Théorie des Nombres de Base

Jean-François Jaulent

Transcription en LaTeX par José-Ibrahim Villanueva.*

Le texte qui suit reproduit les notes du cours de base de théorie des nombres donné à l'Ecole Doctorale de Mathématiques de Bordeaux pendant les années 91/92, 92/93 et 93/94.

Conçu comme complémentaire du libre de P. Samuel sur la "théorie algébrique des nombres", ce cours vise à introduire aux techniques fondamentales de l'arithmétique des corps locaux et aux méthodes analytiques. Il s'articule en trois sections et deux appendices :

1. Corps finis	A1. Théorie de Galois topologique
2. Corps locaux	A2. Symboles continus
3. Séries de Dirichlet	

Suivant les années, certaines sections ont été plus développés que d'autres, l'horaire réduit du cours impliquant de faire des choix. Par example il n'a pas été possible de démontrer la même année le théorème de Kronecker-Weber, le résultat de structure sur $\mathsf{K}_2(\mathbb{Q})$ et le théorème d'Hadamard-La Vallée Poussin. De façon semblable, certains résultats complémentaires, notamment le passage local-global, ont fait l'objet d'exposés particuliers lors de groupes de travail et ne figurent donc pas ici.

Soulac, Février 1994

Table des matières

*En étant doctorant du Professeur Jaulent, il m'a confié son dernier exemplaire de ces notes. La beauté des notes (à l'origine écrites soigneusement à la main, et élégamment ordonnées) reproduites dans les cahiers de l'école doctorale m'a captivé et j'ai décidé de les transcrire en LaTeX pour les préserver numériquement. Ainsi je me suis permis d'ajouter des contenus manquants d'une feuille n'apparaissant pas dans les cahiers (en suivant [1] et [2]) et d'en additionner sans trop perturber l'esprit original de l'ouvrage. Donc je prends la responsabilité de toute faute sur cette édition.

1 Corps Finis

1.1 Généralités

1.1.1 Commutativité des corps finis

Considérons un corps fini K, et notons 0 et 1 ses neutres additif et multiplicatif (qui sont distincts par convention). Le sous-corps premier, disons F, de K (qui est par définition son plus petit sous-corps, ou encore l'intersection de tous ses sous-corps) contient évidemment 0 et 1 donc l'image $\mathbb{Z}.1$ de $\mathbb{Z}$, qui est d'une part un sous-anneau forcément intègre de K, et d'autre part isomorphe à un quotient fini $\mathbb{Z}/p\mathbb{Z}$ de $\mathbb{Z}$. L'entier p, qui est donc premier, est appelé la caractéristique de K. Le sous-corps F, qui est isomorphe de façon unique à $\mathbb{Z}/p\mathbb{Z}$ est noté $\mathbb{F}_p$. C'est aussi le sous-corps premier de tout sous-(ou sur-) corps L de K. En particulier un tel corps L est un $\mathbb{F}_p$-espace vectoriel, isomorphe comme tel à la somme directe de $[L : \mathbb{F}_p]$ exemplaires de $\mathbb{F}_p$. Il est fini si et seulement si sa dimension $[L : \mathbb{F}_p]$ l'est, auquel cas on a $|L| = p^{[L:\mathbb{F}_p]}$. Ainsi :

Proposition 1. *Le cardinal d'un corps fini est une puissance de sa caractéristique qui est un nombre premier.*

Comme nous allons le voir très vite un corps fini est nécessairement commutatif. La démonstration de ce résultat s'appuie sur une propriété élémentaire des polynômes cyclotomiques qui s'énonce comme suit :

Définition & Proposition 1. *Pour chaque entier $n \geqslant 1$, soit μ_n le groupe des racines n-ièmes de l'unité dans $\mathbb{C}$, et μ'_n le sous-ensemble des racines primitives n-ièmes.*

Le n-ième polynôme cyclotomique est le produit

$$\Phi_n(X) = \prod_{\zeta \in \mu'_n} (X - \zeta).$$

Il est à coefficients entiers, et l'on a dans $\mathbb{Z}[X]$ l'identité entre polynômes :

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Preuve : Puisque tout élément de μ_n est dans un unique μ'_n pour un d qui divise n (en vertu du théorème de Lagrange), l'identité $X^n - 1 = \prod_{d|n} \Phi_d(X)$ est immédiate dans $\mathbb{C}[X]$. La seule difficulté consiste à vérifier que les $\Phi_d(X)$ sont à coefficients entiers. Or c'est évident pour $\Phi_1(X) = X - 1$. Supposons donc cette propriété établie pour tous les $d < n$, en particulier pour tous les diviseurs stricts d de n. L'identité dans $\mathbb{C}[X]$

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n \ d \neq n} \Phi_d(X)}$$

nous donne alors $\Phi_n(X)$ comme quotient de deux polynômes unitaires à coefficients entiers, et l'algorithme de la division euclidienne nous montre que les coefficients de $\Phi_n(X)$ sont bien entiers. □

Théorème 1 (Wedderburn)**.** *Tout corps fini est commutatif.*

Preuve : Soit K un corps fini, C son centre (qui est un sous-corps commutatif de K), q le cardinal de C (qui est donc une puissance de la caractéristique p), et n la dimension de K sur C. Faisons opérer le groupe multiplicatif $K^\times$ sur lui-même par conjugaison, et écrivons l'équation des classes :

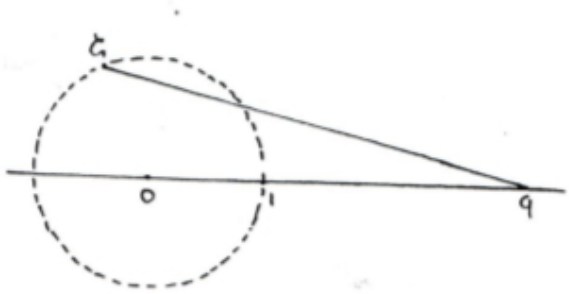
$$|K^\times| = |C^\times| + \sum_x (K^\times : K_x^\times),$$

la sommation à droite portant sur un système de représentants des orbites non ponctuelles.

Dans la formule obtenue, chaque stabilisateur $K_x^\times$ n'est autre que le groupe des éléments non nuls d'un certain sous-corps K_x de K, disons de degré $n_x < n$ sur C. Il vient donc :

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{n_x} - 1},$$

chacun des n_x qui apparaissent à droite étant un diviseur strict de n (puisque K est un K_x-espace vectoriel de dimension $\frac{n}{n_x} > 1$). D'après la proposition (1), l'entier $\Phi_n(q)$ divise donc $q^n - 1$ et chacun des quotients $\frac{q^n-1}{q^{n_x}-1}$ donc, finalment, $q - 1$.



D'un autre côté, nous avons directement :

$$|\Phi_n(q)| = \prod_{\zeta \in \mu'_n} |q - \zeta| > \prod_{\zeta \in \mu'_n} (q - 1) \geqslant q - 1,$$

contrairement à ce qui précède, sauf dans les cas $n = 1$ pour lequel $K = C$ est bien commutatif. □

Corollaire 1. *Le groupe multiplicatif d'un corps fini à q éléments est cyclique d'ordre $q - 1$.*

Preuve : Il suffit de vérifier que tout sous-groupe multiplicatif fini G du groupe multiplicatif $K^\times$ d'un corps commutatif est cyclique. Pour chaque diviseur d de son ordre n, soit onc $\rho(d)$ le nombre de x d'ordre d dans G. D'un côté, nous avons directement $n = \sum_{d|n} \rho(d)$. D'un autre côté, l'équation $X^d - 1$ ayant au plus d racines dans le corps K, dès que G contient un élément x d'ordre d, les racines de $X^d - 1$ sont exactement les puissances de x, et parmi elles $\varphi(d)$ sont précisément d'ordre d. Nous avons donc $\rho(d) = 0$ ou $\varphi(d)$ pour chaque d, et par suite :

$$\rho(n) = n - \sum_{d|n \ d \neq n} \rho(d) \geqslant n - \sum_{d|n \ d \neq n} \varphi(d) = \varphi(n) > 0,$$

comme attendu. □

1.1.2 Treillis des extensions de $\mathbb{F}_p$

Convenons de fixer une fois pour toutes une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Nous allons voir qu'il est possible de décrire très simplement toutes les sous extensions finies de $\overline{\mathbb{F}}_p$:

Théorème 2. *Pour chaque entier $n \geqslant 1$, il existe un unique sous-corps de $\overline{\mathbb{F}}_p$ à $q = p^n$ éléménts ; on le note $\mathbb{F}_q$: c'est le corps (et aussi l'ensemble) des racines dans $\overline{\mathbb{F}}_p$ du polynôme séparable $\Omega_q(X) = X^q - X$.*

Preuve : Soit, s'il existe, F un sous-corps de $\overline{\mathbb{F}}_p$ ayant q éléments. Dans ce cas les $q - 1$ éléments du groupe multiplicatif $F^\times$ vérifient l'identité de Lagrange $x^{q-1} = 1$; et les q éléments de F sont par conséquent les q racines du polynôme $\Omega_q(X) = X(X^{q-1} - 1)$.

Inversement, partons du polynôme $\Omega_q(X)$. Remarquons qu'il est séparable (puisqu'on a identiquement $\Omega'_q(x) = q - 1$), et notons F l'ensemble de ses q racines (distinctes) dans le corps algébriquement clos $\overline{\mathbb{F}}_p$. Pour x et y dans F, nous avons alors :

$$(x + y)^q = x^q + y^q = x + y \quad \text{et} \quad (xy)^q = x^q y^q = xy,$$

ce qui montre, puisque F contient 1, que c'est bien un sous-anneau de $\overline{\mathbb{F}}_p$. Comme il est intègre et fini, c'est un corps. □

Scolie. *A isomorphisme près, il existe pour tout $n \geqslant 1$ un unique corps de cardinal p^n c'est $\mathbb{F}_{p^n}$.*

Preuve : En effet, un tel corps est algébrique sur son sous-corps premier qui s'identifie à $\mathbb{F}_p$, donc se plonge dans le corps algébriquement clos $\overline{\mathbb{F}}_p$. Et son image est évidemment $\mathbb{F}_{p^n}$. □

Proposition 2. *Soient* m *et* n *deux entiers naturels non nuls. On a alors dans* $\overline{\mathbb{F}}_p$ *:*

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \;\Leftrightarrow\; n|m.$$

En particulier, il suit : $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^{n\wedge m}}$ *et* $\mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^{m\vee n}}$

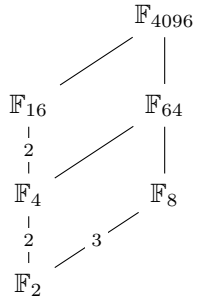
Preuve : Si $\mathbb{F}_{p^m}$ contient $\mathbb{F}_{p^n}$, c'est un $\mathbb{F}_{p^n}$-espace vectoriel de dimension finie, disons k. Il suit $p^m = (p^n)^k = p^{nk}$, i.e. $m = nk$. Inversement, de l'égalité $m = nk$, on tire l'implication

$$x^{p^n} = x \;\Rightarrow\; x^{p^m} = x^{p^{nk}} = (\cdots(x^{p^n})^{p^n}\cdots)^{p^n} = x,$$

i.e. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$.

Les identités faisant intervenir le p.g.c.d. et le p.p.c.m. en résultent directement. □

Exemple 1. Le diagramme des sous-corps de $\mathbb{F}_{4096}$ est représenté ci-dessous.



On notera que $\mathbb{F}_8$ (extension cubique de $\mathbb{F}_2$) ne contient pas $\mathbb{F}_4$ (extension quadratique de $\mathbb{F}_2$).

Pour prendre en compte maintenant les extensions infinies de $\mathbb{F}_p$, introduisons l'ensemble $\mathbb{S}$ des nombres surnatureles, i.e. l'ensemble des produits formels

$$\bar{n} = \prod p^{\nu_p(\bar{n})},$$

où p parcourt l'ensemble des nombres premiers, et l'exposant $\nu_p(\bar{n})$ prend ses valeurs dans $\overline{\mathbb{N}} = \mathbb{N}\cup\{\infty\}$. On définit de façon évidente le produit, le p.g.c.d. et le p.p.c.m. d'une famille quelconque d'éléments de §. Cela posé, il vient :

Théorème 3. *L'application*

$$\bar{n} \in \mathbb{S} \mapsto \mathbb{F}_{p^{\bar{n}}} = \bigcup_{n|\bar{n}} \mathbb{F}_{p^n}$$

(où la réunion à droite porte sur les sous-corps finis de $\overline{\mathbb{F}}_p$ *pour lesquels* n *divise* $\bar{n}$*) est une bijection croissante de l'ensemble* $\mathbb{S}$ *des nombres surnaturels (ordonné par divisibilité) sur l'ensemble (ordonné par inclusion) des sous-corps de* $\overline{\mathbb{F}}_p$*, les sous-corps finis correspondant aux nombres naturels.*

Preuve : Remarquons d'abord que $\mathbb{F}_{p^{\bar{n}}}$ est bien un cous-corps de $\overline{\mathbb{F}}_p$: En effet, pour x et y dans $\mathbb{F}_{p^{\bar{n}}}$, nous avons $x \in \mathbb{F}_{p^m}$ et $y \in \mathbb{F}_{p^n}$ pour deux entiers m et n qui divisent $\bar{n}$, donc $\mathbb{F}_p[x,y] \subset \mathbb{F}_{p^{m\vee n}} \subset \mathbb{F}_{p^{\bar{n}}}$ comme attendu, puisque le p.p.c.m. de m et de n divise encore $\bar{n}$.

Plus précisément, nous avons même

$$x \in \mathbb{F}_{p^{\bar{n}}} \;\Leftrightarrow\; \exists\, n|\bar{n}\; x \in \mathbb{F}_{p^n} \;\Leftrightarrow\; \exists\, n|\bar{n}\; \deg(x)|n,$$

autrement dit $x \in \mathbb{F}_{p^{\bar{n}}} \;\Leftrightarrow\; \deg(x)|\bar{n}$; et l'application étudiée est donc injective.

Reste à vérifier que tout sous-corps F de $\overline{\mathbb{F}}_p$ est bien de la forme $\mathbb{F}_{p^{\bar{n}}}$ pour un $\bar{n}$ convenable : F étant donné, définissons $\bar{n}$ comme p.p.c.m. par $\bar{n} = \bigvee_{\mathbb{F}_{p^n}\subset F} n$. Nous obtenons immédiatement $\mathbb{F}_{p^{\bar{n}}} = \bigcup_{\mathbb{F}_{p^n}\subset F} \mathbb{F}_{p^n} = F$ (puisque F est réunion de ses sous-corps finis). □

1.2 Théorie de Galois

1.2.1 Groupe des automorphismes d'un corps fini

Soit $E/$ une extension de sous-corps finis de $\overline{\mathbb{F}}_p$, disons $F = \mathbb{F}_q$ (avec $q = p^t$) et $E = \mathbb{F}_{q^s}$ (avec $s = [E : F]$). D'aprèes le théorème (2), E est alors le corps des racines du polynôme séparable $\Omega_{q^s}(X) = X^{q^s} - X$. Nous allons voir que son groupe de Galois est cyclique :

Théorème 4. *Dans une extension E/F de corps finis, le groupe $\mathrm{Gal}(E/F)$ des F-automorphismes de E est le groupe cyclique d'ordre $[E : F]$ engendré par l'automorphisme de Frobenius*

$$\sigma : x \mapsto x^q,$$

où q est le cardinal de F.

Preuve : Faisons choix d'un élément primitif x de E/F (par example l'un des générateurs du groupe cyclique $E^\times$). Son polynôme minimal sur F, disons $P_x(X)$, qui divise $\Omega_{q^s}(X)$, a exactement $s = [E : F]$ racines (distinctes) dans E. Cela étant, puisque E est égal à $F[x]$, chaque F-automorphisme de E est uniquement déterminé par l'image de x qui est est l'une, arbitraire, des s racines de $P_x(X)$. Le groupe $\mathrm{Gal}(E/F)$ est ainsi de cardinal s.

Comme l'opérateur de Frobenius $\sigma_q : x \mapsto x^q$ est clairement un F-automorphisme de E, tout le problème se ramène à étudier que σ_q est bien d'ordre s. Or, pour $k = 1, \ldots, s$, le corps des invariants de σ_q^k dans E est l'ensemble des racines du polynôme $X^{q^k} - X$ dans $E = \mathbb{F}_{q^s}$, c'est à dire $\mathbb{F}_{q^s} \cap \mathbb{F}_{q^k}$. Ce n'est donc E que pour $k = s$. □

Corollaire 2. *Pour chaque puissance $q = p^f$ du nombre premier p, le sous-corps à q éléments de $\overline{\mathbb{F}}_p$ est le corps des invariants de la puissance f-ième du Frobenius σ_p. Et l'on a*

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \sigma_p^{\mathbb{Z}}/\sigma_p^{f\mathbb{Z}} \simeq \mathbb{Z}/f\mathbb{Z}.$$

Disons un mot du groupe $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ des automorphismes de $\overline{\mathbb{F}}_p$. Puisque $\overline{\mathbb{F}}_p$ est la réunion des corps finis $\mathbb{F}_{p^n}$ (pour $n \in \mathbb{N} \setminus \{0\}$), le groupe $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ s'interprète comme la limite projective des groupes de Galois finis $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$: Un élément σ de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ est, en effet déterminé par la donnée de ses restrictions $\sigma_n = \sigma|_{p^n}$; c'est à dire qu'il se lit comme une famille $(\sigma_n)_n \in \prod_{\mathbb{F}_{p^n}} \subset \overline{\mathbb{F}}_p \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ d'automorphismes finis satisfaisant aux conditions de cohérence $\sigma|\mathbb{F}_{p^n} = \sigma_m$, pour tous les couples d'indices (m, n) ordonnés par divisibilité.

Dans le cas qui nous occupe, cette limite $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est particulièrement simple : Le corollaire précédent identifie en effet $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ à $\mathbb{Z}/n\mathbb{Z}$, donc $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ à la limite projective $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$, c'est à dire au complété $\hat{\mathbb{Z}}$ de $\mathbb{Z}$ pour la topologie définie par ses sous-groupes d'indice fini. Autrement dit :

Scolie. *Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ est le groupe profini isomorphe à $\hat{\mathbb{Z}}$, qui est engendré topologiquement par l'automorphisme de Frobenius σ_p.*

Nota. *La théorie de Galois topologique établit une bijection entre les sous-extensions de $\overline{\mathbb{F}}_p$ eet les sous-groupes fermés de $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, c'est à dire finalement les sous-groupes fermés de $\hat{\mathbb{Z}}$. Ceux-ci sont donc en bijection avec les nombres surnaturels définis plus haut.*

1.2.2 Propriétés galoisiennes des corps finis

Commençons par établir un résultat d'indépendance linéaire des automorphismes d'ailleurs tout à fait général :

Lemme 1 (Dedekind)**.** *Soit E/F une extension quelconque de corps commutatifs. Si $\sigma_1, \ldots, \sigma_k$ sont autant des F-automorphismes distincts des corps E, ils sont E-linéairement indépendants dans l'espace vectoriel $\mathcal{L}_F(E)$ des F-endomorphismes linéaires de E.*

Preuve : Sinon, soit $\sum_{i\in I} a_i\sigma_i{=}0$ une relation de E-dépendance linéaire de longueur minimale ($\geqslant 2$). Alors pour x et y dans E, nous avons aussi bien :

$$\sum_{i\in I} a_i\sigma_i(x)\sigma_i(y) = \sum_{i\in I} a_i\sigma_i(xy) = 0,$$

ce qui montre que pour x fixé $\sum_{i\in I} a_i\sigma_i(x)\sigma_i = 0$ est encore une relation de E-dépendance entre les σ_i. Maintenant, comme deux σ_i distincts ne prennent pas la même valeur sur au moins un x, nous pouvons choisir celui-ci de telle sorte que cette nouvelle relation ne soit pas proportionnelle à la première. Par élimination, nous sommes alors à même d'obtenir une relation de E-dépendance strictement plus courte que celle de départ : contradiction. □

Corollaire 3. *Dans une extension E/F de corps finis, les éléments de $\mathrm{Gal}(E/F)$ constituent une E-base de $\mathcal{L}_F(E)$. Autrement dit, on a la décomposition directe :*

$$\mathcal{L}_F(E) = \bigoplus_{i=1}^{[E:F]} E\sigma_F^i, \quad \text{où } \sigma_F \text{ est le Frobenius attaché à } F.$$

En effet, $\mathcal{L}_F(E)$ est un F-espace de dimension $[E:F]^2$, donc un E-espace de dimension $[E:F]$.

Théorème 5 (de la base normale)**.** *Dans une extension E/F de corps finis, il existe un élément θ de E dont les conjugués (par $\mathrm{Gal}(E/F)$) forment une F-base de E. En d'autres termes E est un $F[\mathrm{Gal}(E/F)]$-module libre de dimension 1.*

Preuve : Nous savons déjà que le groupe $\mathrm{Gal}(E/F)$ est cyclique, d'ordre $s = [E:F]$, et engendré par le Frobenius σ_F. Maintenant, puisque les s éléments de Galois σ_F^i, pour $i = 0, \dots, s-1$ sont F-linéairement indépendants, le polynôme minimal de σ_F sur F n'est autre que $X^s - 1$ (et, puisqu'il est de degré s, c'est aussi son polynôme caractéristique). D'après le théorème fondamental de l'algèbre linéaire rappelé ci-dessous, il existe donc un θ de E tel que $X^s - 1$ soit encore le polynôme minimal de la restriction de σ_F au sous-espace engendré par θ et ses itérés $\sigma(\theta), \dots, \sigma^{s-1}(\theta)$. En particulier ceux-ci sont donc F-linéairement indépendants. □

Nota (Théorème fondamental d'algèbre linéaire)**.** *Soit σ un endomorphisme d'un F-espace vectoriel E de dimension finie, e $P = \prod P_i^{n_i}$ la factorisation irréductible dans $F[X]$ de son polynôme minimal P. On peutr alors écrire l'espace entier*

$$E = \ker P(\sigma) = \bigoplus \ker P_i^{n_i}(\sigma) = \bigoplus E_i$$

comme somme directe de sous-espaces E_i stables par σ tels que la restriction σ_i de σ à E_i ait pour polynôme minimal $P_i^{n_i}$. Ceci implique qu'il existe dans E_i au moins un vecteur θ_i tel que la restriction de σ_i au sous-espace stable engendré par θ_i ait encore $P_i^{n_i}$ pour polynôme minimal (sans quoi σ serait annulé par $P_i^{n_i-1}$). L'élément $\theta = \sum \sigma_i$ convient alors.

Remarque: Si l'on met ensemble le corollaire (3) et le théorème (5), on voit que tout endomorphisme F-linéaire de E s'écrit de façon unique $\sum_{i,j} a_{ij}\theta^{\sigma_F^i}\sigma_F^j$ avec les a_{ij} dans F.

1.3 Équations algébriques

1.3.1 Polynômes sur les corps finis

Proposition 3. *Il existe des polybömes irréductibles de tous degrés sur $\mathbb{F}_q$.*

Preuve : En effet, pour chaque $n \geqslant 1$, le corps $\mathbb{F}_{q^n}$ est une extension de degré n sur $\mathbb{F}_q$ qui admet des éléments primitifs (par example les générateurs du groupe cyclique $\mathbb{F}_{q^n}^\times$). Les polynômes minimaux de ces

éléments sont donc irréductibles et de degré n. Ce sont d'ailleurs les seuls polynômes unitaires et irréductibles de degré n en vertu de l'unicité de $\mathbb{F}_{q^n}$. □

Désignons par $p(n)$ le nombre de polynômes irréductibles et unitaires de degré n dans $\mathbb{F}_q[X]$. Puisque les éléments de $\mathbb{F}_{q^n}$ sont exactement ceux de degré d (sur $\mathbb{F}_q$) divisant n, la factorisation dans $\mathbb{F}_q[X]$ du polynôme séparable $\Omega_{q^n}(X) = X^{q^n} - X = \prod_{x\in\mathbb{F}_{q^n}}(X-x)$ fait intervenir une fois et une seule chaque polynôme irréductible et unitaire de degré divisant n. Écrivant alors l'égalité des degrés dans la factorisation obtenue, nous en déduisons l'identité :

$$q^n = \sum_{d|n} d\,p(d),$$

qui permet par récurrence le calcul de $p(n)$. Il est d'ailleurs possible d'expliciter ce calcul en s'aidant de la fonction de Möbius :

Définition & Proposition 2. *On appelle fonction de Möbius l'application de $\mathbb{N}^\times = \mathbb{N}\setminus\{0\}$ dans $\mathbb{Z}$ définie par :*

$$\mu(n) = \begin{cases} 0, & \text{si } n \text{ a un facteur carré (non trivial),} \\ (-1)^{k(n)}, & \text{sinon, } k(n) \text{ désignant alors le nombre de facteurs premiers de } n. \end{cases}$$

La fonction μ est faiblement multiplicative (en ce sens qu'on a $\mu(mn) = \mu(m)\mu(n)$ lorsque m et n sont étrangers), et vérifie l'identité :

$$\sum_{d|n} \mu(d) = \delta_{n,1}.$$

Preuve : La multiplicativité (au sens faible) est évident. Quant à l'identité annoncée, elle s'obtient comme suit : Ecrivons $n = p_1^{\nu_1}\cdots p_k^{\nu_k}$ la factorisation irréductible de n. Les seuls diviseurs de n pour lesquels $\mu(d)$ es non nul étant ceux sans facteur carré, ce sont les produits $p_{i_1}\cdots p_{i_h}$ de h parmi k facteurs premiers de n. Il vient dont, comme annoncé :

$$\sum_{d|n}\mu(n) = \sum_{h=0}^{k} C_k^h(-1)^h = (1-1)^k = 0,$$

sauf pour $k=0$, i.e. $n=1$. □

Théorème 6 (Formule d'inversion)**.** *Etant donnés deux applications f et g définies sur $\mathbb{N}^\times = \mathbb{N}\setminus\{0\}$, à valeurs dans un groupe abélien A, les deux propriétés suivantes sont équivalentes :*

(i) $\forall n \in \mathbb{N}^\times \quad f(n) = \sum_{d|n} g(d)$

(ii) $\forall n \in \mathbb{N}^\times \quad g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d).$

Si, de plus A est un anneau (commutatif), f et g sont alors simultanément (faiblement) multiplicatives ou pas.

Preuve : Considérons la loi de composition interne définie dans $A^{\mathbb{N}^\times}$ par :

$$f * g(n) = \sum_{ab=n} f(a)g(b).$$

Elle est clairement commutative et associative (puisqu'on a par un calcul immédiat : $(f*g)*h(n) = \sum_{mc=n} f*g(m)h(c) = \sum_{abc=n} f(a)g(b)h(c) = f*(g*h)(n)$) ; et elle admet comme neutre la fonction δ définie par $\delta(n) = \delta_{n,1}$.

Cela étant, la fonction sommatoire pour la fonction de Möbius s'écrit tout simplement :

$$\mu * 1 = \delta,$$

identité qui exprime que l'inverse de μ est la fonction constante égal à 1. Il vient donc comme annoncé :

$$f = g*1 \;\Leftrightarrow\; g = g*d = g*1*\mu = f*\mu.$$

La fin du théorème résulte simplement du fait que le produit de deux fonctions (faiblement) multiplicatives est encore (faiblement) multiplicatif : Pour m et n étrangers et f, g multiplicatives, il vient en effet (lorsque A est équipé d'une multiplication d'anneau) :

$$\begin{aligned} f*g(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\ &= \sum_{a|m,\ b|n} f(ab)g\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m}\sum_{b|n} f(a)g\left(\frac{m}{a}\right)f(b)g\left(\frac{n}{b}\right) \\ &= f*g(m)f*g(n). \end{aligned}$$

□

Corollaire 4. *Pour chaque $n \geqslant 1$, le nombre de polynômes unitaires et irréductibles de degré n sur le corps à q éléments est donné par la formule :*

$$p(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

Preuve : Il suffit d'appliquer la formule d'inversion de Möbius à l'identité $\sum_{d|n} d\,p(d) = q^n$. □

Exemple 2. Il vient ainsi $p(1) = q$, $p(2) = \frac{1}{2}(q^2-q)$, $p(3) = \frac{1}{3}(q^3-q)$, $p(4) = \frac{1}{4}(q^4-q^2)$, ...

1.3.2 Loi de réciprocité quadratique

Définition & Proposition 3. *Soit $\mathbb{F}_q$ un corps fini de cardinal impair. On appelle caractère de Legendre l'application de $\mathbb{F}_q^\times$ dans $\{\pm 1\}$ définie par :*

$$x \mapsto \left(\frac{x}{q}\right) = x^{(q-1)/2}.$$

Le caractère de Legendre est un morphisme de $\mathbb{F}_q^\times$ sur $\{\pm 1\}$ qui a pour noyau le sous-groupe des carrés. On convient de le prolonger à $\mathbb{F}_q$ en posant $\left(\frac{0}{q}\right) = 0$.

Bien entendu, c'est le caractère cyclique de $\mathbb{F}_q^\times$ qui justifie que le noyau de $\left(\frac{\cdot}{q}\right)$ est le groupe des carrés.

Proposition 4. *On a les formules explicites :*

(i) $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$ *(autrement dit -1 est un carré dans $\mathbb{F}_q$ pour $q \equiv 1 \bmod 4$)*

(ii) $\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}$ *c'est à dire* $\begin{cases} \left(\frac{2}{q}\right) = 1, & \text{pour } q \equiv \pm 1 \bmod 8 \\ \left(\frac{2}{q}\right) = -1, & \text{pour } q \equiv \pm 5 \bmod 8 \end{cases}$

Preuve : La première formule est évidente. Pour établir la seconde, remarquons que le polynôme x^8-1 est séparable sur $\mathbb{F}_q$, et notons ζ une racine primitive 8-ième de l'unité dans $\overline{\mathbb{F}_p}$. De l'égalité $\zeta^8 = 1$, nous tirons $\zeta^4 = -1$ (puisque ζ est supposé primitive) i.e. $\zeta^2 + \zeta^{-2} = 0$, ce qui montre que $\theta = \zeta + \zeta^{-1}$ est une racine carrée de 2 dans $\overline{\mathbb{F}}_p$. Par ailleurs, il vient directement $\theta^q = (\zeta+\zeta^{-1})^q = (\zeta^q + \zeta^{-q}$ d'où :

— pour $q \equiv \pm 1 \bmod 8$: $\zeta^q = \zeta^{\pm 1}$, puis $\theta^q = \theta$ et $\left(\frac{2}{q}\right) = \left(\frac{\theta^2}{q}\right) = \theta^{q-1} = 1$;

— pour $q \equiv \pm 5 \bmod 8$: $\zeta^q = -\zeta^{\pm 1}$, puis $\theta^q = -\theta$ et $\left(\frac{2}{q}\right) = \left(\frac{\theta^2}{q}\right) = \theta^{q-1} = -1$.

□

Définition & Proposition 4. *Soit maintenant ℓ un nombre premier impair distinct de p, et ζ une racine primitive p-ième de l'unité dans $\overline{\mathbb{F}}_\ell$ (Une telle racine existe puisque le polynôme $X^p - 1$ est separable sur $\mathbb{F}_\ell$). On appelle somme de Gauss quadratique associée à ζ la quantité :*

$$\omega = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \zeta^x \ \in \mathbb{F}_\ell[\zeta] \subset \overline{\mathbb{F}}_\ell.$$

On a les identités dans $\overline{\mathbb{F}}_\ell$:

$$\textit{(i)} \quad \omega^{\ell-1} = \left(\frac{\ell}{p}\right) \qquad\qquad \textit{(ii)} \quad \omega^2 = (-1)^{(p-1)/2} p.$$

Preuve : Puisque $\overline{\mathbb{F}}_\ell$ a pour caractéristique ℓ, il vient immédiatement (compte tenu de l'imparité) :

$$\begin{aligned}
\omega^\ell &= \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \zeta^{\ell x} \\
&= \sum_{x \in \mathbb{F}_\ell} \left(\frac{x\ell}{p}\right) \left(\frac{\ell}{p}\right) \zeta^{\ell x} \\
&= \left(\frac{\ell}{p}\right) \sum_{y \in \mathbb{F}_\ell} \left(\frac{y}{p}\right) \zeta^y \\
&= \left(\frac{\ell}{p}\right) \omega,
\end{aligned}$$

ce qui établit *(i)* sous réserve que ω ne soit pas nul. Or, nous avons par ailleurs :

$$\begin{aligned}
\omega^2 &= \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \left(\frac{xy}{p}\right) \zeta^{x+y} \\
&= \sum_{z \in \mathbb{F}_p} \\
&\texttt{zeta}^z \sum_{x+y=z} \left(\frac{xy}{p}\right),
\end{aligned}$$

et la somme droite s'écrit :

$$\begin{aligned}
\sum_{x+y=z} \left(\frac{xy}{p}\right) &= \sum_{x \in \mathbb{F}_p} \left(\frac{x(z-x)}{p}\right) \\
&= \sum_{x \in \mathbb{F}_p^\times} \left(\frac{\frac{z}{x} - 1}{p}\right) \\
&= \begin{cases} \left(\frac{-1}{p}\right)(p-1), \text{ pour } z = 0; \\ \sum_{y \neq 1} \left(\frac{y}{p}\right) = -\left(\frac{-1}{p}\right), \text{ pour } z \neq 0. \end{cases}
\end{aligned}$$

Il vient donc :

$$\begin{aligned}
\omega^2 &= \left(\frac{-1}{p}\right) \left[(p-1) - \sum_{z \neq 0} \zeta^2\right] \\
&= \left(\frac{-1}{p}\right) p \\
&\neq 0, \text{ comme attendu.}
\end{aligned}$$

□

Théorème 7 (Loi de réciprocité quadratique)**.** *Pour* ℓ *et* p *premiers impaires distincts, on a l'identité :*

$$\left(\frac{\mathrm{p}}{\ell}\right)\left(\frac{\ell}{\mathrm{p}}\right) = (-1)^{\frac{\ell-1}{2}\frac{\mathrm{p}-1}{2}}.$$

Preuve : Nous avons en effet, e, vertu de la Definition & Proposition 4 ci-dessus :

$$\begin{aligned}
(-1)^{\frac{\ell-1}{2}\frac{\mathrm{p}-1}{2}} &= \left(\frac{(-1)^{\frac{\mathrm{p}-1}{2}}\mathrm{p}}{\ell}\right) \\
&= \left(\frac{\omega^2}{\ell}\right) \\
&= \omega^{\ell-1} \\
&= \left(\frac{\ell}{\mathrm{p}}\right), \text{ comme annoncé.}
\end{aligned}$$

□

Compte tenu des formules complémentaires données par la Proposition 4, la loi de réciprocité autorise le calcule de proche en proche des symboles de Legendre.

2 Corps Locaux

2.1 Valeurs absolues sur un corps commutatif

2.1.1 Définition et propriétés élémentaires

Définition 1. Une valeur absolue (réelle) sur un corps commutatif K est une application de K dans $\mathbb{R}_+$ qui satisfait les trois axiomes :

(VA 1) $|x| = 0 \quad \Leftrightarrow \quad x = 0$ (séparation)
(VA 2) $|xy| = |x||y|$ (multiplicativité)
(VA 3) $|x + y| \leqslant |x| + |y|$ (inégalité triangulaire)

Nota. *De l'identité* $1^2 = 1$*, on tire par (VA 2) :* $|\pm 1| = 1$*; donc* $|1| = 1$ *en vertu de (VA 1). De même, de* $(\pm 1) = 1$*, on tire* $|\pm 1| = 1$*, et finalement* $|x| = |-x|$*, pour tout* x *de* K*.*

Remarque: Si K est le corps de fractions d'un anneau A (Commutatif unitaire et intègre) ; les propriétés (VAi) lues dans A définissent une valeur absolue sur l'anneau A laquelle se prolonge de façon unique par multiplicativité en un valeur absolue sur K.

Théorème & Définition 1. *On dit qu'une valeur absolue sur un corps* K *est :*

1. *archimédienne, lorsque l'image* $|\mathbb{Z}\cdot 1|$ *de* $\mathbb{Z}$ *dans* $\mathbb{R}$ *n'est pas bornée, auquel cas la valeur absolue satisfait l'axiome d'Archimède :*
   (VAA) $\forall x \in K^\times \quad \forall y \in K \quad \exists n \in \mathbb{N}$ *tel que* $|nx| > y$*.*
2. *ultramétrique, dans le cas contraire, pour lequel on a* $|n \cdot 1| \leqslant 1 \quad \forall n \in \mathbb{Z}$*, et l'inégalité ultramétrique :*
   (VAU) $|x + y| \leqslant \sup\{|x|, |y|\}$

Preuve : Les cas archimédien est immédiat : il suffit de choisir n assez grand pour avoir $|n| > |\frac{y}{x}|$. Supposons donc $|n| \geqslant C$ pour tout n de $\mathbb{Z}$. Dans ce cas, pour tout entier naturl m, nous pouvons écrire :

$$|\pm m| = |m| = |m^k|^{1/k} \leqslant c^{1/k}$$

quelque soit k entier > 1, ce qui implique $|\pm m| \leqslant 1$ comme annoncé. Il suit de façon semblable :

$$|x + y| = |(x + y)^k|^{1/k} = \left| \sum_{h=0}^{k} C_k^h x^h y^{k-h} \right|^{1/k} \leqslant \left(\sum_{h=0}^{k} |C_k^h| |x|^h |y|^{k-h} \right)^{1/k},$$

i.e.

$$|x + y| \leqslant (k + 1)^{1/k} \sup\{|x|, |y|\},$$

et finalement $|x + y| \leqslant \sup\{|x|, |y|\}$, puisqu'on a $\lim_{\infty}(k + 1)^{1/k} = 1$. □

Corollaire 5. *Sur un corps de caractéristique* $p > 0$*, une valeur absolue est toujours ultramétrique.*

Preuve : L'image de $\mathbb{Z}$ y est en effet finie, donc bornée. □

Proposition 5. *Dans la définition d'une valeur absolue l'axiome triangulaire (VA 3) peut être affaibli sous la forme :*

(VA 3') $|x + y| \leqslant 2 \sup\{|x|, |y|\}$.

Preuve : Soit $|\cdot|$ une application de K dans $\mathbb{R}$, satisfaisant les trois axiomes (VA 1), (VA 2) et (VA 3'). Vérifions d'abord que nous avons alors l'inégalité :

$$|\sum_{i=1}^{m} x_i| \leqslant 2m \sup_{i=1,\ldots,m} |x_i|,$$

pour tout m-tuplet $(x_1, \ldots, x_m)$ de K^m. Cette propriété étant vérifiée pour $m = 2$, d'après (VA 3') ; procédons par récurrence sur l'exposant r de la plus petite puissance de 2 qui est supérieure à m. Complétons $(x_1, \ldots, x_m)$ par des 0 pour obtenir un 2^r-uplet, et appliquons r fois l'axiome (VA 3') . Nous obtenons, comme annoncé :

$$|\sum_{i=1}^{m} x_i| = |x_1 + x_2 + \ldots + 0 + \ldots + 0| \leqslant 2^r \sup_{i=1,\ldots,m} |x_i| \leqslant 2m \sup_{i=1,\ldots,m} |x_i|.$$

Ce point acquis, nous avons :

$$|x+y| = |(x+y)^n|^{1/n} = |\sum_{k=0}^{n} C_n^k x^k y^{n-k}|^{1/n} \leqslant [2(n+1)]^{1/n} \sup |C_n^k x^k y^{n-k}|^{1/n}, \text{ puis :}$$

$$|x+y| \leqslant [2(n+1)]^{1/n} \sup(2C_n^k |x|^k |y|^{n-k})^{1/n} \leqslant [4(n+1)]^{1/n} \left(\sum |C_n^k |x|^k |y|^{n-k}\right)^{1/n}, \text{ i.e.}$$

$$|x+y| \leqslant [4(n+1)]^{1/n}(|x| + |y|),$$

d'où l'inégalité triangulaire via $\lim[4(n+1)]^{1/n} = 1$. □

2.1.2 Topologie définie par une valeur absolue

C'est la topologie sur K définie par la métrique $d(x, y) = |x - y|$.

Théorème & Définition 2. *Deux valeurs absolues sont dites équivalentes lorsqu'elles définissent la même topologie, ce qui a lieu si et seulement s'il existe une constante $s > 0$ telle qu'on ait :*

$$|\cdot|_a = |\cdot|_b^s.$$

Elles sont dites indépendantes sinon.

Preuve : Sous la condition $|\cdot|_a = |\cdot|_b^s$, les boules étant les mêmes ; les topologies coïncident. Réciproquement, l'égalité des topologies $\tau_a = \tau_b$ entraîne celle des boules unités ouvertes puisqu'une suite convergeant vers 0 avec la valeur absolue $|\cdot|_a$ converge aussi avec $|\cdot|_b$. On a aussi l'égalité

$$\{x \in K \,|\, |x| < 1\} = \{x \in K \,|\, (x^n)_{n\in\mathbb{N}} \to 0 \text{ for } n \to \infty\},$$

donc $|\cdot|_a \sim |\cdot|_b$ entrain

$$1 < |x|_a \text{ si et seulment si } 1 < |x|_b.$$

Supposons que $|\cdot|_a$ et $|\cdot|_b$ ne sont pas triviales, donc il existe $x \in K$ tel que $|x|_a > 1$ et alors $|x|_b > 1$, posons

$$\lambda = \frac{\log |x|_a}{\log |x|_b} > 0.$$

Soit $y \in K^\times$, il existe $\alpha \in \mathbb{R}$ tel que $|x|_a = |y|_a^\alpha$. Soit $\left(\frac{m_i}{n_i}\right)$ une suite convergeant vers α avec m_i, n_i entiers et $n > 0$, posons que $m_i/n_i > \alpha$ alors on a

$$|x|_a = |y|_a^\alpha < |y|_a^{m_i/n_i},$$

d'où l'on obtient que

$$\frac{|x|_a^{n_i}}{|y|_a^{m_i}} = \left|\frac{x^{n_i}}{y^{m_i}}\right|_a < 1 \quad \Rightarrow \quad \left|\frac{x^{n_i}}{y^{m_i}}\right|_b < 1$$

et donc $|x|_b < |y|_b^{m_i/n_i}$, donc $|x|_b \leqslant |y|_b^\alpha$.

De la même façon si l'on prend la suite $\left(\frac{m_i}{n_i}\right)$ convergeant vers α avec $m_i/n_i < \alpha$, en faisant le même type de raisonnement on obtient que $|x|_b \geqslant |y|_b^\alpha$. Donc $|x|_b = |y|_b^\alpha$

Donc pour tout $y \in K^\times$ on a

$$\lambda = \frac{\log |x|_a}{\log |x|_b} = \frac{\log |y|_a}{\log |y|_b},$$

alors $|y|_a = |y|_b^\lambda$.

□

2.1.3 Complétion d'un corps en une place

Rappelons la définition d'une suite de Cauchy :

Définition 2. On appelle suite de Cauchyt d'un corps valué K toute suite $(\mu_n)_{n\in\mathbb{N}}$ de $K^{\mathbb{N}}$ qui satisfait au critère de Cauchy : $\forall\, \varepsilon > 0 \;\; \exists\, n_0 \in \mathbb{N}$ tel que $\forall n,\, p > n_0$ on ait $|\mu_n - \mu_p| < \varepsilon$. Et on dit que K est complet lorsque toute suite de Cauchy d'éléments de K converge dans K.

La construction du complété $\hat{K}$ d'un corps valué est analogue à celle du corps des réels à partir de $\mathbb{Q}$: On introduit l'anneau $\mathcal{A}_K$ des suites de Cauchy des éléments de K, et on note $\mathcal{M}_K$ l'idéal des suites qui convergent vers 0, puis on pose $\hat{K} = \mathcal{A}_K/\mathcal{M}_K$. On a alors :

Théorème 8. *Le prolongement naturel de la valeur absoulue à $\hat{K}$ fait de $\hat{K}$ un corps valué complet qui contient K comme sous-corps partout dense.*

Démontrons ce résultat en procédant par étapes :

Assertion (1)**.** *Pour chaque suite $(\mu_n)_{n\in\mathbb{N}}$ dans $\mathtt{mathcal}A_K$, la suite $(|\mu_n|)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}$. Elle est en particulier majorée dans tous les cas, et ultimement minorée par une constante strictement positive dès qu'elle n'est pas dans $\mathcal{M}_K$.*

Preuve : L'inégalité $||\mu_n| - |\mu_p|| \leqslant |\mu_n - \mu_p|$ montre, en effet, que la suite $(|\mu_n|)_{n\in\mathbb{N}}$ est de Cauchy donc convergente dans $\mathbb{R}$. □

Assertion (2)**.** $\mathcal{M}_K$ *est un idéal maximal de $\mathcal{A}_K$, autrement dit $\hat{K} = \mathcal{A}_K/\mathcal{M}_K$ est un corps.*

Preuve : Vérifions d'abord que $\mathcal{M}_K$ est un idéal de $\mathcal{A}_K$. D'une part c'est trivialement un sous-groupe additif de $\mathcal{A}_K$. D'autre part, pour $(\mu_n)_{n\in\mathbb{N}}$ dans $\mathcal{A}_K$ et $(m_n)_{n\in\mathbb{N}}$ dans $\mathcal{M}_K$, l'inégalité $|a_n m_n| < |m_n| \cdot \sup_k |a_k|$ montre la suite $(a_n m_n)$ est dans $\mathcal{M}_K$. Ainsi $\mathcal{M}$ est bien un idéal. Cela étant, soit $(a_n)_{n\in\mathbb{N}} \in \mathcal{A}_K/\mathcal{M}_K$. D'après l'assertion 1, il existe un constante $\kappa > 0$ telle qu'on ait $|a_n| > \kappa$ au-delà d'un certain rang n_0. Définissons alors un suite $(b_n)_{n\in\mathbb{N}}$ par $b_n = 0$ pour $n \leqslant n_0$, et $b_n = a_n^{-1}$ pour $n > n_0$. Nous obtenons pour n et $p > n_0$:

$$|b_n - b_p| = \frac{|a_p - a_n|}{|a_n||a_p|} \leqslant \frac{1}{\kappa}|a_n - a_p|,$$

de sorte que $(b_n)_{n\in\mathbb{N}}$ est bien une suite de Cauchy. Et la suite $(1 - a_n b_n)_{n\in\mathbb{N}}$ est trivialement dans $\mathcal{M}_K$ puisqu'elle est ultimement nulle. D'où la maximalité. □

Assertion (3)**.** *L'application $\mu = (\mu_n)_{n\in\mathbb{N}} \;\mapsto\; |\mu| = \lim_n |\mu_n|$ définit par passage au quotient une valeur absolue sur $\hat{K}$.*

Preuve : Il est clair que $|\mu|$ ne dépend que de la classe de μ modulo $\mathcal{M}_K$. Cela étant, la vérification des trois exiomes (VA i) est évidente. □

Assertion (4)**.** $\hat{K}$ *contient* K *comme sous-corps dense.*

Preuve : En premier lieu $\hat{K}$ contient bien K identifié à l'ensemble des classes de suites constantes (la seule suite constante qui tend vers 0 étant la suite nulle). De plus la valeur absolue sur $\hat{K}$ prolonge bien celle de K. Reste donc seulement à vérifier la densité. Prenons donc un élément μ de $\hat{K}$, et observons que c'est la classe dans $\hat{K}$ d'une suite de Cauchy $(\mu_n)_{n\in\mathbb{N}}$ d'éléments de K. Du critère de Cauchy

$$\forall\, \varepsilon \;\; \exists\, n_0 \in \mathbb{N} \;\; \forall\, n, p > n_0 \text{ tel que } |\mu_n - \mu_p| < \varepsilon,$$

nous tirons, par passage à la limite :

$$\forall\, \varepsilon \;\; \exists\, n_0 \in \mathbb{N} \;\; \forall\, n > n_0 \text{ on a } |\mu_n - \mu| < \varepsilon,$$

ce qui nous montre que μ est la limite dans $\hat{K}$ de la suite $(\mu_n)_{n\in\mathbb{N}}$ d'éléments de K. □

Assertion (5)**.** $\hat{K}$ *est complet.*

Preuve : Partons d'une suite de Cauchy $(\mu_n)_{n\in\mathbb{N}}$ d'éléments de $\hat{K}J$. D'après l'assertion 4, pour chaque $n \geqslant 1$, nous pouvons trouver un υ_n dans K qui vérifie $|\mu_n - \upsilon_n| < \frac{1}{n}$. De l'inégalité

$$|\upsilon_n - \upsilon_p| \leqslant |\upsilon_n - \mu_n| + |\mu_n - \upsilon_p| + |\mu_p - \upsilon_p| \leqslant |\mu_n - \mu_p| + \frac{1}{n} + \frac{1}{p},$$

nous concluons que la suite $(\upsilon_n)_{n\in\mathbb{N}}$ est dans $\mathcal{A}_K$ donc convergente dans $\hat{K}$ vers la classe υ qui est donc la limite de $(\mu_n)_{n\in\mathbb{N}}$. □

2.2 Places du corps des rationnels et des corps de nombres

2.2.1 Places du corps des rationnels

Théorème 9 (Ostrowski)**.** *Les seuls topologies de $\mathbb{Q}$ définies par des valeurs absolues sont :*

(i) La topologie discrète, qui est associée à la valeur absolue triviale $|x|_0 = 1$, pour $x \neq 0$.

(ii) La topologie usuelle, qui est associée à la valeur absolue réelle $|x|_\infty = \sup\{x, -x\}$.

(iii) Les topologies p-adiques qui sont associées aux valeurs absolues $|x|_p = p^{-\nu_p(x)}$, définies par les valuations attachés aux nombres premiers.

En d'autres termes, les places de $\mathbb{Q}$ sont la place à l'infini, notée ∞, et les places finies, qui correspondent aux nombres premiers.

Preuve : Considérons une valeur absolue non triviale, disons $|\cdot|$, sur $\mathbb{Q}$; et distinguons deux cas :

1er cas : Il existe un entier naturel non nul n de valeur absolue $|n| < 1$. Dans ce cas, l'un au moins des facteurs premiers de n, disons p, vérifie la même inégalité $|p| < 1$. Posons alors $c = \sup\{|1|, \ldots, |p-1|\}$, puis pour chaque $a \in \mathbb{N}$, écrivons $a = \sum_{i=0}^{k} a_i p^i$ son développement en base p (avec $k = [\log a / \log p]$). Nous obtenons :

$$|a| = |\sum a_i p^i| \leqslant \sum_{i=0}^{k} |a_i||p|^i \leqslant c \sum_{i=0}^{\infty} |p|^i = \frac{c}{1-|p|}.$$

Et la topologie est donc ultramétrique. En particulier, nous avons $|a| \leqslant 1$ pour tout a dans $\mathbb{Z}$. Ce point acquis, pour chaque premier q distinct de p et de n entier arbitrairement grand, nous pouvons trouver une relation de Bézout entre p^n et q^n, disons $\mu_n p^n + \vartheta_n q^n = 1$, de sorte que nous avons :

$$\begin{aligned} 1 &= |\mu_n p^n + \vartheta_n q^n| \\ &\leqslant |\mu_n|\,|p|^n + |\vartheta_n|\,|q|^n \\ &\leqslant |p|^n + |q|^n|, \end{aligned}$$

ce qui implique $|q| = 1$. Il suit donc, comme attendu :

$$|a| = |\prod p_i^{\nu_{p_i}(a)}| = |p|^{\nu_p(a)},$$

et la topologie associée à $|\cdot|$ est la topologie p-adique.

2ème cas : Pour chaque entier $n > 1$, on a $|n| \geqslant 1$. Notons dans ce cas que l'inégalité à droite est toujours stricte : En effet, sinon prenons $b > 1$ avec $|b| = 1$, posons $c(b) = \sup\{1, \ldots, |b-1|\}$ et, pour a dans $\mathbb{N}$, écrivons a^n en base b. Nous obtenons :

$$\begin{aligned} |a| &= |a^n|^{1/n} \\ &= |\sum_{i=0}^{[\log a^n / \log b]} a_i b^i|^{1/n} \\ &\leqslant c(b)^{1/n} \left(n \frac{\log a}{\log b} + 1 \right)^{1/n}, \end{aligned}$$

et donc $|a| \leqslant 1$, contrairement à la non trivialité de la valeur absolue.
En resumé, pour a et b entiers strictement plus grands que 1, nous avons $|a| > 1$ et $|b| > 1$. Reprenons les notations précédents, et écrivons a^n en base b. Nous obtenons ici :

$$\begin{aligned} |a| &= |a^n|^{1/n} \\ &\leqslant \left(\sum_{i=0}^{[\log a^n / \log b]} c(b)|b|^i \right)^{1/n} \\ &\leqslant \left(c(b) \frac{|b|}{|b|-1} \right)^{1/n} |b|^{\log a / \log b}, \end{aligned}$$

et donc :

$$|a| \leqslant |b|^{\log a / \log b}, \text{ i.e. } |a|^{1/\log a} \leqslant |b|^{1/\log b}, \text{ et, par symétrie } |a|^{1/\log a} = |b|^{1/\log b}.$$

Notons s la quantité $\log|a|/\log a$, qui est en fait indépendante de a, nous concluons : $|a| = a^s$, pour $a \in \mathbb{Q}_+$; et la topologie associée est bien la topologie réelle.

□

Corollaire 6 (Formule du produit)**.** *Pour tout rationnel non nul x, les normalisations précédents conduisent à la formule étendue aux places de $\mathbb{Q}$:*

$$\prod_{p \in \mathrm{Pl}_{\mathbb{Q}}} |x|_p = 1.$$

Preuve : Écrivons $x = \mathrm{sg}(x) \prod_{p \mid x} p^{\nu_p(x)}$. Nous obtenons : $|x|_\infty = \prod_{p \mid x} p^{\nu_p(x)} = \prod_{p \mid x} |x|_p^{-1}$. □

Définition 3. On note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la métrique p-adique. C'est un corps valué complet qui contient $\mathbb{Q}$ comme sous-corps dense.

2.2.2 Places des corps de nombres

Rappelons que si K est un corps de nombres (i.e. une extension de degré fini sur le corps des rationnels), l'anneau des entiers A_K est un anneau de Dedekind (i.e. un anneau noethérien, intégralement clos, et dont les idéaux premiers non nuls sont maximaux). En particulier, tout idéal non nul a de A_K s'écrit de façon unique

$$a = \prod_{p \mid a} p^{\nu_p(a)},$$

comme produit de puissances d'idéaux premiers non nuls.

Par ailleurs, si ϑ est un élément primitif de K de $\mathbb{Q}$ (i.e. tel qu'on ait $K = \mathbb{Q}[\vartheta]$), et

$$P(X) = \prod_{i=1}^{r} (X - x_i) \prod_{i=r+1}^{r+c} [(X - x_i)(X - \overline{x}_i)]$$

la factorisation dans $\mathbb{R}[X]$ de son polynôme minimal, on voit que K possède exactement r plongements réels

$$\sigma_i \mid \vartheta \longmapsto x_i, \text{ pour } i = 1, \dots, r;$$

et $2c$ plongements complexes

$$\sigma_i \mid \vartheta \longmapsto x_i \quad \& \quad \overline{\sigma}_i \mid \vartheta \longmapsto \overline{x}_i, \text{ pour } i = r+1, \dots, r+c,$$

avec au total $r + 2c = n = [K : \mathbb{Q}]$. Cela étant, nous avons :

Théorème 10. *Les topologies de K définies par des valeurs absolues sont :*

(i) La topologie discrète, qui est associée à la valeur absolue triviale.

(ii) Les $r + c$ topologies archimédiennes qui sont associées aux plongements réels ou complexes par les formules $|x|_i = |\sigma_i(x)|_\infty$, pour $i = 1, \dots, r$ et $|x|_i = \sigma_i(x)\overline{\sigma}_i(x)$, pour $i = r+1, \dots, r+c$.

(iii) Les topologies ultramétriques qui sont associées aux valeurs absolues $\mathfrak{p}$-adiques normalisées données par

$$|x|_\mathfrak{p} = N\mathfrak{p}^{-\nu_\mathfrak{p}(x)},$$

formule dans laquelle $N\mathfrak{p} = (A_K : \mathfrak{p}) = \mathfrak{p}^{f_\mathfrak{p}(K:\mathbb{Q})}$ désigne la norme absolue de l'idéal premier $\mathfrak{p}$.

Preuve : Considérons une valeur absolue $|\cdot|$ sur K. Puisque sa restriction à $\mathbb{Q}$ est trivialement une valeur absolue sur $\mathbb{Q}$, trois cas seulement peuvent se présenter :

(i) ou bien c'est la valeur absolue triviale : Dans ce cas $|\mathbb{Z}|$ est borné et nous avons donc l'inégalité ultramétrique. En particulier, pour $x \in K^\times$, de polynôme minimal $P(X) = X^n + \sum_{i=0}^{n-1} a_i x^i$ dans $\mathbb{Q}[X]$, il vient donc

$$|x|^n \leqslant \sup\{|a_i x^i|\} \leqslant \sup\{1, |x|^{n-1}\},$$

i.e. $|x| \leqslant 1$; d'où il suit que $|\cdot|$ est constante sur $K^\times$, autrement dit que $|\cdot|$ est la valeur absolue triviale.

(ii) ou bien elle est archimédienne, et induit sur $\mathbb{Q}$ la topologie usuelle : Dans ce cas, si ϑ est un élément primitif de K sur $\mathbb{Q}$, le complété $\hat{K}$ de K contient celui, $\mathbb{R}$, de $\mathbb{Q}$ ainsi que l'élément ϑ, et donc la $\mathbb{R}$-algèbre intègre et de dimension finie $\mathbb{R}[\vartheta]$ qui est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$. Dans les deux éventualités, $\mathbb{R}[\vartheta]$ est complet donc fermé dans $\hat{K}$. Mais comme il contient $K = \mathbb{Q}[\vartheta]$ qui est dense dans $\hat{K}$, cela entraîne $\hat{K} = \mathbb{R}[\vartheta]$, i.e. $\hat{K} = \mathbb{R}$ ou $\mathbb{C}$, et la topologie de K est bien déterminée par le plongement réel ou complexe $K \hookrightarrow \hat{K}$ donné par ϑ.
Inversement, chaque plongement réel ou complexe de K définit clairement une valeur absolu sur K. Reste à vérifier que les $r+c$ valeurs absolues aunsi obtenues ne sont pas équivalentes. Supposons donc $|\cdot|_i \sim |\cdot|_j$, auquel cas σ_i et σ_j induisent des isomorphismes du complété $\hat{K}$ sur $\mathbb{R}$ ou $\mathbb{C}$. Ainsi $\sigma_i \cdot \sigma_j^{-1}$ est alors un automorphisme du corps topologique $\mathbb{R}$ ou $\mathbb{C}$, ce qui entraîne $\sigma_i = \sigma_j$ dans le cas réel, $\sigma_i = \sigma_j$ où $\overline{\sigma}_j$ dans celui complexe, comme attendu.

(iii) ou bien c'est une valeur absolue ultramétrique non triviale qui induit sur $\mathbb{Q}$ la topologie p-adique pour un certain premier p, auquel cas :

— l'anneau des entiers A_K est contenu dans la boule fermée $B' = \{x \in K \,|\, |x| \leqslant 1\}$, puisque de l'existence d'une relation de dépendance intégrale pour un x de K

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0,$$

on déduit immédiatement l'inégalité

$$|x|^n = |x^n| \leqslant \sup_{i=0}^{n-1}\{|a_i x^i|\} \leqslant \sup_{i=0}^{n-1}\{|x|^i\},$$

qui entraîne $|x| \leqslant 1$, i.e. $x \in B'$;

— et son intersection $\mathfrak{p} = A_K \cap B$ avec la boule ouverte $B = \{x \in K \,|\, |x| < 1\}$ est ainsi un idéal premier (puisqu'on a ($|x| \leqslant 1$, $|y| \leqslant 1$ et $|xy| < 1$)$\Rightarrow$($|x| \leqslant 1$ ou $|y| < 1$)), et non nul ($p \in \mathfrak{p}$), donc maximal de A_K.
Soit alors $S = A_K \setminus \mathfrak{p}$ l'intersection de A_K avec la sphère unité. L'anneau des fractions $S^{-1}A_K$ est ainsi un anneau de Dedekind local i.e. un anneau de valuation discrète : si π est un uniformisante (i.e. un élément de valuation $\nu_\mathfrak{p} = 1$), tout élément de $S^{-1}A_K$ s'écrit donc de façon unique $x = \mu\pi^{\nu_\mathfrak{p}(x)}$, avec $\mu \in S$, et il suit $|x| = |\pi|^{\nu_\mathfrak{p}(x)}$ de sorte que la topologie sur K est la topologie $\mathfrak{p}$-adique. □

Scolie (Formule du produit)**.** *Avec les normalisations précédentes, on a pour tout* χ *de* $K^\times$

$$\prod_{\mathfrak{p} \in \mathrm{Pl}_K} |x|_\mathfrak{p} = 1,$$

le produit étant étendu à toutes les places de K.

Preuve : Nous avons d'un coté : $\prod_{\mathfrak{p}|\infty} |x|_\mathfrak{p} = \prod_{i=1}^{r+2c} |\sigma_i(x)| = |\, N_{K/\mathbb{Q}}(x)|_\infty$. Et d'un autre coté :

$$\prod_{\mathfrak{p} \nmid \infty} |x|_\mathfrak{p} = \prod_{\mathfrak{p} | Ax} N\mathfrak{p}^{-\nu_\mathfrak{p}(x)} = N_{K/\mathbb{Q}}(A_K x)^{-1} = |\, N_{K/\mathbb{Q}}(x)|_\infty^{-1};$$

d'où le résultat. □

Naturellement, c'est la formule du produit qui suggère les normalisations retenues, en particulier le chois d'un valeur absolue au sens large pour les places complexes (alors que la valeur absolue usuelle est $\sqrt{\sigma_i(x)\overline{\sigma_i}(x)}$).

Définition 4. On note $K_\mathfrak{p}$ le complété de K pour la topologie $\mathfrak{p}$-adique. C'est donc un corps ultramétrique complet qui contient K comme cous-corps dense.

Nous allons voir que $K_\mathfrak{p}$ est de degré fini sur $\mathbb{Q}_p$.

2.2.3 Propriétés topologiques des extensions de $\mathbb{Q}_p$

Lemme 2 (Lemme de représentation)**.** *Soient* K *un corps de nombres, et* $\mathfrak{p}$ *un idéal premier non nul de l'anneau des entiers* A*. Supposons choisis :*

(i) une suite $(\pi_n)_{n\in\mathbb{Z}}$ *d'éléments de* $K^\times$ *de valuations étagées* $N\mathfrak{p}(\pi_n) = n$ *;*

(ii) et un système de représentants R *dans* A *du corps résiduel* $k = A/\mathfrak{p}$*.*

Alors tout élément x *du complété* $K_\mathfrak{p}$ *s'écrit de façon unique comme somme d'une série :*

$$x = \sum_{m \geqslant \nu_\mathfrak{p}(x)} a_m \pi_m, \text{ avec les } a_m \text{ dans } R \text{ et } a_{\nu_\mathfrak{p}(x)} \notin \mathfrak{p}.$$

Preuve : La convergence de la série résulte immédiatement du critère de Cauchy : l'espace étant ultramétrique, les séries de Cauchy sont exactement celles dont le terme général tend vers 0, ce qui est évidemment le cas ici. L'unicité de l'écriture s'obtient comme suit : Supposons l'égalité $\sum a_m\pi_m = \sum b_m\pi_m$, disons $\sum_{m\geqslant m_0}(a_m - b_m)\pi_m = 0$, avec $a_{m_0} \neq b_{m_0}$. Nous obtenons d'un côté $|a_{m_0} - b_{m_0}| = 1$, et d'un autre

$$|a_{m_0} - b_{m_0}| = \left| \sum_{m > m_0} (a_m - b_m) \frac{\pi_m}{\pi_{m_0}} \right| \leqslant \left| \frac{\pi_{m_0+1}}{\pi_{m_0}} \right| < 1,$$

une contradiction. Enfin, les chiffres a_m du développement d'un x de $K_\mathfrak{p}^\times$ peuvent se construire en deux temps : d'abord, pour $x \in K^\times$, en introduisant l'anneau des fractions $S^{-1}A$ (avec $S = A \setminus \mathfrak{p}$) et en considérant les congruences, pour $n \geqslant \nu_\mathfrak{p}(x)$:

$$a_{n+1} \equiv \left(x - \sum_{i=\nu_\mathfrak{p}(x)}^{n} a_i\pi_i \right) \pi_{n+1}^{-1} \mod (S^{-1}\mathfrak{p}),$$

qui déterminent les a_n par récurrence. Ensuite, pour $x \in K_\mathfrak{p}^\times$, en observant qu'un tel x est limite de x_n dans $K^\times$, qui ont forcément les mêmes m premiers chiffres à partir d'un certain rang $n(m)$. □

Théorème 11. *Le complété ultramétrique d'un corps de nombres en une place $\mathfrak{p}$ est un corps localement compact et totalement discontinu. C'est en particulier les cas de $\mathbb{Q}_p$.*

Preuve : Ul suffit de vérifier que la boule unité ouverte $B = \{x \in K_\mathfrak{p} \,|\, |x| < 1\}$ est compacte. Or d'après le lemme de représentation, les éléments de B sont ceux de la forme :

$$x = \sum_{m \geqslant 1} a_m \pi_m, \text{ avec des } a_m \text{ arbitraires dans } R.$$

Si donc $(x_n)_{n\in\mathbb{N}}$ est une suite quelconque d'éléments de B, avec disons $x_n = \sum_{m\geqslant 1} a_{nm}\pi_m$, une infinité d'entre eux ont même premier chiffre a_1 ; et, parmi ceux-ci une infinité ont également même second chiffre a_2...Par une récurrence immédiate, nous construisons ainsi une valeur d'adhérence $x = \sum_{m\geqslant 1} a_m x_m$ de la suite $(x_n)_{n\in\mathbb{N}}$; d'où le résultat annoncé. □

Proposition 6. *Le degré local $[K_\mathfrak{p} : \mathbb{Q}_p]$ est le produit $d_\mathfrak{p}(K/\mathbb{Q}) = e_\mathfrak{p}(K/\mathbb{Q})f_\mathfrak{p}(K/\mathbb{Q})$ de l'indice de ramification $e_\mathfrak{p}(K/\mathbb{Q}) = v_\mathfrak{p}(p)$ et du degré résiduel $f_\mathfrak{p}(K/\mathbb{Q}) = [A/\mathfrak{p} : \mathbb{F}_p]$.*

Preuve : Fixons un uniformisante π dans l'anneau A, et écrivons e pour $e_\mathfrak{p}(K/\mathbb{Q})$ et f pour $f_\mathfrak{p}(K/\mathbb{Q})$. D'un côté pour construire un système de représentants de $A/\mathfrak{p}$, nous pouvons relever dans A une base $e_1, \ldots, e_f$ de $A/\mathfrak{p}$ sur $\mathbb{F}_p$ et former les sommes finies $\sum_{i=1}^f a_i e_i$ avec $a_i \in \{0, 1, \ldots, p-1\}$ parcourant un système de représentants des classes résiduelles de $\mathbb{Z}$ modulo $p\mathbb{Z}$.

Cela étant, le lemme de représentation nous permet d'écrire tout élémént x de $K_\mathfrak{p}$ sous la forme :

$$x = \sum_{i=0}^{e-1} \sum_{j=1}^{f} \left(\sum_{k\geqslant k_0} a_{ijk} p^k \right) \pi^i e_j$$

où nous retrouvons entre parenthèses la forme générale d'un élément de $\mathbb{Q}_p$, ce qui nous montre que les $\pi^i e_j$ forment une $\mathbb{Q}_p$-base de $K_\mathfrak{p}$. □

Corollaire 7. *Sur chaque extension finie $K_\mathfrak{p}$ de $\mathbb{Q}_p$, il existe une unique valeur absolue $|\cdot|_\mathfrak{p}$ qui prolonge celle de $\mathbb{Q}_p$. Il en résulte que tout $\mathbb{Q}_p$-isomorphisme de $\overline{\mathbb{Q}}_p$ est isométrique, et que pour tout x de $K_\mathfrak{p}$, la valeur absolue $|x|_\mathfrak{p}$ est donnée par :*

$$|x|_\mathfrak{p} = |\, N_{K_\mathfrak{p}/\mathbb{Q}_p}(x)|_p^{1/[K_\mathfrak{p}:\mathbb{Q}_p]}.$$

Preuve : Puisque $\mathbb{Q}_p$ est localement compact, il existe une unique topologie qui fait de $K_\mathfrak{p}$ un $\mathbb{Q}_p$-espace vectoriel normé de dimension finie. En particulier, pour $K_\mathfrak{p}$ galoisienne sur $\mathbb{Q}_p$ et $\sigma \in \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$, les valeurs absolues $x \mapsto |x|_\mathfrak{p}$ et $x \mapsto |\sigma(x)|_\mathfrak{p}$, qui coïncident sur $\mathbb{Q}_p$, sont égales, et il suit :

$$|x|_\mathfrak{p} = \left(\prod_\sigma |x^\sigma|_\mathfrak{p} \right)^{1/d_\mathfrak{p}} = |\, N_{K_\mathfrak{p}/\mathbb{Q}_p}(x)|_p^{1/d_\mathfrak{p}} = |\, N_{K_\mathfrak{p}/\mathbb{Q}_p}(x)|_\mathfrak{p} = |x|_p^{d_\mathfrak{p}}.$$

□

Théorème & Définition 3. *On note $\overline{\mathbb{Q}}_p$ une clôture algèbrique du complété p-adiqu de $\mathbb{Q}$. Il existe sur $\overline{\mathbb{Q}}_p$ une unique valeur absolue qui prolonge celle de $\mathbb{Q}_p$. On la note $|\cdot|_\mathfrak{p}$. Le corps $\overline{\mathbb{Q}}_p$ n'est pas complet pour la métrique associée (En particulier il n'est pas localement compact).*

Preuve : Pour établir ce résultat, nous nous appuierons sur le :

Lemme 3 (Lemme de Krasner)**.** *Soient $K_\mathfrak{p}$ un corps local (i.e. une extension finie de $\mathbb{Q}_p$) et a dans $\overline{\mathbb{Q}}_p$. Si b est un élément de $\overline{\mathbb{Q}}_p$ qui approche mieux a que ses conjugués au-dessus de $K_\mathfrak{p}$, on a $K_\mathfrak{p}[a] \subset K_\mathfrak{p}[b]$.*

Preuve du lemme : Supposons que $a \notin K_p[b]$. Il existe alors un $K_p[b]$-automorphisme de $\overline{\mathbb{Q}}_p$, disons σ, qui ne fixe pas a. Et, par hypothèse nous avons alors $|b-a|_p < |\sigma(a)-a|_p$. Or, il vient ici :

$$\begin{aligned} |\sigma(a)-a| &\leqslant \sup\{|\sigma(a)-b|_p, |b-a|_p\} \\ &= \sup\{|\sigma(a)-\sigma(b)|_p, |a-b|_p\} \\ &= |a-b|_p, \end{aligned}$$

une contradiction. □

Nous allons construire par récurrence une suite de Cauchy d'éléments de $\overline{\mathbb{Q}}_p$ en posant $x_n = \sum_{i=0}^{n} \sqrt[2^i]{p} p^{m_i}$, et en imposant à a suite d'entiers (m_n) des conditions de croissance.

Notons d'abord que nous avons de façon évidente $\mathbb{Q}_p[x_n] \subset \mathbb{Q}_p[\sqrt[2^n]{p}]$ (qui est une extension totalement ramifiée, de degré 2^n sur $\mathbb{Q}_p$), et l'égalité pour $n = 0$. Supposant donc construit x_n vérifiant $\mathbb{Q}_p[x_n] = \mathbb{Q}_p[\sqrt[2^n]{p}]$, et choisissant m_{n+1} assez grand, nous concluons par le lemme de Krasner $\mathbb{Q}_p[x_{n+1}] \supset \mathbb{Q}_p[x_n] = \mathbb{Q}_p[\sqrt[2^n]{p}]$, puis $\mathbb{Q}[x_{n+1}] = \mathbb{Q}_p[\sqrt[2^n]{p}, x_{n+1}] = \mathbb{Q}_p[\sqrt[2^{n+1}]{p}]$, ce qui nous assure que x_n est exactement de degré 2^n pourvu que la suite m_n croisse assez vite.

Ce point acquis, il résulte de là que la fonction continue $P \mapsto |P(x_n)|_p$ qui ne l'annule donc pas sur l'espace compact des polynômes entiers (i.e. de norme $|P|_p = \sup|\text{coef}|_p$ égale au plus à 1) de $\mathbb{Q}_p[X]$ de degré inférieur strictement à 2^n, est minorée sur cet espace pour une constante strictement positive, ce qui permet de choisir m_{n+1} assez grand pour avoir $|x_{n+1}-x_n|_p < |P(x_n)|_p$.

Soit alors x la limite dans $\overline{\mathbb{Q}}_p$ de la suite (x_n), si elle existe, puis P un polynôme non nul à coefficients dans $\mathbb{Q}_p$, que nous pouvons supposer (quitte à le multiplier par une puissance de p) de norme $|P|_p \leqslant 1$. Pour n assez grand (disons $2^{n+1} > \deg P$), l'inégalité ultramétrique nous donne $|x_n - x|_p = |x_n - x_{n+1}|_p < |P(x_n)|_p$ par construction, d'où en développant $P(x)$ en puissances de $(x - x_n)$:

$$|P(x)|_p = |P(x_n)|_p \neq 0,$$

de sorte que x n'est racine d'aucun polynôme à coefficients dans $\mathbb{Q}_p$. □

Scolie. *Le complété $\mathbb{C}_p$ de $\overline{\mathbb{Q}}_p$ pour la topologie p-adique est algébriquement clos.*

Preuve : Il s'agit de vérifier que tout polynôme P de $\mathbb{C}_{p[X]}$ de degré $d > 0$ a une racine dans $\mathbb{C}_p$. Et comme un tel polynôme est limite d'une suite $(P_n)_{n\in\mathbb{N}}$ de polynômes de même degré à coefficients dans $\overline{\mathbb{Q}}_p$, lesquels ont d racines (distinctes ou confondues) dans $\overline{\mathbb{Q}}_p$, tout le problème consiste à s'assurer que l'on peut choisir l'une d'elles, disons x_n, de telle sorte que la suite (x_n) soit de Cauchy.

Nous pouvons évidement nous limiter au cas où les P_n sont unitaires. Cela étant, supposons déjà choisis $x_0, x_1, \ldots, x_n$ jusqu'à un rang n au delà duquel nous ayons $|P_{m+1} - P_m| < 1$. Nous avons alors, en notant $x_{n+1,1}, \ldots, x_{n+1,d}$ les racines de P_{n+1} :

$$\begin{aligned} \prod_{i=1}^{d} |x_n - x_{n+1,i}|_p &= |P_{n+1}(x_n)|_p \\ &= |P_{n+1}(x_n) - P_n(x_n)|_p \\ &\leqslant |P_{n+1} - P_n| \cdot \sup\{1, |x_n|_p^d\}, \end{aligned}$$

de sorte que la suite (x_n) reste bornée par, disons $\kappa \geqslant 1$, puis nous donne :

$$|x_n - x_{n+1}|_p \leqslant \kappa |P_n - P_{n+1}|_p^{1/d},$$

donc la convergence de (x_n) dans $\mathbb{C}_p$ par le critère de Cauchy, vers une racine x de P. □

2.3 Propriétés multiplicatives des corps p-adiques

2.3.1 Structure du groupe multiplicatif $K_p^\times$

Considérons un corps local K_p complété d'un corps de nombres en un place ultramétrique p. Désignons par $A_p = \{x \in K_p \,|\, |x| < 1\}$ la boule unité "fermeé" et par $p_p = \{x \in K_p \,|\, |x| < 1\}$ la boule unité "ouverte" (lesquelles

boules sont l'une et l'autre ouvertes et compacts comme nous l'avons vu). LE lemme de représentation montre que $A_\mathfrak{p}$ (resp. $\mathfrak{p}_\mathfrak{p}$) n'est autre que l'adhérence dans $K_\mathfrak{p}$ de l'anneau des entiers A de K (resp. de l'idéal premier non nul $\mathfrak{p}$ de A) et aussi du localisé $S^{-1}A$ de A pour la partie multiplicative $S = A \setminus \mathfrak{p}$ (resp. du localisé $S^{-1}\mathfrak{p} = K \cap \mathfrak{p}_\mathfrak{p}$ de $\mathfrak{p}$). En d'autres termes $A_\mathfrak{p}$ est le complété $\mathfrak{p}$-adique de A et il contient (strictement) le localisé $S^{-1}A$: c'est un anneau complet de valuation discrète d'idéal maximal $\mathfrak{p}_\mathfrak{p}$ et de corps résiduel fini

$$A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \simeq S^{-1}A/S^{-1}\mathfrak{p} \simeq A/\mathfrak{p}$$

les classes résiduelles de $A_\mathfrak{p}$ modulo $\mathfrak{p}_\mathfrak{p}$ étant bien représentées, en vertu du Lemme 2, par celles de A modulo $\mathfrak{p}$. Cela étant :

Proposition 7. *Le choix d'une uniformisante π de $\mathfrak{A}_\mathfrak{p}$ définit un isomorphisme de groupes topologique*

$$K_\mathfrak{p}^\times \simeq U_\mathfrak{p} \cdot \pi^\mathbb{Z},$$

où $U_\mathfrak{p} = \{x \in K_\mathfrak{p} \,|\, |x| = 1\}$ est le groupe des unités de l'anneau $A_\mathfrak{p}$, et la correspondance est donnée par l'écriture $x = \mu \cdot \pi^{\nu_\mathfrak{p}(x)}$, avec $\mu = x\pi^{-\nu_\mathfrak{p}(x)}$, d'un élément $x \in K_\mathfrak{p}^\times$.

Preuve : La restriction à $K_\mathfrak{p}^\times$ puis à $U_\mathfrak{p}$ de la topologie métrique de $K_\mathfrak{p}$ fait de ceux-ci des groupes topologiques. Il s'agit donc simplement de vérifier que si l'on équipe $\pi^\mathbb{Z} \simeq \mathbb{Z}$ de la topologie discrète, la surjection naturelle $\nu_\mathfrak{p} : K_\mathfrak{p}^\times \to \mathbb{Z}$, qui a précisément pour noyau $U_\mathfrak{p}$ est simultanément ouverte et continue. Or cela résulte de ce qu'elle est localement constante sur $K_\mathfrak{p}^\times$. □

Proposition 8. *Chaque classe résiduelle $x + \mathfrak{p}$ de $U_\mathfrak{p}$ (modulo $\mathfrak{p}$) est représentée par une unique racine $(N\mathfrak{p} - 1)$-ième de l'unité $\omega(x)$. En particulier l'application $x \mapsto \omega(x) \cdot \frac{x}{\omega(x)}$ définit un isomorphisme de groupes topologiques*

$$U_\mathfrak{p} \simeq \mu_\mathfrak{p}^0 \cdot U_\mathfrak{p}^1,$$

où $\mu_\mathfrak{p}^0 \simeq (A/\mathfrak{p})^\times$ est le groupe des racines $(N\mathfrak{p}-1)$-ième de l'unité dans $K_\mathfrak{p}^\times$, et $U_\mathfrak{p}^1 = \{x \in U_\mathfrak{p} \,|\, x \equiv 1 (\bmod \mathfrak{p}_\mathfrak{p})\}$ est le groupe principal de $U_\mathfrak{p}$.

La preuve de ce dernier résultat repose sur le :

Lemme 4 (Lemme de Hensel)**.** *Soient A un anneau complet de valuation discrète, d'idéal maximal $\mathfrak{p}$, et P un polynôme non nul de $A[X]$. Si la réduction de P modulo $\mathfrak{p}$ admet un élément $\bar{a}$ du corps résiduel $A/\mathfrak{p}$ comme racine simple, alors $\bar{a}$ est la réduction d'une unique racine a de P dans A. De plus a est une racine simple de P.*

Preuve du lemme : L'existence de a s'obtient simplement par itération de la méthode de Newton : Partons d'un relèvement arbitraire a_0 de $\bar{a}$ dans A ; remarquons que les hypothèses faites nous donnent :

$$P(a_0) \equiv 0 (\bmod \mathfrak{p}) \quad \& \quad P'(a_0) \not\equiv 0 (\bmod \mathfrak{p}).$$

Et posons : $a_1 = a_0 - \frac{P(a_0)}{P'(a_0)} \equiv a_0 (\bmod \mathfrak{p})$.

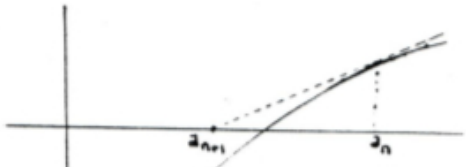
Nous obtenons

$$\begin{cases} P(a_1) = P(a_0) + (a_1 - a_0)P'(a_0) + (a_1 - a_0)^2 P''(a_0) \ldots & \equiv \pmod{\mathfrak{p}^2} \\ P'(a_1) = P'(a_0) + (a_1 - a_0)P''(a_0) + \ldots & \not\equiv \pmod{\mathfrak{p}^2}. \end{cases}$$

Plus généralement, supposant déjà construit un relèvement a_m de $\bar{a}$ vérifiant les deux conditions

$$P(a_m) \equiv 0 (\bmod \mathfrak{p}^{2^m}) \quad \& \quad P'(a_m) \equiv P(a_0) \not\equiv 0 (\bmod \mathfrak{p}),$$

et en posant alors $a_{m+1} = a_m - P(a_m)/P'(a_m) \equiv a_m (\bmod \mathfrak{p}^{2^m})$ nous obtenons ainsi un nouveau relèvement a_{m+1} de $\bar{a}$ qui vérifie les mêmes conditions à l'ordre supérieur :



$$\begin{cases} P(a_{m+1}) = [P(a_m) + (a_{m+1} - a_m)P'(a_m)] + (a_{m+1} - a_m)^2 P''(a_m) \ldots & \equiv \pmod{\mathfrak{p}^{2^{m+1}}} \\ P'(a_{m+1}) = P'(a_m) + (a_{m+1} - a_m)P''(a_m) + \ldots & \not\equiv \pmod{\mathfrak{p}^{2^{m+1}}}. \end{cases}$$

La suite $(a_m)_{m\in\mathbb{N}}$ est naturellement de Cauchy, et la limite
a dans l'anneau complet A satisfait les conditions attendues : $a \equiv a_0 (\mathrm{mod} \mathfrak{p})$ & $P(a) = 0$.

Quant à l'unicité, elle se vérifie comme suit : Soient $a \equiv b (\mathrm{mod}\ \mathfrak{p})$ avec $\begin{cases} P(a) = P(b) = 0 \\ P'(a) \not\equiv 0 \mod \mathfrak{p} \end{cases}$

De l'égalité

$$0 = |P(a) - P(b)| = |(a-b)P'(a) + (a-b)^2| \ldots = |a-b||P'(a)| = |a-b|,$$

nous concluons $a = b$ comme attendu. □

Preuve de la proposition : Le lemme de Hensel appliqué au polynôme $P(X) = X^{N\mathfrak{p}-1}$, dont la réduction $\overline{P}(X) = \prod_{\bar{x}\in(A/\mathfrak{p})^\times}(X - \bar{x})$ est scindée et séparable sur le corps résiduel $A/\mathfrak{p} = k$, nous montre que toute racine résiduelle $(N\mathfrak{p}-1)$-ième de l'unité $\bar{x} \in A/\mathfrak{p}$ se relève de façon unique en une racine locale de l'unité $\zeta = \omega(x) \in A_\mathfrak{p}$.

Ainsi $U_\mathfrak{p}$ contient le groupe $\mu_\mathfrak{p}^0 \simeq (A/\mathfrak{p})^\times$ des racines $(N\mathfrak{p}-1)$-ième de l'unité dans $\overline{K}_\mathfrak{p}$, et l'application localement constante $x \mapsto \omega(x)$ est bien un épimorphisme idempotent ouvert et continu de $U_\mathfrak{p}$ dans $\mu_\mathfrak{p}^0$ qui a pour noyau le sous-groupe $U_\mathfrak{p}^1$ des unités principales de $K_\mathfrak{p}$. □

2.3.2 Groupe des unités principales

Proposition 9. *Le groupe $U_\mathfrak{p}^1$ des unités principales est un $\mathbb{Z}_\mathfrak{p}$-module noethérien.*

Preuve : On définit une action de $\mathbb{Z}_\mathfrak{p}$ sur $U_\mathfrak{p}^1$ en posant : $(1+x)^\alpha = \sum_{n\geqslant 0}\binom{\alpha}{n}x^n$, pour $x \in \mathfrak{p}_\mathfrak{p}$ et $\alpha \in \mathbb{Z}_\mathfrak{p}$. La convergence de la série se montre comme suit :

Le coefficient $\binom{\alpha}{n}$ est la valeur en $\alpha \in \mathbb{Z}_\mathfrak{p}$ su n-ième polynôme de Hilbert $H_n(X) = \binom{X}{n} = \frac{X(X-1)\cdots(X-n+1}{n!}$. Or ce polynôme est continu sur $\mathbb{Z}_\mathfrak{p}$ et prend des valeurs entières aux points entiers (i.e. ici dans $\mathbb{N}$). Il en résulte, par densité, que l'on a $\binom{\alpha}{n} \in \mathbb{Z}_\mathfrak{p}$ pour $\alpha \in \mathbb{Z}_\mathfrak{p}$ donc $\left|\binom{\alpha}{n}x^n\right|_\mathfrak{p} \leqslant |x|^n$, ce qui montre que la série écrite est de Cauchy.

Cela étant, on a clairement $(1+x)^\alpha = \lim_{n\to\infty}(1+x)^{\alpha_n}$ pour chaque suite $(\alpha_n)_{n\in\mathbb{N}}$ d'entiers naturels convergeant vers α, d'où par passage à la limite les trois propriétés :

(i) $[(1+x)(1+y)]^\alpha = (1+x)^\alpha(1+y)^\alpha$,

(ii) $(1+x)^{\alpha+\beta} = (1+x)^\alpha(1+x)^\beta$,

(ii) $((1+x)^\alpha)^\beta = (1+x)^{\alpha\beta}$,

qui jointes à l'identité évidente $(1+x)^1 = 1+x$, montrent que $U_\mathfrak{p}^1$ est bien un $\mathbb{Z}_\mathfrak{p}$-module.

Pour montrer qu'il est noethérien, nous nous appuierons sur un lemme et un proposition :

Lemme 5. *Pour tout $i \geqslant 1$, soit $U_\mathfrak{p}^i = \{1 + x \in U_\mathfrak{p}^1 \,|\, x \in \mathfrak{p}_\mathfrak{p}^i\}$. Les $U_\mathfrak{p}^i$ ($i \geqslant 1$) forment une suite décroissante de sous-groupes ouverts et compacts de $U_\mathfrak{p}$ qui vérifient les isomorphismes*

$$U_\mathfrak{p}^i/U_\mathfrak{p}^{i+1} \simeq A/\mathfrak{p} \quad \textit{et par suite } (U_\mathfrak{p}^1 : U_\mathfrak{p}^i) = N\mathfrak{p}^{i-1}.$$

Preuve : Partons de l'application naturelle $1 + x \mapsto x$ de $U_\mathfrak{p}^1$ dans $\mathfrak{p}_\mathfrak{p}^i$. La congruence

$$(1+x)(1+y) - 1 = x + y + xy \equiv x + y (\mathrm{mod}\ \mathfrak{p}_\mathfrak{p}^{i+1})$$

pour x et y dans $\mathfrak{p}_\mathfrak{p}^i$ nous montre que nous obtenons ainsi par pasage au quotient un morphisme surjectif du groupe multiplicatif $U_\mathfrak{p}^i$ sur le groupe fini

$$\mathfrak{p}_\mathfrak{p}^i/\mathfrak{p}_\mathfrak{p}^{i+1} \simeq A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \simeq A/\mathfrak{p}$$

qui a pour noyau le translaté $U_\mathfrak{p}^i$ de la boule $\mathfrak{p}_\mathfrak{p}^i$. D'où le résultat annoncé. □

En particulier, puisque $U_\mathfrak{p}^i$ est ainsi un sous-$\mathbb{Z}_\mathfrak{p}$-module multiplicatif d'indice fini dans $U_\mathfrak{p}^1$, le caractère noethérien de $U_\mathfrak{p}^1$ peut se lire sur $U_\mathfrak{p}^i$. Or :

Proposition 10. *Soit e l'indice de ramification absolu du corps $K_\mathfrak{p}$, puis $\kappa = \left[\frac{e}{p-1}\right] + 1$. Alors pour tout $i \geqslant \kappa$, l'exponentielle $\mathfrak{p}$-adique définie sur $\mathfrak{p}_\mathfrak{p}^\kappa$ par la formule*

$$\exp x = \sum_{n \in \mathbb{N}} \frac{x^n}{n!},$$

et le logarithme $\mathfrak{p}$-adique défini sur le groupe principal $U_\mathfrak{p}^i$ par

$$\log(1+x) = \sum_{n \geqslant 1} (-1)^{n+1} \frac{x^n}{n},$$

induisent des isomorphismes réciproques entre les $\mathbb{Z}_p$-modules topologiques $\mathfrak{p}_\mathfrak{p}^i$ et $U_\mathfrak{p}^i = 1 + \mathfrak{p}_\mathfrak{p}^i$.

Preuve : Le calcule donne

$$v_\mathfrak{p}(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] e \leqslant ne \sum_{k=1}^{\infty} p^{-k} = n\frac{e}{p-1},$$

d 'où la convergence de la série $\sum \frac{x^n}{n!}$ pour $v_\mathfrak{p}(x) \geqslant \frac{e}{p-1}$. Plus précisément, lorsque cette condition est vérifiée, on a pour $n \geqslant 2$:

$$\begin{aligned} v_\mathfrak{p}\left(\frac{x^n}{n!}\right) - v_\mathfrak{p}(x) &= (n-1)v_\mathfrak{p}(x) - ne\sum_{k=1}^{s} p^{-k}, \quad (\text{ avec } s = [\ln n / \ln p]) \\ &> (n-1)\frac{e}{p-1} - \frac{ne}{p^s}\frac{p^s-1}{p-1} \\ &= \frac{e}{p-1}\left[n - 1 - n\frac{p^s-1}{p-1}\right] \\ &= \frac{e}{p-1}\left(\frac{n}{p^s} - 1\right) \\ &> 0, \end{aligned}$$

ce qui montre que $v_\mathfrak{p}(\exp - 1)$ est égal à $v_\mathfrak{p}(x)$ (égalité ultramétrique), autrement dit que l'exponentielle envoie $\mathfrak{p}_\mathfrak{p}^i$ dans $U_\mathfrak{p}^i$ (et même $\mathfrak{p}_\mathfrak{p}^i \setminus \mathfrak{p}_\mathfrak{p}^{i+1}$ dans $U_\mathfrak{p}^i \setminus U_\mathfrak{p}^{i+1}$).

L'inégalité banale $v_\mathfrak{p}\left(\frac{x^n}{n}\right) \geqslant v_\mathfrak{p}\left(\frac{x^n}{n!}\right)$, pour $n \geqslant 1$, montre de même que la série $-\sum \frac{(-x)^n}{n}$ converge pour $v_\mathfrak{p}(x) > \frac{e}{p-1}$ et que $\log(1+x)$ a alors même valuation que x. (En fait l'inégalité $v_\mathfrak{p}\left(\frac{x^n}{n}\right) = nv_\mathfrak{p}(x) - v_\mathfrak{p}(n) \geqslant nv_\mathfrak{p}(x) - \ln n / \ln p$ assure la convergence pour $v_\mathfrak{p} > 0$, mais ne donne pas d'information sur $v_\mathfrak{p}(\log(1+x))$).

Par spécialisation des identités formelles $\log(\exp X)) = X$ et $\exp(\log(1+X)) = 1+X$ on conclut que pour $i \geqslant \kappa$ le logarithme et l'exponentielle sont bien réciproque l'un de l'autre. Enfin, la $\mathbb{Z}_p$-linéarité $\exp \alpha x = (\exp x)^\alpha$ résulte par continuité du cas trivial $\alpha \in \mathbb{N}$ qui provient lui de l'équation fonctionelle $\exp(X+Y) = \exp X \exp Y$. □

En conclusion, nous avons donc :

Corollaire 8. *Pour $i \geqslant \kappa$, le groupe $U_\mathfrak{p}^i$ est un $\mathbb{Z}_p$-module libre de dimension $[K_\mathfrak{p} : \mathbb{Q}_p]$.*

Preuve : En effet, $U_\mathfrak{p}^i$ est alors isomorphe à $\mathfrak{p}_\mathfrak{p}^i$ comme $\mathbb{Z}_p$-module, et le lemme de représentation montre que ce dernier est un $\mathbb{Z}_p$-module lire de dimension $d_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p]$. □

Théorème 12. *Le groupe $U_\mathfrak{p}^1$ des unités principales d'un corps local $K_\mathfrak{p}$ est le produit du groupe cyclique $\mu_\mathfrak{p}^1$ des racines d'ordre p-primaire de l'unité dans $K_\mathfrak{p}$ et d'un $\mathbb{Z}_p$-module de rang $[K_\mathfrak{p} : \mathbb{Q}_p]$.*

Preuve : $U_\mathfrak{p}^1$ qui contient $U_\mathfrak{p}^\kappa$ comme un sous-module d'indice fini est bien un $\mathbb{Z}_p$-module de même dimension. Quant à son sous-module de torsion $\mu_\mathfrak{p}^1$, il est évidemment cyclique comme sous-groupe fini du groupe multiplicatif $K_\mathfrak{p}^\times$. □

Exemple 3. (i) pour p impair, on a $\mathbb{Q}_p^\times = \mu_p^0 \times (1 + p\mathbb{Z}_p) \times p^\mathbb{Z}$, et $1 + p\mathbb{Z}_p = (1+p)^{\mathbb{Z}_p}$;

(ii) pour $p = 2$, on a $\mathbb{Q}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \times 2^\mathbb{Z}$, et $1 + 4\mathbb{Z}_2 = 5^{\mathbb{Z}_2}$.

2.3.3 Recherche d'une $\mathbb{Z}_p$-base du groupe $U_\mathfrak{p}^1$

Nous nous proposons ici de déterminer effectivement un système minimal de générateurs du groupe $U_\mathfrak{p}^1$. Notre point de départ sera le :

Lemme 6 (Lemme de Nakayama)**.** *Soit M un $\mathbb{Z}_p$-module noethérien. Alors $M = \mathfrak{p}M$ implique $M = 0$. En particulier, pour qu'une famille $(x_i)_{i\in I}$ de vecteurs de M engendre M, il faut et il suffit que les classes modulo $\mathfrak{p}M$ des x_i engendrent le $\mathbb{F}_p$-espace vectoriel $M/\mathfrak{p}M$.*

Preuve : Supposons $M = \mathfrak{p}M \neq 0$, et faisons choix d'un système minimal de générateurs $(m_i)_{i=1,\dots,k}$. L'identité $M = \mathfrak{p}M$ permet alors d'écrire

$$m_k = \sum_{i=1}^{k} p\lambda_i m_i, \text{ avec les } \lambda_i \text{ dans } \mathbb{Z}_p, \text{ i.e. } m_k(1-p\lambda_k) = \sum_{i=1}^{k-1} p\lambda_i m_i$$

ce qui montre, puisque $1 - p\lambda_k$ est inversible dans $\mathbb{Z}_p$, que m_k s'exprime comme combinaison linéaire de $m_i, \dots, m_{k-1}$ contrairement à la minimalité supposé.

La seconde assertion du lemme s'obtient alors en appliquant la première au module quotient $M/\sum_{i\in I}\mathbb{Z}_p x_i$. □

Le lemme de Nakayama ramène ainsi notre problème à l'étude du quotient $U_\mathfrak{p}^1/U_\mathfrak{p}^{1\,p}$.

Proposition 11. *Soient π un uniformisante de $A_\mathfrak{p}$, et $x = 1 + \mu\pi^i$, avec $\mu \in U_\mathfrak{p}$, un élément de $U_\mathfrak{p}^i \setminus U_\mathfrak{p}^{i+1}$ pour $i \geqslant 1$. Soit $e = v_\mathfrak{p}(p)$ l'indice de ramification absolu de $\mathfrak{p}$. Il vient alors :*

$$x^p \equiv \begin{cases} 1 + \mu^p\pi^{ip} & (\bmod\ \mathfrak{p}_\mathfrak{p}^{ip+1}),\ \textit{pour } i < \frac{e}{p-1}; \\ 1 + \mu^p\pi^{ip} + p\mu\pi^i & (\bmod\ \mathfrak{p}_\mathfrak{p}^{ip+1}),\ \textit{pour } i = \frac{e}{p-1}; \\ 1 + \mu\pi^i & (\bmod\ \mathfrak{p}_\mathfrak{p}^{i+e+1}),\ \textit{pour } i > \frac{e}{p-1}. \end{cases}$$

Preuve : C'est clair. □

Conséquence : Il résulte de la proposition que la $\mathfrak{p}$-valuation de $x^p - 1$ est connue à partir de celle de $x - 1$, sauf dans le cas spécial où l'on a $i = \frac{e}{p-1}$ et $\mu^p\pi^{ip} + p\mu\pi^i \in \mathfrak{p}_\mathfrak{p}^{ip+1}$.

Pour étudier cette dernière condition, écrivons :

$$-p = \varepsilon\pi^e.$$

Nous obtenons (puisque ip vaut $e + i$) : $\mu^p\pi^{ip} + p\mu\pi^i = (\mu^p - \varepsilon\mu)\pi^{ip}$.

Théorème & Définition 4. *Soient $K_\mathfrak{p}$ un corps local, π un uniformisante, $e = v_\mathfrak{p}(p)$ l'indice de ramification absolu, et $\varepsilon = -p/\pi^e$.*

On dit que $K_\mathfrak{p}$ est régulier, lorsque l'une des conditions suivantes est vérifiée :

(i) ou bien $\frac{e}{p-1}$ n'est pas entier ;

(ii) ou bien il est entier, mais l'équation $\mu^p \equiv \varepsilon\mu (\bmod\ \mathfrak{p}_\mathfrak{p})$ n'a pas de solution dans $U_\mathfrak{p}$ ce qui a lieu si et seulement si $K_\mathfrak{p}$ ne contient pas de racine primitive p-ième de l'unité.

Preuve : Supposons $K_\mathfrak{p}$ irrégulier. Dans ce cas, la condition *(i)* affirme que π^e est une puissance $(p-1)$-ième dans $A_\mathfrak{p}$; et via le lemme de Hensel, la condition *(ii)* nous dit que ε en est une autre. Ainsi $-p = \varepsilon\pi^e$ est alors une puissance $(p-1)$-ième dans $K_\mathfrak{p}$, et il suit $K_\mathfrak{p} \supset \mathbb{Q}_p[\sqrt[p-1]{-p}]$.

Inversement, si $K_\mathfrak{p}$ contient $\sqrt[p-1]{-p}$, son indice de ramification e est un multiple de celui $(p-1)$ de $\mathbb{Q}_p[\sqrt[p-1]{-p}]$, et $-p$ donc ε est bien une puissance $(p-1)$-ième dans $A_\mathfrak{p}$.

En résumé, tout revient donc à vérifier que $\mathbb{Q}_p[\sqrt[p-1]{-p}]$ n'est autre que le corps cyclotomique $\mathbb{Q}_p[\zeta]$ engendre sur $\mathbb{Q}_p$ par une racine primitive p-ième de l'unité ζ, c'est à dire, compte tenu de l'égalité de degrés, que $\mathbb{Q}_p[\zeta]$ est irrégulier. Or :

— C'est clair pour $p = 2$.

— Et pour $p > 2$, on a d'un côté $e = p - 1$, puisque $\pi = \zeta - 1$ satisfait une équation d'Eisenstein de degré $p - 1$, et d'un autre côté :

$$0 = \frac{1-\zeta^p}{1-\zeta} = \frac{1-(\pi+1)^p}{-\pi} = p + \frac{p^2}{\pi}(\dots\ ) + \pi^{p-1}, \quad \text{d'où} \quad \frac{-p}{\pi^{p-1}} \equiv 1 (\bmod \mathfrak{p}_\mathfrak{p}),$$

ce qui donne le résultat attendu, puisque les unités principales sont trivialement des puissances $(p-1)$-ièmes.

□

Nous sommes dès lors en mesure d'expliciter une base du groupe $U_\mathfrak{p}^1$ dans le cas régulier :

Théorème 13. *Soit $K_\mathfrak{p}$ un corps local régulier, de degré d'inertie f et d'indice de ramification e. Faisons choix d'une uniformisante π, et d'un relèvement $(\zeta_1, \dots, \zeta_f)$ dans $\mu_\mathfrak{p}^0 = \mu_\mathfrak{p}$ d'une $\mathbb{F}_p$-base du corps résiduel $A_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \simeq \mathbb{F}_{p^f}$. Alors les ef éléments :*

$$\eta_{ij} = 1 + \zeta_j \pi^i,\ j = 1, \dots, f;\ 1 \leqslant i \leqslant \frac{pe}{p-1}\ \&\ i \not\equiv 0 (\bmod p),$$

constituent une $\mathbb{Z}_p$-base du module multiplicatif $U_\mathfrak{p}^1$.

Preuve : Par construction, les η_{ij} pour i fixe et j variable constituent un système générateur de $U_\mathfrak{p}^i$ modulo $U_\mathfrak{p}^{i+1}$, disons un système générateur de niveau i. Maintenant, lorsque i vaut

$$1, 2, \dots, \left[\frac{e}{p-1}\right], x, x+1, \dots, x+e-1,$$

succesivement, les η_{ij}^p forment un système générateur de niveau

$$p, 2p, \dots, \left[\frac{e}{p-1}\right] p, x+e, x+e+1, \dots, x+2e-1.$$

D'après le lemme de Nakayamma, nous obtenons donc un système générateur de $U_\mathfrak{p}^1$, en prenant les seuls η_{ij} pour $i = 1, 2, \dots, x+e+1 = \left[\frac{e}{p-1}\right] + e = \left[\frac{pe}{p-1}\right]$, et en excluant les $i \equiv 0 (\bmod p)$. Au total ef éléments, comme attendu. □

2.4 Extensions Cyclotomiques de Corps Locaux

2.4.1 Cas des extensions non ramifiées

Soit $K_\mathfrak{p}$ un corps local (extension finie de $\mathbb{Q}_p$), $A_\mathfrak{p} = \{x \in K_\mathfrak{p} \,|\, |x| \leqslant 1\}$ son anneau d'entiers, $\mathfrak{p} = \{x \in K_\mathfrak{p} \,|\, |x| < 1\}$ l'idéal maximal de $A_\mathfrak{p}$, et π un uniformisante. Écrivons $F_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}$ le corps résiduel associé (qui est de la forme $\mathbb{F}_q$ avec $q = N\mathfrak{p}$). Nous avons vu (à l'aide du lemme de Hensel (4)) qu'un système de représentants des éléments de $F_\mathfrak{p}^\times$ est donné par le groupe $\mu_\mathfrak{p}^0$ des racines de l'unité d'ordre étranger à p, qui est cyclique de cardinal $N\mathfrak{p} - 1 = q - 1$.

Proposition 12. *L'ensemble $R_\mathfrak{p} = \mu_\mathfrak{p}^0 \cup \{0\}$ est un système de représentants dans $A_\mathfrak{p}$ des éléments de $F_\mathfrak{p}$. En particulier tout élément de $K_\mathfrak{p}$ s'écrit de façon unique comme série de Laurent*

$$K_\mathfrak{p} = R_\mathfrak{p}((\pi)) \text{ en l'uniformisante } \pi \text{ à coefficients dans } R_\mathfrak{p}.$$

L'anneau $A_\mathfrak{p}$ est l'ensemble $R_\mathfrak{p}[[\mathfrak{p}]]$ des valeurs en π des séries formelles à coefficients dans $R_\mathfrak{p}$.

Preuve : Ce n'est rien d'autre que le lemme de représentation (2). □

Théorème 14. *Soit* $\mathsf{L}_\mathfrak{P}$ *une extension de degré fini non ramifié sur* $\mathsf{K}_\mathfrak{p}$. *Alors* $\mathsf{L}_\mathfrak{P}$ *est de la forme* $\mathsf{L}_\mathfrak{P} = \mathsf{K}_\mathfrak{p}[\zeta]$, *où* ζ *est une racine primitive* $(N\mathfrak{P}-1)$*-ième de l'unité dans* $\overline{\mathbb{Q}}_\mathfrak{p}$.

Inversement, si $\mathfrak{n}$ *est un entier non multiple de* $\mathfrak{p}$, *l'extension cyclotomique* $\mathsf{L}_\mathfrak{P} = \mathsf{K}_\mathfrak{p}[\zeta_\mathfrak{n}]$ *engendré sur* $\mathsf{K}_\mathfrak{p}$ *par les racines* $\mathfrak{n}$*-ièmes de l'unité est un extension non ramifiée de* $\mathsf{K}_\mathfrak{p}$ *qui a pour degré l'ordre* $\mathfrak{d}$ *de* $\mathfrak{q} = N\mathfrak{p}$ *modulo* $\mathfrak{n}$, *et dont le groupe de Galois* $\mathrm{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p})$ *est cyclique, engendré par l'automorphisme de Frobenius :* $\sigma_\mathfrak{q} \,|\, \zeta_\mathfrak{n} \to \zeta_\mathfrak{q}^\mathfrak{q}$.

Preuve : Supposons d'abord $\mathsf{L}_\mathfrak{P}$ non ramifiée de degré $\mathfrak{d}$ sur $\mathsf{K}_\mathfrak{p}$. Dans ce cas $\mu^0_\mathfrak{P}$ est d'ordre $N\mathfrak{P}-1 = \mathfrak{q}^\mathfrak{d}-1$, et si ζ est une racine primitive $(N\mathfrak{P}-1)$-ième de l'unité, le choix d'une même uniformisante π dans $\mathsf{L}_\mathfrak{P}$ comme pour $\mathsf{K}_\mathfrak{p}$ montre que tout élément de $\mathsf{L}_\mathfrak{P}$ est une série de Laurent en π à coefficients dans $\mu^0_\mathfrak{P} \cup \{0\}$ donc un polynôme en ζ à coefficients dans Kp.

Inversement, si l'on a $\mathsf{L}_\mathfrak{P} = \mathsf{K}_\mathfrak{p}[\zeta]$, pour une racine primitive $\mathfrak{n}$-ième de l'unité ζ avec $\mathfrak{p} \nmid \mathfrak{n}$, l'extension $\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}$ est galoisienne (comme corps des racines du polynôme séparable $\mathrm{x}^\mathfrak{n}-1$), et l'action de $\mathtt{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{Kp})$ est déterminée par sa restriction à $\mu^0_\mathfrak{P}$, de sorte que le morphisme naturel de $\mathrm{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p})$ dans $\mathrm{Gal}(\mathsf{F}_\mathfrak{P}/\mathsf{F}_\mathfrak{p})$ est injectif, donc bijectif (puisque l'ordre $\mathfrak{d} = \mathfrak{e}\mathfrak{f}$ du premier est un multiple de celui $\mathfrak{f}$ du second). En particulier, $\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}$ est donc non ramifiée et $\mathrm{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}) \simeq \mathrm{Gal}(\mathsf{F}_\mathfrak{P}/\mathsf{F}_\mathfrak{p})$ est cyclique, engendré par l'automorphisme de Frobenius. □

Corollaire 9. *Soit* $\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}$ *une extension non ramifiée de corps locaux, et* $\mathsf{F}_\mathfrak{P}/\mathsf{F}_\mathfrak{p}$ *l'extension résiduelle correspondante. Notons* $\mathsf{G} = \mathrm{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{Kp}) \simeq \mathrm{Gal}(\mathsf{F}_\mathfrak{P}/\mathsf{F}_\mathfrak{p})$ *son groupe de Galois. Alors toute base normale* $\bar\zeta$ *de* $\mathsf{F}_\mathfrak{P}$ *sur* $\mathsf{F}_\mathfrak{p}$ *se relève dans l'anneau des entiers* $\mathsf{B}_\mathfrak{P}$ *de* $\mathsf{L}_\mathfrak{P}$ *en une base normale* ζ *de* $\mathsf{B}_\mathfrak{P}$ *sur* $\mathsf{A}_\mathfrak{p}$, *de sorte que l'on a :*

$$\mathsf{B}_\mathfrak{P} = \mathsf{A}_\mathfrak{p}[\mathsf{G}] \cdot \zeta.$$

Preuve : Considérons, en effet, le module quotient $\mathsf{B}_\mathfrak{P}/\mathsf{A}_\mathfrak{p}[\mathsf{G}]\cdot\zeta = \mathsf{M}$. Par hypothèse, nous avons $\mathsf{M}/\pi\mathsf{M} = 0$, et le lemme de Nakayama (6) nous donne donc $\mathsf{M} = 0$, comme annoncé. □

Corollaire 10. *Sous les mêmes hypothèses l'application Trace* $\mathrm{Tr}_{\mathsf{L}_\mathfrak{P}/\mathsf{Kp}}$ *envoie* $\mathsf{B}_\mathfrak{P}$ *sur* $\mathsf{A}_\mathfrak{p}$.

Preuve : Dans l'isomorphisme $\mathsf{B}_\mathfrak{P} \simeq \mathsf{A}_\mathfrak{p}[\mathsf{G}]$, les points fixes de G s'identifient en effet à l'image de la trace : $\sum \mathfrak{a}_\sigma\sigma$ fixe par $\mathsf{G} \Leftrightarrow \forall\,\tau \in \mathsf{G}\ (\tau-1)\sum \mathfrak{a}_\sigma\sigma = \sum(\mathfrak{a}_{\sigma/\tau} - \mathfrak{a}_\sigma)\sigma = 0 \Leftrightarrow \mathfrak{a}_\sigma$ indépendant de σ. □

Théorème 15. *Dans une extension finie* $\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}$ *non ramifiéede corps locaux, l'application norme* $N_{\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p}}$ *envoi* $\mathsf{U}_\mathfrak{P}$ *sur* $\mathsf{U}_\mathfrak{p}$, *et* $\mathsf{L}^\times_\mathfrak{P} = \mathsf{U}_\mathfrak{P} \cdot \pi^\mathbb{Z}$ *sur le sous-groupe* $\mathsf{U}_\mathfrak{p}\pi^{\mathfrak{f}\mathbb{Z}}$ *de* $\mathsf{K}^\times_\mathfrak{p}$.

En particulier, l'application $\omega \,|\, \pi \to \sigma_\mathfrak{q}$ *induit un isomorphisme* $\mathsf{K}^\times_\mathfrak{p} / N(\mathsf{L}^\times_\mathfrak{P}) \simeq \mathrm{Gal}(\mathsf{L}_\mathfrak{P}/\mathsf{K}_\mathfrak{p})$.

Le point essentiel est la surjectivité de la norme restreinte aux unités. Pour l'établir nous allons utiliser le :

Lemme 7 (Lemme de Herbrand)**.** *Soient* α *et* β *deux endomorphismes d'un* $\mathbb{Z}$*-module* M *tels que* $\mathrm{Im}\,\alpha$ *soit d'indice fini dans* $\ker\beta$ *et* $\mathrm{Im}\,\beta$ *dans* $\ker\alpha$. *Alors, pour tout sous-module* M' *de* M *stable par* α *et* β, *les mêmes propriétés sont vraies pour les restrictions* α' *et* β' *de* α *et* β, *et l'on a*

$$\frac{(\ker\alpha' : \mathrm{Im}\,\beta')}{(\ker\beta' : \mathrm{Im}\,\alpha')} = \frac{(\ker\alpha : \mathrm{Im}\,\beta)}{(\ker\beta : \mathrm{Im}\,\alpha)}.$$

Preuve : Les isomorphismes canoniques

$$\mathsf{M}/\mathsf{M}' + \ker\alpha \simeq \mathrm{Im}\,\alpha/\,\mathrm{Im}\,\alpha' \qquad \text{et} \qquad \mathsf{M}' + \ker\alpha/\mathsf{M}' \simeq \ker\alpha/\ker\alpha'$$

permettent d'écrire l'indice fini $(\mathsf{M} : \mathsf{M}')$ come produit de deux facteurs :

$$(\mathsf{M} : \mathsf{M}') = (\mathsf{M} : \mathsf{M}' + \ker\alpha)(\mathsf{M}' + \ker\alpha : \mathsf{M}') = (\mathrm{Im}\,\alpha : \mathrm{Im}\,\alpha')(\ker\alpha : \ker\alpha').$$

D'où le résultat, en écrivant de façon semblable :

$$(\mathsf{M} : \mathsf{M}') = (\mathrm{Im}\,\beta : \mathrm{Im}\,\beta')(\ker\beta : \ker\beta').$$

□

Appliquons maintenant le lemme de Herbrand en prenant $M = U_{\mathfrak{P}}$ pour $\delta = 1-\sigma$ et $\nu = 1+\sigma+\ldots+\sigma^{d-1}$, d'où σ est un générateur du groupe cyclique $G = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

— d'un côté, nous avons $\ker\delta = U_{\mathfrak{p}}$ et $\mathrm{Im}\,\nu = N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}})$ est bien d'indice fini dans $U_{\mathfrak{p}}$ puisqu'il contient en particulier $(U_{\mathfrak{p}})^{\nu} = (U_{\mathfrak{p}})^{d}$.

— d'un autre côté, nous allons voir que $\ker\nu$ coïncide avec $\mathrm{Im}\,\delta$. Nous avons, en effet :

Lemme 8 (Théorème 90 de Hilbert)**.** *Dans une extension cyclique* L/K*, tout élément de norme* 1 *est de la forme* b^{σ}/b *pour un* $b \in L^{\times}$*, si* σ *est un générateur quelconque de* $G = \mathrm{Gal}(L/K)$*.*

Preuve : Soit $a \in L^{\times}$ de norme 1. D'après le lemme d'indépendance de Dedekind, l'élément

$$1 + a\sigma + a^{1+\sigma}\sigma^2 + \ldots + a^{1+\sigma+\sigma^2+\ldots+\sigma^{d-2}}\sigma^{d-1}$$

de $\mathcal{L}_K(E)$ n'est pas identiquement nul, ce qui revient à dire qu'il existe un $\theta \in L$ pour lequel la quantité

$$\rho = \theta + a\theta^{\sigma} + a^{1+\sigma}\theta^{\sigma^2} + \ldots + a^{1+\sigma+\sigma^2+\ldots+\sigma^{d-2}}\theta^{\sigma^{d-1}}$$

n'est pas nulle. De la relation $a^{\nu} = 1$, nous tirons $a\rho^{\sigma} = \rho$, ce qui montre donc que $b = 1/\rho$ convient. □

Preuve du théorème : D'après ce qui précède, la quantité $(U_{\mathfrak{p}} : N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}))$ est le quotient de Herbrand de $U_{\mathfrak{P}}$ associé aux endomorphismes δ et ν. Le lemme de Herbrand (7) permet de le calculer en remplaçant $U_{\mathfrak{P}}$ par un sous-module d'indice fini, par exemple

$$U_{\mathfrak{P}}^{\kappa} \simeq \mathfrak{P}^{\kappa} \simeq B_{\mathfrak{P}} \simeq A_{\mathfrak{p}}[G]$$

pour lequel nous avons trivialement $\ker\delta = \mathrm{Im}\,\nu$ et $\ker\nu = \mathrm{Im}\,\delta$. □

Scolie. *On note* $\mathbb{Q}_p^{nr}$ *la sous-extension maximale de* $\overline{\mathbb{Q}}_p$ *qui est non ramifiée sur* $\mathbb{Q}_p$*. C'est donc l'extension cyclotomique engendré sur* $\mathbb{Q}_p$ *par les racines de l'unité d'ordre étranger à p.*

Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) \simeq \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ *est le groupe procyclique isomorphe à* $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/d\mathbb{Z}$ *engendré topologiquement par l'automorphisme de Frobenius* σ_p*.*

Preuve : C'est immédiat, par passage à la limite depuis le théorème 14. □

Remarque:

(i) La sous -extension macimale de $\overline{\mathbb{Q}}_p$ qui est non ramifiée sur $K_{\mathfrak{p}}$ est la composée $K_{\mathfrak{p}}^{nr} = K_{\mathfrak{p}}\mathbb{Q}_p^{nr}$. C'est une extension procyclique de $K_{\mathfrak{p}}$ et son groupe de Galois est engendré topologiquement par le Frobenius σ_q où $q = N\mathfrak{p}$.

(ii) Toute extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ de corps locaux admet une sous-extension maximale qui est non ramifiée : c'est $K_{\mathfrak{p}}^{ab} \cap L_{\mathfrak{P}}/K_{\mathfrak{p}}$, et l'on a $K_{\mathfrak{p}}^{ab} \cap L_{\mathfrak{P}} = K_{\mathfrak{p}}[\mu_{\mathfrak{P}}^0]$.

2.4.2 Extensions abéliennes modérément ramifiées

Définition 5. On dit qu'une extension (finie) $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ de corps locaux est modérément ramifiée lorsque la caractéristique résiduelle p ne divise pas l'indice de ramification $e(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

Théorème 16. *Soit* $L_{\mathfrak{P}}$ *une extension abélienne, modérément ramifiée d'un corps local* $K_{\mathfrak{p}}$*, et* $K'_{\mathfrak{p}} = K_{\mathfrak{p}}[\mu_{\mathfrak{P}}^0]$ *sa sous-extension maximale non ramifiée. Alors,* $L_{\mathfrak{P}}$ *est de la forme*

$$L_{\mathfrak{P}} = K'_{\mathfrak{P}}[\sqrt[e]{\zeta\pi}], \text{ pour un } \zeta \in \mu_{\mathfrak{P}}^0 \text{ et une uniformisante } \pi \in K_{\mathfrak{p}}.$$

Et le groupe d'inertie $\mathrm{In}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Gal}(L_{\mathfrak{P}}/K'_{\mathfrak{P}})$ *est cyclique d'ordre* e *divisant* $(N\mathfrak{p}-1)$*.*

Preuve : Partons d'une uniformisante ρ de $L_{\mathfrak{P}}$. Si π est une uniformisante de $K_{\mathfrak{p}}$, nous avons (par définition de l'indice de ramification e) : $\rho^e = \mu\pi$ pour un $\mu = \zeta\nu \in U_{\mathfrak{P}} = \mu^0_{\mathfrak{P}} U^1_{\mathfrak{P}}$.

Maintenant, $U^1_{\mathfrak{P}}$ est un $\mathbb{Z}_p$-module et e est supposé inversible dans $\mathbb{Z}_p$. Nous pouvons donc écrire $\nu = \nu'^e$ et, finalement, en remplaçant ρ par ρ/ν' :

$$\rho^e = \zeta\pi, \text{ comme attendu.}$$

De l'inclusion résultante $K_{\mathfrak{p}}[\sqrt[e]{\pi}] \subset L^{nr}_{\mathfrak{P}}$, nous concluons que $K_{\mathfrak{p}}[\sqrt[e]{\pi}]$ est donc également une extension abélienne de $K_{\mathfrak{p}}$, ce qui implique qu'elle contienne les racines e-ièmes de l'unité :

En effet, le polynôme $X^e - \pi$ est un polynôme d'Einsenstein, donc irréductible ; les conjugués de $\sqrt[e]{\pi}$ sont donc les $\zeta\sqrt[e]{\pi}$ pour $\zeta^e = 1$, et la ramification étant totale nous avons donc $\zeta \in K_{\mathfrak{p}}$. Il vient ainsi $\zeta \in \mu^0_{\mathfrak{p}}$, i.e. $e|(N\mathfrak{p} - 1)$.

Ce point acquis, l'application $\sigma \mapsto \rho^{\sigma-1}$ est alors un morphisme injectif de $In(L_{\mathfrak{P}}/K\mathfrak{p})$ (i.e. de $Gal(L_{\mathfrak{P}}/K'_{\mathfrak{P}})$) dans $\mu^0_{\mathfrak{p}}$. □

Corollaire 11. *Sous les hypothèses du théorème, si de plus $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est totalement ramifiée, elle est de la forme $K_{\mathfrak{p}}[\sqrt[e]{\pi}]/K_{\mathfrak{p}}$ pour une uniformisante π.*

Corollaire 12. *Toute extension abélienne modérément ramifiée de $\mathbb{Q}_p$ est cyclotomique.*

Preuve : Soit $K_{\mathfrak{p}}$ une telle extension. L'extension composée $K_{\mathfrak{p}}[\zeta_p]$ de $K_{\mathfrak{p}}$ et $\mathbb{Q}_p[\sqrt[p-1]{-p}]$ est encore abélienne et modérément ramifiée : plus précisément, elle est non ramifiée sur $\mathbb{Q}_p[\zeta_p]$ (dont l'indice de ramification $e = p - 1$ est maximal) donc cyclotomique, de la forme $\mathbb{Q}_p[\zeta_p][\zeta_n] = \mathbb{Q}_p[\zeta_{np}]$, pour un n non multiple de p. □

Intéressons nous plus particulièrement au corps cyclotomique $K_{\mathfrak{p}} = \mathbb{Q}_p[\zeta_p]$. Si π désigne l'uniformisante $\sqrt[p-1]{-p}$, et $R_{\mathfrak{p}} = \mu^0_{\mathfrak{p}} \cup \{0\}$, le lemme de représentation nous permet d'écrire l'anneau des entiers $A_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$ sous la forme

$$A_{\mathfrak{p}} = R_{\mathfrak{p}}[[\pi]] = \mathbb{Z}_p[\pi] = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p \pi^i.$$

Notons Δ le groupe de Galois $Gal(K_{\mathfrak{p}}/\mathbb{Q}_p)$, qui est cyclique d'ordre $p - 1$, et ω le caractère cyclotomique, c'st à dire l'homomorphisme injectif de Δ dans $\mu^0_{\mathfrak{p}}$ qui est défini par :

$$\pi^{\sigma-1} = \omega(\sigma), \quad \forall \sigma \in \Delta.$$

Pour voir comment ω agit concrétement, écrivons $\pi = \mu(\zeta_p - 1)$ avec $\mu \in U_{\mathfrak{P}}$. Si σ_a est l'élément de $Gal(K_{\mathfrak{p}}/\mathbb{Q}_p)$ qui est caractérisé par $\zeta_p \mapsto \zeta_p^a$ (pour un $a \in \{0, 1, \ldots, p-1\}$), il vient :

$$\omega(\sigma_a) = \pi^{\sigma_a - 1} = \mu^{\sigma_a - 1}(\zeta_p - 1)^{\sigma_a - 1} = \mu^{\sigma_a - 1}\frac{\zeta_p^a - 1}{\zeta_p - 1} = \mu^{\sigma_a - 1}(1 + \zeta_p + \ldots + \zeta_p^{a-1})$$

c'est à dire :

$$\omega(\sigma_a) \equiv a (\bmod\ \mathfrak{p}), \text{ puisque } \Delta \text{ agit trivialement sur } \mu^0_{\mathfrak{p}} = \mu^0_p.$$

En d'autres termes, ω est induit par le caractère de Teichmüller $a \mapsto \frac{a}{\langle a \rangle}$ de $\mathbb{Z}_p^\times$ dans $\mu^0_{\mathfrak{p}}$.

La décomposition ainsi obtenue $A_{\mathfrak{p}} = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p \pi^i$ de l'anneau $A_{\mathfrak{p}}$ en somme directe de $\mathbb{Z}_p[\Delta]$-modules isomorphes à $\mathbb{Z}_p$ correspond exactement à celle semi-locale de l'algèbre de Galois :

$$\mathbb{Z}_p[\Delta] \simeq \mathbb{Z}_p[X]/(X^{p-1} - 1) = \mathbb{Z}_p[X]/(\prod_{\zeta \in \mu^0_{\mathfrak{p}}} (X - \zeta)) \simeq \prod_{\zeta \in \mu^0_{\mathfrak{p}}} \mathbb{Z}_p[X]/(X - \zeta_p).$$

Plus précisément, à chaque caractère $\chi = \omega^i$ de Δ à valeurs dans $\mu^0_{\mathfrak{p}}$, est associé un idempotent primitif

$$e_\chi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \chi(\sigma^{-1})\sigma$$

de l'algèbre $\mathbb{Z}_p[\Delta]$, caractérisé par $\sigma \cdot e_\chi = \chi(\sigma)e_\chi$, de sorte que l'on a :

$$\mathbb{Z}_p[\Delta] = \bigoplus_{i=0}^{p-1} \mathbb{Z}_p[\Delta]e_{\omega^i} = \bigoplus_{i=0}^{p-1} \mathbb{Z}_p e_{\omega^i},$$

et :

$$A_\mathfrak{p} = \bigoplus_{i=0}^{p-1} \mathbb{Z}_p[\Delta]\pi^i = \bigoplus_{i=0}^{p-1} \mathbb{Z}_p \pi^i$$

avec $e_{\omega^i} \cdot \pi^i = \delta_{ij}\pi^j$ (δ_{ij} symbole de Kronecker). En particulier la somme $\sum_{i=0}^{p-1} \pi^i$ est une $\mathbb{Z}_p[\Delta]$-base de $A_\mathfrak{p}$.

Théorème 17. *L'anneau des entiers $A_\mathfrak{p}$ du corps cyclotomique $K_\mathfrak{p} = \mathbb{Q}_p[\sqrt[p-1]{-p}]$ est libre sur l'algèbre de Galois $\mathbb{Z}_p[\Delta] = \mathbb{Z}_p[\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)]$, somme directe des $(p-1)$ sous-modules isotypiques de caractère ω^i $(i = 0, \dots, p-1)$ $\mathbb{Z}_p\pi^i$.*

Il en résulte que le quotient $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$ est lui-même un $\mathbb{F}_p[\Delta]$-module de caractère $\chi_{\mathrm{reg}}+1+\omega = \sum_{i=0}^{p-2} \omega^i + 1 + \omega$, dès que p est différent de 2.

Preuve : Partons de la factorisation canonique : $K_\mathfrak{p}^\times = \mu_p^0 U_\mathfrak{p}^1 \pi^\mathbb{Z}$. Nous avons ici

$$U_\mathfrak{p}^1 = \mu_\mathfrak{p}^1 \cdot U_\mathfrak{p}^2 \text{ (puisque } \mu_\mathfrak{p}^1 \text{ est le sous-groupe de torsion de } U_\mathfrak{p}^1)$$

et $U_\mathfrak{p}^2$ est un $\mathbb{Z}_p[\Delta]$-module isomorphe à $\mathfrak{p}^2$ (via le logarithme), donc de caractère $\omega^2\chi_{\mathrm{reg}} = \chi_{\mathrm{reg}}$. Il suit :

$$K_\mathfrak{p}/K_\mathfrak{p}^{\times p} \simeq \mu_\mathfrak{p}^1 \cdot U_\mathfrak{p}^2/(U_\mathfrak{p}^2)^p \cdot \pi^{\mathbb{F}_p} \simeq \mathbb{F}_p e_\omega \oplus \mathbb{F}_p[\Delta] \oplus \mathbb{F}_p$$

comme attendu. □

Corollaire 13. *Soit $\widetilde{K}^\mathfrak{P}$ la composée des p-extensions cycliques de degré p du corps cyclotomique $K_\mathfrak{p} = \mathbb{Q}_p[\zeta_p]$. Alors le radical $\mathrm{Rad}(\widetilde{K}^\mathfrak{P}/K_\mathfrak{p})$ es un $\mathbb{F}_p[\Delta]$-module de caractère $\chi_{\mathrm{reg}} + 1 + \omega$. Et le groupe de Galois $\mathrm{Gal}(\widetilde{K}^\mathfrak{P}/K_\mathfrak{p})$ est un $\mathbb{F}_p[\Delta]$-module de caractère $\chi_{\mathrm{reg}} + \omega + 1$.*

Pour $p \neq 2$, $\mathrm{Gal}(\widetilde{K}^\mathfrak{P}/K_\mathfrak{p})$ contient deux fois la représentation unité, de sorte que la composée avec $K_\mathfrak{p}$ des p-extension cycliques de degrée p sur $\mathbb{Q}_p$ est l'extension de degré p^2 engendrée par $\zeta_{p^{2(p^p-1)}}$.

Preuve : Puisque $K_\mathfrak{p}$ contient les racines p-ièmes de l'unité, toute extension cyclique $L_\mathfrak{P}$ de $K_\mathfrak{p}$ est de la forme $K_\mathfrak{p}[\sqrt[p]{x}]$ pour un x de $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$. En effet, comme ζ_p est dans le noyau de la norme, le théorème 90 de Hilbert (8) permet d'écrire $\zeta_p = \theta^{\sigma-1}$ pour $\theta \in L_\mathfrak{P}^\times$ qui vérifie bien $\theta^p \in K_\mathfrak{p}^\times$. Comme l'on a, par ailleurs

$$K_\mathfrak{p}[\sqrt[p]{x}] = K_\mathfrak{p}[\sqrt[p]{y}] \quad \Leftrightarrow \quad \exists\, i \in \{0, \dots, p-1\} \mid \sqrt[p]{y}/\sqrt[p]{x^i} \in K_\mathfrak{p}^\times,$$

il en résulte que les p-extensions cycliques élémentaires de $K_\mathfrak{p}$ sont en bijection avec les $\mathbb{F}_p$-droites de $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$, et, plus généralement, que les p-extensions abéliennes $L_\mathfrak{P}$ de $K_\mathfrak{p}$ sont en bijection avec les $\mathbb{F}_p$-sous-espaces de $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$ via la correspondance de Kummer :

$$L_\mathfrak{P} \to \mathrm{Rad}(L_\mathfrak{P}/K_\mathfrak{p}) = \{xK_\mathfrak{p}^{\times p} \in K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p} \mid x \in L_\mathfrak{P}^{\times p}\}.$$

En particulier le radical associée à la p-extension abélienne élémentaire maximale $\widetilde{K}_\mathfrak{P}$ est bien $\mathrm{Rad}(\widetilde{K}_\mathfrak{P}/K_\mathfrak{p}) = K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times p}$.Cela étant, l'application bilinéaire non dégénérée

$$\begin{array}{rcl} \mathrm{Gal}(\widetilde{K}_\mathfrak{P}/K_\mathfrak{p}) \times \mathrm{Rad}(\widetilde{K}_\mathfrak{P}/K_\mathfrak{p}) & \to & \mu_\mathfrak{p}^1 \\ (\sigma, x) & \longmapsto & (\sqrt[p]{x})^{\sigma-1} \end{array}$$

identifie $\mathrm{Gal}(\widetilde{K}_{\mathfrak{P}}/K_{\mathfrak{p}})$ au dual de Kummer $\mathrm{Hom}(\mathrm{Rad}(\widetilde{K}_{\mathfrak{P}}/K\mathfrak{p}), \mu_{\mathfrak{p}}^1) = \mathrm{Hom}(K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times p}, \mu_{\mathfrak{p}}^1)$ du groupe $K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times p}$: c'est donc un $\mathbb{F}_{\mathfrak{p}}[\Delta]$-module de caractère $\omega(\chi_{\mathrm{reg}} + 1 + \omega)^{-1} = \chi_{\mathrm{reg}} + \omega + 1$, (reflet du précédent dans l'involution du miroir).

Les $\mathfrak{p}$-extensions provenant par composition avec $K_{\mathfrak{p}}$ d'une extension abélienne de $\mathbb{Q}_{\mathfrak{p}}$ correspondent au sous-module 1-isotypique de $\mathrm{Gal}(\widetilde{K}_{\mathfrak{P}}/K_{\mathfrak{p}})$ (pour lequel Δ agit trivialement) qui est un plan vectoriel. Elles sont donc toutes contenues dans le composée $\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^2(\mathfrak{p}^p-1)}]$ de lacyclotomique $\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^2}]$ et de la non ramifiée $\mathbb{Q}_{\mathfrak{p}}[\zeta_{(\mathfrak{p}^p-1)}]$. □

2.4.3 Le théorème de Kronecker-Weber

Proposition 13. *Soient $\mathfrak{p}$ premier impair et $\mathfrak{m} \geqslant 1$. Alors le corps cyclotomique $\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{m}+1}}]$ engendré par les racines $\mathfrak{p}^{\mathfrak{m}+1}$-ièmes de l'unité est une extension cyclique totalment ramifiée de degré $\varphi(\mathfrak{p}^{\mathfrak{m}+1}) = (\mathfrak{p}-1)\mathfrak{p}^{\mathfrak{m}}$ qui admet $\zeta_{\mathfrak{p}^{\mathfrak{m}+1}} - 1$ comme uniformisante.*

Elle contient en particulier une unique sous-extension de degré $\mathfrak{p}^{\mathfrak{m}}$, que l'on note $\mathbb{Q}_{\mathfrak{p}}^{(\mathfrak{m})}$.

Preuve : Remarquons d'abord que $\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{m}+1}}]$ est un extension galoisienne de $\mathbb{Q}_{\mathfrak{p}}$ (puisque c'est le corps des racines du polynôme séparable $X^{\mathfrak{p}^{\mathfrak{m}+1}} - 1$) et qu'elle est totalment ramifiée de degré $\varphi(\mathfrak{p}^{\mathfrak{m}+1})$ puisque $\zeta_{\mathfrak{p}^{\mathfrak{m}+1}} - 1$ est racine du polynôme d'Eisenstei :

$$\Phi_{\mathfrak{p}}((X+1)^{\mathfrak{p}^{\mathfrak{m}}}) = X^{\mathfrak{p}^{\mathfrak{m}}(\mathfrak{p}-1)} + \mathfrak{p}(\cdots) + \mathfrak{p}.$$

Il en résulte que les conjugués de $\zeta_{\mathfrak{p}^{\mathfrak{m}+1}}$ sont les $\varphi(\mathfrak{p}^{\mathfrak{m}+1})$ racines primitives $\mathfrak{p}^{\mathfrak{m}+1}$-ièmes de l'unité et qu'on a :

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{m}+1}}]/\mathbb{Q}_{\mathfrak{p}}) &\simeq (\mathbb{Z}/\mathfrak{p}^{\mathfrak{m}+1}\mathbb{Z})^\times \\
&\simeq (\mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}^{\mathfrak{m}+1}\mathbb{Z}_{\mathfrak{p}})^\times \\
&\simeq U_{\mathfrak{p}}/U_{\mathfrak{p}}^{\mathfrak{m}+1} \\
&\simeq \mu_{\mathfrak{p}}^0 \times U_{\mathfrak{p}}^1/U_{\mathfrak{p}}^{\mathfrak{m}+1} \\
&\simeq \mu_{\mathfrak{p}}^0 \times \mathfrak{p}\mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}^{\mathfrak{m}+1}\mathbb{Z}_{\mathfrak{p}} \\
&\simeq C_{\mathfrak{p}-1} \times C_{\mathfrak{p}^{\mathfrak{m}}};
\end{aligned}$$

d'où le résultat annoncé. □

Corollaire 14. *Soit $K_{\mathfrak{p}}$ une $\mathfrak{p}$-extension cyclique de $\mathbb{Q}_{\mathfrak{p}}$ de degré $\mathfrak{p}^{\mathfrak{m}}$. Alors $K_{\mathfrak{p}}$ est une sous-extension du corps cyclotomique $\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{p}^{\mathfrak{m}}}-1}]\mathbb{Q}_{\mathfrak{p}}^{(\mathfrak{m})}$.*

Preuve : Sinon $K'_{\mathfrak{p}} = K_{\mathfrak{p}}\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{p}^{\mathfrak{m}}}-1}]\mathbb{Q}_{\mathfrak{p}}^{(\mathfrak{m})}$ serait une $\mathfrak{p}$-extension d'exposant $\mathfrak{p}^{\mathfrak{m}}$ et son groupe de Galois admettant

$$\mathrm{Gal}(\mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}^{\mathfrak{p}^{\mathfrak{m}}}-1}]\mathbb{Q}_{\mathfrak{p}}^{(\mathfrak{m})}) \simeq C_{\mathfrak{p}^{\mathfrak{m}}} \times C_{\mathfrak{p}^{\mathfrak{m}}}$$

comme quotient, il serait de la forme :

$$G \simeq C_{\mathfrak{p}^{\mathfrak{m}}} \times C_{\mathfrak{p}^{\mathfrak{m}}} \times C_{\mathfrak{p}^{\mathfrak{d}}} \text{ avec } \mathfrak{d} > 0.$$

Ainsi G admettrait $C_{\mathfrak{p}}^3$ comme qupotient, de sorte que $\mathbb{Q}_{\mathfrak{p}}$ posséderait 3 extensions cycliques de degré $\mathfrak{p}$ linéairement indépendantes, ce qui n'est pas. □

Théorème 18. *Pour $\mathfrak{p}$ impair, toute extension abélienne de $\mathbb{Q}_{\mathfrak{p}}$ est contenue dans un corps cyclotomique. Plus précisement l'extension abélienne maximale $\mathbb{Q}_{\mathfrak{p}}^{\mathrm{ab}}$ de $\mathbb{Q}_{\mathfrak{p}}$ est la composée directe :*

$$\mathbb{Q}_{\mathfrak{p}}^{\mathrm{ab}} = \mathbb{Q}_{\mathfrak{p}}^{\mathrm{nr}} \cdot \mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{p}}] \cdot \mathbb{Q}_{\mathfrak{p}}^{(\infty)}$$

— *de la pro-extension non ramifiée $\mathbb{Q}_{\mathfrak{p}}^{\mathrm{nr}} = \bigcup_{\mathfrak{p}\nmid\mathfrak{n}} \mathbb{Q}_{\mathfrak{p}}[\zeta_{\mathfrak{n}}]$, de groupe $\hat{\mathbb{Z}}$,*

— *de l'extension modérément ramifiée* $\mathbb{Q}_p[\zeta_p]$*, de groupe* C_{p-1}*,*
— *et de l'extension sauvagement ramifiée* $\mathbb{Q}_p^{(\infty)} = \bigcup_{n\geqslant 1} \mathbb{Q}_p^{(n)}$ *de groupe* $\mathbb{Z}_p$*.*

Preuve : D'après ce qui précède, la pro-q-extension abélienne maximale de $\mathbb{Q}_p$ est

(i) pour $q = p$, la composée de la $\mathbb{Z}_p$-extension cyclotomique $\mathbb{Q}_p^{(\infty)} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_p^{(n)}$ et de la pro-p-sous-extension de $\mathbb{Q}_p^{nr}$, laqielle a pour groupe de Galois la p-partie $\mathbb{Z}_p$ de $\hat{\mathbb{Z}}$.

(ii) pour $q \neq p$, la composée de la p-sous-extension du corps cyclotomique $\mathbb{Q}_p[\zeta_p]$ (qui a donc pour groupe de Galois la p-partie du groupe cyclique C_{p-1}) et de la pro-q-sous-extension de $\mathbb{Q}_p^{nr}$, laquelle a pour groupe de Galois la q-partie $\mathbb{Z}_q$ de $\hat{\mathbb{Z}}$.

Il vient donc comme annoncé (et pour p impair) :

$$\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \simeq \hat{\mathbb{Z}} \times \mathbb{Z}_p \times C_{p-1} = \prod^{q\neq p} \mathbb{Z}_q \times \mathbb{Z}_p^2 \times C_{p-1}.$$

□

Nota. *De la décomposition multiplicative*

$$\mathbb{Q}_p^\times \simeq \mu_p^0 \times U_p^1 \times p^{\mathbb{Z}} \simeq C_{p-1} \times \mathbb{Z}_p \times \mathbb{Z},$$

on tire, en prenant le compactifié profini :

$$\hat{\mathbb{Q}_p} = \varprojlim \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n} = C_{p-1} \times \mathbb{Z}_p \times \hat{\mathbb{Z}} \simeq \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p)$$

Cet isomorphisme est en fait valabre pour toute extension finie de $\mathbb{Q}_p$*, et constitue un cas particulier de la théorie du corps de classes local.*

Considerons maintenant le cas $p = 2$. Nous avons ici :

Proposition 14. *Le cors cyclotomique* $\mathbb{Q}_2[\zeta_{2^{m+2}}]$ *est une extension bicyclique totalement ramifiée de degré* 2^{m+1}*, composée directe de l'extension quadratique* $\mathbb{Q}_2[i]$ *et de l'extension cyclique de degré* 2^m *engendré par* $\theta_m = \zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1}$*.*

Preuve : Ecrivons ζ pour $\zeta_{2^{m+2}}$. Le critère d'Eisenstein nous montre comme plus haut que $\mathbb{Q}_2[\zeta]$ est une extension galoisienne de $\mathbb{Q}_2$, totalement ramifié, de degré 2^{m+1} et de groupe de Galois :

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_2[\zeta]/\mathbb{Q}_2) &\simeq (\mathbb{Z}/2^{m+2}\mathbb{Z})^\times \\ &= (\mathbb{Z}_2/2^{m+2}\mathbb{Z}_2)^\times \\ &= U_2^1/U_2^{m+2} \\ &\simeq \mu_2^1 \times U_2^2/U_2^{m+2} \end{aligned}$$

i.e.

$$\mathrm{Gal}(\mathbb{Q}_2[\zeta]/\mathbb{Q}_2) \simeq \{\pm 1\} \times \mathbb{Z}_2/2^m\mathbb{Z}_2.$$

Reste alors à voir que le sous-corps de $\mathbb{Q}_2[\zeta]$ fixé par la conjugaison $\zeta \mapsto \zeta^{-1}$ est $\mathbb{Q}_2[\theta]$, ce qui se fait constatant par récurrence que θ_m est de degré 2^m, puis qu'il verifie

$$\theta_m^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = \theta_m + 2.$$

□

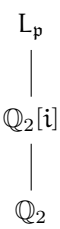
Corollaire 15. *Soit* K_p *une 2-extension cyclique de degré* 2^m *sur* $\mathbb{Q}_2$*. Alors* K_p *est une sous-extension du corps cyclotomique*

$$\mathbb{Q}_2[\zeta_{2^{2^m}-1}]\mathbb{Q}_2[\zeta_{2^{m+2}}] = \mathbb{Q}_2[\zeta_{(2^m-1)2^{m+2}}]$$

Preuve : Sinon $K_p' = K_p[\zeta_{(2^{2^m}-1)2^{m+2}}]$ seraut encore une 2-extension abélienne et son groupe de Galois un 2-groupe abélien d'exposant 2^m admettant $C_{2^m} \times C_2$ comme quotient strict. Nous aurions donc :

— soit $G \simeq C_{2^m}^2 \times C_2 \times C_{2^d}$ (avec $d \geqslant 1$), et $\mathbb{Q}_2$ aurait ainsi 15 extensions quadratiques alors que $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ est d'ordre 8.

— soit $G \simeq C_{2^m}^2 \times C_{2^d}$ (avec $d \geqslant 2$), et $\mathbb{Q}_2[i]$ serait ainsi contenu dans une extension quadratique cyclique $L_\mathfrak{p}$ de $\mathbb{Q}_2$, disons $L_\mathfrak{p} = \mathbb{Q}_2[i][\alpha]$, avec $\alpha^2 \in \mathbb{Q}_2[i]$. Nous aurions alors $\alpha^2 \notin \mathbb{Q}_2$ (sans quoi $L_\mathfrak{p}$ serait biquadratique) donc $L_\mathfrak{p} = \mathbb{Q}_2[\alpha]$. Notons $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_2) = \{1, \sigma, \sigma^2, \sigma^3\}$ et $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_2[i]) = \{1, \sigma^2\}$. De $\alpha^2 \in \mathbb{Q}_2[i]$, nous tirons $\alpha^{\sigma^2} = -\alpha$, i.e. $\alpha^{(\sigma^2-1)} = 1$ donc $\alpha^{(\sigma^2-1)(\sigma-1)} = \pm 1$, i.e. $\alpha^{\sigma-1} \in \mathbb{Q}_2[i]$. Ecrivons donc $\alpha^{\sigma-1} = u + iv$ avec u et v dans $\mathbb{Q}_2$.



Nous obtenons

$$u^2 + v^2 = (u+v)^{\sigma+1} = \alpha^{(\sigma-1)(\sigma+1)} = \alpha^{\sigma^2-1} = -1,$$

autrement dit -1 est somme de deux carrés dans $\mathbb{Q}_2$. Chassant alors les dénominateurs nous endéduisons une identité dans $\mathbb{Z}_2$ de la forme $a^2 + b^2 + c^2 = 0$ (avec a, b, c non tous pairs) mais ceci est impossible modulo $4\mathbb{Z}_2$ puisqu'un carré est congru à 0 ou 1 modulo $4\mathbb{Z}_2$.

□

Théorème 19. *L'extension abélienne maximale $\mathbb{Q}_2^{ab}$ de $\mathbb{Q}_2$ est la composée directe*

— *de la pro-extension non ramifiée $\mathbb{Q}_2^{nr}$ engendrée sur $\mathbb{Q}_2$ par les racines d'ordre impair de l'unité $\mathbb{Q}_2^{nr} = \bigcup_{2\nmid n} \mathbb{Q}_2[\zeta_n]$, de groupe de Galois associé $\hat{\mathbb{Z}}$.*

— *de l'extension quadratique $\mathbb{Q}_2[i]$ totalement ramifiée.*

— *et de la $\mathbb{Z}_\mathfrak{p}$-extension cyclotomique $\mathbb{Q}_2^{(\infty)} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_2[\theta_n]$.*

Nota. *Ici encore il vient* $\mathrm{Gal}(\mathbb{Q}_2^{ab}/\mathbb{Q}_2) \simeq C_2 \times \mathbb{Z}_2 \times \hat{\mathbb{Z}} \simeq \{\pm 1\} \times U_2^1 \times 2^{\hat{\mathbb{Z}}} = \hat{\mathbb{Q}}_2$.

Corollaire 16 (Théorème de Kronecker-Weber local)**.** *Toute extension abélienne de $\mathbb{Q}_\mathfrak{p}$ est contenue dans une extension cyclotomique.*

Application aux corps de nombres

Le passage du cas local au cas global pour le Théorème de Kronecker-Weber est immédiat si l'on sait que toute extension algébrique non triviale de $\mathbb{Q}$ se ramifie en au moins un premier (théorème de Minkovski) et au plus en un nombre fini de premiers.

Soit, en effet, K une extension abélienne de $\mathbb{Q}$. Nous savons, d'après ce qui précède, qu'elle est localement cyclotomique c'est à dire que nous avons en chaque place finie $\mathfrak{p}$:

$$K_\mathfrak{p} \sqsubset \mathbb{Q}_p[\zeta_{p^{n_p} q_p}], \text{ avec } p \nmid q_p \text{ et } n_p = 0 \text{ pour presque tout } p.$$

Posons $m = \prod_p p^{n_p}$, puis $L = K[\zeta_m]$. Pour chaque premier ramifié $\mathfrak{p}$, le groupe de Galois $G = \mathrm{Gal}(L/\mathbb{Q})$ opère transitivement sur les places $\mathfrak{p}$ au dessus de p et le sous-groupe d'isotropie $D_\mathfrak{p}$ (qui ne dépend que de p puisque G est supposé abélien) s'identifie au groupe de Galois local $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$. Son sous-groupe d'inertie $I_\mathfrak{p} = \mathrm{In}(L_\mathfrak{p}/\mathbb{Q}_p)$, d'ordre $\varphi(p^{n_p})$, fixe la sous-extension maximale de L qui est non ramifiée en $\mathfrak{p}$. Le théorème de Minkovski montre alors que G est engendré par les $I_\mathfrak{p}$ et, par suite, que son ordre est au plus

$$|G| \leqslant \prod_p |I_\mathfrak{p}| = \prod_p \varphi(p^{n_p}) = \varphi(m) = [\mathbb{Q}[\zeta_m] : \mathbb{Q}]$$

c'est à dire que l'on a $K[\zeta_m] = \mathbb{Q}[\zeta_m]$ ou encore $K \subset \mathbb{Q}[\zeta_m]$. En d'autres termes :

Théorème 20 (de Kronecker-Weber)**.** *Toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique.*

3 Séries de Dirichlet

3.1 Propriétés formelles des séries de Dirichlet

3.1.1 Algèbre des séries de Dirichlet

Définition 6. On appelle algèbre des séries de Dirichlet formelles sur un corps K (commutatif) le K-espace vectoriel des suites $(a_n)_{n\in\mathbb{N}^\times}$ d'éléments de K équipé du produit de Dirichlet défini par :

$$(a_n)_{n\in\mathbb{N}^\times} * (b_n)_{n\in\mathbb{N}^\times} = (c_n)_{n\in\mathbb{N}^\times} \text{ avec } c_n = \sum_{pq=n} a_p b_q$$

Notation. *On convient de noter* n^{-x} *la suite* $(\delta_{kn})_{k\in\mathbb{N}^\times}$ *et* $\mathrm{Dir}_K[[x]]$ *l'algèbre des séries de Dirichlet sur* K. *Un élément de* $\mathrm{Dir}[[x]]$ *s'écrit donc formellement :*

$$f(x) = \sum_{n\in\mathbb{N}^\times} a_n n^{-x}$$

et la loi multiplicative sur $\mathrm{Dir}_K[[x]]$ *se lit tout simplement :*

$$n^{-x} * m^{-x} = (nm)^{-x}.$$

En particulier, on a donc $(n^{-x})^k = (n^k)^{-x}$ *et le neutre multiplicatif est la suite* $1 = 1^{-x}$.

Théorème 21. *L'application qui à la série de Dirichlet*

$$f(x) = \sum_{p_1^{\nu_1}\cdots p_k^{\nu_k}} a_{p_1^{\nu_1}\cdots p_k^{\nu_k}} (p_1^{-x})^{\nu_1}\cdots(p_k^{-x})^{\nu_k}$$

associe la série formelle

$$\tilde{f} = \sum_{p_1^{\nu_1}\cdots p_k^{\nu_k}} a_{p_1^{\nu_1}\cdots p_k^{\nu_k}} x_{p_1}^{\nu_1}\cdots x_{p_k}^{\nu_k}$$

est un K*-isomorphisme de l'algèbre* $\mathrm{Dir}_K[[x]]$ *des séries de Dirichlet sur* K *sur l'algèbre* $K[[(x_p)_{p\in Pr}]]$ *des séries formelles à une infinité d'indéterminées (indexées par l'ensemble dénombrable* $\mathbb{P}$ *des nombres premiers dans* $\mathbb{N}$*).*

Preuve : C'est immédiat, en vertu du théorème d'Euclide et de l'expression de la loi multiplicative. □

Corollaire 17. *(i) L'anneau* $\mathrm{Dir}_K[[x]]$ *est un anneau local factoriel qui n'est pas noethérien.*
(ii) Les séries $\sum a_n n^{-x}$ *inversibles dans* $\mathrm{Dir}_K[[x]]$ *sont celles vérifiant* $a_1 \neq 0$.

Preuve : Cela résulte des propriétés bien connues des algèbres de séries formelles. En particulier l'idéal maximal $\mathfrak{M}$ de $\mathrm{Dir}_K[[x]]$ est engendré par les p^{-x} pour $p \in \mathbb{P}$. □

3.1.2 Séries de Dirichlet multiplicatives

On dit qu'une série de Dirichlet $f(x) = \sum a_n n^{-x}$ est (faiblement) multiplicative lorsque l'on a $a_{mn} = a_m a_n$ pour $m \wedge n = 1$. Dans la description précédente de $\mathrm{Dir}_K[[x]]$ comme algèbre de séries formelles à une infinité (dénombrable) d'indéterminées, les séries multiplicatives sont exactement celles à variables séparées puisque la condition de multiplicativité

$$a_{p_1\nu_1\cdots p_k\nu_k} = a_{p_1\nu_1} a_{p_2\nu_2}\cdots a_{p_k^{\nu_k}}$$

permet évidement d'écrire :

$$f(x) = \prod_{p\in\mathbb{P}} f_p(x), \text{ avec } f_p(x) = \sum_{k\in\mathbb{N}} a_{p^k} p^{-kx}.$$

Lorsque la série $f(x)$ est strictement multiplicative, i.e. lorsqu'on a $a_{p^k} = a_p^k$, il vient même :

$$f_p(x) = \sum_{k\in\mathbb{N}} a_p^k p^{-xk} = (1 - a_p p^{-x})^{-1}, \text{ i.e. } f(x) = \prod_{p\in\mathbb{P}} (1 - a_p p^{-x})^{-1}.$$

On dit alors que f admet un produit eulérien.

Exemple 4. La fonction $\zeta(x) = \sum_{n\in\mathbb{N}^\times} n^{-x}$ de Riemann est strictement multiplicative. D'après la formule d'inversion de Möbius (cf. 1.3.1), son inverse est donnée par

$$\zeta^{-1}(x) = \sum_{n\in\mathbb{N}^\times} \mu(n) n^{-x} = \prod_{p\in\mathbb{P}} (1 - p^{-x}).$$

Exemple 5. La série indicatrice d'Euler $\Phi(x) = \sum_{n\in\mathbb{N}^\times} \varphi(n) n^{-x}$ est (faiblement) multiplicative. D'après la formule sommatoire $n = \sum_{d|n} \varphi(d)$, on a :

$$\zeta(x-1) = \sum n^{1-x} = \sum n n^{-x} = \sum_n \left(\sum_{d|n} \varphi(d) 1\left(\frac{n}{d}\right) \right) n^{-x} = \Phi(x)\zeta(x).$$

Il vient ainsi :

$$\Phi(x) = \frac{\zeta(x-1)}{\zeta(x)} = \prod_{p\in\mathbb{P}} \frac{1 - p^{-x}}{1 - p^{1-x}}.$$

Exemple 6. La codérivée logarithmique de la fonction ζ définie formellement par

$$Z(x) = -\frac{\zeta'(x)}{\zeta(x)} = \left(\sum \log n n^{-x} \right) \left(\sum \mu(n) n^{-x} \right)$$

n'est pas multiplicative. Elle s'écrit :

$$Z(x) = \sum \Lambda(n) n^{-x} \text{ avec } \Lambda(n) = \begin{cases} \log n, \text{ pour } n \text{ primaire;} \\ 0, \text{ sinon.} \end{cases}$$

3.1.3 Séries L attachées à un caractère de Dirichlet

Définition 7. Supposons que K contienne les racines $\varphi(m)$-ièmes de l'unité pour un $m > 1$. Un caractère modulo m est une application multiplicative de $\mathbb{Z}$ dans $K^\times$ obtenue par relèvement d'un caractère χ de $(\mathbb{Z}/m\mathbb{Z})^\times$ à valeurs dans $K^\times$:

$$\chi(n) = \chi(\bar{n}), \text{ pour } \bar{n} \in (\mathbb{Z}/n\mathbb{Z})^\times \quad \& \quad \chi(n) = 0, \text{ pour } n \wedge m \neq 1.$$

La série de Dirichlet associée (qui dépend donc de m) est donnée par :

$$L(x,\chi) = \sum_{n\in\mathbb{N}^\times} \chi(n) n^{-x} = \sum_{n\wedge m=1} \chi(n) n^{-x} = \prod_{p\nmid m} (1 - \chi(p) p^{-x})^{-1}.$$

Proposition 15. *Pour tout $p \nmid m$ notons f_p l'ordre de p modulo m et $g_p = \frac{\varphi(n)}{f_p}$. Il vient alors :*

$$\prod_{\chi \bmod m} L(x,\chi) = \prod_{p\nmid m} (1 - p^{-f_p x})^{-g_p}.$$

En particulier, pour $\chi = 1$, il suit $L(x,1) = \zeta(x) \prod_{p|m} (1 - p^{-x})$.

Preuve : Pour chaque racine f_p-ième de l'unité ζ, il existe exactement g_p caractères χ modulo m qui vérifient $\chi(p) = \zeta$. Il vient donc :

$$\prod_{\chi \bmod m} (1-\chi(p)p^{-x})^{-1} = \prod_{\zeta \in \mu_{f_p}} (1-\zeta p^{-x})^{-g_p} = (1-p^{-f_p x})^{-g_p},$$

comme attendu. □

Nota. *L'ordre f_p s'interprète comme le degré d'inertie de p dans l'extension cyclotomique $\mathbb{Q}[\zeta_m]/\mathbb{Q}$, et g_p est donc le nombre de premiers $\mathfrak{p}$ au dessus de p. La quantité précédente est donc tout simplement $\prod_{\mathfrak{p}|p}(1-N\mathfrak{p})^{-1}$.*

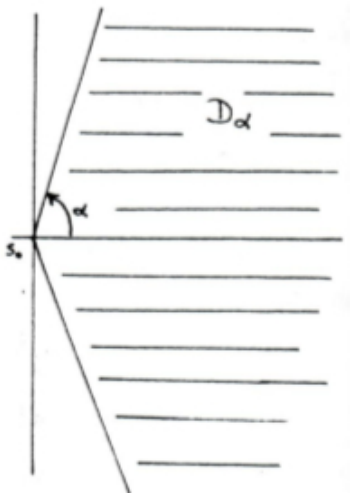
3.2 Propriétés analytiques des séries de Dirichlet

Nous allons maintenant nous intéresser au domaine de convergence des séries de Dirichlet à coefficients complexes.

3.2.1 Abscisse de convergence

Théorème 22. *Si une série de Dirichlet $f(s) = \sum_{n\geqslant 1} a_n n^{-s}$ converge en un point s_0 du plan complexe, elle converge alors uniformément (vers une fonction holomorphe) sur tot domaine $D_\alpha(s_0) = \{s \in \mathbb{C} \,|\, Re(s-s_0) \geqslant 0 \ \& \ |Arg(s-s_0)| \leqslant \alpha < \frac{\pi}{2}\}$.*

Preuve : Notons $\sigma_n = \sum_{k=1}^{n} a_k$ la suite des sommes partielles de la serie a_n, après nous être ramenés au cas $s_0 = 0$, par translation de l'indéterminée. Les hypothèses faites affirment alors la convergence de la série (a_n), i.e. celle de la suite (σ_n). Or, la règle de sommation d'Abel nous donne ici :



$$\begin{aligned}\left|\sum_{k=n}^{m} a_k k^{-s}\right| &= \left|\sum_{k=n}^{m} (\sigma_k - \sigma_{k-1})k^{-s}\right| \\ &\leqslant \left|\sum_{n}^{m-1} \sigma_k (k^{-s} - (k+1)^{-s})\right| + \left|\sigma_{n-1} n^{-s}\right| + \left|\sigma_m m^{-s}\right|.\end{aligned}$$

Dans le premier terme, les $|\sigma_k|$ sont bornés, disons par κ, et nous avons par ailleurs, posant $s = \sigma + i\tau$:

$$\begin{aligned}\left|k^{-s} - (k+1)^{-s}\right| &= \left|[u^{-s}]_k^{k+1}\right| \\ &= \left|\int_k^{k+1} s u^{-s-1} du\right| \\ &\leqslant |s| \int_k^{k+1} u^{-\sigma-1} du \\ &= \frac{|s|}{\sigma}(k^{-\sigma} - (k+1)^{-\sigma}).\end{aligned}$$

Il vient donc :

$$\begin{aligned}\left|\sum_{k=n}^{m} a_k k^{-s}\right| &\leqslant \kappa \frac{|s|}{\sigma}(n^{-\sigma} - m^{-\sigma}) + \kappa n^{-\sigma} + \kappa m^{-\sigma} \\ &\leqslant \kappa \left(\frac{|s|}{\sigma} + 2\right) n^{-\sigma},\end{aligned}$$

d'où le résultat annoncé après le critère uniforme de Cauchy. □

Corollaire 18. *La convergence pour s_0 implique la convergence pour tout s de partie réelle strictement supérieure. Il existe donc un demi-plan ouvert maximal $D_\rho = \{s \in \mathbb{C} \mid Re(s) > \rho\}$ (éventuellement vide) de convergence. La quantité réelle (ou infinie) ρ est appelée abcisse de convergence.*

Corollaire 19. *Si une série de Dirichlet formelle $f(x) = \sum a_n n^{-x}$ converge vers 0 sur un demi-plan ouvert non vide D_ρ, tous ses coefficients sont nuls.*

Preuve : Sinon, soit $a_n n^{-x}$ son monôme de plus bas degré. Il vient $a_n = \lim_{x\to\infty} n^x f(x) = 0$, une contradiction. Une série de Dirichlet est donc déterminée uniquement par la fonction holomorphe qu'elle défini dès que son demi-plan de convergence n'est pas vide. □

Corollaire 20. *Soit $f(x) = \sum a_n n^{-x}$ une série de Dirichlet, puis $\sigma_n = \sum_{k\leqslant n} a_k$. Alors :*
(i) Si les a_n sont bornés, il y a convergence absolue pour $Re(s) > 1$.
(ii) Si les σ_n sont bornés, il y a convergence simple pour $Re(s) > 0$.
(iii) Si les σ_n sont dominés par n^ρ, il y a convergence simple pour $Re(s) > \rho$.

Preuve :
(i) Provient directement de la majoration

$$\begin{aligned}\left|\sum_{n+1}^{m} a_k k^{-s}\right| &\leqslant \kappa \sum_{n+1}^{m} k^{-\sigma} \\ &\leqslant \kappa \int_n^{m-1} \mu^{-\sigma} d\mu \\ &\leqslant \frac{\kappa}{\sigma-1} n^{1-\sigma}.\end{aligned}$$

(ii) est tout simplement la démonstration du théorème.
(iii) résulte du précédent, par translation de la variable :

$$a_n n^{-s} = (a_n n^{-\rho}) n^{-(s-\rho)}.$$

□

Exemple 7. (i) La série $\zeta(s) = \sum n^{-s}$, son inverse $\zeta^{-1}(s) = \sum \mu(n) n^{-s}$ convergent absolument pour $\mathrm{Re}(s) > 1$.
(ii) LEs fonctions $L(s,\chi) = \chi(n) n^{-s}$, pour $\chi \neq 1$, convergent simplement pour $\mathrm{Re}(s) > 0$.

En effet, dans le 1er cas, les a_n sont bornés, et dans le second cas les σ_n (puisque la somme des $\chi(n)$ sur une période est toujours nulle).

3.2.2 Prolongement analytique

Théorème 23. *La fonction ζ de Riemann, définie par son développement $\sum_{n\geqslant 1} n^{-s}$ sur le demi-plan $Re(s) > 1$, admet un prolongement méromorphe sur le demi-plan $Re(s) > 0$ avec un unique pôle en $s = 1$ de résidu égal à 1.*

Preuve : Considérons la quentité

$$\zeta(s) - \frac{1}{s-1} = \sum_{n\geqslant 1} n^{-s} - \int_1^\infty \mu^{-s} d\mu = \sum_{n\geqslant 1} \int_n^{n+1} (n^{-s} - \mu^{-s}) d\mu.$$

Dans la série obtenue, le terme général $\varphi_n(s) = \int_n^{n+1} (n^{-s} - \mu^{-s}) d\mu$ se présente comme l'intégrale sur un segment de longueur 1 d'une fonction C^1 nulle à une extrémité et de la dérivée $-s\mu^{-s-1}$ majorée en module par $|s| n^{-1-\sigma}$. Il vient ainsi $|\varphi_n(s)| \leqslant |s| n^{-1-\sigma}$, ce qui montre que la série obtenue converge uniformément sur tout compact contenue dans le demi-plan ouvert $\mathrm{Re}(s) > 0$. □

Nous allons voir qu'un résultat analogue vaut pour tous les fonctions ζ_k des corps cyclotomiques :

Théorème 24. *Pour tout $m \geqslant 1$, la fonction ζ_k attachée au corps cyclotomique $K = \mathbb{Q}(\zeta_m)$ des racines m-ièmes de l'unité, definie pour $Re(s) > 1$ par la formule*

$$\zeta_K(s) = \sum_a N(a)^{-s} = \prod_p (1 - Np^{-s})^{-1},$$

admet un prolongement méromorphe sur le demi-plan $Re(s) > 0$ avec un unique pôle simple en $s = 1$.

Preuve : Partons du produit infini

$$\prod_p (1 - Np^{-s})^{-1} = \prod_p (1 - p^{-f_p s})^{-g_p} = \prod_{p|m} (1 - p^{-f_p s})^{-g_p} \prod_{\chi \bmod m} L(s, \chi)$$

qui a bien un sens pour $\mathrm{Re}(s) > 1$ puisque nous savons déjà que les $L(s, \chi)$ pour $\chi \neq 1$ convergent sur le demi-plan $\mathrm{Re}(s) > 0$ et qu'il en est de même du facteur $L(s, 1) = \zeta(s) \prod_{p|m} (1 - p^{-s})$ pour $\mathrm{Re}(s) > 1$.

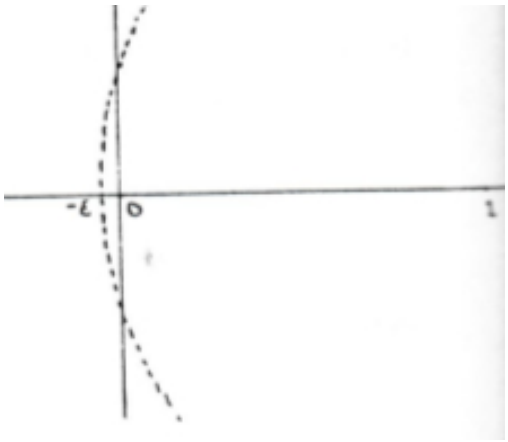
Le théorème 23 nous assure que la fonction $\zeta_K(s)$ ainsi définie est holomorphe sur le demi plan $\mathrm{Re}(s) > 1$ et admet un prolongement méromorphe pour $\mathrm{Re}(s) > 0$. Il nous reste donc à voir que $s = 1$ est encore un pôle (simple) de $\zeta_K(s)$, par exemple en montrant que $\zeta_K(\sigma)$ n'est pas borné pour $\sigma \in (\alpha, \infty)$ avec $\alpha \in (0, 1)$ convenable. Or de l'inégalité

$$\begin{aligned} (1 - p^{-f_p \sigma})^{-g_p} &= (1 + p^{-f_p \sigma} + p^{-2f_p \sigma} + \ldots)^{g_p} \\ &\geqslant 1 + p^{-\varphi(m)\sigma} + p^{-2\varphi(m)\sigma} + \ldots = (1 - p^{-\varphi(m)\sigma})^{-1}, \end{aligned}$$

nous tirons : $\zeta_K(\sigma) \geqslant \zeta(\varphi(m)\sigma)$, et cette dernière quantité diverge pour $\sigma = \frac{1}{\varphi(m)}$. Or :

Lemme 9. *Le domaine de convergence d'une série de Dirichlet à coefficients positifs est limité par une singularité réelle.*

Preuve : Il s'agit de vérifier que si $f(s) = \sum a_n n^{-s}$, convergente pour $\mathrm{Re}(s) > \rho$, est prolongeable analytiquement au voisinage de ρ, elle converge en fait pour $\mathrm{Re}(s) > \rho - \varepsilon$. Par translation éventuelle de la variable s, nous pouvons supposer $\rho = 0$. Cela étant, f est alors holomorphe sur un disque de centre 1 et de rayon, disons, $1 + \varepsilon$, donc somme sur ce disaue de sa série de Taylor :



$$f(s) = \sum_{k \in \mathbb{N}} \frac{(s-1)^k}{k!} f^{(k)}(1),$$

avec ici :

$$f^{(k)}(1) = \sum_{n \geqslant 1} (-\log n)^k a_n n^{-1}.$$

Il vient donc

$$f(-\varepsilon) = \sum_{k \in \mathbb{N}} \frac{(1+\varepsilon)^k}{k!} \sum_{n \geqslant 1} \log^k n \frac{a_n}{n}.$$

Et, puisque tous les termes de la série double convergnet sont positifs, nous pouvons renverser l'ordre de la sommation, ce qui donne

$$f(-\varepsilon) = \sum_{n \geqslant 1} \frac{a_n}{n} \left(\sum_{k \in \mathbb{N}} \frac{(1+\varepsilon)^k \log^k n}{k!} \right) = \sum_{n \geqslant 1} a_n n^{\varepsilon},$$

comme attendu. □
D'où la partie finale du théorème. □

Corollaire 21. *Pour chaque caractère non trivial χ modulo m, on a $L(1, \chi) \neq 0$.*

Preuve : Dans le cas contraire, en effet, le pôle en $s = 1$ de la fonction ζ de Riemann serait compensé par un zéro de l'une des fonctins $L(s, \chi)$ et la fonction ζ_K du corps cyclotomique $K = \mathbb{Q}(\zeta_m)$ serait holomorphe au voisinage de 1. □

3.2.3 Théorème de la progression arithmétique

Désignons par log la détermination principale du logarithme complexe, qui est définie pour $|s| < 1$ par le développement taylorien :

$$\log \frac{1}{1-s} = \sum_{k \geqslant 1} \frac{s^k}{k}.$$

Proposition 16. *La série de Dirichlet $\sum_{p \in \mathbb{P}} p^{-s}$ (où $\mathbb{P}$ est l'ensemble des nombres permiers) converge sur le demi plan $\Re(s) > 0$, et vérifie au voisinage de 1 :*

$$\sum_{p \in \mathbb{P}} p^{-s} \sim \log \frac{1}{s-1}.$$

Preuve : Nous savons déjà que la fonction ζ de Riemman s'écrit $\zeta(s) = \frac{1}{s-1} + \varphi(s)$, où φ est une fonction holomorphe sur le demi-plan $\Re(s) > 0$, donc bornée au voisinage de 1. Il suit :

$$\log \zeta(s) \sim \log \frac{1}{s-1}.$$

Par ailleurs ; le développement eulérien de ζ nous permet d'écrire pour $\Re(s) > 1$:

$$\begin{aligned}
\log \zeta(s) &= \log \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} && (1)\\
&= \sum_{p \in \mathbb{P}} \sum_{k \geqslant 1} \frac{p^{-sk}}{k} && (2)\\
&= \sum_{p \in \mathbb{P}} p^{-s} + \psi(s), && (3)
\end{aligned}$$

avec

$$\begin{aligned}
\psi(s) &\leqslant \sum_{p \in \mathbb{P}} \sum_{k \geqslant 2} \frac{p^{-\sigma k}}{k} && (4)\\
&\leqslant \sum_{p \in \mathbb{P}} \sum_{k \geqslant 2} p^{-\sigma k} && (5)\\
&= \sum_{p \in \mathbb{P}} p^{-2\sigma}/(1 - p^{-\sigma}) && (6)\\
&= \sum_{p \in \mathbb{P}} \frac{1}{p^{\sigma}(p^{\sigma} - 1)} && (7)\\
&\leqslant \sum_{n \geqslant 1} \frac{1}{n-1} && (8)\\
&= 1, && (9)
\end{aligned}$$

où σ désigne la partie réelle de s ; d'où le résultat. □

Définition 8. On dit qu'une partie A de l'ensemble $\mathbb{P}$ des nombres premiers a pour densité analytique $d \in [0,1]$, lorsque le rapport $(\sum_{p \in A} p^{-s})/(\sum_{p \in \mathbb{P}} p^{-s})$ a pour limite d en 1 sur le demi-plan $\Re(s) > 1$.

Par restriction aux s réels, on voit que la limite, quand elle existe, est toujours dans $[0,1]$.

Théorème 25 (Dirichlet)**.** *Soient $m \geqslant 1$ et a étranger à m. L'ensemble $\mathbb{P}_a$ des nombres premiers qui vérifient $p \equiv a \pmod m$ a pour densité analytique $1/\varphi(m)$. En particulier, il est infini.*

Pour établir ce résultat, introduisons la fonction caractéristique δ_a définie par

$$\delta_a(n) = \begin{cases} 1, \text{ pour } n \equiv a (\bmod m) \\ 0, \text{ sinon.} \end{cases}$$

Lemme 10. *Nous avons* $\delta_a = \frac{1}{\varphi(m)} \sum_\chi \chi(n)^{-1}\chi$*, où la sommation porte sur tous les caractères* χ *modulo* m*.*

Preuve du lemme : Le calcule donne

$$\sum_\chi \chi(a)^{-1}\chi(n) = \sum_\chi \left(\frac{n}{a}\right) = \begin{cases} \varphi(m), \text{ pour } n \equiv a (\bmod m) \\ 0, \text{ sinon,} \end{cases}$$

puisque dans ce dernier cas, il existe au moins un caractère χ' vérifiant $\chi'\left(\frac{n}{a}\right) \neq 1$, et qu'on a :

$$\begin{aligned} \left(\chi'\left(\frac{n}{a}\right) - 1\right) \sum_\chi \chi\left(\frac{n}{a}\right) &= \sum_\chi \chi'\left(\frac{n}{a}\right)\chi\left(\frac{n}{a}\right) - \sum_\chi \left(\frac{n}{a}\right) \\ &= \sum_\chi (\chi\chi')\left(\frac{n}{a}\right) - \sum_\chi \chi\left(\frac{n}{a}\right) \\ &= 0. \end{aligned}$$

□

Preuve du théorème : Considérons la quantité

$$\zeta_a(s) = \sum_{p \in \mathbb{P}_a} p^{-s} = \sum_{p \in \mathbb{P}} \delta_a(p) p^{-s}$$

pour $\Re(s) > 1$. Le lemme nous permet d'écrire :

$$\zeta_a(s) = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} \sum_{p \in \mathbb{P}} \chi(p) p^{-s},$$

ce qui invite à distinguer deux cas :

(i) Pour $\chi \neq 1$, la quantité $\log L(s, \chi)$ est bornée au voisinage de 1 (puisque $L(1, \chi)$ est non nul), et donnée par son développement eulérien pour $\Re(s) > 1$:

$$\log L(s, \chi) = \sum_p \sum_{k \geqslant 1} \frac{(\chi(p)p^{-s})^k}{k} = \sum_{p \in \mathbb{P}} \chi(p) p^{-s} + \sum_{p \in \mathbb{P}} \sum_{k \geqslant 2} \frac{(\text{ffl}\chi(p)p^{-s})^k}{k},$$

la somme double à droite étant bornée par 1, en vertu du calcul précédent.

(ii) Pour $\chi = 1$, en revanche, il vient directement

$$\sum_{p \in \mathbb{P}} \chi(p) p^{-s} = \sum_{p \nmid m} p^{-s} \sim \sum_{p \in \mathbb{P}} p^{-s} \sim \log \frac{1}{s-1}$$

et $\chi(a) = 1$, d'où le résultat annoncé.

□

Théorème 26. *Soit* a *un entier relatif qui n'est pas un carré. Alors l'ensemble des nombres premiers* p *tels que* a *soit (resp. ne soit pas) un carré modulo* p *a pour densité analytique* $1/2$*.*

Preuve : La loi de réciprocité quadratique jointe aux formules complémentaires exprimant $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$ affirme que le fait que a soit un carré ou non modulo p se lit sur une congruence de p (modulo un multiple convenable de a), ce qui assure l'existence de la densité annoncée.

Précisons ceci : Ecrivons $a = (-1)^d 2^\beta \ell_1 \cdots \ell_k$ la factorisation irréductible de a (avec α, β dans $\{0,1\}$, $\ell_1, \ldots, \ell_k$ impairs) après élimination des facteurs carrés. Il vient alors :

$$\begin{aligned}\left(\frac{a}{p}\right) &= \left(\frac{-1}{p}\right)^\alpha \left(\frac{2}{p}\right)^\alpha \left(\frac{\ell_1}{p}\right) \cdots \left(\frac{\ell_k}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\left(d+\sum \frac{\ell_i-1}{2}\right)} (-1)^{\frac{p^2-1}{4}\beta} \left(\frac{p}{\ell_1}\right) \cdots \left(\frac{p}{\ell_k}\right),\end{aligned}$$

pour p impair et distinct des ℓ_i, de sorte que $\left(\frac{a}{p}\right)$ ne dépend que des congruences de p modulo $d, \ell_1, \ldots, \ell_k$ i.e. via le lemme chinois, de la congruence de p modulo $m = 4|a|$.

PLus précisement encore, l'application $\chi \,|\, p \mapsto \left(\frac{a}{p}\right)$ est la restriction aux $p \nmid m$ d'un caractère d'ordre 2 modulo m, et il suit :

$$\begin{aligned}\sum_{p\nmid m,\, \left(\frac{a}{p}\right)=1} p^{-s} &= \frac{1}{2}\sum_{p\nmid m}(1+\chi(p))p^{-s} \\ &= \frac{1}{2}\sum_{p\nmid m} p^{-s} + \frac{1}{2}\sum_{p\nmid m}\chi(p)p^{-s} \\ &\sim \frac{1}{2}\sum_{p\in\mathbb{P}} p^{s} \\ &\sim \frac{1}{2}\log\frac{1}{s-1},\end{aligned}$$

pour $\Re(s) > 1$, puisque la somme $\sum \chi(p)p^{-s}$ reste bornée au voisinage de 1. □

3.3 Application a la distribution des nombres premiers

3.3.1 Propriétés élémentaires

Pour étudier la répartition des nombres premiers, il est commode d'introduire les trois fonctions de comptage :

$$\begin{aligned}\pi(x) &= \sum_{p\leqslant x} 1, \text{ la sommation portant sur les seuls premiers,} \\ \theta(x) &= \sum_{p\leqslant x} \log p = \log \prod_{p\leqslant x} p, \\ \psi(x) &= \sum_{m\geqslant 1}\sum_{p^m\geqslant x} \log p = \sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p.\end{aligned}$$

Théorème 27 (Tchebychev)**.** *Pour x grand, on a : $\theta(x) \sim \psi(x) \asymp x$. Et, plus précisément $\psi(x) \geqslant \left(\frac{1}{2}\log 2\right)x$ et $\theta(x) \leqslant (2\log 2)x$.*

Preuve : La démonstration de ce résultat repose sur trois lemmes :

Lemme 11. *Pour $x \geqslant 1$, on a $\theta(x) \leqslant (2\log 2)\,x$.*

Preuve : De l'inégalité

$$\binom{2m+1}{m} = \binom{2m+1}{m+1} \leqslant \frac{1}{2}\sum_k \binom{2m+1}{k} = 2^{2m},$$

on déduit :

$$\theta(2m+1)-\theta(m)=\log\left(\prod_{m+1\leqslant p=2m+1} p\right)\leqslant \log\binom{2m+1}{m}\leqslant (2\log 2)\,m.$$

On procède alors par récurrence, la proprieté $\theta(m)\leqslant m\log 4$ étant vraie pour $m\leqslant 2$.

— Si m est pair, on a directement $\theta(m)=\theta(m-1)\overset{[}{\underset{]}{H}}.R.]\leqslant (m-1)\log 4\leqslant m\log 4$.

— et pour $m=2k+1$, il vient $\theta(m)\leqslant \theta(k)+k\log 4\overset{[}{\underset{]}{H}}.R.]\leqslant 2k\log 4\leqslant m\log 4$.

□

Lemme 12. *Pour $x\geqslant 1$, on a les inégalités $\theta(x)\leqslant\psi(x)\leqslant\theta(x)+2\sqrt{x}\log x$.*

Preuve : On a immédiatement, compre tenu du lemme précédent :

$$\psi(x)\leqslant\theta(x)+\left[\frac{\log x}{\log 2}\right]\theta\left(\sqrt{x}\right)\leqslant\theta(x)+\frac{\log x}{\log 2}(2\log 2)\sqrt{x}=\theta(x)+2\sqrt{x}\log x.$$

□

Lemme 13. *Pour $x\geqslant 2$, on a l'inégalité $\psi(x)\geqslant\left(\frac{1}{2}\log 2\right)\cdot x$.*

Preuve : Ecrivons

$$\binom{2m}{m}=\frac{(2m)!}{(m!)^2}=\prod_{p\leqslant 2m} p^{\nu_p(m)}$$

la factorisation irréductible de $\binom{2m}{m}$. L'exposant de p est donné par la formule

$$\nu_p(m)=\sum_{k\geqslant 1}\left(\left[\frac{2m}{p^k}\right]-2\left[\frac{m}{p^k}\right]\right)$$

comme somme de $[\log 2m/\log p]$ termes égaux à 0 ou à 1. Il vient donc :

$$\log\binom{2m}{m}\leqslant\sum_{p\leqslant 2m}\left[\frac{\log 2m}{\log p}\right]\log p=\psi(2m);$$

et un calcul direct donne :

$$\binom{2m}{m}=\frac{2m\cdot(2m-1)\cdots m+1}{m\cdot(m-1)\cdots 1}\geqslant 2^{m-1}(m+1),$$

i.e. $\log\binom{2m}{m}\geqslant(m-1)\log 2+\log(m+1)\geqslant m\log 2$.

Par suite, pour tout entier $n\geqslant 4$, il vient :

— si $n=2m$ est pair, $\psi(n)=\psi(2m)\geqslant\log\binom{2m}{m}\geqslant m\log 2=\left(\frac{1}{2}\log 2\right)n$;

— si $n=2m+1$ est impair,

$$\psi(n)\geqslant\psi(2m)\geqslant(m-1)\log 2+\log(m+1)=\frac{n}{2}\log 2+\left(\log(m+1)-\frac{3}{2}\log 2\right)$$

et la qualité à droite est positive pour $m\geqslant 2$.

□

Ce dernier résultat achève d'établir la théorème, puisque la différence entre $\theta(x)$ et $\psi(x)$, qui est donnée par $\sqrt{x}\log x$, se trouve être négligeable devant $\psi(x)$.

□

Corollaire 22. *On a*

$$\pi(x) \sim \frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x},$$

et en particulier

$$\pi(x) \asymp \frac{x}{\log x}.$$

Preuve : La définition de θ donne directement

$$\theta(x) = \sum_{p \leqslant x} \log p \leqslant \sum_{p \leqslant x} \log x \pi(x) \log x,$$

i.e. $\pi(x) \geqslant \frac{\theta(x)}{\log x}$.

Inversement, pour tout $\delta \in (0,1)$, nous avons

$$\theta(x) \geqslant \sum_{x^{1-\delta} < p \leqslant x} \log p \geqslant (1-\delta)\log x[\pi(x) - \pi(x^{1-\delta})]$$

i.e. $\theta(x) \geqslant (1-\delta)\log x[\pi(x) - x^{1-\delta}]$.

En résumé, il vien donc :

$$1 \leqslant \frac{\pi(x)\log x}{\theta(x)} \leqslant \frac{1}{1-\delta} + \frac{x^{1-\delta}\log x}{\theta(x)} \leqslant \frac{1}{1-\delta} + c^k \frac{\log x}{x^\delta},$$

ce qui permet, pour tout $\varepsilon > 0$ donné, de choisir δ pour avoir $\frac{1}{1-\delta} \leqslant 1 + \varepsilon/2$, puis x assez grand pour obtenir $c^k \frac{\log x}{x^\delta} \leqslant \varepsilon/2$. □

Corollaire 23 (Postulat de Bertrand)**.** *Pour $n > 1$, l'intervalle $(n, 2n)$ contient au moins un nombre premier.*

Preuve : Sinon, soit $n \geqslant 5$ contredisant le postulat, et considérons la quantité $\binom{2n}{n}$. D'un côté, nous avons $\binom{2n}{n} = \prod_{p<n} p^{\nu_p(n)}$ avec $\nu_p(n) = \sum_{k \geqslant 1} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right)$ (puisqu'il n'y a pas par hypothèse de facteurs premiers entre n et $2n$). Or ici, pour $p \in (\frac{2}{3}n, n]$, nous avons $\left[\frac{2n}{p} \right] = 2$ et $\left[\frac{n}{p} \right] = 1$ et $\left[\frac{2n}{p^2} \right] \leqslant \left[\frac{9}{2n} \right] = 0$, ce qui donne $\nu_p(n) = 0$, de sorte que seuls interviennent les nombres premiers $p \leqslant \frac{2}{3}n$. Il vient donc :

$$\log \binom{2n}{n} = \sum_{p \leqslant \frac{2}{3}n} \nu_p(n) \log p = \sum_{p \leqslant \frac{2}{3}n} p + \sum_{p \leqslant \frac{2}{3}n} (\nu_p(n) - 1) \log p.$$

La première somme, qui n'est autre que $\theta\left(\frac{2}{3}n\right)$, est majorée par $\frac{2}{3}n \log 4$; lq seconde par $\sum_{p^2 \leqslant 2n} \nu_p(n) \log p$, puisque seuls les $p \leqslant \sqrt{2n}$ peuvent conduire à un $\nu_p(n) \geqslant 2$. Elle se présente donc comme la somme d'au plus $\sqrt{2n}$ termes donc chacun est majoré par $\nu_p(n) \log p \leqslant \left[\frac{\log 2n}{\log p} \right] \log p \leqslant \log 2n$.

En conclusion il vient : $\log \binom{2n}{n} \leqslant \frac{2}{3} n \log 4 + \sqrt{2n} \log 2n$. D'un autre côté $\binom{2n}{n}$ est le plus grand des n termes de la somme $2 + \sum_{k=1}^{2n-1} \binom{2n}{k} = 2^{2n}$, de sorte que nous avons inversement : $\log \binom{2n}{n} \geqslant \log \frac{2^{2n}}{2n} = n \log 4 - \log 2n$.

Il vient donc finalement : $\frac{1}{3} n \log 4 \leqslant \log 2n \left(\sqrt{2n+1} \right)$, i.e. $\frac{\sqrt{2n}}{\log 2n} \leqslant \frac{6}{\log 4} \left(1 + \frac{1}{\sqrt{2n}} \right)$, inégalité qui est absurde pour n assez grand. Plus précisement, la fonction $x \mapsto \sqrt{x}/\log x$ étant strictement croissante pour $x > \sqrt{e}$ (puisque sa derivée $(2\log x - 1)/2\sqrt{x}\log^2 x$ est alors strictement positive) on a $\frac{\sqrt{2n}}{\log 2n} > 4,6$

pour $n \geqslant 512$, et $\dfrac{6}{\log 4}\left(1+\dfrac{1}{\sqrt{2n}}\right) < \dfrac{6}{\log 4}\dfrac{33}{32} < 4,5$ toujours pour $n \geqslant 512$, de sorte que l'hypothèse faite entraine $n < 512 = 2^9$.

Ce point acquis, il suffit alors de vérifier le postulat de Bertrand pour $n < 512$, par example en exhibant une chaine de nombres premiers dont chacun est plus petit que le double du précédent. Ainsi : 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631. □

Remarque: Sous une forme équivalente, le postulat de Bertrand affirme précisément que dans la suite $p_1 < p_2 < p_3 < p_4 < \ldots < p_2 < \ldots$ des nombres premiers, on a toujours $p_{k+1} < 2p_k$.

3.3.2 Formule d'inversion pour la fonction ψ

Proposition 17. *La dérivée logaithmique-Z de la fonction ζ de Riemann est holomorphe sur le demi-plan $\Re(s) > 1$, où elle est somme de la série de Dirichlet :*

$$Z(s) = -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geqslant 1} \frac{\Lambda(n)}{n^s},$$

la fonction de Landau $\Lambda(n)$ étant donnée par

$$\Lambda(n) = \begin{cases} \log p & , \ \textit{pour } n = p^k \ (k \geqslant 1) \\ 0 & , \ \text{sinon.} \end{cases}$$

Preuve : Nous savons déjà que la série de Dirichlet $\dfrac{1}{\zeta}(s) = \sum_{n\geqslant 1} \mu(n) n^{-s}$ est absolument convergente sur le demi-plan $\Re(s) > 1$, et qu'il en est de même de la série $-\zeta'(s) = \sum_{n\geqslant 1} \log(n) n^{-s}$, dont les coefficients $\log n$ sont dominées par n^ε pour tout $\varepsilon > 0$, laquelle donne donc buen l'opposé de la dérivée de ζ sur ce demi-plan.

Quant aux coefficients : $\Lambda(n)$, ils peuvent s'obtenir algébriquement, à partir de l'idéntité $\Lambda(n) = \sum_{d|n} \mu(d) \log \dfrac{n}{d}$, soit analytiquement comme suit : Du développement eulérien

$$\zeta(s) = \prod_p (1-p^{-s})^{-1}, \text{ on tire } \log \zeta(s) = \sum_p \log(1-p^{-s})^{-1} = \sum_p \sum_{k\geqslant 1} \frac{p^{-sk}}{k},$$

puis, en dérivant terme à terme :

$$Z(s) = -\frac{\zeta'(s)}{\zeta(s)} = \sum_p \sum_{k\geqslant 1} \log(p) p^{-sk}, \text{ comme attendu.}$$

□

Théorème 28. *Soit $\Psi(t) = \int_0^t \psi(x)dx$ la primitive de la fonction ψ. La dérivée logarithmique de ζ est donnée sur le demi-plan $\Re(s) > 1$ par la formule :*

$$Z(s) = s\int_1^\infty \frac{\psi(t)}{t^{s+1}}dt = s(s+1)\int_1^\infty \frac{\Psi(t)}{t^{s+2}}dt.$$

Preuve : Remarquons d'abord que ψ n'est autre que la fonction sommatoire des $\Lambda(n)$, puisque nous avons par définition :

$$\psi(x) = \sum_{p^k \leqslant x} \log p = \sum_{n\leqslant x} \Lambda(n).$$

Il vient donc, pour $\Re(s) > 1$:

$$\begin{aligned}\mathbb{Z}(s) &= \sum_{n\geqslant 1} \frac{\Lambda(n)}{n^s} \\ &= \sum_{n\geqslant 1} \frac{\psi(n)-\psi(n-1)}{n^s} \\ &= \sum_{n\geqslant 1} \psi(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right) \\ &= \sum_{n\geqslant 1} s\int_n^{n+1} \frac{\psi(t)}{t^{s+1}}dt,\end{aligned}$$

i.e.

$$Z(s) = s\int_1^\infty \frac{\psi(t)}{t^{s+1}}dt = s(s+1)\int_1^\infty \frac{\Psi(t)}{t^{s+2}}dt,$$

par intégration de parties, puisque le terme tout intégré $s\left[\frac{\Psi(t)}{t^{s+2}}\right]_\infty^1$ est nul, en 1 par définition de Ψ, à l'infini d'après l'estimation $\Psi(t) = -\frac{1}{2}t^2$ fonnée par $\Psi(t) \asymp t$. □

Corollaire 24 (Formule d'inversion)**.** *Ecrivons* $s = \sigma + i\tau$*. Alors pour* $x \geqslant 0$*, la quantité* $\Psi(x)$ *est donnée pour tout* $\sigma > 0$ *par la formule :*

$$\Psi(x) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{Z(s)}{s(s+1)}x^{s+1}dx.$$

Preuve : La convergence de l'inégalité à droite est immédiate, puisque $Z(s)$ est borné en module par $\sum_{n\geqslant 1}\frac{\log n}{n^\sigma}$ et x^{s+1} par $x^{\sigma+1}$. Ce point acquis, il vient en vertu du théoréme de Fubini :

$$\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{Z(s)}{s(s+1)}x^{s+1}dx = \int_{\sigma-i\infty}^{\sigma+i\infty}\sum_{n\geqslant 1} n\Lambda(n)\frac{(x/n)^{s+1}}{s(s+1)}ds = \sum_{n\geqslant 1} n\Lambda(n)\int_{\sigma-i\infty}^{\sigma+i\infty}\frac{(x/n)^{s+1}}{s(s+1)}ds.$$

Evaluons cette dernière intégrale à l'aide du théorème des résidus :

— pour $x < n$, l'introduction de l'arc Γ_R donne :

$$0 = \int_{\sigma-i\tau}^{\sigma+i\tau} + \int_{\Gamma_R}$$

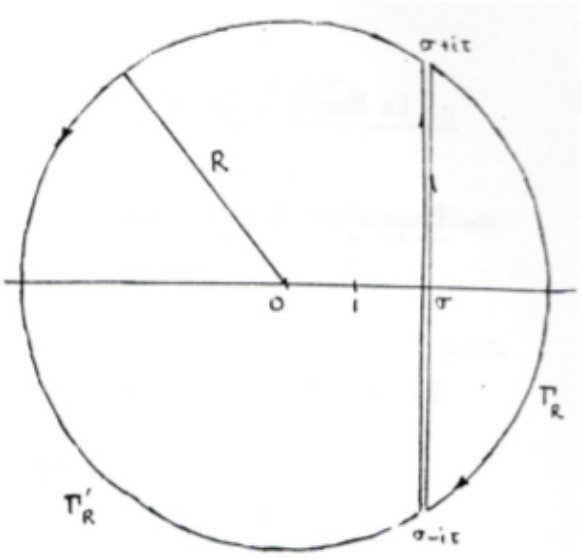
et le module de l'intégrale de droite est majoré par la quantité :

$$\int_{\Gamma_R}\frac{(x/n)^{\sigma+1}}{R^2}Rd\theta \leqslant \pi\frac{(x/n)^{\sigma+1}}{R}$$

qui tend vers 0 avec R grand.

— pour $x > n$, l'introduction de l'arc Γ'_R donne en revanche :

$$2i\pi\left(\frac{x}{n}-1\right) = \int_{\sigma-i\tau}^{\sigma+i\tau} + \int_{\Gamma'_R}$$



et le terme de droite est ici majoré par

$$\int_{\Gamma'_R} \frac{(x/n)^{\sigma+1}}{R(R-1)} R d\theta \leqslant 2\pi \frac{(x/n)^{\sigma+1}}{R-1},$$

quantité qui tend encore vers 0 avec R grand.

En résumé, il vient donc :

$$\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{(x/n)^{s+1}}{s(s+1)} ds = \begin{cases} 0 & , \text{ pour } x < n \\ 2i\pi\left(\dfrac{x}{n} - 1\right) & , \text{ sinon.} \end{cases}$$

D'où finalement :

$$\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{Z(s)}{s(s+1)} x^{s+1} dx = \sum_{n \leqslant x} 2i\pi\Lambda(n)(x-n) = 2i\pi\Psi(x)$$

comme attendu. □

Corollaire 25. *Sous les mêmes hypothèses, on a (pour $x > 1$) :*

$$\frac{\Psi(x)}{x^2} - \frac{1}{2}\left(1 - \frac{1}{x}\right) = \frac{1}{2i\pi} \int_{\sigma-i\infty}^{\sigma+i\infty} \left(\frac{Z(s)}{s(s+1)} - \frac{1}{2s(s-1)}\right) x^{s-1} ds.$$

Preuve : Le calcul de résidues déjà effectué nous donne, en effet (en utilisant l'arc Γ'_R) :

$$\frac{1}{2i\pi} \int_{\sigma-i\infty}^{\sigma+i\infty} \frac{x^{s-1} ds}{2s(s-1)} = \frac{1}{2}\left(1 - \frac{1}{x}\right),$$

d'où la formule annoncée. □

Cette dernière transformation a pour résultat d'éliminer le pôle en $s = 1$ de la fonction (holomorphe pour $\Re(s) > 1$) $\dfrac{Z(s)}{s(s-1)}$, puisque son résidue $\dfrac{1}{2}$ est le même que celui de la fonction méromorphe $\dfrac{1}{2s(s-1)}$.

L'objet de la section qui suit est de montrer que l'intégrale à droite est arbitrairement petite avec x grand, c'est à dire en fin de compte que l'on a

$$\Psi(x) \sim \frac{1}{2}x^2.$$

3.3.3 Le théorème des nombres premiers

Proposition 18 (Inégalité de la Vallée-Poussin)**.** *Pour $\sigma > 1$, on a l'inégalité :*

$$\zeta(\sigma)^3 |\zeta(\sigma + i\tau)|^4 |\zeta(\sigma + 2i\tau)| \geqslant 1.$$

Preuve : Partons de l'inégalité banale $0 \leqslant 2(1 + \cos\varphi)^2 = 3 + 4\cos\varphi + \cos 2\varphi$. Nous en tirons

$$\Re(3\log\zeta(\sigma) + 4\log\zeta(\sigma + i\tau) + \log\zeta(\sigma + 2i\tau)) = \sum_p \sum_{k \geqslant 1} \frac{p^{-k\sigma}}{k}(3 + 4\cos(k\tau\log p) + \cos(2k\tau\log p)) \geqslant 0,$$

ce qui est précisément le résultat annoncé :

$$\log(\zeta(\sigma)^3 |\zeta(\sigma + i\tau)|^4 |\zeta(\sigma + 2i\tau)|) = \Re(\log\zeta(\tau)^3 \zeta(\sigma + i\tau)^4 \zeta(\sigma + 2i\tau)) \geqslant 0.$$

□

Théorème 29. *La fonction ζ de Riemann n'a pas de zéro dans le demi-plan fermé $\sigma \geqslant 1$.*

Preuve : Nous savons déjà que ζ n'a pas de zéro dans le demi-plan ouvert (où ζ^{-1} est bien définie) et qu'elle a un pôle simple de résidu 1 en $s = 1$. Supposons donc que $s = 1 + i\tau$ soit un zéro d'ordre $k \geqslant 1$. Nous aurions alors au voisinage de 1 :

$$\zeta(\sigma)^3 \sim \frac{1}{(\sigma-1)^3}\ , \quad |\zeta(\sigma+i\tau)|^4 \asymp (\sigma-1)^{4k},$$

et l'inégalité de La Vallée-Poussin montre que $1 + 2i\tau$ est forcément un pôle de ζ, ce qui est absurde. □

Corollaire 26. *La fonction* $\zeta(s) + \dfrac{1}{1-s}$ *est holomorphe sur le demi-plan fermé* $\sigma \geqslant 1$.

Proposition 19. *Pour* $|\tau| > 1$*, on a les relations de domination uniformes pour* $\sigma \geqslant 1$ *:*
(i) $|\zeta(\sigma+i\tau)| < \log|\tau|$
(ii) $|\zeta'(\sigma+i\tau)| < \log^2|\tau|$
(iii) $|\zeta^{-1}(\sigma+i\tau)| < \log^7|\tau|$

Schéma de la preuve : C'est résultat très technique étant la clef de la démonstration du théorème des nombres premiers, donnons quelques indications sur sa démonstration :

(i) Partons de l'indentité :

$$\zeta(s) = \sum n^{-s} = \sum_{n\leqslant\tau} n^{-s} + \left[\sum_{n>\tau} n^{-s} - \int_\tau^\infty u^{-s}du\right] - \frac{\tau^{1-s}}{s-1},$$

valable pour $\tau > 1$. Majorant chacun des trois termes en modulo, nous obtenons :

$$|\zeta(s)| \leqslant \sum_{n\leqslant\tau} n^{-\sigma} + \sum_{n\geqslant\tau} |\int_n^{n+1} (n^{-s} - u^{-s})du| + \frac{\tau^{1-\sigma}}{\tau} \leqslant \sum_{n\leqslant\tau} n^{-1} + |s|\int_\tau^\infty \frac{du}{u^{\sigma-1}} + \tau^{-\sigma}$$

c'est à dire

$$|\zeta(s)| \leqslant \sum_{n\leqslant\tau} \frac{1}{n} + \frac{|s|}{\sigma}\tau^{-\sigma} + \tau^{-1}$$

avec $\sum_{n\leqslant\tau} \dfrac{1}{n}\log\tau$, $\dfrac{1}{\tau} \ll \log\tau$ et $\dfrac{|s|}{\sigma}\tau^{-\sigma} \leqslant \dfrac{\tau+\sigma}{\sigma}\tau^{-\sigma}$ bornée, d'où le résultat.

(ii) Le calcul est identique dans le cas de $\zeta'(s)$. Partant de l'identité

$$\zeta(s) = \sum_{n\leqslant\tau} n^{-s} + s\sum_{n\geqslant\tau}\int_n^{n+1} du \int_n^\mu t^{1-s}dt - \frac{\tau^{1-s}}{s-1},$$

puis décrivant chaque terme, nous obtenons cette fois $|\zeta'(s)| < \log^2\tau$, le terme dominant étant, encore une fois le premier $|\sum_{n\leqslant\tau}\log(n)n^{-s}| < \sum_{n\leqslant\tau}\dfrac{\log n}{n} \asymp \log^2\tau$.

(iii) La minoration de $\zeta(s)$ en résulte : D'un côté, l'inégalité de La Vallé-Poussin nous donne, pour tout $\eta > 0$:

$$\zeta(\sigma+\eta)^3|\zeta(\sigma+\eta+i\tau)|^4|\zeta(\sigma+\eta+2i\tau)| \geqslant 1 \ \text{ avec } \ \begin{cases} \zeta(\tau+\eta) < \dfrac{1}{\sigma+\eta-1} < \dfrac{1}{\eta} \\ |\zeta(\sigma+\eta+2i\tau)| < \log\tau \end{cases}$$

c'est à dire $|\zeta(\sigma+\eta+i\tau)| > \dfrac{\eta^{3/4}}{\log^{1/4}\tau}$. D'un autre côté, la majoration de $|\zeta'(s)|$ nous permet d'écrire :

$$|\zeta(\sigma+i\tau) - \zeta(\sigma+\eta+i\tau)| < \eta\log^2\tau, \ \text{ donc finalement } \ |\zeta(\sigma+i\tau)| > \frac{\eta^{3/4}}{\log^{1/4}\tau}$$

pourvu qu'on ait la relation de domination $\eta^{3/4}\log^{-1/4}\tau > \eta\log^2\tau$, ce qui a lieu pour $\eta = \log^{-9}\tau$ et conduit bien à la minoration annoncée. □

Corollaire 27. *Pour* x *grand, on a bien* $\Psi(x) \sim \frac{1}{2}x^2$.

Preuve : Posons $g(s) = \dfrac{Z(s)}{s(s+1)} - \dfrac{1}{2s(s-1)}$. C'est une fonction holomorphe pour $s \geqslant 1$ qui est dominée uniformement en σ par $\log^9 \tau/\tau$ d'après ce qui précède. Considérons la quantité :

$$f(x) = \Psi(x)/x^2 - \frac{1}{2}(1-1/2) = \frac{1}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty} g(s)x^{s-1}ds.$$

Pour $\omega = \log x$, nous obtenons $f(e^\omega) = \dfrac{1}{2\pi}\int_{-\infty}^{+\infty} g(\sigma+i\tau)e^{\omega(\tau-1)}e^{i\omega\tau}d\tau$, donc :

$$f(e^\omega)\left(e^{-\omega(\sigma-1)} - e^{-2\omega(\sigma-1)}\right) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} [g(\sigma+i\tau) - g(2\sigma-1+i\tau)]\, e^{i\omega\tau}d\tau.$$

Et l'intégrale à droite tends vers 0 quand σ tend vers 1 en vertu du théorème de la convergence dominée. Le choix de $\sigma = 1 + \dfrac{1}{\omega}$ nous donne donc $\lim\limits_{\omega\to\infty} f(e^\omega)(e^{-1} - e^{-2}) = 0$ i.e. $\lim\limits_{x\to\infty} f(x) = 0$, comme attendu. □

Théorème 30 (Hadamard-La Vallée-Poussin)**.** *On a* $\psi(x) \sim x$ *i.e.* $\pi(x) \sim \dfrac{x}{\log x}$.

Preuve : Pour $\varepsilon \in (0,1)$, nous avons dès que x est assez grand $\Psi(x)/\dfrac{1}{2}x^2 \in [1-\varepsilon, 1+\varepsilon]$, donc ($\psi$ étant croissante) :

$$\psi(x) \leqslant \frac{1}{x\sqrt{\varepsilon}}\int_x^{x(1+\sqrt{\varepsilon})} \psi(t)dt = \frac{1}{x\sqrt{\varepsilon}}\left(\Psi(x(1+\sqrt{\varepsilon})) - \Psi(x)\right) \leqslant \frac{1}{x\sqrt{\varepsilon}}\left(\frac{1}{2}x^2(1+\sqrt{\varepsilon})^2(1+\varepsilon) - \frac{1}{2}x^2(1-\varepsilon)\right)$$

c'est à dire : $\psi(x)/x \leqslant (1+\sqrt{\varepsilon})(1+\sqrt{\varepsilon}(1+\sqrt{\varepsilon})/2)$; et par symmétrie : $\psi(x)/x \geqslant (1-\sqrt{\varepsilon})(1-\sqrt{\varepsilon}(1-\sqrt{\varepsilon})/2)$.

D'où $\lim\limits_{x\to\infty} \psi(x)/x = 1$, ce qui achève la démonstration. □

A Théorie de Galois Topologique

A.1 Topologie des Groupes de Galois

Soient k un corps (commutatif) et Ω une clôture separable de k. Notons G le groupe $\mathrm{Gal}(\Omega/k)$ des k-automorphismes de Ω, et pour chaque sous-extension K/k de Ω/k désignons G_K le sous-groupe des K-automorphismes de Ω.

La topologie de Krull sur G est définie en prenant comme système fondamental de voisinages ouverts du neutre 1, les sous-groupes G_K lorsque K parcourt l'ensemble des sous-extensions galoisiennes de degré fini sur k.

Théorème 31. *Le groupe G équipé de la topologie de Krull est un groupe topologique compact totalment discontinu dans lequel les sous-groupes ouverts sont exactement les sous-groupes fermés d'indice fini.*

Preuve : Il s'agit de vérifier :

(i) qu'on a bien défini une topologie, autrement dit que l'intersection $G_K \cap G_L$ de deux éléments de la base contient encore un élément de la base. Or nous avons ici $G_K \cap G_L = G_{LK}$ et LK est bien galoisienne sur k comme composée de deux extensions galoisiennes.

(ii) que cette topologie fait de G un groupe topologique, autrement dit que les applications $(\sigma, \tau) \mapsto \sigma\tau$ et $\sigma \mapsto \sigma^{-1}$ sont continues. Or cela est clair puisque la préimage du voisinage $\sigma\tau G_K$ de $\sigma\tau$ contient celui ouvert $\sigma G_K \times \tau G_K$ de (σ, τ) et qu'on a $(\sigma^{-1} G_K)^{-1} = \sigma G_K$.

(iii) que G est séparé. Soient donc $\sigma \neq \tau$, puis K une extension galoisienne finie de k avec $\sigma|_K \neq \tau|_K$. Nous obtenons $\sigma G_K|_K \neq \tau G_K|_K$ i.e. $\sigma G_K \cap \tau G_K = \emptyset$.

(iv) que G est compact. Pour cela, plongeons G dans le produit $\prod_K \mathrm{Gal}(K/k)$ (où K parcourt l'ensemble des sous-extensions galoisiennes finies de k). L'application de plongement p est injective et identifie G au sous-groupe $\varprojlim \mathfrak{Gal}(K/k)$ constitué des familles $(\sigma_K)_K$ qui vérifient les conditions de cohérence $\sigma_L|_K = \sigma_K$ pour $K \overleftarrow{\subset} L$.
Ce point acquis, puisque le groupe d'arrivée est compact, en vertu du théorème de Tychonov, pour la topologie produit de celles discrètes sur les facteurs finis $\mathrm{Gal}(K/k)$, et que p est continue (puisque l'image réciproque σG_L d'un ouvert élémentaire $\{\sigma|_L\} \times \prod_{K \neq L} \mathrm{Gal}(K/k)$ est bien un ouvert de G) et ouverte (puisque l'image directe $p(\sigma G_L) = p(G) \cap (\{\sigma|_L\} \times \prod_{K \neq L} \mathrm{Gal}(K/k))$ d'un ouvert élémentaire de G est un ouvert relatif de $p(G)$), G est isomorphe à $p(G)$ comme groupe topologique, et tout le problème est de vérifier que $p(G)$ est fermé dans le produit. Pour chaque couple $L \subset N$ de sous-extensions galoisiennes de degré fini sur k, convenons d'écrire :

$$C_{N/L} = \{(\sigma_K)_K \in \prod_K \mathrm{Gal}(K/k) \mid \sigma_N|_L = \sigma_L\}.$$

Notons que si $\sigma_1, \ldots, \sigma_\ell$ sont les $[L : k]$ éléments de $\mathrm{Gal}(L/k)$ et $\Sigma_1, \ldots, \Sigma_\ell$ les ensembles de leurs $[N : L]$ prolongements respectifs à N, nous avons tout simplement $C_{N/L} = \bigcup_{i=1}^{\ell} \Big(\{\sigma_i\} \times \Sigma_i \times \prod_{K \neq L,N} \mathrm{Gal}(K/k)\Big)$, de sorte que $C_{N/L}$ est fermé comme réunion finie de fermés et

$$p(G) = \bigcap_{N \supset L} C_{N/L} \quad \text{est fermé comme intersection de fermés.}$$

(v) que G est totalment discontinu, autrement dit que tout point possède un système fondamental de voisinages ouverts et fermés. Or, si H est un sous-groupe ouvert de G, les classes à gauche σH modulo H sont encore ouvertes donc aussi en nombre fini puisqu'elles constituent une partition de l'espace compact G. En particulier le complémentaire de H est réunion finie d'ouverts donc ouvert et H lui-même est fermé. Réciproquement le méme raisonnement montre que tout sous-groupe fermé d'indice fini est forcement ouvert.

□

Définition & Proposition 5. *Un groupe topologique compact qui admet un système fondamental de voisinages du neutre formé de sous-groupes normaux est dit profini. Un tel groupe s'identifie (algébriquement et topologiquement) à la limite projective de ses quotients finis :*

$$G \simeq \varprojlim G/H \quad \textit{(où } H \textit{ parcourt l'ensemble des sous-groupes ouverts et normaux de } G\textit{)}.$$

Preuve : Le groupe topologique G étant supposé compact, ses sous-groupes ouverts H sont d'indice fini (comme vu ci-dessus) et les quotients G/H attachés aux sous-groupes normaux ouverts sont autant de groupes finis. Cela étant, il s'agit de vérifier que l'application naturelle

$$\varphi \mid G \ni \sigma \mapsto (\sigma H_i)_{i\in I} \quad \text{(où les } H_i \text{ sont les sous-groupes ouverts normaux)}$$

est un isomorphisme entre les groupes topologiques G et $\varprojlim G/H_i$, la topologie sur ce dernier étant induite par celle du produit $\prod_{i\in I} G/H_i$. Abrégeons G/H_i en G_i. Il vient alors :

(i) φ est injective puisque, G étant séparé, $\ker\varphi = \bigcap_{i\in I} H_i$ vaut $\{1\}$.

(ii) φ est continue, car si $G_I = \prod_{i\notin J} G_i \prod_{i\in J}\{1\}$ est un ouvert fondamental de $\prod_{i\in I} G_i$ (avec J partie finie de I), la préimage $\varphi^{-1}(G_I) = \bigcap_{i\in I} H_i$ est un ouvert de G.

(iii) φ est ouverte, puisque continue sur le groupe compact G. En particulier, G est isomorphe à $\varphi(G)$ qui est donc un sous-groupe fermé de $\varprojlim G_i$.

(iv) enfin, $\varphi(G)$ est dense dans $\varprojlim G_i$: Donons nous en effet un élément $\bar\sigma \in (\sigma_i)_{i\in I}$ de la limite projective $\varprojlim G_i$, et un ouvert fondamental G_J dans $\prod_{i\in I} G_i$.Posons $H_i = \bigcap_{i\in J} H_i$ (C'est évidemment un sous-groupe normal ouvert de G puisqu'intersection finie de tels sous-groupes). Cela étant, si $\sigma \in G$ est un relèvement de $\sigma_j \in G/H_j$, nous avons évidemment $\varphi(\sigma) \in \bar\sigma G_J$, ce qui montre que chaque voisinage de $\bar\sigma$ rencontre bien G.

□

A.2 Correspondence de Galois

Théorème 32. *L'application* $K \mapsto G_K = \mathrm{Gal}(K/k)$ *est une bijection décroisante entre les sous-extensions de* Ω/k *et les sous-groupes fermés de* $G = \mathrm{Gal}(\Omega/k)$ *dans laquelle les sous-groupes ouverts de* G *correspondent aux sous-extensions finies de* Ω/k*.*

Preuve : Regardons d'abord le cas où F est un extension finie de k, et notons K sa clôture galoisienne qui est donc une extension galoisienne finie de k. Pour chaque élément σ de G_F le translaté σG_K de G_K par σ est ainsi un voisinage ouvert de σ contenu dans G_F ce qui montre bien que G_F est ouvert, i.e. fermé et d'indice fini dans G. Par suite, pour toute sous-extension L de Ω/k, le groupe $G_L = \bigcap_{F\subset L} G_F$ est fermé dans G puisqu'intersection de sous-groupes fermés. Reste donc à vérifier que l'application $L \mapsto G_L$ est bijective, le caractère décroissant étant évident.

Or d'un côté, étant donnée une sous-extension L de Ω, le sous-corps de Ω qui est fixé par G_L est une extension séparable de L fixée par tout L-automorphisme de Ω, donc réduite à L. Il vient donc $L = \Omega^{G_L}$, ce qui établit l'"injectivité.

Inversement, si H est un sous-groupe fermé de G, et $K = \Omega^H$ son corps des invariants, nous avons évidemment $H \subset G_K$ et, par la théorie de Galois finie $H|_L = G_K|_L$ pour toute extension galoisienne finie L de k, i.e. $HG_L = G_K G_L$, de sorte que pour tout σ de G_K le translaté σG_L rencontre H, ce qui entraine $\sigma \in \bar H = H$, c'est à dire finalement $H = G_K$; d'où l'injectivité. □

Scolie. *L'adhèrence dans* G *d'un sous-groupe arbitraire* H *est le sous-groupe fermé* $\bar H = G_K$ *qui est associé au corps des points fixes* $K = \Omega^H$ *dans la correspondance de Galois.*

Preuve : La théorie de Galois finie montre, en effet, que H est dense dans $\bar H$ ainsi défini. □

B Symboles Continus

B.1 Généralités sur les symboles

Définition 9. Un symbole sur un corps commutatif K a valeurs dans un groupe abélien G est une application $\langle\cdot\,,\cdot\rangle$ de $K^\times \times K^\times$ dans G qui vérifie les trois axiomes :

$$\left.\begin{array}{ll}(i) & \langle xx', y\rangle = \langle x, y\rangle\langle x', y\rangle \\ (ii) & \langle x, yy'\rangle = \langle x, y\rangle\langle x, y'\rangle \end{array}\right\}\mathbb{Z}-\text{bilinéarité}$$
$$(iii)\quad \langle x, y\rangle = 1 \text{ pour } x + y = 1.$$

Proposition 20. *Tout symbole sur K satisfait en outre les deux propriétés suivantes :*

$$(ii)\quad \langle x, x\rangle = \langle x, x-1\rangle = \langle x, -1\rangle \text{ ; } \textit{en particulier } \langle x, x\rangle \textit{ est d'ordre 1 ou 2.}$$
$$(iii)\quad \langle x, y\rangle\langle y, x\rangle = 1 \text{ ; } \textit{autrement dit un symbole est antisymétrique.}$$

Preuve : Un calcul immédiat donne en effet :

$$\langle x, x\rangle/\langle x, x-1\rangle = \langle x, \frac{x}{x-1}\rangle = \langle x, \frac{1}{1-x^{-1}}\rangle = \langle x, 1-x^{-1}\rangle^{-1} = \langle x^{-1}, 1-x^{-1}\rangle = 1.$$

$$\langle x, x-1\rangle/\langle x, -1\rangle = \langle x, 1-x\rangle = 1.$$

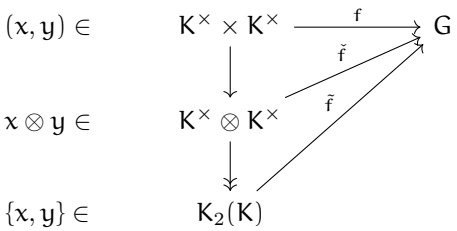
Il vient de même : $\langle xy, xy\rangle = \langle xy, -1\rangle = \langle x, -1\rangle\langle y, -1\rangle = \langle x, x\rangle\langle y, y\rangle$. Et directement : $\langle xy, xy\rangle = \langle xy, x\rangle\langle xy, y\rangle = \langle x, x\rangle\langle x, y\rangle\langle y, x\rangle\langle y, y\rangle$, d'où le résultat. □

Théorème & Définition 5. *On note $K_2(K) = K^\times \otimes_{\mathbb{Z}} K^\times/I_K$ le quotient du carré tensoriel du groupe multiplicatif $K^\times$ par le sous-module engendré par les éléments de la forme $x \otimes (1-x)$ pour $x \in K \setminus \{0, 1\}$. Alors :*

(i) L'application naturelle $(x, y) \mapsto \{x, y\} = (x \otimes y)I_K$ est un symbole sur K à valeurs dans $K_2(K)$ appelée symbole universel.

(ii) Pour tout symbole f à valeurs dans un groupe abélien G, il existe un unique morphisme de $\mathbb{Z}$-modules $\tilde{f} : K_2(K) \to G$ tel qu'on ait $f(x, y) = \tilde{f}(\{x, y\})$, pour tous x et y de $K^\times$.

Preuve : Il résulte de la propriété universelle du produit tensoriel que toute application $\mathbb{Z}$-bilinéaire f de $K^\times \times K^\times$ dans un groupe abélien G se factorise via une unique application linéaire $\check{f}$ de $K^\times \otimes K^\times$ dans G conformément au diagramme commutatif ci-contre : Maintenant, si f est un symbole, $\ker \check{f}$ contient I_K et $\check{f}$ se factorise par $K_2(K)$. □



B.2 Symboles sur les corps finis et sur les corps locaux

Proposition 21. *On a $K_2(\mathbb{F}_q) = 1$. Autrement tout symbole sur un corps fini est trivial.*

Preuve : Le groupe multiplicatif $\mathbb{F}_q^\times$ étant cyclique d'ordre $q-1$, engendré par disons ζ, le groupe $K_2(\mathbb{F}_q)$ est donc engendré par le symbole universel $\{\zeta, \zeta\} = \{\zeta, -1\}$ qui est d'ordre 1 ou 2 et, par ailleurs d'ordre divisant $q-1$.

— Si q est pair, $q-1$ est impair et tout est dit.

— Sinon, $q-1$ est pair et il existe dans $\mathbb{F}_q^\times$ exactement $\dfrac{q-1}{2}$ non carrés mais seulement $\dfrac{q-3}{2}$ carrés distincts de 1. Autrement dit, il existe au moins un non carré $x = \zeta^i$ (avec i impair) telque $1-\zeta^i$ ne soit pas un carré, i.e. s'écrive ζ^j avec j impair. Il suit :

$$\{\zeta,\zeta\} = \{\zeta,\zeta\}^{ij} = \{\zeta^i,\zeta^j\} = \{\zeta^i, 1-\zeta^i\} = 1,$$

comme annoncé.

□

Considérons maintenant le cas d'un corps local i.e. du complété d'un corps de nombres K en une place $\mathfrak{p}$. Dans ce contexte, il est naturel de s'intéresser aux symboles continus sur le corps topologique $K_\mathfrak{p}$. On définit alors $K_2^{\mathrm{cont}}(K_\mathfrak{p})$ comme le quotient du carré topologique du $\mathbb{Z}$-module $K_\mathfrak{p}^\times$ par le sous-module fermé construit sur les éléments de la forme $x \otimes (1-x)$. Le groupe $K_2^{\mathrm{cont}}(K_\mathfrak{p})$ est universel pour les symboles continus. Cela étant :

Théorème 33. *Si $K_\mathfrak{p}$ est un corps local régulier, le groupe $K_2^{cont}(K_\mathfrak{p})$ est cyclique d'ordre $N\mathfrak{p}-1$, engendré par le symbole universel $\{\zeta,\pi\}$, où ζ est une racine primitive de l'unité dans $\mu_\mathfrak{p}^0$ et π un uniformisante.*

En d'autres termes, tout symbole continu sur $K_\mathfrak{p}$ se factorise par le symbole régulier, qui est défini par :

$$(x,y)_\mathfrak{p} = \omega\left((-1)^{\nu_\mathfrak{p}(x)\nu_\mathfrak{p}(y)}\frac{x^{\nu_\mathfrak{p}(y)}}{y^{\nu_\mathfrak{p}(x)}}\right),\ \textit{et à valeurs dans } \mu_\mathfrak{p}^0.$$

Preuve : Le corps $K_\mathfrak{p}$ étant supposé régulier, le groupe multiplicatif $K_\mathfrak{p}^\times$ est engendré topologiquement par

(i) la racine primitive ζ, d'ordre $q-1 = N\mathfrak{p}-1$.

(ii) l'uniformisante π.

(iii) les éléments $\eta_{ij} = 1-\zeta^j\pi^i$ pour $\begin{cases}\text{certains } j\\ \text{certains } i \not\equiv 0 \bmod \mathfrak{p}\end{cases}$

En particulier, tout symbole continu est déterminé uniquement par ses valeurs sur les seuls couples construits sur ces éléments. Or, dans $K_2^{\mathrm{cont}}(K_\mathfrak{p})$, nous avons successivement :

1. $\{\zeta,\mu\} = 1$, $\forall \mu \in U_\mathfrak{p}^1$ par $\{\zeta,\mu\} = \{\zeta^{q-1}, \mu^{1/(q-1)}\} = 1$, $(q-1)$ étant inversible dans $\mathbb{Z}_p$.
2. $\{\zeta,\zeta\} = 1$, car d'un côté nous avons $\{\zeta,\zeta\} = \{\zeta,-1\}$ d'ordre 1 ou 2, et d'un autre côté il existe i et j impair avec $\zeta^i \equiv 1-\zeta^j \pmod{\mathfrak{p}_\mathfrak{p}}$, i.e. $\dfrac{\zeta^i}{1-\zeta^j} \in U_\mathfrak{p}^1$ donc

$$\{\zeta,\zeta\} = \{\zeta,\zeta\}^{ij} = \{\zeta^j,\zeta^i\} = \{\zeta^j, \frac{\zeta^i}{1-\zeta^j}\} = \{\zeta, \frac{\zeta^i}{1-\zeta^j}\}^j = 1.$$

3. $\{\pi,\mu\} = 1$, $\forall \mu \in U_\mathfrak{p}^1$ par $\{\pi, 1-\zeta^j\pi^i\} = \{\pi^i, (1-\zeta^j\pi^i)^{1/i}\} = \{\zeta^{-j}, (1-\zeta^j\pi^i)^{1/i}\} = 1$, puisque i est supposé inversible dans $\mathbb{Z}_p$.
4. $\{\pi,\pi\} = \{\pi,-1\} = \{\pi,\zeta^{(q-1)/2}\} = \{\pi,\zeta\}^{(q-1)/2}$.

Et cela montre que $\{\zeta,\pi\}$ engendre $K_2^{\mathrm{cont}}(K_\mathfrak{p})$. Reste à vérifier que $K_2^{\mathrm{cont}}(K_\mathfrak{p})$ est vraiment d'ordre $q-1$, ce qui peut se faire en exhibant un symbole continu à valeurs dans $\mu_\mathfrak{p}$ qui envoie (ζ,π) sur ζ, c'est à dire en vérifiant que le symbole régulier présenté satisfait bien les trois axiomes de la définition 1. Or la bilinéarité est évidente, ainsi que la continuité. Tout le problème est donc de vérifier l'axiome (iii). Distinguons deux cas :

— Pour $x \in A_\mathfrak{p}$, nous avons
  — soit $\nu_\mathfrak{p}(x) > 0$, $\nu_\mathfrak{p}(1-x) = 0$ et $(x,1-x)_\mathfrak{p} = \omega(1-x)^{-\nu_\mathfrak{p}(x)} = 1$
  — soit $\nu_\mathfrak{p}(1-x) > 0$, $\nu_\mathfrak{p}(x) = 0$ et $(x,1-x)_\mathfrak{p} = \omega(x)^{\nu_\mathfrak{p}(1-x)} = 1$
  — soit $\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(1-x) = 0$ et $(x,1-x)_\mathfrak{p} = 1$

— Pour $x \notin A_\mathfrak{p}$, nous avons $x = \pi^{-\alpha}\mu$ (avec $\alpha > 0$) et $1-x = -\pi^{-\alpha}\mu(1-\pi^\alpha\mu^{-1})$ avec $\nu = 1-\pi^\alpha\mu^{-1} \in U_\mathfrak{p}^1$. Il suit :

$$(x,1-x)_\mathfrak{p} = (-1)^{\alpha^2}\omega\left[(\pi^{-\alpha}\mu)^{-\alpha}/(-\pi^{-\alpha}\mu\nu)^{-\alpha}\right] = (-1)^\alpha\omega((-1)^\alpha\nu) = 1,$$

comme attendu.

□

Scolie. *Le groupe* $K_2^{cont}(\mathbb{R})$ *est cyclique d'ordre 2, engendré par le symbole* $\{-1,-1\}$. *En d'autres termes, tout symbole continu sur* $\mathbb{R}$ *se factorise par le symbole régulier :*

$$(a,b)_\infty = (-1)^{\nu_\infty(a)\nu_\infty(b)}\,\mathrm{sg}\left(\frac{a^{\nu_\infty(b)}}{b^{\nu_\infty(a)}}\right) = \begin{cases} -1 & \textit{pour } a<0 \textit{ et } b<0 \\ +1 & \textit{sinon,} \end{cases}$$

où la valuation à l'infini est donnée par $\nu_\infty(a)=0$ *pour* $a>0$, $\nu_\infty(a)=1$ *pour* $a<0$.

B.3 Symboles sur le corps des rationnels

En chaque place impaire p de $\mathbb{Q}$, le symbole régulier $(\ ,\ )_p$ défini sur le complété $\mathbb{Q}_p$ induit par restriction un symbole sur $\mathbb{Q}$ à valeurs dans le groupe cyclique μ_p^0 avec

$$\mu_\infty^0 = \{\pm 1\} \text{ pour } p \text{ infinie}, \qquad \mu_p^0 \simeq \mathbb{F}_p^\times \text{ pour } p \text{ finie}.$$

Comme de plus $(a,b)_p$ vaut 1 dès que a et b sont étrangers à p (pour p finie), donc pour presque tout p, la propriété universemme du K_2 nous donne un morphisme de groupes

$$\{x,y\} \in K_2(\mathbb{Q}) \longrightarrow \bigoplus_{p\neq 2} \mu_p^0 \ni ((x,y)_p)_{p\neq 2},$$

dont nous allons voir que c'est un isomorphisme.

Théorème 34. *Les symboles réguliers attachés aux places impaires du corps des rationes induisent un isomorphisme* $K_2(\mathbb{Q}) \simeq \bigoplus_{p\neq 2} \mu_p^\infty$.

En d'autres termes tout symbole $\langle,\rangle$ *sur* $\mathbb{Q}$ *à valeurs dans un groupe* G *sont les applications de la forme* $(x,y)\mapsto \langle x,y\rangle = \prod_{p\neq 2} f_p((x,y)_p)$, *où* $(f_p)_{p\neq 2}$ *est une famille de morphismes de* μ_p^0 *dans* G.

Preuve : Pour chaque nombre premier p, notons S_p (resp. S_p') le sous-groupe multiplicatif de $\mathbb{Q}^\times$ engendré par -1 et les premiers $q \leqslant p$ (resp $q<p$), puis M_p (resp. M_p') le sous-groupe de $K_2(\mathbb{Q})$ engendré par les symboles $\{a,b\}$ pour a et b dans S_p (resp. S_p').

1er point : Nous avons $M_2 \simeq \mu_\infty^0$.

Il vient, en effet : $\{2,2\}=\{2,-1\}=1$ de sorte que M_2 est engendré par le symbole $\{-1,-1\}$ qui est effectivement d'ordre 2 puisqu'on a $(-1,-1)_\infty=-1$.

2ème point : Nous avons $M_p/M_p' \simeq \mu_p^0$.

Partons de deux éléments ap^α et bp^β de S_p (avec a et b dans S_p'). Le calcul donne :

$$\{ap^\alpha, bp^\beta\} = \{p,p\}^{\alpha\beta}\{a,p\}^\beta\{b,p\}^{-\alpha}\{a,b\} = \{(-1)^{\alpha\beta}\frac{a^\beta}{b^\alpha},p\}\{a,b\} \ \text{ avec } \{a,b\}\in M_p'.$$

Il en résulte que toute classe de M_p/M_p' est représenté par un $\{m,p\}$ pour un m de S_p', autrement dit, puisque $\{-1,p\}$ vaut $\{p-1,p\}$, que M_p/M_p' est engendré par les classes des $\{m,p\}$ pour $m\in\{1,\dots,p-1\}$. Plus précisement, pour $(m,n)\in\{1,\dots,p-1\}^2$, écrivons :

$$mn = pq + r \ \text{ avec } \ r\in\{1,\dots,p-1\} \text{ et } q\in\{0,\dots,p-1\}, \text{i.e.} \frac{mn}{r} - \frac{pq}{r} = 1.$$

Pour $q=0$, nous avons banalement $\{mn,p\}=\{r,p\}$, tandis que pour $q\neq 0$, nous obtenons :

$$\{\frac{mn}{r},p\} = \frac{\{mn/r,p\}}{\{mn/r,-pq/r\}} = \{mn/r,-r/q\}\in M_p',$$

donc dans tous les cas : $\{mn,p\}M_p' = \{r,p\}M_p'$. En particulier, le quotient M_p/M_p' est représenté par les $p-1$ éléments $\{m,p\}$ pour $m\in\{1,\dots,p-1\}$.

Et comme nous disposons d'un morphisme surjectif $\{m,p\}M_p'\mapsto (m,p)_p=\omega_p(m)\in\mu_p^0$, induit par le symbole régulier $(\ ,\ )_p$ sur M_p, l'isomorphisme annoncé en résulte.

3ème point : Nous avons $M_p \simeq \bigoplus_{q\neq 2,\, q\leqslant p} \mu_q^0$ (avec la convention $\infty \leqslant p$!)

Un récurrence immédiate à partir des deux premiers points nous assure de l'égalité des ordres :

$$|M_p| = \left(\prod_{q=3}^{p} (M_q : M_q')\right) |M_2| = |\mu_\infty^0| \prod_{q=3}^{p} |\mu_q^0|.$$

L'existence d'un morphisme naturel $M_p \to \mu_\infty^0 \oplus \ldots \oplus \mu_\infty^0$ induit par les symboles réguliers donne alors l'isomorphisme attendu, sous réserve, par exaple, de l'injectivité. Or celle-ci peut s'établir comme suit : Les calculs qui précèdent montrent que le noyau de $(\ ,\ )_p$ dans M_p est $M_p' = M_q$ (où q est prédécesseur de p) ; l'hypothèse de récurrence appliquée à M_q donne donc le résultat. Par passage à la limite, nous en déduisons l'isomorphisme annoncé :

$$K_2(\mathbb{Q}) = \varinjlim M_p = \bigoplus_{p\neq 2} \mu_p^0.$$

□

B.4 Les symboles quadratiques sur $\mathbb{Q}$

Définition 10. On appelle symbole quadratique en un place p de $\mathbb{Q}$ l'application définie pour a et b dans $\mathbb{Q}_p^\times$ par :

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) = \begin{cases} +1 & , \text{ si l'équation } ax^2 + by^2 - z^2 = 0 \text{ a une solution non triviale dans } \mathbb{Q}_p^3 \\ -1 & , \text{sinon.} \end{cases}$$

Nota. *Nous allons voir que* $\left(\frac{\ ,\ }{\mathbb{Q}_p}\right)$ *est effectivement un symbole non trivial sur* $\mathbb{Q}_p$. *Comme il est évidemment symétrique et qu'il vérifie trivialement* $\left(\frac{a,1-a}{\mathbb{Q}_p}\right) = 1$ *(puisque l'équation* $ax^2 + (1-a)y^2 - z^2 = 0$ *a* $(1,1,1)$ *comme solution), tout le problème consiste à vérifier la multiplicativité en l'une des variables. Or, nous avons la caractèrisation :*

Proposition 22.

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) = 1 \quad \Leftrightarrow \quad a \textit{ est norme dans l'extension } \mathbb{Q}_p[\sqrt{b}]/\mathbb{Q}_p$$
$$(\Leftrightarrow \quad b \textit{ est norme dans l'extension } \mathbb{Q}_p[\sqrt{a}]/\mathbb{Q}_p).$$

Preuve : Si b est un carré dans $\mathbb{Q}_p^\times$, disons $b = \beta^2$, l'équation $ax^2 + \beta^2 y^2 - z^2 = 0$ admet la solution non triviale $(0,1,\beta)$ et l'extension $\mathbb{Q}_p[\sqrt{b}]$ est égale à $\mathbb{Q}_p$.

Si b n'est pas un carré dans $\mathbb{Q}_p^\times$, les solutions non triviales (x,y,z) de l'équation vérifient $x \neq 0$, ce qui permet de les écrire sous la forme $a = \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2 = N\left(\frac{z}{x} + \frac{y}{x}\sqrt{b}\right)$.

Ce point acquis, examinons successivement les trois cas :

1er cas : $p = \infty$ i.e. $\mathbb{Q}_p = \mathbb{R}$.

Dans ce cas, comme les sommes de deux carrés dans $\mathbb{R}^\times$ sont les éléments positifs, le sous-groupe des normes dans $\mathbb{C}/\mathbb{R}$ est $\mathbb{R}_+^\times$, et nous avons :

$$\left(\frac{a,b}{\mathbb{Q}_p}\right) = -1 \Leftrightarrow b < 0 \text{ (i.e. } \mathbb{R}[\sqrt{b}] = \mathbb{C}) \text{ et } a < 0 (\text{ i.e. } a \notin N(\mathbb{C}^\times)).$$

En d'autres termes $\left(\frac{\ ,\ }{\mathbb{Q}_p}\right)$ n'est autre que le symbole régulier $(\ ,\ )_\infty$.

2ème cas : $\mathfrak{p}$ premier impair.

Dans ce cas, $\mathbb{Q}_\mathfrak{p}$ admet exactement trois extensions quadratiques : celle non ramifiée $\mathbb{Q}_\mathfrak{p}[\sqrt{\zeta}]$ (pour ζ racine primitive $(\mathfrak{p}-1)$-ième), la cyclotomique $\mathbb{Q}_\mathfrak{p}[\sqrt{-\mathfrak{p}}]$ et leur *composée* $\mathbb{Q}_\mathfrak{p}[\sqrt{-\zeta_\mathfrak{p}}]$. Dans le premier cas, l'uniformisante $\mathfrak{p}$ n'est pas norme ; dans le deux autres les unités qui sont normes sont les carrés modulo $\mathfrak{p}$, e t ζ n'est pas norme. En revanche $-\zeta$, $\mathfrak{p}$ et $\zeta_\mathfrak{p}$ sont respectivement normes (de $\sqrt{\zeta}$, $\sqrt{-\mathfrak{p}}$, $\sqrt{-\zeta_\mathfrak{p}}$) de sorte que dans tous les cas le sous-groupe des normes, qui contient $\mathbb{Q}_\mathfrak{p}^{\times 2}$, est d'indice 2 dans $\mathbb{Q}_\mathfrak{p}^\times$, ce qu'on peut résumer par le tableau :

$$\begin{array}{c}\mathbb{Q}_\mathfrak{p}^\times = \mu_\mathfrak{p}^0 U_\mathfrak{p}^1 \mathfrak{p}^\mathbb{Z} \\ \mathbb{Q}_\mathfrak{p}^{\times 2} = \mu_\mathfrak{p}^{0\,2} U_\mathfrak{p}^1 \mathfrak{p}^{2\mathbb{Z}} \\ \mathbb{Q}_\mathfrak{p}^\times/\mathbb{Q}_\mathfrak{p}^{\times 2} = \mu_\mathfrak{p}^0/\mu_\mathfrak{p}^{0\,2}\mathfrak{p}^{\mathbb{Z}/2\mathbb{Z}}\end{array}$$

Radical	ζ	$-\mathfrak{p}$	$-\zeta_\mathfrak{p}$
Norme	$-\zeta$	$\mathfrak{p}$	$\zeta_\mathfrak{p}$
Non norme	$\mathfrak{p}$	ζ	ζ
Groupe des normes	$\langle -\zeta\rangle\mathbb{Q}_\mathfrak{p}^\times$	$\langle \mathfrak{p}\rangle\mathbb{Q}_\mathfrak{p}^\times$	$\langle -\zeta_\mathfrak{p}\rangle\mathbb{Q}_\mathfrak{p}^\times$

De $\left(\frac{\mathfrak{a},\mathfrak{b}}{\mathbb{Q}_\mathfrak{p}}\right) = \left(\frac{\mathfrak{a}',\mathfrak{b}}{\mathbb{Q}_\mathfrak{p}}\right) = -1$ on tire donc $\left(\frac{\mathfrak{a}\mathfrak{a}',\mathfrak{b}}{\mathbb{Q}_\mathfrak{p}}\right) = 1$, ce qui établit la multiplicativité en $\mathfrak{a}$, les autres cas étant évidents.

En résumé, $\left(\frac{,}{\mathbb{Q}_\mathfrak{p}}\right)$ est bien un symbole à valeurs dans $\{\pm 1\}$, et, puisqu'il est d'ordre 2, c'est necessairement la puissance $\frac{\mathfrak{p}-1}{2}$-ième du symbole régulier $(\ ,\ )_\mathfrak{p}$, ce qui s'écrit :

$$\left(\frac{\mathfrak{a},\mathfrak{b}}{\mathbb{Q}_\mathfrak{p}}\right) = (\mathfrak{a},\mathfrak{b})_\mathfrak{p}^{(\mathfrak{p}-1)/2} = \left(\frac{(\mathfrak{a},\mathfrak{b})_\mathfrak{p}}{\mathfrak{p}}\right),$$

à l'aide du caractère de Dirichlet.

3ème cas : $\mathfrak{p} = 2$.

La situation est un peu plus compliqué ici puisque la décomposition multiplicative $\mathbb{Q}_2^\times = \{\pm 1\}\cdot U_2^2 2^\mathbb{Z}$ montre que $\mathbb{Q}_2$ admet 7 extensions quadratiques que l'on peut toutes obtenir à partir que $\mathbb{Q}_2[\mathfrak{i}]$, de la cyclotomique $\mathbb{Q}_2[\sqrt{2}]$, et de la non ramifiée $\mathbb{Q}_2[\sqrt{5}] \subset \mathbb{Q}_2[\zeta_5]$. Comme -1 n'est pas somme de deux carrés dans $\mathbb{Q}_2$, il n'est pas norme dans l'extension $\mathbb{Q}_2[\mathfrak{i}]/\mathbb{Q}_2$. Ainsi, le symbole $\left(\frac{-1,-1}{\mathbb{Q}_2}\right)$ vaut -1.

Cela étant :

— On a $2 = N(1+\mathfrak{i})$ et $5 = N(2+\mathfrak{i})$ normes dans $\mathbb{Q}_2[\mathfrak{i}]/\mathbb{Q}_2$ de sorte que 10 l'est aussi. Cela donne $\left(\frac{2,-1}{\mathbb{Q}_2}\right) = \left(\frac{-2,-5}{\mathbb{Q}_2}\right) = \left(\frac{10,-1}{\mathbb{Q}_2}\right) = 1$ et, par symétrie, $\left(\frac{-1,2}{\mathbb{Q}_2}\right) = \left(\frac{-1,5}{\mathbb{Q}_2}\right) = \left(\frac{-5,10}{\mathbb{Q}_2}\right) = 1$.

— On a $5 = N(\sqrt{-5})$ et $6 = (-2)\times(-3) = N(1+\sqrt{-5})$ normes dans $\mathbb{Q}_2[\sqrt{-5}]/\mathbb{Q}_2$. Comme $-3/5$ est un carré, il suit que -2 et, par suite, -10 sont encore normes. Cela donne $\left(\frac{5,-5}{\mathbb{Q}_2}\right) = \left(\frac{-2,-5}{\mathbb{Q}_2}\right) = \left(\frac{-10,-5}{\mathbb{Q}_2}\right) = 1$ et, par symétrie $\left(\frac{-5,5}{\mathbb{Q}_2}\right) = \left(\frac{-5,-2}{\mathbb{Q}_2}\right) = \left(\frac{-5,-10}{\mathbb{Q}_2}\right) = 1$. En résumé, on obtient le tableau suivant :

Radical	-1	5	2	-5	-2	10	-10
Normes	$2,5$	$-5,-1$	$-2,-1$	$5,-2$	$2,-5$	$-1,-10$	$10,-5$
	10	5	2	-10	-10	10	-2

Et on constate que, dans tous les cas, le sous groupe des normes est au moins d'indice 2 (on pourrait vérifier qu'il est exactement d'indice 2 dans $\mathbb{Q}_2^\times$, mais c'est inutile à la démonstration). On conclut donc, comme plus haut, à la multiplicativité en $\mathfrak{a}$, ce qui montre que $\left(\frac{,}{\mathbb{Q}_2}\right)$ est bien un symbole (non trivial car $\left(\frac{-1,-1}{\mathbb{Q}_2}\right)$ vaut -1) sur $\mathbb{Q}_2$.

□

Théorème 35. *L'application* $(\mathfrak{a},\mathfrak{b}) \mapsto \left(\frac{\mathfrak{a},\mathfrak{b}}{\mathbb{Q}_\mathfrak{p}}\right)$ *est un symbole non trivial sur* $\mathbb{Q}_2$ *à valeurs dans* $\{\pm 1\}$.

— *Pour* $\mathfrak{p}=\infty$, *ce n'est rien d'autre que le symbole régulier* $(\ ,\ )_\infty$.

— *pour* $\mathfrak{p}$ *premier impair, c'est la puissance* $\frac{\mathfrak{p}-1}{2}$*-ième du symbole régulier, i.e. le composé du symbole régulier et du caractère de Legendre :*

$$\left(\frac{\ ,\ }{\mathbb{Q}_\mathfrak{p}}\right) = \left(\frac{(\ ,\ )_\mathfrak{p}}{\mathfrak{p}}\right).$$

— *enfin, pour* $\mathfrak{p}=2$, *c'est un symbole non trivial sur* $\mathbb{Q}_2$, *qui vérifie* $\left(\frac{-1,-1}{\mathbb{Q}_2}\right)=-1$.

Scolie. *Le groupe* $\mathsf{K}_2^{cont}(\mathbb{Q}_2)$ *es cyclique d'ordre 2, isomorphe à* μ_2, *engendré par* $\{-1,-1\}$.

Preuve : Nous avons déjà que $-1,5$ et 2 engendrent topologiquement $\mathbb{Q}_2^\times$. Comme il vient :

$$\{2,2\}=\{2,-1\}=1 \quad \text{et} \quad \{5,5\}=\{5,-1\}=\{5,4\}=\{5,2\}^2,$$

il suit que $\mathsf{K}_2^{\mathrm{cont}}(\mathbb{Q}_2)$ est engendré par $\{-1,-1\}$ et $\{5,2\}$ qui est au plus d'ordre 4. Cela étant, écrivant $-3=5^\alpha$ avec $\alpha \in 1+4\mathbb{Z}_2$, nous obtenons :

$$\{5,2\}=\{5,2\}^\alpha=\{-3,2\}=\{3,2\}=\{3,1\}=\{-5,-1\}=\{-1,-1\}\{5,-1\}$$

i.e. $\{5,2\}^{-1}=\{5,2\}^3=\{-1,-1\}$ soit encore $\{5,2\}=\{-1,-1\}$. Ainsi $\mathsf{K}_2^{\mathrm{cont}}(\mathbb{Q}_2)$ est engendré par $\{-1,-1\}$, et il est non trivial puisqu'on a $\left(\frac{-1,-1}{\mathbb{Q}_2}\right)=-1$. □

B.5 Loi de réciprocité sur $\mathbb{Q}$

La restriction du symbole sauvage $\left(\frac{\ ,\ }{\mathbb{Q}_2}\right)$ est un symbole sur $\mathbb{Q}$, à valeurs dans $\mu_2=\{\pm 1\}$, qui s'exprime donc, en vertu de la description de $\mathsf{K}_2(\mathbb{Q})$ donnée plus haut à l'aide des symboles réguliers attachés aux places impaires de $\mathbb{Q}$.

En d'autres termes, nous avons

$$\left(\frac{\ ,\ }{\mathbb{Q}_2}\right) = (\ ,\ )_\infty^{\varepsilon_\infty} \prod_{\mathfrak{p}\,\mathrm{impair}} \left(\frac{(\ ,\ )_\mathfrak{p}}{\mathfrak{p}}\right)^{\varepsilon_\mathfrak{p}},$$

pour des $\varepsilon_\mathfrak{p}$ dans $[0,1]$.

Pour déterminer les $\varepsilon_\mathfrak{p}$, nous aurons besoin d'une formule explicite pour $\left(\frac{\ ,\ }{\mathbb{Q}_2}\right)$:

Lemme 14. *Pour* $\mathfrak{a}\in \mathsf{U}_2$, *on a les formules explicites :*

$$\textit{(i)}\ \left(\frac{-1,\mathfrak{a}}{\mathbb{Q}_2}\right)=(-1)^{(\mathfrak{a}-1)/2} \qquad \textit{(ii)}\ \left(\frac{2,\mathfrak{a}}{\mathbb{Q}_2}\right)=(-1)^{(\mathfrak{a}^2-1)/8}$$

Preuve : Les calculs effectués plus haut montrent que l'on a $\left(\frac{5,2}{\mathbb{Q}_2}\right)=\left(\frac{-1,-1}{\mathbb{Q}_2}\right)=-1$. Pour chacune des deux extensions quadratiques $\mathbb{Q}_2[\mathrm{i}]/\mathbb{Q}_2$ et $\mathbb{Q}_2[\sqrt{2}]/\mathbb{Q}_2$, le groupe des normes est donc d'indice 2 dans $\mathbb{Q}_2^\times$: c'est $\mathsf{U}_2^2\cdot 2^\mathbb{Z}$ dans le premier cas, $\mu_2\mathsf{U}_2^3 2^\mathbb{Z}$ dans le second.

Il vient donc :

$$\left(\frac{-1,\mathfrak{a}}{\mathbb{Q}_2}\right)=1 \Leftrightarrow \mathfrak{a}\equiv 1 \bmod 4 \Leftrightarrow (-1)^{(\mathfrak{a}-1)/2}=+1$$

et

$$\left(\frac{2,a}{\mathbb{Q}_2}\right)=1\Leftrightarrow a^2\equiv 1 \bmod 16\Leftrightarrow (-1)^{(a^2-1)/8}=1.$$

□

Théorème 36 (Loi de réciprocité quadratique sur $\mathbb{Q}$)**.** *Les symboles quadratiques sur $\mathbb{Q}$ vérifient la loi de réciprocité :*

$$\left(\frac{,}{\mathbb{Q}_2}\right)=(\ ,\ )_\infty\prod_{p\ impair}\left(\frac{(\ ,\ )_p}{p}\right)$$

En d'autre termes on a la formule du produit :

$$\prod_{p\in \mathrm{Pl}_{\mathbb{Q}}}\left(\frac{,}{\mathbb{Q}_p}\right)=1.$$

Preuve : Il s'agit de vérifier que l'on a $\varepsilon_p=1$ pour tout p. Or :

- pour $p=\infty$, le calcul donne : $-1=\left(\frac{-1,-1}{\mathbb{Q}_2}\right)=(-1,-1)_\infty^{\varepsilon_\infty}$, donc $\varepsilon_\infty=1$.
- pour $p\equiv 3 \bmod 4$, il vient : $-1=\left(\frac{-1,p}{\mathbb{Q}_2}\right)=\left(\frac{-1,p}{\mathbb{Q}_p}\right)^{\varepsilon_p}$, donc $\varepsilon_p=1$.
- pour $p\equiv 5 \bmod 8$, il vient : $-1=\left(\frac{2,p}{\mathbb{Q}_2}\right)=\left(\frac{2,p}{\mathbb{Q}_p}\right)^{\varepsilon_p}$, donc $\varepsilon_p=1$.

Et seul reste à considérer le cas $p\equiv 1 \bmod 8$. Nous nous appuyerons pour cela sur un lemme établi par Gauss au cours de sa démonstration de la loi de réciprocité quadratique.

Lemme 15. *Soit p un nombre premier $p\equiv 1 \bmod 8$. Il existe alors un premier impair $q<\sqrt{p}$ tel que p ne soit pas un carré modulo q.*

Preuve du lemme : Procédons par l'absurde en supposant $\left(\frac{p}{q}\right)=+1$ pour tout premier impair $q<\sqrt{p}$; posons $m=[\sqrt{p}]$ et considérons le rationnel :

$$a=\frac{1}{m+1}\frac{p-1}{(m+1)^2-1}\cdots\frac{p-k^2}{(m+1)^2-k^2}\cdots\frac{p-m^2}{(m+1)^2-m^2}=\frac{\prod_{k=0}^{m}(p-k^2)}{(2m+1)!}.$$

D'un côté, nous avons $a\in(0,1)$ puisque chacun des facteurs à gauche vérifie cette identité. D'un autre côté, comme $2m+1$ est majoré par p, les seuls nombres premier qui interviennent dans lq factorisation de a sont ceux strictement inférieurs à p ; et pour chacun d'eux p est un carré dans $\mathbb{Z}_q$ (en vertu de la congruence $p\equiv 1 \bmod 8$ pour $q=2$, du lemme de Hensel et de l'hypothèse $\left(\frac{p}{q}\right)=+1$ pour $q\neq 2$). Comme $\mathbb{N}$ est dense dans $\mathbb{Z}_q$, pour chaque $\varepsilon>0$ donné, nous pouvons de ce fait trouver une ε-approximation f^2 de p dans $\mathbb{Z}_q$ avec $f>m$. Il suit :

$$|a-\frac{\prod_{k=0}^{m}(f^2-k^2)}{(2m+1)!}|_q=|a-f\binom{m+f}{2m+1}|_q<1\ \text{ pour }\ \varepsilon<|(2m+1)!|_q.$$

Ainsi a est dans $\mathbb{Z}_q$ (i.e. q-entier) pour tout $q<p$ donc entier : une contradiction. □*Fin de la démonstration :* Procedons par l'absurde en supposant qu'il existe un plus petit premier p avec $\varepsilon_p=0$. Les calculs qui précèdent impliquent alors $p\equiv 1 \bmod 8$, et le lemme 15 nous assure l'existence d'un premier $q<p$, impair, avec $\left(\frac{p}{q}\right)=-1$. Or, p étant un carré dans $\mathbb{Z}_2$, il vient ici :

$$1=\left(\frac{p,q}{\mathbb{Q}_2}\right)=\left(\frac{p,q}{\mathbb{Q}_q}\right)^1\left(\frac{p,q}{\mathbb{Q}_p}\right)^0=\left(\frac{(p,q)_q}{q}\right)=\left(\frac{p}{q}\right),$$

une contradiction. □

Corollaire 28 (Loi de réciprocité quadratique)**.** *Pour* p *et* q *premiers impairs, on a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2}.$$

Preuve : La formule du produit pour les symboles quadratiques sur $\mathbb{Q}$ donne, en effet :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{(p,q)_q}{q}\right)\left(\frac{(p,q)_p}{p}\right) = \left(\frac{p,q}{\mathbb{Q}_q}\right)\left(\frac{p,q}{\mathbb{Q}_p}\right) = \left(\frac{p,q}{\mathbb{Q}_2}\right)$$

— Pour $p \equiv 1 \bmod 4$, nous avons soit $\mathbb{Q}_2[\sqrt{p}] = \mathbb{Q}_2$ (pour $p \equiv 1 \bmod 8$), soit $\mathbb{Q}_2[\sqrt{p}] = \mathbb{Q}_2[\sqrt{5}]$ (pour $p \equiv 5 \bmod 8$), et dans les deux cas, toutes les unités sont normes.
— Pour $p \equiv -1 \bmod 4$, nous avons soit $\mathbb{Q}_2[\sqrt{p}] = \mathbb{Q}_2[i]$ (pour $p \equiv -1 \bmod 8$), soit $\mathbb{Q}_2[\sqrt{p}] = \mathbb{Q}_2[\sqrt{-5}]$ (pour $p \equiv -5 \bmod 8$), et dans les deux cas le sous-groupe des normes dans U_2 est U_2^2.

Il vient donc dans tous les cas :

$$\left(\frac{p,q}{\mathbb{Q}_2}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

comme annoncé. □

Références

[1] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[2] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.