# Grand crible et applications

David Michel

25/05/15 – 03/07/15

## Table des matières

*Ce rapport est le compte-rendu d'un stage de six semaines effectué sous la direction de Florent Jouve à l'École Normale Supérieure. Durant ce stage, j'ai pu partager le quotidien des chercheurs partageant mon bureau, mais également assister à un séminaire de théorie des nombres à l'Institut Henri Poincaré, accompagné par mon maître de stage.*

On va s'intéresser au théorème suivant, démontré par Gallagher en 1973.

**Théorème** (Gallagher)**.** Soit $r \geq 1$ un entier. Pour tout entier $N \geq 1$, définissons $E_r(N)$ comme l'ensemble des polynômes $f \in \mathbb{Z}[T]$ unitaires de degré $r$ tels que

$$f = T^r + a_{r-1}T^{r-1} + \cdots + a_1 T + a_0$$

avec $|a_i| \leq N$ pour tout $0 \leq i < r$ et tels que le groupe de Galois de $f$ n'est pas isomorphe au groupe symétrique $\mathfrak{S}_r$. Alors

$$|E_r(N)| \ll r^3(2N+1)^{r-\frac{1}{2}}(\log N)$$

pour $N \geq 2$, où la constante sous-entendue est absolue.

On commencera par étudier le résultat suivant :

**Théorème.** Soit $r \geq 1$ un entier. Pour tout entier $N \geq 1$, définissons $E_r(N)$ comme l'ensemble des polynômes $f \in \mathbb{Z}[T]$ unitaires réductibles de degré $r$ tels que

$$f = T^r + a_{r-1}T^{r-1} + \cdots + a_1 T + a_0$$

où $|a_i| \leq N$ pour tout $0 \leq i < r$. Alors,

$$|E_r(N)| \ll r^2(2N+1)^{r-\frac{1}{2}} \log N$$

pour $N \geq 2$, où la constante sous-entendue est absolue.

**Remarque.** En particulier

$$\frac{|\{f \in \mathbb{Z}[T],\ \deg(f) = r,\ |a_i| \leq N\ \forall 1 \leq i < r,\ f \text{ réductible}\}|}{|\{f \in \mathbb{Z}[T],\ \deg(f) = r,\ |a_i| \leq N\ \forall 1 \leq i < r\}|} = \frac{|E_r(N)|}{(2N+1)^r} \xrightarrow[N \to +\infty]{} 0.$$

La preuve repose sur le résultat suivant.

**Lemme.** Soit $f \in \mathbb{Z}[T]$ un polynôme unitaire réductible. Pour tout nombre premier $\ell$, la réduction $f$ mod $\ell$ est réductible dans $\mathbb{F}_\ell[T]$

À partir d'une minoration du cardinal de l'ensemble des polynômes unitaires irréductibles de degré $r$ de $\mathbb{F}_\ell[T]$, on obtient une majoration du cardinal de $E_r(N)$. C'est le principe du grand crible.

**Notations.** Pour un ensemble $X$, si $f$ et $g$ sont des applications définies sur $X$, on note $f \ll g$ ou $f = O(g)$ lorsqu'il existe une constante $C \geq 0$ telle que pour tout $x \in X$, $|f(x)| \leq Cg(x)$. On appellera "constante sous-entendue" toute valeur admissible de $C$.

Si $A$ est un anneau et $r \geq 1$ un entier, on note $A^{(r)}[T]$ l'ensemble des polynômes unitaires de degré $r$ à coefficients dans $A$.

# 1 Grand crible

Le formalisme que nous allons introduire est dû à Kowalski [9].

## 1.1 Cadre général

Dans cette partie, on expose le principe du grand crible dans un contexte très général.

On se donne un triplet $\Psi = (Y, \Lambda, (\rho_\ell)_{l\in\Lambda})$ où :
— $Y$ est un ensemble ;
— $\Lambda$ est un ensemble d'indices ;
— Pour tout $\ell \in \Lambda$, $\rho_\ell : Y \to Y_\ell$ est une application surjective de $Y$ sur un ensemble fini $Y_\ell$.

À ce triplet on associe $\Upsilon = (X, \mu, F)$ où :
— $(X, \mu)$ est un espace mesuré tel que $\mu(X) < +\infty$ ;
— $F : X \to Y$ est une application telle que les composées $\rho_\ell \circ F : X \to Y \to Y_l$ sont mesurables, *ie.*, les ensembles $\{x \in X,\ \rho_\ell(F_x) = y\}$ sont mesurables pour tout $\ell$ et tout $y \in Y_\ell$.

On écrira $|B|$ pour $\mu(B)$ si $B \subset X$ est un ensemble mesurable.

Enfin, on se donne un sous-ensemble $\mathcal{L}^*$ de $\Lambda$, appelé *support premier de crible*, et une famille $(\Omega_\ell)_{\ell\in\mathcal{L}^*}$ où $\Omega_\ell \subset Y_\ell$ pour $\ell \in \mathcal{L}^*$.

Le principe du grand crible est de majorer la mesure $|S(X, (\Omega_\ell), \mathcal{L}^*)|$ où

$$S(X, (\Omega_\ell), \mathcal{L}^*) = \{x \in X,\ \rho_\ell(F_x) \notin \Omega_\ell \text{ pour tout } \ell \in \mathcal{L}^*\}.$$

**Exemple 1.1.** Pour la démonstration du théorème de Gallagher pour les polynômes réductibles, on se placera dans le cadre

$$Y = \mathbb{Z}^{(r)}[T],\ \Lambda = \mathbb{P},\ Y_\ell = \mathbb{F}_\ell^{(r)}[T],\ \rho_l : \mathbb{Z}^{(r)}[T] \twoheadrightarrow \mathbb{F}_\ell^{(r)}[T]$$

$$X = \{(a_0, \dots, a_{r-1}),\ |a_i| \le N\ \forall 0 \le i < r\} \text{ et } F = X \to Y;$$

$$\mathcal{L}^* = \{\ell \in \mathbb{P},\ \ell \le L\} \text{ pour un entier } L \ge 2,\ \Omega_\ell = \{f \in \mathbb{F}_\ell^{(r)}[T] \text{ irréductible}\}.$$

## 1.2 Inégalité du grand crible

Avec les notations ci-dessus, on définit le *support de crible* $\mathcal{L}$ come un sous-ensemble de $\mathfrak{P}(\mathcal{L}^*)$.

Pour chaque $\ell \in \Lambda$, on suppose donnée une densité $\nu_\ell$ sur $Y_\ell$ :

$$\nu_\ell : Y_\ell \to ]0, 1]$$

qui pourra être notée $\nu$ lorsqu'il n'y a pas d'ambigüité possible. On suppose que $\nu_\ell$ est une mesure de probabilité :

$$\sum_{y\in Y_\ell} \nu_\ell(y) = 1.$$

On définit un produit scalaire sur l'ensemble $L^2(Y_\ell, \nu_\ell)$ (ou $L^2(Y_\ell)$) des fonctions $f : Y_\ell \to \mathbb{C}$ par

$$\forall f, g \in L^2(Y_\ell), \qquad \langle f, g \rangle = \sum_{y \in Y_\ell} \nu_\ell(y) f(y) \overline{g(y)}.$$

Muni de ce produit scalaire ($\nu > 0$), $L^2(Y_\ell)$ est un espace de Hilbert.

On note $S(\Lambda)$ l'ensemble des parties finies de $\Lambda$. Quand $\Lambda$ est l'ensemble des nombres premiers, $S(\Lambda)$ peut être vu comme l'ensemble des nombres sans facteur carré. Pour $m \in S(\Lambda)$, on écrit $\ell | m$ pour $\ell \in m$ (et de même pour $n \in S(\Lambda)$, $n | m$ pour $n \subset m$).

Pour $m \in S(\Lambda)$, on pose

$$Y_m = \prod_{\ell | m} Y_\ell$$

et $\rho_m : Y \to Y_m$ qui à $y \in Y$ associe $(\rho_\ell(y))_{\ell | m}$.

On peut aussi définir les densités $\nu_m$ et les produits scalaires correspondant :

$$\forall y = (y_\ell)_{\ell | m} \in Y_m, \qquad \nu_m(y) = \prod_{\ell | m} \nu_\ell(y_\ell)$$

et

$$\forall f, g \in L^2(Y_m), \qquad \langle f, g \rangle = \sum_{y \in Y_m} \nu_m(y) f(y) \overline{g(y)}.$$

En particulier, on a toujours

$$\sum_{y \in Y_m} \nu_m(y) = 1$$

et, si $f, g$ sont de la forme $f = \bigotimes_{\ell | m} f_\ell, g = \bigotimes_{\ell | m} g_\ell$,

$$\langle f, g \rangle = \prod_{\ell | m} \langle f_\ell, g_\ell \rangle.$$

On suppose donnée, pour chaque $\ell \in \Lambda$, une base orthonormale $\mathcal{B}_\ell$ de $L^2(Y_\ell, \nu_\ell)$ telle que la fonction constante 1 est un vecteur de la base. On pose $\mathcal{B}_\ell^* = \mathcal{B}_\ell \backslash \{1\}$, qui est une base orthonormée de $L_0^2(Y_\ell) = \{1\}^\perp$.

Pour $m \in S(\Lambda)$, on pose

$$\mathcal{B}_m = \prod_{\ell | m} \mathcal{B}_\ell, \qquad \mathcal{B}_m^* = \prod_{\ell | m} \mathcal{B}_\ell^*$$

où $\varphi \in \mathcal{B}_m$ s'écrit $\bigotimes_{\ell | m} \varphi_\ell$ avec $\varphi_\ell \in \mathcal{B}_\ell$.

$\mathcal{B}_m$ est une base orthonormale de $L^2(Y_m)$ et $\mathcal{B}_m^*$ est une base orthonormale de

$$L_0^2(Y_m) = \bigotimes_{\ell | m} L_0^2(Y_\ell).$$

On remarque que tous les espaces vectoriels définis ci-dessus sont de dimension fine.

On définit enfin l'opérateur

$$T : \begin{array}{rcl} L^2(X,\mu) & \to & \bigoplus_{m\in\mathcal{L}} L_0^2(Y_m)' \\ \alpha & \mapsto & \left(f \mapsto \int_X \alpha(x) f(\rho_m(F_x))\mathrm{d}\mu(x)\right)_m \end{array}$$

où $\mathcal{L} \subset \mathfrak{P}(\mathcal{L}^*)$ est un support de crible, la somme directe sur $m$ est orthogonale et $L_0^2(Y_m)'$ est l'espace des formes linéaires sur $L_0^2(Y_m)$.

**Proposition 1.2**

*Pour tout support de crible $\mathcal{L} \subset \mathfrak{P}(\mathcal{L}^*)$, $T$ est une application linéaire continue. On note $\Delta = \|T\|^2$. Alors $\Delta = \Delta(X,\mathcal{L})$ est la plus petite constante positive telle que*

$$\sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} \left| \int_X \alpha(x)\varphi(\rho_m(F_x))d\mu(x)\right|^2 \leq \Delta \int_X |\alpha(x)|^2 d\mu(x)$$

*pour toute fonction de carré intégrable $\alpha : X \to \mathbb{C}$.*

*De plus, pour toute famille $(\Omega_\ell)_{\ell\in\mathcal{L}^*}$,*

$$|S(X,(\Omega_\ell),\mathcal{L}^*)| \leq \Delta H^{-1} \qquad \textit{(inégalité du grand crible)}$$

*où*

$$H = \sum_{m\in\mathcal{L}} \prod_{\ell|m} \frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}.$$

Soient $\alpha \in L^2(X,\mu)$ et $m \in \mathcal{L}$. Soit $U_m$ la forme linéaire définie par

$$\forall f \in L_0^2(Y_m), \qquad U_m(f) = \int_X \alpha(x) f(\rho_m(F_x))\mathrm{d}\mu(x).$$

$U_m$ est linéaire. Calculons sa norme. Soit $f \in L_0^2(Y_m)$. En décomposant $f$ dans la base $\mathcal{B}_m^*$, on obtient

$$\begin{aligned} \left|\int_X \alpha(x) f(\rho_m(F_x))\mathrm{d}\mu(x)\right| &= \left|\sum_{\varphi\in\mathcal{B}_m^*} \langle f,\varphi\rangle \int_X \alpha(x)\varphi(\rho_m(F_x))\mathrm{d}\mu(x)\right| \\ &\leq \sum_{\varphi\in\mathcal{B}_m^*} |\langle f,\varphi\rangle| \left|\int_X \alpha(x)\varphi(\rho_m(F_x))\mathrm{d}\mu(x)\right| \end{aligned}$$

donc, par l'inégalité de Cauchy-Schwarz,

$$\left|\int_X \alpha(x) f(\rho_m(F_x))\mathrm{d}\mu(x)\right| \leq \left(\sum_{\varphi\in\mathcal{B}_m^*} |\langle f,\varphi\rangle|^2\right)^{1/2} \left(\sum_{\varphi\in\mathcal{B}_m^*} \left|\int_X \alpha(x)\varphi(\rho_m(F_x))\mathrm{d}\mu(x)\right|^2\right)^{1/2}$$

soit

$$|U_m(f)| \leq \left( \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 \right)^{1/2} \|f\|_{L_0^2(Y_m)} .$$

Considérons la fonction $f$ égale à la projection sur $L_0^2(Y_m)$ de la fonction

$$y \in Y_m \mapsto \frac{1}{\nu_m(y)} \overline{\int_{\rho_m(F_x)=y} \alpha(x) \mathrm{d}\mu(x)}$$

définie de sorte que

$$\int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) = \overline{\langle f, \varphi \rangle}.$$

Ainsi,

$$\begin{aligned} U_m(f) &= \left| \sum_{\varphi \in \mathcal{B}_m^*} \langle f, \varphi \rangle \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right| \\ &= \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 \\ &= \left( \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 \right)^{1/2} \|f\|_{L_0^2(Y_m)} . \end{aligned}$$

On a donc montré que

$$\|U_m\|^2_{L_0^2(Y_m)'} = \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 .$$

Or $T$ est linéaire et

$$\begin{aligned} \|T(\alpha)\|^2_{\bigoplus_{m \in \mathcal{L}} L_0^2(Y_m)'} &= \sum_{m \in \mathcal{L}} \|U_m\|_{L_0^2(Y_m)'} = \sum_{m \in \mathcal{L}} \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 . \\ &\leq \sum_{m \in \mathcal{L}} \sum_{\varphi \in \mathcal{B}_m^*} \left( \int_X |\alpha(x) \varphi(\rho_m(F_x))| \, \mathrm{d}\mu(x) \right)^2 \\ &\leq \left( \sum_{m \in \mathcal{L}} \sum_{\varphi \in \mathcal{B}_m^*} \int_X |\varphi(\rho_m(F_x))|^2 \mathrm{d}\mu(x) \right) \int_X |\alpha(x)|^2 \mathrm{d}\mu(x) \end{aligned}$$

donc $T$ est continue et $\Delta$ est la plus petite constante vérifiant

$$\sum_{m \in \mathcal{L}} \sum_{\varphi \in \mathcal{B}_m^*} \left| \int_X \alpha(x) \varphi(\rho_m(F_x)) \mathrm{d}\mu(x) \right|^2 \leq \Delta \int_X |\alpha(x)|^2 \mathrm{d}\mu(x)$$

Pour prouver l'inégalité du grand crible, on énonce deux lemmes. Pour $m \in S(\Lambda)$, $y \in Y_m$, $\varphi \in \mathcal{B}_m$ et $\alpha \in L^2(X,\mu)$, on définit

$$S(m,y) = \int_{\{\rho_m(F_x)=y} \alpha(x)\mathrm{d}\mu(x)$$

(bien défini car $\mu(X) < +\infty$ par hypothèse) et

$$S(\varphi) = \int_X \alpha(x)\varphi(\rho_m(F_x))\mathrm{d}\mu(x),$$

**Lemme 1.3**

*Pour tout $\ell \in \Lambda$,*

$$\sum_{\varphi\in\mathcal{B}_\ell^*} |S(\varphi)|^2 = \sum_{y\in Y_\ell} \frac{|S(\ell,y)|^2}{\nu(y)} - \left|\int_X \alpha(x)d\mu(x)\right|^2.$$

▷ Par le théorème de Fubini,

$$\sum_{\varphi\in\mathcal{B}_\ell^*} |S(\varphi)|^2 = \int_X\int_X \alpha(x)\overline{\alpha(y)} \sum_{\varphi\in\mathcal{B}_\ell^*} \varphi(\rho_\ell(F_x))\overline{\varphi(\rho_\ell(F_y))}\mathrm{d}\mu(x)\mathrm{d}\mu(y).$$

En notant $\delta$ le symbole de Kronecker, pour $y \in Y_\ell$, on peut écrire $\delta(y,\cdot)$ dans la base $\mathcal{B}_\ell$ :

$$\forall z \in Y_\ell, \qquad \delta(y,z) = \sum_{\varphi\in\mathcal{B}_\ell} \langle\delta(y,\cdot),\varphi\rangle\varphi(z) = \sum_{\varphi\in\mathcal{B}_\ell} \nu(y)\overline{\varphi(y)}\varphi(z).$$

Donc, en conjuguant,

$$\sum_{\varphi\in\mathcal{B}_\ell} \varphi(y)\overline{\varphi(z)} = \frac{1}{\nu(y)}\delta(y,z).$$

Ainsi,

$$\sum_{\varphi\in\mathcal{B}_\ell^*} \varphi(\rho_\ell(F_x))\overline{\varphi(\rho_\ell(F_y))} = \frac{1}{\nu(\rho_\ell(F_x))}\delta(\rho_\ell(F_x),\rho_\ell(F_y)) - 1$$

donc

$$\begin{aligned}
\sum_{\varphi\in\mathcal{B}_\ell^*} |S(\varphi)|^2 &= \iint_{\{\rho_\ell(F_x)=\rho_\ell(F_y)\}} \frac{\alpha(x)\overline{\alpha(y)}}{\nu(\rho_\ell(F_x))}\mathrm{d}\mu(x)\mathrm{d}\mu(y) - \iint_{X\times X} \alpha(x)\overline{\alpha(y)}\mathrm{d}\mu(x)\mathrm{d}\mu(y) \\
&= \sum_{z\in Y_\ell} \frac{1}{\nu(z)} \iint_{\{\rho_\ell(F_x)=z=\rho_\ell(F_y)\}} \alpha(x)\overline{\alpha(y)}\mathrm{d}\mu(x)\mathrm{d}\mu(y) - \left|\int_X \alpha(x)\mathrm{d}\mu(x)\right|^2 \\
&= \sum_{z\in Y_\ell} \frac{|S(\ell,z)|^2}{\nu(z)} - \left|\int_X \alpha(x)\mathrm{d}\mu(x)\right|^2.
\end{aligned}$$

□

**Lemme 1.4**

*Pour toute fonction $\alpha \in L^2(X,\mu)$ à support inclus dans $S(X,\Omega,\mathcal{L}^*)$ et pour tout $m \subset \mathcal{L}^*$,*

$$\sum_{\varphi\in\mathcal{B}_m^*} |S(\varphi)|^2 \geq \left|\int_X \alpha(x)d\mu(x)\right|^2 \prod_{\ell|m} \frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}$$

▷ On montre le résultat par récurrence forte sur le cardinal de $m$.

– Pour $m = \varnothing$, par convention, $Y_m$ contient un seul élément, $\rho_m$ est une application constante, $\mathcal{B}_m = \mathcal{B}_m^* = \{1\}$ et le résultat est vrai.

– Pour $m = \{\ell\}$, comme $m \subset \mathcal{L}^*$, $\ell \in \mathcal{L}^*$ et en utilisant la restriction sur le support de $\alpha$ et l'inégalité de Cauchy-Schwarz on obtient :

$$\begin{aligned}\left|\int_X \alpha(x)\mathrm{d}\mu(x)\right|^2 &= \left|\sum_{\substack{y\in Y_\ell\\ y\notin\Omega_\ell}} S(\ell,y)\right|^2 \leq \left(\sum_{y\notin\Omega_\ell}\nu(y)\right)\left(\sum_{y\in Y_\ell}\frac{|S(\ell,y)|^2}{\nu(y)}\right)\\ &\leq \nu(Y_\ell\backslash\Omega_\ell)\sum_{y\in Y_\ell}\left(\sum_{\varphi\in\mathcal{B}_\ell^*}|S(\varphi)|^2 + \left|\int_X\alpha(x)\mathrm{d}\mu(x)\right|^2\right)\end{aligned}$$

d'après le lemme précédent. En regroupant les termes, il vient

$$\left|\int_X \alpha(x)\mathrm{d}\mu(x)\right|^2 (1-\nu(Y_\ell\backslash\Omega_\ell)) \leq \nu(Y_\ell\backslash\Omega_\ell)\sum_{\varphi\in\mathcal{B}_\ell^*}|S(\varphi)|^2$$

d'où, comme $\nu(Y_\ell) = 1$,

$$\sum_{\varphi\in\mathcal{B}_\ell^*}|S(\varphi)|^2 \geq \left|\int_X\alpha(x)\mathrm{d}\mu(x)\right|^2 \frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}.$$

– Soit $m \subset \mathcal{L}^*$, $m$ n'étant pas un singleton. Écrivons $m = m_1m_2 = m_1 \cup m_2$ avec $m_1$ et $m_2$ non vides (et toujours des sous-ensembles de $\mathcal{L}^*$). Alors

$$\sum_{\varphi\in\mathcal{B}_{m_1m_2}^*}|S(\varphi)|^2 = \sum_{\varphi_1\in\mathcal{B}_{m_1}^*}\sum_{\varphi_2\in\mathcal{B}_{m_2}^*}|S(\varphi_1\otimes\varphi_2)|^2$$

où $\varphi_1\otimes\varphi_2 : (y,z)\mapsto\varphi_1(y)\varphi_2(z)$. On peut écrire

$$S(\varphi_1\otimes\varphi_2) = \int_X \beta(x)\varphi_2(\rho_{m_2}(F_x))\mathrm{d}\mu(x)$$

avec $\beta(x) = \alpha(x)\varphi_1(\rho_{m_1}(F_x))$, qui est également à support inclus dans $S(X,\Omega,\mathcal{L}^*)$. On

peut donc appliquer l'hypothèse de récurrence, d'abord à $m_2$, puis à $m_1$ :

$$\begin{aligned}\sum_{\varphi\in\mathcal{B}^*_{m_1m_2}}|S(\varphi)|^2 &\geq \prod_{\ell|m_2}\frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}\sum_{\varphi_1\in\mathcal{B}^*_{m_1}}\left|\int_X\beta(x)\mathrm{d}\mu(x)\right|^2\\ &\geq \prod_{\ell|m_2}\frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}\sum_{\varphi_1\in\mathcal{B}^*_{m_1}}|S(\varphi_1)|^2\\ &\geq \prod_{\ell|m_1m_2}\frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}\left|\int_X\alpha(x)\mathrm{d}\mu(x)\right|^2.\end{aligned}$$

□

On peut désormais démontrer l'inégalité du grand crible. Considérons $\alpha$ la fonction caractéristique de $S(X,\Omega,\mathcal{L}^*)$. En appliquant le dernier lemme et en sommant les inégalités sur $m\in\mathcal{L}$, on obtient

$$|S(X,\Omega,\mathcal{L}^*)|^2\sum_{m\in\mathcal{L}}\prod_{\ell|m}\frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)}\leq\sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m}|S(\varphi)|^2=\sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m}\left|\int_X\alpha(x)\varphi(\rho_m(F_x))\mathrm{d}\mu(x)\right|^2$$

donc, par définition de $\Delta$,

$$|S(X,\Omega,\mathcal{L}^*)|^2H\leq\Delta|S(X,\Omega,\mathcal{L}^*)|,$$

d'où le résultat.

### 1.3 Majoration de $\Delta$ par dualité

On utilise la dualité pour caractériser $\Delta$. En effet, comme $\Delta$ est le carré de la norme d'un opérateur, c'est aussi le carré de la norme de son adjoint.

**Proposition 1.5**

*Pour tout support de crible $L\subset\mathfrak{P}(L^*)$, $\Delta=\Delta(X,\mathcal{L})$ est la plus petite constante positive telle que*

$$\int_X\left|\sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m}\beta(m,\varphi)\varphi(\rho_m(F_x))\right|^2d\mu(x)\leq\Delta\sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m}|\beta(m,\varphi)|^2$$

*pour toute famille $(\beta(m,\varphi))_{m,\varphi}$.*

▷ On calcule, pour $f\in\left(\bigoplus_{m\in\mathcal{L}}L^2_0(Y_m)'\right)'$, $\left\|{}^tT(f)\right\|=\|f\circ T\|$. On introduit l'isomorphisme canonique

$$\begin{aligned}J:\ \bigoplus_{m\in\mathcal{L}}L^2_0(Y_m) &\to \left(\bigoplus_{m\in\mathcal{L}}L^2_0(Y_m)'\right)'\\ g &\mapsto (\psi\mapsto\psi(g)).\end{aligned}$$

Soit $f \in \left(\bigoplus_{m\in\mathcal{L}} L_0^2(Y_m)'\right)'$. Soit $g \in \bigoplus_{m\in\mathcal{L}} L_0^2(Y_m)$ tel que $f = J(g)$. Alors, pour $\alpha \in L^2(X,\mu)$ et en écrivant $g = \sum_{m\in\mathcal{L}} g_m$,

$$^tT(f)(\alpha) = (f\circ T)(\alpha) = J(g)(T(\alpha)) = T(\alpha)(g) = \sum_{m\in\mathcal{L}} \int_X \alpha(x) g(\rho_m(F_x))\mathrm{d}\mu(x)$$

donc

$$\left\|{}^tT(f)\right\|^2 = \left\|\alpha \mapsto \sum_{m\in\mathcal{L}} \int_X \alpha(x) g_m(\rho_m(F_x))\mathrm{d}\mu(x)\right\|^2.$$

Or,

$$\left|\int_X \alpha(x) \sum_{m\in\mathcal{L}} g_m(\rho_m(F_x))\mathrm{d}\mu(x)\right| \leq \|\alpha\|_{L^2} \left\|\sum_{m\in\mathcal{L}} g_m\circ\rho_m\circ F\right\|_{L^2}$$

et avec $\alpha = \overline{\sum_{m\in\mathcal{L}} g_m\circ\rho_m\circ F}$ on en déduit que

$$\left\|{}^tT(f)\right\|^2 = \int_X \left|\sum_{m\in\mathcal{L}} g_m(\rho_m(F_x))\right|^2 \mathrm{d}\mu(x).$$

En écrivant $g_m$ dans la base $(\varphi)_{\varphi\in\mathcal{B}_m^*}$ de $L_0^2(Y_m)$ comme

$$g_m = \sum_{\varphi\in\mathcal{B}_m^*} \beta(m,\varphi)\varphi$$

on obtient

$$\left\|{}^tT(f)\right\|^2 = \int_X \left|\sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} \beta(m,\varphi)\varphi(\rho_m(F_x))\right|^2 \mathrm{d}\mu(x)$$

d'où le résultat. □

Pour $\varphi \in \mathcal{B}_m$ et $\varphi' \in \mathcal{B}_n$ on pose

$$W(\varphi,\varphi') = \int_X \varphi(\rho_m(F_x))\overline{\varphi'(\rho_n(F_x))}\mathrm{d}\mu(x).$$

Alors, la proposition 1.5 permet de majorer $\Delta$.

**Proposition 1.6**

*La constante $\Delta$ du grand crible vérifie*

$$\Delta \leq \max_{m\in\mathcal{L}} \max_{\varphi\in\mathcal{B}_m^*} \sum_{n\in\mathcal{L}} \sum_{\varphi'\in\mathcal{B}_n^*} |W(\varphi,\varphi')|.$$

▷ Soit $(\beta(m,\varphi))_{\substack{m\in\mathcal{L}\\ \varphi\in\mathcal{B}_m^*}}$ une famille de complexes. On a

$$0 \leq \int_X \left| \sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} \beta(m,\varphi)\varphi(\rho_m(F_x)) \right|^2 \mathrm{d}\mu(x) = \sum_{m,n\in\mathcal{L}} \sum_{\varphi,\varphi'} \beta(m,\varphi)\overline{\beta(n,\varphi')}W(\varphi,\varphi')$$

donc on peut majorer ceci par

$$\sum_{m,n\in\mathcal{L}} \sum_{\varphi,\varphi'} |\beta(m,\varphi)\overline{\beta(n,\varphi')}W(\varphi,\varphi')| \leq \sum_{m,n\in\mathcal{L}} \sum_{\varphi,\varphi'} \frac{1}{2}\left(|\beta(m,\varphi)|^2 + |\beta(n,\varphi')|^2\right)|W(\varphi,\varphi')|$$

ce qui est inférieur à

$$\frac{1}{2}\left( \sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} |\beta(m,\varphi)|^2 \sum_{n\in\mathcal{L}} \sum_{\varphi'\in\mathcal{B}_n^*} |W(\varphi,\varphi')| + \sum_{n\in\mathcal{L}} \sum_{\varphi'\in\mathcal{B}_n^*} |\beta(n,\varphi')|^2 \sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} |W(\varphi,\varphi')| \right)$$

ce qui est inférieur à

$$\frac{1}{2}\left( \sum_{m,\varphi} |\beta(m,\varphi)|^2 \right) \max_{m,\varphi} \sum_{n,\varphi'} |W(\varphi,\varphi')| + \frac{1}{2}\left( \sum_{n,\varphi'} |\beta(n,\varphi')|^2 \right) \max_{n,\varphi'} \sum_{m,\varphi} |W(\varphi,\varphi')|.$$

Or $W(\varphi,\varphi') = \overline{W(\varphi',\varphi)}$ donc

$$\max_{m,\varphi} \sum_{n,\varphi'} |W(\varphi,\varphi')| = \max_{n,\varphi'} \sum_{m,\varphi} |W(\varphi,\varphi')|$$

donc finalement on majore par

$$\left( \max_{m\in\mathcal{L}} \max_{\varphi\in\mathcal{B}_m^*} \sum_{n\in\mathcal{L}} \sum_{\varphi'\in\mathcal{B}_n^*} |W(\varphi,\varphi')| \right) \left( \sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} |\beta(m,\varphi)|^2 \right)$$

d'où le résultat. □

On obtient ainsi une majoration de $\Delta$ en estimant les sommes $W(\varphi,\varphi')$ uniformément. Ici, le choix de la base orthonormée peut avoir une influence sur cette estimation et donc sur le $\Delta$ "choisi".

## 1.4 Application : une inégalité de grand crible

À partir de la définition de $\Delta$ donnée par la proposition 1.5, on peut obtenir des inégalités du type suivant.

**Proposition 1.7**

*Soient $(Y,\Lambda,(\rho_\ell))$, $(X,\mu,F)$ et $\mathcal{L}^*$. Soit $\Delta$ la constante de grand crible $\mathcal{L}=\mathcal{L}^*$ ($\mathcal{L}=$*

$\{\{\ell\}, \ell \in \mathcal{L}^*\}$). *Pour tout* $(\Omega_\ell)$ *on a*

$$\int_X (P(x,\mathcal{L}) - P(\mathcal{L}))^2 d\mu(x) \leq \Delta Q(\mathcal{L})$$

*où*

$$P(x,\mathcal{L}) = \sum_{\substack{\ell\in\mathcal{L} \\ \rho_\ell(F_x)\in\Omega_\ell}} 1, \qquad P(\mathcal{L}) = \sum_{\ell\in\mathcal{L}} \nu(\Omega_\ell),$$

$$Q(\mathcal{L}) = \sum_{\ell\in\mathcal{L}} \nu(\Omega_\ell)(1-\nu(\Omega_\ell)).$$

▷ On développe la fonction caractéristique $\chi_\ell$ de $\Omega_\ell \subset Y_\ell$ dans la base orthonormée $\mathcal{B}_\ell$ et on obtient :

$$\begin{aligned}
P(x,\mathcal{L}) &= \sum_{\ell\in\mathcal{L}} \chi_{\Omega_\ell}(\rho_\ell(F_x)) \\
&= \sum_{\ell\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_\ell} \langle \chi_{\Omega_\ell}, \varphi\rangle \varphi(\rho_\ell(F_x)) \\
&= \sum_{\ell\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_\ell} \sum_{y\in Y_\ell} \nu_\ell(y)\chi_{\Omega_\ell}(y)\overline{\varphi(y)}\varphi(\rho_\ell(F_x)) \\
&= \underbrace{\sum_{\ell\in\mathcal{L}} \sum_{y\in Y_\ell} \nu_\ell(y)\chi_{\Omega_\ell}(y)}_{P(\mathcal{L})} + \sum_{\ell\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_\ell^*} \beta(\ell,\varphi)\varphi(\rho_\ell(F_x))
\end{aligned}$$

où

$$\beta(\ell,\varphi) = \sum_{y\in\Omega_\ell} \nu_\ell(y)\overline{\varphi(y)}$$

Ainsi,

$$\int_X (P(x,\mathcal{L}) - P(\mathcal{L}))^2 \mathrm{d}\mu(x) = \int_X \left| \sum_{\ell\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_\ell^*} \beta(\ell,\varphi)\varphi(\rho_\ell(F_x)) \right|^2 \mathrm{d}\mu(x) \leq \Delta \sum_{\ell\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_\ell^*} |\beta(\ell,\varphi)|^2$$

d'après la proposition 1.5.

Or

$$\sum_{\varphi\in\mathcal{B}_\ell^*} |\beta(\ell,\varphi)|^2 = \sum_{\varphi\in\mathcal{B}_\ell} |\beta(\ell,\varphi)|^2 - |\beta(\ell,1)|^2 = \langle \chi_\ell, \chi_\ell\rangle - \nu(\Omega_\ell)^2 = \nu(\Omega_\ell)(1-\nu(\Omega_\ell))$$

d'où le résultat. □

En particulier, on en déduit, comme $P(x,\mathcal{L}) = 0$ pour $x \in S(X,(\Omega_\ell),\mathcal{L}^*)$ et $Q(\mathcal{L}) \leq P(\mathcal{L})$,

$$\Delta P(\mathcal{L}) \geq \Delta Q(\mathcal{L}) \geq \int_X (P(x,\mathcal{L}) - P(\mathcal{L}))^2 \geq P(\mathcal{L})^2 |S(X,(\Omega_\ell),\mathcal{L}^*)|$$

d'où

$$|S(X,(\Omega_\ell),\mathcal{L}^*)| \leq \Delta P(\mathcal{L})^{-1}.$$

On pouvait déduire ce résultat directement de la proposition 1.2. En effet, on a

$$|S(X,(\Omega_\ell),\mathcal{L}^*)| \leq \Delta H^{-1}$$

où

$$H = \sum_{\ell\in\mathcal{L}} \frac{\nu(\Omega_\ell)}{\nu(Y_\ell\backslash\Omega_\ell)} \geq \sum_{\ell\in\mathcal{L}} \nu(\Omega_\ell) = P(\mathcal{L}).$$

C'est ce résultat que l'on va utiliser pour démontrer le théorème de Gallagher. Dans sa démonstration publiée en 1973 [3], il se place dans le cadre

$$Y = \mathbb{Z}^r, \qquad , \Lambda = \mathbb{P}, \qquad Y_\ell = \mathbb{F}_\ell^r, \qquad \rho_\ell : \mathbb{Z}^r \twoheadrightarrow \mathbb{F}_\ell^r$$

$$X = \{a \in \mathbb{Z}^r,\ |a| \leq N\}, \qquad F = \mathrm{Id}_X$$

$$\mathcal{L}^* = \{\ell \in \mathbb{P}, \ell \leq L\}, \qquad \mathcal{L} = \{\{\ell\}, \ell \in \mathcal{L}^*\}.$$

**Proposition 1.8**

*Pour $\ell$ premier, soit $\Omega_\ell$ un sous-ensemble de $\mathbb{F}_\ell^r$. On a*

$$\sum_{\substack{a\in\mathbb{Z}^r \\ |a|\leq N}} (P(a,L) - P(L))^2 \leq (\sqrt{2N}+L)^{2r} P(L)$$

*où $P(a,L) = P(a,\mathcal{L})$ et $P(L) = P(\mathcal{L})$ avec les notations précédentes.*

▷ On donne la preuve présentée par Gallagher.
On note $\chi_\ell$ la fonction caractéristique de l'ensemble $\{a \in \mathbb{Z}^r, a \bmod \ell \in \Omega_\ell\}$.
Les caractères du groupe $(\mathbb{Z}/\ell\mathbb{Z})^r$ sont les $e_\ell(\alpha\cdot.)$, $\alpha \in (\mathbb{Z}/\ell\mathbb{Z})^r$ :

$$\forall x \in (\mathbb{Z}/\ell\mathbb{Z})^r, \qquad e_\ell(\alpha\cdot x) = \exp\left(\frac{2i\pi\alpha\cdot x}{\ell}\right).$$

Les caractères formant une base orthonormée de $L^2((\mathbb{F}_\ell)^r)$, on peut décomposer $\chi_\ell$ dans cette base. Comme $\chi_\ell$ est $\ell\mathbb{Z}^r$ périodique, on peut l'identifier une fonction définie sur $(\mathbb{F}_\ell)^r$ :

$$\begin{aligned}\forall x \in (\mathbb{F}_\ell)^r,\ \chi_\ell(x) &= \sum_{\alpha\in(\mathbb{F}_\ell)^r} \langle \chi, e_\ell(\alpha\cdot.)\rangle e_\ell(\alpha\cdot x) \\ &= \sum_{\alpha\in(\mathbb{F}_\ell)^r} \frac{1}{\ell^r} \sum_{\beta\in(\mathbb{F}_\ell)^r} \chi_\ell(\beta) e_\ell(-\alpha\cdot\beta) e_\ell(\alpha\cdot x)\end{aligned}$$

Ainsi,

$$P(a,L) = \sum_{\ell\leq L} \chi_\ell(a) = P(L) + R(a,L)$$

où

$$R(a,L) = \sum_{\ell\leq L} \sum_{\alpha\in(\mathbb{F}_\ell^\times)^r} \underbrace{\langle \chi_\ell, e_\ell(\alpha\cdot.)\rangle}_{c_\ell(\alpha)} e_\ell(\alpha\cdot a).$$

On écrit

$$\sum_{|a|\leq N}(R(a,L))^2 = \sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r} c_\ell(\alpha)\sum_{|a|\leq N} R(a,L)e_\ell(\alpha\cdot a).$$

$$\leq \left(\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|c_\ell(\alpha)|^2\right)^{1/2}\left(\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|S(\alpha)|^2\right)^{1/2}$$

où

$$S(\alpha)=\sum_{|a|\leq N}R(a,L)e_\ell(\alpha\cdot a).$$

Or

$$\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|c_\ell(\alpha)|^2=\|\chi_\ell\|^2=\frac{|\Omega_\ell|}{\ell^n}$$

donc

$$\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|c_\ell(\alpha)|^2=P(L).$$

Alors, en admettant provisoirement que

$$\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|S(\alpha)|^2\leq(\sqrt{2N}+L)^{2r}\sum_{|a|\leq N}|R(a,L)|^2,$$

on a montré que

$$\sum_{|a|\leq N}(P(a,L)-P(L))^2=\sum_{|a|\leq N}(R(a,L))^2\leq\left(P(L)(\sqrt{2N}+L)^{2r}\sum_{|a|\leq N}(R(a,L))^2\right)^{1/2}$$

d'où le résultat. □

Démontrons l'inégalité admise ci-dessus. Nous aurons besoin du résultat suivant, dont la démonstration est due à Huxley [6] :

**Théorème 1.9**

*Pour tout vecteur $x=(x_1,\dots,x_r)\in\mathbb{R}^r$ on pose*

$$S(x)=\sum_{|n_1|\leq N_1}\dots\sum_{|n_r|\leq N_r}c(n_1,\dots,n_r)e(n_1x_1+\dots+n_rx_r).$$

*Soient $x^{(1)},\dots,x^{(K)}\in\mathbb{R}^r$ vérifiant*

$$\max_{1\leq j\leq r}\delta_j^{-1}\left\|x_j^{(k)}-x_j^{(k')}\right\|\geq 1$$

*pour $k \neq k'$, où $\delta_1, \dots, \delta_r$ sont des constantes positives inférieures à $\frac{1}{2}$ et $\|\alpha\| = d(\alpha, \mathbb{Z})$. Alors,*

$$\sum_{k=1}^{K} |S(x^{(k)})|^2 \leq B_1 \dots B_k \sum_{|n_1| \leq N_1} \dots \sum_{|n_r| \leq N_r} |c(n_1, \dots, n_r)|^2$$

*où, pour $1 \leq j \leq r$,*

$$B_j = (\sqrt{2N_j} + \delta_j^{-1/2})^2.$$

▷ Pour $1 \leq j \leq r$, on définit une fonction de carré intégrable $\psi^{(j)}$ nulle pour $\|x\| > \frac{1}{2}\delta_j$ par :

$$\psi^{(j)}(x) = \sum_{n=-\infty}^{+\infty} d_n^{(j)} e(nx)$$

où pour tout $n \in \mathbb{Z}$, $d_{-n}^{(j)} = d_n^{(j)}$.

Pour $x \in \mathbb{R}^r$ posons

$$T(x) = \sum_{|n_1| \leq N_1} \dots \sum_{|n_r| \leq N_r} \frac{c(n_1, \dots, n_r)}{d_{n_1}^{(1)} \dots d_{n_r}^{(r)}} e(n_1 x_1 + \dots + n_k n_r).$$

Alors, par un produit de Cauchy, on vérifie que

$$S(x) = \int_0^1 \dots \int_0^1 T(x - y)\psi^{(1)}(y_1) \dots \psi^{(r)}(y_r) \mathrm{d}y_1 \dots \mathrm{d}y_r.$$

Par l'inégalité de Cauchy-Schwarz,

$$\begin{aligned} |S(x)|^2 &\leq \Psi \int_{-\frac{\delta_1}{2}}^{\frac{\delta_1}{2}} \dots \int_{-\frac{\delta_r}{2}}^{\frac{\delta_r}{2}} |T(x - y)|^2 \mathrm{d}y_1 \dots \mathrm{d}y_r \\ &\leq \Psi \int_{x_1 - \frac{\delta_1}{2}}^{x_1 + \frac{\delta_1}{2}} \dots \int_{x_r - \frac{\delta_r}{2}}^{x_r + \frac{\delta_r}{2}} |T(z)|^2 \mathrm{d}z_1 \dots \mathrm{d}z_r \end{aligned}$$

où

$$\Psi = \prod_{j=1}^{r} \int_{-\frac{\delta_j}{2}}^{\frac{\delta_j}{2}} |\psi^{(j)}(y)|^2 \mathrm{d}y.$$

On en déduit que

$$\sum_{k=1}^{K} |S(x^{(k)})|^2 \leq \Psi \int_{\Omega} |T(z)|^2 \mathrm{d}z_1 \dots \mathrm{d}z_r$$

où

$$\Omega = \bigcup_{k=1}^{K} \prod_{j=1}^{r} \left] x_j^{(k)} - \frac{\delta_j}{2}, x_j^{(k)} + \frac{\delta_j}{2} \right[.$$

Modulo 1, ces pavés sont disjoints par hypothèse donc $\Omega$ peut être remplacé par le cube $]0,1[^r$ ce qui donne

$$\begin{aligned}\sum_{k=1}^{K}|S(x^{(k)})|^2 &\leq \Psi \sum_{|n_1|\leq N_1}\cdots\sum_{|n_r|\leq N_r}\left|\frac{c(n_1,\ldots,n_r)}{d_{n_1}^{(1)}\ldots d_{n_r}^{(r)}}\right|^2\\ &\leq \Psi D_1^{-2}\ldots D_r^{-2}\sum_{|n_1|\leq N_1}\cdots\sum_{|n_r|\leq N_r}|c(n_1,\ldots,n_r)|^2\end{aligned}$$

où

$$D_j=\min_{|n|\leq N_j}|d_n^{(j)}|.$$

Bombieri et Davenport [1], en démontrant ce théorème en dimension 1, on construit, pour tout $N$ et $\delta$ donnés, une fonction $\psi$ telle que

$$\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}}|\psi(x)|^2\mathrm{d}x\leq(\sqrt{2N}+\delta^{-1/2})^2\min_{|n|\leq N}|d_n|^2$$

donc en utilisant cette fonction avec $N_j$ et $\delta_j$, on obtient

$$\Psi\leq B_1\ldots B_rD_1^2\ldots D_2^2,$$

ce qui conclut la preuve. □

On souhaite désormais majorer

$$\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|S(\alpha)|^2$$

où

$$S(\alpha)=\sum_{|a|\leq N}R(a,L)e_\ell(\alpha\cdot a)=\sum_{|a_1|,\ldots,|a_r|\leq N}R(a,L)e\left(\frac{\alpha_1a_1+\cdots+\alpha_ra_r}{\ell}\right).$$

On va appliquer le théorème précédent à la famille

$$(x^{(\ell,\alpha)})=\left(\frac{\alpha_1}{\ell},\ldots,\frac{\alpha_r}{\ell}\right)$$

où $\ell\leq L$ et $\alpha=(\alpha_1,\ldots,\alpha_r)\in(\mathbb{F}_\ell^\times)^r$.

Pour $\ell,\ell'\leq L$ premiers, $(\alpha,\alpha')\in(\mathbb{F}_\ell^\times)^r\times(\mathbb{F}_{\ell'}^\times)^r$, $(\ell,\alpha)\neq(\ell',\alpha')$, on a

$$\max_{0\leq j\leq r}\left\|\frac{\alpha_j}{\ell}-\frac{\alpha_j'}{\ell}\right\|\geq\frac{1}{\ell\ell'}\geq\frac{1}{L^2}$$

donc en posant, pour tout $j$, $\delta_j=\frac{1}{L^2}$, on a, pour $\ell,\ell'\leq L$ premiers, $(\alpha,\alpha')\in(\mathbb{F}_\ell^\times)^r\times(\mathbb{F}_{\ell'}^\times)^r$, $(\ell,\alpha)\neq(\ell',\alpha')$

$$\max_{1\leq j\leq r}\delta_j^{-1}\left\|x_j^{\ell,\alpha}-x_j^{\ell',\alpha'}\right\|\geq 1.$$

Le théorème précédent permet de conclure que

$$\sum_{\ell\leq L}\sum_{\alpha\in(\mathbb{F}_\ell^\times)^r}|S(\alpha)|^2\leq(\sqrt{2N}+L)^{2r}\sum_{|a|\leq N}|R(a,L)|^2.$$

# 2 Théorème de Gallagher pour les polynômes réductibles

## 2.1 Énoncé

On a désormais l'outil essentiel pour démontrer le résultat énoncé en introduction :

**Théorème 2.1**

*Soit $r \geq 1$ un entier. Pour tout entier $N \geq 1$, définissons $E_r(N)$ comme l'ensemble des polynômes $f \in \mathbb{Z}[T]$ unitaires réductibles de degré $r$ tels que*

$$f = T^r + a_{r-1}T^{r-1} + \cdots + a_1 T + a_0$$

*où $|a_i| \leq N$ pour tout $0 \leq i < r$. Alors,*

$$|E_r(N)| \ll r^2(2N+1)^{r-\frac{1}{2}} \log N$$

*pour $N \geq 2$, où la constante sous-entendue est absolue.*

On suit la preuve de Kowalski [9]. On pose

$$Y = \mathbb{Z}^{(r)}[T],\ \Lambda = \mathbb{P},\ Y_\ell = \mathbb{F}_\ell^{(r)}[T],\ \rho_l : \mathbb{Z}^{(r)}[T] \twoheadrightarrow \mathbb{F}_\ell^{(r)}[T]$$

$$X = \{(a_0, \ldots, a_{r-1}),\ |a_i| \leq N\ \forall 0 \leq i < r\} \text{ et } F : X \to Y;$$

$$\mathcal{L}^* = \{\ell \in \mathbb{P},\ \ell \leq L\} \text{ pour un entier } L \geq 2,\ \Omega_\ell = \{f \in \mathbb{F}_\ell^{(r)}[T] \text{ irréductible}\};$$

$$\forall f \in \mathbb{F}_\ell^{(r)}[T], \qquad \nu_\ell(f) = \frac{1}{|\mathbb{F}_\ell^{(r)}[T]|} = \frac{1}{\ell^r}.$$

Si un polynôme $f \in \mathbb{Z}^{(r)}[T]$ vérifie ($f$ mod $\ell$ est irréductible dans $\mathbb{F}_\ell[T]$) alors $f$ est irréductible. On en déduit que

$$E_r(N) \subset S(X, (\Omega_\ell), \mathcal{L}^*).$$

Comme $\Delta = \Delta(X, \mathcal{L})$, la proposition 1.8 s'applique , $\Delta \leq (\sqrt{2N+1} + L)^{2r}$ et, de la proposition 1.7, on déduit :

$$|E_r(N)| \leq |S(X, (\Omega_\ell), \mathcal{L}^*)| \leq \Delta P(L)^{-1} \leq (\sqrt{2N+1} + L)^{2r} P(L)^{-1}$$

où

$$P(L) = \sum_{\ell \leq L} \frac{|\Omega_\ell|}{\ell^r}.$$

## 2.2 Dénombrement des polynômes unitaires de degré $r$ irréductibles sur $\mathbb{F}_\ell$

On introduit tout d'abord la fonction de Möbius, dans un cadre général, et quelques unes de ses propriétés qui seront utiles par la suite.

On définit les ensembles $\mathcal{S}$ et $\mathcal{A}$ par :

$$\mathcal{S} = \{f : \mathbb{R} \to \mathbb{C},\ f(x) = 0 \text{ pour } x < 1\},$$

$$\mathcal{A} = \{f \in \mathcal{S},\ f(x) = 0 \text{ pour } x \notin \mathbb{N}\}.$$

Pour $f, g \in \mathcal{S}$, on définit le produit de convolution $f * g$ dans $\mathcal{S}$ par

$$(f * g)(x) = \sum_{1 \leq n \leq x} f\left(\frac{x}{n}\right) g(n).$$

Si $f \in \mathcal{A}$ et $g \in \mathcal{S}$ alors on vérifie que $f * g \in \mathcal{A}$ et

$$\forall n \in \mathbb{N}, \qquad (f * g)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d).$$

En général, l'opérateur $*$ n'est pas commutatif sur $\mathcal{S}$, mais il l'est sur $\mathcal{A}$.

On définit la fonction $\varepsilon \in \mathcal{A}$ par

$$\varepsilon(x) = \begin{cases} 1 & \text{pour } x = 1 \\ 0 & \text{sinon.} \end{cases}$$

On vérifie que

$$\forall f \in \mathcal{S}, \qquad f * \varepsilon = f$$

et

$$\forall f \in \mathcal{S}, \qquad (\varepsilon * f)(x) = \begin{cases} f(x) & \text{si } x \in \mathbb{N} \\ 0 & \text{sinon.} \end{cases}$$

On définit la fonction $\mathbf{1}_0 = \varepsilon * \mathbf{1}_{[1,+\infty[} \in \mathcal{A}$ et la fonction de Möbius $\mu \in \mathcal{A}$ par

$$\mathbf{1}_0 * \mu = \varepsilon.$$

**Proposition 2.2 (*Formule d'inversion de Möbius*)**

*Soient $f, g \in \mathcal{S}$. $f = g * \mathbf{1}_0$ si et seulement si $g = f * \mu$.*

▷ Si $f = g * \mathbf{1}_0$ alors $f * \mu = g * \mathbf{1}_0 * \mu = g * \varepsilon = g$. Réciproquement, si $g = f * \mu$ alors $g * \mathbf{1}_0 = f * \mu * \mathbf{1}_0 = f * \varepsilon = g * \mathbf{1}_0$. □

Nous aurons également besoin de deux lemmes sur les polynômes à coefficients dans un corps fini [10].

**Lemme 2.3**

*Soit $P \in \mathbb{F}_\ell[T]$ un polynôme irréductible de degré $d$. Alors $P$ divise $T^{\ell^r} - T$ si et seulement si $d$ divise $r$.*

▷ Supposons que $P$ divise $T^{\ell^r} - T$. Soit $\alpha$ une racine de $P$ dans un corps de décomposition de $P$ sur $\mathbb{F}_\ell$. Alors $\alpha^{\ell^r} = \alpha$, donc $\mathbb{F}_\ell(\alpha)$ est un sous-corps de $\mathbb{F}_{\ell^r}$, donc de degré, égal à $d$, sur $\mathbb{F}_\ell$ divisant $r$.

Réciproquement, si $d$ divise $r$, alors $\mathbb{F}_{\ell^d} \subset \mathbb{F}_{\ell^r}$. Si $\alpha$ est une racine de $P$ dans un corps de décomposition de $P$ sur $\mathbb{F}_\ell$, alors $[F_\ell(\alpha) : \mathbb{F}_\ell] = d$ et donc $\mathbb{F}_\ell(\alpha) = \mathbb{F}_{\ell^d}$. On en déduit que $\alpha \in \mathbb{F}_{\ell^r}$ et donc que $\alpha$ est racine de $T^{\ell^r} - T$. Mais $P$ étant irréductible, c'est le polynôme minimal de $\alpha$, et donc il divise $T^{\ell^r} - T$. □

**Lemme 2.4**

*Pour tout entier $r \geq 0$, le produit des polynômes irréductibles unitaires de $\mathbb{F}_\ell[T]$ dont le degré divise $r$ est égal à $T^{\ell^r} - T$.*

$\triangleright$ Par le lemme précédent, les facteurs irréductibles de $T^{\ell^r} - T$ sont exactement les polynômes irréductibles unitaires de degré divisant $r$. Comme $(T^{\ell^r} - T)' = -1$, $T^{\ell^r} - T$ ne possède pas de facteurs multiples, d'où le résultat. $\square$

On peut désormais exprimer le nombre $|\Omega_\ell|$ de polynômes irréductibles de degré $r$ dans $\mathbb{F}_\ell[T]$. D'après le lemme précédent, en comparant les degrés, on obtient

$$\ell^r = \sum_{d|r} d m_d$$

où $m_d$ est le nombre de polynômes irréductibles unitaires de degré $d$ sur $\mathbb{F}_\ell$. En appliquant la formule d'inversion de Möbius, on trouve

$$\forall r \geq 1, \qquad |\Omega_\ell| = \frac{1}{r} \sum_{d|r} \mu(d) \ell^{r/d}.$$

## 2.3 Minoration de $P(L)$

D'après le résultat du paragraphe précédent, on peut écrire

$$\begin{aligned} |\Omega_\ell| &= \frac{1}{r} \sum_{d|r} \mu(d) \ell^{r/d} \\ &= \frac{\ell^r}{r} + \frac{1}{r} \sum_{1<d|r} \mu(d) \ell^{r/d} \\ &\geq \frac{\ell^r}{r} - \frac{\ell^{r/2}}{r} \sum_{1<d\leq r} 1 \\ &\geq \frac{\ell^r}{r} - \ell^{r/2} \end{aligned}$$

Or, pour $r \geq 4$ et $\ell > 2r$,

$$\frac{\ell^{r-1}}{r} > 2\ell^{r-2} \geq \ell^{r/2} + \ell^{r-2} \geq \ell^{r/2} + \ell \geq \ell^{r/2} + 1.$$

De plus, si $r = 3$ et $\ell > 4r$, on montre que la fonction

$$\ell \mapsto \frac{\ell^2}{3} - \ell^{3/2} - 1$$

est croissante sur $[6, +\infty[$ donc pour $\ell > 4r > 6$, il suffit de vérifier que

$$\frac{16r^2}{3} - (4r)^{3/2} - 1 > 0.$$

Ainsi, pour tout $r \geq 3$,

$$|\Omega_\ell| \geq \frac{\ell^r}{r}\left(1-\frac{1}{\ell}\right)$$

et l'inégalité est encore vraie pour $r = 2$.

Ainsi, pour $L > 4r$,

$$\begin{aligned} P(L) &= \sum_{\ell \leq L} \frac{|\Omega_\ell|}{\ell^r} \geq \frac{1}{r} \sum_{4r<\ell\leq L} \left(1-\frac{1}{\ell}\right) \\ &\geq \frac{\pi(L)}{r} - \frac{1}{r}\sum_{\ell\leq L}\frac{1}{\ell} - \frac{\pi(4r)}{r} + \frac{1}{r}\sum_{\ell\leq 4r}\frac{1}{\ell}. \end{aligned}$$

Il faut donc minorer $\pi(L)$ et

$$\sum_{\ell\leq L}\frac{1}{\ell}.$$

On a le résultat suivant [2].

**Théorème 2.5**

$$\forall x \geq 2, \qquad \left(\frac{\log 2}{4}\right)\frac{x}{\log x} \leq \pi(x) \leq (6\log 2)\frac{x}{\log x}.$$

▷ − Minoration de $\pi(x)$.

On utilisera la formule de Legendre :

**Lemme 2.6 (*Formule de Legendre*)**

*On a*

$$\forall n \geq 2, \qquad v_p(n!) = \sum_{k=1}^{+\infty}\left\lfloor \frac{n}{p^k}\right\rfloor$$

*où, pour $p$ premier, $v_p$ désigne la valuation $p$-adique.*

▷ On a :

$$v_p(n!) = \sum_{j=1}^{n} v_p(j) = \sum_{k=1}^{n}\sum_{k=1}^{+\infty}(p^k|j)$$

où $(p^k|j) = \begin{cases} 1 & \text{si } p^k|j \\ 0 & \text{sinon} \end{cases}$ donc

$$v_p(n!) = \sum_{k=1}^{+\infty}\sum_{j=1}^{n}(p^k|j) = \sum_{k=1}^{+\infty}\left|\left\{ip^k,\ i \in \left[\!\left[1, \left\lfloor\frac{n}{p^k}\right\rfloor\right]\!\right]\right\}\right| = \sum_{k=1}^{+\infty}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

□

En notant $\alpha_p(n) = v_p\left(\binom{2n}{n}\right)$, d'après la formule de Legendre,

$$\alpha_p(n) = v_p(2n) - 2v_p(n) = \sum_{k=1}^{+\infty}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) = \sum_{k=1}^{\gamma_p(n)}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

où $\gamma_p(n) = \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor$ est le plus grand entier tel que $p^\gamma \leq 2n$. Or, pour tout $x \in \mathbb{R}$,

$$\begin{cases} 2x - 1 < \lfloor 2x \rfloor \leq 2x \\ -2x \leq -2 \lfloor x \rfloor < -2x + 2 \end{cases}$$

donc la quantité $\lfloor 2x \rfloor - 2 \lfloor x \rfloor$ vaut 0 ou 1 et donc

$$\alpha_p(n) \leq \sum_{k=1}^{\gamma_p(n)} 1 = \gamma_p(n).$$

Par ailleurs, si $p$ est un diviseur premier de $\binom{2n}{n}$, alors $p$ divise $(2n)! = \binom{2n}{n} (n!)^2$ donc $p \leq 2n$.

Ainsi,

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\alpha_p(n)} \leq \prod_{p \leq 2n} p^{\gamma_p(n)} \leq \prod_{p \leq 2n} 2n = (2n)^{\pi(2n)}.$$

Or

$$\frac{1}{2^n} \binom{2n}{n} = \frac{(2n)!}{2^n (n!)^2} = \prod_{k=1}^{n} \frac{n+k}{2k} \geq 1$$

donc

$$\pi(2n) \log(2n) \geq n \log 2.$$

Ainsi,

$$\forall n \geq 1, \qquad \pi(2n) \geq \frac{n \log 2}{\log(2n)}.$$

Soit désormais $x \geq 2$ et $n \in \mathbb{N}^*$ tel que $2n \leq x < 2n + 2$. Alors

$$\pi(x) \geq \pi(2n) \geq \frac{n \log 2}{\log 2n} \geq \frac{n \log 2}{\log x}$$

et

$$n \geq \frac{n+1}{2} \geq \frac{x}{4}$$

donc

$$\pi(x) \geq \left( \frac{\log 2}{4} \right) \frac{x}{\log x}.$$

– Majoration de $\pi(x)$.

Soit $p$ tel que $n < p \leq 2n$. Alors $p$ divise $(2n)! = \binom{2n}{n} (n!)^2$ donc, comme $p$ est premier avec $(n!)^2$, $p$ divise $\binom{2n}{n}$. On en déduit que $\prod_{n < p \leq 2n} p$ divise $\binom{2n}{n}$ et donc

$$\binom{2n}{n} \geq \prod_{n < p \leq 2n} p \geq n^{\pi(2n) - \pi(n)}.$$

Or

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \geq \binom{2n}{n}$$

donc

$$n^{\pi(2n)-\pi(n)} \leq 4^n$$

d'où

$$\pi(2n) - \pi(n) \leq \frac{2n \log 2}{\log n}.$$

Par ailleurs, pour $k \geq 1$, l'ensemble $\{3, 4, \ldots, 2^{k+1}\}$ contient $2^k - 1$ entiers impairs donc $\pi(2^{k+1}) \leq 1 + (2^k - 1) = 2^k$, et le résultat reste vrai pour $k = 0$. De plus, pour $n = 2^k$, $k \geq 1$, l'inégalité obtenue ci-dessus s'écrit :

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1}}{k}.$$

Ainsi,

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) \leq 2^{k+1} + \pi(2^{k+1}) \leq 3 \times 2^k.$$

En sommant ceci pour $1 \leq k \leq n$, on obtient

$$(n+1)\pi(2^{n+1}) \leq 3(2^{n+1} - 1) \leq 3 \times 2^{n+1}.$$

Soit $x \geq 2$ et $n \in \mathbb{N}$ tel que $2^n \leq x \leq 2^{n+1}$. On a

$$\pi(x) \leq \pi(2^{n+1}) \leq \frac{6 \times 2^n}{n+1} \leq (6 \log 2)\frac{x}{\log x}.$$

□

On peut en déduire l'estimation suivante.

**Théorème 2.7**

$$\sum_{\ell \leq L} \frac{1}{\ell} = \Theta(\log \log L)$$

*où les constantes sous-entendues sont absolues.*

▷ On peut écrire

$$\sum_{\ell \leq L} \frac{1}{\ell} = \sum_{k=2}^{L} \frac{\pi(k) - \pi(k-1)}{k} = \frac{\pi(L)}{L} + \sum_{k=2}^{L-1} \left( \frac{\pi(k)}{k} - \frac{\pi(k)}{k+1} \right) = \frac{\pi(L)}{L} + \sum_{k=2}^{L-1} \frac{\pi(k)}{k(k+1)}.$$

De l'encadrement du théorème précédent on déduit

$$\frac{\log 2}{4(k+1)\log k} \leq \frac{\pi(k)}{k(k+1)} \leq \frac{6 \log 2}{(k+1)\log k}$$

d'où

$$\frac{\pi(L)}{L} + \frac{\log 2}{4} \sum_{k=2}^{L-1} \frac{1}{(k+1)\log k} \leq \sum_{\ell \leq L} \frac{1}{\ell} \leq \frac{\pi(L)}{L} + 6 \log 2 \sum_{k=2}^{L-1} \frac{1}{(k+1)\log k}.$$

Mais

$$\sum_{k=2}^{L-1} \frac{1}{(k+1)\log k} \geq \sum_{k=3}^{L} \frac{1}{k \log k}$$

et, par comparaison avec une intégrale,

$$\sum_{k=2}^{L-1} \frac{1}{(k+1)\log k} \geq \sum_{k=3}^{L} (\log\log(k+1) - \log\log k) = \log\log(L+1) - \log\log 3.$$

De même,

$$\begin{aligned} \sum_{k=2}^{L-1} \frac{1}{(k+1)\log k} &\leq \sum_{k=2}^{L-1} \frac{1}{k\log k} \leq \frac{1}{2\log 2} + \sum_{k=3}^{L-1} (\log\log k - \log\log(k-1)) \\ &\leq \frac{1}{2\log 2} + \log\log(L-1) - \log\log 2. \end{aligned}$$

Ainsi, comme

$$\frac{\log 2}{4\log L} \leq \frac{\pi(L)}{L} \leq \frac{6\log 2}{\log L}$$

et

$$\log\log(L-1) \leq \log\log L \leq \log\log(L+1),$$

on obtient

$$\frac{\log 2}{4}\left(\frac{1}{\log L} + \log\log L - \log\log 3\right) \leq \sum_{\ell \leq L} \frac{1}{\ell} \leq 6\log 2\left(\frac{1}{\log L} + \frac{1}{2\log 2} + \log\log L - \log\log 2\right)$$

que l'on écrit

$$\gamma(L) \leq \sum_{\ell \leq L} \frac{1}{\ell} \leq \delta(L).$$

Or

$$\lim_{L\to+\infty} \frac{\gamma(L)}{\log\log L} = \frac{\log 2}{4} \qquad \text{et} \qquad \lim_{L\to+\infty} \frac{\delta(L)}{\log\log L} = 6\log 2$$

donc $\left(\dfrac{\gamma(L)}{\log\log L}\right)_{L\geq 3}$ est minorée par un réel $\lambda > 0$, et $\left(\dfrac{\delta(L)}{\log\log L}\right)_{L\geq 3}$ est majorée par un réel $\mu > 0$. Ainsi,

$$\lambda \log\log L \leq \sum_{\ell \leq L} \frac{1}{\ell} \leq \mu \log\log L.$$

□

Ainsi, pour $L > 4r$,

$$P(L) \geq \left(\frac{\log 2}{4}\right) \frac{L}{r\log L} - \frac{\mu}{r}\log\log L - \frac{24\log 2}{\log(4r)} + \frac{\lambda \log\log(4r)}{r}.$$

On en déduit que

$$P(L) \gg \frac{L}{r\log L}$$

la constante sous-entendue étant absolue.

### 2.4 Conclusion

Supposons $\sqrt{2N+1} > 4r^2$ et prenons $L = \frac{\sqrt{2N+1}}{r} > 4r$. Alors, on a montré que

$$\begin{aligned} |E_r(N)| &\leq (\sqrt{2N+1} + L)^{2r} P(L)^{-1} \\ &\leq (2N+1)^r \left(1 + \tfrac{1}{r}\right)^{2r} P(L)^{-1} \\ &\ll r^2 (2N+1)^{r-1/2} (\log(2N+1)). \end{aligned}$$

Par ailleurs, si $\sqrt{2N+1} < 4r^2$,

$$r^2 (2N+1)^{r-1/2} \log(2N+1) \gg (2N+1)^r \log(2N+1) > |\{f,\ |a_i| \leq N\}| > |E_r(N)|$$

et l'estimation est encore vraie.

## 3 Théorème de Gallagher pour les polynômes réciproques réductibles

### 3.1 Énoncé

On dit qu'un polynôme $f \in A[T]$ de degré $r$ est réciproque s'il satisfait

$$f(T) = T^r f\left(\frac{1}{T}\right).$$

On énonce quelques propriétés générales sur ces polynômes qui vont nous être utiles par la suite [5].

**Proposition 3.1**

*(i) Si $f \in \mathbb{Z}[T]$ est réciproque alors l'ensemble des racines de $f$ est stable par l'application $\alpha \mapsto \alpha^{-1}$.*

*(ii) Si $f \in \mathbb{F}_\ell^{(r)}[T]$ est irréductible et si l'ensemble des racines de $f$ est stable par $\alpha \mapsto \alpha^{-1}$, alors*

$$X^r f\left(\frac{1}{T}\right) = \begin{cases} -f(T) & \text{si } f(T) = T-1 \text{ et } \ell \neq 2 \\ f(T) & \text{sinon.} \end{cases}$$

*(iii) Si $f \in \mathbb{Z}[T]$ est réciproque et $f(-1) \neq 0$ alors $f$ est de degré pair.*

**Remarque 3.2.** On déduit de cette proposition que si $f$ est un polynôme réciproque irréductible, alors $f$ est de degré pair.

**Théorème 3.3**

*Soit $r \geq 1$ un entier. Pour tout entier $N \geq 1$, définissons $X_{2r}(N)$ comme l'ensemble des*

*polynômes $f \in \mathbb{Z}[T]$ unitaires réciproques réductibles de degré $2r$ tels que*

$$f = T^{2r} + a_{2r-1}T^{2r-1} + \cdots + a_1 T + a_0 = a_0 T^{2r} + a_1 T^{2r-1} + \cdots + a_{2r-1}T + 1 = T^{2r} f\left(\frac{1}{T}\right)$$

*où $|a_i| \leq N$ pour tout $0 \leq i < 2r$. Alors*

$$|X_{2r}(N)| \ll r^2 (2N+1)^{r-1/2} \log N,$$

*la constante sous-entendue étant absolue.*

Pour la démonstration, on se place dans le cadre

$$Y = \{f \in \mathbb{Z}^{(2r)}[T],\ \text{unitaire},\ \text{réciproque},\ |a_i| \leq N\}$$

$$Y_\ell = \{f \in \mathbb{F}_\ell^{(2r)}[T],\ \ \text{unitaire},\ \text{réciproque}\}$$

$$\rho_\ell : Y \twoheadrightarrow Y_\ell$$

$$X = \{(a_1, \ldots, a_r) \in \mathbb{Z}^r,\ |a_i| \leq N\}$$

$$F : X \longleftrightarrow Y$$

$$\mathcal{L}^* = \{\ell \in \mathbb{P},\ \ell \leq L\} \text{ pour un entier } 2 \leq L < N$$

$$\Omega_\ell = \{f \in \mathbb{F}_\ell[T],\ \deg(f) = 2r,\ \text{unitaire, réciproque, irréductible}\}.$$

$$\forall f \in Y_\ell, \qquad \nu_\ell(f) = \frac{1}{|Y_\ell|} = \frac{1}{\ell^r}.$$

Si un polynôme $f \in \mathbb{Z}^{(2r)}[T]$ vérifie ($f$ mod $\ell$ est irréductible sur $\mathbb{F}_\ell[T]$), alors $f$ est irréductible. On en déduit que

$$X_{2r}(N) \subset S(X, (\Omega_\ell), \mathcal{L}^*).$$

Comme $\Delta = \Delta(X, \mathcal{L})$, la proposition 1.8 s'applique , $\Delta \leq (\sqrt{2N+1} + L)^{2r}$ et, de la proposition 1.7, on déduit :

$$|X_{2r}(N)| \leq |S(X, (\Omega_\ell), \mathcal{L}^*)| \leq \Delta P(L)^{-1} \leq (\sqrt{2N+1} + L)^{2r} P(L)^{-1}$$

où

$$P(L) = \sum_{\ell \leq L} \frac{|\Omega_\ell|}{\ell^r}.$$

## 3.2 Dénombrement des polynômes réciproques de degré $2r$ irréductibles sur $\mathbb{F}_\ell$

Dans la partie 2.2, on a pu constater que le polynôme $T^{\ell^r} - T$ jouait un rôle particulier qui nous a permis de compter les polynômes irréductibles unitaires de degré $r$ sur $\mathbb{F}_\ell$.

Ici, nous allons voir que c'est le polynôme

$$H_{\ell,r} = T^{\ell^r+1} - 1 \in \mathbb{F}_\ell[T]$$

qui a le même rôle pour les polynômes réciproques irréductibles de degré $2r$ sur $\mathbb{F}_\ell$.

Énonçons tout d'abord un résultat général sur les polynômes irréductibles sur un corps fini qui va nous être utile [10] :

**Théorème 3.4**

*Soit $P \in \mathbb{F}_\ell^{(m)}[T]$ un polynôme irréductible de degré $m$. Alors $P$ possède une racine $\alpha$ dans $\mathbb{F}_{\ell^m}$. De plus, toutes les racines de $P$ sont simples, données par $\alpha, \alpha^\ell, \ldots, \alpha^{\ell^m-1}$.*

▷ Un corps de rupture de $P$ est $\mathbb{F}_{\ell^m}$. Si $\alpha$ est une racine de $P$, alors, comme $P(\alpha^\ell) = P(\alpha)^\ell$, $\alpha^\ell$ est également racine. Ainsi, $\alpha, \alpha^\ell, \ldots, \alpha^{\ell^m-1}$ sont les racines de $P$.

Supposons qu'elles ne soient pas distinctes : soient $0 \leq i < j < m-1$ tels que

$$\alpha^{\ell^i} = \alpha^{\ell^j}.$$

En élevant à la puissance $\ell^{m-j}$, on obtient

$$\alpha^{\ell^{m-j+i}} = \alpha^{\ell^m} = \alpha.$$

Ainsi, $P$ divise $T^{\ell^{m-j+i}} - T$.

Alors, d'après le lemme 2.3, $m | m-j+i < m$, ce qui est absurde. □

La clé pour dénombrer les polynômes réciproques irréductibles est le théorème suivant [5].

**Théorème 3.5**

*(i) Tout polynôme unitaire réciproque irréductible de degré $2r$ sur $\mathbb{F}_\ell$ est un facteur de*

$$H_{\ell,r}(T) = T^{\ell^r+1} - 1 \in \mathbb{F}_\ell[T].$$

*(ii) Tout facteur irréductible de degré $\geq 2$ de $H_{\ell,r}$ est un polynôme unitaire réciproque irréductible de degré $2d$ où $d | r$ et $\frac{r}{d}$ est impair.*

▷ $(i)$ Soit $f$ un polynôme réciproque irréductible de degré $2r$ sur $\mathbb{F}_\ell$. Par le théorème précédent, notons $\alpha, \ldots \alpha^{\ell^{2r-1}}$ ses racines distinctes dans $\mathbb{F}_{\ell^{2r}}$. L'ensemble des racines de $f$ étant stable par l'application $\alpha \mapsto \alpha^{-1}$, il existe un unique $0 \leq j \leq 2r-1$ tel que

$$\alpha^{\ell^j} = \alpha^{-1}$$

donc $H_{\ell,j}(\alpha) = 0$ d'où $f$ divise $H_{\ell,j}$.

Or, si $\beta$ est racine de $H_{\ell,j}$,

$$\beta^{\ell^{2j}} = \left(\beta^{\ell^j}\right)^{\ell^j} = \beta^{-\ell^j} = \beta$$

donc $H_{\ell,j}$ divise $T^{\ell^{2j}} - T$.

Ainsi, $f$ divise $T^{\ell^{2j}} - T$. $f$ étant irréductible, d'après le lemme 2.3, $2r$ divise $2j : 2j = 2rk$ où $k \in \mathbb{N}$. Or $j \leq 2r-1$ donc $k = 0$ ou 1 et $k \neq 0$ car sinon $\alpha^2 = 1$ et $f$ n'est pas irréductible. Ainsi, $j = r$.

$(ii)$ Soit $g$ un facteur irréductible de degré $m \geq 2$ de $H_{\ell,r}$. Soit $\alpha$ une racine de $g$. Alors $\alpha^{\ell^r} = \alpha^{-1}$.

Soit $\{\alpha, \alpha^\ell, \ldots, \alpha^{\ell^{m-1}}\} \subset \mathbb{F}_{\ell^m}$ les racines de $g$. Il existe $k \leq m-1$ tel que $\alpha^{\ell^r} = \alpha^{\ell^k}$ et donc l'ensemble des racines de $g$ est stable par $\alpha \mapsto \alpha^{-1}$.

D'après la proposition 3.1, $g$ est réciproque de degré pair $m = 2d$. Comme au point $(i)$, on en déduit que $2d|2r$ puis $d|r$ et que $g$ divise $H_{\ell,d}$ et $H_{\ell,r}$ donc $g$ divise $\text{pgcd}(H_{\ell,d}, H_{\ell,r})$.

**Lemme 3.6**

*Soient $m, n \in \mathbb{Z}$.*

$$pgcd(T^m - 1, T^n - 1) = T^{\text{pgcd}(m,n)} - 1.$$

▷ Supposons que $m \geq n$ et soit $m = qn + r$ la division euclidienne de $m$ par $n$. On a

$$T^m - 1 = T^r(T^{qn} - 1) + T^r - 1 = T^r(T^n - 1)\left(\sum_{i=0}^{q-1} T^{ni}\right) + T^r - 1$$

donc, comme $\text{pgcd}(T^m - 1, T^n - 1)$ divise $T^m - 1$ et $T^n - 1$, $\text{pgcd}(T^m - 1, T^n - 1)$ divise $T^r - 1$. Ainsi, $\text{pgcd}(T^m - 1, T^n - 1)$ divise $\text{pgcd}(T^n - 1, T^r - 1)$. De même, on déduit de l'égalité précédente que $\text{pgcd}(T^n - 1, T^r - 1)$ divise $\text{pgcd}(T^m - 1, T^n - 1)$. Ainsi,

$$\text{pgcd}(T^m - 1, T^n - 1) = \text{pgcd}(T^n - 1, T^r - 1)$$

et en itérant ce procédé et en appliquant l'algorithme d'Euclide, on obtient

$$\text{pgcd}(T^m - 1, T^n - 1) = \text{pgcd}(T^n - 1, T^r - 1) = \cdots = \text{pgcd}(T^{\text{pgcd}(m,n)} - 1, T^0 - 1) = T^{\text{pgcd}(m,n)} - 1.$$

□

Ainsi, $g$ divise $\text{pgcd}(H_{\ell,d}, H_{\ell,r}) = T^{\text{pgcd}(\ell^r+1, \ell^d+1)}$.

Supposons par l'absurde que $\frac{r}{d}$ est pair : $r = 2kd$, $k \in \mathbb{N}$. Alors

$$\ell^r + 1 = (\ell^d)^{2k} - (-1)^{2k} + 2 = (\ell^d + 1) \sum_{i=0}^{2k-1} \ell^{d(r-1-i)}(-1)^i + 2$$

donc

$$\text{pgcd}(\ell^r + 1, \ell^d + 1) = \text{pgcd}(\ell^d + 1, 2) = \begin{cases} 1 & \text{si } \ell = 2 \\ 2 & \text{sinon} \end{cases}$$

ce qui contredit l'irréductibilité de $g$ ou $\deg(g) \geq 2$. Ainsi, $\frac{r}{d}$ est impair. □

Définissons $R_{\ell,r}$ comme le produit des polynômes unitaires réciproques irréductibles de degré $2r$. D'après le théorème précédent,

$$H_{\ell,r} = (T^{1+e_\ell} - 1) \prod_{\substack{d|n \\ \frac{r}{d} \text{ impair}}} R_{\ell,d}$$

où $e_\ell = (\ell \bmod 2)$ *ie.*

$$(T^{1+e_\ell} - 1) = \begin{cases} T-1 & \text{si } \ell = 2 \\ (T-1)(T+1) & \text{si } \ell \text{ est impair} \end{cases}$$

Afin de "normaliser", posons

$$H^0_{\ell,r} = \frac{H_{\ell,r}}{T^{1+e_\ell} - 1} = \prod_{\substack{d|r \\ \frac{r}{d} \text{ impair}}} R_{\ell,d}.$$

Par la formule d'inversion de Möbius (multiplicative), on en déduit que

$$R_{\ell,r} = \prod_{\substack{d|r \\ d \text{ impair}}} (H^0_{\ell,r/d})^{\mu(d)}.$$

Comme

$$\sum_{d|r} \mu(d) = 0,$$

la normalisation se simplifie si $r \neq 2^s$ et on obtient

$$R_{\ell,r} = \prod_{\substack{d|r \\ d \text{ impair}}} H^{\mu(d)}_{\ell,r/d} \qquad \text{si } r \neq 2^s.$$

En égalisant les degrés, on obtient

$$|\Omega_\ell| = \begin{cases} \dfrac{1}{2r}(\ell^r - 1) & \text{si } \ell \text{ est impair et } r = 2^s \\ \dfrac{1}{2r} \displaystyle\sum_{\substack{d|r \\ d \text{ impair}}} \mu(d)\ell^{r/d} & \text{si } r \neq 2^s \end{cases}$$

### 3.3 Conclusion

Supposons $r \neq 2^s$. Comme dans la démonstration du théorème de Gallagher, on peut minorer $|\Omega_\ell|$ :

$$|\Omega_\ell| = \frac{1}{2r} \sum_{\substack{d|r \\ d \text{ impair}}} \mu(d)\ell^{r/d} \geq \frac{\ell^r}{2r} - \frac{\ell^{r/2}}{2} \geq \frac{\ell^r}{2r}\left(1 - \frac{1}{\ell}\right),$$

où la constante est absolue Ainsi, comme précédemment, pour $L > 4r$,

$$P(L) = \sum_{\ell \leq L} \frac{|\Omega_\ell|}{\ell^r} \gg \frac{L}{r \log L}.$$

En prenant $L = \frac{\sqrt{2N+1}}{r}$, $\sqrt{2N+1} > 4r^2$, on obtient

$$|X_{2r}(N)| \ll r^2 (2N+1)^{r-1/2} \log N,$$

la constante étant absolue et l'estimation étant triviale si $\sqrt{2N+1} < 4r^2$.

### 3.4 Autre approche

On s'appuie sur les résultats suivants.

**Proposition 3.7**

*Soit $k$ un corps et $f \in k[T]$ un polynôme réciproque unitaire de degré $2r$. Il existe un unique polynôme unitaire $h \in k[T + T^{-1}]$ de degré $r$ tel que*

$$f(T) = T^r h(T + T^{-1}).$$

$\triangleright$ − Existence : Soit $f = T^{2r} + a_1 T^{2r-1} + \cdots + a_{r-1} T^{r+1} + a_r T^r + a_{r-1} T^{r-1} + \cdots + a_1 T + 1$. En mettant $T^r$ en facteur, on obtient

$$\begin{aligned} f &= T^r \left( T^r + a_1 T^{r-1} + \cdots + a_{r-1} T + a_r + a_{r-1} \frac{1}{T} + \cdots + a_1 \frac{1}{T^{r-1}} + \frac{1}{T^r} \right) \\ &= T^r \left( \left( T^r + \frac{1}{T^r} \right) + a_1 \left( T^{r-1} + \frac{1}{T^{r-1}} \right) + \cdots + a_{r-1} \left( T + \frac{1}{T} \right) + a_r \right). \end{aligned}$$

Or, on montre par récurrence que, pour tout $i \in \mathbb{N}$, $T^i + \frac{1}{T^i} \in k^{(i)}[T + T^{-1}]$ :
$i = 2 : \left(T + T^{-1}\right)^2 = T^2 + 2 + T^{-2}$ donc $T^2 + T^{-2} = (T + T^{-1})^2 - 2$
$i \geq 2 : (T + T^{-1})^{i+1} = (T + T^{-1})(T + T^{-1})^i$ d'où le résultat.

Ainsi, il existe $h \in k[T + T^{-1}]$ unitaire de degré $r$ tel que

$$f(T) = T^r h(T + T^{-1}).$$

− Unicité : Si $h_1, h_2 \in k[T]$ conviennent, alors $h_1(T + T^{-1}) = h_2(T + T^{-1})$. Soit $K/k$ une extension de $k$ telle que $|K| > \deg(f) = 2\deg(h_{1,2})$. Alors si $T$ prend ses valeurs dans $K$, $T + T^{-1}$ prend au plus $\frac{|K|}{2} > \deg(h_{1,2})$ valeurs. Ainsi, $h_1$ et $h_2$ prennent les valeurs en un nombre strictement supérieur à $\deg(h_1) = \deg(h_2)$ points. Ces polynômes sont donc égaux. □

On montre facilement que si $h$ est réductible, alors $f$ l'est également. Cependant, la réciproque est fausse en général. On a seulement le résultat suivant [5],[8].

**Proposition 3.8**

*Si $h$ est irréductible sur $\mathbb{F}_\ell$ de degré $r > 1$ alors on a l'alternative suivante :*

— *soit* $T^r h\left(T+T^{-1}\right)$ *est un polynôme réciproque irréductible unitaire de degré* $2r$ *;*
— *soit* $T^r h\left(T+T^{-1}\right) = T^r g(T) g(T^{-1})$ *où* $g$ *est un polynôme irréductible de degré* $r$ *qui n'est pas réciproque.*

▷ Posons $f = T^r h\left(T+T^{-1}\right)$. Si $\alpha \neq 0$ est une racine de $f$, alors $\alpha+\alpha^{-1}$ est une racine de $h$. Comme $h$ est irréductible, $r$ est le plus petit entier tel que

$$(\alpha+\alpha^{-1})^{\ell^r} = \alpha+\alpha^{-1},$$

ce qui équivaut à, en multipliant par $\alpha^{\ell^r}$,

$$\alpha^{2\ell^r} - \alpha^{\ell^r+1} - \alpha^{\ell^r-1} + 1 = 0$$

soit

$$(\alpha^{\ell^r+1}-1)(\alpha^{\ell^r-1}-1) = 0.$$

– 1er cas : $\alpha^{\ell^r+1}-1=0$.

Soit $g$ un facteur irréductible de $f$ ayant pour racine $\alpha$. Alors, $g$ divise $H_{\ell,r}$.

Si $g$ est de degré 1, alors $\alpha = \pm 1$ et $h$ ne serait pas irréductible.

Ainsi, $\deg(g) \geq 2$. Alors, par le théorème 3.5, comme $g$ divise $H_{\ell,r}$ et est irréductible, $g$ est un polynôme unitaire réciproque irréductible de degré $2d$, où $d|r$ et $\frac{r}{d}$ est impair.

Si $d < r$, alors $\alpha^{\ell^{2d}} = \alpha$ d'où $(\alpha+\alpha^{-1})^{\ell^{2d}} = \alpha+\alpha^{-1}$. Par minimalité de $r$, $d \geq \frac{r}{2}$, ce qui contredit le fait que $\frac{r}{d}$ est impair.

Ainsi, $d = r$ et $f$ est irréductible.

– 2e cas : $\alpha^{\ell^r-1}-1=0$.

Soit $g$ un facteur irréductible de $f$ ayant pour racine $\alpha$. Alors $g$ divise $T^{\ell^r}-T$ donc, d'après le lemme 2.3, le degré $d$ de $g$ divise $r$. On a donc $\alpha^{\ell^d} = \alpha$ puis $(\alpha+\alpha^{-1})^{\ell^d} = \alpha+\alpha^{-1}$ ce qui impose $d = r$.

Ainsi, $f$ possède deux facteurs irréductibles de degré $r$.

Si $g$ était un polynôme réciproque (ce qui ne serait possible que pour $r$ pair), alors $\alpha^{\ell^{r/2}+1}-1=0$ ce qui contredirait la minimalité de $r$.

De plus, si $\alpha$ est racine de $g$, alors $\alpha^{-1}$ est racine de $f$ (réciproque), donc $\alpha^{-1}$ est racine de $\frac{f}{g}$. Ainsi, les racines de $\frac{f}{g}$ sont exactement les inverses des racines de $g$, donc $\frac{f}{g}$ est le polynôme réciproque de $g$. □

Ainsi, on a l'inclusion

$$X_{2r}(N) \hookrightarrow \{h \in \mathbb{Z}^{(r)}[T],\ \rho_\ell(h) \notin \Omega_\ell,\ \forall \ell \leq L\}$$

où

$$\Omega_\ell = \{h \in \mathbb{F}_\ell^{(r)}[T], \text{irréductible}\} \backslash A_\ell$$

avec

$$A_\ell = \{f \in \mathbb{F}_\ell^{(2r)}[T],\ f(T) = T^r g(T) g(T^{-1}), g \in \mathbb{F}_\ell^{(r)}[T], \text{irréductible, non réciproque}\}.$$

Soit $f \in A_\ell$ et $g \in \mathbb{F}_\ell^{(r)}[T]$ irréductible non réciproque tel que $f(T) = T^r g(T) g(T^{-1})$. Posons $h(T) = T^r g(T^{-1})$. Alors $h \neq g$ est de degré $r$, irréductible, non réciproque et vérifie

$$T^r h(T) h(T^{-1}) = T^r g(T) g(T^{-1}) = f(T).$$

Ainsi, $|A_\ell| \leq \frac{1}{2} |\{h \in \mathbb{F}_\ell^{(r)}[T], \text{irréductible}\}|$.

On est donc ramené au calcul effectué dans la partie 2. On obtient

$$|X_{2r}| \ll r^2 (2N+1)^{r-1/2} (\log N).$$

# 4 Théorème de Gallagher

## 4.1 Outils de théorie de Galois

**Définition 4.1**

*Soient $k$ un corps et $L$ une extension algébrique de $k$. On dit que $L$ est une extension séparable de $k$ si tout élément de $L$ admet un polynôme minimal sans facteur carré.*

**Proposition 4.2**

*Soit $k$ un corps. Les assertions suivantes sont équivalentes :*
*(i) Tout polynôme irréductible de $k[T]$ est séparable ;*
*(ii) Toute extension algébrique de $k$ est séparable.*
*Un corps vérifiant ces conditions est dit parfait.*

▷ $(i) \Rightarrow (ii)$ : Soit $L$ une extension algébrique de $k$. Pour $x \in L$, le polynôme minimal de $x$ est irréductible donc séparable.

$(ii) \Rightarrow (i)$ : Soit $f$ un polynôme irréductible. Soit $L = k(\alpha)$ un corps de rupture de $f$ sur $k$. Alors $L$ est une extension algébrique de $k$ donc le polynôme minimal de $\alpha$ est séparable. Or c'est $f$ (à un inversible près). □

**Définition 4.3**

*Soient $L$ et $M$ deux extension d'un corps $k$. On appelle $k$-morphisme de $L$ dans $M$ tout morphisme (de corps) de $L$ dans $M$ laissant invariant chaque élément de $K$.*

**Définition 4.4**

*Soient $k$ un corps et $L$ une extension algébrique de $k$. En notant $\overline{k}$ une clôture algébrique de $k$, on dit que $L$ est une extension normale de $k$ si tout $k$-morphisme $\sigma : L \to \overline{k}$ est un $k$-automorphisme de $L$.*

**Proposition 4.5**

*Soient $k$ un corps et $f \in k[T]$. Alors le corps de décomposition $K_f$ de $f$ dans une clôture algébrique $\overline{k}/k$ est une extension normale de $k$.*

▷ Notons $\alpha_1, \ldots, \alpha_r$ les racines de $f$ de sorte que $K_f = k(\alpha_1, \ldots, \alpha_r)$. Soit $\sigma : K_f \to \overline{k}$ un $k$-morphisme. Comme $f \in k[T]$, on a

$$\forall x \in K_f, \qquad \sigma(f(x)) = f(\sigma(x))$$

donc, pour tout $1 \leq i \leq r$,

$$f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$$

donc il existe $1 \leq j \leq r$ tel que $\sigma(\alpha_i) = \alpha_j \in K_f$. Ainsi, $\sigma(K_f) \subset K_f$.

Alors, $[\sigma(K_f) : k] = [K_f : k] = [K_f : \sigma(K_f)][\sigma(K_f) : k]$ donc $[K_f : \sigma(K_f)] = 1$ soit $\sigma(K_f) = K_f$. □

**Définition 4.6**

*Soit $k$ un corps. Soit $L$ une extension de degré fini de $k$. Si $L$ est normale et séparable, alors $L$ est dite galoisienne finie.*

Des propositions précédentes on déduit le résultat suivant.

**Proposition 4.7**

*Soient $k$ un corps parfait et $f \in k[T]$. Alors le corps de décomposition $K_f$ de $k$ est une extension galoisienne finie de $k$.*

On aura besoin du lemme suivant

**Lemme 4.8**

*Soient $k$ un corps et $f \in k[T]$ un polynôme irréductible. Alors,*
*(i) $f$ est non séparable si et seulement si $f' = 0$ ;*
*(ii) si $k$ est de caractéristique $p$, $f$ est non séparable si et seulement si $f \in k[T^p]$.*

▷ (*i*) Si $f$ n'est pas séparable, alors il existe $\alpha$ tel que $f(\alpha) = f'(\alpha) = 0$. Le polynôme minimal $\mu$ de $\alpha$ divise donc $f$ et $f'$. Comme $f$ est irréductible, $f = \lambda\mu$ avec $\lambda \in k$ donc, en comparant les degré de $f'$ et $\mu$, $f' = 0$.

Réciproquement, si $f' = 0$ alors $f$ et $f'$ ont un zéro commun et $f$ n'est pas séparable.

(*ii*) Notons $f = a_r T^r + \cdots + a_1 T + a_0$ où $a_i \in k$. On a les équivalences suivantes :

$$\begin{aligned} f' = 0 &\iff \forall 1 \leq i \leq r,\ ia_i = 0 \\ &\iff \forall 1 \leq i \leq r,\ i = 0\ [p] \text{ ou } a_i = 0 \\ &\iff f = \sum b_j X^{pj} \end{aligned}$$

□

**Proposition 4.9**

*Soit $k$ un corps. Si $k$ est fini ou de caractéristique 0 alors $k$ est parfait.*

▷ D'après le lemme précédent, $f' = 0$. Comme $k$ est de caractéristique 0, on en déduit que $f \in k$ ce qui est absurde.

Supposons que $k$ est fini de caractéristique $p$. Alors $\mathcal{F} : x \mapsto x^p$ est un morphisme de corps, donc est injectif. Par égalité des cardinaux finis, $\mathcal{F}$ est bijectif. Soit $f \in k[T]$ un polynôme irréductible. D'après le lemme précédent $f = \sum_{j=0}^{n} b_j T^{pj}$. Comme $\mathcal{F}$ est bijectif, pour $1 \leq j \leq n$, il existe $a_j \in k$ tel que $b_j = a_j^p$. Alors,

$$f = \left( \sum_{j=0}^{n} a_j T^j \right)^p$$

ce qui contredit l'irréductibilité de $f$. □

Dans toute la suite, on fixe un corps parfait $k$.

**Définition 4.10**

*Soit $L$ une extension de $k$. On appelle groupe de Galois de $L$ sur $k$, et on note $Gal(L/k)$, l'ensemble des $k$-automorphismes de $L$.*

**Proposition 4.11**

*$Gal(L/k)$ est un groupe pour la loi de composition des applications.*

**Définition 4.12**

*Soit $f \in k[T]$ un polynôme de degré $r \geq 1$. On appelle groupe de Galois de $f$ sur $k$, et on note $Gal_k(f)$, le groupe de Galois "du" corps de décomposition $K_f$ de $f$ sur $k$ :*

$$Gal_k(f) = Gal(K_f/k).$$

**Proposition 4.13**

*Soit $f \in k[T]$ un polynôme de degré $r \geq 1$. On peut plonger $Gal_k(f)$ dans le groupe symétrique $\mathfrak{S}_r$.*

▷ Soit $K_f$ un corps de décomposition de $f$. Alors $K_f = k(\alpha_1, \ldots, \alpha_n)$ où $R = \{\alpha_1, \ldots, \alpha_n\}$ est l'ensemble des racines de $f$.

Soit $\sigma \in \mathrm{Gal}_k(f)$. Comme $\sigma$ est une bijection $K_f \to K_f$ , on obtient que $\sigma_{\restriction R}$ est une permutation de $R$. □

La connaissance du groupe de Galois permet en particulier de déterminer le caractère irréductible d'un polynôme comme le montre le théorème suivant [4].

**Théorème 4.14**

*Soit $f \in k[T]$ un polynôme unitaire séparable de degré $r \geq 2$. $f$ est irréductible sur $k$ si et seulement si $Gal_k(f)$ agit transitivement sur l'ensemble des racines $R$ de $f$ dans $K_f$.*

▷ Supposons que $f$ est irréductible. Soient $\alpha_i$ et $\alpha_j$ deux racines de $f$. $\alpha_i$ et $\alpha_j$ ont le même polynôme minimal $(f)$ donc il existe $\sigma \in \mathrm{Gal}(\Omega/k)$, où $\Omega$ est une clôture algébrique de $k$ (et $K_f$ à isomorphisme près), tel que $\alpha_j = \sigma(\alpha_i)$. Or peut montrer que la restriction de $\sigma$ à $K_f$ appartient à $\mathrm{Gal}(K_f/K)$. Ainsi, $\alpha_j = \tau(\alpha_i)$ avec $\tau \in \mathrm{Gal}(K_f/k)$. On a donc montré que $\mathrm{Gal}(K_f/k) = \mathrm{Gal}_k(f)$ agit transitivement sur $R$.

Supposons que $\mathrm{Gal}_k(f)$ agit transitivement sur $R$. Soit $g$ un facteur irréductible de $f$ dans $k[T]$. $g$ est scindé sur $K_f$. Soit $\alpha$ une racine de $g$ dans $K_f$, alors $\alpha \in R$. Comme l'action de $\mathrm{Gal}_k(f)$ sur $R$ est transitive, pour tout $1 \leq i \leq n$, il existe $\sigma_i \in \mathrm{Gal}_k(f)$ tel que $\alpha_i = \sigma_i(\alpha)$.

Alors, $g(\alpha_i) = g(\sigma_i(\alpha)) = \sigma_i(g(\alpha)) = \sigma_i(0) = 0$ donc $\alpha_i$ est racine de $g$. Ainsi, $f$ divise $g$ et donc $f = g$ est irréductible. □

**Définition 4.15**

*Soit $A$ un anneau, soit $f \in A[T]$ un polynôme de degré $r$. Soit $\alpha_1, \ldots, \alpha_r$ les racines de $f$ dans un corps de décomposition. On définit le discriminant de $f$ par*

$$d(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

**Théorème 4.16**

*Soit $A$ un anneau, soit $f \in A[T]$. On a*

$$d(f) \in A.$$

▷ On a

$$d(f) = \prod_{i<j}(\alpha_i - \alpha_j) = (-1)^{r(r-1)/2} \prod_{i \neq j}(\alpha_i - \alpha_j).$$

Or le polynôme

$$S = (-1)^{r(r-1)/2} \prod_{i \neq j}(T_i - T_j)$$

est un polynôme symétrique de $A[T_1, \ldots, T_r]$. D'après le résultat fondamental sur les polynômes symétriques, il existe $Q \in A[T_1, \ldots, T_r]$ tel que

$$S(T_1, \ldots, T_r) = Q(\Sigma_1, \ldots, \Sigma_r)$$

où les $\Sigma_i$ sont les polynômes symétriques élémentaires définis par :

$$\Sigma_i = \sum_{1 \leq n_1 \leq \cdots \leq n_i \leq r} T_{n_1} \ldots T_{n_i}.$$

En notant $\sigma_i = \Sigma_i(\alpha_1, \ldots, \alpha_r)$, on a

$$d(f) = S(\alpha_1, \ldots, \alpha_r) = Q(\sigma_1, \ldots, \sigma_r).$$

Or, les relations coefficients-racines s'écrivent, en notant $(a_i)_{0 \leq i < r}$ les coefficients de $f$,

$$\forall 1 \leq i \leq r, \qquad a_{r-i} = (-1)^i \sigma_i$$

donc

$$d(f) = Q(-a_{r-1}, a_{r-2}, \ldots, (-1)^r a_0) \in A.$$

□

Soient $f \in \mathbb{Z}[T]$ et $p$ un nombre premier. Soit $f_p$ le polynôme obtenu en réduisant les coefficients de $f$ modulo $p$. $d(f)$ étant un polynôme, à coefficients entiers, en les coefficients de $f$ donc on peut réduire $d(f) \in \mathbb{Z}$ et $d(f_p) = d(f)_p$ où $d(f)_p \equiv d(f) \bmod p$. En particulier, si $d(f_p) \neq 0$ alors $d(f) \neq 0$.

Cette observation permet d'obtenir des informations sur le groupe de Galois de $f$, à partir de sa réduction $f_p$, par le théorème suivant [7].

**Théorème 4.17**

*Soient $f \in \mathbb{Z}^{(r)}[T]$ et un nombre premier $p$ tel que $d(f_p) \neq 0$ ($f_p$ est à racines simples). Supposons que $f_p$ se factorise en $n_1$ facteurs irréductibles de degré 1, $n_2$ facteurs irréductibles de degré 2, …, $n_r$ facteur irréductible de degré $r$ ($n_1 + 2n_2 + \cdots + rn_r = r$). Alors le groupe de Galois de $f$, $Gal_{\mathbb{Q}}(f)$, contient une permutation dont la décomposition en*

*produit de cycles à support disjoints comprend $n_2$ transpositions, $n_3$ 3-cycles, ..., $n_r$ $r$-cycle (et laisse $n_1$ points fixes).*

**Définition 4.18**

*Lorsqu'une permutation $\sigma \in \mathfrak{S}_r$ se décompose en produit de $n_2$ transpositions, $n_3$ 3-cycles,...,$n_r$ $r$-cycle et laisse $n_1$ points fixes, on dit que $\sigma$ est de type $t = (n_1, \ldots, n_r)$.*

La preuve de ce résultat, s'appuie sur le théorème suivant.

**Théorème 4.19**

*Soient $f \in \mathbb{Z}^{(r)}[T]$, $K/\mathbb{Q}$ un corps de décomposition de $f$, $p$ un nombre premier et $K_p/\mathbb{F}_p$ un corps de décomposition de $f_p$. On suppose que $p$ est tel que $f_p$ est à racines simples dans le corps de décomposition $K_p/\mathbb{F}_p$. Soit $D$ le sous-anneau de $K$ engendré par les racines de $f$.*

*(i) Il existe des morphismes (unitaires) $\psi : D \to K_p$ ;*

*(ii) Un tel morphisme donne une bijection de l'ensemble $R$ des racines de $f$ dans $K$ sur l'ensemble $R_p$ des racines de $f_p$ dans $K_p$ ;*

*(iii) Si $\psi$ et $\psi'$ sont deux tels morphismes, alors $\psi' = \psi\sigma$ pour un $\sigma \in Gal(K/\mathbb{Q})$.*

▷ (*i*) On a $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ et $f(T) = \prod_{i=1}^{r}(T - \alpha_i)$ dans $K[T]$. Comme $d(f_p) \neq 0$, $d(f) \neq 0$ et les $\alpha_i$ sont distincts. On a $D = \mathbb{Z}[\alpha_1, \ldots, \alpha_r]$.

Soit $D' = \sum_{0 \leq \varepsilon_i \leq r-1} \mathbb{Z}\alpha_1^{\varepsilon_1} \ldots \alpha_r^{\varepsilon_r}$. Pour tout $1 \leq i \leq r$, $f(\alpha_i) = 0$ donc $\alpha_i^r$ s'écrit comme une combinaison linéaire à coefficients entiers de $1, \alpha_i, \ldots, \alpha_i^{r-1}$. Donc $\alpha_i D' \subset D'$, et en itérant, $\alpha_1^{m_1} \ldots \alpha_r^{m_r} D' \subset D'$ pour tous entiers $m_1, \ldots, m_r$. Ainsi, $D'$ est un sous-anneau de $D$ contenant les $\alpha_i$, donc $D' = D$.

$D$ est donc un $\mathbb{Z}$-module de type fini. Comme $K$ est de caractéristique nulle, $D$ est sans torsion. Ainsi, $D$ est un $\mathbb{Z}$-module libre. Notons $(u_1, \ldots, u_N)$ une base de $D$ :

$$D = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_N.$$

Montrons, ce qui nous sera utile au point (*iii*), que $(u_1, \ldots, u_N)$ est une base de $E/\mathbb{Q}$ (et donc $N = [E : \mathbb{Q}]$). La liberté sur $\mathbb{Q}$ est claire puisque qu'une relation de liaison à coefficients dans $\mathbb{Q}$ se ramène par multiplication par un entier non nul à une relation de liaison à coefficients dans $\mathbb{Z}$. De plus, $\mathbb{Q}D = \sum \mathbb{Q}u_i$ est un sous-anneau de $K$ contenant $\mathbb{Q}$. Soit $x \in \mathbb{Q}D$, $x \neq 0$. Alors $x \in K^\times$ est inversible dans $K$. Mais $x$ est algébrique sur $\mathbb{Q}$ donc $\mathbb{Q}(x) = \mathbb{Q}[x]$ et donc $x^{-1} \in \mathbb{Q}[x] \subset \mathbb{Q}D$. Ainsi, $\mathbb{Q}D$ est un sous-corps de $K$. Comme $\mathbb{Q}D$ contient les $\alpha_i$, $\mathbb{Q}D = K$ ce qui conclut.

Considérons désormais $pD = \sum_{i=1}^{N} p\mathbb{Z}u_i$. $pD$ est un idéal de $D$ et $\left|D/pD\right| = p^N$. Comme $D/pD$ est fini, il contient un idéal maximal, qui est de la forme $M/pD$ où $M$ est un idéal maximal de $D$ contenant $pD$. Alors, $D/M$ est un corps, image de $D/pD$ par un certain morphisme car

$$(D/pD)/(M/pD) \simeq D/M.$$

Comme $D/_{pD}$ est de caractéristique $p$, $D/_M$ également donc son sous-corps premier est $\mathbb{F}_p$ et $|D/_M| = p^m$ pour un $m \leq N$.

La projection canonique $\pi : D \to D/_M$ envoie $\mathbb{Z}$ sur le sous-corps premier donc

$$D/_M = \mathbb{F}_p[\overline{\alpha_1}, \ldots, \overline{\alpha_r}]$$

où $\overline{\alpha_i} = \pi(\alpha_i)$ et $\overline{f} = \prod_{i=1}^{r}(T - \overline{\alpha_i})$. De plus, comme $f$ est à coefficients dans $\mathbb{Z}$, on a en fait $\overline{f} = f_p$. Ainsi, $D/_M$ est un corps de décomposition de $f_p$ sur $\mathbb{F}_p$ donc on a un isomorphisme

$$\varphi : D/_M \xrightarrow{\sim} K_p.$$

Alors, en posant $\psi = \varphi \circ \pi$, on obtient un morphisme $D \to K_p$.

$(ii)$ Soit $\psi$ un morphisme de $D$ sur $K_p$. Alors, $\psi_{|\mathbb{Z}}$ est un morphisme $\mathbb{Z} \to \mathbb{F}_p$ et, comme $\psi(1) = 1_{\mathbb{F}_p}$, $\psi_{|\mathbb{Z}}$ est la projection canonique de $\mathbb{Z}$ dans $\mathbb{F}_p$. Ainsi,

$$f_p = \psi(f) = \prod_{i=1}^{r}(T - \psi(\alpha_i))$$

donc $\psi(\alpha_i)$ sont les racines de $f_p$ dans $K_p$ et donc $\psi_{|R}$ est une bijection de $R$ sur $R_p$.

$(iii)$ Soit $\psi$ un morphisme de $D$ sur $K_p$. Soit $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. $\sigma$ induit une permutation des $\alpha_i$ et donc $\sigma(D) = D$. Ainsi, $\sigma_{|D}$ est un automorphisme de $D$ et $\psi\sigma$ est un morphisme de $D$ dans $K_p$. Soient $\sigma \neq \sigma' \in \mathrm{Gal}(E/\mathbb{Q})$. Comme $\psi_{|R}$ est une bijection, $\psi\sigma \neq \psi\sigma'$. Ainsi, on obtient $[E : \mathbb{Q}]$ morphismes $\psi_j = \psi\sigma_j$, où $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{[E:\mathbb{Q}]}\}$. Par ailleurs, on peut montrer que $[E : \mathbb{Q}] = N$.

Montrons qu'il n'y en a pas d'autres. Supposons qu'il existe un tel morphisme $\psi_{N+1} \neq \psi_j$, $j = 1, \ldots, N$. Le système

$$\begin{cases} \sum_{i=1}^{N+1} x_i\psi_i(u_1) = 0 \\ \vdots \\ \sum_{i=1}^{N+1} x_i\psi_i(u_N) = 0 \end{cases}$$

possède plus d'inconnues que de lignes, donc il possède une solution non triviale $(a_1, \ldots, a_{N+1})$, $a_i \in K_p$. Ainsi,

$$\forall 1 \leq j \leq N, \qquad \sum_{i=1}^{N+1} a_i\psi_i(u_j) = 0$$

d'où,

$$\sum_{i=1}^{N+1} a_i\psi_i = 0$$

ce qui contredit le lemme suivant [4], d'où le résultat. □

**Lemme 4.20 (*Dedekind*)**

*Soient $K$ un corps et $G$ un groupe. Les caractères de $G$ à valeurs dans $K^*$ sont $K$-linéairement indépendants.*

▷ On montre par récurrence sur $n \in \mathbb{N}^*$ que $n$ caractères distincts sont linéairement indépendants.

– $n = 1$. La propriété est vraie puisque les caractères ne sont pas nuls.

– Soit $n \in \mathbb{N}^*$. Supposons le résultat vrai pour $n-1$ caractères distincts. Soient $\chi_1, \dots, \chi_n$ $n$ caractères distincts et $\lambda_1, \dots, \lambda_n \in K$ tels que

$$\sum_{i=1}^{n} \lambda_k \chi_k = 0.$$

Alors, pour $g, h \in G$

$$\sum_{i=1}^{n} \lambda_i \chi_i(gh) = \sum_{i=1}^{n} \lambda_i \chi_i(g)\chi_i(h) = 0.$$

et

$$\sum_{i=1}^{n} \lambda_i \chi_i(g)\chi_n(h) = \left( \sum_{i=1}^{n} \lambda_i \chi_i(g) \right) \chi_i(h) = 0.$$

On en déduit que

$$\sum_{i=1}^{n-1} \lambda_i \chi_i(g)(\chi_n(h) - \chi_i(h)) = 0.$$

On en déduit, comme $K$ est commutatif,

$$\forall h \in G, \qquad \sum_{i=1}^{n-1} \lambda_i (\chi_n(h) - \chi_i(y))\chi_i = 0.$$

Par hypothèse de récurrence, $(\chi_i)_{1 \leq i \leq n-1}$ est une famille $K$-linéairement indépendante donc

$$\forall 1 \leq i \leq n-1, \forall g \in G, \qquad \lambda_i(\chi_n(g) - \chi_i(g)) = 0.$$

Or, pour chaque $1 \leq i \leq n-1$, $\chi_i \neq \chi_n$ donc il existe $g \in G$ tel que $\chi_n(g) - \chi_i(g) \neq 0$. Ainsi, $\lambda_1 = \cdots = \lambda_{n-1} = 0$. En reportant dans

$$\sum_{i=1}^{n} \lambda_i \chi_i = 0$$

il vient $\lambda_n \chi_n = 0$ d'où $\lambda_n = 0$. □

On peut désormais démontrer le théorème 4.17. En effet, puisque $K_p$ est un corps à $p^m$ éléments, $\varphi : a \mapsto a^p$ est un automorphisme. Si $\psi : D \to K_p$ est un morphisme, alors $\varphi\psi$ également. Il existe donc un unique $\sigma$ tel que

$$\varphi\psi = \psi\sigma.$$

Comme $\psi_{|R}$ est une bijection,

$$\sigma_{|R} = \psi^{-1}\varphi\psi_{|R}$$

donc les orbites de $R_p$ par $\langle\varphi\rangle$ sont envoyés par ${\psi_{|R}}^{-1}$ sur les orbites de $R$ par $\langle\sigma\rangle$. Or on vérifie que les orbites de $R_p$ par $\langle\varphi\rangle$ sont les ensembles de racines des facteurs irréductibles de $f_p$. Donc les orbites de $R$ par $\langle\sigma\rangle$ ont les mêmes cardinaux, d'où le résultat.

## 4.2 Résultats sur le groupe symétrique

Comme nous l'avons vu ci-dessus, le type d'une permutation du groupe de Galois d'un polynôme est lié à sa factorisation. On a les résultats suivant.

**Théorème 4.21**

*Deux permutations sont conjuguées dans $\mathfrak{S}_r$ si et seulement si elles ont même type.*

▷ La preuve repose sur le calcul

$$\tau(i_1 \dots i_n)\tau^{-1} = (\tau(i_1) \dots \tau(i_n))$$

pour tout $\tau \in \mathfrak{S}_r$ et $i_1, \dots, i_n$ des éléments distincts de $[\![1, r]\!]$. □

**Théorème 4.22**

*Soit $c$ une classe de conjugaison de $\mathfrak{S}_r$, décrite par le type $t = (n_1, \dots, n_r)$. Alors*

$$|c| = r! \prod_{i=1}^{r} \frac{1}{i^{n_i} n_i!}.$$

On aura besoin du lemme suivant

**Lemme 4.23**

*Soit $G$ un groupe. Soit $g \in G$. Soit $c$ la classe de conjugaison de $g$. Alors*

$$|c| = [G : C_G(g)]$$

*où $C_G(g) = \{h \in G, gh = hg\}$ est le centralisateur de $g$.*

▷ Notons $G/C_G(g)$ l'ensemble des classes à gauche modulo $C_G(g)$. On pose

$$f : \begin{array}{rcl} c & \to & G/C_G(g) \\ hgh^{-1} & \mapsto & hC_G(g). \end{array}$$

$f$ est bien définie car si $h_1 g h_1^{-1} = h_2 g h_2^{-1}$ alors

$$h_2^{-1} h_1 g h_1^{-1} h_2 = g$$

donc $h_2^{-1} h_1$ commute avec $g$, *ie.* $h_2^{-1} h_1 \in C_G(g)$ et donc $h_1 C_G(g) = h_2 C_G(g)$.

$f$ est injective. En effet, si $h_1 C_G(g) = f(h_1 g h_1^{-1}) = f(h_2 g h_2^{-1}) = h_2 C_G(g)$ alors $h_2^{-1} h_1$ commute avec $g$ et donc $h_2^{-1} h_1 g h_1^{-1} h_2 = g$ soit $h_1 g h_1^{-1} = h_2 g h_2^{-1}$.

$f$ est surjective. En effet, si $h \in G$, alors $hC_G(g) = f(hgh^{-1})$.

$f$ est donc une bijection et

$$|c| = \left| G/C_G(g) \right| = [G : C_G(g)].$$

□

Pour démontrer le théorème, on calcule donc le cardinal du centralisateur d'une permutation $\sigma \in c$ et on en déduit

$$|c| = \frac{|\mathfrak{S}_r|}{|C_{\mathfrak{S}_r}(\sigma)|}$$

Prenons en exemple le cas des cycles. Soit $\sigma = (i_1 \dots i_k)$ un $k$-cycle. Soit $\tau \in C_{\mathfrak{S}_r}(\sigma)$. Comme $\tau\sigma\tau^{-1} = \sigma$, on a

$$(\tau(i_1) \dots \tau(i_k)) = (i_1 \dots i_k).$$

Ainsi, l'ensemble des points fixes de $\sigma$ doit être stable par $\tau$. Ainsi, il y a $(r-k)!$ possibilités pour leur attribuer une image. De plus, la permutation $(\tau(i_1) \dots \tau(i_k)) = (i_1 \dots i_k)$ est uniquement déterminée par l'image de $i_1$. Ainsi, on a $k$ possibilités. On conclut donc que

$$|C_{\mathfrak{S}_r}(\sigma)| = k(r-k)!.$$

Soit $\sigma \in \mathfrak{S}_r$ une permutation de type $t = (n_1, \dots, n_r)$. Notons

$$\sigma = (\sigma_1^{(2)} \dots \sigma_{n_2}^{(2)}) \dots (\sigma_{n_r}^{(r)})$$

une décomposition de $\sigma$ en cycle à support disjoints (écrits dans l'ordre croissant de longueur). Soit $\tau \in C_{\mathfrak{S}_r}(\sigma)$. Comme $\tau\sigma\tau^{-1} = \sigma$, pour chaque $j = 2 \dots r$ et chaque $1 \leq k \leq n_j$ il existe un $1 \leq m \leq n_j$ tel que

$$\tau\sigma_k^{(j)}\tau^{-1} = \sigma_m^{(j)}.$$

Il y a $n_j$ cycles à permuter, et pour une permutation donnée, il y a $j$ possibilités pour le faire, comme on l'a vu dans l'exemple ci-dessus. Ainsi, pour chaque longueur, on a $n_j! j^{n_j}$ possibilités pour $\tau$. Comme les cycles sont à supports disjoints, on en conclut que

$$|C_{\mathfrak{S}_r}(\sigma)| = \prod_{i=1}^{r} i^{n_i} n_i!.$$

**Théorème 4.24**

*Soient $G$ un sous-groupe de $\mathfrak{S}_r$ et $p > \frac{r}{2}$ un nombre premier. S'il existe $\sigma \in G$ tel que la décomposition de $\sigma$ en cycles à supports disjoints contient un $p$-cycle, alors $G$ contient un $p$-cycle.*

▷ Notons $\sigma = \sigma_1 \circ \dots \circ \sigma_k \circ \tau_p$ la décomposition de $\sigma$ en cycle à support disjoints, avec $\tau_p$ un cycle d'ordre $p$. $\sigma_1, \dots, \sigma_k$ sont des permutations d'ordre $\omega_i < p$ donc $\omega = \omega_1 \dots \omega_k$ et $p$ sont premiers entre eux. On en déduit que $\sigma^\omega \in G$ est un $p$-cycle. □

On énonce enfin un résultat démontré par Knutson et cité par Gallagher [3].

**Théorème 4.25**

*Soit $G$ un sous-groupe de $\mathfrak{S}_r$. Si $G$ est transitif, contient une transposition et un $p$-cycle pour un nombre premier $p > \frac{r}{2}$, alors $G = \mathfrak{S}_r$.*

$\triangleright$ On considère le graphe de nœuds 1,2,...,$n$ et d'arêtes correspondantes aux transpositions $(ij)$ contenues dans $G$. Comme $\mathfrak{S}_r$ est engendré par les transpositions, il suffit de montrer que le graphe est complet (*ie.* il existe une arête entre chaque nœud).

Si $(ij)$ et $(jk)$ appartiennent à $G$, alors $(ik) = (ij)(jk)(ij) \in G$. Ainsi, chaque composante connexe du graphe est un graphe complet.

Or $G$ agit transitivement sur chaque composante connexe. Elles sont donc isomorphes, de même cardinal $d|r$.

Si le $p$-cycle contenu dans $G$ ne laisse pas stable chaque composante connexe, alors il y a au moins $p$ composantes et donc $dp \leq r$, d'où $d = 1$. Ceci est absurde car le graphe contient une arête. Ainsi, le $p$-cycle stabilise chaque composante donc $d \geq p$ et donc $d = r$. Le graphe est donc connexe, et donc complet. $\square$

## 4.3 Énoncé du théorème

**Théorème 4.26 (*Gallagher*)**

*Soit $r \geq 1$ un entier. Pour tout entier $N \geq 1$, définissons $E_r(N)$ comme l'ensemble des polynômes $f \in \mathbb{Z}[T]$ unitaires de degré $r$ tels que*

$$f = T^r + a_{r-1}T^{r-1} + \cdots + a_1T + a_0$$

*avec $|a_i| \leq N$ pour tout $0 \leq i < r$ et tels que le groupe de Galois de $f$ n'est pas isomorphe au groupe symétrique $\mathfrak{S}_r$. Alors*

$$|E_r(N)| \ll r^3(2N+1)^{r-\frac{1}{2}}(\log N)$$

*pour $N \geq 2$, où la constante sous-entendue est absolue.*

On suit à nouveau le schéma de preuve de Kowalski [9]. On se place dans le cadre

$$Y = \mathbb{Z}^{(r)}[T],\ \Lambda = \mathbb{P},\ Y_\ell = \mathbb{F}_\ell^{(r)}[T],\ \rho_\ell : \mathbb{Z}^{(r)}[T] \twoheadrightarrow \mathbb{F}_\ell^{(r)}[T];$$

$$X = \{(a_0, \ldots, a_{r-1}),\ |a_i| \leq N\ \forall 0 \leq i < r\} \text{ et } F : X \to Y;$$

$$\mathcal{L}^* = \{\ell \in \mathbb{P}, \ell \leq L\} \text{ pour un entier } L \geq 2;$$

$$\forall f \in \mathbb{F}_\ell^{(r)}[T], \qquad \nu_\ell(f) = \frac{1}{|\mathbb{F}_\ell^{(r)}[T]|} = \frac{1}{\ell^r};$$

pour $c$ une classe de conjugaison de $\mathfrak{S}_r$, décrite par le type $t = (n_1, \ldots, n_r)$ des permutation quelle contient, on pose

$$\Omega_{\ell,c} = \{f \in \mathbb{F}_\ell^{(r)}[T], f = f_1 \ldots f_r\}$$

où, pour $1 \leq i \leq r$, $f_i$ est produit de $n_i$ polynômes irréductibles unitaires de degré $i$. On dit qu'un tel $f$ factorise avec type $t$.

D'après le théorème 4.17,

$$E_r(N) \subset \bigcup_{c \in \mathfrak{S}_r^\#} S(X, \Omega_c, \mathcal{L}^*)$$

où $\mathfrak{S}_r^{\#}$ est l'ensemble des classes de conjugaison de $\mathfrak{S}_r$.

On pourrait se servir de cette inclusion pour démontrer le résultat, mais on ne pourrait obtenir l'uniformité (en $r$), de la constante sous-entendue (on obtiendrait seulement du $r!$). L'idée est de se restreindre à des classes de conjugaisons suffisamment grandes pour qu'un sous-groupe propre de $\mathfrak{S}_r$ ne puisse contenir un élément de chacune des classes choisies. On se sert donc des théorèmes 4.24 et 4.25. Comme le groupe de Galois d'un polynôme agit transitivement sur les racines si et seulement si le polynôme est irréductible, on peut se limiter aux ensembles $C1$ et $C_2$ où $C_1$ est la classe des éléments dont la décomposition en cycles à supports disjoints contient une seule transposition et pas d'autre cycle de longueur paire, et $C_2$ est l'union des classes des éléments dont la décomposition en cycles à supports disjoints contient un cycle d'ordre premier $p > \frac{r}{2}$. Ainsi,

$$E_r(N) \subset \{f \in \mathbb{Z}^{(r)}[T], |a_i| \leq N, \text{réductible}\} \cup S(X, \Omega^1, \mathcal{L}^*) \cup S(X, \Omega^2, \mathcal{L}^*)$$

où $\Omega_\ell^i$ est l'ensemble des polynômes unitaires de degré $r$ de $\mathbb{F}_\ell[T]$ qui factorisent avec type défini par un élément de $C_i$.

## 4.4 Dénombrement des polynômes de $\mathbb{F}_\ell[T]$ de degré $r$ factorisant avec type $t$ donné

On montre l'encadrement suivant [9], qui généralise le résultat démontré dans la partie 2.3.

**Théorème 4.27**

*Soient $\ell$ un nombre premier et $r \geq 1$ un entier. Soient $n_1, \ldots, n_r \geq 0$ des entiers tels que*

$$r = n_1 + 2n_2 + \cdots + rn_r.$$

*Le cardinal de l'ensemble $\Omega_{\ell,c}$ des polynômes $f \in \mathbb{F}_\ell^{(r)}[T]$ factorisant avec type $(n_1, \ldots, n_r)$ (décrivant la classe de conjugaison $c \subset \mathfrak{S}_r$) vérifie*

$$\frac{|c|}{|\mathfrak{S}_r|}\ell^r \left(1 - \frac{1}{\ell}\right)^{2n_2+n_3+\cdots+n_r} \left(1 - \frac{1}{\sqrt{l}}\right)^{n_1} \leq |\Omega_{\ell,c}| \leq \frac{|c|}{|\mathfrak{S}_r|}\ell^r$$

*pour tout $\ell > r^2$, et pour $\ell > 4r$ si $n_1 = 0$, avec*

$$|c| = r! \prod_{i=1}^{r} \frac{1}{i^{n_i} n_i!}.$$

▷ On a

$$|\Omega_{\ell,c}| = \prod_{i=1}^{r} \binom{m_i}{n_i}$$

où $m_i$ est le nombre de polynômes unitaires irréductibles de degré $i$ sur $\mathbb{F}_\ell$. On a vu dans la partie 2.2 que

$$m_i = \frac{1}{i} \sum_{d|i} \mu(d) \ell^{i/d} \leq \frac{\ell^i}{i}$$

d'où

$$\binom{m_i}{n_i} \leq \frac{1}{n_i!}\left(\frac{\ell^i}{i}\right)^{n_i}.$$

En multipliant toutes ces inégalités, on obtient la majoration souhaitée.

Par ailleurs, pour tout $\ell > r^2$, on a

$$m_1 = \ell \geq \ell\left(1 - \frac{1}{\sqrt{\ell}}\right) + r - 1.$$

De plus

$$m_2 = \frac{1}{2}\ell(\ell-1) \geq \frac{1}{2}(\ell-1)^2 + \frac{r}{2} - 1$$

pour $\ell \geq r$.

Pour $i \geq 3$, on a

$$m_i = \frac{\ell^i}{i} + \frac{1}{i}\sum_{\substack{d|i \\ d<i}} \mu(d)\ell^{i/d} \geq \frac{\ell^i}{i} - \frac{\ell^{i/2}}{i}\sum_{d<i} 1 \geq \frac{\ell^i}{i} - \ell^{i/2}.$$

Or, pour $i \geq 4$ et $\ell > 2r$,

$$\frac{\ell^{i-1}}{i} \underset{\ell>2r}{>} 2\ell^{i-2} \underset{i\geq 4}{\geq} \ell^{i/2} + \ell^{i-2} \geq \ell^{i/2} + \ell \geq \ell^{i/2} + \frac{r}{i}$$

et l'inégalité est valable pour $\ell > 4r$ et $i = 3$ (et donc $r \geq 3$). En effet, on montre que la fonction

$$\ell \mapsto \frac{\ell^2}{3} - \ell^{3/2} - \frac{r}{3}$$

est croissante sur $[6, +\infty[$ donc, pour $\ell > 4r > 6$, il suffit de vérifier que

$$\frac{16r^2}{3} - (4r)^{3/2} - \frac{r}{3} \geq 0.$$

Ainsi, pour tout $i \geq 3$, $\ell > 4r$,

$$m_i \geq \frac{\ell^i}{i}\left(1 - \frac{1}{\ell}\right) + \frac{r}{i} - 1.$$

On en déduit que, pour $\ell > 4r$, $3 \leq i \leq r$ et $n_i \leq \frac{r}{i}$,

$$\binom{m_i}{n_i} = \frac{m_i(m_i-1)\dots(m_i-n_i+1)}{n_i!} \geq \frac{(m_i - \frac{r}{i}+1)^{n_i}}{n_i!} \geq \left(1-\frac{1}{\ell}\right)^{n_i}\frac{\ell^{in_i}}{i^{n_i}n_i!};$$

pour $\ell > r^2$, $i = 1$ et $n_1 \leq r$

$$\binom{m_1}{n_1} = \frac{m_1(m_1-1)\dots(m_1-n_1+1)}{n_1!} \geq \frac{(m_1 - r+1)^{n_1}}{n_1!} \geq \left(1-\frac{1}{\sqrt{\ell}}\right)^{n_1}\frac{\ell^{n_1}}{n_1!};$$

et pour $\ell \geq r$, $i = 2$ et $n_2 \leq \frac{r}{2}$,

$$\binom{m_2}{n_2} \geq \frac{(m_2 - \frac{r}{2}+1)^{n_2}}{n_2!} \geq \left(1-\frac{1}{\ell}\right)^{2n_2}\frac{\ell^{2n_2}}{2^{n_2}n_2!}.$$

Ainsi,

$$|\Omega_{\ell,c}| \geq \left(1-\frac{1}{\sqrt{\ell}}\right)^{n_1}\left(1-\frac{1}{\ell}\right)^{2n_2+n_3+\cdots+n_r}\left(\prod_{i=1}^{r}\frac{1}{i^{n_i}n_i!}\right)\ell^{\sum in_i}$$

soit

$$|\Omega_{\ell,c}| \geq \frac{|c|}{|\mathfrak{S}_r|}\left(1-\frac{1}{\sqrt{\ell}}\right)^{n_1}\left(1-\frac{1}{\ell}\right)^{2n_2+n_3+\cdots+n_r}\ell^r.$$

□

En particulier, on déduit de ce résultat que

$$\frac{|\Omega_{\ell,c}|}{|\mathbb{F}_\ell^{(r)}[T]|} \geq \frac{|c|}{|\mathfrak{S}_r|}.$$

### 4.5 Minoration de $P^i(L)$

On applique ce qui précède pour minorer $|\Omega_\ell^1|$ et $|\Omega_\ell^2|$.
D'après la partie précédente, pour $\ell > r^2$,

$$\frac{|\Omega_\ell^1|}{\ell^r} \gg \sum_{\substack{n_1+2n_2+\cdots+rn_r=r\\ n_2=1,n_4=n_6=\cdots=0}}\prod_{i=1}^{r}\frac{1}{i^{n_i}n_i!}.$$

Or le membre de droite est le coefficient de $x^{r-2}$ dans le développement en série entière de

$$\exp\left(x+\frac{x^3}{3}+\frac{x^5}{5}+\dots\right).$$

Comme

$$\exp\left(x+\frac{x^3}{3}+\frac{x^5}{5}+\dots\right) = \sqrt{\frac{1+x}{1-x}} = (1+x)(1-x^2)^{-1/2} = (1+x)\sum_{k=0}^{+\infty}\frac{(2k)!}{4^k k!^2}x^{2k},$$

c'est également la moitié du coefficient de $x^{2k}$ dans la dernière somme, avec $2k = r-2$ ou $r-3$ selon la parité de $r$. Avec la formule de Stirling, on en déduit

$$\frac{|\Omega_\ell^1|}{\ell^r} \gg (2\pi r)^{-1/2}.$$

Ainsi,

$$P^1(L) = \sum_{\ell\leq L}\frac{|\Omega_\ell^1|}{\ell^r} \gg \frac{L}{\sqrt{r}\log L}.$$

Par ailleurs,

$$\frac{|\Omega_\ell^2|}{\ell^r} = \sum_{\frac{r}{2}<p\leq r}\frac{|\{\sigma\in\mathfrak{S}_r,\ \sigma\text{contient un } p\text{-cycle}\}|}{r!} = \sum_{\frac{r}{2}<p\leq r}\frac{1}{r!}\binom{r}{p}(r-p)! = \sum_{\frac{r}{2}<p\leq r}\frac{1}{p}.$$

Ainsi, par le théorème 2.7,

$$\frac{|\Omega_\ell^2|}{\ell^r} \gg \log\left(\frac{\log r}{\log r - \log 2}\right) \gg \log\left(1 + \frac{\log 2}{\log r}\right) \gg \frac{\log 2}{\log r}.$$

On en déduit donc que

$$P^2(L) = \sum_{\ell \leq L} \frac{|\Omega_\ell^2|}{\ell^r} \gg \frac{L}{\log r \log L}.$$

## 4.6 Conclusion

On rappelle l'inclusion

$$E_r(N) \subset \{f \in \mathbb{Z}^{(r)}[T], |a_i| \leq N, \text{réductible}\} \cup S(X, \Omega^1, \mathcal{L}^*) \cup S(X, \Omega^2, \mathcal{L}^*),$$

On suppose $\sqrt{2N+1} > r^3$ et on pose $L = \frac{\sqrt{2N+1}}{r} > r^2$. Alors,

$$|E_r(N)| \ll (r^2 + r^{3/2} + r\log r)(2N+1)^{r-1/2}(\log N) \ll r^3(2N+1)^{r-1/2}(\log N).$$

Si $\sqrt{2N+1} < r^3$, alors

$$r^3(2N+1)^{r-1/2}(\log N) > (2N+1)^r(\log N) > |\{f, |a_i| \leq N\}| \geq |E_r(N)|$$

et l'estimation est encore vraie.

## Références


[1] H. Davenport E. Bombieri. On the large sieve method. In Paul Turán, editor, *Number Theory and Analysis*, pages 9–22. Plenum Press, 1969.

[2] Jean-Michel Ferrard. Inégalités de Chebyshev et applications. `www.mathprepa.fr-pb-approfondissement-inegalites_chebyshev_et_applications.pdf`.

[3] P. X. Gallgher. The large sieve and probabilistic galois theory. *American Mathematical Society*, Proc. Sympos. Pure Math.(Vol XXIV) :91–101, 1973.

[4] Ivan Goazrd. *Théorie de Galois*. Ellipses, 2009.

[5] W. Gotz H. Meyn. Self-reciprocal Polynomials Over Finite Fields. `http://www.emis.de/journals/SLC/opapers/s21meyn.pdf`.

[6] M. N. Huxley. The large sieve inequality for algebraic number fields. *Mathematika 15*, pages 178–187, 1968.

[7] Nathan Jacobson. *Basic Algebra I*. W.H. Freeman, 1985.

[8] R. Hyon-Chol K. Ryul, S. Ok-Hyon. Some properties of generalized self-reciprocal polynomials over finite fields. `http://arxiv.org/pdf/1302.3051.pdf`.

[9] E. Kowalski. *The Large Sieve and its Applications : Arithmetic Geometry, Random Walks and Discrete Groups*. Cambridge University Press, 2008.

[10] Matieu Vienney. Corps finis. `http://www.umpa.ens-lyon.fr/~mvienney/agreg/corps_finis.pdf`.