= \mathrm{ord}_p(a_j) + \mathrm{ord}_p(b_j) \geq \mathrm{ord}_p(b_j) \quad \text{(car les } a_j \text{ sont entiers)} \\ &> \mathrm{ord}_p(b_0) - \frac{j}{k} = \mathrm{ord}_p(a_0 b_0) - \frac{j}{k}. \end{aligned}$$

Ça implique

$$-\mathrm{ord}_p(a_j b_j) < -\mathrm{ord}_p(a_0 b_0) + \frac{j}{k}.$$

Donc on a $\gamma_1 < \frac{1}{k}$. De plus, les $a_j b_j$ sont des nombres entiers, donc $-\mathrm{ord}_p(a_j b_j) \leq 0$. Donc $\gamma_r \geq 0$ car le dernier point est $(n, 0)$. Le dernier côté du polygone de Newton peut éventuellement avoir la pente 0. Considérons un côté qui n'a pas pour pente 0 : on note (a, b) et (c, d) les deux sommets de ce côté. On a donc

$$\frac{1}{k} > \frac{|d-b|}{|c-a|} \geq \frac{1}{|c-a|}.$$

Donc $|c-a| > k$, c'est-à-dire que la différence en abscisses des deux extrémités de ce côté strictement supérieur à k. Comme $\deg u = k$, on prend un facteur pur w de u, $\deg w \leq k$. Soit γ la pente de w. Et par le théorème principal sur le polygone de Newton, cette pente est l'une des γ_i, qui sont tous $\in [0, \frac{1}{k}[$. Comme w est à coefficients entiers, γ soit est 0, soit vérifie $\gamma \geq \frac{1}{\deg w} \geq \frac{1}{k}$. Donc la seule possibilité est $\gamma = 0$. Ceci est vrai pour tous les facteurs de u. On a ainsi u est pur et de pente 0. Ceci montre que f a un facteur de pente 0 de degré $\geq k$, ainsi nécessairement il existe $j \leq n-k$ tel que $\mathrm{ord}_p(b_j) = 0$ qui n'est pas possible par l'hypothèse $p \,|\, b_i$ pour $0 \leq j \leq n-k$ L'hypothèse est donc contredite ef f n'a pas de facteur de degré k. □

On montre maintenant le théorème 5.15 en utilisant ce lemme.

Démonstration. Soit $\alpha \in \mathbb{Q} \setminus \mathbb{Z}^-$. On écrit $\alpha = \frac{u}{v}$ avec $u \in \mathbb{Z}, v \in \mathbb{N}_{>}0$ premiers entre eux. Comme α n'est pas un entier négatif, on a que pour tout $j \in \{0, 1, ..., m-1\}$, $m - j + \alpha$ est non nul, ainsi $v(m-j) + u \neq 0$. On pose pour $0 \leq j \leq m$,

$$\begin{aligned} c_j &= (-1)^j \binom{m}{j} (m+\alpha)(m-1+\alpha)...(j+1+\alpha) \\ &= (-1)^j \binom{m}{j} \frac{(vm+u)(v(m-1)+u)...(v(j+1)+u)}{v^{m-j}}. \end{aligned}$$

On a que $m! L_m^{(\alpha)} = \sum_{j=0}^m c_j X^j$, pour alléger la notation, on note

$$g = m!\, v^m\, L_m^{(\alpha)} = v^m \sum_{j=0}^m c_j X^j \in \mathbb{Z}[X].$$

On suppose par l'absurde que g a un facteur de degré $k \in [1, m/2]$ dans $\mathbb{Z}[X]$. Ici, on prend k_0 un entier qui vérifie

1. Pour tout $k \geq k_0$, on a

$$(k - \frac{2k\sqrt{\log\log k}}{\log k})\,(\log k + 2\log\log k - \log 2) > k \log k.$$

2. On a

$$\sqrt{\log\log k_0} > v + |u|.$$

3. D'après le théorème des nombres premiers B.3, on suppose que pour tout $k \geq k_0$,

$$\pi(k\sqrt{\log\log k}) \leq \frac{2k\sqrt{\log\log k}}{\log k}.$$

On prend $m > m_0$, où m_0 vérifie les propriétés suivante :

1. Par le théorème B.4, il existe une constante $D(v)$ telle que pour tout $x \geq D(v)$ et $h \geq x/(2\log^2 x)$, l'intervalle $[x-h, x]$ contient un nombre premier congru à u modulo v. On demande que pour tout $m > m_0$, il existe j_0 tel que $vj_0 + u \in]m - \frac{m}{\log^2 m}, m]$ soit un nombre premier.
2. Pour tout $m > m_0$, on a

$$v(m - \frac{m}{\log^2 m}) + u \geq \max(\frac{2vm}{3}, \frac{1}{2}(vm+u), -v-u).$$

3. On utilise le lemme B.6 pour $a = v, b = u, c = v$, et $d = u - v$, le plus grand diviseur premier de $(vm+u)(v(m-1)+u)$ tend vers ∞ quand m tend vers ∞. On demande que pour tout $m > m_0$, il existe un diviseur premier p de $(vm + u)(v(m - 1) + u)$ tel que $p > (v + |u|)k_0$.
4. Si $u \neq 0$, par le lemme B.6, le plus grand diviseur premier de $m(vm + u)$ tend vers ∞ quand m tend vers ∞. On suppose que pour tout $m > m_0$ il existe p un tel diviseur premier de $m(vm + u)$ tel que $p > v + |u|$.

On établira une contradiction selon les quatre cas suivants :
Premier cas : $k > m/\log^2 m$.
Par hypothèse de m, il existe un $j_0 \in]m - k, m]$ tel que $vj_0 + u$ soit un nombre premier, noté p et $p \geq 2vm/3$. On a que p ne divise pas v. On a ainsi dans les coefficients de g :

$$v^m c_j = v^j \binom{m}{j} (vm + u)(v(m - 1) + u)...(v(j + 1) + u). \tag{10}$$

Pour tout $0 \leq j \leq m - k$, le nombre $vj_0 + u$ apparaît dans le produit. Donc on a

$$\mathrm{ord}_p(v^m c_j) \geq 1 \quad \text{pour } 0 \leq j \leq m - k.$$

Comme p ne divise pas v et $c_m = 1$, on a $\mathrm{ord}_p(v^m c_m) = 0$. Pour obtenir une contradiction avec le lemme 5.16, on va commencer par montrer que $\mathrm{ord}_p(v^m c_0) = 1$. Par hypothèse de m, on a $2p > vm + u$ et $p > -v - u$. Donc pour $j \in \{0, 1, ..., m - 1\}$, on a

$$2p > vm + u \geq v(m - j) + u \geq v + u > -p.$$

Comme les $v(m - j) + u$ sont non nuls, p est le seul multiple de p parmi les nombres $v(m - j) + u$ pour $0 \leq j \leq m - 1$. Or $v^m c_0 = (vm + u)(v(m - 1) + u) \dots (v + u)$, on a ainsi $\mathrm{ord}_p(v^m c_0) = 1$. Comme k un entier de $[1, m/2]$, on a $k \leq m - k$, on a pour $1 \leq j \leq k \leq m - k$

$$\mathrm{ord}_p(v^m c_j) \geq 1 > 1 - \frac{j}{k} = \mathrm{ord}_p(v^m c_0) - \frac{j}{k};$$

et pour $k < j \leq m$, on a

$$\mathrm{ord}_p(v^m c_j) \geq 0 > 1 - \frac{j}{k}.$$

Donc les conditions du lemme 5.16 sont vérifiées ; ceci est contradictoire avec le fait que g a un facteur de degré k.
Deuxième cas : $k_0 \leq k \leq m/\log^2 m$.
On note

$$z = k\sqrt{\log\log k}.$$

Dans un premier temps, on montre qu'il existe un nombre premier $p > z$ qui divise l'un des $v(m - j) + u$ pour $j \in \{0, 1, \dots, k - 1\}$. Posons

$$T = \{v(m - j) + u \,|\, 0 \leq j \leq k - 1\}.$$

Pour hypothèse de m, tous les éléments de T sont supérieurs ou égaux à $m/2$. De plus, comme $\mathrm{pgcd}(u, v) = 1$, tous les éléments de T sont premiers avec v. Pour tout nombre premier $p \leq z$, soient $r_p = \max\{\mathrm{ord}_p t \,|\, t \in T\}$ et $a_p \in T$ atteignant ce maximum : $r_p = \mathrm{ord}_p a_p$. On pose

$$S = T \setminus \{a_p \,|\, p \nmid v, p \leq z\}.$$

Par hypothèse de k_0,

$$\pi(z) \leq \frac{2k\sqrt{\log\log k}}{\log k}. \tag{11}$$

On a de plus $\mathrm{Card}(S) \geq k - \pi(z)$. Comme $k \leq m/\log^2 m$, on a $m \geq k\,\log^2 m \geq k\,\log^2 k$. Soit p un nombre premier et ne divise pas v. Par définition de a_p, pour $j > r_p$, il n'y a pas de multiple de p^j dans T (donc dans S). Pour $1 \leq j \leq r_p$, comme p ne divise pas v, il y a au plus $\lfloor k/p^j \rfloor + 1$ multiples de p^j dans T, donc au plus $\lfloor k/p^j \rfloor$ multiples de p^j dans S car $a_p \in S$. S'ensuivent les inégalités

$$\mathrm{ord}_p(\prod_{s\in S} s) \leq \sum_{j=1}^{r_p} \left\lfloor \frac{k}{p^j} \right\rfloor \leq \mathrm{ord}_p(k!) \quad \text{et} \quad \prod_{s\in S}\prod_{p\leq z} p^{\mathrm{ord}_p(s)} \leq \prod_{p\leq z} p^{\mathrm{ord}_p(k!)} \leq k! \leq k^k. \tag{12}$$

D'autre part, comme tous les éléments de T sont supérieurs ou égaux à $m/2$, on écrit

$$\prod_{s\in S} s \geq (\frac{m}{2})^{\mathrm{Card}(S)} \geq (\frac{k\,\log^2 k}{2})^{k-\pi(z)}.$$

En utilisant la majoration (11) de $\pi(z)$, on obtient

$$\begin{aligned}
\log(\prod_{s\in S} s) &\geq (k-\pi(z))(\log k + 2\log\log k - \log 2) \\
&\geq (k - \frac{2k\sqrt{\log\log k}}{\log k})(\log k + 2\log\log k - \log 2) \\
&> k\log k \quad \text{(par hypothèse sur } k_0\text{)}.
\end{aligned}$$

On a ainsi par (12)

$$\log(\prod_{s\in S} s) > k\log k \geq \log(\prod_{s\in S}\prod_{p\leq z} p^{\mathrm{ord}_p(s)}).$$

Donc il existe un nombre premier $p > z$ qui divise certains éléments de S et donc certains éléments de $T = \{v(m-j)+u : 0 \leq j \leq k-1\}$. Puisque p divise l'un des facteurs de (10), on a alors l'inégalité suivante :

$$\mathrm{ord}_p(v^m c_j) \geq 1 \quad \text{pour } 0 \leq j \leq m-k.$$

Fixons un nombre premier $p > z$ qui divise un élément de T, et soit $j \in [1, m]$; on montre $\mathrm{ord}_p(v^m c_j) > \mathrm{ord}_p(v^m c_0) - j/k$ comme suit :

$$\begin{aligned}
\mathrm{ord}_p(v^m c_0) - \mathrm{ord}_p(v^m c_j) &\leq \mathrm{ord}_p((vj+u)(v(j-1)+u)...(v+u)) \\
&\leq \mathrm{ord}_p((vj+|u|)!) = \sum_{i=1}^{\infty}[\frac{vj+|u|}{p^i}] \\
&< \sum_{i=1}^{\infty} \frac{vj+|u|}{p^i} = \frac{vj+|u|}{p-1} \\
&\leq \frac{vj+|u|}{k\sqrt{\log\log k}} \quad (\text{car } p > z = k\sqrt{\log\log k}) \\
&< \frac{j}{k} \quad \text{(par hypothèse sur } k_0\text{)}.
\end{aligned}$$

Donc on a

$$\mathrm{ord}_p(v^m c_j) = \mathrm{ord}_p(c_j) > \mathrm{ord}_p(v^m c_0) - \frac{j}{k}.$$

Comme $\mathrm{ord}_p(v^m c_m) = 0$, on aboutit à une contradiction d'après le lemme 5.16.
Troisième cas : $2 \leq k \leq k_0$.
Par hypothèse sur m, il existe un diviseur premier p de $(vm+u)(v(m-1)+u)$ tel que $p > (v+|u|)k_0$. Comme $(vm+u)(v(m-1)+u)$ apparaît dans le produit du numérateur de c_j pour tout $j \leq m-2$, on a ainsi $p | v^m c_j$ pour tout $0 \leq j \leq m-2$, donc

$$\mathrm{ord}_p(v^m c_j) \geq 1 \quad \text{pour } 0 \leq j \leq m-k.$$

On utilise le même calcul que dans le deuxième cas, pour tout $j \in [1, m]$

$$\frac{\mathrm{ord}_p(v^m c_0) - \mathrm{ord}_p(v^m c_j)}{j} < \frac{vj+|u|}{j(p-1)} \leq \frac{v+|u|}{p-1} \leq \frac{1}{k_0} < \frac{1}{k}.$$

Ce qui donne l'inégalité $\mathrm{ord}_p(v^m c_j) > \mathrm{ord}_p(v^m c_0) - j/k$. Et on a une contradiction d'après le lemme 5.16 comme dans les deux cas précédents.
Quatrième cas : $k = 1$.
Si $u = 0$, on peut le vérifier à la main, en utilisant encore le lemme 5.16. Si $u \neq 0$, par hypothèse de m, il existe un diviseur premier p tel que $p > v + |u|$. Cela nous dit que $p \nmid v$. Le cas $p | vm+u$ est comme le troisième cas. On considère le cas $p | m$. On utilise le même calcul que dans le deuxième cas, pour tout $j \in [1, m]$

$$\frac{\mathrm{ord}_p(v^m c_0) - \mathrm{ord}_p(v^m c_j)}{j} < \frac{vj+|u|}{j(p-1)} \leq \frac{v+|u|}{p-1} \leq 1.$$

Cela nous donne tout de suite $\mathrm{ord}_p(v^m c_j) > \mathrm{ord}_p(v^m c_0) - j$.

Il reste à vérifier que $\mathrm{ord}_p(v^m c_j) \geq 1$ pour tout $0 \leq j \leq m-1$. On a

$$v^m c_j = v^j \binom{m}{j} (vm+u)(v(m-1)+u)...(v(j+1)+u).$$

Pour $m-p+1 \leq j \leq m$, on a que p divise $\binom{m}{j}$, donc $\mathrm{ord}_p(v^m c_j) \geq 1$. Pour $j \leq m-p$, le numérateur de la fraction contient un produit de $\geq p$ termes consécutifs dans la progression arithmétique $vt+u$ avec $\mathrm{pgcd}(p, v) = 1$. Donc p divise ce produit et $\mathrm{ord}_p(v^m c_j) \geq 1$. Cela nous donne la contradiction par le lemme 5.16.

En regroupant ces quatre cas, on a que pour un α fixé, pour un n assez grand, les $L_n^{(\alpha)}$ sont tous irréductibles. □

5.3.2 Le groupe de Galois sur $\mathbb{Q}$ des polynômes de Laguerre généralisés

On revient au problème de groupe de Galois pour les polynômes de Laguerre généralisés. On formalise en un seul lemme les analogues des lemmes 5.11 et 5.13 concernant les polynômes de Taylor de l'exponentielle. Il s'agira ensuite de vérifier que l'on peut l'appliquer aux $L_n^{(\alpha)}$.

Lemme 5.18. *Soit p un nombre premier dans $]\frac{n}{2}, n-2[$, et soit $P = \sum_{j=0}^{n} \binom{n}{j} c_j X^j \in \mathbb{Q}[X]$ un polynôme irréductible de degré n et $\mathrm{ord}_p(c_p) \geq 0$ pour $j = 0, 1, \ldots, n$. Supposons de plus*

1. $\mathrm{ord}_p(c_0) = 1$ *;*

2. $\mathrm{ord}_p(c_j) \geq 1$ *pour* $1 \leq j \leq n-p$;
3. $\mathrm{ord}_p(c_p) = 0$.

Alors le groupe de Galois de P *sur* $\mathbb{Q}$ *contient le groupe alterné* A_n.

Démonstration. On voit que $\binom{n}{j}$ est divisible par p si et seulement si $n-p+1 \leq j \leq p-1$. L'hypothèse sur les ordres des coefficients donne que le segment qui lie $(0, -1)$ et $(p, 0)$ est le premier côté du polygone de Newton de P et que sa pente vaut $\frac{1}{p}$. Le même raisonnement que pour la preuve du lemme 5.2 donne p divise n, donc p divise l'ordre du groupe de Galois de P. Par le théorème de Cauchy, le groupe de Galois de P admet un p-cycle (puisque ce sont les seuls éléments d'ordre $p \in]\frac{n}{2}, n-2[$ dans un sous-groupe de S_n). Par le théorème A.3, il est A_n ou S_n. Donc le groupe de Galois de P est A_n si $disc(P) \in \mathbb{Q}^2$, S_n sinon. □

On note $\Delta_n^{(\alpha)}$ comme le discriminant de $L_n^{(\alpha)}$.

Théorème 5.19. *Soit* $\alpha \in \mathbb{Q} \setminus \mathbb{Z}_-$ *fixé. Sauf un nombre fini d'entiers, pour tout nombre entier positif* n*, le groupe de Galois de* $L_n^{(\alpha)}$ *sur* $\mathbb{Q}$ *contient* A_n.

Remarque 5.20. Par le lemme 5.1, on voit que le groupe de Galois de $L_n^{(\alpha)}$ sur $\mathbb{Q}$ est A_n si le discriminant de $L_n^{(\alpha)}$ est un carré dans $\mathbb{Q}$. Le groupe de Galois est S_n, sinon.

Démonstration. Soit $\lambda, \mu \in \mathbb{Z}$ vérifiant $\alpha = \frac{\lambda}{\mu}$ avec $\mu \geq 1$ et $\mathrm{pgcd}(\lambda, \mu) = 1$. On normalise le polynôme de Laguerre généralisé en posant

$$P = \mu^n \, n! \, L_n^{\left(\frac{\lambda}{\mu}\right)}\left(\frac{-X}{\mu}\right) = \sum_{j=0}^{n} \binom{n}{j} (n\mu+\lambda)\big((n-1)\mu+\lambda\big)...\big((j+1)\mu+\lambda\big)X^j.$$

On voudrait appliquer le lemme 5.18 avec

$$c_j = \prod_{k=j+1}^{n} (k\mu+\lambda), \quad 0 \leq j \leq n.$$

On cherche un nombre premier p qui vérifie les conditions du lemme 5.18.

Par le théorème B.4, on a qu'il existe $D(\mu)$ tel que pour tout $x \geq D(\mu)$ et $h \geq \frac{x}{2\log^2 x}$, l'intervalle $[x-h, x]$ contient au moins un nombre premier congru à λ mod μ. On prend n assez grand, posons $x = n-3 \geq D(\mu)$, on note que pour n assez grand, on a

$$\frac{1-\frac{3}{n}}{2\log^2(n-3)} + \frac{3+\frac{\lambda+\mu}{\mu+1}}{n} \leq \frac{1}{\mu+1}.$$

Ce qui est équivalent à

$$x - \frac{n\mu+\mu+\lambda}{\mu+1} \geq \frac{x}{2\log^2 x}.$$

Posons $h = x - \frac{n\mu+\mu+\lambda}{\mu+1}$. Par le théorème A.3, il existe $l \in [1, n]$ tel que $p = \mu l + \lambda$ est un nombre premier et

$$\frac{n\mu+\mu+\lambda}{\mu+1} \leq p \leq n-3.$$

On montre que ce nombre premier p vérifie les conditions du lemme 5.18.

Pour cela, on doit avoir $p > \frac{n}{2}$, on voit que

$$\frac{n\mu+\mu+\lambda}{\mu+1} > \frac{n}{2} \Longleftrightarrow n(\mu-1) > -2\mu-2\lambda.$$

Comme α n'est pas un entier négatif, on a :

1. Si μ =1, alors $\lambda \geq 0$ qui donne l'inégalité précédente pour tout n ;
2. Si $\mu > 1$, il suffit que $n > -\frac{2(\mu+\lambda)}{\mu-1}$ pour que $p > \frac{n}{2}$ ce qui est vrai si n est assez grand.

Maintenant, on vérifie les conditions sur les valuations p-adiques (i.e ord_p) des coefficients c_j. Pour cela, on regarde les nombres congrus à λ mod μ, comme $p = \mu l + \lambda$ et $\mathrm{pgcd}(\mu, \lambda) = 1$, on a que $p \,|\, k\mu + \lambda \Leftrightarrow p \,|\, k - l$, donc p est le seul nombre de la forme $\lambda + k\mu$ divisible par p dans l'intervalle $[p - \mu p + 1, p + \mu p - 1]$. On montre alors pour n assez grand que

$$(-\mu + 1)p < \lambda + \mu \quad \text{et } \lambda + \mu n < (\mu + 1)p.$$

En fait la deuxième inégalité est une conséquence de l'inégalité $\frac{n\mu+\mu+\lambda}{\mu+1} \leq p$ posée pendant qu'on construit p. Pour la première inégalité, si $\mu = 1$, $\lambda \geq 0$, elle est vraie pour tout n. Si $\mu \geq 2$, il suffit que $n \geq -2\lambda$ pour avoir cette inégalité.

Donc on a que, pour n assez grand, $p = \mu l + \lambda$ est le seul nombre divisible par p parmi $\mu + \lambda, 2\mu + \lambda, ..., n\mu + \lambda$. Donc comme $c_j = \prod_{k=j+1}^{n}(k\mu + \lambda)$, on a clairement que $\mathrm{ord}_p(c_j) = 1 \quad$ pour $0 \leq j \leq l - 1$, et $\mathrm{ord}_p(c_j) = 0 \quad$ pour $l \leq j \leq n$. De plus, les deux inégalités précédentes donnent exactement $p > l - 1$ et $n - p < l$, donc p vérifie la condition du 5.18 et aussi $L_n^{(\alpha)}$ est irréductible si n est assez grand. La démonstration du théorème est complète. □

Remarque 5.21. Schur [S] a calculé les discriminants des polynômes de Laguerre généralisés explicitement :

$$\Delta_n^{(\alpha)} = \prod_{j=2}^{n} j^j (\alpha + j)^{j-1}.$$

On considère un cas particulier. Prenons $\alpha = -2 - n$. On a

$$\Delta_n^{(\alpha)} = (n!)^{n+1}(-1)^{n(n-1)/2},$$

d'où pour n assez grand, le groupe de Galois G_n de $L_n^{(-2-n)}$ est A_n si 4 divise $n - 1$, et S_n sinon. En fait, c'est vrai pour tout n, on peut voir [H2].

A Appendice : Théorème de Jordan

Définition A.1. Soient $r \leq n$ et G un groupe agissant sur $\{1, 2, \ldots, n\}$. Le groupe G est dit m-transitif sur k éléments $\{i_1, i_2, \ldots, i_k\} (k \geq m)$, si $G \cdot \{i_1, i_2, \ldots, i_k\} \subseteq \{i_1, i_2, \ldots, i_k\}$ et pour tous $a_1, a_2, \ldots, a_m$ et $b_1, b_2, \ldots, b_m$ où $a_i, b_l \in \{i_1, i_2, \ldots, i_k\}$ et $a_i \neq a_j$, $b_l \neq b_k$ si $i \neq j$, $l \neq k$, il existe $g \in G$ satisfaisant

$$g(a_i) = b_i, \quad \text{pour } 1 \leq i \leq m.$$

On dit que G est m-transitif s'il est m-transitif sur $\{1, 2, \ldots, n\}$. Et on dit que G est transitif, s'il est 1-transitif.

Remarque A.2. Soit G un groupe agissant r-transitivement sur $\{1, 2, \ldots, n\}$. Si le sous-groupe H fixant r lettres est lui-même s-transitif sur les autres $(n - r)$ lettres, alors G est $(r + s)$-transitif.

Théorème A.3 (Jordan, version faible)**.** *Soit G un sous-groupe de S_n qui agit transitivement sur $\{1, 2, \ldots, n\}$. Soit $p \in]\frac{n}{2}, n-2[$ un nombre premier. Si G contient un p-cycle, alors G est soit S_n, soit A_n.*

Définition A.4. Soit G un sous-groupe agissant sur $\{1, 2 \ldots, n\}$ qui peut être divisé en les ensembles disjoints $S_1, S_2, \ldots, S_m$ tel que tout $g \in G$ soit envoie les éléments de S_i dans lui-même, soit les envoie dans un autre S_j. Sauf dans le cas trivial où tous les S_i sont de cardinal 1, on dit que G est imprimitif ; sinon, on dit que G est primitif.

Lemme A.5. *Soient $n, p \in \mathbb{N}_{>0}$ et $p \in]\frac{n}{2}, n]$. Soient G un sous-groupe transitif de S_n contenant un p-cycle. Alors G est $(n - p + 1)$-transitif.*

Démonstration. Soit H un sous-groupe de G engendré par le p-cycle. L'action de H est transitive sur l'ensemble de p éléments formant le support du p-cycle et fixe les autres $n-p$ éléments. Chaque conjugué de H est transitif sur un certain ensemble de p éléments. Comme on a $p > \frac{n}{2}$, deux conjugués quelconques de H ont des éléments communs dans leur supports.

Soit H' un conjugué de H dont le support est différent de celui de H. De plus, on suppose que H' a le plus grand nombre d'éléments communs s avec H dans son support. On écrit

$$\begin{aligned} &\text{supp}H : \{a_1, a_2, \ldots, a_r, c_1, c_2, \ldots, c_s\}; \\ &\text{supp}H' : \{b_1, b_2, \ldots, b_r, c_1, c_2, \ldots, c_s\}, \qquad \text{avec } r + s = p. \end{aligned}$$

On va montrer que $r = p - s = 1$. Considérons un élément $h' \in H'$

$$h' = \begin{pmatrix} b_1 & \ldots & b_u & b_{u+1} & \ldots & b_r & c_1 & \ldots & c_{r-u} & c_{r-u+1} & \ldots & c_s \\ b_{i_1} & \ldots & b_{i_u} & c_{i_{u+1}} & \ldots & c_{i_r} & b_{j_1} & \ldots & b_{j_{r-u}} & c_{j_{r-u+1}} & \ldots & c_{j_s} \end{pmatrix}$$

où cela signifie que les b_k sont envoyés vers b_{i_k} pour $1 \leq k \leq u$, etc. Donc $h'Hh'^{-1}$ agit sur un ensemble contenant r éléments de type a, $(r - u)$ éléments de type b et $(s - r + u)$ éléments de type c. Il a $s + u$ éléments dans son support communs avec H. Supposons $r > 1$. Comme H' est cyclique d'ordre p premier, H' est primitif. On peut choisir un h' avec $1 \leq u < r$. Donc $s < s + u < p$ contredit la maximalité de s. Donc on a bien $r = 1$.

Maintenant, considérons le groupe H_1 engendré par H et H' ; H_1 est doublement transitif (donc primitif) sur $p + 1$ éléments par la remarque A.2. Dans la preuve, on n'a utilisé que les propriétés suivantes sur H :

1. $\mathrm{Card}(H) > \frac{n}{2}$;
2. H est primitif.

Le groupe H_1 satisfait aussi les propriétés. En remplaçant H par H_1, on répètè le même argument. On obtient un sous-groupe de G 3-transitif sur $p+2$ éléments....Enfin, on a que G est $(n-p+1)$-transitif. □

Lemme A.6. *Soient G un groupe t-transitif sur $\{1, 2, \ldots, n\}$, H un sous-groupe de G fixant t éléments et P un p-sous-groupe de Sylow de H. On suppose que P fixe $w \geq t$ éléments. Alors, le normalisateur $N_G P$ de P dans G est t-transitif sur l'ensemble des éléments fixés par P.*

Démonstration. Soient $\{a_1, a_2, \ldots, a_t\}$ et $\{b_1, b_2, \ldots, b_t\}$ deux sous-ensembles des points fixés par P et $a_i \neq a_j, b_l \neq b_k$ si $i \neq j, l \neq k$. Alors, comme G est t-transitif, il y un élément $x \in G$ envoyant a_i vers b_i pour $i = 1, 2, \ldots, t$. Alors, xPx^{-1} fixe $b_1, b_2, \ldots, b_t$ et donc P et xPx^{-1} sont tous les deux des sous-groupes de Sylow du groupe H' fixant $b_1, b_2, \ldots, b_t$. Par les théorèmes de Sylow, il existe $y \in H'$ tel que on ait $y(xPx^{-1})y^{-1} = P$. Posons $z = yx$. Alors, z envoie a_i vers b_i pour $1 \leq i \leq t$ et $zPz^{-1} = P$. Donc il y a un élément $N_G P$ qui envoie $(a_1, a_2, \ldots, a_t)$ vers $(b_1, b_2, \ldots, b_t)$. Par ailleurs, tout élément de N envoie un élément fixé par P à un autre élément fixé par P. Donc $N_G P$ est t-transitif sur les w éléments fixés par P. □

Lemme A.7. *Soient n, p, r des entiers avec $n = p + r$, où p est premier et $r \geq 3$. Tout sous-groupe $(r+1)$-transitif de S_n est soit S_n soit A_n.*

Démonstration. Soit G un sous-groupe $(r+1)$-transitif de S_n. On note $\{1, 2, \ldots, n\}$ l'ensemble sur lequel S_n agit naturellement. Soit H le sous-groupe de G fixant les r premiers éléments $1, 2 \ldots, r$, il est transitif sur les p autres éléments. Donc p divise $\mathrm{Card}(H)$ et H contient un p-sous-groupe de Sylow P avec $\mathrm{Card}(P) = p$. Donc P est engendré par un p-cycle, noté a. Maintenant, soit N le normalisateur de P dans G. Par le lemme A.6, quand on ne considère que l'action de N sur les r premiers éléments, on a une surjection $N \twoheadrightarrow S_r$ donnée par la restriction, puisque l'action de N stabilise $\{1, 2, \ldots, r\}$ ainsi que son complémentaire $\{r+1, r+2, \ldots, n\}$. On discute en deux cas.

Cas 1. $r \geq 5$. Posons $N_1 = \{g \in N \mid$ la restriction de g sur $\{1, 2, \ldots, r\}$ est dans $A_r\}$. Considérons l'application ϕ suivante :

$$\begin{aligned} \phi = (\phi_1, \phi_2) : \quad N_1 &\to A_r \times S_p \\ g &\mapsto (g|_{\{1,2,\ldots,r\}}, g|_{\{r+1,r+2,\ldots,r+p\}}). \end{aligned}$$

Posons

$$H_1 = \{g \in N_1 \mid \phi_2(g) = \mathrm{id}\}, \quad H_2 = \{g \in N_1 \mid \phi_1(g) = \mathrm{id}\},$$

i.e

$$H_1 = \ker \phi_2, \quad H_2 = \ker \phi_1.$$

Alors, il est facile de voir que

$$\phi_1(H_1) \lhd A_r \quad \text{et } \phi_2(H_2) \lhd \phi_2(N_1).$$

On montre

$$A_r/\phi_1(H_1) \simeq \phi_2(N_1)/\phi_2(H_2).$$

On définit un morphisme des groupes

$$\begin{array}{rccc} \eta: & A_r/\phi_1(H_1) & \to \phi_2(N_1)/\phi_2(H_2) \\ & \overline{g_1} & \mapsto \overline{g_2}, \end{array}$$

où $\overline{g_2}$ vérifie $(g_1, g_2) \in \phi(N_1)$. D'abord, on montre que cette application est bien définie. Soient $g_1, g_1' \in A_r$ vérifiant $\overline{g_1} = \overline{g_1'}$. Soient $g_2, g_2' \in S_p$ vérifiant $(g_1, g_2), (g_1', g_2') \in \phi(N_1)$. On montre $\overline{g_2} = \overline{g_2'}$. Comme $\overline{g_1} = \overline{g_1'}$, il existe $\tilde{g_1} \in \phi_1(H_1)$ avec $g_1' = g_1\tilde{g_1}$. Donc, $(g_1', g_2') \cdot (\tilde{g_1}^{-1}, \mathrm{id}) \cdot (g_1^{-1}, g_2^{-1}) = (\mathrm{id}, g_2' g_2^{-1}) \in \phi(N_1)$. On a donc $\overline{g_2} = \overline{g_2'}$. Il est facile de voir que η est un morphisme des groupes. Si $\eta(\overline{g_1}) = \overline{\mathrm{id}}$, par définition de η, on a $(g_1, \mathrm{id}) \in \phi(N_1)$. Donc $g_1 \in H_1$ et on a $\overline{g_1} = \overline{\mathrm{id}}$. Ça implique que η est injective. Par définition, pour chaque $\overline{g_2} \in \phi_2(N_1)/\phi_2(H_2)$, il existe $g_1 \in A_r$ avec $(g_1, g_2) \in \phi(N_1)$. Donc on a $\eta(\overline{g_1}) = \overline{g_2}$. Ça implique que η est surjective. On conclut que η est un isomorphisme entre les deux groupes et on a

$$A_r/\phi_1(H_1) \simeq \phi_2(N_1)/\phi_2(H_2).$$

Comme $P \in N_1$, $\phi_2(N_1)$ contient $\phi_2(P)$ qui est un sous-groupe distingué d'ordre p. Donc on a une application naturelle ψ de $\phi_2(N_1)$ dans le groupe des automorphismes de $\phi_2(P)$, noté $\mathrm{Aut}(\phi_2(P))$, dont le noyau est $\phi_2(P)$. Comme $\mathrm{Im}\psi$ est un sous-groupe de $\mathrm{Aut}\phi_2(P) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, le quotient $\phi_2(N_1)/\phi_2(P)$ est commutatif. Aussi, on a $P \subseteq H_2$; ainsi, $\phi_2(N_1)/\phi_2(H_2)$ est commutatif. Comme A_r est un groupe simple et non-commutatif pour $r \geq 5$, $\phi_1(H_1)$ est égal à A_r. Donc G contient un 3-cycle. Comme G est r-transitif, donc 3-transitif, il contient tous les 3-cycles. Donc G est soit S_n, soit A_n.

Cas 2. $r = 3, 4$. On prend les mêmes définitions de ψ, ϕ, ϕ_1 et ϕ_2 que dans le cas 1. Si $p = 3$, on a fini, car P contient déjà un 3-cycle. On suppose $p \neq 3$. Par le lemme A.6, N est r-transitif sur $\{1, 2, \ldots, r\}$. Donc il existe $u = (1\,2)(3)\cdots$ et $v = (1)(2\,3)\cdots$ dans N. P est engendré par a. Comme $\psi(\phi_2(u)\phi_2(v))(\phi_2(a)) = \psi(\phi_2(v)\phi_2(u))(\phi_2(a))$, on a $w = u^{-1}v^{-1}uv = (1\,2\,3)\cdots$ commute avec a. Donc quand on restreint w sur $\{r+1, r+2, \ldots, r+p\}$, il est une puissance de $\phi_2(a)$. Donc $w^p = (1\,2\,3)$ ou $(1\,3\,2)$. Et, comme avant, on a fini la preuve. □

La démonstration du théorème. Combinant les lemmes A.5 et A.7, on achève la preuve. □

B Appendice : Répartition des nombres premiers

B.1 Postulat de Bertrand

Le postulat de Bertrand original est : pour chaque $n \geq 1$, il y a un nombre premier p avec $n < p \leq 2n$. Il est conjecturé et vérifié pour $n < 3000000$ par Joseph Bertrand. Il est prouvé pour la première fois par Pafnuty Chebychev en 1850. Dans notre exposé, on le modifie un peu.

Théorème B.1. *Pour $n \geq 8$, il y a un nombre premier $p \in]\frac{n}{2}, n-2[$.*

Remarque B.2. Pour $n = 7$, il n'y a pas de premier dans $]\frac{7}{2}, 5[$.

Démonstration. On le discute en trois cas.

Cas 1. $8 \leq n \leq 26$. On peut le faire à la main.

Dans les deux cas suivants, on montre que pour $n > 13$, il y a un nombre premier $p \in]n, 2n-3[$.

Cas 2. $13 < n \leq 6000$. Considérons une suite de nombres premiers

$$13, 17, 23, 29, 43, 53, 83, 97, 163, 209, 317, 421, 631, 1259, 2503, 4001, 5009, 6131.$$

Chaque terme $a_s \leq 2a_{s-1} - 4$, d'où tout intervalle $\{y \mid n < y \leq 2n-3\}$ avec $n \leq 6000$ contient l'un de ces premiers.

Cas 3. $n > 6000$. D'abord, on montre

$$\prod_{p \leq x} p \leq 4^{x-1} \quad \text{pour } x \geq 2 \text{ réel.} \tag{13}$$

Ici et dans la suite, cela signifie que le produit est pris sur tous les premiers $p \leq x$. Pour $x = 2, 3$, c'est vrai. Après, il suffit de le faire pour $x \in \mathbb{N}$ impair. Supposons l'inégalité (13) vraie pour $x < 2m+1$. Par l'hypothèse de récurrence, on a

$$\prod_{p \leq m+1} p \leq 4^m.$$

L'inégalité

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

provient de l'observation que $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ est entier, et que les nombres premiers dans le produit divisent le numérateur mais pas le dénominateur. Enfin, on a

$$\binom{2m+1}{m} \leq 2^{2m},$$

parce que

$$\binom{2m+1}{m} = \binom{2m+1}{m+1},$$

et

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}.$$

Donc

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \leq 4^m \binom{2m+1}{m} \leq 4^m 2^{2m} = 4^{2m}.$$

On va estimer $\binom{2n-3}{n}$. Pour p un nombre premier, $\binom{2n}{n}$ contient le facteur premier p exactement

$$\sum_{k \geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

fois. Ici, chaque terme est ≤ 1, car

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1 \right) = 2.$$

En plus, quand $p^k > 2n$, le terme est nul. Donc $\binom{2n}{n}$ contient p exactement

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \leq \max\{r \mid p^r \leq 2n\}$$

fois. Donc $p^{\mathrm{ord}_p\binom{2n}{n}} \leq 2n$. En particulier, les nombres premiers $p > \sqrt{2n}$ apparaissent au plus une fois dans $\binom{2n}{n}$. En plus, les nombres premiers $p \in]\frac{2}{3}n, n]$ ne divisent pas $\binom{2n}{n}$. Comme $3p > 2n$ entraîne que les seuls multiples de p qui apparaissent dans $(2n)!$ sont p et $2p$. Puisque p apparaît aussi dans $n!$, on a $p \nmid \binom{2n}{n}$. Comme

$$\sum_{k=0}^{2n}\binom{2n}{k} = 4^n,$$

et

$$\binom{2n}{n} \geq \binom{2n}{k}, \quad \text{pour } k = 0, 1, \ldots, 2n,$$

on a

$$\binom{2n}{n} \geq \frac{4^n}{2n}.$$

Maintenant, on estime $\binom{2n-3}{n}$:

$$\frac{4^n}{2n}\frac{n(n-1)(n-2)}{2n(2n-1)(2n-2)} \leq \binom{2n-3}{n} \leq \prod_{p\leq\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \cdot \prod_{n<p\leq 2n-3} p.$$

S'il n'y a pas de premiers entre n et $2n-3$, on a

$$\frac{4^{n-1}}{6n} \leq (2n)^{\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \leq (2n)^{\sqrt{2n}} 4^{\frac{2}{3}n-1},$$

i.e

$$\frac{1}{3}4^{\frac{1}{3}n} \leq (2n)^{\sqrt{2n}+1}.$$

Mais, on a

$$2n = (\sqrt[6]{2n})^6 < (\lfloor\sqrt[6]{2n}\rfloor + 1)^6 < 2^{6\lfloor\sqrt[6]{2n}\rfloor} \leq 2^{6\sqrt[6]{2n}};$$

Donc pour $n \geq 50$ (et donc $18 < 2\sqrt{2n}$), on obtient

$$\frac{1}{27}2^{2n} \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Donc on a

$$2n \leq 20(2n)^{2/3} + \log_2 27,$$

qui contredit le fait $n > 6000$. Donc on finit la preuve. □

B.2 Autour du théorème des nombres premiers

On admet les théorèmes suivants. On peut trouver la preuve du premier théorème dans le chapitre 4 de [M], et la preuve du deuxième théorème dans le chapitre 5 de [IK].

Théorème B.3 (Théorème des nombres premiers)**.** *En définissant pour tout réel positif x, le nombre $\pi(x)$ comme le nombre de nombres premiers inférieures à x, alors on a*

$$\pi(x) \sim \frac{x}{\log x}, \quad \text{quand } x \to \infty.$$

Théorème B.4 (Théorème de Siegel-Walfisz)**.** *Soient $a, b \in \mathbb{N}^*$ premiers entre eux et $A > 0$, on note $\pi(x; b, a)$*

$$\text{Card}\{p \,|\, p \leq x \,\text{premier}, \, p \equiv a \pmod{b}\}.$$

Alors

$$\pi(x; b, a) = \frac{\text{Li}(x)}{\phi(b)} + O\Big(\frac{x}{(\log x)^A}\Big),$$

où $\text{Li}(x) = \int_2^x \frac{1}{\ln t} dt$.

B.3 Le plus grand nombre premier divisant $(am + b)(cm + d)$

La preuve du théorème suivant se trouve dans les paragraphes 6 et 7 du chapitre 4 de [BC]. On l'admet ici.

Théorème B.5 (Thue)**.** *Soient u, v, w sont des entiers et $w \neq 0$, alors l'équation suivante*

$$ux^3 - vy^3 = w$$

n'a qu'un nombre fini de solutions entières.

On en déduit un résultat qui nous est bien utile.

Corollaire B.6. *Soit a, b, c et d sont des nombres entiers tel que $bc - ad \neq 0$, alors le plus grand facteur premier de $(am + b)(cm + d)$ tend vers ∞ quand le nombre entier m tend vers ∞.*

Démonstration. Supposons qu'il y a un nombre entier N et une suite (m_i) croissante vers ∞ vérifiant pour p premier

$$p \,|\, (am_i + b)(cm_i + d) \Rightarrow p < N.$$

Donc il existe un nombre entier l et des nombres premiers $p_1, p_2, \ldots, p_l$ vérifiant

$$am_i + b = p_1^{a_1^{(i)}} p_2^{a_2^{(i)}} \ldots p_l^{a_l^{(i)}}, \quad cm_i + d = p_1^{b_1^{(i)}} p_2^{b_2^{(i)}} \ldots p_l^{b_l^{(i)}},$$

pour des entiers $a_j^{(i)}$ et $b_j^{(i)}$ convenables. On les reécrit

$$am_i + b = p_1^{r_1^{(i)}} p_2^{r_2^{(i)}} \ldots p_l^{r_l^{(i)}} x_i^3, \quad cm_i + d = p_1^{s_1^{(i)}} p_2^{s_2^{(i)}} \ldots p_l^{s_l^{(i)}} y_i^3,$$

où $r_j^{(i)}, s_j^{(i)}$ sont dans $\{0,1,2\}$, et x_i, y_i sont entiers. Comme (m_i) est infinie, on peut trouver deux l-uplets $(r_1, r_2, \ldots, r_l)$ et $(s_1, s_2, \ldots, s_l) \in \{0,1,2\}^l$, tel qu'on ait un nombre infini de i vérifiant

$$(r_1^{(i)}, r_2^{(i)}, \ldots, r_l^{(i)}) = (r_1, r_2, \ldots, r_l), \quad (s_1^{(i)}, s_2^{(i)}, \ldots, s_l^{(i)}) = (s_1, s_2, \ldots, s_l).$$

Donc l'équation

$$ap_1^{s_1} p_2^{s_2} \ldots p_l^{s_l} y^3 - cp_1^{r_1} p_2^{r_2} \ldots p_l^{r_l} x^3 = ad - bc \neq 0.$$

admet un nombre infini de solutions entières, ce qui contredit le théorème de Thue. Ceci termine la démonstration. □

Références

[AZ] M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, Springer, 1998.

[BC] Z. I. Borevitch, I. R. Chafarevitch, *Théorie des nombres* (traduite du russe), Gauthier-villars, 1967.

[C] J. W. S. Cassels, *Local fields*, London Mathematical Society Student Texts 3, 1986.

[Co] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, Enseign. Math. (2) **33** (1987), no. 3-4, 183-189.

[F1] M. Filaseta, *The irreductibility of all but finitely many Bessel polynomials*, Acta Math. **174** (1995), 383-396.

[FT] M. Filaseta, T.-Y. Lam, *On the irreducibility of the generalized Laguerre polynomials*, Acta Arith. **105** (2002), no 2, 177-182.

[H1] F. Hajir, *On the Galois groups of generalized Laguerre polynomials*, J.Th. Nombres Bordeaux **17** (2005), no 2, 517-525.

[H2] F. Hajir, *Some $\tilde{A}_n$-Extensions Obtained from Generalized Laguerre Polynomials*, J. Number Theory **50** (1995), no 2, 206-212.

[Ha] M. Hall, *The theory of groups*, The Macmillan Company, 1959.

[M] M. R. Murty, *Problems in analytic number theory*, Springer, 2000.

[IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society, Colloquium Publications v53, 2004.

[K] N. Koblitz, *P-adic numbers, p-adic analysis and zeta functions*, Springer-Verlag, 1984.

[P] G. Pólya, *Zur arithmetischen Untersuchung der polynome*, Math. Z.**1** (1918), 143-148.

[S] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, J. Reine Angew. Math. **165** (1931),52-58.