Autour de la thèse de Tate sur les corps de nombres

Arnaud Girand et Aurélien Sagnier

Table des matières

Dans tout ce document, tous les groupes considérés seront supposés abéliens et les anneaux commutatifs unitaires. On désignera par *corps* toute algèbre à division commutative. On appelera norme (ou valeur absolue) sur un corps k toute norme d'algèbre sur $(k, +, \times, .)$.

1 Corps de nombres

1.1 Généralités

Définition 1.1 (Corps de nombres)
On appelle corps de nombres toute extension finie de $\mathbb{Q}$.

On rappelle la caractérisation suivante des entiers (sur $\mathbb{Z}$) d'un corps de nombres :

Proposition 1.1
Soit k un corps de nombres.
Alors $x \in k$ est entier si et seulement si il existe un $\mathbb{Z}$–module de type fini $M \subset k$ tel que $xM \subset M$.

Corollaire 1.1.1
Soit k un corps de nombres.
Alors l'ensemble des entiers de k (sur $\mathbb{Z}$) est un sous–anneau de k.

Dans la suite, nous nous donnons un corps de nombres k et nous noterons $\mathcal{O}$ son anneau des entiers. Remarquons que comme k est un corps et que $1 \in \mathcal{O}$, $\mathcal{O}$ est un anneau intègre.

Proposition 1.2
Le corps des fractions de $\mathcal{O}$ est k.

Démonstration : Comme $\mathcal{O} \subset k$, $\mathrm{Frac}(\mathcal{O}) \subset \mathrm{Frac}(k) = k$. Réciproquement, si on se donne $x \in k$, alors comme x est algébrique sur $\mathbb{Q}$ il existe $a_0, \ldots, a_n \in \mathbb{Z}$ (avec $a_n \neq 0$) tels que :

$$\sum_{i=0}^{n} a_i x^i = 0$$

Et donc $y := a_n x$ est solution de l'équation :

$$y^n \sum_{i=0}^{n-1} a_{n-i}^{n-1-i} a_i y^i = 0$$

Et donc $x = \dfrac{y}{a_n}$ est quotient d'un élément de $\mathcal{O}$ et d'un élément de $\mathbb{Z} \subset \mathcal{O}$, ergo $x \in \mathrm{Frac}(\mathcal{O})$.

Définition 1.2 (Idéal inverse, idéal fractionnaire)
Soient I, J deux idéaux de $\mathcal{O}$.
On définit alors :

$$I^{-1} := \{x \in k \,|\, \forall y \in I,\, xy \in \mathcal{O}\} \text{ et } I/J := I.J^{-1}$$

Nous admettrons ensuite le résultat suivant :

Proposition 1.3 (Groupe des idéaux de k)
L'ensemble des idéaux fractionnaires non triviaux de $\mathcal{O}$ forme un groupe pour la multiplication des idéaux (avec la notion d'inverse introduite en 1.2), d'élément neutre $\mathcal{O}$ et appelé groupe des idéaux de k. De plus, tout idéal fractionnaire non trivial de $\mathcal{O}$ admet une unique factorisation comme produit et quotient (au sens 1.2) d'idéaux premiers de $\mathcal{O}$.

Remarquons que comme $\mathcal{O}$ est unitaire, le produit (resp. l'inverse) de deux idéaux principaux est principal engendré par le produit des générateurs (resp. l'inverse du générateur). Ainsi, l'ensemble des idéaux principaux de $\mathcal{O}$ forme un sous–groupe du groupe des idéaux de k.

Définition 1.3 (Groupe de classes, nombre de classes)
Soit Γ le groupe des idéaux de k.
Soit $H \subset \Gamma$ le sous–groupe des idéaux principaux.
Alors on appelle groupe de classes de k le groupe quotient Γ/H. L'indice $(\Gamma : H)$ est appelé nombre de classes de k.

Définition 1.4 (Différent inverse)
On définit le différent inverse de k comme l'ensemble suivant :

$$\mathcal{D}^{-1} := \{x \in k \,|\, \forall y \in \mathcal{O},\, \mathrm{Tr}(xy) \in \mathbb{Z}\}$$

Proposition 1.4
$\mathcal{D}^{-1}$ est un sous $\mathcal{O}$–module propre de k contenant $\mathcal{O}$.

Démonstration : Soient $a, b \in \mathcal{D}^{-1}$. Alors, si $y \in \mathcal{O}$, $\mathrm{Tr}((a+b)y) = \mathrm{Tr}(ay) + \mathrm{Tr}(by) \in \mathbb{Z}$. De même, si $x \in \mathcal{O}$ alors $\forall y \in \mathcal{O}$, $\mathrm{Tr}(ax.y) \in \mathbb{Z}$ et donc $ax \in \mathcal{D}^{-1}$. Ainsi, Dr^{-1} est un sous $\mathcal{O}$–module de k, qui est propre car si on prend $x \in k$ tel que $[k:\mathbb{Q}]x \notin \mathbb{Z}$ alors $\mathrm{Tr}(x) = [k:\mathbb{Q}]x \notin \mathbb{Z}$. Soit à présent $x \in \mathcal{O}$. Comme $\mathrm{Tr}(x)$ est un multiple entier du second coefficient du polynôme minimal unitaire π de x et que x est entier donc est racine d'un polynôme unitaire f à coefficients dans $\mathbb{Z}$ alors, si l'on note g le produit de π par le ppcm de ses dénominateurs on a $g|f$. Ainsi, par lemme de Gauss, $\dfrac{f}{g} \in \mathbb{Z}[X]$ et donc g est unitaire, ce qui implique que $g = \pi$ et donc que $\mathrm{Tr}(x)$ est entier.

1.2 Normes, complétés

Définition 1.5 (Norme d'un idéal premier)
Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$.
On définit la norme $\mathcal{N}\mathfrak{p}$ de $\mathfrak{p}$ comme étant le cardinal de l'anneau quotient $\mathcal{O}/\mathfrak{p}$.

On étend alors $\mathcal{N}$ à tous les idéaux fractionnaires de $\mathcal{O}$ en tant que morphisme du groupe des idéaux de k. On sait alors que le localisé $\mathcal{O}_\mathfrak{p} := \mathcal{O}[\mathcal{O} \setminus \mathfrak{p}^{-1}]$ est un anneau local, d'unique idéal maximal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Nous admettrons que cet idéal est principal, engendré par un certain élément π.

Définition 1.6 (Norme $\mathfrak{p}$–adique)
Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$.
Soit $x \in k$.
Si on écrit x sous la forme $x = \pi^\nu \dfrac{a}{b}$, avec $a, b \in \mathcal{O} \setminus \mathfrak{p}$ et $\nu \in \mathbb{Z}$ (appelé valuation $\mathfrak{p}$–adique de x) alors on pose $|x|_\mathfrak{p} := \dfrac{1}{\mathcal{N}\mathfrak{p}^\nu}$. Ceci définit une norme sur k, appelée norme $\mathfrak{p}$–adique.

On a alors le résultat suivant :

Proposition 1.5
Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$.
On suppose k complet pour la norme $|.|_\mathfrak{p}$.
Alors tous les sous $\mathcal{O}_\mathfrak{p}$–modules propres de k sont de la forme $\mathfrak{p}^n$, avec $n \in \mathbb{Z}$. En particulier, tous les idéaux de $\mathcal{O}$ sont de la forme $\mathfrak{p}^n$ avec $n \in \mathbb{N}$.

Définition 1.7
On dit qu'un idéal premier $\mathfrak{p}$ de $\mathcal{O}$ est au dessus d'un nombre premier $p \in \mathbb{Z}$ s'il vérifie :

$$\mathfrak{p} \cap \mathbb{Z} = (p)$$

Remarquons que comme $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier, il existe toujours un tel premier p. Il découle de plus de cette définition que si $\mathfrak{p}$ est au dessus de p alors la restriction à $\mathbb{Q}$ de la norme $\mathfrak{p}$–adique est égale (à une puissance près) à la norme p–adique. Ainsi, les deux normes précitées induisent sur $\mathbb{Q}$ une même topologie et donc si l'on note $k_\mathfrak{p}$ (respectivement $\mathbb{Q}_p$) le complété de k (resp. $\mathbb{Q}$) pour la norme $\mathfrak{p}$–adique (resp. p–adique) alors $\mathbb{Q}_p \subset k_\mathfrak{p}$. On peut donc définir une trace $\mathrm{Tr} : k_\mathfrak{p} \to \mathbb{Q}_p$.

Définition 1.8 (Différent inverse local)
Soit $\mathfrak{p}$ un idéal premier au dessus d'un premier $p \in \mathbb{Z}$.
On définit le différent inverse local de $k_\mathfrak{p}$ comme l'ensemble suivant :

$$\mathcal{D}_\mathfrak{p}^{-1} := \{x \in k_\mathfrak{p} \,|\, \forall y \in \mathcal{O}_\mathfrak{p},\, \mathrm{Tr}(xy) \in O_p\}$$

Où O_p est l'anneau des entiers de $\mathbb{Q}_p$ (appelés entiers p–adiques).

On montre de façon analogue à ce qui a été fait pour le différent inverse la proposition suivante :

Proposition 1.6
Soit $\mathfrak{p}$ un idéal premier au dessus d'un premier $p \in \mathbb{Z}$.
Alors $\mathcal{D}^{-1}$ est un sous $\mathcal{O}_\mathfrak{p}$–module propre de $k_\mathfrak{p}$ contenant $\mathcal{O}_\mathfrak{p}$.

Définition 1.9 (Idéal premier ramifié)
Un idéal premier $\mathfrak{p}$ de $\mathcal{O}$ est dit ramifié si pour tout $p \in \mathbb{Z}$ premier tel que $\mathfrak{p}$ soit au dessus de p on a :

$$\mathfrak{p}^2 \cap \mathbb{Z} \neq (p)$$

2 Théorie locale

Dans ce paragraphe, nous nous intéresserons à un complété k d'un corps de nombres pour une certaine norme $|.|$. Pour simplifier les notations dans le cas $\mathfrak{p}$–adique, nous dénoterons les ensembles $\mathcal{O}_\mathfrak{p}$ et $\mathcal{D}_\mathfrak{p}^{-1}$ par $\mathcal{O}$ et $\mathcal{D}^{-1}$. Nous noterons également k^+ (resp. k^* le groupe $(k, +)$ (resp $(k \setminus \{0\}, \times)$).

2.1 Caractères additifs

Définition 2.1 (Caractère)
Soit G un groupe topologique.
On appelle caractère de G tout morphisme de groupe continu $\chi : G \to \mathbb{S}^1$.

Afin de ne pas surcharger le lecteur et le présent document, nous admettrons les résultats suivants (cf [RV99] pour une démonstration) :

Proposition 2.1
Soit G un groupe localement compact.
Alors l'ensemble des caractères de G forme un groupe (multiplicatif) localement compact, noté $\widehat{G}$.

Proposition 2.2 (Dualité de Pontryagin)
Soit G un groupe localement compact.
Alors :

$$\widehat{\widehat{G}} \cong G$$

Plus précisément, l'application suivante est un isomorphisme :

$$\begin{aligned} G &\to \widehat{\widehat{G}} \\ y &\mapsto (\chi \mapsto (x \mapsto \chi(x.y))) \end{aligned}$$

Intéressons–nous à présent aux caractères additifs de k, i.e aux caractères du groupe k^+.

Proposition 2.3
Le groupe $\widehat{k^+}$ est non trivial.

Démonstration : k est un complété d'un corps de nombres : nous allons donc construire un caractère non trivial pour chaque grand "type" de complété : réel, complexe ou $\mathfrak{p}$–adique. On va chercher ce caractère sous la forme $x \mapsto e^{-2i\pi f(x)}$, avec $f : k \to \mathbb{R}$ continue, non triviale et additive.
- Si k est réel, $f : x \mapsto -x$ convient.
- Si k est complexe, $f : x \mapsto -2\Re(x)$ convient.
- Si k est $\mathfrak{p}$–adique, avec $\mathfrak{p}$ situé au dessus du premier p, alors k est une extension finie de $\mathbb{Q}_p$. De plus, si $x \in \mathbb{Q}_p$, il admet une décomposition p–adique :

$$x = \sum_{i=\nu}^{\infty} a_j p^j, \quad \nu \in \mathbb{Z}$$

On peut alors définir une application continue additive λ sur $\mathbb{Q}_p$ par la formule :

$$\lambda(x) = \sum_{i=\nu}^{-1} a_j p^j$$

Et donc $f := \lambda \circ \mathrm{Tr}$ convient.

Proposition 2.4
Les groupes k^+ et $\widehat{k^+}$ sont isomorphes aux sens algébrique et topologique, i.e il existe un isomorphisme de groupes bicontinu $\phi : k^+ \to \widehat{k^+}$.

Démonstration : Considérons l'application suivante :

$$\begin{aligned} \phi : k^+ &\to \widehat{k^+} \\ \eta &\mapsto \chi(\eta.) \end{aligned}$$

Où χ est un caractère non trivial de k^+. Comme χ est un morphisme de groupes, il est clair que ϕ en est également un.

De plus, comme χ est non trivial et que $\forall \eta \in k$, $\eta.k = k$, ϕ est injective. Posons à présent $H := \mathrm{Im}(\phi)$ et soit $I := \overline{H}$ son adhérence dans $\widehat{k^+}$. On obtient ainsi un groupe topologique (muni de la topologie quotient) $\widehat{k^+}/I$. Supposons que $I \neq k^+$: il existe alors un caractère θ non trivial de $\widehat{k^+}$ qui est trivial sur I. Par dualité de Pontryagin, il existe $y \in k^+$ tel que $\forall x \in k$, $\chi(xy)$ soit trivial ce qui n'est possible que si $y = 0$ car $y.k = k$. Ergo, toujours par dualité de Pontryagin, $\forall \kappa \in \widehat{k^+}$, $\theta(\kappa) = \kappa(0.) = 1$ et donc θ est trivial, ce qui est absurde. De fait $I = \widehat{k^+}$, i.e H est dense dans $\widehat{k^+}$.

La démonstration de la bicontinuité de ϕ nécessite de détailler la topologie compacte–ouverte sur $\widehat{k^+}$, ce que nous ne ferons pas ici. On déduit de cette bicontinuité que H est localement compact et donc fermé, ce qui achève la démonstration de la surjectivité.

Proposition 2.5
On se place dans le cas où $|.|$ est $\mathfrak{p}$–adique, avec $\mathfrak{p}$ au dessus de p.
Soit χ un caractère non–trivial sur $\widehat{k^+}$. Alors pour tout $\eta \in \mathcal{O}$, le caractère $\chi(\eta.)$ est trivial sur $\mathcal{D}^{-1}$.

Démonstration : Remarquons que pour tout $y \in k$, si $\mathrm{Tr}(y) \in O_p$ alors $\chi(y) = 1$ et donc si $x \in \mathcal{D}^{-1}$ et $\eta \in \mathcal{O}$ alors $\chi(\eta x) = 1$.

Définition 2.2 (Différent (local))
On définit le différent (différent local dans le cas $\mathfrak{p}$–adique) comme l'idéal $\mathcal{D} := (\mathcal{D}^{-1})^{-1}$.

2.2 Mesures de Haar

Définition 2.3 (Mesure de Haar)
Soit G un groupe localement compact.
On appelle mesure de Haar sur G toute mesure μ sur G telle que :

(i) pour tout ouvert $O \neq \emptyset$ de G, $\mu(G) > 0$;
(ii) pour tout compact K de G, $\mu(K) < \infty$;
(iii) μ est invariante par translation, i.e :

$$\forall E \in \mathcal{B}(G), \forall s \in G, \mu(s.E) = \mu(E)$$

Où $\mathcal{B}(G)$ dénote la tribu borélienne sur G.

Nous admettrons le résultat suivant (cf [RV99] pour une preuve) :

Proposition 2.6
Soit G un groupe localement compact.
Alors G admet une unique (à constante multiplicative près) mesure de Haar.

Donnons–nous une mesure de Haar μ sur k^*. On peut alors vérifier que la formule suivante définit bien une norme sur k : étant donné un borélien M de k, on définit $|x|$ comme étant l'unique réel positif vérifiant $\mu(xM) = |x|\mu(M)$. Avec ce fait en tête particularisons la norme $|.|$ que nous nous étions donné précédemment pour qu'elle coïncide avec celle ci :
- si k est réel, on fixe $|.|$ comme étant la valeur absolue usuelle sur $\mathbb{R}$;
- si k est complexe, on prend pour $|.|$ le carré du module usuel sur $\mathbb{C}$;
- si k est $\mathfrak{p}$–adique, on conserve la définition vu précédemment (définition 1.6).

Dans toute la suite, nous nous fixons une mesure de Haar dx sur k^+ :
- si k est réel, dx sera la mesure de Lebesgue sur $\mathbb{R}$;
- si k est complexe, dx sera deux fois la mesure de Lebesgue sur $\mathbb{C}$;
- si k est $\mathfrak{p}$–adique, dx sera la mesure de Haar sur k telle que $dx(\mathcal{O}) = \dfrac{1}{\sqrt{\mathcal{N}\mathcal{D}}}$.

Proposition 2.7
La mesure $\mu^* : M \mapsto \int_M \frac{dx}{x}$ est une mesure de Haar sur k^*.

DÉMONSTRATION : Comme $\forall x \in k, \forall M \in \mathcal{B}(k)$, $\mu(xM) = |x|\mu(M)$ on a :

$$\forall a \in k \setminus \{0\}, \int_M f(x)\frac{dx}{|x|} = |a| \int_M f(ax)\frac{dx}{|ax|} = \int_M f(ax)\frac{dx}{|x|}$$

On obtient donc le résultat en posant $f = 1_M$.

Pour k réel ou complexe (on dit aussi archimédien), on définit ainsi une mesure de Haar $d^*x := \dfrac{dx}{|x|}$ sur le groupe k^*. Dans le cas $\mathfrak{p}$–adique, les choses sont un peu plus complexes et il nous faut poser $d^*x := \dfrac{\mathcal{N}\mathfrak{p}}{\mathcal{N}\mathfrak{p} - 1}\dfrac{dx}{|x|}$.

2.3 Analyse de Fourier sur k

Pour commencer, rappelons les bases de l'analyse de Fourier sur les groupes localement compacts. Les démonstrations pourront être trouvées dans [RV99].

Définition 2.4 (Transformée de Fourier)
Soit G un groupe localement compact.
Soit χ un caractère non trivial de G.
Soit $f \in L^1(G)$.
On définit alors la transformée de Fourier de f par la formule suivante ($y \in G$) :

$$\widehat{f}(y) = \int_G f(x)\chi(xy)dx$$

Proposition 2.8
Soit G un groupe localement compact.
Soit $f \in L^1(G)$.
Alors, si $\widehat{f} \in L^1(G)$ il existe une constante n indépendante de f telle que :

$$\forall x \in G, \, \widehat{\widehat{f}}(x) = nf(-x)$$

Revenons en à notre corps k et à la mesure de Haar dx introduite précédemment. On fixe également dans toute la suite un caractère non trivial $\chi \in \widehat{k^+}$.

Proposition 2.9
Soit $f \in L^1(k)$.
On suppose que $\widehat{f} \in L^1(k)$.
Alors $\forall x \in k$, $\widehat{\widehat{f}}(x) = f(-x)$.

2.4 Caractères multiplicatifs

Définition 2.5 (Quasi–caractère, caractère unitaire)
On appelle quasi-caractère (multiplicatif) tout morphisme continu $\chi : k^* \to \mathbb{C}^*$. Un tel caractère est dit unitaire si c'est un caractère au sens précédent, i.e si $\chi(k^*) \subset \mathbb{S}^1$.

Dans toute la suite, nous noterons $\mathcal{U}$ l'ensemble des éléments de norme 1 dans k.

Définition 2.6 (Quasi–caractère ramifié)
Un quasi–caractère est dit ramifié si il est non trivial sur $\mathcal{U}$.

Proposition 2.10 (Classification des quasi–caractères non ramifiés)
Les quasi–caractères non ramifiés sont exactement ceux de la forme $x \mapsto |x|^s$, où $s \in \mathbb{C}$ est uniquement (resp à un multiple entier de $\frac{2i\pi}{\log(\mathcal{N}\mathfrak{p})}$ près) déterminé dans le cas archimédien (resp. $\mathfrak{p}$–adique).

Démonstration : Il est clair que les $x \mapsto |x|^s$ sont triviaux sur $\mathcal{U}$. Réciproquement, si c est un quasi–caractère trivial sur $\mathcal{U}$ alors il est constant sur tous les ensembles de la forme $\{|.| = a\}$ ($a \in \mathbb{R}_+$) et donc c est en fait un caractère sur le groupe $\{x \in \mathbb{R}_+ \mid \exists y \in k^*, |y| = x\}$. Dans le cas archimédien, ce groupe est $\mathbb{R}_+^*$, dont les quasi–caractères sont bien ceux de la forme $x \mapsto |x|^s$, tandis que dans le cas $\mathfrak{p}$–adique il s'agit de l'ensemble des puissances entières de $\mathcal{N}\mathfrak{p}$. De fait, les quasi–caractères doivent bien être de la forme spécifiée et :

$$\begin{aligned}\forall x \in k^*, \forall s \in \mathbb{C}, \forall k \in \mathbb{Z},\ |x|^{s+\frac{2ik\pi}{\log(\mathcal{N}\mathfrak{p})}} &= |x|^s |x|^{\frac{2ik\pi}{\log(\mathcal{N}\mathfrak{p})}} \\ &= |x|^s (\mathcal{N}\mathfrak{p})^{n\frac{2ik\pi}{\log(\mathcal{N}\mathfrak{p})}} \text{ pour un certain } n \in \mathbb{Z} \\ &= |x|^s e^{n\frac{2ik\pi}{\log(\mathcal{N}\mathfrak{p})}\log(\mathcal{N}\mathfrak{p})} \\ &= |x|^s\end{aligned}$$

D'où le résultat.

D'un point de vue géométrique, l'espace des quasi–caractères non–ramifiés s'apparente donc au plan complexe dans le cas archimédien et à un cylindre infini dans le cas $\mathfrak{p}$–adique.

Définition 2.7
Soient c, d deux quasi–caractères.
On dit que c et d sont équivalents, ce que l'on note $c \sim d$, si et seulement si le quotient $\dfrac{c}{d}$ est non ramifié.

Il est clair que l'on définit ainsi une relation d'équivalence et pour décrire les classes d'équivalences il nous suffit d'examiner la façon dont les quasi–caractères agissent sur $\mathcal{U}$: en effet, si $x \in k^*$ alors $\dfrac{x}{|x|}$ (dans le cas réel), $\dfrac{x}{\sqrt{|x|}}$ (dans le cas complexe) ou $\dfrac{x}{\pi^\nu}$ (où ν est la valuation $\mathfrak{p}$–adique de x) dans le cas $\mathfrak{p}$–adique est un élément de $\mathcal{U}$. Si on se donne un quasi–caractère c de restriction $\tilde{c}$ à $\mathcal{U}$ (qui constitue un caractère au sens classique de $\mathcal{U}$) alors $\dfrac{c}{\tilde{c}}$ est non ramifié et donc est de la forme $|.|^s$. Ainsi, l'espace des quasi–caractères est une collection de copies de $\mathbb{C}$ ou d'un cylindre infini indexées par les caractères de $\mathcal{U}$.

Proposition 2.11 (Exposant d'un quasi–caractère)
Soit c un quasi–caractère.
Alors il existe $\sigma \in \mathbb{R}$, appelé exposant de c, tel que :

$$\forall x \in k^*,\ |c(x)| = |x|^\sigma$$

Démonstration : D'après la digression précédente, $\forall x \in k^*$, $|c(x)| = |\tilde{c}(x)||x|^s| = ||x|^s| = |x|^{\Re(s)}$. Il nous suffit donc de poser $\sigma = \Re(s)$.

Examinons donc les caractères de $\mathcal{U}$.

- Dans le cas réel, $\mathcal{U} = \{-1, 1\}$ et donc il n'existe que deux caractères sur $\mathcal{U}$: le caractère trivial et l'identité. L'espace des quasi–caractères est donc isomorphe à deux copies du plan complexe, i.e à $\mathbb{C} \times \mathbb{C}$.
- Dans le cas complexe, $\mathcal{U} = \mathbb{S}^1$ et donc les caractères sur $\mathcal{U}$ sont de la forme $x \mapsto e^{2i\pi nx}$, pour $n \in \mathbb{Z}$. Ergo l'espace des quasi–caractères est isomorphe à $\mathbb{Z} \times \mathbb{C}$.
- Dans le cas $\mathfrak{p}$–adique, commençons par remarquer que les ensembles $1 + \mathfrak{p}^n$ pour $n \geq 1$ sont des sous–groupes de $\mathcal{U}$. Fixons $\tilde{c}$ un caractère de $\mathcal{U}$. Alors pour tout voisinage de 1 dans $\mathbb{C}$ ne contenant aucun sous–groupe multiplicatif de $\mathbb{C}^*$ et pour n assez grand $\tilde{c}(1 + \mathfrak{p}^n)$ se trouve dans ce voisinage et donc doit être égal à 1. Soit n le plus petit entier tel que cette égalité soit réalisée : $\mathfrak{p}^n$ est alors appelé conducteur de $\tilde{c}$. L'ensemble des caractères de conducteur $\mathfrak{p}^n$ est en fait l'ensemble des caractères du groupe quotient $\mathcal{U}/(1 + \mathfrak{p}^n)$. Ce groupe étant fini, il n'y a qu'un nombre fini de tels caractères et comme il n'y a qu'un nombre dénombrable de possibilités pour le conducteur, il n'existe au final qu'un nombre dénombrable de caractère de $\mathcal{U}$. Ainsi l'espace des quasi–caractères est isomorphe à un produit dénombrable de cylindres infinis.

2.5 Fonctions Zêta locales

Définition 2.8 (Espace de Schwartz–Bruhat)
L'espace de Schwartz–Bruhat sur k^*, noté $\mathcal{S}$, est l'espace de Schwartz (resp. l'espace des fonctions $\mathcal{C}^\infty$ à support compact) sur k^* dans le cas où k est archimédien (resp. $\mathfrak{p}$–adique).

Définition 2.9 (Fonction Zêta locale)
Soit $f : k^* \to \mathbb{C}$ une fonction de $\mathcal{S}$.
Soit c un quasi–caractère d'exposant strictement positif.
On définit alors :

$$\zeta(f,c) := \int_{k^*} f(x)c(x)d^*x$$

Définition 2.10 (Quasi–caractère inverse)
Soit c un quasi–caractère.
Alors on définit son quasi–caractère inverse comme étant le quasi–caractère $\widehat{c}$ défini sur k^* par :

$$\widehat{c}(x) = \frac{|x|}{c(x)}$$

Il est alors clair que si c est d'exposant σ, $\widehat{c}$ est d'exposant $1-\sigma$.

Proposition 2.12
Soient $f, g \in \mathcal{S}$.
Soit c un quasi–caractère d'exposant $\sigma \in (0,1)$.
Alors :

$$\zeta(f,c)\zeta(\widehat{g},\widehat{c}) = \zeta(g,c)\zeta(\widehat{f},\widehat{c})$$

En particulier, il existe une application ρ indépendante de f telle que :

$$\zeta(f,c) = \rho(c)\zeta(\widehat{f},\widehat{c})$$

Démonstration : On a :

$$\begin{aligned}
\zeta(f,c)\zeta(\widehat{g},\widehat{c}) &= \int_{k^*} f(x)c(x)d^*x \int_{k^*} \widehat{g}(y)\frac{|y|}{c(y)}d^*y \\
&= \int_{k^*} f(x)c(x) \int_{k^*} \widehat{g}(xy)\frac{|xy|}{c(xy)}d^*yd^*x \text{ par changement de variable } y \mapsto xy \text{ ("}d^*(xy) = d^*y\text{")} \\
&= \int_{k^*}\int_{k^*} f(x)\widehat{g}(xy)c(y^{-1})|xy|d^*yd^*x \\
&= \int_{k^*}\int_{k^*} f(x)\left(\int_{k^*} g(z)\chi(xyz)dz\right)c(y^{-1})|xy|d^*yd^*x
\end{aligned}$$

D'après les discussions précédents, $dz = K|z|d^*z$, avec K ne dépendant que de k. Ergo :

$$\begin{aligned}
\zeta(f,c)\zeta(\widehat{g},\widehat{c}) &= K\int_{k^*}\left(\int_{k^*}\int_{k^*} f(x)g(z)\chi(xyz)|xz|d^*xd^*z\right)|y|d^*y \\
&= K\int_{k^*}\int_{k^*} \widehat{f}(yz)g(z)|yz|c(y^{-1})d^*yd^*z \\
&= \zeta(g,c)\zeta(\widehat{f},\widehat{c})
\end{aligned}$$

Comme $\widehat{c}$ est un quasi–caractère d'exposant $1-\sigma$ et que la formule précédente est valable pour $0 < \sigma < 1$ alors ce théorème nous permet de prolonger "de façon analytique" nos fonctions ζ locales à l'espace de tous les quasi–caractères. Le tout est à présent de savoir calculer ρ, ce à quoi nous allons à présent nous attacher.

Les calculs qui suivent seront menés dans le cas $\mathfrak{p}$–adique, où ils sont les plus intéressants. On rappelle que $dx(\mathcal{O}) = \sqrt{\mathcal{N}\mathcal{D}}$ et que $d^*x(\mathcal{U}) = \sqrt{\mathcal{N}\mathcal{D}}$. Soit c' un caractère unitaire de conducteur $\mathfrak{p}^n$: alors c' est équivalent à un caractère unitaire c de même conducteur et vérifiant $c(\pi) = 1$. On cherche ici à calculer $\rho(c) = \dfrac{\zeta(f,c)}{\zeta(\widehat{f},\widehat{c})}$. Comme cette quantité est indépendant de f, nous pouvons nous permettre de prendre f suffisamment simple. Par exemple, posons :

$$f_n(x) := \begin{cases} \chi(-x) & \text{si } x \in \mathcal{D}^{-1}\mathfrak{p}^{-n} \\ 0 & \text{sinon} \end{cases}$$

Alors, pour $x \in k^*$, on a :

$$\widehat{f_n}(x) = \int_{\mathcal{D}^{-1}\mathfrak{p}^{-n}} \chi(y(x-1))dy$$

Cette intégrale est nulle si $\chi((x-1).)$ est non–trivial sur $\mathcal{D}^{-1}\mathfrak{p}^{-n}$, i.e d'après la proposition 2.5, quand $(x-1)\mathfrak{p}^{-n} \not\subset \mathcal{O}$, i.e quand $x \notin \mathfrak{p}^n + 1$. Dans le cas contraire, comme le caractère est trivial, $\widehat{f_n}(x) = dx(\mathcal{D}^{-1}\mathfrak{p}^{-n})$. In fine, on a :

$$\widehat{f_n}(x) := \begin{cases} \dfrac{1}{\sqrt{\mathcal{N}\mathcal{D}}(\mathcal{N}\mathfrak{p})^n} & \text{si } x \in \mathfrak{p}^n + 1 \\ 0 & \text{sinon} \end{cases}$$

Pour la suite des calculs, il est utile de remarquer que si on pose $A_\nu := \{|.| = (\mathcal{N}\mathfrak{p})^{-\nu}\}$ alors :

$$k^* = \bigsqcup_{\nu \in \mathbb{Z}} A_\nu \text{ constitue une partition de } k^*$$

De plus, pour tout $\nu \in \mathbb{Z}$, $d^*x(A_\nu) = \dfrac{1}{\sqrt{\mathcal{N}\mathcal{D}}}$. Calculons à présent ρ sur chaque classe d'équivalence pour $\sim$, i.e pour chaque valeur de conducteur $\mathfrak{p}^n$. Commençons par le cas des caractères non ramifiés, i.e de la forme $|.|^s$ (et $n = 0$). Dans ce cas, f_0 est exactement la fonction caractéristique de $\mathcal{D}^{-1}$. On sait de plus qu'il existe d tel que $\mathcal{D} = \mathfrak{p}^d$, et donc $\mathcal{D}^{-1} = \mathfrak{p}^{-d} = \cup_{\nu \geq -d} A_\nu$. Ainsi :

$$\begin{aligned}
\zeta(f_0, |.|^s) &= \sum_{\nu=-d}^{\infty} \int_{A_\nu} |x|^s d^*x \\
&= \sum_{\nu=-d}^{\infty} \frac{1}{\sqrt{\mathcal{N}\mathcal{D}}(\mathcal{N}\mathfrak{p})^{\nu s}} \\
&= \frac{(\mathcal{N}\mathfrak{p})^{ds}}{1 - \dfrac{1}{\mathcal{N}\mathfrak{p}^s}} \frac{1}{\sqrt{\mathcal{N}\mathcal{D}}} \\
&= \frac{(\mathcal{N}\mathcal{D})^{s-\frac{1}{2}}}{1 - \dfrac{1}{(\mathcal{N}\mathfrak{p})^s}}
\end{aligned}$$

Or $\widehat{f_0}$ est égale à $\sqrt{\mathcal{N}\mathcal{D}}$ fois la fonction caractéristique de $\mathcal{O}$ et $\widehat{|.|^s} = |.|^{1-s}$ donc on a :

$$\begin{aligned}
\zeta(\widehat{f_0}, \widehat{|.|^s}) &= \sqrt{\mathcal{N}\mathcal{D}} \int_{\mathcal{O}} |x|^{1-s} d^*x \\
&= \sum_{\nu=0}^{\infty} (\mathcal{N}\mathfrak{p})^{(s-1)\nu} \\
&= \frac{1}{1 - (\mathcal{N}\mathfrak{p})^{s-1}}
\end{aligned}$$

Ce qui nous permet donc de conclure la détérmination de ρ dans ce cas précis :

$$\rho(|.|^s) = (\mathcal{N}\mathcal{D})^{s-\frac{1}{2}} \frac{1 - (\mathcal{N}\mathfrak{p})^{s-1}}{1 - (\mathcal{N}\mathfrak{p})^{-s}}$$

Soit à présent un quasi–caractère (ramifié) c de conducteur $\mathfrak{p}^n$. Comme on travaille modulo $\sim$, on peut de plus supposer que $c(\pi) = 1$. Alors :

$$\begin{aligned}
\zeta(f_n, c|.|^s) &= \int_{\mathcal{D}^{-1}\mathfrak{p}^{-n}} \chi(-x)c(x)|x|^s d^*x \\
&= \sum_{\nu=-(d+n)}^{\infty} \frac{1}{(\mathcal{N}\mathfrak{p})^{\nu s}} \int_{A_\nu} \chi(-x)c(x) d^*x
\end{aligned}$$

Nous nous proposons à présent de démontrer la propriété suivante :

$$\forall \nu > -(d+n), \qquad \int_{A_\nu} \chi(-x)c(x)d^*x = 0$$

- Si $\nu \geq -d$, alors $A_\nu \subset \mathcal{D}^{-1}$ donc χ est trivial sur A_ν. Par changement de variable $x \mapsto \pi^\nu x$ on obtient, comme $c(\pi) = 1$, que :

$$\int_{A_\nu} \chi(-x)c(x)d^*x = \int_{A_\nu} c(x)d^*x = \int_{\mathcal{U}=A_0} c(\pi^\nu x)d^*x = \int_{\mathcal{U}} c(x)d^*x$$

  Or c est non trivial sur $\mathcal{U}$ donc cette intégrale est nulle.
- Si $-(d+n) < \nu < -d$, alors comme on peut écrire A_ν comme réunion disjointe de boules $x_0 + \mathcal{D}^{-1} = x_0(1+\mathfrak{p}^{-d-\nu})$. Or χ est constant sur de tels sous–ensembles donc :

$$\int_{x_0+\mathcal{D}^{-1}} \chi(-x)c(x)d^*x = \chi(-x_0)\int_{x_0+\mathcal{D}^{-1}} c(x)d^*x$$

  Par changement de variable $x \mapsto x_0.x$ on obtient alors :

$$\int_{x_0+\mathcal{D}^{-1}} c(x)d^*x = c(x_0)\int_{1+\mathfrak{p}^{-d-\nu}} c(x)d^*x$$

  Et cette dernière intégrale est nulle car c est non trivial sur $1+\mathfrak{p}^{-d-\nu}$.

On a donc démontré qu'il existe une constante $z_c := \int_{A_{-(d+n)}} \chi(-x)c(x)d^*x \in \mathbb{C}$ telle que :

$$\zeta(f_n, c|.|^s) = (\mathcal{N}\mathfrak{p})^{(d+n)^s} z_c$$

Étant donné que $\widehat{f_n}$ est égale à $\dfrac{1}{\sqrt{\mathcal{N}\mathcal{D}}(\mathcal{N}\mathfrak{p})^n}$ fois la fonction caractéristique de $1+\mathfrak{p}^n$, qui lui–même est un sous–groupe sur lequel c est constant, on a :

$$\begin{aligned}\zeta(\widehat{f_n}, \widehat{c|.|^s}) &= \frac{1}{\sqrt{\mathcal{N}\mathcal{D}}(\mathcal{N}\mathfrak{p})^n}\int_{1+\mathfrak{p}^n} c(x^{-1})|x|^{1-s}d^*x \\ &= \frac{1}{\sqrt{\mathcal{N}\mathcal{D}}(\mathcal{N}\mathfrak{p})^n}\int_{1+\mathfrak{p}^n} d^*x \\ &= \frac{1}{\sqrt{\mathcal{N}\mathcal{D}}}\end{aligned}$$

Ainsi on a :

$$\rho(c|.|^s) = (\mathcal{N}\mathcal{D})^{s-\frac{1}{2}}(\mathcal{N}\mathfrak{p}^n)^s z_c = \mathcal{N}(\mathcal{D}\mathfrak{p}^n))^{s-\frac{1}{2}}(\mathcal{N}\mathfrak{p})^{-\frac{n}{2}} z_c$$

On fait alors usage du lemme technique suivante, dont on trouvera une démonstration dans [RV99] :

Lemme 2.1
Tout quasi–caractère d'exposant $\frac{1}{2}$ vérifie $|\rho(c)| = 1$.

En particulier, on en déduit que $z_c \neq 0$. En effet, comme $c|.|^{\frac{1}{2}}$ est d'exposant $\dfrac{1}{2}$ on a $1 = |\rho(c|.|^{\frac{1}{2}}) = (\mathcal{N}\mathfrak{p})^{-\frac{n}{2}} z_c$.

Nous ne mènerons pas ici les calculs pour le cas archimédien, nous contentant d'en donner les résultats :

- Dans le cas réel, il n'y a que deux classes d'équivalences. Dans le cas non ramifié on trouve :

$$\rho(|.|^s) = \frac{2^{1-s}}{\pi^s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)$$

  Tandis que dans le cas ramifié on a (i.e pour c tel que $c(-1) = -1$) :

$$\rho(c|.|^s) = i\frac{2^{1-s}}{\pi^s}\sin\left(\frac{\pi s}{2}\right)\Gamma(s)$$

- Dans le cas complexe on peut indexer les classes d'équivalences par les caractères $c_n : z \in \mathbb{S}^1 \mapsto z^n$ $(n \in \mathbb{Z})$ et on a :

$$\rho(c_n|.|^s) = (-i)^{|n|}\frac{(2\pi)^{1-s}\Gamma\left(s+\frac{|n|}{2}\right)}{(2\pi)^s\Gamma\left((1-s)+\frac{|n|}{2}\right)}$$

3 Produit direct restreint

3.1 Définition, topologie

Définition 3.1 (Produit direct restreint)
Soit $(G_i)_{i\in I}$ une famille de groupes localement compacts possèdant presque tous un sous–groupe H_i à la fois ouvert et compact.
On définit alors le produit direct restreint des G_i selon les H_i comme suit :

$$G = \prod_{i\in I}{}' G_i := \{(x_i)_{i\in I} \mid \text{ les } x_i \in G_i \text{ et pour presque tout } i \ x_i \in H_i\}$$

Examinons à présent la topologie d'un tel groupe G. Si $S \subset I$ est un ensemble fini alors on note G_S l'ensemble des éléments x de G tels que $\forall i \in S$, $x_i \notin H_i$. G_S est alors homéomorphe au produit $\prod_{i\in S} G_i \times \prod_{i\notin S} H_i$. Or $\prod_{i\in S} G_i$ est localement compact et $\prod_{i\notin S} H_i$ est compact d'après le théorème de Tychonoff, ergo G_S est localement compact. De plus, G_S est également ouvert et :

$$G = \bigcup_{S\subset I \text{ fini}} G_S$$

Tous les G_S étant munis de la topologie produit, on en déduit une topologie sur G tout entier pour laquelle il est localement compact.

Proposition 3.1
La famille constituée des rectangles $N = \prod_i N_i$ telle que pour tout i N_i soit un ouvert contenant 1 et que $N_i = H_i$ pour presque tout i est une base de voisinages de 1 dans G.

Démonstration : Par construction de la topologie sur G il nous suffit de vérifier que si $S \subset I$ est fini alors la famille des tels rectangles N tels que $\{i \in I \mid N_i \neq H_i\} \subset S$ est une base de voisinages de 1 dans G_S, ce qui est clair car G_S est muni de la topologie produit. Notons que l'on peut également démontrer que ces rectangles sont ouverts dans G.

On démontre selon le même schéma la proposition suivante :

Proposition 3.2
Un sous ensemble de G est relativement compact si et seulement si il est inclus dans un rectangle de la forme $\prod_i B_i$, où les B_i sont compacts et presques tous égaux à H_i

3.2 Caractères sur un produit direct restreint

On se donne à nouveau un produit direct restreint G. Si $S \subset I$ est fini alors on note G^S le sous–groupe de G_S constitué des éléments x tels que $\forall i \in S$, $x_i = 1$. G^S est alors isomorphe au produit $\prod_{i\notin S} H_i$ et on a :

$$G_S = G^S \times \prod_{i\in S} G_i$$

Pour tout quasi–caractère c sur G, on notera c_i ses restrictions aux G_i.

Lemme 3.1
Soit c un quasi–caractère sur G.
Alors c_i est trivial sur H_i pour presque tout i et on a :

$$\forall x \in G, \quad c(x) = \prod_{i\in I} c_i(x_i)$$

Notons que le produit est bien défini car les c_i sont presques tous triviaux sur les H_i.

Démonstration : Soit U un voisinage de 1 dans $\mathbb{C}^*$. On peut choisir U suffisamment petit pour qu'aucun sous–groupe non trivial de $\mathbb{C}^*$ ne soit contenu dans U et alors, par continuité de c, il existe un rectangle (au sens de la proposition 3.1) $N = \prod_i N_i$ tel que $c(N) \subset U$. Comme $N_i = H_i$ pour presque tout i alors il existe $S \subset I$ fini tel que $G^S \subset N$ et comme G^S est un sous–groupe de G on doit avoir $c(G_S) = \{1\}$. En particulier, pour tout $i \notin S$ on a $c_i(H_i) = \{1\}$. Pour obtenir la formule qui clôt ce lemme, on écrit $x \in G$ sous la forme $x = x^S \prod_{i\in S} x_i$, avec $x^S \in G^S$.

Lemme 3.2
Soit $(c_i)_i$ une famille de caractères sur $(G_i)_i$ telle que pour presque tout i c_i soit trivial sur H_i. Alors la formule suivante définit un quasi caractère sur G :

$$c(x) = \prod_{i \in I} c_i(x_i)$$

DÉMONSTRATION : Pour $x \in G$, $x_i \in H_i$ pour presque tout i et donc $c_i(x_i) = 1$ pour presque tout i, donc c est bien défini et est un morphisme de groupes. Pour démontrer la continuité de c, il nous suffit de démontrer sa continuité en 1. On se donne un ensemble fini S contenant les indices i pour lesquels c_i est non trivial sur H_i et on considère un voisinage U de 1 dans $\mathbb{C}^*$ et soit A un ensemble tel que $A^{\mathrm{card}(S)} \subset U$. Pour $i \in S$, comme c_i est continu, il existe un ouvert N_i tel que $c_i(N_i) \subset A$. En posant $N = \prod_{i \in S} N_i \prod_{i \notin S} H_i$, on a bien $c(N) \subset U$ et donc c est continu.

Étudions à présent les caractères unitaires de G. Remarquons tout d'abord que c est un tel caractère si et seulement si tous les c_i associés sont des caractères unitaires de G_i. Notons H_i^* le sous–groupe de $\widehat{G_i}$ formé des caractères qui sont triviaux sur H_i. On a alors :

$$H_i^* \cong \widehat{G_i/H_i} \text{ et } \widehat{H_i} \cong \widehat{G_i}/H_i^*$$

En particulier, on peut démontrer à partir de ces relations que H_i^* est à la fois ouvert et compact (une fois n'est pas coutume, [RV99] propose une démonstration de ce résultat).

Proposition 3.3
Le groupe $\widehat{G}$ est isomorphe (algébriquement et topologiquement) au produit direct des $\widehat{G_i}$ selon les H_i^*.

DÉMONSTRATION : On considère l'application $\phi : c \in \widehat{G} \mapsto (x \mapsto \prod_i c_i(x_i))$. D'après les deux lemmes précédents, cette application est un isomorphisme de groupes. La démonstration de la bicontinuité de ϕ faisant appel à la topologie compacte–ouverte sur $\widehat{G}$, nous renvoyons le lecteur à [RV99] pour la preuve complète.

3.3 Mesure

On souhaite définir une mesure sur G cohérente avec sa structure de produit direct restreint. On se donne une famille de mesures dx_i sur les G_i vérifiant que pour presque tout i $dx_i(H_i) = 1$. Pour tout $S \subset I$ fini, on définit alors une mesure dx^S sur G^S vérifiant $dx^S(G^S) = \prod_{i \notin S} dx_i(H_i)$. On peut ainsi définir une mesure dx_S sur G_S comme suit :

$$dx_S := \prod_{i \in S} dx_i \otimes dx^S$$

On vérifie alors que cette mesure est indépendante de S et donc qu'elle définit bien une mesure dx sur G.

Si on se donne $f \in L^1(G)$ et que l'on sait que tous les compacts de G sont inclus dans un G_S, on a alors :

$$\int_G f(x)dx = \lim_{S \nearrow I} \int_{G_S} f(x)dx$$

Proposition 3.4
On se donne une famille de fonctions continues $f_i \in L^1(G_i)$ telles que $f_i(H_i) = \{1\}$ pour presque tout i.
On pose, pour $x \in G$:

$$f(x) := \prod_{i \in I} f_i(x_i)$$

Alors :

$$\int_G f(x)dx = \prod_{i \in I} \int_{G_i} f_i(x_i)dx_i$$

Démonstration : Soit $S \subset I$ un ensemble fini contenant les i tels que $f_i(H_i) \neq \{1\}$ ou $dx_i(H_i) \neq 1$. On a alors :

$$\begin{aligned}
\int_{G_S} f(x)dx &= \int_{G_S} f(x)dx_S \\
&= \int_{G_S} \left(\prod_{i\in S} f_i(x_i)\right)\left(\prod_{i\in S} dx_i dx^S\right) \\
&= dx(G^S)\prod_{i\in S}\int_{G_i} f_i(x_i)dx_i \text{ car } f = 1 \text{ sur } G^S \\
&= \prod_{i\in S}\int_{G_i} f_i(x_i)dx_i \text{ par construction de } S
\end{aligned}$$

D'où le résultat en "passant à la limite".

Pour tout $i \in I$, on note dc_i la mesure duale de dx_i (i.e celle apparaissant dans la formule d'inversion de Fourier). Considérons la fonction caractéristique f_i de H_i : on sait alors que $\widehat{f_i}$ est égale à $dx_i(H_i)$ la fonction caractéristique de H_i^*. En particulier, $dx_i(H_i)dc_i(H_i^*) = 1$ et donc $dc_i(H_i^*) = 1$ pour presque tout i. Ainsi on peut bien définir une mesure dc sur $\widehat{G}$ à partir des dc_i de la même façon que l'on a construit dx précédemment.

Proposition 3.5
La mesure dc est la mesure duale de dx.

Démonstration : On sait qu'il existe une constante n telle que $\forall x \in G$, $\widehat{\widehat{f}}(-x) = nf(x)$, donc on peut se permettre de vérifier la proposition sur une fonction en particulier. On considère la fonction caractéristique f_i de H_i et on pose :

$$f : x \mapsto \prod_{i\in I} f_i(x_i)$$

On a alors, par la proposition précédente, que :

$$\begin{aligned}
\forall c \in \widehat{G}, \quad \widehat{f}(c) &= \int_G f(x)\overline{c(x)}dx \\
&= \prod_{i\in I}\int_{G_i} f_i(x_i)\overline{c_i(x_i)}dx_i \\
&= \prod_{i\in I}\widehat{f_i}(c_i)
\end{aligned}$$

Ainsi, on a :

$$\forall x \in G,\ \widehat{\widehat{f}}(x) = \prod_{i\in I}\widehat{\widehat{f_i}}(x_i)$$

Comme les dc_i et les dx_i sont duales, on a $\widehat{\widehat{f_i}}(x_i) = f_i(-x_i)$, d'où $n = 1$ et donc le résultat.

4 Théorie globale

Dans toute cette section $\mathfrak{p}$ représente une norme sur k, $\mathfrak{p}$-adique si $\mathfrak{p}$ est un vrai idéal premier ou une norme archimédienne sinon (et on appellera donc une norme archimédienne un "premier à l'infini"). Dans le paragraphe précédent on a étudié les propriétés des complétions locales de k. Nous allons maintenant étudier les propriétés globales de k et pour ce faire nous introduirons de nouveaux objets.

4.1 Groupe des adèles

Définition 4.1
Le groupe $\mathbb{A}$ des adèles de k est le produit restreint direct des groupes additifs des complétions $k_\mathfrak{p}$ relativement aux sous groupes $\mathcal{O}_\mathfrak{p}$ des éléments entiers. On note un adèle quelconque de la manière suivante $x = (\dots, x_\mathfrak{p}, \dots)$.

On peut remarquer qu'on est bien dans le cas du paragraphe précédent car pour définir un produit restreint direct on a seulement besoin qu'un sous–groupe compact ouvert $H_{\mathfrak{p}}$ existe pour presque toute place, c'est le cas ici où les sous groupes $\mathcal{O}_{\mathfrak{p}}$ sont définis pour toutes les places sauf les places archimédiennes. Rappelons aussi qu'on a $\mu(\mathcal{O}_{\mathfrak{p}}) = 1$ pour presque tout $\mathfrak{p}$ et que toutes les mesures additives sur $k_{\mathfrak{p}}$ ont été choisies pour être autoduales.

Proposition 4.1
Le groupe des adèles $\mathbb{A}$ est isomorphe à son groupe des caractères en identifiant chaque élément $y \in \mathbb{A}$ avec le caractère $x \mapsto \chi_0(xy)$ où $\chi_0(x) = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(x_{\mathfrak{p}})$ et $xy = (\ldots, x_{\mathfrak{p}}, \ldots)(\ldots, y_{\mathfrak{p}}, \ldots) = (\ldots, x_{\mathfrak{p}}y_{\mathfrak{p}}, \ldots)$.

Démonstration : Comme $k_{\mathfrak{p}}^+$ est naturellement isomorphe à son groupe de caractères et comme $\chi_{\mathfrak{p}}(\eta x)$ est trivial sur $\mathcal{O}_{\mathfrak{p}}$ si et seulement si $\eta \in \mathcal{D}_{\mathfrak{p}}^{-1}$, le groupe $\hat{\mathbb{A}}$ est le produit direct restreint des $k_{\mathfrak{p}}^+$ relativement aux sous–groupes $\mathcal{D}_{\mathfrak{p}}^{-1}$. Mais comme $\mathcal{D}_{\mathfrak{p}}^{-1} = \mathcal{O}_{\mathfrak{p}}$ pour presque toutes les places, $\hat{\mathbb{A}} \simeq \mathbb{A}$.

De plus on avait choisi les $dx_{\mathfrak{p}}$ pour être autoduales donc c'est aussi le cas pour la mesure dx sur $\mathbb{A}$, donc on a le théorème suivant.

Proposition 4.2
Soit $f \in L^1(\mathbb{A})$. On définit alors sa transformée de Fourier par $\hat{f}(y) = \int_{\mathbb{A}} f(x)\chi_0(xy)dx$ et alors $\hat{\hat{f}}(x) = f(-x)$

Nous allons maintenant nous intéresser de plus près à la structure des adèles. Tout d'abord on peut voir que k s'injecte dans $\mathbb{A}$. En effet soit $\xi \in k$, on a $\xi = a/b$ avec $a, b \in \mathcal{O}$ et si $\xi \in \mathcal{O}_{\mathfrak{p}}$ alors $\mathfrak{p}|(b)$ et on peut alors identifier ξ avec $(\xi, \xi, \ldots)$. Ainsi k est un sous–groupe de $\mathbb{A}$.

Pour étudier les propiétés de k en tant que sous–groupe de $\mathbb{A}$ il nous faut trouver un ensemble D tel que $\mathbb{A} = \bigcup_{\xi \in k}(k + D)$ et que cette union soit disjointe, on appelera un tel D un domaine fondamental pour $\mathbb{A}/k$.

On note S_∞ l'ensemble des places archimédiennes et $\mathbb{A}_{S_\infty}$ l'ensemble des éléments de $\mathbb{A}$ tel que $x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ pour tous les $\mathfrak{p}$ finis. On a alors :

Lemme 4.1
$k \cap \mathbb{A}_{S_\infty} = \mathcal{O}$ et $k + \mathbb{A}_{S_\infty} = \mathbb{A}$

Démonstraion : Un élément de k est entier pour chaque idéal premier si et seulement si il appartient à l'anneau des entiers de k, d'où la première assertion.

Soit $x \in \mathbb{A}$. Alors $x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ pour presque toute place, notre but est alors d'ajouter un élément de k de sorte que pour toutes les places finies on soit dans $\mathcal{O}_{\mathfrak{p}}$. On corrige alors les places les unes après les autres. Soit $\mathfrak{p}$ tel que $x_{\mathfrak{p}} \notin \mathcal{O}_{\mathfrak{p}}$. Il faut donc trouver un $y_{\mathfrak{p}} \in k$ tel que $y_{\mathfrak{p}} + x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ et $y_{\mathfrak{p}} \notin \mathcal{O}_q$ pour tout $q \neq \mathfrak{p}$. Soit $y'_{\mathfrak{p}} \in k \cap (-x_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}})$. Soit S l'ensemble fini des places finies q telles que $y'_{\mathfrak{p}} \notin \mathcal{O}_q$. Posons alors $N_q = -\mathrm{ord}_q(y'_{\mathfrak{p}})$ pour tout $q \in S$ et $N = -\mathrm{ord}_{\mathfrak{p}}(y'_{\mathfrak{p}})$. Alors d'après le théorème chinois on peut trouver $a \in \mathcal{O}$ tel que $a \in q^{N_q}$ pour tout $q \in S$ et $a \in 1 + \mathfrak{p}^N$. Posons alors $y_{\mathfrak{p}} = ay'_{\mathfrak{p}}$ et montrons que cela convient. On a $y_{\mathfrak{p}} \in (-x_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}})(1 + \mathfrak{p}^N) = -x_{\mathfrak{p}} + \mathcal{O}_{\mathfrak{p}}$ donc la première condition est satisfaite. Si $q \in S$, on a pris a assez proche de 0 dans k_q pour que $y_{\mathfrak{p}} \in \mathcal{O}_q$ et si $q \notin S$ c'est évident. Comme il n'y a q'un nombre fini de places fines à corriger c'est fini.

Il apparaît donc que $\mathbb{A}_{S_\infty}$ joue un rôle important dans notre recherche d'un domaine fondamental. Notons $\mathbb{A}^\infty$ le produit cartésien fini des complétions archimédiennes de k on note r_1 le nombre de complétions réelles et r_2 le nombre de complétions complexes de k. Alors $\mathbb{A}^\infty$ est un espace vectoriel réel de dimension $r_1 + 2r_2 = [k : \mathbb{Q}]$. Soit $(\omega_1, \ldots, \omega_n)$ un base du $\mathbb{Z}$–module $\mathcal{O}$ et notons pour tout $i \in [|1; n|]$ ω_i^∞ l'image de ω_i dans $\mathbb{A}^\infty$. Notons $D^\infty = \sum_{i=1}^n t_i\omega_i^\infty / 0 \leq t_i < 1 \subset \mathbb{A}^\infty$. Enfin posons $D = D^\infty \times \prod_{\mathfrak{p} \notin S_\infty} \mathcal{O}_{\mathfrak{p}} \subset \mathbb{A}_{S_\infty}$.

Proposition 4.3
L'ensemble D ainsi défini est un domaine fondamental de $\mathbb{A}/k$ ie $D + k = \mathbb{A}$ et chaque élément de $\mathbb{A}$ se décompose de manière unique en une somme d'un élément de D et d'un élément de k.

Démonstration : On sait qu'on peut ramener n'importe quel élément de $\mathbb{A}$ dans $\mathbb{A}_{S_\infty}$ en lui soustrayant un élément de k. Comme $k \cap \mathbb{A}_{S_\infty} = \mathcal{O}$ cet élément est unique modulo $\mathcal{O}$. Une fois qu'on est dans $\mathbb{A}_{S_\infty}$ il ne nous reste plus qu'à modifier les composantes infinies de l'adèle de sorte qu'on soit dans D^∞ et vu la manière dont on l'a défini, il n'y a qu'un seul élément de $\mathcal{O}$ qui convient.

Proposition 4.4
k est discret et $\mathbb{A}/k$ est compact

DÉMONSTRATION : D a un intérieur non vide et est relativment compact d'où les résultats.

On cherche maintenant le groupe dual de k, ie le groupe $\tilde{k} \subset \mathbb{A}$ tel que $\chi_0(xy) = 1$ pour tous $y \in \tilde{k}$, $x \in k$.

Lemme 4.2
$\forall \xi \in k, \chi_0(\xi) = 1$

DÉMONSTRATION : χ_0 est le produit des caractères locaux et comme chacun est déterminé par la quantité $\lambda_p(\mathrm{Tr}_{\mathfrak{p}}(\xi))$ avec $\mathfrak{p}$ au dessus de p. Ainsi il suffit de montrer que $\sum_{\mathfrak{p}} \lambda_p(\mathrm{Tr}_{\mathfrak{p}}(\xi))$ est entier.

Donc $\sum_{\mathfrak{p}} \lambda_p(\mathrm{Tr}_{\mathfrak{p}}(\xi)) = \sum_p \lambda_p(\sum_{\mathfrak{p}|p} \mathrm{Tr}_{\mathfrak{p}}(\xi))$, et on a aussi $\sum_{\mathfrak{p}|p} \mathrm{Tr}_{\mathfrak{p}}(\xi) = \mathrm{Tr}(\xi)$.

Ainsi $\sum_{\mathfrak{p}} \lambda_p(\mathrm{Tr}_{\mathfrak{p}}) = \sum_p \lambda_p(\mathrm{Tr}(\xi))$.

Comme $\mathrm{Tr}(\xi) = r$ est rationnel il suffit de montrer que $\lambda_p(r)$ est entier pour tout premier q. Si $p \neq q$, $\lambda_p(r)$ est entier par rapport à q car $\lambda_p(r)$ est une somme de fractions dont les dénominateurs sont égaux à des puissances de p. Il ne reste plus qu'à comparer avec l'infini, mais on a $\lambda(r) = -r$ donc $\lambda_p(r) - r$ est premier par rapport p par définition.

Proposition 4.5
$\tilde{k} = k$

DÉMONSTRATION : $\tilde{k}$ est le groupe dual de $\mathbb{A}/k$ donc $\tilde{k}$ est discret. Considérons $\tilde{k}/k$, c'est inclus dans le groupe compact $\mathbb{A}/k$, donc $\tilde{k}/k$ est fini. De plus on peut voir que $\tilde{k}$ est un k espace vectoriel et comme k est infini on a que $\tilde{k} = k$.

4.2 Groupe des idèles

Définition 4.2
Le groupe $\mathbb{I}$ des idèles de k est le produit restreint direct des groupes multiplicatifs des complétions $k_{\mathfrak{p}}$ relativement aux sous–groupes $\mathcal{U}_{\mathfrak{p}}$ des unités multiplicatives.

On peut faire ici les mêmes remarques à propos de $\mathcal{U}_{\mathfrak{p}}$ que celles faites à propos de $\mathcal{O}_{\mathfrak{p}}$ lors de la construction des adèles au paragraphe précédent.

On peut alors remarquer qu'on a un homomorphisme continu du groupe des idèles dans le groupe des idéaux muni de la topologie discrète et de noyau $\mathbb{I}_{S_\infty}$ donné par $\phi(a) = \prod_{\mathfrak{p} \notin S_\infty} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}$.

Grâce aux préliminaires on sait aussi que les quasi-caractères sur $\mathbb{I}$ sont les $c = \prod_{\mathfrak{p}} c_{\mathfrak{p}}$ où les $c_{\mathfrak{p}}$ sont non-ramifiés (triviaux sur $\mathcal{U}_{\mathfrak{p}}$) en presque toutes les places. On choisit aussi la mesure $d^\star a = \prod_{\mathfrak{p}} d^\star a_{\mathfrak{p}}$.

Comme pour les adèles, on peut plonger $k^\star$ dans $\mathbb{I}$ et alors $\phi(\alpha)$ est égal à l'idéal principal $\alpha\mathcal{O}$. On sait que D est un domaine fondamental pour k dans $\mathbb{A}$ donc αD l'est aussi pour $\alpha \in k$. Ainsi, on peut écrire $\alpha D = \cup_\xi(\alpha D \cap (\xi + D))$ et $D = \cup_\xi(D \cap (-\xi + \alpha D))$, et ces deux réunions sont disjointes. De plus, chaque tel "morceau" de αD est un translaté par un certain ξ d'un "morceau" de D qui a donc même mesure. Ergo $dx(\alpha D) = dx(D)$. Ainsi, pour tout $\alpha \in k^*$, $|\alpha| = 1$.

Appelons J le sous–groupe des éléments de norme 1 de $\mathbb{I}$. Considérons les sous–groupes $J_{S_\infty} \subset J$ des idèles dont les coordonnées valent 1 en toutes les places finies et qui sont de norme 1. On se donne une place archimédienne $\mathfrak{p}_0$ et on considère l'ensemble $S'_\infty := S_\infty \setminus \{\mathfrak{p}_0\}$ et $r := \mathrm{card}(S'_\infty)$. On a alors un morphisme continu et surjectif donné par :

$$\begin{aligned} \ell : J_{S_\infty} &\to \mathbb{R}^r \\ b &\mapsto (\log|b_{\mathfrak{p}_1}|, \ldots, \log|b_{\mathfrak{p}_r}|) \end{aligned}$$

On montre alors comme précédemment que :

$$\mathcal{U} = J_{S_\infty} \cap k^*$$

À l'aide d'un théorème de Kronecker (cf. [RV99]), on montre que le noyau de la restriction à k^* de ℓ est exactement l'ensemble des racines de l'unité dans k^*. En particulier, si $(e_1 \ldots e_r)$ est un système générateur minimal de $\mathcal{U}$, alors $(\ell(e_1)\dots\ell(e_r))$ est une $\mathbb{Z}$–base de $\ell(U) \subset \mathbb{R}^r$. On pose alors :

$$P := \left\{ \sum_{i=1}^{r} t_i \ell(e_i) \,\middle|\, 0 \leq t_i < t \right\}$$

On note $E_0 \subset \ell^{-1}(P)$ l'ensemble des éléments $b \in \ell^{-1}(P)$ vérifiant $0 \leq \arg(b_{\mathfrak{p}_0}) < \dfrac{2\pi}{\omega}$, où ω est le nombre de racines distinctes de l'unité dans k.

Notons h le nombre de classes de k et donnons–nous des idèles $b_1 \dots b_h \in J$ tel que $\varphi(b_1)\dots\varphi(b_h)$ soient dans des classes d'idéaux distinctes. Enfin, posons :

$$E := \bigcup_{i=1}^{h} E_0 b_i$$

On a alors le résultat suivant (la démonstration étant relativement technique sans trop apporter au sujet, nous renvoyons le lecteur vers [RV99]) :

Proposition 4.6
L'ensemble E est un domaine fondamental de k dans J, i.e :

$$J = \bigsqcup_{\alpha \in k^*} \alpha E_0$$

Avec réunion disjointe.

Dans toute la suite, nous noterons κ le volume de E. Un calcul explicite en est possible, que nous ne mènerons pas ici. On déduit des résultats qui précèdent que, comme E a un intérieur, k^* est discret à l'intérieur de J et comme E est relativement compact, le quotient J/k^* est compact.

Intéressons–nous à présent aux quasi–caractères sur $\mathbb{I}$. Remarquons tout d'abord que comme J/k^* est compact, tout quasi–caractère trivial sur k^* sera unitaire sur J. Notons également que $I = J \times T$, où T est l'ensemble des valeurs absolues atteintes dans le groupe des idèles. On munit T de la mesure $\dfrac{dt}{t}$ et J de l'unique mesure de Haar d^*b telle que $d^*a = d^*b\dfrac{dt}{t}$.

Pour $a \in I$, on note $\tilde{a}$ sa projection sur $\mathbb{I}$. On se donne un caractère $\tilde{c}$ sur J. Comme $T \cong \mathbb{R}_+^*$, tous les quasi–caractères sur T sont de la forme $t \mapsto t^s$, pour $s \in \mathbb{C}$ et donc tous les quasi–caractères sur $\mathbb{I}$ sont de la forme :

$$c : a \mapsto \tilde{c}(\tilde{a})|a|^s$$

Comme dans la théorie locale, on appelle $\Re(s)$ l'exposant de c. On dira qu'un tel c est ramifié s'il est non trivial sur J et on dira que deux quasi–caractères sont équivalents si leur quotient est non–ramifié. En particulier, chaque classe d'équivalence est isomorphe à $(\mathbb{C}, +)$, ce qui nous permettra de parler par la suite de fonctions holomorphes sur l'ensemble des quasi–caractères et de prolongement analytique.

4.3 Théorème de Riemann–Roch

On dira dans la suite qu'une fonction f est périodique sur $\mathbb{A}$ si elle admet une période $\xi \in k$. On peut voir une telle fonction comme une application définie sur le groupe quotient $\mathbb{A}/k$ totalement déterminée par son action sur D. Le groupe quotient A/k est un groupe topologique que l'on munit de la mesure de Haar induite par celle sur D de masse 1.

Définition 4.3 (Transformée de Fourier sur $\mathbb{A}/k$)
Soit φ une fonction continue sur $\mathbb{A}/k$. On définit alors sa transformée de Fourier comme suit :

$$\forall \xi \in k,\ \widehat{\varphi}(\xi) := \int_D \varphi(x)\chi_0(\xi x)dx$$

Lemme 4.3
Soit φ une fonction continue périodique sur $\mathbb{A}$ telle que :

$$\sum_{\xi \in k} |\widehat{\varphi}(\xi)| < \infty$$

Alors $\forall x \in \mathbb{A}$, $\widehat{\widehat{\varphi}}(x) = \varphi(-x)$, *i.e*

$$\varphi(x) = \sum_{\xi \in k} \widehat{\varphi}(\xi)\chi_0(-\xi x)$$

DÉMONSTRATION : Comme $\widehat{\varphi} \in L^1(k)$ alors il nous suffit de vérifier l'égalité pour une fonction φ particulière, ici $\varphi = 1$. Comme χ_0 est périodique et non trivial sur D alors $\chi(\xi.)$ est non trivial sur le groupe $\mathbb{A}/k$ si $\xi \neq 0$. Ainsi $\widehat{\varphi}$ est nulle sur k^* et $\widehat{\varphi}(0) = dx(D)$ et donc $\widehat{\widehat{\varphi}} = dx(D)$. Nous démontrerons par la suite que $dx(D) = 1$.

Lemme 4.4
Soit $f \in L^1(\mathbb{A})$ *une fonction continue telle que la série* $\sum_{\eta \in k} f(. + \eta)$ *soit uniformément et absolument convergente sur* D.
On peut alors définir une fonction périodique :

$$\varphi : x \mapsto \sum_{\eta \in k} f(x + \eta)$$

Alors on a :

$$\forall \xi \in k,\ \widehat{\varphi}(\xi) = \widehat{f}(\xi)$$

DÉMONSTRATION : Soit $\xi \in k$. Alors :

$$\begin{aligned}
\widehat{\varphi}(\xi) &= \int_D \varphi(x)\chi_0(\xi x)dx \\
&= \int_D \left(\sum_{\eta \in k} f(x + \eta)\chi_0(\xi x) \right) dx \\
&= \sum_{\eta \in k} \int_D f(x + \eta)\chi_0(\xi x)dx \text{ comme la série converge uniformément et que } dx(D) < \infty \\
&= \sum_{\eta \in k} \int_{D+\eta} f(x)\chi_0(\xi(x - \eta))dx \\
&= \sum_{\eta \in k} \int_{D+\eta} f(x)\chi_0(\xi x)dx \text{ car } \chi(\xi\eta) = 1 \\
&= \sum_{\eta \in k} \int_{\mathbb{A}} f(x)\chi_0(\xi x)dx \\
&= \widehat{f}(\xi)
\end{aligned}$$

En combinant les deux lemmes précédents, on obtient un analogue de la formule sommatoire de Poisson :

Proposition 4.7
Soit $f \in L^1(\mathbb{A})$ *une fonction continue telle que* $\widehat{f} \in L^1(k)$.
Alors :

$$\sum_{\xi \in k} \widehat{f}(\xi) = \sum_{x \in k} f(x)$$

Ce résultat nous montre que $dx(D) = 1$. En effet, si nous n'avions pas fait cette hypothèse dans les démonstrations précédentes nous aurions obtenus la formule suivante :

$$\sum_{\xi \in k} \widehat{f}(\xi) = dx(D) \sum_{x \in k} f(x)$$

Et donc, en appliquant deux fois cette formule, on trouve $dx(D)^2 = dx(D)$, d'où le résultat.

Proposition 4.8
Soit a *un idèle.*
Alors :

$$|a| = \prod_{\mathfrak{p}} |a_{\mathfrak{p}}|$$

Ce produit étant bien défini car $a_{\mathfrak{p}} = 1$ *pour presque tout* $\mathfrak{p}$.

DÉMONSTRATION : On se donne un rectangle compact $N = \prod_{\mathfrak{p}} N_{\mathfrak{p}}$. On a alors :

$$\int_N dx = \prod_{\mathfrak{p}} \int_{N_{\mathfrak{p}}} dx$$

De plus :

$$\int_{aN} dx = \prod_{\mathfrak{p}} \int_{a_{\mathfrak{p}} N_{\mathfrak{p}}} dx = \prod_{\mathfrak{p}} |a_{\mathfrak{p}}| \int_{N_{\mathfrak{p}}} dx$$

D'où le résultat.

Nous sommes à présent en mesure de démontrer le théorème de Riemann–Roch :

Théorème 4.9 (Riemann–Roch)
Soit $f \in L^1(\mathbb{A})$ une fonction continue telle que la série $\sum_{\eta \in k} f(a(. + \eta))$ soit uniformément et absolument convergente sur D pour tout idèle a.
On suppose que pour tout idèle a, $\widehat{f(a.)} \in L^1(k)$.
Alors :

$$\frac{1}{|a|} \sum_{\xi \in k} \widehat{f}\left(\frac{\xi}{a}\right) = \sum_{\xi \in k} f(\xi a)$$

DÉMONSTRATION : Posons $g := f(a.)$. Par le changement de variable $\eta \mapsto a\eta$ on trouve que $\widehat{g} = \dfrac{\widehat{f}(a.)}{|a|}$. Ainsi, on peut appliquer la formule sommatoire de Poisson (proposition 4.7), ce qui nous donne le résultat.

4.4 Théorème fondamental

Fort de l'étude que nous venons de mener, nous sommes à présent en mesure de trouver une équation fonctionelle satisfaite par les fonctions Zêta globales. Pour commencer, donnons–nous $f : \mathbb{A} \to \mathbb{C}$ vérifiant les conditions suivantes :

(i) f et $\widehat{f}$ sont des fonctions continues de $L^1(\mathbb{A})$;

(ii) les séries $\sum_{\xi \in k} f(a(x + \xi))$ et $\sum_{\xi \in k} \widehat{f}(a(x + \xi))$ convergent absolument pour tout idèle a et adèle x, avec convergence uniforme pour les couples $(a, x) \in K \times D$, où K est un sous–ensemble compact de $\mathbb{I}$ et D est le domaine fondamental additif de k dans $\mathbb{A}$;

(iii) pour tout $\sigma > 1$, $f|.|^{\sigma}$ et $\widehat{f}|.|^{\sigma}$ sont dans $L^1(\mathbb{I})$.

Les conditions (i) et (ii) vont nous permettre d'appliquer le théorème de Riemann–Roch à f, tandis que (iii) va nous permettre de définir des fonctions Zêta qui soient holomorphes sur un sous–ensemble de chaque classe d'équivalence pour $\sim$.

Définition 4.4
Pour tout quasi–caractère c, on pose :

$$\zeta(f, c) := \int_{\mathbb{A}} f(a)c(a)d^*a$$

D'après la condition (iii) cette intégrale est absolument convergente si c est d'exposant strictement supérieur à 1, ce qui implique que $\zeta(f, .)$ est holomorphe sur l'ensemble formé des tels quasi–caractères.

Théorème 4.10 (Théorème fondamental de la théorie globale)
Pour un quasi–caractère c, on note $\widehat{c} := \dfrac{|.|}{c}$.
Alors les fonctions $\zeta(f, .)$ admettent un prolongement à l'ensemble de tous les quasi–caractères. Ce prolongement est entier sur toutes les classes d'équivalences à l'exception de celle des quasi–caractères non ramifiés, i.e l'ensemble des $x \mapsto |x|^s$, $s \in \mathbb{C}$. Sur cette dernière, $\zeta(f, .)$ admet un pôle simple en $s = 0$ et $s = 1$, de résidus respectifs $\kappa f(0)$ et $-\kappa \widehat{f}(0)$.
Ce prolongement satisfait de plus l'équation fonctionnelle suivante (pour c quasi–caractère) :

$$\zeta(f, c) = \zeta(f, \widehat{c})$$

DÉMONSTRATION : On rappelle que $\mathbb{I} = J \times T$. Soit c un quasi–caractère. On définit, pour $t \in \mathbb{R}^*$:

$$\zeta_t : (f, c) \mapsto \int_J f(tb)c(tb)d^*b$$

On a alors, par théorème de Fubini :

$$\begin{aligned}\zeta(f,c) &= \int_{\mathbb{A}} f(a)c(a)d^*a \\ &= \int_0^\infty \left(\int_J f(tb)c(tb)d^*b\right)\frac{dt}{t} \\ &= \int_0^\infty \zeta_t(f,c)\frac{dt}{t}\end{aligned}$$

Démontrons à présent que l'on a l'équation fonctionnelle suivante :

$$\forall t > 0,\ \zeta_t(f,c) + f(0)\int_E c(tb)d^*b = \zeta_{\frac{1}{t}}(\widehat{f},\widehat{c}) + \widehat{f}(0)\int_E \widehat{c}\left(\frac{1}{t}b\right)d^*b$$

Comme E est un domaine fondamental de k^* dans J, on a, pour $t > 0$:

$$\begin{aligned}\zeta_t(f,c) + f(0)\int_E c(tb)d^*b &= \sum_{\alpha\in k^*}\int_{\alpha E} f(tb)c(tb)d^*b + f(0)\int_E c(tb)d^*b \\ &= \sum_{\alpha\in k^*}\int_E f(\alpha tb)c(\alpha tb)d^*b + f(0)\int_E c(tb)d^*b \text{ via } b\mapsto \alpha b \\ &= \sum_{\alpha\in k^*}\int_E f(\alpha tb)c(tb)d^*b + f(0)\int_E c(tb)d^*b \text{ car } c(\alpha) = 1 \\ &= \int_E\left(\sum_{\alpha\in k^*} f(\alpha tb)\right)c(tb)d^*b + f(0)\int_E c(tb)d^*b \text{ la série convergeant uniformément} \\ &= \int_E\left(\sum_{\xi\in k} f(\xi tb)\right)c(tb)d^*b \text{ car } k = k^*\cup\{0\} \\ &= \int_E\left(\sum_{\xi\in k}\widehat{f}\left(\frac{\xi}{tb}\right)\right)\frac{1}{|tb|}c(tb)d^*b \text{ par théorème de Riemann–Roch} \\ &= \int_E\left(\sum_{\xi\in k}\widehat{f}\left(\frac{\xi b}{t}\right)\right)\widehat{c}\left(\frac{1}{t}b\right)d^*b \text{ via } b\mapsto\frac{1}{b}\end{aligned}$$

D'où l'équation voulue.

Calculons à présent l'intégrale $\int_E c(tb)d^*b = c(t)\int_E c(b)d^*b$. Celle–ci est l'intégrale sur J/k^* d'un caractère sur ce groupe, donc est nulle si c et non trivial sur J (i.e est ramifié) et est égale au volume κ de E si c est non–ramifié, auquel cas on a également $c(t) = |t|^s = t^s$. Ainsi :

$$\int_E c(tb)d^*b = \begin{cases}\kappa t^s & \text{si } c \text{ est non ramifié} \\ 0 & \text{sinon}\end{cases}$$

Remarquons ensuite que :

$$\zeta(f,c) = \int_0^1 \zeta_t(f,c)\frac{dt}{t} + \int_1^\infty \zeta_t(f,c)\frac{dt}{t}$$

La seconde intégrale de cette expression est égale à $\int_{|a|>1} f(a)c(a)d^*a$ et la première converge lorsque l'exposant de c est strictement supérieur à 1 car c'est le cas de $\zeta(f,c)$. Mieux, comme on intègre sur $|a| > 1$, elle convergera également si l'exposant est inférieur à 1 et donc on définit bien ainsi une fonction holomorphe sur l'ensemble des quasi–caractères.

D'après l'équation fonctionnelle que nous venons de démontrer, on a :

$$\int_0^1 \zeta_t(f,c)\frac{dt}{t} = \int_0^1 \zeta_{\frac{1}{t}}(\widehat{f},\widehat{c})\frac{dt}{t} + \left[\kappa\widehat{f}(0)\int_0^1\left(\frac{1}{t}\right)^{1-s}\frac{dt}{t} - \kappa f(0)\int_0^1 t^s\frac{dt}{t}\right]$$

Où la partie entre crochets n'est à prendre en compte que dans le cas non ramifié et où s est le complexe tel que $c = |.|^s$ dans ce cas. En particulier, si c est d'exposant strictement supérieur à 1, on a $\Re(s) > 1$ et donc les deux intégrales entre crochets convergent.

On obtient ensuite, par changement de variable $t \mapsto \dfrac{1}{t}$ dans la première intégrale :

$$\int_0^1 \zeta_t(f,c)\frac{dt}{t} = \int_1^\infty \zeta_t(\widehat{f},\widehat{c})\frac{dt}{t} + \left[\frac{\kappa\widehat{f}(0)}{s-1} - \frac{\kappa f(0)}{s}\right]$$

On montre ensuite de même façon que pour la première intégrale que la seconde définit bien une fonction holomorphe : on obtient bien ainsi un prolongement de notre fonction ζ, entière dans le cas non ramifié et avec les pôles et résidus précisés dans l'énoncé du théorème sinon. Enfin, remarquons que cette expression est invariante par la transformation $(f,c) \mapsto (\widehat{f},\widehat{c})$, on obtient l'équation fonctionnelle voulue :

$$\zeta(f,c) = \zeta(f,\widehat{c})$$

D'où le théorème.

5 Conclusion, applications

Bien que certains des résultats que nous venons de démontrer puissent sembler relativement "opaques", ils permettent de démontrer ou retrouver de nombreux résultats de la théorie des nombres, dont nous proposons ici un florilège [1].

5.1 Réciprocité de Langlands

Soit K/k une extension galoisienne et soit $\sigma : \mathrm{Gal}(K/k) \to \mathrm{GL}(n,\mathbb{C})$ une représentation galoisienne de dimension n. Alors la fonction L d'Artin de σ est définie comme suit :

$$L(s,\sigma) = \prod_{\mathfrak{p} \text{ non ramifié dans } K} \frac{1}{\det\left(I_n - \frac{\sigma(Fr_\mathfrak{p})}{(\mathcal{N}\mathfrak{p})^{-s}}\right)}$$

Soit $\omega \in \widehat{\mathbb{I}_k/k^*}$. Alors l'espace $L^2(GL(n,k)\backslash GL(n,\mathbb{A}_k),\omega)$ des formes automorphes pour $GL(n,\mathbb{A}_k)$ est l'espace des fonctions mesurables de $f : GL(n,\mathbb{A}_k) \to \mathbb{C}$ qui vérifient certaines propriétés, entre autres :

$$\forall g \in GL(n,\mathbb{A}), \quad \forall \gamma \in GL(n,k), \quad \forall z \in Z_n = Z(GL(n,k)), \quad f(z\gamma g) = \omega(z)f(g)$$

Et

$$\int_{Z_n GL(n,k)\backslash GL(n,\mathbb{A}_k)} |f(g)|^2 dg < \infty$$

En fait l'espace des formes automorphes pour $GL(n,\mathbb{A}_k)$ avec caractère central ω est une sous représentation de la représentation $\rho : GL(n,\mathbb{A}_k) \to GL(L^2(GL(n,\mathbb{A}_k))$ avec $(\rho(g)(f))(x) = f(xg)$.

Alors, une représentation automorphe de $GL(n)$ sur k est une représentation unitaire de $GL(n,\mathbb{A}_k)$ dans $L^2(GL(n,k)\backslash GL(n,\mathbb{A}_k),\omega)$. En particulier si $\omega \in \widehat{\mathbb{I}_k/k^*}$ alors $\omega \in L^2(GL(n,k)\backslash GL(n,\mathbb{A}_k),\omega)$ et donc c'est une représentation automorphe de $GL(1)$ sur k.

Soit π une représentation automorphe de $GL(n)$ sur k on peut lui associer une fonction L qui est le produit pour presque toutes les places de facteurs locaux $L_\mathfrak{p}(s,\pi)$.

Conjecture 1 (Réciprocité de Langlands)
Soit K/k une extension galoisienne.
Alors pour chaque représentation galoisienne $\sigma : Gal(K/k) \to GL(n,\mathbb{C})$ il existe une représentation automorphe π_σ de $GL(n,\mathbb{A}_k)$ telle que $L(s,\sigma) = L(s,\pi_\sigma)$.

1. Non exhaustif !

Exemple de la puissance de cette philosophie : soit E une courbe elliptique lisse définie sur $\mathbb{Z}$ on peut lui associer une fonction L (qui provient d'une certaine représentation galoisienne), alors le théorème de modularité (ex conjecture de Taniyama Shimura Weil) en partie démontré par Wiles et Taylor puis entièrement par Breuil, Conrad, Diamond et Taylor dit que cette fonction L provient d'une forme modulaire (qui peut se voir aussi comme une représentation automorphe). De plus Ribet et d'autres avaient déjà montré que s'il y avait une solution au problème de Fermat alors on pouvait définir une courbe elliptique dont la fonction L associée provenait d'une forme modulaire de poids 2, or il n'y a qu'une seule forme modulaire de poids 2, la forme nulle mais cela ne donne pas la bonne fonction L et on a donc une démonstration du dernier théorème de Fermat.

Lien avec notre sujet : Lorsque $n = 1$ la conjecture précédente est vraie grâce à la théorie du corps de classes et à la loi de réciprocité d'Artin. La thèse de Tate est alors l'étude des propriétés des fonctions L dans ce cas là. La théorie du corps de classes (et le théorème de Kronecker-Weber) permet d'avoir en particulier le lemme suivant :

Lemme 5.1 *Soit K une extension abélienne de $\mathbb{Q}$ de groupe de Galois G.*
Alors $\zeta_K(s) = \prod_{\chi \in \hat{G}} L(s, \chi)$

5.2 Théorème de la progression arithmétique

Soit K une extension abélienne de $\mathbb{Q}$ de groupe de Galois G. Du lemme précédent et du calcul du résidu de ζ_K en 1 on obtient que :

Proposition 5.1 (Formule des classes de Dirichlet)

$$\prod_{\chi \in \hat{G}-1} L(1, \chi) = \kappa = \frac{2^{r_1(K)}(2\pi)^{r_2(K)} h_K R_K}{\omega_K \sqrt{|d_K|}}$$

On en déduit en particulier le théorème de la progression arithmétique :

Théorème 5.2 (Progression arithmétique)
Soient a et m deux entiers premiers entre eux.
Alors il existe une infinité de nombres premiers congrus à a modulo m.

En effet, les travaux de Dirichlet nous montrent qu'il sufft de montrer que $\prod_{\{\chi \mod m, \chi \neq 1\}} L(1, \chi) \neq 0$. Il s'agit d'un cas particulier de la formule des classes en prenant pour K l'extension cyclotomique de degré m.

5.3 Théorème de Čebotarev

En étudiant plus précisément les fonctions L, on peut montrer qu'elle ne s'annulent pas sur $Re(s) = 1$ et grâce à ce qu'on a déjà vu sur la théorie du corps de classes, on peut appliquer un théorème (cf. [Ser97]) pour obtenir le théorème de Čebotarev.

Proposition 5.3
Soit G un groupe compact et X l'espace des classes de conjugaison de G. Soit $(x_\nu)_{\nu \in \Sigma}$ une famille d'éléments de X indexée par un ensemble dénombrable Σ et soit $N : \nu \to N\nu$ un fonction sur Σ à valeurs dans les entiers supérieurs ou égaux à 2. On fait en plus les deux hypothèses suivantes :

1. *Le produit infini $\prod_{\nu \in \Sigma} \frac{1}{1-(N\nu)^{-s}}$ converge pour tout $s \in \mathbb{C}$ avec $Re(s) > 1$ et se prolonge en une fonction méromorphe sur $Re(s) \geq 1$ qui n'a ni zéro ni pôle sauf peut-être un pôle simple en $s = 1$;*
2. *Soit ρ une représentation irréductible de G avec caractère χ et soit $L(s, \rho) = \prod_{\nu \in \Sigma} \frac{1}{det(1-\frac{\rho(x_\nu)}{(N\nu)^s})}$, alors ce produit converge pour tout $s \in \mathbb{C}$ avec $Re(s) > 1$ et se prolonge en une fonction méromorphe sur $Re(s) \geq 1$ qui n'a ni zéro ni pôle sauf peut-être un pôle simple en $s = 1$ et l'ordre de $L(s, \rho)$ en $s = 1$ sera noté $-c_\chi$.*

Alors :

1. *Le nombre de $\nu \in \Sigma$ avec $N\nu \leq n$ est équivalent à $\frac{n}{ln(n)}$ quand n tend vers $+\infty$;*
2. *Pour tout caractère irréductible χ de G on a $\sum_{N\nu \leq n} \chi(x_\nu) =_{n \to +\infty} c_\chi \frac{n}{ln(n)} + o(\frac{n}{ln(n)})$.*

Supposons de plus qu'il existe une constante $C \in \mathbb{N}$ telle que pour tout $n \in \mathbb{N}$, le nombre de $\nu \in \Sigma$ avec $N\nu = n$ est inférieur ou égal à C.

Ainsi on peut réordonner les éléments de Σ en une suite $(\nu_i)_{i \in \mathbb{N}^*}$ telle que pour $i \leq j$, $N\nu_i \leq N\nu_j$, on peut alors parler d'équidistribution et on a (cf [Ser97]) :

Proposition 5.4
Une suite (x_n) d'éléments de X est équidistribuée pour une mesure μ si et seulement si pour tout caractère irréductible χ de G, on a $lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\chi(x_i) = \mu(\chi)$.

Et on a alors :

Proposition 5.5
Les éléments de x_ν sont équidistribués dans X par rapport à la mesure μ vérifiant pour tout caractère irréductible χ de G : $\mu(\chi) = c_\chi$.

Et donc avec quelques notions de plus sur les mesures de Haar (cf [Ser97]), on obtient (en fait pour l'application au théorème de Čebotarev on n'aura pas besoin de ces notions en plus sur les mesures de Haar car on sera dans le cas d'un groupe G fini alors la mesure de Haar normalisée est l'inverse du cardinal du groupe fois la mesure discrète et on s'en tire alors en utilisant $\frac{1}{\phi(m)}\sum_\chi \bar{\chi(a)}\chi(x) = \delta_a(x)$ qui se démontre de manière plus élémentaire) :

Corollaire 5.5.1
Les éléments x_ν sont équidistribués pour la mesure de Haar normalisée sur G ssi $c_\chi = 0$ pour tout caractère irréductible $\chi \neq 1$ de G, ie si et seulement si les fonctions L associées aux caractères irréductibles non triviaux de G sont holomorphes et non nulles en $s = 1$.

Soit L/K une extension galoisienne finie d'un corps de nombres. On pose $G = Gal(L/K)$, Σ l'ensemble des places non ramifiées de K et pour tout $\nu \in \Sigma$, x_ν la classe de conjugaison du Frobenius définie par $\nu \in \Sigma$ et $N\nu$ la norme de ν. Alors grâce à tout ce qu'on a fait jusqu'à présent on sait que les hypothèses des théorèmes précédents sont vérifiées. On a donc :

Théorème 5.6 (Čebotarev)
Soit $\sigma \in G$, notons $< \sigma >$ sa classe de conjugaison dans G et $n \in \mathbb{N}$. Soit l'ensemble $P_{L|K}(\sigma)(n)$ des premiers $\mathfrak{p}$ non ramifiés de K tels qu'il existe un idéal q au dessus de $\mathfrak{p}$ tel que l'image de σ soit égale au Frobenius en q (propriété qui ne dépend que de la classe de conjugaison de σ) et tels que $N\mathfrak{p} \leq n$. Alors :

$$\mathrm{card}(P_{L|K}(\sigma)(n)) =_{n\to\infty} \frac{\mathrm{card}(<\sigma>)}{\mathrm{card}(G)}\frac{n}{\ln(n)} + o(\frac{n}{\ln(n)})$$

Applications : Soient a et m deux entiers premiers entre eux. Si on considère $\mathbb{Q}(\mu_m)/\mathbb{Q}$ le corps cyclotomique de degré m alors le théorème de Čebotarev n'est rien d'autre que le théorème des nombres premiers généralisé :

Théorème 5.7 (des nombres premiers)
$\mathrm{card}\{p \in \mathcal{P}/p \equiv a \mod m,\, p \leq n\} =_{n\to\infty} \frac{1}{\phi(m)}\frac{n}{ln(n)} + o(\frac{n}{ln(n)})$.

On a aussi une application amusante du théorème de Čebotarev :

Théorème 5.8
On ne peut prouver le théorème des progressions arithmétiques par une méthode euclidienne (au sens défini dans l'introduction) ssi $a^2 \equiv 1 \ mod\ m$.

La preuve est exposée dans le papier de Keith Conrad "Euclidian proofs of Dirichlet's theorem".

5.4 Analogie corps de fonctions/corps de nombres

Soit C une "gentille" courbe projective sur un corps fini, on considère alors son corps de fonctions, c'est une extension finie de $\mathbb{F}_q(T)$. Comme pour $\mathbb{Q}$ on voit qu'en chaque point on peut définir une valuation puis ensuite compléter, on peut alors reproduire tout le formalisme et les raisonnements de la thèse de Tate (la seule différence ici c'est qu'on a aucune place archimédienne (ce qui simplifie les choses)) qui montre l'équation fonctionnelle de la fonction zêta associée à cette courbe.

L'avantage ici d'être sur une courbe sur un corps fini c'est qu'on a un éclairage géométrique les adèles deviennent le groupe des diviseurs de la même courbe définie sur la clôture algébrique de $\mathbb{F}_q$ et le groupe des idèles devient le groupe de Picard de la "courbe"(courbe au sens précédent) et la formule de Poisson devient le théorème de Riemann-Roch géométrique. Cela nous conduit alors à une nouvelle formule d'Euler :

$$\zeta(X_0, T) = \prod_{x \in |X_0|} \frac{1}{1 - T^{deg(x)}}$$

Avec $T = q^{-s}$. De manière plus générale pour un schéma X on peut définir :

$$\zeta(s, X) = \prod_{x \in |X|} \frac{1}{1 - \frac{1}{(\mathrm{card}(k(x))^s}}$$

5.5 Lien avec l'hypothèse de Riemann

En revenant sur le cas des variétés sur des corps finis on a la formule suivante :

$$Z(X_0, T) = \exp\left(\sum_{n \geq 1} |X_0(\mathbb{F}_{q^n})| \frac{T^n}{n}\right)$$

Mais la formule des traces de Grothendieck-Lefschetz-Verdier donne :

$$|X_0(\mathbb{F}_{q^n})| = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}((Fr^n)^* | H^i(X, \mathbb{Q}_l))$$

De plus on a :

$$\sum_{n \geq 1} \mathrm{Tr}(f^n|V) \frac{T^n}{n} = -\ln(\det(1 - fT))$$

Donc :

$$Z(X_0, T) = \prod_{i=0}^{2d} \det(1 - F^*T | H^i(X, \mathbb{Q}_l))^{(-1)^{i+1}}$$

Ainsi les zéros de Z sont les valeurs propres de l'endomorphisme de Frobenius sur les espace de cohomologie impaire, on a donc une interprétation spectrale de zéros de Z. Le formalisme cohomologique fournit donc des résultats très importants dans le cas des variétés (dont des courbes) définies sur des corps finis mais comme les corps de nombres et les courbes définies sur des corps finis se ressemblent, on a envie de développer pour les corps de nombres un formalisme cohomologique aussi puissant et il a été montré que si on arrive à en trouver un qui se comporte bien alors en sera en mesure de prouver l'hypothèse de Riemann.

Références

[Ber10] Laurent Berger. Théorie algébrique des nombres. http ://www.umpa.ens-lyon.fr/ lberger/coursM2/TAN2010.pdf, 2010.

[Bin09] John Binder. Tate's thesis on zeta functions on number fields. http ://math.uchicago.edu/ may/VIGRE/VIGRE2009/REUPapers/Binder.pdf, 2009.

[Pra07] Dipendra Prasad. Lectures on tate's thesis. In *Summer School and Conference on Automorphic Forms and Shimura Varieties*, 2007.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier Analysis on Number Fields.* Springer-Verlag, 1999.

[Ser94] Jean Pierre Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1994.

[Ser97] Jean Pierre Serre. *Abelian l-adic Representations and Elliptic Curves.* A K Peters, 1997.