Université de Bordeaux
Département de Mathématiques

Rapport de stage de fin de licence 3

Introduction à la théorie analytique des nombres

Théorèmes de Gallagher

Présenté par :
Théo Gherdaoui

Encadré par :
Florent Jouve

Année universitaire 2018-2019

Sommaire

Je tiens premièrement à remercier très chaleureusement toutes les personnes qui se sont investies et qui ont contribué au bon déroulement de mon stage.

Je tiens plus particulièrement à remercier Florent Jouve, mon maître de stage, qui s'est montré très disponible, accueillant, et dévoué, qui a su m'aider, m'accorder du temps, mais aussi me laisser travailler en autonomie. Je tiens également à souligner l'investissement indéfectible des autres membres de l'université de Bordeaux, notamment Cyril, le responsable de la BMI, qui s'est toujours montré très prévenant, et efficace.

Je tiens enfin à remercier Simon, pour l'hébergement sur Bordeaux, les moments passés ensemble, et les conseils précieux qu'il a su m'apporter quant à la rédaction de ce rapport, Ophélie, mon ancienne colocataire et élève au magistère d'Orsay, ainsi que mes parents, pour la relecture de ce document.

Ce rapport est le fruit du travail que j'ai produit au cours de mon stage de fin de licence 3, qui a été effectué à l'université de Bordeaux, durant 4 semaines, sous la tutelle de Florent Jouve. J'y ai partagé le quotidien des chercheurs, mais j'ai aussi assisté à un cours, dispensé par mon tuteur de stage, intitulé : Graphes expanseurs et propriétés d'écart spectral, qui rejoignait de près le thème de mes recherches. Vous pouvez retrouver le descriptif du cours ici : https ://www.adum.fr/script/formations.pl ?mod=200735&site=edmi. J'ai enfin pu assister à certaines conférences Iwasawa, qui avaient lieu à Bordeaux, fin juin.

L'objectif principal de ce stage a été de démontrer le résultat suivi, énoncé par Gallagher en 1973 :

Théorème

Soient N et r deux entiers naturels, $r > 2$.
Définissons :

$$E_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N, \text{réductible sur } \mathbb{Q} \right\}$$

$$X_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N \right\}$$

Alors,

$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq C r^2 \frac{\ln(N)}{\sqrt{2N+1}}$$

où C est une constante absolue.

La deuxième partie de ce rapport est consacrée à un raffinement de ce résultat, qui utilise la théorie de Galois, et qui fait le lien entre la décomposition en produit d'irréductibles d'un polynôme, et son corps de décomposition.

Théorème

Soient N et r deux entiers naturels, $r > 2$.
Définissons :

$$E_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N,\ \text{tel que } Gal_{\mathbb{Q}}(f) \ncong \mathfrak{S}_r \right\}$$

$$X_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N \right\}$$

Alors,

$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq C r^3 \frac{\ln(N)}{\sqrt{2N+1}}$$

où C est une constante absolue.

1 Principe du grand crible

1.1 Premières définitions - axiomatiques

Définition 1. *On appelle crible, tout ensemble de deux triplets : $\psi = (Y, \Lambda, (\rho_l))$ où*

- *Y est un ensemble.*
- *Λ est un ensemble d'indices.*
- *$\forall l \in \Lambda$, $\rho_l : Y \to Y_l$ est surjective et Y_l est un ensemble fini.*

et $\gamma = (X, \mu, F)$ où :

- *(X, μ) est un espace mesuré de mesure finie.*
- *$F : X \to Y$, rendant les composées $p_l \circ F$ mesurables.*

On appelle support premier du crible, un sous-ensemble $\mathcal{L}^*$ de Λ, fini. On se donne enfin une famille d'ensembles $\Omega := (\Omega_l)_{l \in \mathcal{L}^*}$, où, $\forall l \in \mathcal{L}^*, \Omega_l \subseteq Y_l$. Il s'agit alors d'estimer la mesure de l'ensemble :

$$S(X, \Omega, \mathcal{L}^*) := \{x \in X \mid \forall l \in \mathcal{L}^*,\ \rho_l(F(x)) \notin \Omega_l\}$$

Nous nous attacherons dans toute la suite à illustrer les outils développés à l'aide d'un exemple fil-rouge, qui est le suivant :

Exemple. *Considérons $Y = \mathbb{Z}$, $\Lambda = \mathbb{P}$*
$\forall l \in \mathbb{P}, \rho_l : \mathbb{Z} \to \mathbb{Z}/l\mathbb{Z}$ est le morphisme associant à un élément sa classe mod l.
$X = [|M; M + N|]$ et μ est la mesure de comptage. F est l'application identité, $\mathcal{L}^*$ est un ensemble fini de nombres premiers et $\forall l \in \mathcal{L}^*$, $\Omega_l = \{0\}$. Alors :

$$S(X, \Omega, \mathcal{L}^*) := \{x \in [|M; M + N|] \mid \forall l \in \mathcal{L}^*,\ x \not\equiv 0[l]\}$$

C'est l'ensemble des entiers d'un certain intervalle qui n'admettent aucun des éléments de $\mathcal{L}^*$ dans leur décomposition en produit de facteurs premiers.

Notation. *On notera $S(\Lambda)$ l'ensemble des parties finies de Λ. Il correspond dans le cas exposé précédemment aux entiers sans facteur carré.*
Notons $l|m$ pour $l \in m$ et $m \in S(\Lambda)$. Nous considérons enfin $\mathcal{L}$ les sous-ensembles (finis) de $\mathcal{L}^*$. C'est ici l'ensemble de tous les entiers sans facteur carré, seulement divisibles par les premiers de $\mathcal{L}^*$.

Définition 2. *Soit X un ensemble fini. On appelle densité sur X toute application v, définie sur X à valeurs dans $[0; 1]$ vérifiant :*

- *$\forall x \in X, v(x) > 0$*
- *$\sum_{x \in X} v(x) = 1$*

Proposition 1. *Soit $l \in \Lambda$, et v_l une densité sur Y_l.*
L'application $(.|.) := \begin{cases} \mathcal{F}(Y_l, \mathbb{C})^2 \to \mathbb{C} \\ (f, g) \mapsto \sum_{y \in Y_l} v_l(y) f(y) \overline{g(y)} \end{cases}$ munit $\mathcal{F}(Y_l, \mathbb{C})$ d'un produit scalaire hermitien.

Démonstration. La quantité est bien définie puisque, par hypothèse, Y_l est fini. L'application est trivialement linéaire en la première variable, et semi-linéaire en la seconde, par linéarité de la somme. Elle est donc sesquilinéaire.
De plus, $\forall f, g \in \mathcal{F}(Y_l, \mathbb{C})$ $\overline{(f|g)} = \overline{\sum_{y\in Y_l} v_l(y)f(y)\overline{g(y)}} = \sum_{y\in Y_l} v_l(y)\overline{f(y)}g(y) = (g|f)$ puisque v_l est à valeurs réelles. Étant à valeurs dans un corps, c'est une forme hermitienne.
Enfin, $\forall f \in \mathcal{F}(Y_l, \mathbb{C}), (f|f) = \sum_{y\in Y_l} v_l(y)|f(y)|^2$, qui est une quantité positive, et v_l ne s'annulant pas, on en déduit que l'application est définie positive, ce qui en fait un produit hermitien. □

Proposition 2. *Soit $l \in \Lambda$, et v_l une densité sur Y_l. L'espace $\mathcal{L}^2(Y_l, v_l) := (\mathcal{F}(Y_l, \mathbb{C}), (.|.))$ est un espace de Hilbert.*

Démonstration. L'ensemble $\mathcal{F}(Y_l, \mathbb{C})$ est bien un espace-vectoriel, et l'application $(.|.)$ est un produit scalaire sur cet espace d'après la propositon 1. Montrons qu'il est complet pour la norme (notée N) associée au produit scalaire.
Soit $(f_n)_{n\in\mathbb{N}}$ une suite de Cauchy de $(\mathcal{F}(Y_l, \mathbb{C}), N)$. Alors :

$$(*) : \forall \epsilon > 0, \exists n_o \in \mathbb{N}/\forall n \geq n_o, \forall p \geq n_o, N(f_n - f_p) \leq \frac{\epsilon}{\sqrt{\sum_{y\in Y_l} \frac{1}{v_l(y)}}} := \epsilon'$$

donc,

$$\sum_{y\in Y_l} v_l(y)|f_n - f_p|^2(y) \leq \epsilon'^2$$

$$\forall y \in Y_l,\ |f_n(y) - f_p(y)| \leq \sum_{y\in Y_l} \frac{1}{\sqrt{v_l(y)}}.\sqrt{v_l(y)}|f_n - f_p|(y) \underset{C.S}{\leq} \sqrt{\sum_{y\in Y_l} \frac{1}{v_l(y)}}.\epsilon' = \epsilon$$

Par suite, $(f_n(y))_{n\in\mathbb{N}}$ est une suite de Cauchy à valeurs dans $\mathbb{C}$ qui est complet donc elle converge. $\forall y \in Y_l$, notons $f(y) := \lim_{n\to+\infty} f_n(y)$. f appartient à $\mathcal{F}(Y_l, \mathbb{C})$. Vérifions enfin que la convergence a lieu en norme N : il suffit de faire tendre p vers $+\infty$ dans la relation $(*)$. □

Notation. *Dans la suite, lorsque l'on note $\mathcal{L}^2(X, \mu)$, alors :*

- *Si X est un ensemble fini, on considère l'espace de Hilbert défini précédemment.*
- *Si X n'est pas fini, on considère l'espace de Hilbert standard, muni de la norme :*

$$\|\alpha\|_{\mathcal{L}^2(X,\mu)} = \left(\int_X |\alpha(x)|^2 d\mu(x)\right)^{1/2}$$

Définition 3. *$\forall m \in S(\Lambda)$, on définit : $Y_m := \prod_{l|m} Y_l$ et $\rho_m := \begin{cases} Y \to Y_m \\ y \mapsto (\rho_l(y))_{l|m} \end{cases}$*

Proposition 3. *Soit $m \in S(\Lambda)$, et $\forall\ l|m, v_l$ une densité sur Y_l.*
Alors : $v_m := \begin{cases} Y_m \to [0;1] \\ y = (y_l) \mapsto \prod_{l|m} v_l(y_l) \end{cases}$ est une densité sur Y_m.

Démonstration. $\forall y = (y_l) \in Y_m$, $v_m(y) > 0$ comme produit fini de telles quantités. De plus, si $m = (l_1, \cdots, l_r)$ alors, $\sum_{y\in Y_m} v(y) = \sum_{l_1\in Y_1} \cdots \sum_{l_r\in Y_r} v_{l_1}(y_{l_1}) \cdots v_{l_r}(y_{l_r}) = \prod_{i=1}^{r} 1 = 1$ □

Proposition 4. *Soit $m \in S(\Lambda)$. Supposons donnée $\forall\ l|m$, v_l, une densité sur Y_l. L'application* $(.|.) := \left\{ \begin{array}{l} \mathcal{F}(Y_m,\mathbb{C})^2 \to \mathbb{C} \\ (f,g) \mapsto \sum\limits_{y\in Y_m} v_m(y) f(y)\overline{g(y)} \end{array} \right.$ *munit $\mathcal{F}(Y_m,\mathbb{C})$ d'un produit scalaire hermitien.*

Démonstration. On procède comme pour la proposition 1. □

Notation. *$\forall l \in \Lambda$, on notera* $v(\Omega_l) := \sum\limits_{y\in\Omega_l} v(y)$

Remarque. *On vérifie aisément que l'espace $\mathcal{L}^2(Y_m, v_m) := (\mathcal{F}(Y_m,\mathbb{C}),(.|.))$ est un espace de Hilbert.*

1.2 Inégalité du grand crible

Proposition 5. *Soit $l \in \Lambda$. Supposons fixée une densité de Y_l, et une base orthonormée $\mathcal{B}_l$ de $\mathcal{L}^2(Y_l, v_l)$, qui contient la fonction constante égale à 1, et $\mathcal{B}_l^* = \mathcal{B}_l - \{1\}$. Soit $m \in S(\Lambda)$. Alors $\mathcal{B}_m := \prod\limits_{l|m} \mathcal{B}_l$ est une base orthonormée de $\mathcal{L}^2(Y_m, v_m)$ où $(\varphi_l) : (y_l) \mapsto \prod\limits_{l|m} \varphi_l(y_l)$.*

Démonstration. Remarquons tout d'abord qu'une base orthonormée d'un tel espace existe, puisque c'est un $\mathbb{C}$-espace vectoriel de dimension finie. En effet, $\{x \mapsto \mathbb{1}_y(x) | y \in Y_l\}$ est une famille génératrice.
Soit $\varphi = \bigotimes\limits_{l|m} \varphi_l$ et $\psi = \bigotimes\limits_{l|m} \psi_l$.
$(\varphi|\psi) = \sum\limits_{y\in Y_m} v_m(y)\varphi(y)\overline{\psi(y)} = \sum\limits_{(y_l)\in Y_m} \prod\limits_{l|m} v_l(y_l) \prod\limits_{l|m} \varphi_l(y_l) \overline{\prod\limits_{l|m} \psi_l(y_l)} = \prod\limits_{l|m} (\varphi_l|\psi_l)$ donc la famille est bien orthonormée. Vérifions que c'est une base :
Soit $f \in \mathcal{F}(Y_m,\mathbb{C})$, alors $f = (f_i)_{i=1,..,r}$ avec $m = \{1,..,r\}$.
Or pour tout $1 \le i \le r$, $\exists l_i, \exists (\lambda_j^i)_{1\le j\le l_i}$ tel que $f_i = \sum\limits_{j=1}^{l_i} \lambda_j^i.\phi_j^i$ avec $\phi_j^i \in \mathcal{B}_i$ pour tout j. Donc, $f = (\sum\limits_{j=1}^{l_i} \lambda_j^i.\phi_j^i)_{i=1,..,r} \in \mathrm{Vect}((\phi_j^i)_i, 1 \le i \le r, 1 \le j \le l_i)$. On vérifie aisément qu'elle est libre. □

Théorème 1. *(Inégalité du grand crible) Soit ψ, γ, les deux triplets d'un crible, $\mathcal{L}^*$ le support premier du crible, $\mathcal{L}$ étant les sous-ensembles (finis) de ce dernier. Soit $\Delta = f^\theta(X,\mathcal{L})$ la plus petite constante positive vérifiant pour tout $\alpha : X \to \mathbb{C}$, de carré intégrable sur l'espace de Hilbert $(\mathcal{L}(X,\mu), \|.\|_X)$:*

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

Alors, $\forall \Omega = (\Omega_l)$,

$$|S(X,\Omega,\mathcal{L}^*)| \le \Delta H^{-1}$$

avec

$$H = \sum_{m\in\mathcal{L}} \prod_{l|m} \frac{v(\Omega_l)}{1 - v(\Omega_l)}$$

Notation. $\forall m \in S(\Lambda)$, $\forall y \in Y_m$, $\forall \varphi \in \mathcal{B}_m$, $\forall \alpha \in \mathcal{L}^2(X,\mu)$, *notons :*

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

$$S(\varphi) = \int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)$$

Lemme 1.

$$\forall l \in \Lambda,\ \sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \sum_{y\in Y_l} \frac{|S(l,y)|^2}{v(y)} - \left|\int_X \alpha(x)d\mu(x)\right|^2$$

Démonstration. Soit $l \in \Lambda$, Par le théorème de Fubini-Lebesgue,

$$\sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \iint_{X^2} \alpha(x)\overline{\alpha(y)} \sum_{y\in\mathcal{B}_l^*} \varphi(p_l(F(x)))\overline{\varphi(\rho_l(F(y)))}d\mu(x)d\mu(y)$$

Or $(\varphi)_{\varphi\in\mathcal{B}_l}$ est une base orthonormée de l'ensemble des fonctions sur Y_l, donc, en introduisant δ le symbole de Kronecker :

$$(\delta(y,.)|\varphi) = v(y)\varphi(y)$$

donc,

$$\sum_{\varphi\in\mathcal{B}_l} \varphi(y)\overline{\varphi(z)} = \frac{\delta(y,z)}{v(y)}$$

Par suite, $\sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \iint_{X^2} \alpha(x)\overline{\alpha(y)}\left[\frac{\delta(\rho_l(F(x)),\rho_l(F(y)))}{v(\rho_l(F(x)))} - 1\right] d\mu(x)d\mu(y)$ en ôtant la contribution due à la fonction constante égale à 1.

Par suite, $\sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \iint_{\{\rho_l(F(x))=\rho_l(F(y))\}} \frac{\alpha(x)\overline{\alpha(y)}}{v(\rho_l(F(x)))}d\mu(x)d\mu(y) - \left|\int_X \alpha(x)d\mu(x)\right|^2$

$$\sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \sum_{z\in Y_l} \frac{1}{v(z)} \iint_{\{\rho_l(F(x))=\rho_l(F(y))=z\}} \alpha(x)\overline{\alpha(y)}d\mu(x)d\mu(y) - \left|\int_X \alpha(x)d\mu(x)\right|^2$$

$$\sum_{\varphi\in\mathcal{B}_l^*} |S(\varphi)|^2 = \sum_{y\in Y_l} \frac{|S(l,y)|^2}{v(y)} - \left|\int_X \alpha(x)d\mu(x)\right|^2$$ □

Lemme 2. *Soit $\alpha : X \to \mathbb{C}$, de carré intégrable sur l'espace mesuré (X,μ), supportée dans $S(X,\Omega,\mathcal{L}^*)$. $\forall m \subseteq \mathcal{L}^*$,*

$$\sum_{\varphi\in\mathcal{B}_m^*} |S(\varphi)|^2 \geq \left|\int_X \alpha(x)d\mu(x)\right|^2 \prod_{l|m} \frac{v(\Omega_l)}{1-v(\Omega_l)}$$

Démonstration. On raisonne par récurrence forte sur $|m|$.

Si $m = \{l\}$:

$\left|\int_X \alpha(x)d\mu(x)\right|^2 = \left|\sum_{y\in Y_l\setminus\Omega_l} S(l,y)\right|^2$ au vu de la condition portant sur le support de α.

L'inégalité de Cauchy-Schwarz assure que :

$$\left|\int_X \alpha(x)d\mu(x)\right|^2 \underset{C.S.}{\leq} \left(\sum_{y\in Y_l\setminus\Omega_l} v(y)\right)\left(\sum_{y\in Y_l} \frac{|S(l,y)|^2}{v(y)}\right) = v(Y_l\setminus\Omega_l)\sum_{y\in Y_l} \frac{|S(l,y)|^2}{v(y)}$$

$\left|\int_X \alpha(x)d\mu(x)\right|^2 \leq v(Y_l \setminus \Omega_l)\left[\sum_{\varphi\in\mathcal{B}_l^*}|S(\varphi)|^2 + \left|\int_X \alpha(x)d\mu(x)\right|^2\right]$ par le lemme 1.

Donc, $\left|\int_X \alpha(x)d\mu(x)\right|^2\left[\frac{1}{v(Y_l \setminus \Omega_l)} - 1\right] \leq \sum_{\varphi\in\mathcal{B}_l^*}|S(\varphi)|^2$

Or $v(Y_l \setminus \Omega_l) = v(Y_l) - v(\Omega_l) = 1 - v(\Omega_l)$ par définition de la densité.

Par suite : $\sum_{\varphi\in\mathcal{B}_l^*}|S(\varphi)|^2 \geq \left|\int_X \alpha(x)d\mu(x)\right|^2 \frac{v(\Omega_l)}{1-v(\Omega_l)}$ ce qui démontre l'initialisation.

Supposons le résultat acquis jusqu'au rang n, et considérons $m \subseteq \mathcal{L}^*$, $|m| = n+1$. Écrivons $m = m_1m_2$ où $m_1, m_2 \neq \emptyset$.

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

Or, $S(\varphi_1\bigotimes\varphi_2) = \int_X \alpha(x)\varphi_1(\rho_{m_1}(F(x)))\varphi_2(\rho_{m_2}(F(x)))d\mu(x)$

Posons $\beta = \alpha.\varphi_1(\rho_{m_1}(F(.)))$, elle est supportée dans $S(X,\Omega,\mathcal{L}^*)$, donc, par hypothèse de récurrence, puis en sommant :

$$\sum_{\varphi\in\mathcal{B}^*_{m_1m_2}}|S(\varphi)|^2 \geq \sum_{\varphi_1\in\mathcal{B}^*_{m_1}}\left|\int_X \beta(x)d\mu(x)\right|^2\prod_{l|m_2}\frac{v(\Omega_l)}{1-v(\Omega_l)} = \sum_{\varphi_1\in\mathcal{B}^*_{m_1}}|S(\varphi_1)|^2\prod_{l|m_2}\frac{v(\Omega_l)}{1-v(\Omega_l)}$$

$$\sum_{\varphi\in\mathcal{B}^*_{m_1m_2}}|S(\varphi)|^2 \geq \prod_{l|m_1m_2=m}\frac{v(\Omega_l)}{1-v(\Omega_l)}\left|\int_X \alpha(x)d\mu(x)\right|^2$$

en appliquant à nouveau l'hypothèse de récurrence. □

Démonstration. (du théorème) Soit $\alpha = \mathbb{1}_{S(X,\Omega,\mathcal{L}^*)}$.
Remarquons que $|S(X,\Omega,\mathcal{L}^*)| = \int_X \alpha(x)d\mu(x) = \int_X \alpha^2(x)d\mu(x)$.
Elle vérifie par défintion la condition de support et est de carré intégrable, donc, le lemme 2 affirme que :

$$|S(X,\Omega,\mathcal{L}^*)|^2\sum_{m\in\mathcal{L}}\prod_{l|m}\frac{v(\Omega_l)}{1-v(\Omega_l)} \leq \sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m}|S(\varphi)|^2 \leq \Delta\int_X|\alpha(x)|^2d\mu(x) = \Delta|S(X,\Omega,\mathcal{L}^*)|$$

par définition de Δ, ce qui donne la majoration annoncée. □

1.3 Interprétation de Δ

Proposition 6. *Soit*

$$\mathcal{L}_0^2(Y_l) := \left\{f \in \mathcal{L}^2(Y_l) \mid (f|1) = 0\right\}$$
$$\mathcal{L}_0^2(Y_m) := \left\{f \in \mathcal{L}^2(Y_m) \mid (f|1) = 0\right\}$$

$$T : \begin{cases} (\mathcal{L}^2(X,\mu), \|.\|_X) \to \left(\bigoplus_{m\in\mathcal{L}} \mathcal{L}_0^2(Y_m)', \|.\|\right) \\ \alpha \mapsto \left(f \mapsto \int_X \alpha(x) f(\rho_m(F(x)))d\mu(x)\right)_m \end{cases}$$

est une application linéaire continue dont la carré de la norme subordonnée vaut Δ.

Plus précisément, $\forall f \in \bigoplus_{m\in\mathcal{L}} \mathcal{L}_0^2(Y_m)', \exists!(f_m)_{m\in\mathcal{L}} \in \mathcal{L}_0^2(Y_m)'$ *tel que* $f = \sum_{m\in\mathcal{L}} f_m$. *Alors,*
$\|f\| := \sqrt{\sum_{m\in\mathcal{L}} \|f_m\|^2_{\mathcal{L}_c(\mathcal{L}_0^2(Y_m),\mathbb{C})}}$ *munit* $\bigoplus_{m\in\mathcal{L}} \mathcal{L}_0^2(Y_m)'$, *d'une norme.*

Démonstration. Remarquons premièrement que l'espace $\mathcal{L}_0^2(Y_l)$ est l'orthogonal du sous-espace vectoriel engendré par la fonction constante égale à 1. Par suite, $\mathcal{B}_l^*$ en est une base orthonormée. Ainsi, $\mathcal{B}_m^*$ est une base orthonormée de $\mathcal{L}_0^2(Y_m)$. Soit $m \in \mathcal{L}$, soit $\alpha \in \mathcal{L}^2(X,\mu)$. Considérons l'application :

$$T_m^\alpha : \begin{cases} (\mathcal{L}_0^2(Y_m), (.|.)) \to (\mathbb{C}, |.|) \\ f \mapsto \int_X \alpha(x) f(\rho_m(F(x)))d\mu(x) \end{cases}$$

$\forall f \in \mathcal{L}_0^2(Y_m)$,

$$\left|\int_X \alpha(x) f(\rho_m(F(x)))d\mu(x)\right| = \left|\sum_{\varphi\in\mathcal{B}_m^*} (f|\varphi).\int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)\right|$$

$$\underset{C.S.}{\leq} \left(\sum_{\varphi\in\mathcal{B}_m^*} |(f|\varphi)|^2\right)^{1/2} \cdot \left(\sum_{\varphi\in\mathcal{B}_m^*} \left|\int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)\right|^2\right)^{1/2}$$

Le premier facteur correspondant à la norme de f induite par le produit scalaire, et T_m^α étant linéaire, on en déduit que T_m^α est une application linéaire continue dont la norme d'opérateur vérifie :

$$\|T_m^\alpha\|_{\mathcal{L}_c(\mathcal{L}_0^2(Y_m),\mathbb{C})} \leq \left(\sum_{\varphi\in\mathcal{B}_m^*} \left|\int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)\right|^2\right)^{1/2}$$

Soit :

$$f : \begin{cases} Y_m \to (\mathbb{C}, |.|) \\ y \mapsto p_{\mathcal{L}_0^2(Y_m)}\left[\dfrac{1}{v_m(y)} \displaystyle\int_{\{\rho_m(F(x))=y\}} \alpha(x)d\mu(x)\right] \end{cases}$$

où p désigne l'opérateur de projection.
Cette application est conçue de sorte que pour tout $\varphi \in \mathcal{B}_m^*$,

$$\overline{(f|\varphi)} = \int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)$$

C'est un cas d'égalité. On en déduit donc :

$$(*) : \|T_m^\alpha\|_{\mathcal{L}_0^2(Y_m)'} = \left(\sum_{\varphi\in\mathcal{B}_m^*} \left|\int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x)\right|^2\right)^{1/2}$$

Par suite, $\forall \alpha \in \mathcal{L}^2(X,\mu)$, on obtient grâce à $(*)$

$$\|T(\alpha)\|^2 = \sum_{m\in\mathcal{L}} \|T_m^\alpha\|^2_{\mathcal{L}_0^2(Y_m)'} = \sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} \left| \int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x) \right|^2$$

$$\sum_{m\in\mathcal{L}} \sum_{\varphi\in\mathcal{B}_m^*} \left| \int_X \alpha(x)\varphi(\rho_m(F(x)))d\mu(x) \right|^2 = \|T(\alpha)\|^2 \leq \|T\|_{\mathcal{L}_c(\mathcal{L}^2(X,\mu),\bigoplus_{m\in\mathcal{L}} \mathcal{L}_0^2(Y_m)')} \|\alpha\|^2_{\mathcal{L}^2(X,\mu)}$$

Enfin, T est une application linéaire continue, et

$$\|T\|^2_{\mathcal{L}_c(\mathcal{L}^2(X,\mu),\bigoplus_{m\in\mathcal{L}} \mathcal{L}_0^2(Y_m)')} = \Delta$$

par définition de la norme subordonnée. □

Remarque. *Cette interprétation de Δ permet de montrer que cette quantité ne dépend en fait pas de la base fixée.*

1.4 Majoration de Δ par dualité

1.4.1 Transposée d'applications linéaires et propriétés

Définition 4. *Soit E et F deux espaces vectoriels et $u \in \mathcal{L}(E,F)$. Alors, $\exists! {}^t u \in \mathcal{L}(F^*,E^*)$ vérifiant pour tout $\varphi \in F^*$,*

$$^t u \circ \varphi = \varphi \circ u$$

On appelle alors l'application ${}^t u$ transposée de u.

(elle existe et est unique puisqu'elle est uniquement determinée).

Le but est de démontrer la proposition suivante :

Proposition 7. *Si $(E,\|.\|_E)$ et $(F,\|.\|_F)$ sont deux espaces vectoriels normés, alors, $\forall u \in \mathcal{L}_c(E,F)$,*

$$\|u\|_{\mathcal{L}_c(E,F)} = \|^t u\|_{\mathcal{L}_c(F^*,E^*)}$$

On admet pour cela le théorème suivant :

Théorème 2. *(Hann-Banach)(Admis) Soit $(E,\|.\|)$ un espace vectoriel normé, F un sous-espace vectoriel de E et g une forme linéaire continue de norme $\|g\|$ sur F. Alors, il existe une forme linéaire continue f qui prolonge g sur E et telle que $\|f\| = \|g\|$.*

Référence : http ://perso.eleves.ens-rennes.fr/people/Antoine.Mouzard/DEV/hahnbanach.pdf - ENS de Mathématqiues de Rennes.

Corollaire 1. *Soit $(E,\|.\|)$ un espace vectoriel normé et $x \neq 0$, un vecteur de E. Alors, $\exists f \in \mathcal{L}_c(E,\mathbb{K})$ vérifiant : $\|f\|_{\mathcal{L}_c(E,\mathbb{K})} = 1$ et $f(x) = \|x\|$.*

Démonstration. Soit $x \neq 0$. $H = \mathbb{K}x$, c'est un sous-espace vectoriel de E.
Soit $f : \lambda.x \in H \mapsto \lambda\|x\|$. C'est une forme linéaire continue de norme 1. On peut donc lui appliquer la théorème de Hann-Banach, et on conlut à l'existence d'une forme linéaire continue, g, sur E, de norme 1, et elle vérifie trivialement l'identité $g(x) = f(x) = \|x\|$ □

Proposition 8. *Soit $(E, \|.\|)$ un espace vectoriel normé de dimension finie, alors il existe un isomorphisme isométrique entre E et son bidual.*

Démonstration. Soit :

$$J : \begin{cases} (E, \|.\|) \to ((E^*)^*, \|.\|_{\mathcal{L}_c(\mathcal{L}_c(E,\mathbb{K}),\mathbb{K})}) \\ x \mapsto ev_x : \begin{cases} E^* \to \mathbb{K} \\ g \mapsto g(x) \end{cases} \end{cases}$$

C'est évidemment une application linéaire. On sait de plus que $\dim(E) = \dim(E^*) = \dim((E^*)^*)$. Il suffit donc de montrer que l'application est injective, montrons donc que c'est une isométrie, cela permettra de conclure :
On a, $\forall x \in E$, non nul,

$$\|J(x)\|_{\mathcal{L}_c(\mathcal{L}_c(E,\mathbb{K}),\mathbb{K})} = \|ev_x\|_{\mathcal{L}_c(\mathcal{L}_c(E,\mathbb{K}),\mathbb{K})} = \sup_{\|f\|_{\mathcal{L}_c(E,\mathbb{K})}=1} |ev_x(f)| = \sup_{\|f\|_{\mathcal{L}_c(E,\mathbb{K})}=1} |f(x)| \ (*)$$

Or le corallaire 1 affirme l'existence d'une application $g \in \mathcal{L}_c(E, \mathbb{K})$ de norme 1, et vérifiant $g(x) = \|x\|$.
Donc, $(*)$ donne $\|J(x)\|_{\mathcal{L}_c(\mathcal{L}_c(E,\mathbb{K}),\mathbb{K})} \geq \|x\|$. L'autre inégalité étant évidente (si $\|f\|_{\mathcal{L}_c(E)} = 1$, alors $|f(x)| \leq \|x\|$), on conclut à l'égalité. J est isométrique, donc injective. On pourrait montrer qu'elle est bijective ssi E est de dimension finie. □

Démonstration. (Proposition 7) Soit $\varphi \in F^*$, $x \in E$,

$$|{}^t u(\varphi)(x)| = |\varphi \circ u(x)| \leq \|\varphi\|_{F^*}.\|u\|_{\mathcal{L}_c(E,F)}.\|x\|_E$$

Donc

$$\|{}^t u(\varphi)\|_{\mathcal{L}_c(E,\mathbb{K})} \leq \|\varphi\|_{F^*}.\|u\|_{\mathcal{L}_c(E,F)}$$

et

$$\|{}^t u\|_{\mathcal{L}_c(F^*,E^*)} \leq \|u\|_{\mathcal{L}_c(E,F)}$$

De plus, la proposition 8 affirme que ${}^t({}^t(u))$ et u sont de même norme d'opérateur. On applique l'inégalité précédente à ${}^t u$ et cela permet de conclure. □

1.4.2 Majoration par dualité

Proposition 9. *Avec les notations précédentes, Δ est la plus petite constante vérifiant :*

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

pour tout famille de complexes $(\beta(m, \varphi))_{m,\varphi}$.

Démonstration. La proposition 6 a permis d'identifier Δ au carré de la norme d'un opérateur linéaire. C'est aussi, par ce qui précède, le carré de la norme de sa transposée :

$${}^t T : \left(V := \left(\bigoplus_{m \in \mathcal{L}} \mathcal{L}_0^2(Y_m)' \right)', \|.\|_V \right) \to \left((\mathcal{L}^2(X, \mu))', \|.\|_{\mathcal{L}_c(\mathcal{L}^2(X,\mu),\mathbb{K})} \right)$$

Soit $f \in V$, on note $g \in \bigoplus_{m \in \mathcal{L}} \mathcal{L}_0^2(Y_m)$ l'application qui vérifie $f = J(g)$ où J est l'isomorphisme évoqué précédemment.

$$\forall \alpha \in \mathcal{L}^2(X, \mu), \ {}^t T(f)(\alpha) = f \circ T(\alpha) = J(g)(T(\alpha)) = T(\alpha)(g)$$

Écrivons $g = \sum_{m\in\mathcal{L}} g_m$,

$$|{}^tT(f)(\alpha)| = \left|\int_X \alpha(x) \sum_{m\in\mathcal{L}} g_m(\rho_m(F(x)))d\mu(x)\right| \underset{C.S.}{\leq} \|\alpha\|_{\mathcal{L}^2(X,\mu)}.\|\sum_{m\in\mathcal{L}} g_m(\rho_m(F))\|_{\mathcal{L}^2(X,\mu)}$$

Traitons le cas d'égalité : Soit $\alpha_0 = \sum_{m\in\mathcal{L}} g_m(\rho_m(F)) \in \mathcal{L}^2(X,\mu)$. Alors :

$$|{}^tT(f)(\alpha_0)| = \int_X \left[\sum_{m\in\mathcal{L}} g_m(\rho_m(F(x)))\right]^2 d\mu(x) = \sqrt{\int_X \left[\sum_{m\in\mathcal{L}} g_m(\rho_m(F(x)))\right]^2 d\mu(x)}^2$$

est un cas d'égalité (celui de Cauchy-Schwarz, là où les vecteurs sont liés).
Par suite,

$$\|{}^tT\circ f\| = \|\sum_{m\in\mathcal{L}} g_m(\rho_m(F))\|_{\mathcal{L}^2(X,\mu)}$$

On exprime $g_m \in \mathcal{L}^2_0(Ym)$ dans la base : $g_m = \sum_{\varphi\in\mathcal{B}^*_m} \beta(m,\varphi)\varphi$.

Par suite,

$$\|{}^tT(f)\|^2 = \int_X \left|\sum_{m\in\mathcal{L}}\sum_{\varphi\in\mathcal{B}^*_m} \beta(m,\varphi)\varphi(\rho_m(F(x)))\right|^2 d\mu(x) \leq \|{}^tT\|^2.\|f\|^2 = \|T\|^2.\|J(g)\|^2 = \Delta\|g\|^2$$

la deuxième égalité valant puisque, par la proposition 8, J est une isométrie. (On ne précise pas ici les normes, afin de ne pas alourdir davantage les notations, ce sont les normes d'opérateurs usuelles qui munissent naturellement les espaces). Donc,

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

et c'est la plus petite constante qui vérifie cette inégalité. □

Proposition 10. *Avec les notations précédentes, supposons donné un crible, alors,*

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

$$\textit{et}\ \ \forall m,n\in S(\Lambda),\ \forall\varphi,\varphi'\in\mathcal{B}_m\times\mathcal{B}_n,\ W(\varphi,\varphi') = \int_X \varphi(\rho_m(F(x)))\overline{\varphi'(\rho_n(F(x)))}d\mu(x)$$

Démonstration. Notons que :

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

$$\leq \frac{1}{2}\sum_m\sum_n\sum_\varphi\sum_{\varphi'}(|\beta(m,\varphi)|^2 + |\beta(n,\varphi')|^2)|W(\varphi,\varphi')|$$

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

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

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

Or, Δ est la plus petite constante qui vérifie cette inégalité, par suite, $\Delta \leq \max_{m\in\mathcal{L}}\max_{\varphi\in\mathcal{B}_m^*}\sum_n\sum_{\varphi'}|W(\varphi,\varphi')|$

□

Nous avons développé les outils nécessaires afin de démontrer le théorème de Gallagher, ce qui est l'objet de la seconde partie, il reste néanmoins à établir quelques résultats classiques liés à la répartition des nombres premiers, et les polynômes irréductibles sur $\mathbb{F}_p$.

2 Théorème de Gallagher pour les polynômes

2.1 Application de l'inégalité du grand crible

Théorème 3. *(de Gallagher) Soient N et r deux entiers naturels, $r > 2$.*
Définissons :

$$E_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N, \textit{réductible sur } \mathbb{Q} \right\}$$

$$X_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N \right\}$$

Alors,

$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq Cr^2\frac{\ln(N)}{\sqrt{2N+1}}$$

où C est une constante absolue.

Démonstration. Remarquons que $\sharp X_r(N) = (2N+1)^r$
On applique l'inégalité du grand crible avec :

$$Y = \mathbb{Z}_r[X] \quad \Lambda = \mathbb{P} \quad Y_l = \mathbb{F}_r^l[X] \quad \rho_l \text{ est le morphisme quotient}$$

$$X = X_r(N) \quad F = I_d \quad \mathcal{L}^* = \{p \in \mathbb{P}\ p \leq L\} \quad \Omega_l = \left\{P \in \mathbb{F}_r^l[X],\ \text{irréductible}\right\}$$

$$\forall f \in \mathbb{F}_r^l[X],\ v_l(f) = \frac{1}{l^r}$$

$$S(X,\Omega,\mathcal{L}^*) := \left\{P \in X_r(N) \mid \forall p \in \mathcal{P}|\ p \leq L,\ \bar{P} \text{ n'est pas irréductible}\right\}$$

Tout polynôme unitaire (afin de conserver le même degré) irréductible dans $\mathbb{F}_r^l[X]$ où $l \in \mathbb{P}$, l'est dans $\mathrm{Frac}(\mathbb{Z}_r[X]) = \mathbb{Q}_r[X]$. Par suite, la négation de cette proposition fournit :

$$E_r(N) \subseteq S(X,\Omega,\mathcal{L}^*)$$

Donc, $\sharp E_r(N) \leq \sharp S(X,\Omega,\mathcal{L}^*) \leq \Delta H^{-1}$ où $H = \sum_{l\in\mathbb{P},l\leq L}\frac{v(\Omega_l)}{v(Y_l-\Omega_l)} \geq \sum_{l\in\mathbb{P},l\leq L}\frac{|\Omega_l|}{l^r}$

On commence par fournir une estimation de $|\Omega_l|$.

2.2 Dénombrement des polynômes irréductibles de $\mathbb{F}_r^l[X]$, où l est premier

2.2.1 Fonction de Möbius

Définition 5. *On introduit la fonction μ de Möbius :* $\mu := \begin{cases} \mathbb{N}^* \to \{-1,0,1\} \\ n \mapsto 1 \text{ si } n = 1. \\ n \mapsto 0 \text{ si } n \text{ a un facteur carré.} \\ n \mapsto (-1)^r \text{ si } n = p_1 \cdots p_r \text{ distincts.} \end{cases}$

Lemme 3.

- *Soient $n, m \in \mathbb{N}^*$, si $n \wedge m = 1$, alors $\mu(nm) = \mu(n)\mu(m)$.*
- $\sum_{d|n} \mu(d) = 0$, *si $n \geq 2$, 1 si $n = 1$.*

Démonstration.

- Si $n = 1$, $\mu(mn) = \mu(m) = 1.\mu(m)$. On raisonne de façon analogue avce le cas $m = 1$.
  Si n ou m a un facteur carré, alors nm aussi, et $\mu(nm) = \mu(n)\mu(m) = 0$.
  Si on suppose que n et m sont supérieurs à 2, sans facteurs carrés, alors : $n = p_1 \cdots p_r$, $m = q_1 \cdots q_s$, et puisque $n \wedge m = 1$, les p_i et q_i sont tous distincts, et
  $$\mu(nm) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m).$$
- Le cas $n = 1$ est évident. Sinon, on écrit la décomposition de n en produit de facteurs premiers, et : $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$
  Donc, $\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{1 \leq i < j \leq r} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_r) = \sum_{j=0}^{r} \binom{r}{j} (-1)^j = 0$

□

Proposition 11. *(Inversion de Möbius)*

$$\text{Si } g(n) = \sum_{d|n} f(d), \text{ alors } f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} g\left(\frac{n}{d}\right)\mu(d)$$

Démonstration. Supposons que $g(n) = \sum_{d|n} f(d)$

$$\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d|n} \sum_{d'|\frac{n}{d}} f(d')\mu(d) = \sum_{dd'|n} f(d')\mu(d) = \sum_{d'|n} \left(\sum_{d|\frac{n}{d'}} \mu(d) \right) f(d')$$

Or, le lemme 3 affirme que $\sum_{d|\frac{n}{d'}} \mu(d) = 1$ si $n = d'$, 0 sinon.

Donc,

$$\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = f(n)$$

□

2.2.2 Extension de corps et corps de décomposition

Définition 6. *Soit k un corps. On dit que $\mathbb{K}$ est une extension du corps k s'il existe $j : k \mapsto \mathbb{K}$ un morphisme de corps. $\mathbb{K}$ est alors une $k-$algèbre. Sa dimension est appelée degré de l'extension et est notée $[\mathbb{K} : k]$.*

Définition 7. *Soit $\mathbb{L}$ un corps et k un sous-corps de $\mathbb{L}$. Soit $\mathcal{P}$ une partie finie de $\mathbb{L}$, alors l'ensemble des sous-corps de $\mathbb{L}$ qui contiennent k et $\mathcal{P}$ admet un plus petit élément, il est noté $k(\mathcal{P})$.*
(Il suffit en effet de considérer l'intersection de tous les sous-corps de $\mathbb{L}$ qui contiennent k et $\mathcal{P}$).

Définition 8. *Soit k un corps et $P \in k[X]$, irréductible. On dit que $\mathbb{L}$ est un corps de rupture de P si c'est une extension monogène de k, engendrée par une racine de P.*

Proposition 12. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Alors, $[\mathbb{K}[X]/(P) : \mathbb{K}] = \deg(P)$*

Démonstration. Soit π le morphisme quotient. Notons $P = \sum_{k=0}^{n} a_k X^k$. Notons x l'image de X dans le quotient. Montrons que $(1, x, .., x^{n-1})$ est une base de $\mathbb{K}[X]/(P)$.
On sait que la famille est libre : en effet, $\forall a_0, ..., a_{n-1} \in \mathbb{K}$ tel que $\sum_{k=0}^{n-1} a_k x^k = 0$. Soit $R = \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}[X]$. On sait que $\pi(R) = 0$ donc $R \in (P)$. Par suite, $P|R$. Or $\deg(R) < \deg(P)$. Donc, $R = 0$, et pout tout i, $a_i = 0$.

Elle est également génératrice : Soit $S \in \mathbb{K}[X]/(P)$, il existe $T \in \mathbb{K}[X]$ tel que $S = \pi(T)$. On sait qu'il existe un unique couple $(A, B) \in \mathbb{K}[X]^2$ vérifiant : $T = AP + B$ et $\deg(B) < \deg(P) = n$. Or,

$$S = \pi(T) = \pi(AP) + \pi(B) = \pi(B)$$

Ceci conclut puisque $B \in Vect_{\mathbb{K}}(1, .., x^{n-1})$. □

Proposition 13. *Soit l un nombre premier, et Ω_l^d l'ensemble des polynômes irréductibles de degré d de $\mathbb{F}_l[X]$. Alors, $X^{l^n} - X = \prod_{d|n} \prod_{P \in \Omega_l^d} P$ pour tout entier naturel n non nul.*

Démonstration. Soit $d|n$ et $P \in \Omega_l^d$. Soit x une racine de P. On considère un corps $\mathbb{F}_l(x)$ de rupture de P. On sait que, par la proposition 12, $[\mathbb{F}_l(x) : \mathbb{F}_l] = \deg(P) = d$. Donc, $\mathbb{F}_l(x) \simeq \mathbb{F}_{l^d}$ (Unicité des corps finis).
On a $x^{l^d} = x$, donc, par récurrence, $x^{l^{d(k+1)}} = \left(x^{l^{dk}}\right)^{l^d} = x^{l^{dk}} \underset{H.R.}{=} x$.
Montrons que les racines de P sont simples : En effet, supposons par l'absurde que x soit une racine double de P dans une extension L. Alors x est une racine de P'. Or, l'algorithme d'Euclide affirme que le P.G.C.D. est invariant par extension de corps. Comme P est irréductible dans $\mathbb{F}_l$, $\text{pgcd}_{\mathbb{F}_l}(P, P') = P$ ou 1 donc $\text{pgcd}_{\mathbb{F}_l}(P, P') = P$ car ils ont une racine commune. L'égalité des degrés implique $P' = 0$, ceci donne $P = Q(X^l)$ et contredit son irreductibilité.
Donc, $P|X^{l^n} - X$, et,

$$\prod_{d|n} \prod_{P \in \Omega_l^d} P | X^{l^n} - X$$

par irréductibilité.
Réciproquement, si α est une racine de $X^{q^n} - X$ dans un corps $\mathbb{K}$, contenant $\mathbb{F}_q$. Soit P_α son polynôme minimal sur $\mathbb{F}_q$. Il est unitaire, de degré $\deg(\alpha)$. Considérons

$$E = \left\{\text{racine de } X^{q^n} - X\right\}$$

C'est un corps à q^n éléments. Par suite,

$$\prod_{\beta\in E, P_\alpha(\beta)=0}(X-\beta)|P_\alpha$$

En regroupant les polynômes et en choisissant un représentant, on en déduit le résultat. □

Conséquence : $X^{l^r}-X=\prod_{d|r}\prod_{P\in\Omega_l^d}P$, donc $l^r=\sum_{d|r}\sum_{P\in\Omega_l^d}\deg(P)=\sum_{d|r}d|\Omega_l^d|$

Par la formule d'inversion de Möbius (proposition 11),

$$r|\Omega_l|=\sum_{d|r}l^d\mu(r/d)$$

Par suite,

$$|\Omega_l|=\frac{l^r}{r}+\frac{1}{r}\sum_{d|r,d\leq r/2}\mu(r/d)l^d\geq\frac{l^r}{r}+\frac{1}{r}\sum_{d\leq r/2}(-1)l^d=\frac{l^r}{r}-\frac{l(l^{r/2}-1)}{r(l-1)}=\frac{l^r}{r}\left(1-\frac{l(l^{r/2}-1)}{l^r(l-1)}\right)$$

Or, $\frac{l}{l-1}\leq 2$ (puisque $l\geq 2$), et $l^{r/2}-1\leq l^{r/2}$

$$|\Omega_l|\geq\frac{l^r}{r}\left(1-\frac{2}{l^{r/2}}\right)$$

On remarque que si $r>2$, alors,

$$\frac{2}{l^{r/2}}\leq\frac{9}{10}$$

Donc,

$$|\Omega_l|\geq\frac{l^r}{10r}$$

Introduisons la fonction de comptage des nombres premiers :

$$\pi(n):=\sum_{k=0}^{n}\mathbb{1}_{\mathbb{P}}(n)=\sharp\mathbb{P}\bigcap\{0,..,n\}$$

Ainsi,

$$H\geq\frac{1}{10r}\sum_{l\in\mathbb{P},l\leq L}1=\frac{\pi(L)}{10r}$$

Il nous reste encore à minorer $\pi(L)$

.

2.3 Évaluation de $\pi(n)$

2.3.1 Préliminaires

Proposition 14. *Soient $a,b\in\mathbb{N}$ tels que $1\leq b\leq a$, alors*

$$I(a,b)=\int_0^1 x^{b-1}(1-x)^{a-b}dx=\sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\frac{1}{k+b}$$

Démonstration. On utilise simplement le binôme de Newton.

$$I(a,b)=\int_0^1 x^{b-1}(1-x)^{a-b}dx=\int_0^1 x^{b-1}\sum_{k=0}^{a-b}\binom{a-b}{k}(-x)^k dx=\sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\left[\frac{x^{k+b}}{k+b}\right]_0^1$$

□

Proposition 15.

$$\forall a, b \in \mathbb{N},\ 1 \leq b \leq a,\ I(a,b) = \frac{1}{b\binom{a}{b}} = \frac{1}{a\binom{a-1}{b-1}}$$

Démonstration.

$$I(a,b+1) = \int_0^1 x^b(1-x)^{a-b-1} \underset{IPP}{=} \left[-x^b\frac{(1-x)^{a-b}}{a-b}\right]_0^1 + \int_0^1 bx^{b-1}\frac{(1-x)^{a-b}}{a-b} = \frac{b}{a-b}I(a,b)$$

Par itération du principe,

$$I(a,b) = \frac{(b-1)...1}{(a-b+1)...(a-1)}I(a,1) = \frac{(b-1)!}{\frac{(a-1)!}{(a-b)!}}I(a,1)$$

et,

$$I(a,1) = \int_0^1 (1-x)^{a-1} = \left[-\frac{(1-x)^a}{a}\right]_0^1 = \frac{1}{a}$$

Donc,

$$I(a,b) = \frac{b!(a-b)!}{b.a!}$$

D'où le résultat. □

Notation. *Notons* $\forall n \in \mathbb{N}^*,\ \Delta_n = PPCM(1,..,n)$.

Proposition 16. $\forall a, b \in \mathbb{N}$ *tels que* $1 \leq b \leq a$,

$$b\binom{a}{b} | \Delta_a$$

Démonstration. $I(a,b)\Delta_a = \sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\frac{\Delta_a}{k+b}$
Or, $b \leq k+b \leq a$, et on sait que Δ_a est un multiple de tout ces entiers, donc $\exists m_k \in \mathbb{N}$ tel que $\Delta_a = (k+b)m_k$
Ainsi,

$$I(a,b)\Delta_a = \sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}m_k = \frac{\Delta_a}{b\binom{a}{b}} \in \mathbb{N}$$

□

Lemme 4.

$$\forall n \geq 2,\ \Delta_{2n+1} \geq n.4^n$$

Démonstration. Par la proposition 16, on obtient avec $a = 2n$ et $b = n$ la relation :

$$n\binom{2n}{n} | \Delta_{2n}$$

On sait de plus que Δ_{2n+1} est un multiple commun des entiers $1, ..., 2n+1$, donc en particulier des entiers compris entre 1 et $2n$. Par suite, on a : $\Delta_{2n} | \Delta_{2n+1}$, donc,

$$n\binom{2n}{n} | \Delta_{2n+1}\ (*)$$

De plus, $I(a,b)\Delta_a \in \mathbb{N}$ donc, en prenant $a = 2n+1$ et $b = n+1$, on déduit :

$$(2n+1)\binom{2n}{n} | \Delta_{2n+1} \ (**)$$

Par $(*)$, $\exists k \in \mathbb{N}$ tel que $\Delta_{2n+1} = kn\binom{2n}{n}$ Ainsi,

$$(**) \Rightarrow (2n+1)\binom{2n}{n} \left| kn\binom{2n}{n} \right. \Rightarrow 2n+1 | kn$$

Or $(2n+1) \wedge n = 1$, donc par Gauss, $2n+1|k$, donc $k = (2n+1)k'$ Par suite,

$$n(2n+1)\binom{2n}{n} | \Delta_{2n+1} \text{ donc } n(2n+1)\binom{2n}{n} \leq \Delta_{2n+1}$$

Enfin, $4^n = 2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \leq \sum_{k=0}^{2n} \binom{2n}{n} = (2n+1)\binom{2n}{n}$ Donc,

$$\Delta_{2n+1} \geq n(2n+1)\binom{2n}{n} \geq n4^n$$

□

Proposition 17.

$$\forall n \geq 7, \ \Delta_n \geq 2^n$$

Démonstration.

- Si n est impair, alors, $n = 2k+1$. La condition $n \geq 7$ est équivalente à la condition $k \geq 3$ et, par le lemme 4,
$$\Delta_n = \Delta_{2k+1} \geq k4^k \geq 2.4^k = 2^{2k+1} = 2^n$$
- Si n est pair, étant supérieur à 2, on peut écrire $n = 2k+2$, et,
$$\Delta_{2k+2} \geq \Delta_{2k+1} \underset{\text{Lemme 4}}{\geq} k.4^k \geq 4.4^k = 2^{2k+2} = 2^n \text{ si } k \geq 4, \text{ i.e. } n \geq 10$$
On traîte le cas $n = 8$ à la main, et, Δ_8=840, et $2^8 = 256$.

□

2.3.2 Minoration de $\pi(n)$

Lemme 5.

$$\forall n \in \mathbb{N}^*, \ \Delta_n = \prod_{p \in \mathbb{P}, p \leq n} p^{v_p(\Delta_n)}$$

avec $v_p(k)$ la valuation $p-$adique d'un entier naturel k.

Démonstration. On sait déjà que,

$$\Delta_n = \prod_{p \in \mathbb{P}} p^{v_p(\Delta_n)}$$

Or, c'est le plus petit multiple commum aux n premiers entiers. Ainsi, sa décomposition en produit de facteurs premiers ne contient que les premiers nécessaires à la décomposition des entiers $1, .., n$, qui sont eux mêmes plus petit que n. D'où le résultat. □

Lemme 6.

$$\forall n \in \mathbb{N}^*, \forall p \in \mathbb{P},\ p^{v_p(\Delta_n)} \leq n$$

Démonstration. On sait que $v_p(\Delta_n)$ est l'exposant de la décomposition en produit de facteurs premiers de Δ_n. Il peut apparaître avec différents exposants dans les décompositions en produits de facteurs premiers des entiers $1, ..., n$ mais Δ_n étant divisible par les n premiers entiers, cet exposant est maximal, et

$$v_p(\Delta_n) = \max_{1 \leq i \leq n} v_p(i)$$

Ainsi, il existe k tel que

$$p^{v_p(\Delta_n)} = p^{v_p(k)} \leq k \leq n$$

□

Théorème 4.

$$\forall n \geq 3,\ \ln(2)\frac{n}{\ln(n)} \leq \pi(n)$$

Démonstration. On sait que :

$$\forall n \geq 7, \forall p \in \mathbb{P},\ p^{v_p(\Delta_n)} \leq n \text{ par le lemme 6}$$

Donc on a,

$$\Delta_n = \prod_{p \in \mathbb{P}, p \leq n} p^{v_p(\Delta_n)} \leq n^{\pi(n)} \text{ par le lemme 5}$$

Donc, par la proposition 17, $2^n \leq n^{\pi(n)}$ et,

$$2^n \leq n^{\pi(n)} \Leftrightarrow n\ln(2) \leq \pi(n)\ln(n)$$

ce qui fournit le résultat.
Les cas $n = 3, 4, 5, 6$ se traîte à la main, et le cas $n = 2$ montre que l'inégalité n'est plus valable pour ce rang. □

$$\textbf{On en déduit enfin } H \geq \frac{\ln(2)L}{10r\ln(L)}$$

On pourrait montrer que

$$\pi(n) \sim_{+\infty} \frac{n}{\ln(n)}$$

à l'aide d'outils d'analyse complexe.

2.4 Majoration de Δ dans le cadre proposé

Nous nous plaçons dans le cas de base du crible, cité précedemment. On sait que le théorème des restes chinois permet d'identifier Y_m à $\mathbb{Z}/m\mathbb{Z}$. Choisissons la densité $v_l(y) = \frac{1}{l}$. Ainsi, pour tout entier m sans facteur carré, $v_m(y) = \frac{1}{m}$.

Proposition 18. *Une base orthonormée de Y_l pour le produit scalaire associé à la densité uniforme est :* $\varphi_a := \begin{cases} \mathbb{Z}/l\mathbb{Z} \to \mathbb{C}^* \\ x \mapsto \exp\left(\frac{2i\pi ax}{l}\right) \end{cases} \quad \forall a \in \mathbb{Z}/l\mathbb{Z}$

Démonstration. Montrons que la famille est orthonormée : $\forall a, a' \in \mathbb{Z}/l\mathbb{Z}$, $a \neq a'$

$$(\varphi_a|\varphi_{a'}) = \sum_{x\in\mathbb{Z}/l\mathbb{Z}} \exp\left(\frac{2i\pi ax}{l}\right)\exp\left(\frac{-2i\pi a'x}{l}\right)\frac{1}{l} = \frac{1}{l}\sum_{k=0}^{l-1}\left(\exp\left(\frac{2i\pi(a-a')}{l}\right)\right)^{\bar{k}} = \frac{1}{l}\frac{1-\exp(2i\pi(a-a'))}{1-\exp(\frac{2i\pi(a-a')}{l})} = 0$$

Enfin,

$$(\varphi_a|\varphi_a) = \sum_{x\in\mathbb{Z}/l\mathbb{Z}} \frac{1}{l} = 1$$

C'est évidemment une base, puisque : $\varphi := \left\{ \begin{array}{l} \mathcal{F}(\mathbb{Z}/l\mathbb{Z},\mathbb{C}) \to \mathcal{F}(\mathbb{Z}/l\mathbb{Z},\mathbb{C}) \\ \mathbb{1}_x \mapsto (x \mapsto \exp\left(\frac{2i\pi ax}{l}\right)) \end{array} \right.$ est une application linéaire bijective, elle transforme donc une base en une base. □

Par suite, la base orthonormée correspondante, pour l'espace $Y_m \simeq \mathbb{Z}/m\mathbb{Z}$ est :

$$\left(x \mapsto \exp\left(\frac{2i\pi ax}{m}\right)\right)_{a\in\mathbb{Z}/m\mathbb{Z}}$$

Remarquons enfin que

$$\mathcal{B}_m^* = \left(x \mapsto \exp\left(\frac{2i\pi ax}{m}\right)\right)_{a\in\mathbb{Z}/m\mathbb{Z}, a\wedge m=1}$$

Proposition 19. *Supposons le crible $\psi = (\mathbb{Z}^r, \mathbb{P}, \rho_l : \mathbb{Z}^r \to (\mathbb{Z}/l\mathbb{Z})^r)$, donné, avec*

$$X = \{(a_1, .., a_r) \mid M_i \leq a_i < N_i + M_i\}$$

et F l'application identité. Alors :

$$\sum_{m\leq L}\left[\sum_{\substack{(a_i)\in(\mathbb{Z}/m\mathbb{Z})^r \\ a_i\wedge m=1}}\left|\sum_{M_i<n_i\leq M_i+N_i} a_n \exp\left(\frac{2i\pi(a|n)}{m}\right)\right|^2\right] \leq \prod_{i=1}^{r}(\sqrt{N_i}+L)^2 \sum_{M_i<n_i\leq M_i+N_i}|b_n|^2$$

pour toute suite de vecteurs complexes (b_n).

On en déduit donc par la propriété 9 que

$$\Delta \leq \prod_{i=1}^{r}(\sqrt{N_i}+L)^2$$

Démonstration. On prouve le théorème dans le cas où $r = 1$ uniquement, et avec une inégalité moins forte. Montrons que :

$$\sum_{m\leq L}\left[\sum_{\substack{a\in\mathbb{Z}/m\mathbb{Z} \\ a\wedge m=1}}\left|\sum_{M<n\leq M+N} a_n \exp\left(\frac{2i\pi an}{m}\right)\right|^2\right] \leq (2\pi N + L^2)\sum_{M<n\leq M+N}|a_n|^2$$

pour toute suite de complexes (a_n). En effet : Supposons $M = 0$. Remarquons que, pour toute fonction régulière, f, une simple intégration par partie donne :

$$\int_0^1 f(t)dt + \int_0^{1/2} tf'(t)dt + \int_{1/2}^1 (t-1)f'(t)dt = f(1/2)$$

Donc,

$$|f(1/2)| \leq \int_0^1 \left[|f(t)| + \frac{1}{2}|f'(t)| \right] dt$$

Par un changement de variable,

$$|f(x)| \leq \frac{1}{\delta} \int_{x-\delta/2}^{x+\delta/2} |f(t)|dt + \frac{1}{2} \int_{x-\delta/2}^{x+\delta/2} |f'(t)|dt$$

On applique l'inégalité à :

$$f(t) = \left(\sum_{1 \leq n \leq N} a_n \exp(2i\pi nt) \right)^2$$

avec $x = a/q$, $q \leq L$, et $a \wedge q = 1$, et $\delta = L^{-2}$
On obtient :

$$\left| \sum_{1 \leq n \leq N} a_n \exp(\frac{2i\pi na}{q}) \right|^2 \leq \frac{1}{\delta} \int_{a/q-\delta/2}^{a/q+\delta/2} \left| \sum_{1 \leq n \leq N} a_n \exp(2i\pi nt) \right|^2 dt$$

$$+ \int_{a/q-\delta/2}^{a/q+\delta/2} \left| \left(\sum_{1 \leq n \leq N} a_n \exp(2i\pi nt) \right) \left(2i\pi \sum_{1 \leq n \leq N} a_n n \exp(2i\pi nt) \right) \right|$$

Les intervalles $]a/q - \delta/2; a/q + \delta/2[$ ne contiennent pas d'entier premier avec q. En utilisant la périodicité et la positivité, on en déduit :

$$\sum_{q \leq Q}^{\flat} \sum_{a \wedge q = 1} \left| \sum_{1 \leq n \leq N} a_n \exp(\frac{2i\pi na}{q}) \right|^2 \leq L^2 \int_0^1 \left| \sum_{1 \leq n \leq N} a_n \exp(2i\pi nt) \right|^2 dt +$$

$$\int_0^1 \left| \left(\sum_{1 \leq n \leq N} a_n \exp(2i\pi nt) \right) \left(2i\pi \sum_{1 \leq n \leq N} a_n n \exp(2i\pi nt) \right) \right|$$

Le $\flat$ indiquant que la somme ne se fait que sur les entiers sans facteur carré. En utilisant à gauche l'identité de Parseval, et à droite, l'inégalité de Cauchy-Schwarz, on en déduit :

$$\sum_{q \leq Q}^{\flat} \sum_{a \wedge q = 1} \left| \sum_{1 \leq n \leq N} a_n \exp\left(\frac{2i\pi na}{q} \right) \right|^2 \leq L^2 \sum_n |a_n|^2 + 2\pi \left(\sum_n |a_n|^2 \right)^{1/2} \left(\sum_n n^2 |a_n|^2 \right)^{1/2}$$

Enfin,

$$\sum_{q \leq Q}^{\flat} \sum_{a \wedge q = 1} \left| \sum_{1 \leq n \leq N} a_n \exp\left(\frac{2i\pi na}{q} \right) \right|^2 \leq (L^2 + 2\pi N) \sum_n |a_n|^2$$

□

On en déduit que

$$\Delta \leq (\sqrt{2N+1} + L)^{2r}$$

Il s'ensuit :

$$\sharp E_r(N) \leq (\sqrt{2N+1} + L)^{2r} \frac{10r \ln(L)}{\ln(2)L}$$

Prenons $L = r^{-1}\sqrt{2N+1}$. Alors,

$$\sharp E_r(N) \leq (\sqrt{2N+1} + r^{-1}\sqrt{2N+1})^{2r} \frac{10r \ln(r^{-1}\sqrt{2N+1})}{\ln(2) r^{-1}\sqrt{2N+1}} = (2N+1)^{r-1/2} \left(1 + \frac{1}{r} \right) \frac{10r^2 \ln(r^{-1}\sqrt{2N+1})}{\ln(2)}$$

Enfin,

$$\sharp E_r(N) \leq Cr^2(2N+1)^{r-1/2}\ln(2N+1)$$
$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq Cr^2\frac{\ln(N)}{\sqrt{2N+1}}$$

ce qui conclut la preuve. □

On remarque donc qu'en rendant les coefficients arbitrairement grands, la proportion de polynômes réductibles tend vers 0.

3 Théorie de Galois

3.1 Définition et premières propriétés

Définition 9. *On appelle automorphisme d'un corps $\mathbb{K}$ tout morphime de $\mathbb{K}$ dans $\mathbb{K}$ bijectif, compatible avec les deux lois de composition interne, et laissant fixe le neutre.*

Définition 10. *Soit $\mathbb{K}$ un corps et L une extension. On appelle $\mathbb{K}-$automorphisme du corps L tout automorphisme de L, laissant fixe les élements de $\mathbb{K}$.*

Définition 11. *Soit $\mathbb{K}$ un corps et L une extension. On appelle groupe de Galois de L sur $\mathbb{K}$ et on note $Gal(L/\mathbb{K})$ l'ensemble des $\mathbb{K}-$automorphismes de L.*

Proposition 20. *C'est un groupe pour la composition des applications.*

Démonstration. On sait que l'identité est une application bijective, qui est compatible avec les opérations et qui laisse par définition fixe les éléments de $\mathbb{K}$.
La composition de deux applications bijectives l'est, elle respecte toujours les lois, et laisse fixe les éléments de $\mathbb{K}$. Enfin, tout élément bijectif admet un inverse pour la composition qui vérifie les mêmes propriétés.
Donc, $(Gal(L/\Bbbk), \circ)$ est un groupe comme sous-groupe de $(\mathrm{Aut}(L), \circ)$ □

Exemple. $Gal(\mathbb{R}/\mathbb{Q}) = \{I_d\}$
En effet, l'application idendité convient. Réciproquement, soit $\varphi : \mathbb{R} \to \mathbb{R}$ laissant fixe $\mathbb{Q}$, compatible avec les opérations (on peut même se passer de l'hypothèse de bijectivité).
Alors, $\forall x \in \mathbb{R}^+$, $\exists y \in \mathbb{R}$ tel que $x = y^2$, donc, $\varphi(x) = \varphi(y)^2 \geq 0$. Par suite, si $x, y \in \mathbb{R}$ avec $x \leq y$ alors $\varphi(y-x) = \varphi(y) - \varphi(x) \geq 0$ et φ est croissante. Or, par densité, $\forall x \in \mathbb{R}, \exists (x_n)_{n\in\mathbb{N}}$, croissante, et $(y_n)_{n\in\mathbb{N}}$ décroissante, suites de rationnels, de limite commune x.
Donc, $x_n \leq x \leq y_n$, soit $x_n \leq \varphi(x) \leq y_n$. Un passage à la limite permet de conclure.

Lemme 7. *(Lemme de Dedekind) Soit G un groupe, $\mathbb{K}$ un corps, et une famille $(\sigma_i)_{i\in I}$ de morphismes de G dans $\mathbb{K}^*$, tous distincts. Alors, la famille est libre sur $\mathbb{K}$.*

Démonstration. On raisonne par récurrence sur $|I|$. La proposition est vraie au rang 1, puisque, si $\lambda\sigma = 0$, il suffit d'évaluer cette égalité en l'élément neutre de G pour conclure que $\lambda = 0$.

On suppose le résultat acquis au rang n. Soient $\sigma_1, ..\sigma_{n+1}$ des morphismes distincts de G dans $\mathbb{K}^*$. Soient $\lambda_1, .., \lambda_{n+1}$ tels que $\sum_{i=1}^{n+1} \lambda_i \sigma_i = 0$. Par suite,

$$\forall x, y \in G,\ \sum_{i=1}^{n+1} \lambda_i \sigma_i(x)\sigma_i(y) = 0$$

Or,

$$\forall x, y \in G,\ \sum_{i=1}^{n+1} \lambda_i \sigma_i(x)\sigma_n(y) = 0$$

Donc,

$$\forall x, y \in G,\ \sum_{i=1}^{n} \lambda_i \sigma_i(x)(\sigma_i(y) - \sigma_n(y)) = 0$$

Donc, par hypothèse de récurrence,

$$\forall y \in G, \forall i \in \{1, ..., n\}, (\sigma_i(y) - \sigma_n(y))\lambda_i = 0\ (*)$$

Or, on sait que les σ_i sont distincts deux à deux, donc, on peut appliquer $(*)$ pour un y tel que $\sigma_i(y) - \sigma_n(y) \neq 0$. Par suite, $\forall i \in \{1, ..., n\}, \lambda_i = 0$, on reporte ceci dans l'égalité de départ et on obtient, $\lambda_{n+1}\sigma_{n+1} = 0$. L'initialisation conclut.

Le résultat est désormais vrai pour un intervalle I quelconque puisque toute combinaison linéaire est nécessairement finie. □

Théorème 5. *Soit $\mathbb{K}$ un corps et L une extension de degré fini. Alors,*

$$|Gal(L/\mathbb{K})| \leq [L : \mathbb{K}]$$

Démonstration. On raisonne par l'absurde. On note $n = [L : \mathbb{K}]$. Supposons que $|Gal(L/\mathbb{K})| > n$. Alors, on peut trouver $(n+1)$ $\mathbb{K}-$automorphismes de corps L, distincts. Soit $(x_1, .., x_n)$ une base du $\mathbb{K}-$espace vectoriel L. On note $M = (\sigma_j(x_i))_{(i,j)\in\{1,..,n\}\times\{1,..,n+1\}}$. Les vecteurs colonnes de la matrice sont au nombre de $n+1$ dans un espace vectoriel de dimension n, donc sont liés. On peut donc trouver $\lambda_1, .., \lambda_{n+1}$ des scalaires non tous nuls tels que :

$$\sum_{k=1}^{n+1} \lambda_k C_k = 0 \text{ i.e. } \forall i \in \{1, .., n\},\ \sum_{k=1}^{n+1} \lambda_k \sigma_k(x_i) = 0$$

Donc, l'application linéaire $\sum_{k=1}^{n+1} \lambda_k \sigma_k$ s'annule sur une base, elle est par conséquent nulle. Or, les scalaires ne sont pas tous nuls. La famille est donc liée. Or, le lemme précédent affirme que la famille est libre, ce qui fournit la contradiction cherchée. □

Définition 12. *Soit $\mathbb{K}$ un corps. On appelle extension galoisienne finie de $\mathbb{K}$ toute extension L, de degré fini vérifant : $|Gal(L/\mathbb{K})| = [L : \mathbb{K}]$*

3.2 Séparabilité et normalité

Définition 13. *Soit a un nombre algébrique sur un corps $\mathbb{K}$. Soit :*

$$I(a) := \{P \in \mathbb{K}[X] |\ P(a) = 0\}$$

C'est un idéal non nul de $\mathbb{K}[X]$, qui est principal donc, $\exists \pi_a^{\mathbb{K}}$ unitaire tel que $I(a) = \pi_a^{\mathbb{K}}\mathbb{K}[X]$. Ce polynôme est appelé polynôme minimal de a sur $\mathbb{K}$.

Proposition 21. *Soit P un polynôme de $\mathbb{K}[X]$, et a un nombre algébrique sur $\mathbb{K}$, alors :*

$$P = \pi_a^{\mathbb{K}} \text{ ssi } P \text{ est unitaire, } P(a) = 0 \text{ et } P \text{ est irréductible dans } \mathbb{K}[X].$$

Démonstration. Pour le sens direct, le polynôme est bien unitaire et vérifie $P(a) = 0$ par définition. Montrons qu'il est irréductible.
Soit $D \in \mathbb{K}[X]$ tel que $D|P = \pi_a^{\mathbb{K}}$, alors $\exists G \in \mathbb{K}[X]$ tel que $P = \pi_a^{\mathbb{K}} = D.G$, donc, $D(a)G(a) = 0$
Si $G(a) = 0$, alors $P = \pi_a^{\mathbb{K}}|G$, donc les polynômes sont associés, par suite, D est constant.
Sinon, $D(a) = 0$, donc D est associé à $P = \pi_a^{\mathbb{K}}$
Réciproquement, on sait que $\forall P \in \mathbb{K}[X]$ tel que $P(a) = 0$, $P \in \pi_a^{\mathbb{K}}\mathbb{K}[X]$, donc, $\pi_a^{\mathbb{K}}|P$. Or, P est irréductible, donc les polynômes sont associés, étant unitaires, on peut conclure à leur égalité. □

Définition 14.

1. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré ≥ 1. On dit que P est séparable si P et P' sont premiers entre eux (dans $\mathbb{K}[X]$).*
2. *Soit L une extension de $\mathbb{K}$. À tout élément algébrique α sur $\mathbb{K}$, on associe son polynôme minimal $\pi_\alpha^{\mathbb{K}}$. On dit que α est séparable sur $\mathbb{K}$ si son polynôme minimal l'est.*
3. *Soit L une extension de $\mathbb{K}$. On dit que L est une extension séparable si tout élément de L est séparable dans $\mathbb{K}$.*

Définition 15. *Soit $\mathbb{K}$ un corps, et L une extension algébrique de $\mathbb{K}$. On dit que L est une extension normale (ou quasi-galoisienne) si, chaque fois qu'un polynôme irréductible à coefficients dans $\mathbb{K}$ a une racine dans L, alors il est scindé sur L.*

Théorème 6. *(Admis) Soit $\mathbb{K}$ un corps et L une extension de degré fini. Alors, les conditions suivantes sont équivalentes :*

1. *$L/\mathbb{K}$ est une extension galoisienne, i.e. $|Gal(L/\mathbb{K})| = [L : \mathbb{K}]$. (définition 12)*
2. *$L/\mathbb{K}$ est normale et séparable.*

Référence : Théorie de Galois - Ivan Gozard, Théorème XI.25., page 137.

Définition 16. *Soit $\mathbb{K}$ un corps, et L une extension de $\mathbb{K}$. Soit $P \in \mathbb{K}[X]$ avec $n = \deg(P)$. On dit que L est un corps de décomposition de P si*

1. *$\exists a \in L$, $\exists(\alpha_1, .., \alpha_n) \in L$ telle que $P = a(X - \alpha_1) \cdots (X - \alpha_n)$.*
2. *$L = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$.*

Définition 17. *Soit $\mathbb{K}$ un corps. On appelle groupe de Galois d'un polynôme $f \in \mathbb{K}[X]$ le groupe de Galois de son corps de décomposition K_f sur $\mathbb{K}$.*

$$Gal_{\mathbb{K}}(f) = Gal(K_f/\mathbb{K})$$

Proposition 22. *Soit $f \in \mathbb{K}[X]$ un polynôme de degré $d \geq 1$. On peut plonger $Gal_{\mathbb{K}}(f)$ dans le groupe symétrique $\mathfrak{S}_d$.*

Démonstration. Soit f un polynôme de degré d. On considère le corps de décomposition de f, $\mathbb{K}_f = \mathbb{K}(\alpha_1, \cdots, \alpha_d)$, où les α_i sont les racines de f dans une clôture algébrique, L, de $\mathbb{K}$.
$\forall \sigma \in Gal_{\mathbb{K}}(f)$, on sait que σ vaut l'identité sur $\mathbb{K}$. Son action consiste donc en une permutation (car elle est bijective) des racines de f, donc elle s'identifie naturellement à un élément de $\mathfrak{S}_d$. □

Définition 18. *Soit A un anneau commutatif et B une $A-$algèbre. On dit que $b \in B$ est entier sur A s'il existe un polynôme unitaire à coefficients dans A qui annule b.*

Définition 19. *Soit A et B deux anneaux commutatifs, $A \subseteq B$. On dit que B est finiment engendré sur A, ou de type fini sur A, s'il existe $b_1, .., b_r \in B$ tels que tout élément de B puisse s'écrire $\sum_{i=1}^{r} a_i b_i$ avec $\forall i \in \{1, .., r\}$, $a_i \in A$.*

Proposition 23. *Soit A un anneau commutatif, B une $A-$algèbre, et $b \in B$. Alors,*

1. *b est entier sur A ssi $A[b]$ est finiment engendré sur A.*
2. *Soit $A \subseteq B \subseteq C$ des anneaux commutatifs tels que B est finiment engendré par A, et C est finiment engendré sur B, alors, C est finiment engendré sur A.*
3. *Si $b_1, .., b_r \in B$ sont des entiers sur A, alors $A[b_1, .., b_r]$ est finiment engendré sur A.*

Démonstration.

1. Pour le premier point, supposons que b est entier sur A. Alors, on peut trouver $P = \sum_{i=0}^{m} p_i X^i \in A[X]$ tel que $P(b) = 0$, P unitaire. Soit $c \in A[b]$. Alors, $c = \sum_{i=0}^{r} a_i b^i$ avec $a_i \in A$. Par suite, $b^m = -\sum_{j=0}^{m-1} p_i . b^i$. Ceci permet d'assurer que m est une borne uniforme des puissance de b, donc, la famille $\left\{b^0, ..., b^{m-1}\right\}$ est génératrice et $A[b]$ est de type fini sur A.

   Réciproquement, si $A[b]$ est finiment engendré, alors : on peut trouver $b_0, .., b_r$ qui engendre A. Par suite, on sait que $b = \sum_{i=0}^{r} a_i b_i$. Le polynôme $X - \sum_{i=0}^{r} a_i b_i$ convient.
2. On note $\{b_1, .., b_r\}$ et $\{c_1, .., c_s\}$ les familles génératrices respectives. On sait que :

$$\forall c \in C, \exists \beta_1, .., \beta_s \in B \text{ tel que } c = \sum_{j=1}^{s} \beta_j c_j$$

   Or, $\forall 1 \leq j \leq s, \exists \alpha_1^j, .., \alpha_r^j$ vérifiant : $\beta_j = \sum_{i=1}^{r} \alpha_i^j b_i$. Par suite,

$$c = \sum_{j=1}^{s} \sum_{i=1}^{r} \alpha_i^j b_i c_j$$

   et la famille $\{b_i c_j, 1 \leq i \leq r,\ 1 \leq j \leq s\}$ convient.
3. On sait que $A \subseteq A[b_1] \subseteq ... \subseteq A[b_1, ..b_r]$. Le premier point de la proposition assure que les ensembles sont finiment générés de proche en proche. Le point 2 permet de conclure.

□

Lemme 8. *Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible, de degré d. Soit p un nombre premier et f_p l'image de f dans $\mathbb{F}_p[X]$. Supposons que f_p admette d racines dans une clôture algébrique de $\mathbb{F}_p$, alors, $Gal_{\mathbb{F}_p}(f_p)$ est isomorphe à un sous-groupe de $Gal_{\mathbb{Q}}(f)$.*

Démonstration. Admis □

Théorème 7. *Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible, de degré d. Soit p un nombre premier et f_p l'image de f dans $\mathbb{F}_p[X]$. Supposons que f_p admette d racines dans une clotûre algébrique de $\mathbb{F}_p$ et qu'il s'écrive comme produit de r facteurs irréductibles sur $\mathbb{F}_p$ de degré n_1,..,n_r, alors, vu comme un sous-groupe de $\mathfrak{S}_d$, $Gal_{\mathbb{Q}}(f)$ contient une permutation σ pouvant s'écrire comme un produit de r cycles à supports disjoints de longueurs respectives $n_1, ..n_r$.*

Démonstration. Écrivons f comme le produit de ses r facteurs irrédictibles, $f = g_1..g_r$, où $g_1, .., g_r$ sont des polynômes irréductibles sur $\mathbb{F}_p$ de degrés respectifs $n_1, .., n_r$. On commence par montrer que l'on peut trouver cette permutation dans le groupe de Galois de f_p, c'est-à-dire $Gal_{\mathbb{F}_p}(f_p)$.
Puisque l'extension est finie, et que le corps est lui aussi fini, alors, le groupe de Galois est cyclique, engendré par σ. Afin de déterminer la décomposition en produit de cycles à supports disjoints de cette permutation, on examine l'action de $Gal_{\mathbb{F}_p}(f_p)$ sur les racines de f_p, et on détermine les orbites de cette action.
On note, α_{ij} les racines de g_i où $i \in \{1, ..r\}$ et $j \in \{1, .., n_i\}$.
Or,

$$\text{Orb}(\alpha_{11}) = \left\{\tau(\alpha_{11})|\ \tau \in Gal_{\mathbb{F}_p}(f_p)\right\} = \left\{\sigma^i(\alpha_{11}), i \in \{1, ..t\}\right\}$$

puisque σ est générateur, et t est le plus entier naturel non nul, vérifiant $\sigma^t(\alpha_{11}) = \alpha_{11}$.

Montrons que $t = n_1$.
Remarquons d'abord que, pour tout j,

$$g_1(\sigma^j(\alpha_{11})) = \sum_{i=1}^{r} a_i(\sigma^j(\alpha_{11}))^i = \sigma^j(\sum_{i=1}^{r} a_i\alpha_{11}^i) = \sigma^j\left(g_1(\alpha_{11})\right) = 0$$

Par suite, les $\sigma^j(\alpha_{11})$ sont racines de g_1, donc, $t \leq n_1$. Enfin, si on se donne α_{1j} une racine de g_1, alors, on peut trouver un isomorphisme de corps, τ qui envoie α_{11} sur α_{1j}. On étend cet élément en un élément de $Gal_{\mathbb{F}_p}(f_p)$, et, puisque σ est générateur, on a : $\tau = \sigma^s$ pour un certain s, et α_{1j} est dans l'orbite de α_{11}. Il s'ensuit $t = n_1$, donc, une partie de la décomposition en produit de cycles à supports disjoints de σ est le n_1-cycle : $(\alpha_{11}, .., \sigma^{n_1-1}(\alpha_{11}))$.
On réitère le principe avec les racines de g_2,..g_r et on a déterminé une décomposition en produits de cycles de σ. Étant unique à l'ordre près des facteurs, on en déduit le résultat.
On utilise l'isomorphisme entre $Gal_{\mathbb{F}_p}(f_p)$ et un sous-groupe de $Gal_{\mathbb{Q}}(f)$ pour conclure (lemme 8). □

4 Théorème de Gallagher pour les groupes de Galois

4.1 Groupe symétrique

Définition 20. *Soit G un groupe et X un ensemble, on dit que G agit transitivement sur X si X est non vide, et si $\forall x, y \in X$, $\exists g \in G$ tel que $y = g.x$, où . représente l'action du groupe.*

Lemme 9. *Soit G un sous-groupe de $\mathfrak{S}_n$, transitif, contenant une transposition et un $p-$cycle, avec p premier, $p > n/2$, alors $G = \mathfrak{S}_n$*

Démonstration. Puisque $\mathfrak{S}_n$ est engendré par les transpositions, il suffit de vérifier que G contient toutes les transpositions, c'est-à-dire, en considérant les graphes de sommets $1, 2.., n$, qu'il est complet. (On considère un graphe où une arête entre deux sommets i et j symbolise la présence de la transposition (ij) dans le groupe G).
Supposons $(ij), (jk) \in G$. Alors, $(ik) = (ij)(jk)(ij)$ aussi. Chaque composante connexe de G est donc complète.
Or G agit transitivement, donc les composantes connexes sont de même cardinal, d, avec $d|n$.
Si l'on suppose qu'il existe une composante connexe de G qui ne laisse pas stable le $p-$cycle, alors, il y a au moins p composantes, puisque l'équation au classe assure qu'il existe une orbite de cardinal p et, $dp \leq n$ ce qui assure $d = 1$, impossible car G contient une transposition. Par suite, $d = n$, Ainsi, le graphe est connexe, donc complet. □

Lemme 10. *Soit c la classe de conjugaison de $\sigma \in \mathfrak{S}_r$, une permutation de type $(n_1, .., n_r)$, i.e. possédent n_1 cycles de taille 1 (point fixe), ..., n_r cycles de taille r. Alors,*

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

Démonstration. La relation orbite-stabilisteur (classe de conjugaison-centralisateur) fournit :

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

Commençons par nous intéresser au cas d'un $k-$cycle, $c = (i_1, .., i_k)$. On sait que, pour tout $\tau \in C_{\mathfrak{S}_r}(c)$, on a : $\tau c \tau^{-1} = c$.
Par suite, $\tau c \tau^{-1} = (\tau(i_1), .., \tau(i_k)) = (i_1, .., i_k) = c$. Pour ceux, il suffit de fixer l'image du premier élément, il y a donc k possibilités. Enfin, il est nécessaire d'attribuer de manière bijective une image aux $(r - k)$ éléments, il y a $(r - k)!$ possibilités. Donc,

$$|c| = \frac{r!}{k(r-k)!} = (k-1)! \binom{r}{k}$$

Dans le cas général, écrivons $c = \prod_{i=1}^{p} c_i$ avec $p = \sum_{i=1}^{r} n_i$, où les c_i sont les cycles de la décomposition en produit de cycles à supports disjoints. $\forall \tau \in C_{\mathfrak{S}_n}(c)$, $\tau c \tau^{-1} = \prod_{i=1}^{p} \tau c_i \tau^{-1} = c = \prod_{i=1}^{p} c_i$. Par suite, chacun des $\tau c_i \tau^{-1}$ corrrespond au c_i, il y a donc $n_i!$ possibilités d'associer entre eux les cycles de même ordre. Il y a pour chaque cycle i possibilités comme vu dans l'exemple précédent. Étant à supports disjoints, on en déduit l'égalité. □

4.2 Application du grand crible

Théorème 8. *(de Gallagher) Soient N et r deux entiers naturels, $r > 2$.*
Définissons :

$$E_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N,\ \textit{tel que } Gal_{\mathbb{Q}}(f) \not\simeq \mathfrak{S}_r \right\}$$

$$X_r(N) := \left\{ X^r + \sum_{i=0}^{r-1} a_i X^i \in \mathbb{Z}_r[X],\ \forall i, |a_i| \leq N \right\}$$

Alors,

$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq C r^3 \frac{\ln(N)}{\sqrt{2N+1}}$$

où C est une constante absolue.

Démonstration. On note :

$$\Omega_l^{r\ irr} = \{f \in \mathbb{F}_l[X], \deg(f) = r, \text{ unitaire irréductible}\}$$

$\Omega_l^{r\ transp} = \{f \in \mathbb{F}_l[X], \deg(f) = r, \text{de type : irréductible de degré 2} \times \text{irréductibles de degré impair}\}$

$\Omega_l^{r\ p-cy} = \{f \in \mathbb{F}_l[X], \deg(f) = r, \text{possédant un facteur irréductible de degré } p, \text{ premier, } p > r/2\}$

On remarque premièrement que :

- Si f mod p appartient à $\Omega_l^{r\ transp}$, alors le groupe $Gal_{\mathbb{Q}}(f)$ possède une permutation dont la décomposition en produit de cycles s'écrit : $\sigma = \tau.\gamma_1, .., \gamma_q$ (par le théorème 7). Ainsi, $\sigma^{ppcm(o(\gamma_1),..,o(\gamma_q))} = \tau \in Gal_{\mathbb{Q}}(f)$ donc le groupe possède une transposition.
- De la même façon, si f mod p appartient à $\Omega_l^{r\ p-cy}$, alors $Gal_{\mathbb{Q}}(f)$ possède un $p - cycle$, avec p premier, et $p > r/2$.

Par suite, le lemme 9 montre que :

$$\sharp E_r(N) \leq |S(X, \Omega_l^{r\ irr}, \mathcal{L}^*)| + |S(X, \Omega_l^{r\ transp}, \mathcal{L}^*)| + |S(X, \Omega_l^{r\ p-cy}, \mathcal{L}^*)|$$

L'application de l'inégalité du grand crible se fait avec :

$$Y = \mathbb{Z}_r[X] \quad \Lambda = \mathbb{P} \quad Y_l = \mathbb{F}_r^l[X] \quad \rho_l \text{ est le morphisme quotient}$$

$$X = X_r(N) \quad F = I_d \quad \mathcal{L}^* = \{p \in \mathbb{P}\ p \leq L\} \quad \Omega_l = \left\{P \in \mathbb{F}_r^l[X], \text{ irréductible}\right\}$$

$$\forall f \in \mathbb{F}_r^l[X],\ v_l(f) = \frac{1}{l^r}$$

Elle affirme que :

$$\sharp E_r(N) \leq \Delta \left[H_{irr}^{-1} + H_{transp}^{-1} + H_{p-cy}^{-1}\right]$$

La majoration établie dans le grand 2 est toujours valable et, $\Delta \leq (\sqrt{2N+1} + L)^{2r}$.

De plus, la majoration de H_{irr}^{-1} a déjà été établie dans le grand 2, et on a : $H_{irr}^{-1} \leq \dfrac{10r\ln(L)}{L\ln(2)}$.
Il est donc nécessaire d'estimer H_{transp}^{-1} et H_{p-cy}^{-1}.

4.2.1 Premier type de décomposition

L'inégalité du grand crible fournit :

$$H_{p-cy} \geq \sum_{l \in \mathbb{P}, l \leq L} \frac{|\Omega_l^{r\ p-cy}|}{l^r}$$

Or

$$\frac{|\Omega_l^{r\ p-cy}|}{l^r} \sim \sum_{r/2 < p \leq r} \frac{|\left\{\sigma \in \mathfrak{S}_r\ \sigma \text{ contient un } p\text{-cycle}\right\}|}{r!}$$

On cherche à expliciter : $|\left\{\sigma \in \mathfrak{S}_r\ \sigma \text{ contient un } p\text{-cycle}\right\}|$.
Il faut commencer par choisir p éléments parmi les r disponibles afin de constituer le cycle : il y a $\binom{r}{p}$ possibilités. On choisit le premier élément : p possibilités, puis le deuxième, soit $(p-1)$ possibilités, etc.., soit $p!$ choix. Or, si l'on décale chaque élément d'un rang, on obtient le même cycle ($(123) = (231) = (312)$). Le même $p-$cycle a donc été comptabilisé p fois. Il faut donc diviser le résultat par p. On constitue enfin une permutation en attribuant au $(r-p)$ éléments restants, il y a donc $(r-p)!$ possibilités. Par suite,

$$|\left\{\sigma \in \mathfrak{S}_r\ \sigma \text{ contient un } p\text{-cycle}\right\}| = \binom{r}{p}(r-p)!(p-1)!$$

$$\frac{|\Omega_l^{r\ p-cy}|}{l^r} \sim \sum_{r/2<p\leq r} \frac{\binom{r}{p}(r-p)!(p-1)!}{r!} = \sum_{r/2<p\leq r} \frac{1}{p} \geq C\left[\ln(\ln(r)) - \ln(\ln(r/2))\right] = C\ln\left(\frac{\ln(r)}{\ln(r)-\ln(2)}\right)$$

La première inégalité valant par le théorème de Mertens, qui est démontré dans l'annexe. Donc,

$$\frac{|\Omega_l^{r\ p-cy}|}{l^r} \geq C\ln\left(1+\frac{\ln(2)}{\ln(r)}\right) \geq C\frac{\ln(2)}{\ln(r)}$$

La constante C est absolue, elle change de ligne en ligne, sans modification de notation, pour ne pas les alourdir. Par suite,

$$H_{p-cy} \geq \sum_{l\in\mathbb{P}, l\leq L} C\frac{\ln(2)}{\ln(r)} \geq C\frac{L}{\ln(r)\ln(L)}$$

par l'encadrement de la fonction de répartition des nombres premiers qui a été établi précédemment.

4.2.2 Deuxième type de décomposition

Une nouvelle fois, on utilise l'identité :

$$\frac{|\Omega_l^{r\ transp}|}{l^r} \sim \frac{|\{\sigma\in\eta_1\}|}{r!} = \sum_{\substack{n_1+2n_2+..+rn_r=r\\ n_2=1, n_4=n_6=..=0}} \prod_{i=1}^{r} \frac{r!}{i^{n_i}i!}.\frac{1}{r!}$$

grâce au lemme 10. Cette quantité correspond au coefficient de x^{r-2} de la quantité :

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

On obtient donc un équivalent à l'aide de la formule de Stirling :
Si r est pair : $\frac{(r-1)!}{4^{\frac{r}{2}-1}.((\frac{r}{2}-1)!)^2} \sim \frac{1}{\sqrt{2\pi r}}$
Idem si r est impair.

$$\frac{|\Omega_l^{r\ transp}|}{l^r} \sim \frac{1}{\sqrt{2\pi r}}$$

Enfin,

$$H_{transp} \geq C\frac{L}{\ln(L)\sqrt{r}}$$

On en déduit donc que :

$$\sharp E_r(N) \leq (\sqrt{2N+1}+L)^{2r}\left[\frac{10r\ln(L)}{L\ln(2)} + C\frac{\ln(r)\ln(L)}{L} + C'\frac{\ln(L)\sqrt{r}}{L}\right]$$

$$\sharp E_r(N) \leq (\sqrt{2N+1}+L)^{2r}\frac{\ln(L)}{L}\left[\frac{10r}{\ln(2)} + C\ln(r) + C'\sqrt{r}\right]$$

Posons $L = \frac{\sqrt{2N+1}}{r}$ On obtient :

$$\sharp E_r(N) \leq C''(2N+1)^{r-1/2}\ln(N)r.\left[\frac{10r}{\ln(2)} + C\ln(r) + C'\sqrt{r}\right] \leq C\ln(N)r^3(2N+1)^{r-1/2}$$

Enfin,

$$\frac{\sharp E_r(N)}{\sharp X_r(N)} \leq C\frac{\ln(N)r^3}{\sqrt{2N+1}}$$

□

5 Annexe : Majoration de $\pi(n)$ et théorème de Mertens

5.1 Majoration de $\pi(n)$

Lemme 11.

$$\forall m \in \mathbb{N}^*, \quad \prod_{\substack{p\in\mathbb{P}\\ m+1<p\leq 2m+1}} p \,|\, \binom{2m+1}{m+1}$$

Démonstration. On sait que :

$$\binom{2m+1}{m+1} = \frac{(2m+1)...(m+2)}{m!} \text{ donc }, m!\binom{2m+1}{m+1} = (2m+1)..(m+2) = N. \prod_{\substack{p\in\mathbb{P}\\ m+1<p\leq 2m+1}} p$$

Par suite,

$$\prod_{\substack{p\in\mathbb{P}\\ m+1<p\leq 2m+1}} p \,\Big|\, m!\binom{2m+1}{m+1}$$

La décomposition en produits de facteurs premiers de $m!$ est le produit des décompositions en facteurs premiers des entiers de 1 à m. Elle ne contient donc que des entiers inférieurs à m. De plus, les premiers du produit sont tous supérieurs à $m+1$. Donc,

$$\left(\prod_{\substack{p\in\mathbb{P}\\ m+1<p\leq 2m+1}} p\right) \wedge m! = 1.$$

Le lemme de Gauss fournit le résultat énoncé. □

Proposition 24.

$$\forall n \in \mathbb{N}^*, \quad \prod_{p\in\mathbb{P}, p\leq n} p \leq 4^n$$

Démonstration. Remarquons premièrement que :

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

D'où

$$\binom{2m+1}{m+1} \leq 2^{2m} = 4^m$$

Soit

$$\mathcal{P}_n : \forall k \in \{1,..,2n\}, \quad \prod_{p\in\mathbb{P}, p\leq k} p \leq 4^k$$

Prouvons $\mathcal{P}_n$ par récurrence :
Si $n = 1$, alors

$$\prod_{p\in\mathbb{P}, p\leq 1} p = 1 \leq 4 \text{ et } \prod_{p\in\mathbb{P}, p\leq 2} p = 2 \leq 16$$

Supposons le résultat acquis au rang n, il faut prouver $\mathcal{P}_{n+1}$. Grâce à l'hypothèse de récurrence, il suffit de montrer que le résultat est vrai pour $k = 2n+1$ et $k = 2n+2$. Or, $2n+2$ étant pair, $\prod_{p\in\mathbb{P}, p\leq 2n+1} p = \prod_{p\in\mathbb{P}, p\leq 2n+2} p$ et il suffit de montrer le résultat pour $k = 2n+1$.

$$\prod_{p\in\mathbb{P}, p\leq 2n+1} p = \prod_{p\in\mathbb{P}, p\leq n+1} p \prod_{\substack{p\in\mathbb{P}\\ n+1<p\leq 2n+1}} p \leq 4^{n+1}.\binom{2n+1}{n+1}$$

en utilisant l'hypothèse de récurrence et la relation de divisibilité du lemme 11. Par la remarque formulée en début de preuve,

$$\prod_{p\in\mathbb{P},p\leq 2n+1} \leq 4^{n+1}.4^n = 4^{2n+1}$$

ce qui conclut l'hérédité. □

Proposition 25.

$$\forall n \geq 2,\ \pi(n)! \leq 4^n$$

Démonstration.

$$\pi(n)! \leq \prod_{i=1}^{\pi(n)} p_i = \prod_{p\in\mathbb{P},p\leq n} p \leq 4^n$$

où $(p_n)_{n\in\mathbb{N}}$ est la suite ordonnée des nombres premiers, la dernière inégalité valant en vertu de la proposition 24. □

Lemme 12.

$$\forall n \geq 2,\ (\ln(\pi(n)) - 1)\pi(n) \leq n\ln(4)$$

Démonstration. Montrons que :

$$\forall m \in \mathbb{N}^*,\ \left(\frac{m}{e}\right)^m < m!$$

Il suffit de constater que,

$$e^m = \sum_{k=0}^{+\infty} \frac{m^k}{k!},\ \text{donc}\ \left(\frac{e}{m}\right)^m - \frac{1}{m!} = \sum_{k=0}^{m-1} \frac{m^{k-m}}{k!} + \sum_{k=m+1}^{+\infty} \frac{m^{k-m}}{k!} > 0$$

Par suite, d'après la proposition 25,

$$\left(\frac{\pi(n)}{e}\right)^{\pi(n)} < \pi(n)! \leq 4^n$$

Il suffit d'appliquer le logarithme népérien à l'inégalité pour conclure. □

Théorème 9.

$$\forall n \geq 3,\ \pi(n) \leq e\frac{n}{\ln(n)}$$

Démonstration. On raisonne par l'absurde en supposant qu'il existe $n_0 \geq 3$ tel que $\pi(n_0) > e\dfrac{n_0}{\ln(n_0)}$
$f : x \mapsto x\ln(x) - x$ est une application strictement croissante sur $[1;+\infty[$.
De plus, $n_0 \geq 3 \Rightarrow \dfrac{n_0}{\ln(n_0)} > 1$, donc $\pi(n_0) \geq e\dfrac{n}{\ln(n)} \geq e > 1$, il vient :

$$f(\pi(n_0)) > f\left(e\frac{n}{\ln(n)}\right)$$

i.e.

$$n_0\ln(4) \geq \pi(n_0)\ln(\pi(n_0)) - \pi(n_0) > en_0 - en_0\frac{\ln(\ln(n_0))}{\ln(n_0)}$$

en exploitant le lemme 12. D'où,

$$\frac{e-\ln(4)}{e} < \frac{\ln(\ln(n_0))}{\ln(n_0)}$$

Or, une simple étude de fonction fournit que $x \mapsto \dfrac{\ln(x)}{x}$ admet un maximum global : e^{-1}
Par suite,

$$\frac{e - \ln(4)}{e} < e^{-1}$$

ce qui est faux, d'où le résultat. □

On en déduit donc l'encadrement suivant :

$$\forall n \geq 3,\ \ln(2)\frac{n}{\ln(n)} \leq \pi(n) \leq e\frac{n}{\ln(n)}$$

C'est la clef pour démontrer le théorème de Mertens.

5.2 Théorème de Mertens

Théorème 10.

$$\sum_{p\in\mathbb{P}, p\leq L} \frac{1}{p} = O_{+\infty}(\ln(\ln(L))$$

Démonstration.

$$\sum_{p\in\mathbb{P}, p\leq L} \frac{1}{p} = \sum_{k=2}^{L} \frac{\pi(k) - \pi(k-1)}{k} = \frac{\pi(L)}{L} + \sum_{k=2}^{L-1}\left(\frac{\pi(k)}{k} - \frac{\pi(k)}{k+1}\right) = \frac{\pi(L)}{L} + \frac{1}{6} + \sum_{k=3}^{L-1}\frac{\pi(k)}{k(k+1)}$$

Or,

$$\ln(2)\frac{n}{\ln(n)} \leq \pi(n) \leq e\frac{n}{\ln(n)}$$

Donc,

$$\frac{\pi(L)}{L} + \frac{1}{6} + \ln(2)\sum_{k=3}^{L-1}\frac{1}{\ln(k)(k+1)} \leq \sum_{p\in\mathbb{P}, p\leq L}\frac{1}{p} \leq \frac{\pi(L)}{L} + \frac{1}{6} + e\sum_{k=3}^{L-1}\frac{1}{\ln(k)(k+1)}$$

D'une part, à l'aide d'une comparaison série-intégrale,

$$\sum_{k=3}^{L-1}\frac{1}{\ln(k)(k+1)} = \sum_{k=4}^{L}\frac{1}{\ln(k-1)k} \geq \sum_{k=4}^{L}\frac{1}{\ln(k)k} \geq \sum_{k=4}^{L}[\ln(\ln(k+1)) - \ln(\ln(k))] = \ln(\ln(L+1)) - \ln(\ln(4))$$

D'autre part,

$$\sum_{k=3}^{L-1}\frac{1}{\ln(k)(k+1)} \leq \sum_{k=3}^{L-1}\frac{1}{\ln(k)k} \leq \sum_{k=3}^{L-1}[\ln(\ln(k)) - \ln(\ln(k-1))] = \ln(\ln(L-1)) - \ln(\ln(2))$$

Enfin, puisque

$$\frac{\ln(2)}{\ln(n)} \leq \frac{\pi(n)}{n} \leq \frac{e}{\ln(n)}$$

Alors,

$$\gamma(L) := \frac{\ln(2)}{\ln(L)} + \frac{1}{6} + \ln(2)(\ln(\ln(L)) - \ln(\ln(4)) \leq \sum_{p\in\mathbb{P}, p\leq L}\frac{1}{p} \leq \frac{e}{\ln(L)} + \frac{1}{6} + e(\ln(\ln(L)) - \ln(\ln(2)) := \delta(L)$$

On a de plus :

$$\lim_{L\to+\infty}\frac{\gamma(L)}{\ln(\ln(L))} = \ln(2) \text{ et } \lim_{L\to+\infty}\frac{\delta(L)}{\ln(\ln(L))} = e$$

Les suites convergent donc sont bornées, et il existe λ, μ tel que

$$\lambda\ln(\ln(L)) \leq \sum_{p\in\mathbb{P}, p\leq L}\frac{1}{p} \leq \mu\ln(\ln(L))$$

ce qui conclut. □

Références

[1] Emmanuel KOWALSKI. *The Large Sieve and its Applications : Artithmetic Geometry, Random Walks and Discrete Groups.*. Cambridge University Press, 2008.

[2] Yvan GOZARD. *Théorie de Galois*, Ellipses, 2ème édition, 2009.

[3] *À propos d'un théorème de Techbychev sur la répartition des nombres premiers*, 2008, sujet de la deuxième épreuve du C.A.P.E.S. externe de Mathématiques.

[4] A.J. HILDEBRAND. *Introduction to Analytic Number Theory*, Lecture Notes, accès : http ://www.math.uiuc.edu/ hildebr/ant.