

Théorie d'Iwasawa

José Ibrahim Villanueva Gutiérrez

Après les notes du cours mené à l'Université de Bordeaux 1 dirigé par le professeur
Jean-François Jaulent (Janvier-Avril 2014).

Toutes les fautes dans ces notes sont miennes, pour corrections veuillez écrire à jovillan@math.u-bordeaux1.fr.

Version 2015-10-01.

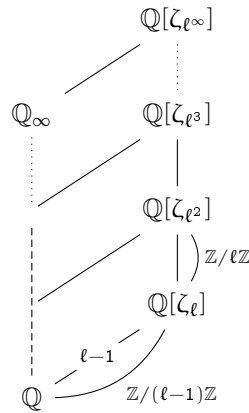
Table des matières

1	Motivation Initial	2
2	Préliminaires Algebriques	4
2.1	L'algèbre d'Iwasawa	4
2.2	Modules noethériens sur Λ	7
2.2.1	Λ -modules sans torsion	7
2.2.2	Λ -modules de torsion	9
2.3	Structure des Λ -modules noethériens et de torsion	10
2.4	Appendice : Suites Admissibles	12
3	Théorème de paramétrage	13
3.1	Le contexte arithmétique	13
3.2	Complements sur les représentations	14
3.3	Les paramètres structurels d'un $\Lambda[\Delta]$ -module	15
3.4	Enoncé du théorème fondamental	16
3.5	Application arithmétique	19
4	Introduction à la théorie des corps de classes	22
4.1	La théorie de Chevalley	22
4.2	La théorie ℓ -adique.	23
4.2.1	Point de vue local	23
4.2.2	Point de vue global	24
4.3	Quelques Exemples	25
4.4	Valeurs absolues ℓ -adiques	27
4.5	Unités logarithmiques	28
4.6	Interprétation par les corps de classes	29
5	Interprétation des corps de classes des classes logarithmiques	30
5.1	Point de vue local	31
5.2	Méthode de Baker-Brumer	32
5.3	Cas d'une extension Galoisienne quelconque	33

6	La descente en théorie d'Iwasawa	33
6.1	Structure du groupe X	36
7	Dualité dans la $\mathbb{Z}_\ell$-extension cyclotomique	37
7.1	Description Kummerienne	38
7.2	Dualité	39
7.3	étude préliminaire	40
7.4	La dualité de Gras	41
7.4.1	Principe	42
7.4.2	Première suite exacte (Interpretation Kummerienne)	42
7.4.3	Interpretation du noyau	42
7.4.4	Deuxième suite exacte (Interpretation Galoisienne)	43
7.4.5	Conclusions	44
7.5	Cas general	44
7.5.1	Préliminaire	44
7.5.2	Preuve de l'assertion	45
7.5.3	Enoncé des resultats en termes de caractères	45
7.5.4	Preuve des identités	45
7.5.5	Identities de dualité	46
7.6	Détermination des invariants ρ	47
7.7	Determination des invariants μ	47
7.8	Détermination des invariants λ	48

1 Motivation Initial

Nous sommes intéressés dans l'étude des corps cyclotomiques. Soit ℓ un nombre premier impair.



On a

$$\begin{aligned}
 \text{Gal}(\mathbb{Q}[\zeta_{\ell^n}]/\mathbb{Q}) &\simeq (\mathbb{Z}/\ell^n\mathbb{Z})^\times \\
 &\simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}/\ell^{(n-1)}\mathbb{Z}
 \end{aligned}$$

d'où

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}[\zeta_{\ell^\infty}]/\mathbb{Q}) &\simeq \varprojlim (\mathbb{Z}/\ell^n \mathbb{Z})^\times \\ &\simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \varprojlim \mathbb{Z}/\ell^{(n-1)}\mathbb{Z} \\ &\simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}_\ell.\end{aligned}$$

En général soit K un corps de nombres, alors une suite de corps de nombres

$$K = K_0 \subset K_1 \subset \dots \subset K_n \subset \dots \subset K_\infty = \bigcup_{n \in \mathbb{N}} K_n,$$

est dite une $\mathbb{Z}_\ell$ -extension si $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/\ell^n \mathbb{Z}$, il en vient que $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_\ell$.

Théorème 1.1 (Iwasawa). *Soit K un corps de nombres, et $K_\infty = \bigcup K_n$ une $\mathbb{Z}_\ell$ extension. Alors il existe $\lambda, \mu \in \mathbb{N}$ et $\nu \in \mathbb{Z}$ tels que*

$$x_n = \nu \ell^n + \lambda n + \nu,$$

pour tout n assez grand.

Clé de la preuve : Théorème de Structure de modules noëtheriens sur l'algèbre $\Lambda = \mathbb{Z}_\ell[[T]]$.

$$\begin{array}{ccc} K_\infty & \xrightarrow{\mathcal{C} = \varprojlim \mathcal{C}_{\ell_{K_n}}} & H_\infty \\ \vdots & \nearrow & \vdots \\ K_r & \xrightarrow{\mathcal{C}_{\ell_{K_n}}} & H_n \\ \vdots & & \vdots \\ \mathbb{Z}/\ell^r \mathbb{Z} \left(\begin{array}{c} K_1 \\ \vdots \\ K \end{array} \right. & & \end{array}$$

$\mathcal{C}$ est un module sur $\Lambda = \mathbb{Z}_\ell[[\gamma - 1]]$.

Développements récents :

Soient S et T deux ensembles finis de places. $\mathcal{C}_T^S(K_n)$ group des S -classes T -infinitésimales. Pour la théorie de corps de classes

$$\mathcal{C}_T^S(K_n) \simeq \mathrm{Gal}(H_T^S(K_n)/K_n)$$

la pro- ℓ -extension abélienne S -décomposée T -ramifiée.

$$\text{Soit } \ell^{x_T^S} = |\mathcal{C}_T^S(K_n)/\mathcal{C}_T^S(K_n)^{\ell^n}|$$

Théorème 1.2. *Il existe $\rho_T^S, \mu_T^S, \lambda_T^S$ tels qu'on ait*

$$x_T^S(n) \approx \rho_T^S n \ell^n + \mu_T^S \ell^n + \lambda_T^S n.$$

étude générale des $\mathbb{Z}_\ell$ -extensions.

Conjecture 1.1 (Leopoldt). *Si K est totalement réel il possède une unique $\mathbb{Z}_\ell$ -extension K_∞ . Plus généralement le comp. Z des $\mathbb{Z}_\ell$ -extensions a pour groupe de Galois*

$$\mathrm{Gal}(Z/K) \simeq \mathbb{Z}_\ell^{c+1},$$

où c est le nombre des plongements complexes ($[K : \mathbb{Q}] = r + 2c$).

Une autre motivation est la Conjecture de Gross, qu'on énoncera après.

2 Préliminaires Algébriques

2.1 L'algèbre d'Iwasawa

Notation : Soit A un anneau local de valuation discrète, complet pour la topologie définie par puissances de l'idéal maximal πA de corps résiduel $k = A/\pi A$ fini, de sorte que A est compact.

Exemple 2.1. $A = \mathbb{Z}_\ell$, $\pi = \ell$, $k = \mathbb{F}_\ell$.

Théorème 2.1 (Théorème de Représentation). *Soit R un système de représentations de k dans A . Alors tout élément de A s'écrit de façon unique :*

$$x = \sum_{i \in \mathbb{N}} a_i \pi^i, \quad (1)$$

avec $a_i \in R$.

Preuve : Soit $x \in A$. $x \equiv a_0 \pmod{\pi}$ avec $a_0 \in R$. Donc $x - a_0 = \pi x_1$ avec $x_1 \in A$, puis $x_1 = a_1 + \pi x_2$, etc. Ce qui donne $x = \sum_{i=0}^n a_i \pi^i + \underbrace{\pi^{n+1} x_{n+1}}_{\rightarrow 0}$. Donc finalement $x = \sum_{i \in \mathbb{N}} a_i \pi^i$. $\square$

Exemple 2.2. Pour $A = \mathbb{Z}_\ell$, $R = \{0, 1, \dots, \ell - 1\}$ convient, donc tout $x \in \mathbb{Z}_\ell$ s'écrit $x = \sum_{i \geq 0} a_i \ell^i$ avec $a_i \in \{0, 1, \dots, \ell - 1\}$.

Remarque: $\mathbb{Z}_\ell$ contient les racines $(\ell - 1)$ -ièmes de l'unité μ_ℓ^0 , lesquelles forment un système de représentants de k^* . De sorte que $R = \mu_\ell^0 \cup \{0\}$ convient aussi.

Lemme 2.1 (Hensel). *Si P est un polynôme unitaire de $A[x]$, dont la réduction $\bar{P} \in k[x]$ admet une racine simple $\bar{a}$, celle-ci est la réduction de une racine simple de P dans A .*

Exemple 2.3. Pour $A = \mathbb{Z}_\ell$, $P = x^{\ell-1} - 1$ on a $\bar{P}(x) = \prod_{\bar{x} \in k^*} (x - \bar{x})$.

Preuve du Lemme 2.1 : On part d'un relèvement a_0 de $\bar{a}$. On a par hypothèse

$$\begin{aligned} P(a_0) &\equiv 0 \pmod{\pi} \\ P'(a_0) &\not\equiv 0 \pmod{\pi}, \end{aligned}$$

on pose

$$a_1 = a_0 - \frac{P(a_0)}{P'(a_0)} \equiv a_0 \pmod{\pi}.$$

Alors on a

$$\begin{aligned} P(a_1) &= P(a_0) + (a_1 - a_0)P'(a_0) + (a_1 - a_0)^2 P''(a_0) + \dots \equiv 0 \pmod{\pi^2} \\ P'(a_1) &= P'(a_0) + (a_1 - a_0)P''(a_0) + (a_1 - a_0)^2 P'''(a_0) + \dots \equiv 0 \pmod{\pi^2}, \end{aligned}$$

et on continue le processus. $\square$

Définition 2.1. On appelle algèbre d'Iwasawa attaché à A , l'algèbre $\Lambda = A[[T]]$, des séries formelles à une indéterminée à coefficients dans A .

Proposition 2.1. Λ est un anneau local d'unique idéal maximal $\mathfrak{M} = \Lambda\pi + \Lambda T$.

Preuve : On sait que $f \in \Lambda \setminus \{0\}$ est inversible $\Leftrightarrow a_0 \neq 0$, où $f = f_0 + f_1 T + \dots$ et $f_0 = a_0 + a_1 \pi + \dots$. Pour $f = \sum_{i \in \mathbb{N}} f_i T^i$, on écrit $f = f_0(1 - Tg)$, ce qui donne bien

$$f^{-1} = f_0^{-1}(1 - Tg)^{-1} = f_0^{-1} \sum_{i \in \mathbb{N}} T^i g^i.$$

On a donc $\Lambda^* = \Lambda \setminus \mathfrak{M}$. □

Remarque: Notons que $\mathfrak{M}$ n'est plus principal, comme c'était le cas pour l'anneau A .

Définition 2.2. On équipe Λ de la topologie $\mathfrak{M}$ -adique (On prend les $(\mathfrak{M}^n)_{n \in \mathbb{N}}$ comme système fondamental de voisinages de 0). Ce qui fait de Λ un anneau local complet, de corps résiduel $k = \Lambda/\mathfrak{M} = A/\pi A$ fini. En fait Λ est compact (car il est séparé) et noethérien.

Lemme 2.2 (Lemme de division). *Soit f une série $\notin \pi\Lambda$ et v son degré de Weierstrass (i.e. la valuation de sa réduction $\bar{f} \in k[[T]]$).*

$$f = T^v \mu + \pi R, \text{ avec } R \in A_{v-1}[T], \quad (2)$$

pour un $\mu \in \Lambda^*$. Ceci étant, on a :

$$\Lambda = \Lambda f \oplus A_{v-1}[T],$$

où $A_{v-1}[T]$ est le A -module des polynômes de degré au plus $v-1$.

Preuve : (Existence) Partons d'une série $g \in \Lambda$ et écrivons-la $g = T^v g' + r$, avec $r \in A_{v-1}[T]$.

Posons $a_0 = \mu^{-1} g'$. Il vient

$$\begin{aligned} g - a_0 f &= g - T^v g' + \mu^{-1} g' R \\ &= r_0 + \pi g_1. \end{aligned}$$

Posons $a_1 = \mu^{-1} g'_1$. Il vient $g_2 - a_1 f = r_1 + \pi g_2$, c'est à dire $g - (a_0 + \pi a_1) f = (r_0 + \pi r_1) + \pi^2 g_2$.

$$\text{Itérons } g - \left(\sum_{i=0}^n a_i \pi^i \right) f = \underbrace{\sum_{i=0}^n r_i \pi^i}_{\rightarrow r \in A_{v-1}[T]} + \underbrace{\pi^{n+1} g_{n+1}}_{\rightarrow 0}.$$

à la limite il vient $g - \lambda f = r$.

(Unicité) Supposons on a deux décompositions : Soit $\lambda f = r \in \Lambda f \cap A_{v-1}[T]$. Modulo π il vient $\bar{\lambda} \bar{f} = \bar{\lambda} \bar{\mu} T^v = \bar{r}$, donc $\bar{\lambda} \bar{f} = \bar{r} = 0$, i.e. $\pi | \lambda f$ et $\pi | r$, ceci entrain que $\pi | \lambda$ et $\pi | r$, on a donc

$$\frac{\lambda}{\pi} f = \frac{r}{\pi},$$

d'où $\pi^2 | \lambda$ et $\pi^2 | r$ et en iterant : $\pi^n | \lambda$ et $\pi^n | r$ pour tout $n \geq 0$ et finalement $\lambda = r = 0$. □

Théorème 2.2 (Théorème de Préparation de Weierstrass). *Tout élément $f \in \Lambda \setminus \pi\Lambda$ s'écrit de façon unique*

$$f = \mu(T^v + \pi Q), \quad (3)$$

avec $Q \in A_{v-1}[T]$. C'est à dire, comme produit d'un inversible $\mu \in \Lambda^*$ et d'un polynôme distingué $P = T^v + \pi Q$.

Preuve : Appliquons à $T^\vee$ le lemme de division : $T^\vee = \lambda f + R$ avec $R \in A_{v-1}[T]$. Module π il vient :

$$T^\vee = \bar{\lambda}\bar{\mu}T^\vee + \bar{R},$$

donc $\bar{R} = 0$ et $\bar{\lambda}\bar{\mu} = 1$, en particulier, λ est inversible dans Λ et il suit que $f = \lambda^{-1}(T^\vee - R)$ comme attendu. $\square$

Corollaire 2.1. *Les polynômes distingués $P \in A[T]$ irréductibles dans $A[T]$, sont encore irréductibles dans Λ .*

Preuve : Pour $P = f_1 f_2$ dans Λ , écrivons $f_i = \mu_i P_i$, il vient $P = (\mu_1 \mu_2) P_1 P_2$ donc pour unicité $P_1 P_2 = P$ et $\mu_1 \mu_2 = 1$. $\square$

Remarque: En particulier les polynômes d'Eisenstein dans $A[T]$ sont irréductibles dans $\Lambda[T]$.

Corollaire 2.2. *L'anneau Λ est encore un anneau factoriel qui a pour système d'irréductibles*

- *L'uniformisante π de Λ .*
- *Les polynômes distingués et irréductibles dans $A[T]$.*

Théorème 2.3. *Tout idéal (non nul) $\mathfrak{U}$ de l'algèbre Λ est contenu dans un plus petit idéal principal $\hat{\mathfrak{U}} = \Lambda a$. On dit que a est un pseudo générateur de l'idéal $\mathfrak{U}$, et on a $(\Lambda a : \mathfrak{U})$ fini.*

Remarque: Noter que si $\mathfrak{U}$ n'est pas principal, on a $a \notin \mathfrak{U}$. Par exemple, prenons $\mathfrak{U} = (\pi, T) = \mathfrak{M}$ donc $\mathfrak{U} \subset (1) = \Lambda$ car $\mathfrak{M}$ est maximale.

Preuve : Puisque Λ est noethérien, l'idéal $\mathfrak{U}$ est à type fini, disons $\mathfrak{U} = \sum_{i=1}^d \Lambda f_i$. Notons $\bigwedge_{i=1}^d f_i$ le plus grand

commun diviseur des f_i . On a

$$\begin{aligned} \mathfrak{U} \subset \Lambda a &\Leftrightarrow a | f_i, \forall i = 1, \dots, d \\ &\Leftrightarrow a | \bigwedge_{i=1}^d f_i, \end{aligned}$$

de sorte que le plus petit idéal principal qui contient $\mathfrak{U}$ est $\Lambda \left(\bigwedge_{i=1}^d f_i \right)$.

Il reste à montrer que l'indice $(\hat{\mathfrak{U}} : \mathfrak{U})$ est fini.

Lemme 2.3. *Pour f, g non nuls dans Λ de PGCD (Plus Grand Commun Diviseur) $d = f \wedge g$, la somme $\Lambda f + \Lambda g$ est contenue dans Λd avec un indice fini.*

Preuve du lemme : On a évidemment $\Lambda f + \Lambda g = d \left(\Lambda \frac{f}{d} + \Lambda \frac{g}{d} \right) \subset \Lambda d$, ce qui permet de se ramener au cas où f et g sont copremiers. Par le Théorème de Préparation (2.2) on peut supposer que ce sont des polynômes, dont l'un au moins, par exemple f , est distingué : $f = T^n + \pi Q$.

Puis que f et g sont pris copremiers, leur résultant $\text{res}(f, g)$, n'est pas nul dans Λ . On a donc $\text{res}(f, g) = \mu \pi^\alpha$ avec $\mu \in \Lambda^*$ et $\alpha \in \mathbb{N}$. On a aussi $\pi^\alpha \in \Lambda f + \Lambda g$. En particulier, modulo $\Lambda f + \Lambda g$, on a $\pi^\alpha \equiv 0 \pmod{\Lambda f + \Lambda g}$ et $T^n \equiv \pi Q$, donc $T^{n\alpha} \equiv \pi^\alpha Q^\alpha \equiv 0$. Aussi $\Lambda f + \Lambda g$ contient π^α et $T^{n\alpha}$, et maintenant écrivons $\beta = n\alpha$, alors

$$\begin{aligned} (\Lambda : \Lambda f + \Lambda g) &\leq (\Lambda : \Lambda \pi^\alpha + \Lambda T^\beta) \\ &= |\Lambda / \pi^\alpha \Lambda[T] / (T^\beta)| \\ &= |k|^{\alpha\beta}, \end{aligned}$$

qui est fini, car on a supposé que le corps résiduel était fini. Ce qui achève la démonstration du lemme et donc celle du théorème. $\square$

Remarque: Si Λf et Λg sont idéaux principaux emboîtés, l'indice $(\Lambda f : \Lambda g)$ est soit 1 soit infini, parce que pour $g = fd$ on a

$$(\Lambda f : \Lambda g) = (\Lambda : \Lambda d),$$

- Pour d inversible c'est 1.
- Pour d non inversible on a :
 - $\pi|d$ et $(\Lambda : \Lambda d) \geq (\Lambda : \pi\Lambda) = |k[[T]]|$ infini avec $k = \Lambda/\pi\Lambda$.
 - ou $(T^n + \pi Q)|d$ avec $T^n + \pi Q$ distingué non constant et $(\Lambda : \Lambda d) = |\Lambda^n|$ infini. On a $(\Lambda : \Lambda d) = (\Lambda[T] : (T^n + \pi Q)\Lambda[T])$.

2.2 Modules noethériens sur Λ

2.2.1 Λ -modules sans torsion

On s'intéresse ici aux Λ -modules qui sont noethériens et sans torsion. On note M un tel module, et $V = M_\Phi$ le Φ -espace engendré où $\Phi = \text{Frac}(\Lambda) = K((T))$ est le corps de fractions de l'anneau $\Lambda = A[[T]]$ (et $K = \text{Frac}(A)$). Pour $S = \Lambda \setminus \{0\}$ on a

$$M \subset M_\Phi = S^{-1}M \simeq \Phi \otimes_\Lambda M.$$

M_Φ est un Φ -espace de dimension finie, disons

$$d = \dim_\Phi M_\Phi (= \dim_\Lambda M).$$

Il existe alors une Φ -base de M_Φ disons $(e_1, \dots, e_d)$ telle qu'on ait

$$M \subset \bigoplus_{i=1}^d \Lambda e_i = L.$$

Proposition 2.2. *M est contenu avec un indice fini dans un Λ -module libre de dimension d.*

Preuve : On va procéder par récurrence sur d .

Por $d = 1$, on a $L = \Lambda e$ et $M = \mathfrak{U}e$ pour un idéal $\mathfrak{U}$, donc

$$M \subset \widehat{\mathfrak{U}}e = \Lambda \mathfrak{a}e,$$

libre avec $(\widehat{\mathfrak{U}}e : M) = (\widehat{\mathfrak{U}} : \mathfrak{U})$ fini.

Supposons que l'hypothèse de récurrence est vérifiée au $d - 1$.

Prenons $x \in M$ tel que $M/\Lambda x$ soit sans torsion, partons de $x_0 \neq 0$ arbitraire dans M ; si $M/\Lambda x_0$ a des éléments de torsion, soit $x_1 \in M$, $x_1 \notin \Lambda x_0$ avec $\lambda x_1 \in \Lambda x_0$, c'est à dire $\lambda x_1 = \mu x_0$ avec $\mu \in \Lambda$, $\lambda \nmid \mu$.

En décomposant x_0 et x_1 sur la base (e_i) , et simplifiant l'égalité pour avoir $\lambda \wedge \mu = 1$. On obtient que λ divise tous les coefficients de x_0 , de sorte qu'on a finalement $x_1 = \frac{x_0}{\lambda} \in M$.

On itère alors en construisant une suite croissante

$$\Lambda x_0 \subset \Lambda x_1 \subset \Lambda x_2 \subset \dots \subset M,$$

qui station (par la propriété noethérienne). Ce qui fournit un $x = x_n$ avec $M/\Lambda x$ sans torsion, de dimension $d - 1$. Par hypothèse de récurrence, ce module est contenu avec un indice fini dans un module libre

$$M/\Lambda x \subseteq \bigoplus_{i=1}^{d-1} \Lambda(x_i + \Lambda x),$$

relevons les $x_i + \Lambda x$ en des $x_i \in M_\Phi$ et posons

$$N = \bigoplus_{i=1}^{d-1} \Lambda x_i.$$

Alors la somme $N \oplus \Lambda x$ est libre, et par construction, contient M avec un indice fini. $\square$

Théorème 2.4. *Tout Λ -module noethérien et sans torsion M , est contenu avec un indice fini dans un unique Λ -module libre $\widehat{M}$ de M_Φ .*

Preuve : Supposons $M \subseteq L_1$ et $M \subseteq L_2$, où $\subseteq$ dénote une inclusion avec indice fini. Alors L_1/M et L_2/M sont finis, donc aussi $(L_1 + L_2)/M$ et $L_1 + L_2$ est contenu avec un indice fini dans L_3 libre.

On peut supposer $L_1 \subset L_2$ emboîtés. Soit (e_i) une base de L_2 et (f_i) une base de L_1 , puis on note m la matrice des (f_i) dans la base (e_i) . On regarde son déterminant, $d = \det(m)$,

- si d est inversible, alors m est inversible et on a $L_1 = L_2$.
- Sinon, il existe un irréductible $p \in \Lambda$ qui divise d . Regardons la réduction de m modulo p . $\hat{m} \in \mathfrak{M}_\Lambda(\Lambda/p\Lambda)$, on trouve que l'image de L_1 dans L_2/pL_2 est contenue dans un hyperplane, noyau d'une forme linéaire φ .

Il suit

$$\begin{aligned} (L_2 : L_1) &\geq (L_2 : L_1 + pL_2) \\ &\geq |\varphi(L_2)| \\ &= (\Lambda : p\Lambda), \end{aligned}$$

infini. $\square$

Remarque: Dans un anneau principal, un sous module M d'un anneau libre L (de dimension finie) possède toujours une base adaptée :

$$\begin{aligned} L &= \bigoplus_{i=1}^d \Lambda e_i \\ M &= \bigoplus_{i=1}^d \Lambda f_i e_i \text{ avec } f_1 | f_2 | \dots | f_d. \end{aligned}$$

Ici on a M contenu avec un indice fini dans $\widehat{M}$

$$\widehat{M} = \bigoplus_{i=1}^d \Lambda x_i,$$

on dispose d'une pseudo-base et, pour $M \subset L$ on peut demander s'il existe une pseudo-base de L qui donne une pseudo-base de M .

Exemple 2.4 (Contre-exemple). $L = \Lambda e_1 + \Lambda e_2$, f, g copremiers dans Λ , $M = \Lambda(fe_1 + ge_2)$, $M \subset L$.

Une pseudo-base de M est nécessairement de la forme $\mu(fe_1 + ge_2)$ avec $\mu \in \Lambda^*$.

Une pseudo-base de L ne peut être formée (à multiplication près par des inversibles), qu'en complétant $c = fe_1 + ge_2$ en une (pseudo) base $(fe_1 + ge_2, f'e_1 + g'e_2)$. Mais la matrice

$$\begin{bmatrix} f & f' \\ g & g' \end{bmatrix}$$

n'est pas inversible puis qu'on a $fg' - f'g \in \mathfrak{M}$, l'idéal maximal de Λ .

2.2.2 Λ -modules de torsion

On s'intéresse maintenant aux Λ -modules noethériens de torsion M .

Définition 2.3. Pour $x \in M$, on note

$$\text{Ann}(x) = \{\lambda \in \Lambda \mid \lambda x = 0\} \neq \{0\},$$

l'annulateur de x , et pour $M = \sum_{i=1}^d \Lambda x_i$

$$\begin{aligned} \text{Ann}(M) &= \{\lambda \in \Lambda \mid \forall x \in M, \lambda x = 0\} \\ &= \bigcap_{i=1}^d \text{Ann}(x_i). \end{aligned}$$

Proposition 2.3. M possède un plus grand sous module fini F , et M/F n'en a pas (autre que le sous module nul).

Preuve : L'ensemble des sous modules finis possède un élément maximal (car M est noethérien). F qui contient tous les sous modules finis (car pour G fini, $F + G$ est encore fini).

□

L'annulateur à priori est un idéal, la proposition suivante révèle sa nature.

Proposition 2.4. Si M est un sous module fini, son annulateur $\mathfrak{A} = \text{Ann}(M)$ est principal.

Preuve : Sinon $\widehat{\mathfrak{A}}M$ serait un sous module fini non nul de M , d'où $(M : \widehat{\mathfrak{A}}M) \leq (\widehat{\mathfrak{A}} : \mathfrak{A})^d$.

□

Définition 2.4. Un Λ -module fini sera dit *pseudo-nul*. Un morphisme φ de Λ -modules sera dit *pseudo-injectif* (resp. *pseudo-surjectif*) lorsque son noyau $\ker(\varphi)$ (resp. son co-noyau) est pseudo-nul ; un *pseudo-isomorphisme* lorsque les deux conditions précédentes sont réunies.

Proposition 2.5. Pour chaque idéal premier de hauteur 1 (i.e. principal)

$$\mathfrak{p} = \Lambda\pi \text{ ou } \Lambda p, \text{ avec } p \in A[T] \text{ distingué et irréductible,}$$

soit $S = \Lambda \setminus \mathfrak{p}$ et $M_{\mathfrak{p}} = S^{-1}M$ le module des fractions (le localisé) de M en $\mathfrak{p}$. On a alors :

- (i) Pour M de torsion d'annulateur $\mathfrak{A} = \text{Ann}(M)$, $M_{\mathfrak{p}} = 0$ pour presque tout $\mathfrak{p}$ (en fait pour $\mathfrak{p} \not\supset \mathfrak{A}$).
- (ii) M fini $\Leftrightarrow M_{\mathfrak{p}} = 0 \ \forall \mathfrak{p}$.
- (iii) $M \sim N$ (sont pseudo-isomorphes) $\Leftrightarrow M_{\mathfrak{p}} \cong N_{\mathfrak{p}} \ \forall \mathfrak{p}$.

Preuve :

- (i) Pour $x \in M$ on a $x_{\mathfrak{p}} = 0$, où $x_{\mathfrak{p}}$ est l'image de x dans $M_{\mathfrak{p}}$. On a $x_{\mathfrak{p}} = 0 \Leftrightarrow \exists \lambda \notin \mathfrak{p}$ avec $\lambda x = 0 \Leftrightarrow \text{Ann}(M) \not\subset \mathfrak{p}$, d'où suit la première assertion.
- (ii) Si M est fini, on a $\text{Ann}(M) \supset \mathfrak{M}^k$ pour un certain k , de sorte qu'on a $\text{Ann}(M) \not\subset \mathfrak{p}$ quelque soit $\mathfrak{p}$, c'est à dire $M_{\mathfrak{p}} = 0$ pour tout $\mathfrak{p}$.

Remarque: La suite $(\mathfrak{M}^k M)_{k \in \mathbb{N}}$ est une suite décroissante de modules finis, d'intersection nulle pour k assez grand.

Inversement, si on a $M_{\mathfrak{p}} = 0$ pour tout $\mathfrak{p}$ quelque soit $x \in M$, $\text{Ann}(x)$ n'est pas contenu dans $\mathfrak{p}$ donc $\text{Ann}(x) \supset \mathfrak{M}^k$ pour un certain k , de sorte que M est annulé par $\mathfrak{M}^k$ pour k assez grand et on a $|M| \leq (\Lambda : \mathfrak{M}^k)^d$ fini.

(iii) Pour $\varphi : M \rightarrow N$ pseudo-isomorphisme. La suite exacte

$$0 \rightarrow \ker(\varphi) \rightarrow M \rightarrow N \rightarrow \operatorname{coker}(\varphi) \rightarrow 0,$$

donne

$$0 \rightarrow \ker(\varphi_p) \rightarrow M_p \rightarrow N_p \rightarrow \operatorname{coker}(\varphi_p) \rightarrow 0.$$

□

Remarque: Pour modules noethériens de torsion, les pseudo-isomorphismes donnent lieu à une relation d'équivalence. En fait on montrera que $M \sim N \Leftrightarrow N \sim M$.

Exemple 2.5 (Contre-exemple). Canoniquement $\mathfrak{M} \sim \Lambda$ mais $\Lambda \not\sim \mathfrak{M}$, où $1 \mapsto$ certain élément α .

Remarque: IL FAUT FAIRE ATTENTION AUX PSEUDO-MORPHISMS !

Proposition 2.6. Soit M un Λ -module noethérien et $T(M)$ son sous module de torsion. Alors M est pseudo-isomorphe à la somme directe

$$M \sim T(M) \oplus L,$$

de $T(M)$ et d'un Λ -module libre (de dimension finie).

Preuve : On sait déjà que $M/T(M)$ est pseudo-libre, i.e. contenu avec un indice fini dans un module libre. Soit $\mathfrak{A} = \operatorname{Ann}(T(M))$, disons $\mathfrak{A} = \Lambda\alpha$. Prenons $c \in \Lambda$, vérifiant $\alpha \wedge c = 1$ et $cL \subset M/T(M)$. Posons $S = c^{\mathbb{N}}$. Nous avons $M \hookrightarrow S^{-1}M$, la suite exacte

$$0 \rightarrow T(M) \rightarrow M \rightarrow M/T(M) \rightarrow 0,$$

donne

$$0 \rightarrow S^{-1}T(M) \rightarrow S^{-1}M \rightarrow S^{-1}(M/T(M)) = S^{-1}L \rightarrow 0.$$

Rélevons dans $S^{-1}M$ une base de $L \subset S^{-1}(M/T(M))$, disons $(x_1, \dots, x_n)$. Et posons

$$M' = \left(\bigoplus_{i=1}^n \Lambda x_i \right) \oplus T(M) \subset S^{-1}M,$$

(qu'est-ce qu'on peut dire de $(M' : M)$?). Nous avons $(M' : M) \leq (L : M/T(M))$ fini, d'où le résultat.

□

2.3 Structure des Λ -modules noethériens et de torsion

Lemme 2.4. Soit M un Λ -module noethérien et de torsion, sans sous module fini, et $f = f_1 f_2$ une factorisation de son annulateur avec $f_1 \wedge f_2 = 1$. On a alors

$$M \sim f_1 M \oplus f_2 M \quad \text{et} \quad f_1 M \oplus f_2 M \sim M,$$

avec $\operatorname{Ann}(f_1 M) = \Lambda f_2$ et $\operatorname{Ann}(f_2 M) = \Lambda f_1$.

Preuve : Observons que la somme $f_1M + f_2M$ est direct, en fait si $x \in f_1M \cap f_2M$, on a $f_2x = 0 = f_1x$, donc $f_1\Lambda + f_2\Lambda \subset \text{Ann}(x)$, ce qui montre que $\Lambda x \cong \Lambda/\text{Ann}(x)$ est fini, mais M n'a pas de module fini, alors Λx est nul.

De même, le quotient $M/(f_1M \oplus f_2M)$ es annulé par f_1 comme pour f_2 , donc est pseudo-nul, de sorte que $f_1M \oplus f_2M$ est un sous module d'indice fini de M . Inversement, l'application naturelle

$$M \ni x \mapsto f_1x + f_2x \in f_1M \oplus f_2M,$$

a pour noyau $\{x \in M \mid f_1x = -f_2x\}$ lequel est annulé par f_1 et f_2 donc pseudo-nul. On va voir que c'est presque surjective car $f_1M \oplus f_2M$ est d'indice fini dans M .

□

Lemme 2.5. *Soient M, N modules noethériens et de torsion, alors $M \sim N \Leftrightarrow N \sim M$.*

Preuve : Supposons $M \sim N$, et soit φ un pseudo isomorphisme $M \xrightarrow{\varphi} N$. Prenons c copremier avec $\widehat{\text{Ann}(M)}$ annihilant $\ker(\varphi)$. Alors $\varphi|_{cM}$ est injectif et cM est d'indice fini dans M (parce que le quotient M/cM est annulé par c et par f).

Ainsi $\varphi(cM)$ est d'indice fini dans N , ce que permet de prendre un élément d copremier avec $\widehat{\text{Ann}(N)} = \Lambda g$ qu'on ait $dN \subset \varphi(cM)$. La multiplication par d dans N est pseudo injective (par $d \wedge g = 1$), de sorte qu'on obtient le pseudo isomorphisme :

$$N \xrightarrow{d} dN \xrightarrow{\varphi^{-1}} cM \hookrightarrow M$$

□

Théorème 2.5. *Soit M un Λ -module noethérien et de torsion sans sous module fini d'annulateur primaire p^e . Alors M est pseudo-isomorphe à une somme directe*

$$M \sim \bigoplus_{i=1}^k \Lambda/p^{e_i}.$$

Preuve : Distinguons les cas $p = \Lambda\pi$ et $p = \Lambda p$ avec p distingué et irréductible.

1er cas ($p = \Lambda p$) : Dans ce cas Λ/p^e est un Λ -module, libre de dimension $e \deg(p) < \infty$, de sorte que M est un A -module de type fini qui est sans A -torsion : son sous module de A -torsion est annulé à la fois par une puissance π^k de l'uniformisante π de A , et par p^e ; il est donc pseudo-nul donc nul. Ainsi M est A -libre, ce qui permet de raisonner par récurrence sur $d = \dim_A(M)$.

✓ $d = 0$ est trivial.

✓ Supposons (HR) la propriété vraie pour M de dimension $< d$.

✓ Prenons x dans M d'annulateur minimal p^e (Un tel x existe sans quoi M serait annulé par p^{e-1}) et reformons la suite exacte

$$0 \rightarrow \underbrace{\Lambda x}_{\cong \Lambda/p^e} \rightarrow M \rightarrow \underbrace{M/\Lambda x}_{\cong M' = \bigoplus \Lambda/p^{e_i}} \rightarrow 0$$

où le quatrième term de la suite est isomorphe a une somme directe $M' = \bigoplus \Lambda/p^{e_i}$, choisissons un $x \notin p$ tel que l'image de $M/\Lambda x$ contienne $cM' = \bigoplus_{i=1}^k \Lambda cx_i$. Relevons les cx_i dans M en disons $y_i \in M$. Nous avons alors $p^{e_i}y_i = fp^{e_i}x \in \Lambda x$ avec $p \nmid f$, de sorte qu'il vient $e'_i \geq e_i$. Remplaçons y_i par $z_i = y_i - fp^{e'_i - e_i}x$ (ce qui ne change pas son image $\bar{z}_i = \bar{y}_i$ dans $M/\Lambda x$). Il suit $p^{e_i}z_i = 0$, donc

$\Lambda z_i \cong \Lambda/p^{e_i}$ et la somme $\sum_{i=1}^k \Lambda z_i$ est directe, isomorphe à

$$\bigoplus_{i=1}^k \Lambda/p^{e_i}.$$

Posons maintenant : $M'' = \left(\bigoplus_{i=1}^k \Lambda z_i \right) + \Lambda x$, cette somme es directe par construction puis qu'on a

$$\Lambda''/\Lambda x \cong \bigoplus_{i=1}^k \Lambda \bar{z}_i = \bigoplus_{i=1}^k \Lambda/\mathfrak{p}^{e_i},$$

et comme $M''/\Lambda x$ contient cM' d'indice fini dans M' , il suit que M'' est d'indice fini dans M . Ceci conclut la preuve.

2ème cas ($\mathfrak{p} = \Lambda\pi$) : Dans ce cas $M/\pi M$ est un $k[[T]]$ module noethérien, somme directe d'un module fini et d'un module libre. On procède comme précédement par recurrence sur la dimension de ce module.

✓ Pour $d = 0$, $M/\pi M$ est fini, donc annulé par une puissance de T , disons $T^k M \subset \pi M$. De $\pi^e M = 0$ on conclut $T^{ke} M = 0$. Ainsi M est annulé par π^e et T^{ke} donc pseudo nul, donc nul, la récurrence se poursuit comme plus haut.

□

Corollaire 2.3 (Théorème fondamental). *Tout Λ -module noethérien est pseudo-isomorphe à un unique Λ -module élémentaire :*

$$M \sim \Lambda^p \oplus \left(\bigoplus_{i=1}^k \Lambda/\pi^{\mu_i} \Lambda \right) \oplus \left(\bigoplus_{i=1}^k \Lambda/\mathfrak{p}_i \Lambda \right),$$

où les $\mathfrak{p}_i$ sont des polynômes distingués, ordonnés par divisibilité.

Définition 2.5. On note $\mu = \sum_{i=1}^k \mu_i$ et $P = \prod_{i=1}^k \mathfrak{p}_i$ et on dit que $\pi^\mu P$ est le polynôme caractéristique du sous module de Λ -torsion de M .

Preuve du corollaire : (Existence) On sait déjà qu'on a

1. $M \sim \Lambda^p \oplus T(M)$

2. $T(M) \sim \bigoplus_{\mathfrak{p}_i} T_{\mathfrak{p}_i}(M)$

3. $T_{\mathfrak{p}_i}(M) \sim \bigoplus_{j=1}^k \Lambda/\mathfrak{p}_i^{e_{i,j}}$, où $e_{i,1} \geq e_{i,2} \geq \dots \geq e_{i,k} > 0$, avec $\mathfrak{p} = \Lambda\pi$ ou $\mathfrak{p} = \Lambda\mathfrak{p}_i$.

Il reste à écrire $\mathfrak{p}_1 = \prod_{\mathfrak{p}_i \neq \pi} \mathfrak{p}_i^{e_{i,1}}$, $\mathfrak{p}_2 = \prod_{\mathfrak{p}_i \neq \pi} \mathfrak{p}_i^{e_{i,2}}$ (avec la convention $e_{i,k} = 0$ pour $k > k_i$)

(Unicité)

·) On a déjà $\rho = \dim_{\Phi}(\Phi \oplus_{\Lambda} M)$, d'où l'unicité de ρ . On écrit par convention $\rho = \dim_{\Lambda} M$.

·) Pour la torsion, le plus simple est de localiser : pour $\mathfrak{p}$ fixe, on prend $S = \Lambda \setminus \mathfrak{p}$ et un regarde $M_{\mathfrak{p}} = S^{-1}M$, comme $\Lambda_{\mathfrak{p}} = S^{-1}\Lambda$ -module, et $\Lambda_{\mathfrak{p}}$ est un anneau local d'unique idéal maximal $\mathfrak{p}_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}\pi$ où $\Lambda_{\mathfrak{p}}\mathfrak{p}$ principal, donc $\Lambda_{\mathfrak{p}}$ est un anneau de valuation discrète. Et l'unicité resulte de l'unicité sur les anneaux principaux.

□

2.4 Appendice : Suites Admissibles

Définition 2.6. On dit qu'une suite $(\omega_n)_{n \in \mathbb{N}}$ d'éléments de Λ est admissible pour un Λ -module noethérien et de torsion M lorsqu'on a :

1. $\omega_n \wedge \mathfrak{p} = 1$, où $\mathfrak{p} = \chi_M(T)$ est le polynôme caractéristique de M .

2. $\omega_0 \in \mathfrak{M}$ et $\frac{\omega_{n+1}}{\omega_n} \in \mathfrak{M}$ pour tout $n \in \mathbb{N}$.

Proposition 2.7. So $(\omega_n)_{n \in \mathbb{N}}$ est une suite admissible par M , on a

$$\left(\bigcup_{n \in \mathbb{N}} \omega_n^{-1} \Lambda \right) \otimes_{\Lambda} M \cong \prod_{p | \chi_M} M_p,$$

$$\omega_n^{-1} \otimes x \mapsto (\omega_n^{-1} x)_p.$$

Remarque: On a $M_p = 0$ pour $p \nmid \chi_M$ et $\omega_n \in \Lambda_p^*$ pour $p | \chi_M$.

Preuve : (Injectivité) Supposons $\omega_n^{-1} \otimes x = \omega_{n+k}^{-1} \otimes \frac{\omega_{n+k}}{\omega_n} x$, ce qui montre l'injectivité.

(Surjectivité) Il s'agit de voir que pour $p | \chi_M$ fixe, $s_p^{-1} x \in M_p$ provient d'un élément $\omega_n^{-1} \otimes y$. écrivons $\chi_M = P^c Q$ avec $p = \Lambda P$ et $Q \wedge P = 1$. Regardons le quotient $QM/Q^2 s_p M$ ($s_p \in \Lambda \setminus p$). Il est annulé par P^c et par $Q s_p$ qui sont copremiers. Il est donc pseudo-nul, donc annulé par ω_n pour n assez grand : $\omega_n QM \subset Q^2 s_p M$, donc $\omega_n Qx = Q^2 s_p y$ pour un $y \in M$. Il suit $(\omega_n^{-1} y)_p = (s_p^{-1} x)_p$ comme attendu et pour $q \neq p$

$$(\omega_n^{-1} y)_q = 0,$$

par $Q \in q$, et finalement $\varphi(\omega_n^{-1} \otimes Qy) = (0, \dots, s_p^{-1} x, \dots, 0)$. Ce qui montre la surjectivité. □

Remarque: Si on regarde $\text{Hom}(\text{coker}(\varphi), K/\Lambda) = M^*$ est appelé le adjoint du module M .

Définition 2.7.

$$\lambda = \sum \deg p_i \quad \text{et} \quad \mu = \sum \mu_i.$$

3 Théorème de paramétrage

3.1 Le contexte arithmétique

$$\begin{array}{c} K_{\infty} \\ \vdots \\ K_n \\ | \\ K_{n-1} \\ \vdots \\ K \end{array} \quad \begin{array}{l} \gamma^{\mathbb{Z}_{\ell}} = \Gamma \\ \mathbb{Z}/\ell^n \mathbb{Z} = \text{Gal}(K_n/K) \end{array}$$

On dispose d'un corps de nombres K , d'une $\mathbb{Z}_{\ell}$ -extension, $K_{\infty} = \bigcup_{n \in \mathbb{N}} K_n$ de group de Galois

$$\text{Gal}(K_{\infty}/K) = \varprojlim \mathbb{Z}/\ell^n \mathbb{Z} = \gamma^{\mathbb{Z}_{\ell}}$$

(celle dernière étant la notation multiplicative) et aussi d'une extension abélienne L/K de degré étranger à ℓ , de group de Galois Δ qu'on regarde en haut de la tour :

$$\Delta = \text{Gal}(LK_{\infty}/K_{\infty}) \cong \text{Gal}(L/K).$$

On note $\Lambda = \mathbb{Z}_\ell[[\gamma - 1]]$ l'algèbre d'Iwasawa en l'indeterminée $\gamma - 1$ et l'algèbre de group

$$\Lambda[\Delta] = \mathbb{Z}_\ell[\Delta][[\gamma - 1]].$$

3.2 Complements sur les représentations

Le groupe Δ est un produit direct de groupes cycliques $\Delta = \prod_{i=1}^r \Delta_i$ d'ordres respectives d_i ; avec $\ell \nmid d_i$.¹ L'algèbre $\mathbb{Q}_\ell[\Delta]$ est une algèbre semi-simple, produit direct de corps $\mathbb{Q}_\ell[\Delta] = \prod_{\varphi} \mathbb{Q}_\varphi$. Plus précisément, on a

$$\mathbb{Q}_\ell[\Delta] = \bigotimes \mathbb{Q}_\ell[\Delta_i]$$

avec

$$\mathbb{Q}_\ell[\Delta_i] \cong \mathbb{Q}_\ell[X]/(X^{d_i} - 1) \cong \prod \mathbb{Q}_\ell[X]/(P_{ij})$$

où les P_{ij} sont les facteurs irréductibles de $X^{d_i} - 1$. Il en result que les facteurs $\mathbb{Q}_\ell[\Delta_i]$ sont des extensions cyclotomiques de $\mathbb{Q}_\ell$ engendrées par des racines d_i -ièmes de l'unité, donc non ramifiées, de sorte que ℓ est encore une uniformisante de $\mathbb{Q}_\ell$. En termes de caractères, les idempotents e_φ associés à la décomposition

$$\mathbb{Q}_\ell[\Delta] = \bigoplus_{\varphi} \underbrace{\mathbb{Q}_\ell[\Delta] e_\varphi}_{\mathbb{Q}_\varphi}$$

sont indexés par les caractères ℓ -adiques φ du group Δ et donnés par

$$e_\varphi = \frac{1}{d} \sum_{\tau \in \Delta} \varphi(\tau^{-1}) \tau \tag{4}$$

Remarque: e_φ est primitif par φ irréductible et on a $\deg(\varphi) = [\mathbb{Q}_\varphi : \mathbb{Q}_\ell]$

Exemple 3.1. $\ell = 3$, $\Delta = V_4 = C_2 \times C_2$, $\Delta = \{1, \sigma, \tau, \sigma\tau\}$ les 4 idempotentes primitifs sont :

$$\begin{aligned} e_1 &= \frac{1}{4}(1 + \tau)(1 + \sigma) \\ e_{\omega_1} &= \frac{1}{4}(1 + \tau)(1 - \sigma) \\ e_{\omega_2} &= \frac{1}{4}(1 - \tau)(1 + \sigma) \\ e_{\omega_3} &= \frac{1}{4}(1 - \tau)(1 - \sigma) \end{aligned}$$

avec la table de caractères

	1	ω_1	ω_2	ω_3
1	1	1	1	1
σ	1	-1	1	-1
τ	1	1	-1	-1
$\tau\sigma$	1	-1	-1	1

1. Cas standard $L = K[\zeta_\ell]$

L'hypothèse $\ell \nmid d$ assure que les idempotents e_φ sont dans $\mathbb{Z}_\ell[\Delta]$. Aussi

$$\mathbb{Z}_\ell[\Delta] = \bigoplus_{\varphi} \mathbb{Z}_\ell[\Delta] e_\varphi$$

est un anneau semi-local, produit direct d'anneaux locaux Z_φ extensions cyclotomiques non ramifiées de $\mathbb{Z}_\ell$, de degré $d_\varphi = \deg \varphi$.

De même l'algèbre de groupe :

$$\Lambda[\Delta] = \bigoplus_{\varphi} \Lambda[\Delta] e_\varphi = \bigoplus_{\varphi} Z_\varphi[[\gamma - 1]]$$

est une somme directe d'algèbres d'Iwasawa sur des anneaux locaux principaux Z_φ d'uniformisante ℓ , de corps résiduel

$$F_\varphi = Z_\varphi / \ell Z_\varphi \cong \mathbb{F}_{\ell^{d_\varphi}}$$

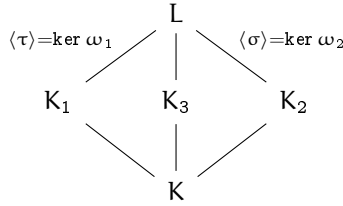
l'unique extension de degré d_φ de $\mathbb{F}_\ell$ (la non ramification donnant $[\mathbb{F}_\varphi : \mathbb{F}_\ell] = [Z_\varphi : \mathbb{Z}_\ell] = d_\varphi$).

Plus généralement, tout $\Lambda[\Delta]$ -module M s'écrit comme somme directe de ses composantes isotypiques :

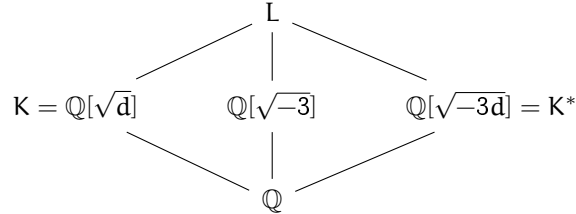
$$M = \bigoplus_{\varphi} e_\varphi M,$$

chaque $M_\varphi = e_\varphi M$ étant un $\Lambda_\varphi = Z_\varphi[[\gamma - 1]]$ -module.

Exemple 3.2. En reprenant l'Exemple 3.1. On a



et $\ker \omega_3 = \langle \sigma\tau \rangle$. Par exemple, pour



Le 3-groupe des classes d'ideaux de L , est la somme directe

$$Cl_L = Cl_K \oplus Cl_{K^*}.$$

3.3 Les paramètres structurels d'un $\Lambda[\Delta]$ -module

Soit M un $\Lambda[\Delta]$ -module noethérien. Ses composantes isotypiques M_φ sont des $\Lambda_\varphi = Z_\varphi[[\gamma - 1]]$ -module noethériens, pseudo isomorphes comme tels à des modules élémentaires

$$M_\varphi \sim \Lambda_\varphi^{e_\varphi} \oplus \left(\bigoplus_i \Lambda_\varphi / \ell^{\mu_{\varphi,i}} \Lambda_\varphi \right) \oplus \left(\bigoplus_j \Lambda_\varphi / P_{\varphi,j} \Lambda_\varphi \right)$$

où, pour φ fixé, les $P_{\varphi,j}$ sont des polynômes distingués de l'anneau $Z_\varphi[\gamma-1] = Z_\varphi[\gamma]$ ordonnés par divisibilité. On pose :

$$\rho_\varphi = \dim_{\Lambda_\varphi} M_\varphi; \quad \mu_\rho = \sum_i \mu_{\varphi,i}; \quad \lambda_\varphi = \sum_j \deg(P_{\varphi,j}).$$

Définition 3.1. On dit que les caractères de $R_{\mathbb{Z}_\ell(\Delta)}$

$$\rho = \sum_\varphi \rho_\varphi \rho, \quad \mu = \sum_\varphi \mu_\varphi \varphi \quad \text{et} \quad \lambda = \sum_\varphi \lambda_\varphi \varphi,$$

sont les invariants structurels du $\Lambda(\Delta)$ -module M .

Définition 3.2. On dit qu'une suite $(\chi_n)_{n \in \mathbb{N}}$ de $\mathbb{Z}_\ell[\Delta]$ -modules finis est paramétrée pour les caractères (ρ, μ, λ) lorsque l'ordre $\ell^{\chi_\varphi(n)}$ de la ϕ -composante de χ_n est asymptotiquement donnée par la formule

$$\chi_\varphi(n) \approx d_\varphi \rho_\varphi n \ell^n + d_\varphi \mu_\varphi \ell^n + d_\varphi \lambda_\varphi n \quad (5)$$

où le symbole $\approx$ signifie que la différence entre les nombres de droite et de gauche est bornée (Strictement paramétrée lorsque la différence est ultimement constante).

3.4 Enoncé du théorème fondamental

Pour tout $n \geq 1$, on pose $\nabla_n = \Lambda \ell + \Lambda \omega_n$ avec $\omega_n = \gamma^{\ell^n} - 1$. Ainsi :

·) $\nabla_1 = \Lambda \ell + \Lambda(\gamma - 1)$ est l'idéal maximal de l'algèbre d'Iwasawa $\mathbb{Z}_\ell[[\gamma - 1]]$.

Lemme 3.1. On a $\gamma^{\ell^n} - 1 \equiv (\gamma - 1)^{\ell^n} \pmod{\ell}$.

(Via $(x + a)^\ell = x^\ell + a^\ell$ dans $\mathbb{F}_\ell[x]$.) Il suit :

·) $\nabla_n \subset \nabla_1^n$, donc les ∇_n forment donc une filtration de Λ par des idéaux d'indice fini.

Théorème 3.1. Si M est un $\Lambda[\Delta]$ -module noethérien d'invariants structurels (ρ, μ, λ) la suite des quotients $(M/\nabla_n M)_{n \in \mathbb{N}}$ est paramétrée par les mêmes caractères (ρ, μ, λ) .

$\Lambda/\nabla_n \cong \mathbb{Z}/\ell^n \mathbb{Z}[\gamma - 1]/(\omega_n) = \mathbb{Z}/\ell^n \mathbb{Z}[\gamma]/(\omega_n)$ donne :

$$(\Lambda : \nabla_n) = \ell^{n \ell^n}.$$

Preuve du théorème : Regardons d'abord les cas où M est un module indécomposable et élémentaire.

1er cas $M_\varphi = \Lambda_\varphi$. On a alors

$$\begin{aligned} M_\varphi / \nabla_n M_\varphi &= \Lambda_\varphi / \nabla_n \Lambda_\varphi \\ &= \mathbb{Z}_\varphi[[\gamma - 1]]/(\ell^n, \omega_n) \\ &= (\mathbb{Z}_\varphi / \ell^n \mathbb{Z}_\varphi)[\gamma - 1]/(\omega_n) \\ &= (\mathbb{Z}_\varphi / \ell^n \mathbb{Z}_\varphi)[\gamma]/(\omega_n) \\ &= \bigoplus_{i=0}^{\ell^n - 1} (\mathbb{Z}_\varphi / \ell^n \mathbb{Z}_\varphi) \tilde{\gamma}^i. \end{aligned}$$

D'où $(M_\varphi : \nabla_n M_\varphi) = (\mathbb{Z}_\varphi : \ell^n \mathbb{Z}_\varphi)^{\ell^n}$, ce qui donne bien $\chi_\varphi(n) = d_\varphi n \ell^n$, puisque $\mathbb{Z}_\varphi / \ell^n \mathbb{Z}_\varphi$ est un $\mathbb{Z}/\ell^n \mathbb{Z}$ -module libre de dimension d_φ .

2ème cas $M_\varphi = \Lambda_\varphi / \ell^{m=\mu_\varphi} \Lambda_\varphi$. Pour $n \geq \mu_\varphi$, on a directement

$$M_\varphi / \nabla_n M_\varphi = (\mathbb{Z}_\varphi / \ell^{\mu_\varphi} \mathbb{Z}_\varphi)[\gamma]/(\omega_n)$$

d'où, après ce qui précède :

$$\chi_\varphi(n) = d_\varphi \mu_\varphi \ell^n.$$

3ème cas $M_\varphi = \Lambda_\varphi / P_\varphi \Lambda_\varphi$. Comme opérateur sur M_φ on a vu qu'on a $\frac{\omega_{n+1}}{\omega_n} = \mu_n \ell$ pour un inversible $\mu_n \in \Lambda_\varphi$, de sorte qu'on a (pour $n \geq n_0$) $M_\varphi / \nabla M_\varphi = M_\varphi / \ell^{n-n_0} \nabla_{n_0} M_\varphi$.

Il suit

$$(M_\varphi : \nabla_n M_\varphi) = \underbrace{(M_\varphi : \nabla_{n_0} M_\varphi)}_{\text{constant finie}} \times \underbrace{(\nabla_n M_\varphi : \ell^{n-n_0} \nabla_{n_0} M_\varphi)}_{Z_\varphi\text{-module libre de dimension } \deg(P_\varphi)}.$$

Donc $M_\varphi = \Lambda_\varphi / (P_\varphi) \cong Z_\varphi^{\deg(P_\varphi)}$.

Finalement, on obtient $(M_\varphi : \nabla_n M_\varphi) \approx (Z_\varphi : \ell^{n-n_0} Z_\varphi)^{\deg(P_\varphi)}$ ce qui donne bien

$$\chi_\varphi(n) \approx n \deg(P_\varphi) d_\varphi,$$

puisque Z_φ est lui même un $\mathbb{Z}$ -module libre de dimension $d_\varphi = [Q_\varphi : \mathbb{Q}_\ell]$.

Remarque: La formule de paramétrage annoncée est donc valable pour tout $\Lambda[\Delta]$ -module élémentaire E .

Cas général : Soit maintenant M un $\Lambda[\Delta]$ -module noethérien arbitraire.

étape 1 : Soit F le sous-module fini de M . Alors M et $\widetilde{M} = M/F$ ont leur quotients respectifs

$$M_n = M / \nabla_n M \text{ et } \widetilde{M}_n = \widetilde{M} / \nabla_n \widetilde{M}$$

identiquement paramétrés.

Preuve : Partons de la suite exacte courte :

$$0 \rightarrow F \rightarrow M \rightarrow \widetilde{M} \rightarrow 0.$$

De $\bigcap_{n \in \mathbb{N}} \nabla_n F = 0$ on conclut que à partir d'un certain n assez grand (disons $n \geq n_0$) $\nabla_n F = 0$, puisque les $\nabla_n F$ forment une suite décroissant de sous modules finis. On a aussi la suite exacte :

$$0 \rightarrow \underbrace{F + \nabla_n M / \nabla_n M}_{\cong F / (F \cap \nabla_n M)} \rightarrow M / \nabla_n M \rightarrow \underbrace{\widetilde{M} / \nabla_n \widetilde{M}}_{= M / F + \nabla_n M} \rightarrow 0$$

où $F \cap \nabla_n M$ est une suite décroissante de sous modules finis d'intersection 0 car $\bigcap \nabla_n M = 0$, donc nulle pour n assez grand.

On conclut qu'on a

$$0 \rightarrow F \rightarrow M / \nabla_n M \rightarrow \widetilde{M} / \nabla_n \widetilde{M} \rightarrow 0,$$

donc $(M_\varphi : \nabla_n M_\varphi) = |F_\varphi| (\widetilde{M}_\varphi : \nabla_n \widetilde{M}_\varphi)$ pour $n \geq n_0$. □

étape 2 : On suppose maintenant M est un sous module fini, i.e. d'indice fini donc un module élémentaire E , autrement dit qu'on a une suite exacte

$$0 \rightarrow M \hookrightarrow E \rightarrow F \rightarrow 0$$

avec F fini, et donc $\nabla_n F = 0$ pour $n \geq n_0$, i.e. $\nabla_n E \subset M$. Il suit :

$$0 \rightarrow \nabla_n E / \nabla_n M \rightarrow M / \nabla_n M \rightarrow E / \nabla_n E \rightarrow E / M + \nabla_n E \rightarrow 0.$$

Et il s'agit de voir que la suite des noyaux $\nabla_n E / \nabla_n M$ est de paramètres tous nuls.

On peut observer que l'ordre du quotient à gauche $(\nabla_n E : \nabla_n M)$ est borné, écrivons :

$$E/M \cong \prod_{i=1}^k \mathbb{Z}_\ell / \ell^{e_i} \mathbb{Z}_\ell,$$

la factorization du ℓ -groupe fini E/M , et relevons en $(x_1, \dots, x_k) \in E^k$ une système de générateurs. Il suit que

$$E = \sum_{i=1}^k \mathbb{Z}_\ell x_i + M$$

donc

$$\begin{aligned} \nabla_n E &= \ell^n E + \omega_n E \\ &= \sum_{i=1}^k \mathbb{Z}_\ell \ell^n x_i + \sum_{i=1}^k \mathbb{Z}_\ell \omega_n x_i + \nabla M, \end{aligned}$$

de sorte que $\nabla_n E / \nabla_n M$ est engendré pour les classes des $\ell^n x_i$ et des $\omega_n x_i$ qui sont d'ordre fini (majoré par ℓ^{e_i}). On a donc :

$$\begin{aligned} (\nabla_n E : \nabla_n M) &\leq \prod_{i=1}^k \ell^{e_i} \times \ell^{e_i} \\ &= (E : M)^2, \end{aligned}$$

de sorte que les $E / \nabla_n E$ et les $M / \nabla_n M$ sont identiquement paramétrés.

Remarque: En fait, si E est sans torsion, on peut montrer que le quotient à gauche est ultimement constant $(\nabla_n E / \nabla_n M)$.

Pour voir cela, regardons la suite exacte

$$\begin{aligned} 0 \rightarrow \ell^n \omega_n E / \ell^n \omega_n M \rightarrow \ell^n E / \ell^n M \oplus \omega_n E / \omega_n M &\rightarrow \nabla_n E / \nabla_n M \rightarrow 0, \\ (x + \ell^n M, y + \omega_n M) &\mapsto x - y + \nabla_n M. \end{aligned}$$

Ici E_φ est supposé Λ_φ -libre de sorte qu'on a : $\ell^n E_\varphi \cap \omega_n E_\varphi = \ell^n \omega_n E_\varphi$ pour chaque φ , donc finalement

$$\ell^n E \cap \omega_n E = \ell^n \omega_n E.$$

On a

$$\begin{aligned} \ell^n E / \ell_n M &\xrightarrow{\ell} \ell^{n+1} E / \ell^{n+1} M \\ \omega_n E / \omega_n M &\xrightarrow{\omega_{n+1} / \omega_n} \omega_{n+1} E / \omega_{n+1} M \\ \ell^n \omega_n E / \ell^n \omega_n M &\xrightarrow{\ell \frac{\omega_{n+1}}{\omega_n}} \ell^{n+1} \omega_{n+1} E / \ell^{n+1} \omega_{n+1} M. \end{aligned}$$

En général, on peut écrire $E = T \oplus P$ avec T de torsion et P projectif et remarquer que les facteurs : $\Lambda_\varphi / \ell^\mu \Lambda_\varphi$ sont tués par ℓ^n pour $n \geq \mu$, tandis que pour les facteurs $\Lambda_\varphi / P_\varphi \Lambda_\varphi$, on a (comme operateur) $\frac{\omega_{n+1}}{\omega_n} \sim \ell$, donc le module $\partial^n E := \ell^n E \cap \omega_n E$ est donné par :

•

$$\begin{aligned} \partial^n T &= \ell^n T \wedge \omega_n T \\ &= \begin{cases} \text{Pour les facteurs } \Lambda_\varphi / \ell^\mu \Lambda_\varphi \text{ on a } \omega_n T(\ell) \\ \text{Pour les facteurs } T(P) \text{ on a } \ell^{n-n_0} \partial^{n_0} T(\ell) \end{cases} \end{aligned}$$

Où $T = T(\ell) + T(P)$.

- $\partial^n P = \ell^n P \cap \omega_n P = \ell^n \omega_n P$ (déjà vu).

□

3.5 Application arithmétique

Dans la situation arithmétique c'est en fait un peu plus compliqué. On dispose d'un $\Delta[\Lambda]$ -module noethérien X et on s'intéresse aux quotients non pas $X/\omega_n X$ mais $X/\frac{\omega_n}{\omega_e}(\omega_e X + Y_e)$, où Y_e est un $\mathbb{Z}_\ell$ -module module de type fini telque $\omega_e X + Y_e$ soit un $\Lambda[\Delta]$ -sous module de X . En particulier, on est amené à étudier si la suite

$$X_n = X/\nabla_n X + \frac{\omega_n}{\omega_e} Y_e$$

est paramétrée. Le résultat alors est le suivant :

Théorème 3.2. *Dans la situation précédente soient (ρ, μ, λ) les paramètres structurels du $\Lambda[\Delta]$ -module X . Il existe alors un caractère $\kappa \leq \ell^e \rho$, tel que la suite $(X_n)_{n \in \mathbb{N}}$ soit paramétrée par $(\rho, \mu, \bar{\lambda} = \lambda - \kappa)$.*

Preuve :

1ère étape : Réduction au cas élémentaire.

- Le remplacement de X par $\tilde{X} = X/F$ où F est son sous module fini, conduit à la suite exacte

$$0 \rightarrow F/F \cap (\nabla_n X + \frac{\omega_n}{\omega_e} Y_e) \rightarrow X_n \rightarrow \underbrace{X/\nabla_n X + \frac{\omega_n}{\omega_e} Y_e + F}_{=: \tilde{X}_n} \rightarrow 0,$$

où $F \cap (\nabla_n X + \frac{\omega_n}{\omega_e} Y_e)$ est une suite décroissante de sous modules finis, donc stationnaire.

- On peut aussi supposer que X s'injecte dans E élémentaire ce qui donne la suite :

$$0 \rightarrow X \rightarrow E \rightarrow F \rightarrow 0$$

puis

$$0 \rightarrow \frac{X_n \cap (\nabla_n E + \frac{\omega_n}{\omega_e} Y_e)}{\nabla_n X + \frac{\omega_n}{\omega_e} Y_e} \rightarrow X_n \rightarrow E_n \rightarrow E/X + \nabla_n E + \frac{\omega_n}{\omega_e} Y_e$$

où le terme de droite est une suite croissante donc stationnaire et on a

$$\frac{X_n \cap (\nabla_n E + \frac{\omega_n}{\omega_e} Y_e)}{\nabla_n X + \frac{\omega_n}{\omega_e} Y_e} = \frac{(\nabla_n E + \frac{\omega_n}{\omega_e} Y_e)}{\nabla_n X + \frac{\omega_n}{\omega_e} Y_e},$$

le quotient à droite ayant order $\leq (E : X)^2$.

2ème étape : étude du cas élémentaire.

Soit $E = T \oplus P$ avec T de torsion et P projectif.

- Partie projective $P \cong E/T := \bar{E}$. Pour chaque caractère φ regardons le quotient $P_n = E/(\nabla_n E + \frac{\omega_n}{\omega_e} Y_e + T)$, i.e.

$$P_n = E/(T + \ell^n E + \underbrace{\frac{\omega_n}{\omega_e} (\omega_e E + Y_e)}_{=: F_e})$$

En oubliant provisoirement d'écrire l'indice φ . Le quotient $\bar{E}/\bar{F}_e$ est un Λ_φ -module annulé par ω_e . Sa décomposition élémentaire donne

$$\bar{E}/\bar{F}_e \sim \bigoplus_{P_\varphi} \Lambda_\varphi / P_\varphi \Lambda_\varphi$$

où les P_φ sont des polynômes distingués qui divisent $\omega_e = (\gamma - 1)^{\ell^e} - \lambda$.

Et nous avons à étudier $\bar{E}/(\ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e)$. On décompose $(\bar{E} : \ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e)$ en deux facteurs :

$$(\bar{E} : \ell^n \bar{E} + \bar{F}_e)(\ell^n \bar{E} + \bar{F}_e : \ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e).$$

$\bar{E}/\bar{F}_e$ est un Z_φ -module libre de dimension $\sum \deg(P_\varphi) = \kappa_\varphi$, sa valuation est donc $n\kappa_\varphi$ le deuxième facteur est $(\bar{F}_e : \bar{F}_e \cap (\ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e))$.

On peut supposer que Y_e est un $\mathbb{Z}_\ell[\Delta]$ -module (Quitte à remplacer Y_e par $\mathbb{Z}_\ell[\Delta]Y_e$) et on impose à F_e d'être stable par $\mathbb{Z}_\ell[[\gamma - 1]]$ donc finalement d'être un $\Lambda[\Delta]$ -module.

Ceci permet de décomposer en φ composants à l'aide des idempotents

$$e_\varphi = \frac{1}{|\Delta|} \sum_{\tau \in \Delta} \varphi(\tau^{-1}) \tau.$$

• On est aussi ramenés au cas où E est un Λ module élémentaire pour $\Lambda = A[[\gamma - 1]]$ où $A = Z_\varphi$ est une extension non ramifiée de $\mathbb{Z}_\ell$ de degré $d = [A : \mathbb{Z}_\ell]$, les théorèmes de structure donnent :

$$E = L \oplus T$$

avec $L \cong \Lambda^\rho$ libre, T de torsion.

Strategie : On decoupe l'indice en 2 parties :

$$\left(E : \ell^n E + \frac{\omega_n}{\omega_e} F_e \right) = \left(E : \ell^n E + \frac{\omega_n}{\omega_e} F_e + T \right) \times \left(T : T \cap (\ell^n E + \frac{\omega_n}{\omega_e} F_e) \right)$$

1ère étape : La contribution de la partie libre.

On note $\bar{E} = E/T \cong L = \Lambda^\rho$. On s'intéresse au quotient $\bar{E}/\ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e$.

On observe que E/F_e et donc $\bar{E}/\bar{F}_e$ est de Λ -torsion. Puisqu'on a

$$\begin{aligned} \dim_\Lambda(F_e) &\geq \dim_\Lambda(\omega_e E) \\ &\geq \dim_\Lambda E = \rho, \end{aligned}$$

donc l'égalité $\dim_\Lambda(F_e) = \rho$.

Le théorème de structure donne : $\bar{E}/\bar{F}_e \sim \bigoplus_{i=1}^r \Lambda/(P_i)$ avec $P_1|P_2|\dots|P_r|\omega_e$ et donc $\sum_{i=1}^r \deg(P_i) \leq r\ell^e \leq \rho\ell^e$, disons $\sum \deg(P_i) = \rho\ell^e - \kappa$.

On a :

$$\left(\bar{E} : \ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e \right) = (\bar{E} : \ell^n \bar{E} + \bar{F}_e) \left(\bar{F}_e : \bar{F}_e \cap (\ell^n \bar{E} + \frac{\omega_n}{\omega_e} \bar{F}_e) \right)$$

• d'un côté on a : $\bar{E}/\bar{F}_e \approx \Lambda^{\sum \deg(P_i)}$ donc

$$(\bar{E} : \bar{F}_e + \ell^n \bar{E}) \approx (\Lambda : \ell^n \Lambda)^{\sum \deg(P_i)}$$

est paramétrée par

$$(0, 0, d \sum \deg(P_i)).$$

- D'un autre côté on a : $\overline{F_e} \cap (\ell^n \overline{E} + \frac{\omega_n}{\omega_e} \overline{F_e}) = \frac{\omega_n}{\omega_e} \overline{F_e} \underbrace{(\overline{F_e} \cap \ell^n \overline{E})}_{\ell^n \sqrt{\overline{F_e}}}$.

La suite $\ell^n \sqrt{\overline{F_e}} = \{\chi \in \overline{E} \mid \ell^n \chi \in \overline{F_e}\}$ est une suite croissante de sous modules de $\overline{E}$ qui stationne : on a $\sqrt{\overline{F_e}} = \ell^\alpha \sqrt{\overline{F_e}}$ pour un certain $\alpha = n_0$.

Le deuxième indice est donc

$$(\overline{F_e} : \frac{\omega_n}{\omega_e} \overline{F_e} + \ell^n \sqrt{\overline{F_e}}) = \frac{(\overline{F_e} : \frac{\omega_n}{\omega_e} \overline{F_e} + \ell^n \overline{F_e})}{(\frac{\omega_n}{\omega_e} \overline{F_e} + \ell^n \sqrt{\overline{F_e}} : \frac{\omega_n}{\omega_e} \overline{F_e} + \ell^n \overline{F_e})}$$

au numerateur on a $\overline{F_e} \sim \overline{E} \cong \Lambda^\rho$ (car $\overline{F_e}$ est pseudo-libre de dimension ρ), l'indice en haut est donc (à une borné près)

$$\left(\Lambda : \frac{\omega_n}{\omega_e} \Lambda + \ell^n \Lambda \right)^\rho = (\Lambda : \rho^n \Lambda)^{\rho \deg(\frac{\omega_n}{\omega_e})}$$

avec $\deg(\frac{\omega_n}{\omega_e}) = \ell^n - \ell^e$.

En conclusion l'indice est paramétré par

$$(\rho, 0, -\rho \ell^e)$$

Au dénominateur on a :

$$\left(\ell^n \sqrt{\overline{F_e}} : \underbrace{\left(\ell^n \sqrt{\overline{F_e}} \cap \frac{\omega_n}{\omega_e} \overline{F_e} \right)}_{\in \ell^n \frac{\omega_n}{\omega_e} \sqrt{\overline{F_e}}} + \ell^n \overline{F_e} \right)$$

Ces indices forment une suite décroissante donc stationnaire.

En conclusion : La contribution de la partie libre est paramétrée par

$$d(\rho, 0, -\kappa)$$

2ème étape : Contribution de la torsion T.

$\left(T : T \cap \left(\ell^n E + \frac{\omega_n}{\omega_e} F_e \right) \right)$ avec $T = \bigoplus_{i=1}^r \Lambda / f_i \Lambda$, $\ell^n E + \frac{\omega_n}{\omega_e} F_e = \nabla_n E + \frac{\omega_n}{\omega_e} Y_e$, l'indice c'est une fonction décroissante de Y_e .

Notons $\hat{Y}_e = \bigoplus Y_i$ la somme directe des projections de Y_e sur les divers facteurs $\Lambda / f_i \Lambda$. On a

$$0 \subset Y_e \subset \hat{Y}_e$$

On fait le calcul pour 0 et pour $\hat{Y}_e$ en raisonnant facteur par facteur.

- Pour 0 et $T_i = \Lambda / f_i \Lambda$ on obtient :

$$(T_i : T_i \cap \nabla_n E) = (T_i : \nabla_n T_i),$$

on obtient (calcul déjà fait) que les paramètres sont les paramètres structuels

$$(0, \mu, \lambda_i) d.$$

- Pour $\hat{Y}_e$ et $T_i = \Lambda/f_i\Lambda$ on obtient

$$\begin{aligned} \left(T_i : (T_i \cap \nabla_n E) + \frac{\omega_n}{\omega_e} Y_i \right) &= \left(T_i : \nabla_n T_i + \frac{\omega_n}{\omega_e} Y_i \right) \\ &= \left(\Lambda : f_i \Lambda + \nabla_n + \frac{\omega_n}{\omega_e} Y_i \right). \end{aligned}$$

La difference par rapport au calcul précédent est donc donnée par

$$(\nabla_n T_i + \frac{\omega_n}{\omega_e} Y_i : \nabla_n T_i)$$

- Pour $f_i = \ell^{e_i}$ on a : $\ell^n T_i = 0$ pour $n \geq e_i$ et il reste :

$$\left(\omega_n T_i + \frac{\omega_n}{\omega_e} Y_i : \omega_n T_i \right)$$

et on passe de n à $n+1$ par action de $\frac{\omega_n}{\omega_{n+1}}$ donc la suite décroît donc stationne.

- Pour $f_i = (r-1)^{d_i} + \ell g_i$ distingué, avec (comme operateur) $\frac{\omega_n}{\omega_{n+1}} \sim \ell$, de sorte qu'aussi on passe de n à $n+1$ par action de ℓ et la suite décroît donc stationne.

□

4 Introduction à la théorie des corps de classes

4.1 La théorie de Chevalley

- Point de vue local :

Soit K_p un corps local (i.e. une extension finie de $\mathbb{Q}_p$). On a la décomposition

$$\begin{aligned} K_p^\times &= U_p \times \pi_p^\mathbb{Z} \\ &= \mu_p^0 \times U_p^1 \times \pi_p^\mathbb{Z}, \end{aligned}$$

où μ_p^0 est l'ensemble de racines de l'unité d'ordre étranger à p ; on a que $\mu_p^0 \simeq K_p^\times$, le groupe multiplicative du corps résiduel d'ordre $N(p) - 1$. Le groupe $U_p^1 \simeq \mu_p \times \mathbb{Z}_p^{[K_p:\mathbb{Q}_p]}$ sont les unités principales, racines de l'unité d'ordre divisible par p et π_p est un uniformisante arbitraire.

Théorème 4.1. *Il existe une application injective continue (dite d'Artin) d'image dense,*

$$K_p^\times \longrightarrow \text{Gal}(K_p^{ab}/K_p)$$

à valeurs dans le groupe de Galois de l'extension abélienne maximale de K_p , qui envoie U_p sur le sous groupe d'innertie.

Voir [1].

- Point de vue global :

On définit le groupe des idèles

$$\begin{aligned} J_K &= \prod_{p \in \text{Pl}(K)}^{\text{res}} K_p^\times \\ &= \{ (x_p) \in \prod K_p^\times \mid x_p \in U_p \text{ pour presque tout } p \} \end{aligned}$$

- Pour p finie : $K_p^\times = U_p \times \pi_p^\mathbb{Z}$ et $\text{Gal}(K_p^{\text{ab}}/K_p) \simeq U_p \times \pi_p^\mathbb{Z}$.
- Pour p réelle : $K_p^\times = \mathbb{R}^\times \simeq \{\pm 1\} \times \mathbb{R}$ et $\text{Gal}(\mathbb{C}/\mathbb{R}) \simeq \{\pm 1\}$.
- Pour p complexe : $K_p^\times = \mathbb{C}^\times = \mathbb{R} \times \mathbb{R}/\mathbb{Z}$ et $\text{Gal}(\mathbb{C}/\mathbb{C}) = 1$.

On note $U_K = \prod_{p \in \text{Pl}(K)} U_p$ le sous groupe des idèles unité (avec la convention $U_p = 1$ pour $p|\infty$).

Théorème 4.2. *Les applications d'Artin locales induisent un morphisme surjectif :*

$$J_K \twoheadrightarrow \text{Gal}(K^{\text{ab}}/K)$$

(pour la topologie produit sur J_K) qui envoie $K_p^\times$ dans le sous groupe de décomposition $D_p(K^{\text{ab}}/K)$ et U_p sur le sous groupe d'inertie $I_p(K^{\text{ab}}/K)$.

Le noyau de ce morphisme contient le sous groupe des idèles principaux. Image diagonale de $K^\times$ dans J_K et le noyau du morphisme induit sur $J_K/K^\times$ est la composante connexe de 1 dans ce quotient.

Scolie : Dans la correspondance du corps de classes (héritée de la théorie de Galois) les extensions (abéliennes) finies sont associées aux sous groupes de normes :

- Dans le cas local : les extensions abéliennes L_p de K_p sont associés aux sous groupes $N_{L_p/K_p}(L_p^\times)$ de $K_p^\times$ et on a donc :

$$\begin{aligned} \text{Gal}(L_p/K_p) &= K_p^\times / N_{L_p/K_p}(L_p^\times) \\ I(L_p/K_p) &= U_p / N_{L_p/K_p}(U_p) \end{aligned}$$

- Dans le cas global on a :

$$\text{Gal}(L/K) \simeq J_K / N_{L/K}(J_K) K^\times.$$

Remarque:

1. Pour une extension finie quelconque L/K on a :

$$\begin{array}{ccccc} K^* & & K^{\text{ab}} & & K^{\text{ab}}L & & L^{\text{ab}} \\ & & | & & | & & / \\ N_{L/K}(J_L)K^* & & K^{\text{ab}} \cap L & \xrightarrow{\quad} & L & & \\ & & | & & & & \\ J_K & & K & & & & \end{array}$$

2. La norme $N_{L/K}$ regardée des $J_L/L^\times$ vers $J_K/K^\times$ correspond à la restriction des automorphismes de $\text{Gal}(L^{\text{ab}}/L)$ dans $\text{Gal}(K^{\text{ab}}/K)$, où $\sigma \mapsto \sigma|_{K^{\text{ab}}}$.

4.2 La théorie ℓ -adique.

On se donne un nombre premier ℓ et on se focalise sur les (pro)- ℓ -extensions et on va remplacer les groupes classiques (locaux et globaux) par des $\mathbb{Z}_\ell$ -modules (topologiques).

4.2.1 Point de vue local

- Pour une place finie, on a la décomposition $K_p^\times = \mu_p^0 \times U_p^1 \times \pi_p^\mathbb{Z}$. On pose

$$\mathcal{R}_{K_p} := \varprojlim_k K_p^\times / K_p^{\times \ell^k} = \left(\varprojlim_k U_p / U_p^{\ell^k} \right) \times \pi_p^{\mathbb{Z}_\ell},$$

le ℓ -completé profini de $K_p^\times$.

— Pour $p \nmid \ell$, on a $\mathcal{U}_p = \mu_p^0 \mathcal{U}_p^{(1)}$ étant $\mathcal{U}_p^{(1)}$ un $\mathbb{Z}_p$ -module ℓ divisible, on obtient

$$\mathcal{U}_p = \varprojlim_k \mathcal{U}_p / \mathcal{U}_p^{\ell^k} \simeq \mu_p$$

le ℓ -sous groupe de Sylow de μ_p^0 .

— Pour $p|\ell$, on a $\mathcal{U}_p = \mu_p^0 \mathcal{U}_p^{(1)}$ où μ_p^0 est un groupe ℓ -divisible et $\mathcal{U}_p^{(1)}$ est un $\mathbb{Z}_\ell$ -module de type fini (en fait $\dim_{\mathbb{Z}_\ell} \mathcal{U}_p^{(1)} = [K_p : \mathbb{Q}_\ell]$). Il vient ici

$$\mathcal{U}_p = \mathcal{U}_p^{(1)}.$$

En résumé, on obtient

$$\mathcal{R}_{K_p} = \mathcal{U}_p \pi_p^{\mathbb{Z}_\ell} \text{ avec } \mathcal{U}_p = \begin{cases} \mu_p & \text{pour } p \nmid \ell \\ \mathcal{U}_p^{(1)} & \text{pour } p \mid \ell \end{cases}$$

• Pour p réelle, la même construction donne :

$$\mathcal{R}_{\mathbb{R}} = \mu_p = \begin{cases} \{\pm 1\} & \text{pour } \ell = 2, \\ 1 & \text{sinon.} \end{cases}$$

• Pour p complexe, on obtient :

$$\mathcal{R}_{\mathbb{C}} = 1 \text{ toujours.}$$

Théorème 4.3. *L'application d'Artin induit un isomorphisme de $\mathbb{Z}_\ell$ -modules topologiques de $\mathcal{R}_{K_p}$ sur le groupe de Galois $G_p = \text{Gal}(K^{\text{ab}}/K)$ de la pro- ℓ -extension abélienne maximale de K_p ; qui envoie $\mathcal{U}_p$ sur $\text{In}(K^{\text{ab}}/K)$.*

Exemple 4.1. On a deux cas :

1. Pour $p \nmid \ell$, on a donc $G_p \simeq \mathcal{R}_{K_p} = \mu_p \cdot \pi_p^{\mathbb{Z}_\ell}$.

$$\begin{array}{ccc} & \mu_p & \\ & \swarrow \quad \searrow & \\ K_p^{\text{nr}} & \xrightarrow{\quad} & K_p^{\text{ab}} \\ \mathbb{Z}_\ell \left(\begin{array}{c} | \\ | \\ \vdots \end{array} \right. & & \vdots \\ & K_p & \end{array}$$

2. Pour $p \mid \ell$, on a

$$\begin{aligned} G_p &\simeq \mathcal{U}_p \cdot \pi_p^{\mathbb{Z}_\ell} \\ &\simeq \mu_p^1 \mathbb{Z}_\ell^{d_p+1} \end{aligned}$$

avec μ_p^1 groupe des racines d'ordre ℓ primaire de l'unité dans K_p et $d_p = [K_p : \mathbb{Q}_\ell]$.²

4.2.2 Point de vue global

Pour fabriquer un $\mathbb{Z}_\ell$ -module à partir de $K^\times$ on prend tout simplement $\mathcal{R}_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$.

2. [3, 2.3.2, Thm 12])

- Pour les idèles, on remplace J_K par :

$$\begin{aligned} \mathcal{J}_K &= \prod_{\mathfrak{p} \in \text{Pl}(K)}^{\text{res}} \mathcal{R}_{K_{\mathfrak{p}}} = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod \mathcal{R}_{K_{\mathfrak{p}}} \mid x_{\mathfrak{p}} \in \mathcal{U}_{\mathfrak{p}} \text{ pour presque tout } \mathfrak{p}\} \\ &= \bigcup_{S \text{ fini}} \mathcal{J}_K^S \text{ avec } \mathcal{J}_K^S = \prod_{\mathfrak{p} \in S} \mathcal{R}_{K_{\mathfrak{p}}} \prod_{\mathfrak{p} \notin S} \mathcal{U}_{\mathfrak{p}}. \end{aligned}$$

On équipe chaque $\mathcal{J}_K^S$ avec la topologie produit (qui est en fait un module compact³), et $\mathcal{J}_K$ de la topologie limite inductive.

Théorème 4.4. *L'application $K^{\times} \rightarrow J$ induit une injection de $\mathcal{R}_K$ dans $\mathcal{J}_K$ d'image fermée. Le quotient*

$$\mathcal{C}_K = \mathcal{J}_K / \mathcal{R}_K$$

est compact pour la topologie quotient. L'application induit un isomorphisme de groupes topologiques compacts de $\mathcal{C}_K$ sur le groupe de Galois $G_K = \text{Gal}(K^{\text{ab}}/K)$ de la pro- ℓ -extension abélienne maximale de K .

Dans cet isomorphisme les sous groupes fermés de $\mathcal{C}_K$ correspondent aux sous extensions de K^{ab}/K et les sous groupes ouverts aux sous extensions finies. Et on a $\text{Gal}(L/K) \simeq \mathcal{J}_K / N_{L/K}(\mathcal{J}_L) \mathcal{R}_K$.

4.3 Quelques Exemples

- Considérons la ℓ -extension abélienne non ramifiée⁴ maximale K^{nr} (ℓ -corps de classes de Hilbert H) C'est l'extension fixée par $\mathcal{U}_K = \prod_{\mathfrak{p} \in \text{Pl}_K} \mathcal{U}_{\mathfrak{p}}$ ⁵. On a donc

$$N_{K^{\text{nr}}/K}(K^{\text{nr}}) \mathcal{R}_K = \mathcal{U}_K \mathcal{R}_K \text{ et } \text{Gal}(K^{\text{nr}}/K) = \mathcal{J}_K / \mathcal{U}_K \mathcal{R}_K.$$

Or on a

$$\begin{aligned} \mathcal{J}_K / \mathcal{U}_K &= \prod_{\mathfrak{p}}^{\text{res}} \mathcal{R}_{K_{\mathfrak{p}}} / \mathcal{U}_{\mathfrak{p}} \\ &= \bigoplus_{\mathfrak{p} \text{ fini}} \pi_{\mathfrak{p}}^{\mathbb{Z}_{\ell}} \\ &= \mathbb{Z}_{\ell} \otimes_{\mathbb{Z}} \text{Id}_K \end{aligned}$$

donc, par passage au quotient $\text{Gal}(K^{\text{nr}}/K) \simeq \mathbb{Z}_{\ell} \otimes_{\mathbb{Z}} \text{Cl}_K = \text{Cl}_K$, le ℓ -groupe des classes d'idéaux (au sens ordinaire) du corps K .⁶

- Pro- ℓ -extension abélienne ℓ -ramifiée, ∞ -décomposée maximale $M = K^{\text{pr}}$.

Son groupe de normes est : $\prod_{\mathfrak{p} \nmid \ell} \mathcal{U}_{\mathfrak{p}} \prod_{\mathfrak{p} \mid \infty} \mathcal{R}_{K_{\mathfrak{p}}} \mathcal{R}_K$. Il suit que

$$\begin{aligned} \text{Gal}(M/H) &\simeq \prod_{\mathfrak{p}} \mathcal{U}_{\mathfrak{p}} \prod_{\mathfrak{p} \mid \infty} \mathcal{R}_{K_{\mathfrak{p}}} \mathcal{R}_K / \prod_{\mathfrak{p} \nmid \ell} \mathcal{U}_{\mathfrak{p}} \prod_{\mathfrak{p} \mid \infty} \mathcal{R}_{K_{\mathfrak{p}}} \mathcal{R}_K \\ &= \prod_{\mathfrak{p} \mid \ell} \mathcal{U}_{\mathfrak{p}} / \prod_{\mathfrak{p} \mid \ell} \mathcal{U}_{\mathfrak{p}} \cap \left(\prod_{\mathfrak{p} \nmid \ell} \mathcal{U}_{\mathfrak{p}} \prod_{\mathfrak{p} \mid \infty} \mathcal{R}_{K_{\mathfrak{p}}} \mathcal{R}_K \right). \end{aligned}$$

3. Théorème de Tykhonov

4. ∞ -décomposée

5. $\mathcal{U}_{\mathfrak{p}} = \mathcal{R}_{K_{\mathfrak{p}}}$ pour $\mathfrak{p}$ archimédienne, voir [2, Def. 1.1.3.].

6. [2, Prop. 1.1.5.].

Les idéaux principaux qui interviennent au dénominateur sont des unités en ℓ et en dehors de ℓ , donc des unités globales, c'est à dire des éléments du groupe :

$$\begin{aligned}\varepsilon_K &= \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K \text{ où } E_K \text{ est le groupe des unités} \\ &\simeq \mu_K \mathbb{Z}_\ell^{r+c-1}\end{aligned}$$

avec μ_K le ℓ -groupe des racines de l'unité, r le nombre de places réelles et c le nombre de places complexes.

Finalement on obtient :

$$\text{Gal}(M/H) \simeq U_\ell / S_\ell(\varepsilon)$$

avec

$$\begin{aligned}U_\ell &= \prod_{p|\ell} U_p \\ &= \prod_{p|\ell} U_p^{(1)} \\ &= \prod_{p|\ell} \mu_p^1 \mathbb{Z}_\ell^{\sum d_p} \\ &= \left(\prod_{p|\ell} \mu_p^1 \right) \mathbb{Z}_\ell^{r+2c},\end{aligned}$$

avec μ_p^1 groupe des racines d'ordre ℓ primaire de l'unité dans K_p et $d_p = [K_p : \mathbb{Q}_\ell]$.

$S_\ell(\varepsilon)$ est l'image canonique de $\varepsilon_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K$ dans U_ℓ .

Conjecture 4.1 (Leopoldt). *L'application de semi-localisation*

$$S_\ell : \varepsilon_K \rightarrow U_\ell$$

est injective, autrement dit on a

$$\text{rg}_{\mathbb{Z}_\ell} S_\ell(\varepsilon_K) = \text{rg}_{\mathbb{Z}_\ell}(\varepsilon_K) = r + c + 1$$

où $\text{rg}_{\mathbb{Z}_\ell}$ est la dimension sur $\mathbb{Z}_\ell$ modulo la torsion, ou encore

$$\text{rg}_{\mathbb{Z}_\ell} \text{Gal}(M/H) = c + 1,$$

c'est à dire $\text{rg}_{\mathbb{Z}_\ell} \text{Gal}(M/K) = c + 1$.

Remarque: Toute $\mathbb{Z}_\ell$ -extension d'un corps de nombres est ℓ -ramifiée et ∞ -décomposée. En effet, le sous-groupe d'inertie, le sous-groupe de décomposition d'une place p sont des sous groupes fermés de $\mathbb{Z}_\ell$ donc soit triviaux, soit d'indice fini dans $\mathbb{Z}_\ell$.

Pour $p|\infty$ on a $|D_p| < 2$. Pour $p \nmid \infty, \ell$, on a $I_p \leq |\mu_p|$ fini.

Cas Local

Cas Global

$$\begin{array}{c} K_\infty \\ \vdots \\ \vdots \Big) I_p \\ K_n \\ \vdots \\ K \end{array}$$

$$\begin{array}{c} K_\infty \\ \vdots \\ \vdots \Big) D_p = \text{sous groupe de décomposition} \\ K_n \\ \vdots \\ K \end{array}$$

Une $\mathbb{Z}_\ell$ -extension K_∞/K est donc une sous-extension de M/K et la conjecture de Leopoldt affirme donc qu'il existe $c + 1$ indépendantes.

Remarque: La conjecture de Leopoldt affirme que les idéles principaux qui sont localement des racines de l'unité sont globalement des racines de l'unité.

• Considérons l'extension non ramifiée ℓ -décomposée maximale C' , c'est à dire, les places au-dessus de ℓ se décomposent complètement, c'est l'extension fixée par

$$\mathcal{J}_K^{C'} = \prod_{p \nmid \ell} \mathcal{U}_p \prod_{p \mid \ell} \mathcal{R}_{K_p},$$

et le groupe de Galois

$$\text{Gal}(C'/K) \simeq \mathcal{J}_K / \prod_{p \nmid \ell} \mathcal{U}_p \prod_{p \mid \ell} \mathcal{R}_{K_p} \simeq \text{Cl}_K / \text{Cl}_K(\ell) = \mathbb{C}\ell'_K,$$

où Cl_K est le ℓ -groupe des classes de diviseurs et $\text{Cl}_K(\ell)$ est le sous-groupe engendré par les classes des diviseurs au-dessus de ℓ .⁷

4.4 Valeurs absolues ℓ -adiques

Sur un corp de nombres K , sont classiquement définies des valeurs absolues réels.

- Pour p réelle (i.e. pour un plongement $\sigma : K \rightarrow \mathbb{R}$)

$$|x|_p = |\sigma(x)|_p.$$

- Pour p complexe :

$$|x|_p = |\sigma(x)|_{\mathbb{C}}^2.$$

- Pour p fini :

$$|x|_p = N_p^{-v_p(x)}$$

(on écrit $(x) = \prod_p p^{v_p(x)}$ avec $v_p(x) \in \mathbb{Z}$).

Remarque: Les valeurs absolues vérifient la formule du produit :

$$\prod_p |x|_p = 1.$$

Preuve : On a en effet :

$$\prod_p |x|_{p|\infty} = \prod_{\sigma} |\sigma(x)| = N_{K/\mathbb{Q}}(x),$$

et

$$\prod_p |x|_{p|\infty} = \prod_{p|\infty} N_p^{-v_p(x)} = \prod_p \prod_{p \mid p} N_p^{-v_p(x)} = N((x))^{-1},$$

en vertu de l'égalité $N\mathcal{U} = \prod_p (N_p)^{v_p \mathcal{U}}$ on a le résultat.

Remarque: Pour un idéal principal $\mathcal{U} = Ax$ entier, on a par définition $N\mathcal{U} = (\wedge : \mathcal{U})$ et c'est la valeur absolue du déterminant de l'application $a \mapsto ax$, c'est à dire du produit des conjugués de x .

7. $\mathbb{C}\ell'_K$ correspond au groupe dans [2, Scolie 1.1.6.] avec S l'ensemble des places au-dessus de ℓ .

Pour $M = \mathbb{Z}^m$ et $f \in \text{End}(M)$ on a $M/f(M) = \mathbb{Z}/d_i\mathbb{Z}$ et $(M : f(M)) = \prod d_i = |\det(f)|$.

Fixons maintenant un nombre premier p . On définit des valeurs absolues ℓ -adiques (en fait dans le sous groupe principal $\Lambda + \ell\mathbb{Z}_\ell$ de $\mathbb{Z}_\ell^\times$) par :

- Pour p complexe : $|x|_p = 1$.
- Pour p réelle : $|x|_p = \langle \text{sg}(x) \rangle$, c'est à dire la projection du sign de x sous le morphism

$$\mathbb{Z}_\ell^\times \rightarrow 1 + \ell\mathbb{Z}_\ell.$$

- Pour $p \nmid \ell, \infty$: $|x|_p = \langle N_p^{-v_p(x)} \rangle$.
- Pour $p|\ell$: $|x|_p = \langle N_{K_p/\mathbb{Q}_p} N_p^{-v_p(x)} \rangle$.

Remarque: Ces formules transitent dans tous les cas pour la norme locale $K_p/\mathbb{Q}_p$ (avec $\mathbb{Q}_\infty = \mathbb{R}$).

Pour $K = \mathbb{Q}$, la 4ième formule est induite par la formule du produit

$$\prod_{p \nmid \ell, \infty} |x|_p = \left\langle \prod_{p \nmid \ell, \infty} p^{v_p(x)} \right\rangle$$

et on a $x = \text{sg}(x) \prod_p p^{v_p(x)} = \text{sg}(x) \ell^{v_\ell(x)} \prod_{p \neq \ell} p^{v_p(x)}$ donc

$$\begin{aligned} \prod_p |x|_p &= |x|_\infty \langle (x \cdot \ell^{-v_\ell(x)}) \prod_{p \neq \ell, \infty} p^{-v_p(x)} \rangle \\ &= \left\langle \frac{x}{x} \right\rangle \\ &= 1. \end{aligned}$$

Conséquence : Les valeurs absolues ℓ -adiques vérifient encore la formule du produit

$$\prod_p |x|_p = \prod_p \prod_{p|p} |x|_p = \prod_p |N_{K/\mathbb{Q}}(x)|_p = 1.$$

Définition 4.1. Les applications $|\cdot|_p$ obtenues se prolongent canoniquement depuis K_p à R_{K_p} en des $\mathbb{Z}_\ell$ -morphismes.

$$R_{K_p} \rightarrow 1 + \ell\mathbb{Z}_\ell,$$

donc aussi en des $\mathbb{Z}_\ell$ -morphismes

$$R_K \rightarrow R_{K_p} \rightarrow 1 + \ell\mathbb{Z}_\ell$$

qui vérifient la formule du produit

$$\forall x \in R_K, \prod_p |x|_p = 1.$$

4.5 Unités logarithmiques

On note $\tilde{U}_{K_p}$ le noyau de la valeur absolue ℓ -adique dans R_{K_p} et on définit la valuation logarithmique par la formule

$$\tilde{v}_p(x) = -\frac{\log_\ell |x|_p}{\deg(p)},$$

où $\deg(p)$ est ajusté pour avoir $\tilde{v}_p(R_{K_p}) = \mathbb{Z}_\ell$.

Un élément $\hat{\pi}_p \in R_p$ de valuation $\tilde{v}_p(x)$ est dit uniformisante logarithmique ; et on a ainsi :

$$R_{K_p} = \hat{U}_{K_p} \hat{\pi}_p^{\mathbb{Z}_\ell},$$

analoguement à la décomposition ordinaire :

$$R_{K_p} = U_{K_p} \pi_p^{\mathbb{Z}_\ell}.$$

4.6 Interprétation par les corps de classes

$\tilde{U}_K$ est le sous groupe de normes d'une extension abélienne de K_p , la quelle ?

- Pour $p \nmid \ell, \infty$ on a : $\tilde{v}_p(x) = -\frac{\log_\ell |N_p^{-v_p(x)}|}{\deg(p)}$, la normalisation $\deg(p) = \log_\ell \langle N_p \rangle$ donne $\tilde{v}_p(x) = v_p(x)$, donc $\tilde{U}_p = U_p = \mu_p$

$$\begin{array}{ccc} & \mu_p & \\ & \swarrow \quad \searrow & \\ K_p^{nr} & \xrightarrow{\quad} & K_p^{ab} \\ \mathbb{Z}_\ell \left(\begin{array}{c} | \\ K_p \end{array} \right. & & \end{array}$$

Ainsi $\tilde{\mu}_p$ détermine le groupe de normes attaché à l'unique $\mathbb{Z}_\ell$ -extension du K_p qui est à la fois la non ramifiée et la cyclotomique.

- Pour $p \mid \ell$ on observe qu'on a :

$$\tilde{U}_{K_p} = N_{K_p/\mathbb{Q}_\ell}(\tilde{U}_{\mathbb{Q}_\ell})$$

où $\tilde{U}_{\mathbb{Q}_\ell}$ es le groupe de normes d'une pro- ℓ -extension abélienne $\mathbb{Q}_\ell^c$ de $\mathbb{Q}_\ell$ de sorte qu'on a le schema :

$$\begin{array}{ccc} \mathbb{Q}_\ell^c & \xrightarrow{\quad} & K_p^c = \mathbb{Q}_\ell^c K_p \\ | & & | \\ & \xrightarrow{\quad} & K_p \\ | & & \\ \mathbb{Q}_\ell & & \end{array}$$

Que vaut $\mathbb{Q}_\ell^c$?

Regardons les extensions abéliennes de $\mathbb{Q}$ (pour $\ell \neq 2$) :

$$J_{\mathbb{Q}}/R_{\mathbb{Q}} = \prod^{\text{res}} R_{\mathbb{Q}_p}/R_{\mathbb{Q}_p}$$

avec

$$R_{\mathbb{Q}_p} = \begin{cases} \text{pour } p \neq \ell, \infty & R_{\mathbb{Q}_p} = \mu_p p^{\mathbb{Z}_\ell} \\ \text{pour } p = \ell & R_{\mathbb{Q}_p} = (1 + \ell \mathbb{Z}_\ell) \ell^{\mathbb{Z}_\ell} \end{cases}$$

et $R_{\mathbb{Q}} = \prod_p^{\text{res}} p^{\mathbb{Z}_\ell}$ ce qui donne :

$$J_{\mathbb{Q}}/R_{\mathbb{Q}} \simeq (1 + \ell \mathbb{Z}_\ell) \prod_{p \neq \ell, \infty} \mu_p.$$

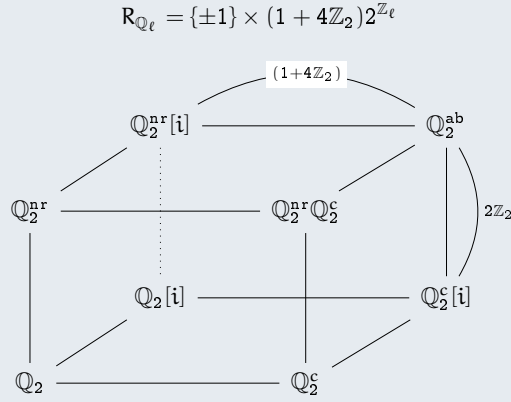
En particulier la ℓ -extension abélienne maximale $\mathbb{Q}_\ell^c$ -ramifiée de $\mathbb{Q}$ est fixée par $\prod_{p \neq \ell, \infty} \mu_p$ et on a $\text{Gal}(\mathbb{Q}^c/\mathbb{Q}) \simeq 1 + \ell \mathbb{Z}_\ell \simeq \mathbb{Z}_\ell$ c'est la $\mathbb{Z}_\ell$ -extension cyclotomique.

Revenons à $\mathbb{Q}_\ell : R_{\mathbb{Q}_\ell} = (1 + \ell \mathbb{Z}_\ell) \ell^{\mathbb{Z}_\ell}$

$$\begin{array}{ccc} & 1 + \ell \mathbb{Z}_\ell & \\ & \xrightarrow{\quad} & \\ \mathbb{Q}_\ell^{nr} & \xrightarrow{\quad} & \mathbb{Q}_\ell^{ab} \\ | & & | \\ \mathbb{Q}_\ell & \xrightarrow{\quad} & \mathbb{Q}_\ell^c \end{array} \Bigg) \ell^{\mathbb{Z}_\ell}$$

$\mathbb{Q}_\ell^c$ est la $\mathbb{Z}_\ell$ -extension cyclotomique et $\mathbb{Q}_\ell^{nr}$ est la $\mathbb{Z}_\ell$ -extension non-ramifiée. Pour $\mathbb{Q}_\ell$ on a $R_{\mathbb{Q}_\ell} = \underbrace{(1 + \ell \mathbb{Z})}_{U_{\mathbb{Q}_\ell}} \underbrace{\ell^{\mathbb{Z}_\ell}}_{\tilde{U}_{\mathbb{Q}_\ell}}.$

Remarque: Pour $\ell = 2$ on a :



5 Interprétation des corps de classes des classes logarithmiques

On a défini, pour chaque place finie p d'un corps de nombres K une valuation absolue ℓ -adique

$$R_{K_p} \xrightarrow{\tilde{v}_p} \mathbb{Z}_\ell$$

de noyau $\tilde{u}_{K_p} = \{x \in R_{K_p} \mid \tilde{v}_p(x) = 0\}$. Via le morphisme naturel $R_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times \rightarrow R_{K_p}$ induit par le plongement $K \hookrightarrow K_p$. Cette valuation est définie sur R_K et on a la formule du produit :

$$\forall x \in R_K \quad \prod_p |x|_p = 1,$$

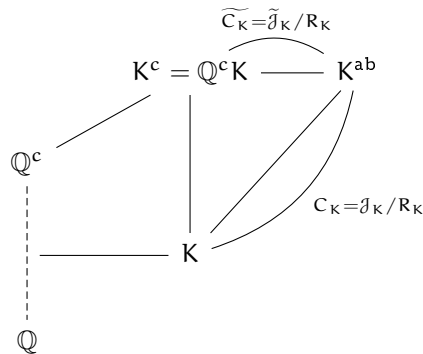
de sorte que si l'on pose :

$$\deg(x_p)_p := \sum_p \tilde{v}_p(x_p) \deg(p)$$

pour tout idèle $\chi = (x_p)_p \in \mathcal{J}_K$, il vient

$$\deg(\chi) = 0 \quad \forall \chi \in \mathcal{J}_K.$$

Soit $\tilde{\mathcal{J}}_K = \{(\chi_p)_p \in \mathcal{J}_K \mid \deg(\chi_p)_p = 0\}$. Le sous module de $\mathcal{J}_K$ formé des idèles de degré nul $\tilde{\mathcal{J}}_K = \ker(\deg)$, est un sous module formé de $\mathcal{J}_K$ que contient R_K . Par les corps de classes $\tilde{\mathcal{J}}_K$ est le group des normes d'une certaine pro- ℓ -extension K^c de K . Comme on a $\tilde{\mathcal{J}}_K = \{(\chi_p)_p \mid N_{K/\mathbb{Q}}((\chi_p)_p) \in \tilde{\mathcal{J}}_{\mathbb{Q}}\}$, K^c n'est rien d'autre que la composition avec K de la pro- ℓ -extension de $\mathbb{Q}$ associée à $\tilde{\mathcal{J}}_{\mathbb{Q}}$.



Lemme 5.1. $\mathbb{Q}^c$ n'est rien d'autre que la $\mathbb{Z}_\ell$ -extension cyclotomique de $\mathbb{Q}$.

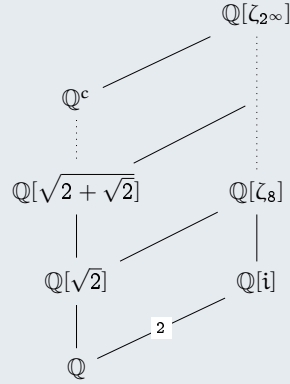
Preuve : La théorie de Galois nous donne :

$$\text{Gal}(\mathbb{Q}^c/\mathbb{Q}) = \tilde{\mathcal{J}}_K/\tilde{\mathcal{J}}_K \simeq_{\deg} \mathbb{Z}_\ell.$$

□

Remarque: Soit M la pro- ℓ -extension ℓ -ramifiée ∞ -décomposée maximal de $\mathbb{Q}$ et H son sous extension non ramifiée.

- $\text{Gal}(H/\mathbb{Q}) = \text{Cl}_\mathbb{Z} = 1$.
- $\text{Gal}(M/H) \simeq \mathbb{U}_\ell/s_\ell(\varepsilon)$
- Pour ℓ -impair $\varepsilon = 1$, $\mathbb{U} = (1 + \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell$. Il suit $\text{Gal}(M/\mathbb{Q}) = \mathbb{Z}_\ell$.
- Pour $\ell = 2$, $\varepsilon = \{\pm 1\}$ $\mathbb{U} = 1 + 2\mathbb{Z}_2 = \{\pm 1\} \times \{1 + u\mathbb{Z}_2\} \simeq \mathbb{Z}_2$, d'où on obtient le même resultat.



5.1 Point de vue local

$\tilde{\mathbb{U}}_{K_p} = \tilde{\mathcal{R}}_K \cap \tilde{\mathcal{J}}_K$ est le sous groupe de normes de la complétée K_p^c/K_p de l'extension K^c/K , i.e. la $\mathbb{Z}_\ell$ -extension cyclotomique de K_p .

En particulier, le produit $\tilde{\mathbb{U}}_K = \prod_p \tilde{\mathbb{U}}_{K_p}$ fixe la pro- ℓ -extension maximale abélienne maximale de K qui est localement cyclotomique, disons K^{lc}

$$\begin{array}{ccc} K^c & \xrightarrow{\quad} & K^{lc} \\ \mathbb{Z}_\ell \left(\begin{array}{c} | \\ | \end{array} \right. & & \\ K & & \end{array}$$

Le quotient $\widetilde{\text{Cl}}_K := \tilde{\mathcal{J}}_K/\tilde{\mathbb{U}}_K \mathcal{R}_K$ isomorphe à $\text{Gal}(K^{lc}/K^c)$ est, par définition, le ℓ -groupe des classes logarithmiques de degré nul.

Si on définit $\mathcal{D}\ell_K = \mathcal{J}_K/\tilde{\mathbb{U}}_K \simeq \bigoplus_p \mathbb{Z}_{\ell_p}$ (puis qu'on a $\mathbb{Q}_{K_p} = \tilde{\mathbb{U}}_{K_p} \tilde{\pi}_p^{\mathbb{Z}_\ell}$) comme groupe des diviseurs logarithmiques et $\widetilde{\mathcal{P}\ell}_K = \mathcal{R}_K \tilde{\mathbb{U}}_K/\tilde{\mathbb{U}}_K$ comme le sousgroupe principale (image canonique de $\mathcal{R}_K$ pour l'application $\text{div} : x \mapsto \sum_p \tilde{v}_p(x)p$).

On a bien $\widetilde{\text{Cl}}_K = \widetilde{\mathcal{D}\ell}_K/\widetilde{\mathcal{P}\ell}_K$ en notant :

$$\widetilde{\mathcal{D}\ell}_K = \tilde{\mathcal{J}}_K/\tilde{\mathbb{U}}_K$$

avec

$$\widetilde{\mathcal{D}\ell}_K = \{a \in \sum v_p p \in \mathcal{D}\ell_K \mid \deg(a) = \sum v_p \deg(p) = 0\}$$

Conjecture 5.1 (Gross). *Le groupe $\mathcal{C}l_K$ est fini.*

Remarque: On a vu $\mathcal{C}l_{\mathbb{Q}} = 1$.

Définition 5.1. On note $\tilde{\varepsilon}_K$ le noyau de l'application canonique

$$R_K \rightarrow \mathcal{D}l_K,$$

c'est à dire

$$\tilde{\varepsilon}_K = \{x \in R_K \mid v_p(x) = 0\},$$

le groupe des unités logarithmiques.

Remarque: On a par construction $\tilde{v}_p = v_p$ pour $p \nmid \ell$ donc le schéma

$$\begin{aligned} 1 \rightarrow \bigoplus_{p|\ell} \mathbb{Z}_\ell p &\rightarrow \mathcal{D}l_K \rightarrow \bigoplus_{p \nmid \ell} \mathbb{Z}_\ell p \rightarrow 1 \\ 1 \rightarrow \bigoplus_{p|\ell} p^{\mathbb{Z}_\ell} &\rightarrow \mathcal{D}_K \rightarrow \bigoplus_{p \nmid \ell} p^{\mathbb{Z}_\ell} \rightarrow 1 \end{aligned}$$

Notons $\mathcal{D}'_K = \mathcal{D}_K / \prod_{p|\ell} p^{\mathbb{Z}_\ell}$ le groupe des ℓ -diviseurs (au sens ordinaire) $\mathcal{D}l \rightarrow \mathcal{D}'_K$ et $\mathcal{C}l'_K = \mathcal{D}'_K / \mathcal{P}'_K$ où $\mathcal{P}'_K$ es le sous groupe principal de $\mathcal{D}'_K$ (image canonique de R_K dans $\mathcal{D}'_K$). Ce groupe $\mathcal{C}l_K$ est fini (comme quotient du groupe des classes au sens ordinaire). On a donc la suite exacte :

$$1 \rightarrow \tilde{\varepsilon}_K \rightarrow \varepsilon'_K \rightarrow \bigoplus_{p|\ell} \mathbb{Z}_\ell p \rightarrow \widetilde{\mathcal{C}l}_K \rightarrow \mathcal{C}l_K$$

où $\varepsilon'_K = \mathbb{Z}_\ell \otimes E'_K$ groupe des ℓ -unités.

On a $\varepsilon'_K \simeq \mu_K \cdot \mathbb{Z}_\ell^{r+c+l-1}$, où

r = nombre de places réels.

c = nombre de places complexes.

l = nombre de places ℓ -adiques.

On a $\bigoplus_{p|\ell} \mathbb{Z}_\ell p = \mathbb{Z}_\ell^{l-1}$.

$\widetilde{\mathcal{C}l}_K \simeq \text{fini} \times \mathbb{Z}_\ell^\delta$, est un $\mathbb{Z}_\ell$ -module de type fini. δ est le défaut de Gross, la conjecture de Gross dit $\delta = 0$.

Il suit $\tilde{\varepsilon}_K \simeq \mu_K \cdot \mathbb{Z}_\ell^{r+c+\delta}$. Et donc la conjecture de Gross affirme $\dim(\tilde{\varepsilon}_K) = r + c$.

5.2 Méthode de Baker-Brumer

On suppose $K/\mathbb{Q}$ abélienne de groupe de Galois G . On a alors $\overline{\mathcal{C}l}_\ell = \bigoplus \tilde{Q}_\ell e_\varphi$ avec $e_\varphi = \frac{1}{|G|} \sum_{\tau \in G} \varphi(\tau^{-1})\tau$, φ décrivant les caractères absolument irréductibles de G .

Pour la conjecture de Leopoldt, on doit vérifier que le rang ℓ -adique des unités est encore $r + c - 1$.

On a :

$$E_K \rightarrow \prod_{p|\ell} u_p^1 \xrightarrow{\log} \bigoplus_{p|\ell} O_p$$

qui induit une application

$$\tilde{Q}_\ell \otimes_{\mathbb{Z}} E_K \rightarrow \bigoplus_{p|\ell} K_p \simeq \mathbb{Q}_\ell \otimes_{\mathbb{Q}} K$$

avec $K \simeq \mathbb{Q}[G]$ donc $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K \simeq \mathbb{Q}_\ell[G]$.

On sait que $\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Z}} E_K$ est un $\overline{\mathbb{Q}_\ell}[G]$ -module, somme directe de sous modules irréductibles. On prend une unité de Minkowski i.e. $\varepsilon \in E_K$ telle que $\varepsilon^{\mathbb{Z}[G]}$ soit l'indice fini dans E_K .

Si $\chi = \sum \varphi$ est le caractère des $\mathbb{Z}[G]$ -module $E_K \simeq \mu_K \mathbb{Z}^{r+c-1}$ (i.e. le caractère des $\overline{\mathbb{Q}_\ell}[G]$ -module $\overline{\mathbb{Q}_\ell} \otimes_{\mathbb{Z}} E_K$); on a

$$\mathbb{Q}_\ell^{r+c-1} \simeq \varepsilon^{\tilde{\mathbb{Q}_\ell}[G]} = \bigoplus \varepsilon_{\varphi}^{\overline{\mathbb{Q}_\ell}}$$

avec $\varepsilon_{\varphi} = \varepsilon^{\frac{1}{|G|} \sum \varphi(\tau^{-1})\tau} \neq 1$. à droite, on a donc $f(\varepsilon^{\overline{\mathbb{Q}_\ell}[G]}) = \bigoplus_{\varphi} \overline{\mathbb{Q}_\ell} \log(\varepsilon_{\varphi})$, avec $\log(\varepsilon_{\varphi}) = \frac{1}{|G|} \sum_{\tau \in G} \varphi(\tau^{-1}) \log(\varepsilon_{\varphi}^{\tau}) \neq 0$ n'est pas null par Baker-Brumer.

$$\chi_E = \left(\sum_{p|\infty} \text{Ind}_{D_p}^G 1_{D_p} \right) - 1 \leq \chi_{\text{rég}}.$$

Pour $K = \mathbb{Q}$, on a $\chi_E = \text{Ind}_{D_\infty}^G 1_{D_\infty} - 1 \leq \chi_{\text{rég}} - 1 \leq \chi_{\text{rég}}$.

Lemme 5.2. *Pour tout sous module de type fini M de $K^\times$ stable pour G , on a : $\mathbb{Q} \otimes_{\mathbb{Z}} M$ est $\mathbb{Q}[G]$ -monogène $\Leftrightarrow \chi_M \leq \chi_{\text{rég}}$, si et seulement si M contient un sous module $\mathbb{Z}[G]$ -monogène d'indice fini.*

Conjecture 5.2 (Jaulent). *Si M est un tel module et si M rencontre invariablement $\ell^{\mathbb{Q}}$ alors le rang ℓ -adique de l'image $\log_{\omega}(M)$ dans $\prod K_p$ est donné par $\log_{Iw}(M) = \text{rg}_{\mathbb{Z}}(M)$.*

Plus généralement sous l'hypothèse $\chi_M \leq \chi_{\text{rég}}$, on a :

$$\chi_{\log}(M) = \chi_{\text{rég}} \wedge \chi_M$$

où $\chi_{\log}(M)$ est un caractère du $\mathbb{Z}_\ell[G]$ -module $\log(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$ et χ_M es un caractère de $\mathbb{Z}[G]$ -module M .

5.3 Cas d'une extension Galoisienne quelconque

On suppose $\text{Gal}(K/k) = G$ fini. On écrit $\chi_{\text{rég}} - \sum n_i \chi_i$ avec les χ_i irréductibles. Pour $M \subset K^\times$ stable par G ne rencontrant pas $\ell^{\mathbb{Z}}$ de caract'ere $\chi_M = \sum M_i \chi_i \leq \chi_{\text{rég}}$.

Le théorème de Baker-Brumer donne

$$\chi_{\log}(M) \geq \sum \chi_i$$

(d'où le résultat pour $M_i \leq 1 \ \forall i$)

Le théorème de Wald Schmidt donne

$$\chi_{\log}(M) \geq \frac{M_i}{2} \chi_i$$

Plus généralement sous l'hypothèse

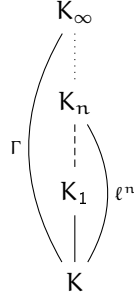
$$\chi_M \leq \chi_{\text{rég}}$$

on a conjecturellement $\chi_{\log}(M) = \sum \min(M_i, n_i) \chi_i$ par Baker-Brumer $\chi_{\log}(M) \geq \sum_{M_i > 0} \chi_i$. Par Waldschmidt $\chi_{\log}(M) \geq \sum \frac{M_i n_i}{M_i + n_i} \chi_i$.

6 La descente en théorie d'Iwasawa

On se donne

1. Une $\mathbb{Z}_\ell$ -extension K_∞/K d'un corp de nombres de groupe de Galois $\Gamma = \text{Gal}(K_\infty/K) = \gamma^{\mathbb{Z}_\ell}$.



2. Deux ensembles finis S et T disjoints de places finies de K , on note $R = \text{Pl}_K(\ell)$ l'ensemble des places ramifiées dans K_∞/K .

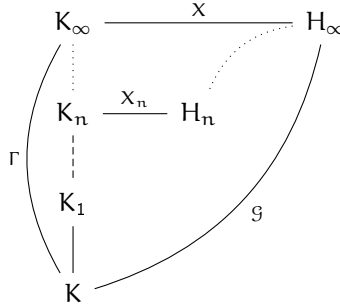
3. On choisit n_0 assez grand pour qu'aucune de ces places ne se décompose dans K_∞/K_{n_0} . On note S_∞, R_∞ et T_∞ les ensembles finis de places de K_∞ au-dessus de S, R et T .

Problème : On s'intéresse aux pro- ℓ -extensions abéliennes maximales S -décomposées et T -ramifiées, disons $H_T^S(K_n) = H_n$ de corps K_n .

$\text{Gal}(H_n/K_n) = \text{Cl}_T^S(u_n)$ est le groupe des S -classes T -infinitésimales de K_n :

$$\text{Cl}_T^S(K_n) \simeq \mathcal{J}_{K_n} / \left(\prod_{p_n \in S_n} R_{K_{p_n}} \right) \left(\prod_{p_n \notin T_n} U_{K_{p_n}} \right) R_{K_n}.$$

On note $H_\infty = \bigcup_{n \in \mathbb{N}} H_n$; c'est la pro- ℓ -extension abélienne maximale S_∞ -décomposée T_∞ -ramifiée de H_∞ .



$$X = X_T^S(K_\infty) = \varprojlim_N \text{Cl}_T^S(K_n)$$

On observe que H_∞ est galoisienne sur K et que le groupe de Galois $\mathcal{G} = \text{Gal}(H_\infty/K)$ satisfait à la suite exacte :

$$1 \rightarrow X \rightarrow \mathcal{G} \rightarrow \Gamma = \gamma^{\mathbb{Z}_\ell} \rightarrow 1.$$

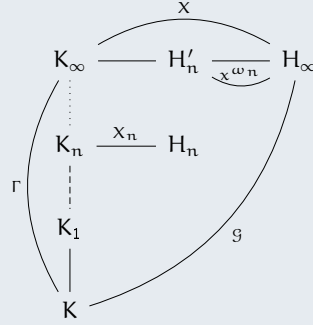
Cette suite est scindée (puisque Γ est procyclique) ce qui permet (en relevant γ dans $\mathcal{G}$) d'écrire $\mathcal{G}$ comme produit semi-direct :

$$\mathcal{G} = X \rtimes \Gamma,$$

la loi sur $\mathcal{G}$ étant déterminée par l'action de Γ sur le sous groupe normal X ,

$$\gamma x \gamma^{-1} = x^\gamma.$$

Remarque: Le sous groupe dérivé $\mathcal{G}'$ est le sous groupe formé engendré par les commutateurs $[x, \gamma] = x\gamma x^{-1}\gamma^{-1} = x^{1-\gamma}$. C'est l'image de x pour l'idéal d'augmentation de l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_\ell[[\gamma - 1]]$.

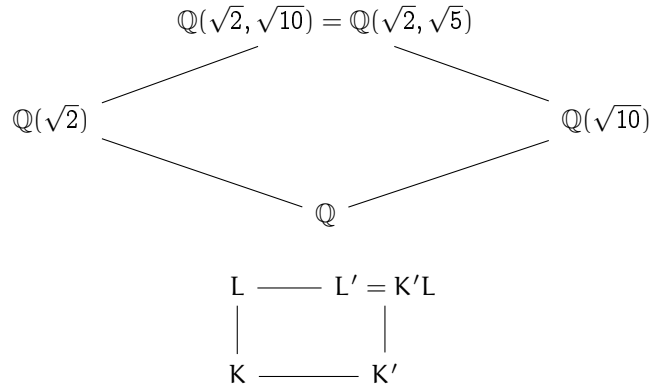


Plus généralement, si on pose $\mathcal{G}_n = \text{Gal}(H_\infty/K_n)$ on obtient

$$\mathcal{G}'_n = x^{1-\gamma^{\ell^n}} = x^{\omega_n},$$

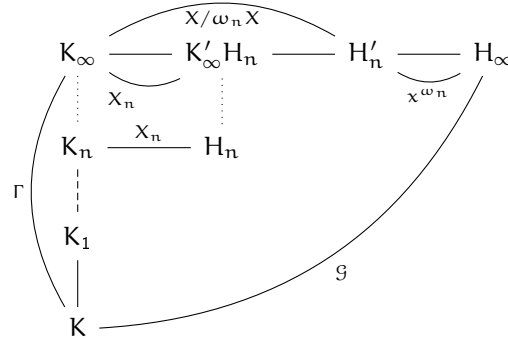
qui fixe la sous extension maximale de H_∞ , disons H'_n qui est abélienne sur K_n .

En résumé H'_n est la pro- ℓ -extension maximale T-ramifiée et S-décomposée sur K_∞ et abélienne sur K_n , il suit $H'_n \supset H_n$.



Plus précisément, pour chaque place p_∞ de K_∞ contenue dans $R \setminus T$ ou dans S , soit D_{p_∞} le sous groupe d'inertie (pour $p_\infty \in R_\infty \setminus T_\infty$) ou de décomposition (pour $p_\infty \in S_\infty$) associé à p_∞ (avec $x_{p_\infty} \in X$ et $\gamma_{p_\infty} \in \gamma^{\mathbb{Z}_\ell}$).

Cas générique : H_n et K_∞ , K_n -linéairement disjoints



Soit Y_{n_0} le $\mathbb{Z}_\ell$ -module de type fini engendré par les images de D_{p_∞} . On a alors :

$$X_{n_0} \simeq X/(\omega_{n_0}X + Y_{n_0}).$$

Passage de n_0 à $n_0 + 1$: Il faut remplacer $\omega_{n_0}x$ par $\omega_{n_0+1}x$, et les $x_p\gamma_p$ par

$$\begin{aligned} (x_{p_\infty}\gamma_{p_\infty})^\ell &= (x_p\gamma_p)(\underbrace{x_p\gamma_p^{-1}\gamma_p}_x)^2(\underbrace{x_p\gamma_p^{-2}\gamma_p^3}_{x_p^{\gamma_p^2}})\dots(x_p^{-\ell+1}\gamma_p^\ell) \\ &= x_p^{1+\gamma_p+\gamma_p^2+\gamma_p^3+\dots+\gamma_p^{\ell-1}}\gamma_p^\ell, \end{aligned}$$

ce qui donne finalement $X_{n_0+1} = X/\frac{\omega_{n_0+1}}{\omega_{n_0}}(\omega_{n_0}X + Y_{n_0})$ et généralement pour $n \geq n_0$:

$$X_n \simeq X/\frac{\omega_n}{\omega_{n_0}}(\omega_{n_0}X + Y_{n_0}).$$

Cas special : $K_{\infty \subset H_n}$ (pour n assez grand) autrement dit K_∞/K_n est S -décomposée et T -ramifiée.

MANQUE UN DIAGRAMME

On a ici $X_n \simeq X'_n \oplus \Gamma_n$. On a directement $X'_n = X/\omega_n X$.

Exemple 6.1. Si K_∞/K est la $\mathbb{Z}_\ell$ -extension cyclotomique, le cas special se produit pour $T = \text{Pl}(\ell)$ et $S = \emptyset$.

6.1 Structure du groupe X

Les calculs précédents montrent que le quotient $X/\omega_n X$ contient comme sous quotient de ce type fini X_n , qui est fini, para la théorie des corps de classes un $\mathbb{Z}_\ell$ -module de type fini.

$$X_0 = \mathcal{J}_K / \prod_{p \in S} R_{K_p} \prod_{p \notin T} U_{K_p} R_K$$

est un quotient des groupes (où $T' = T \cup \text{Pl}(\ell)$).

$$\mathcal{J}_K / \prod_{p \in T'} U_{K_p} R_K$$

qui correspond à la pro- ℓ -extension T' -ramifiée maximale de K , laquelle diffère des groupes de Galois $\mathcal{J}_K / \prod_{p \nmid \ell} U_{K_p} R_{K_p}$ (isomorphe à $\text{fini} \times \mathbb{Z}_\ell^{c+1+\delta}$ où δ est le défaut de Leopoldt) de l'image du groupe fini

$$\prod_{p \in T' \setminus \text{Pl}(\ell)} U_{K_p} = \prod_{p \in T' \setminus \text{Pl}(\ell)} U_{K_p}.$$

En particulier $X/\nabla_0 X = X/\ell X + (\gamma - 1)X$ est un $\mathbb{F}_\ell$ -module de dimension finie, et le lemme de Nakayama montre que X est un R -module de type fini.

Les théorèmes structuraux donnent alors la pseudo-décomposition :

$$X \sim \Lambda^\rho \oplus \left(\bigoplus \Lambda/\ell^{\mu_i} \Lambda \right) \oplus \left(\bigoplus \Lambda/P_i \Lambda \right),$$

avec P_i distingués.

Théorème 6.1. *Dans le cas générique, la suite des ordres ℓ^{x_n} des modules finis $X_n/\ell^n X_n$ est paramétrée par $x_n \sim \rho_n \ell^n + \mu \ell^n + (\lambda - x)n$, où ρ, μ, λ sont les paramètres structuraux du Λ -module X et où $x \leq \rho$.*

- Dans le cas special, on a directement :

$$x_n \sim \rho_n \ell^n + \mu \ell^n + (\lambda - 1)n.$$

Remarque: Si T ne contient aucune place des ??? de ℓ , le module X es de Λ -torsion et il vient alors $x_n \sim \mu \ell^n + \lambda_n$
Preuve de la remarque : Dans le cas $T \cap Pl(\ell) = \emptyset$, les groupes X_n son en effet, finis. Le groupe de Galois

$$\text{Gal}(H_T^S(K_n)/H_\emptyset^S(K_n))$$

est engendré par l'image (finie) des U_{K_p} pour $p \in T$ et de sorte que $[H_T^S(K_n) : H_\emptyset^S(K_n)]$ est fini, de même que $[H_\emptyset^S(K_n) : K_n]$ puisque $H_\emptyset^S(K_n)$ est contenu dans le corp de classes de Hilbert $H_\emptyset^\emptyset(K_n)$ qui vérifie

$$\text{Gal}(H_\emptyset^\emptyset(K_n)/K_n) \simeq Cl(K_n).$$

MANQUE UN DIAGRAMME

□

Plus precisement le théorème precedent, appliqué avec $S = T = \emptyset$ donne $x_\emptyset^\emptyset(n) \sim \mu_\emptyset^\emptyset \ell^n + \lambda_\emptyset^\emptyset n$ et on a $|U_{K_p}| = \ell^{\mu_{p_n}}$ avec $\mu_{p_n} \sim n$. De sorte que la formule de paramétrage des $x_T^S(n)$ e peut dans ce cas, faire intervenir de terme en $\rho_n \ell^n$!!

Remarque: Ni μ_T^S ni ρ_T^S ne dependent pas des places de $T \setminus Pl(\ell)$ car leur impact sur la formule finale provient des $U_{K_{p_n}}$ pour $p_n \in T$.

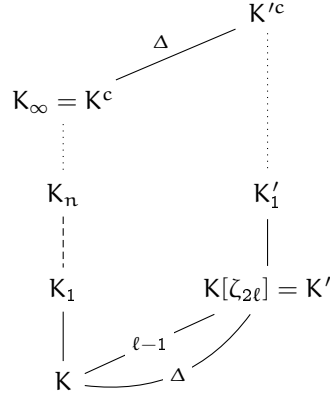
Remarque: Ni ρ_T^S , ni μ_T^S ni λ_T^S ne dependent des places de S qui ne divisent pas ℓ .
 En effet, on a imposé aux places de S d'être finiment décomposées dans K_∞/K . Car si elles ne divisent pas ℓ , elles ne peuvent se ramifier : elle sont donc presque totalement inertes.
 MANQUE UN DIAGRAMME

L'extension ??? associée est donc la $\mathbb{Z}_\ell$ -extension de $\mathbb{F}_p$ ⁸. Autrement dit, la montée des K_∞/K epuisse toute possibilité d'inertie. Il suite qu'une telle place, des ??? qu'elle est non ramifiée au dessus de K_∞ et forcement totalement décomposée.

7 Dualité dans la $\mathbb{Z}_\ell$ -extension cyclotomique

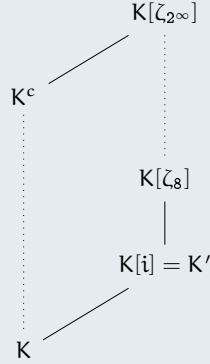
Soit K un corps de nombres, $K_\infty = \bigcup_{n \in \mathbb{N}} K_n = K^c$ sa $\mathbb{Z}_\ell$ -extension cyclotomique. Pour faire de la théorie de Kummer, on a besoin des racines de l'unité, qu'on peut introduire en remplaçant (si nécessaire) K par $K' = K[\zeta_{2\ell}]$. Supposer ici (pour simplifier) $\ell \neq 2$

8. $\text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$



auquel cas $\Delta = \text{Gal}(K'/K) \simeq \text{Gal}(K'_\infty/K_\infty)$ est cyclique d'ordre d divisant $(\ell - 1)$, de sorte que $\mathbb{Z}_\ell[\Delta] \simeq \bigoplus_{\varphi \in \hat{\Delta}} \mathbb{Z}_\ell e_\varphi$ est un produit d'exemplaires de $\mathbb{Z}_\ell$ (indexés par caractères irréductibles $\varphi : \Delta \rightarrow \mathbb{Z}_\ell^\times$) On pourra donc se ramener au cas $\zeta_\ell \in K$.

Remarque: Pour $\ell = 2$ notons : Rappelons que $e_\varphi = \frac{1}{d} \sum_{\tau \in \Delta} \varphi(\tau^{-1}) \tau$.



7.1 Description Kummerienne

Supposons $\zeta_{\ell^\nu} \in K$. Sous cette hypothèse, les ℓ -extensions abéliennes L d'exposant ℓ^ν de K sont décrites par leur radical $\text{Rad}(L/K)$ regardé dans $K^\times/K^{\times \ell^\nu}$

$$\text{Rad}(L/K) = \{x K^{\times \ell^\nu} \in K^\times / K^{\times \ell^\nu} \mid K[\sqrt[\ell^\nu]{x}] \subset L\}$$

Voir Théorème 90 de Hilbert. Pour simplicité, plutôt que de regarder les radicaux dans $K^\times/K^{\times \ell^\nu} = \mathbb{Z}/\ell^\nu \mathbb{Z} \otimes_{\mathbb{Z}} K^\times$ on va les regarder dans $\ell^\nu \mathbb{Z}/\mathbb{Z} \otimes_{\mathbb{Z}} K^\times$, i.e.

$$\ell^\nu \text{Rad}(L/K) = \{\ell^{-k} \otimes x \in \ell^{-\nu} \otimes_{\mathbb{Z}} K^\times \mid K[\sqrt[\ell^k]{x}] \subset L\}$$

Plus généralement, en haut de la tour cyclotomique on regardera :

$$\begin{aligned} \text{Rad}(K_\infty^{\text{ab}}/K_\infty) &= (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}} K_\infty^\times \\ &= (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} R_{K_\infty} \\ &=: \mathfrak{R}_{K_\infty} \end{aligned}$$

avec $R_{K_\infty} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K_\infty^\times = \bigcup_{n \in \mathbb{N}} R_{K_n}$.

Remarque: On peut vérifier qu'on a alors

$$\mathfrak{R}_{K_n} = \mathfrak{R}_{K_\infty}^{T_n}$$

pour $\mathfrak{R}_{K_n} := (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} R_{K_n}$.

Remarque: Le produit tensoriel par $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ (groupe ℓ -divisible) a tué le sous groupe de torsion de R_{K_n} , i.e. U_{K_n} . En effet pour $x^{\ell^k} = 1 \in R_K$ on a bien :

$$\begin{aligned} \ell^{-k} \otimes x &= \ell^{-h-k} \otimes x^{\ell^k} \\ &= \ell^{-(h+k)} \otimes 1 \\ &= 1 \end{aligned}$$

dans $(\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} R_K$.

7.2 Dualité

Supposons toujours $\zeta_{\ell^\vee} \in K$ et soit L la ℓ -extension abélienne d'exposant $\ell^\vee$ de K . On dispose de deux descriptions de L

- La théorie de corps de classes donne :

$$\text{Gal}(L/K) \simeq \mathcal{I}_K / \mathcal{I}_K^{\ell^\vee} R_\vee.$$

- La théorie de Kummer donne :

$$\text{Rad}(L/K) = (\ell^\vee \mathbb{Z}/\mathbb{Z}) \otimes K^\times.$$

Et on dispose d'un couplage (forme bilinéaire non dégénérée) :

$$\begin{aligned} \text{Rad}(L/K) \times \text{Gal}(L/K) &\rightarrow \mu_{\ell^\vee} \\ (\ell^{-\vee} \otimes x, \sigma) &\mapsto (\ell^\vee \sqrt{x})^{\sigma-1} = \langle \ell^{-\vee} \otimes x, \sigma \rangle \end{aligned}$$

Remarque: Le symbole est bien défini car on a $\zeta^{\sigma-1} = 1$ pour $\zeta \in \mu_{\ell^\vee}$.

Il est multiplicative en x de façon évidente. Il est multiplicative en σ car on a $\ell^\vee \sqrt{x}^{(\sigma-1)(\tau-1)} = (\ell^\vee \sqrt{x})^{\sigma\tau - \sigma - \tau + 1} = 1$, donc $(\ell^\vee \sqrt{x})^{\sigma\tau-1} = \ell^\vee \sqrt{x}^{(\sigma-1)} \ell^\vee \sqrt{x}^{(\tau-1)}$.

C'est non dégénérée, car on a les deux implications :

$$\begin{aligned} \ell^\vee \sqrt{x}^{(\sigma-1)} \quad \forall x \in K^\times &\Rightarrow \sigma = 1. \\ \ell^\vee \sqrt{x}^{(\sigma-1)} \quad \forall \sigma \in \text{Gal}(L/K) &\Rightarrow \ell^\vee \sqrt{x} \in K, \end{aligned}$$

alors le couplage est non dégénéré.

Autrement dit on a $\text{Gal}(L/K) \simeq \text{Hom}_{\mathbb{Z}_\ell}(\text{Rad}(L/K), \mu_{\ell^\vee})$.

Conséquence (miroir). Si l'on n'a pas $\zeta_\ell \in K$ et qu'on travaille dans la tour $K' = K[\zeta_\ell]$, on a alors de $\mathbb{Z}_\ell[\Delta]$ -modules, pour une extension L/K et $L' = LK'$, on obtient (avec $\ell^\vee \in K'$)

$$\text{Rad}(L/K) = \text{Rad}(L'/K')^{e_1},$$

où e_1 est le caractère unité, et $\text{Gal}(L/K) = \text{Gal}(L'/K')^{e_1}$, mais dans la dualité de Kummer, si $\text{Gal}(L'/K')$ est un $\mathbb{Z}_\ell[\Delta]$ -module d'exposant ℓ^ν de caractère χ , et si ω est le caractère de l'action de Δ sur $\mu_{\ell^{\text{nu}}}$:

$$\zeta^\tau = \zeta^{\omega(\tau)} \quad \forall \tau \in \Delta.$$

Le caractère de $\text{Rad}(L/K)$ est $\chi^* = \omega\chi^{-1}$ puis qu'on a

$$\langle \ell^{-1} \otimes x, \sigma \rangle^\tau = \langle \ell^{-k} \otimes x, \sigma \rangle^{\omega(\tau)}$$

et pour $\ell^{-k} \otimes x$ isotypique de caractère φ

$$(\ell^{-k} \otimes x)^\tau = (\ell^{-k} \otimes x)^{\varphi(\tau)}$$

et pour σ isotypique de caractère ψ :

$$\begin{aligned} \sigma^\tau &= \sigma^{\psi(\tau)} \\ \langle \ell^{-k} \otimes x, \sigma \rangle &= \langle (\ell^{-k} \otimes x)^\tau, \sigma^\tau \rangle \\ &= \langle \ell^{-k} \otimes x, \sigma \rangle^{\varphi(\tau)\psi(\tau)} \end{aligned}$$

qui ne peut être non trivial que pour

$$\varphi(\tau)\psi(\tau) = \omega(\tau),$$

c'est à dire $\psi = \varphi^*$.

Notation : On dit que $\chi^* = \omega\chi$ est le réflet de χ dans l'involution du miroir.

7.3 étude préliminaire

Supposons $\zeta_{\ell^\nu} \in K$ (avec $\nu \geq 1$) et intéressons nous à la pro- ℓ -extension abélienne ℓ -ramifiée d'exposant ℓ^ν disons M de K .

$$\begin{aligned} \text{Rad}(M/K) &= \{ \ell^{-\nu} \otimes x \in (\ell^{-\nu}\mathbb{Z}/\mathbb{Z}) \otimes_{\mathbb{Z}} K^\nu \mid K[\sqrt[\ell^\nu]{x}]/K \text{ } \ell\text{-ramifiée} \} \\ &= \{ \ell^{-\nu} \otimes x \mid \forall p \nmid \ell, K_p[\sqrt[\ell^\nu]{x}]/K \text{ non ramifiée} \} \\ &= \{ \ell^{-\nu} \otimes x \mid \forall p \nmid \ell, x \in K_p^{\times \ell^\nu} \mathcal{U}_p \} \\ &= \{ \ell^{-\nu} \otimes x \mid (x)' \in \text{Id}_K'^{\ell^\nu} \} \end{aligned}$$

où $(x)'$ est l'image de x dans le groupe de ℓ -ideaux de K (quotient du groupe des ideaux par le sous groupe des ideaux construits sur les $p|\ell$),

$$\text{Rad}(L/K) = \{ \ell^{-\nu} \otimes x \mid v_p(x) \equiv 0 \pmod{\ell^\nu} \quad \forall p \nmid \ell \}$$

Théorème 7.1. *On obtient ainsi une suite exacte :*

$$1 \rightarrow (\ell^{-\nu}\mathbb{Z}/\mathbb{Z}) \otimes E'_K \rightarrow \text{Rad}(M/K) \xrightarrow{\varphi_{\ell^\nu}} Cl'_K \rightarrow 1$$

où ${}_{\ell^\nu}Cl'_K$ est le sous groupe de ℓ^ν -torsion du ℓ -groupe des ℓ -classes d'ideaux de K .

Preuve : Soit

$$\ell^{-\nu} \otimes x \mapsto Cl(\underbrace{\sqrt[\ell^\nu]{(x)'}}_{=:a})$$

avec $(x) = a^{\ell^v} b$ (où b ne fait intervenir que les places au-dessus de ℓ). C'est un morphisme surjectif puisque toute classe d'exposant ℓ^v est représentée par un idéal a qui vérifie $a^{\ell^v} = xb$ avec b construit sur les places au-dessus de ℓ .

Le noyau

$$\ker(\varphi) = \{\ell^{-v} \otimes x \mid (x)' = (\alpha)^{\ell^v} b\}$$

pour un $\alpha \in K^\times$ et b . On a donc $(x\alpha^{-\ell^v}) = b$ et $x\alpha^{-\ell^v}$ est donc un ℓ -unité, de sorte que la classe $\ell^{-v} \otimes x$ est représentée par $\ell^{-v} \otimes (x\alpha^{-\ell^v})$ une ℓ -unité.

□

Remarque: On a ${}_{\ell^v} Cl'_K \simeq {}^{\ell^v} Cl'_K$ (non canoniquement) quotient d'exposant ℓ^v , et Cl'_K est le groupe de Galois de la ℓ -extension abélienne non ramifiée ℓ -décomposée maximale de K .

Le théorème de Dirichlet donne :

$$E'_K \simeq \mu_K \mathbb{Z}^{r+c+l-1}$$

où

r = nombre de places réelles.

c = nombre de places complexes.

l = nombre de places ℓ -adiques.

i.e. $|\ell^{-v} \mathbb{Z}/\mathbb{Z} \otimes E'_K| = (E'_K : I_K^{\ell^v}) = \ell^{v(r+c+l)}.$

Corollaire 7.1. Notons $(0, \mu, \lambda)$ les invariants structurels de groupe $X = \varprojlim Cl'_{K_n}$. On a alors $|{}^{\ell^n} Cl'_{K_n}| = \ell^{x_n}$ avec $x_n \sim \mu \ell^n + \lambda n$

Il suit $|\text{Rad}(M_n/K_n)| = \ell^{y_n}$ avec $r_n = \ell^n r$; $c_n = \ell^n c$; $l_n = l_\infty$, donc $(E'_{K_n} : E_{K_n}^{\ell^n}) = \ell^{z_n}$ avec $z_n \sim n \ell^n (r+c) + l_\infty n$, ce qui donne :

$$y_n = n \ell^n (r+c) + \mu \ell^n + (\lambda + l_\infty) n.$$

$\text{Rad}(M_n/K_n)$ est le dual de Kummer du groupe $\text{Gal}(M_n/K_n)$.

$$\begin{array}{ccccc} & & X & & \\ & \swarrow & & \searrow & \\ K_\infty & \text{---} & M_n & \text{---} & M_\infty \\ & \downarrow & & \uparrow & \\ & K & & X^{D_n} & \end{array}$$

On conclut que les invariants structurels de $X = \text{Gal}(M_\infty/K_\infty)$ sont $(r+c, \mu, \lambda + l_\infty)$.

Remarque: On a pris $S = \text{Pl}(\ell) = R$ et $T = \emptyset$ au départ, on a obtenu $S = \emptyset$, $T = R$ à l'arrivée.

7.4 La dualité de Gras

On suppose donnés

1. Un premier ℓ impair et un entier $v \geq 1$.
2. Un corps de nombres K contenant les racines ℓ^v -ièmes de l'unité.

3. Deux ensembles finis S et T disjoints de places finies verifiant $S \cup T \supset \text{Pl}_K(\ell)$.

On choisit un diviseur $\mathfrak{M} = \prod_{p \in T} p^{v_p}$ de tel sorte qu'on ait

$$U_{p^{v_p}}^{(up)} = 1 - p^v \subset (U_p^1)^{\ell^v}.$$

On construit un pseudo-radical ${}_{\ell^v}\mathfrak{R}_{\mathfrak{M}}^S$ dont l'écart à un vrai radical comme à un groupe de Galois va être contrôlé.

Dans une deuxième temps, on applique cette construction aux étages finis $(K_n)_{n \in \mathbb{N}}$ de la $\mathbb{Z}_{\ell}$ -extension cyclotomique d'un corps de nombres K contenant $\mathcal{G}_{\ell}$.

7.4.1 Principe

On utilise la description ℓ -adique et on introduit :

$$R_{\mathfrak{M}} = \{x \in R = \mathbb{Z}_{\ell} \otimes_{\mathbb{Z}} K^{\times} \mid x \equiv 1 \pmod{\mathfrak{M}}\}$$

en d'autres termes, pour $x = (x_p)_p$ dans $\mathcal{J}$ on demande $x_p \in U_{p^v} \subset U_p^{\ell^v}$.

Puis on pose

$$\mathfrak{R} = \{\ell^{-v} \otimes x \in \ell^{-v}\mathbb{Z}/\mathbb{Z} \otimes R_{\mathfrak{M}} \mid x \in \mathcal{J}^S \mathcal{J}^{\ell^v}\}$$

avec $\mathcal{J}^S = \prod_{p \in S} R_p \prod_{p \notin S} U_p$ (groupe de S -idéles), on demande donc $x_p \in U_p R_p^{\ell^v}$ pour $p \notin S$.

7.4.2 Première suite exacte (Interpretation Kummerienne)

Soit ${}_{\ell^v}\text{Rad}_S^T$ le radical kummerien de la ℓ -extension abélienne S -ramifiée, T -décomposée d'exposant ℓ^v maximale de K

$${}_{\ell^v}\text{Rad}_S^T = \{\ell^{-v} \otimes x \in \ell^{-v}\mathbb{Z}/\mathbb{Z} \otimes_{\mathbb{Z}_{\ell}} R \mid x \in \mathcal{J}_T^S \mathcal{J}^{\ell^v}\},$$

avec

$$\mathcal{J}_T^S = \prod_{p \in S} R_p \prod_{p \notin T} U_p.$$

En effet aux places de S , l'extension locale $K_p[\sqrt[\ell^v]{x_p}]$ est arbitraire (pas de conditions sur x_p) ; aux places de T , elle doit être triviale, i.e. $x_p = y_p^{\ell^v}$.

Théorème 7.2. *On a la suite canonique :*

$$\begin{array}{ccccccc} 1 & \rightarrow & {}_{\ell^v}(R/R_{\mathfrak{M}})/{}_{\ell^v}\mu & \rightarrow & {}_{\ell^v}\mathfrak{R}_{\mathfrak{M}}^S & \xrightarrow{\varphi} & {}_{\ell^v}\text{Rad}_S^T \rightarrow 1 \\ & & & & \ell^v \otimes x & \mapsto & \ell^{-v} \otimes x \end{array}$$

Preuve : $\ker(\varphi) = \{\ell^{-v} \otimes x \in \ell^{-v}\mathbb{Z}/\mathbb{Z} \otimes_{\mathbb{Z}_{\ell}} R_{\mathfrak{M}} \mid x \in R^{\ell^v}, \text{ i.e. } \exists y \in R \text{ avec } x = y^{\ell^v}\}$, provient des $y \in R$ qui vérifient $y^{\ell^v} \in R_{\mathfrak{M}}$.

□

7.4.3 Interpretation du noyau

Regardons $R/R_{\mathfrak{M}}$ dans $U_T/U_{\mathfrak{M}}$ avec $U_T = \prod_{p \in T} U_p$ et $U_{\mathfrak{M}} = \prod_{p \in T} U_p^{v_p}$. En relevant (par le théorème d'approximation simultanée) U_T dans R : étant donnée une famille $(x_p)_p \in T$ on peut toujours trouver un $x \in R$ qui vérifie $x_p = x_p$ pour $p \in T$.

On obtient un

$$\psi : R \rightarrow U_T \rightarrow U_T/U_{\mathfrak{M}}$$

de noyau $R_{\mathfrak{M}}$ c'est à dire qu'on a

$$R/R_{\mathfrak{M}} \simeq U_T/U_{\mathfrak{M}}.$$

Par hypothèse, on a pris $U_{\mathfrak{M}} \subset U_T^{\ell^\vee}$. Il vient donc :

$$\begin{aligned} {}_{\ell^\vee}(R/R_{\mathfrak{M}}) &= R/R_{\mathfrak{M}} \\ &= U_T/U_{\mathfrak{M}} \\ &= {}_{\ell^\vee}U_T/U_{\mathfrak{M}} \\ &\simeq {}_{\ell^\vee}U_T/U_{\mathfrak{M}} \\ &\simeq {}_{\ell^\vee}U_T. \end{aligned}$$

Pour $p \nmid \ell$, $U_p = \mu_p$. Pour $p|\ell$, $U_p = \mu_p \mathbb{Z}_\ell^{[U_p:\mathbb{Q}_\ell]}$.

Proposition 7.1. *On a ainsi*

$${}_{\ell^\vee}R/R_{\mathfrak{M}} \simeq \left(\prod_{{}_{\ell^\vee}p \in T} \mu_p \right) \times (\mathbb{Z}/{}_{\ell^\vee}\mathbb{Z})^{p|\ell; \sum_{p \in T} [K_p:\mathbb{Q}_\ell]}$$

7.4.4 Deuxième suite exacte (Interpretation Galoisienne)

Soit Gal_T^S le groupe de Galois de la ℓ -extension S -décomposée, T -ramifiée maximale

$$\text{Gal}_T^S = \mathcal{J} / \prod_{p \in S} R_p \prod_{p \notin T} U_p R.$$

On définit un morphisme de ${}_{\ell^\vee}\mathfrak{R}_{\mathfrak{M}}^S$ dans le groupe de Galois du ℓ -corps de S -classes de rayon $\mathfrak{M}$ de K d'exposant $\ell^\vee$

$${}_{\ell^\vee}\text{Cl}_{\mathfrak{M}}^S \simeq {}_{\ell^\vee}\text{Cl}_M^S = \text{Cl}_T^S = {}_{\ell^\vee}\text{Gal}_T^S.$$

Alors, on obtient :

Théorème 7.3. *On a la suite exacte canonique :*

$$1 \rightarrow {}_{\ell^\vee}\mathcal{G}_{\mathfrak{M}}^S = (\ell^{-\vee}/\mathbb{Z}) \otimes_{\mathbb{Z}_\ell} \varepsilon_{\mathfrak{M}}^S \rightarrow {}_{\ell^\vee}\mathfrak{R}_{\mathfrak{M}}^S \rightarrow {}_{\ell^\vee}\text{Gal}_T^S \rightarrow 1$$

avec $\varepsilon^S = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E^S$ le groupe des S -unités de K

$$\varepsilon^S \simeq \mu \times \mathbb{Z}_\ell^{r+c-1+s}$$

où s est le nombre de places au-dessus de S , d'où

$${}_{\ell^\vee}\mathcal{G}_{\mathfrak{M}}^S \simeq {}_{\ell^\vee}\mu \times (\mathbb{Z}/\ell^\vee\mathbb{Z})^{r+c-1+s}.$$

Remarque: $\varepsilon_{\mathfrak{M}}^S$ est le sous groupe de $R_{\mathfrak{M}} \cap \varepsilon^S$.

7.4.5 Conclusions

On applique tout ceci dans le cadre de la $\mathbb{Z}_\ell$ -extension cyclotomique K_∞/K .

- ${}_{\ell^\vee} \text{Rad}_S^\top$ est paramétrée par $(\rho_S^\top, \mu_S^\top, \tilde{\lambda}_S^\top)$.
- ${}_{\ell^\vee} \text{Gal}_T^S$ est paramétrée par $(\rho_T^S, \mu_T^S, \tilde{\lambda}_T^S)$.
- ${}_{\ell^\vee} \mathcal{G}_{\mathfrak{M}}$ est paramétrée par $(r+c, 0, s-1)$.
- ${}_{\ell^\vee} (R/R_{\mathfrak{M}})/{}_{\ell^\vee} \mu$ est paramétrée par $(\delta_T, 0, t-1)$,

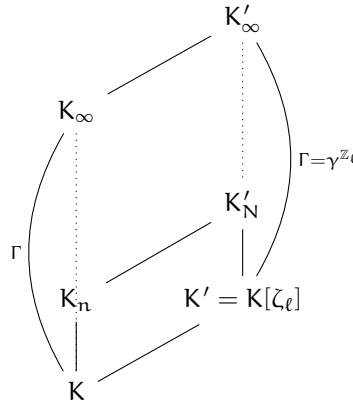
où est la somme des degrés locaux à T de ${}_{\ell^\vee} (\prod_{p \in T} \mu) {}_{\ell^\vee} \mu \times \mathbb{Z}_\ell^{\sum_{p \in T} d_\mu} \delta_T$.

Finalement, avec $r = 0$, $c = \frac{1}{2}[K : \mathbb{Q}] = \frac{1}{2}(\delta_T + \delta_S)$, on a les trois identités suivantes :

- (i) $\rho_S^\top + \frac{1}{2}\delta_T = \rho_T^S + \frac{1}{2}\delta_S$.
- (ii) $\mu_S^\top = \mu_T^S$ (Conjecturalement nul).
- (iii) $\tilde{\lambda}_S^\top + t - 1 = \tilde{\lambda}_T^S + s - 1$.

7.5 Cas general

Suppose $\zeta_\ell \notin K$. On se ramène au cas précédent en introduisant $K' = K[\zeta_\ell]$ (ℓ impair), on a bien $K'_\infty = K[\zeta_{\ell^\infty}]$,



ce qui permet de regarder les divers objets étudiés comme des $\mathbb{Z}_\ell[\Delta]$ (Ou $\Lambda[\Delta]$) modules

$$M = \bigoplus_{\varphi \in \Delta^\times} M_\varphi$$

et on retrouve M_K à partir de $M_{K'}$ en prenant la 1-composante (qui correspond à l'idempotent $e_1 = \frac{1}{|\Delta|} \sum_{\tau \in \Delta} \tau$ attaché au caractère unité).

7.5.1 Préliminaire

Le défaut δ de la conjecture de Leopoldt reste borné dans la $\mathbb{Z}_\ell$ -tour cyclotomique.

Rappel Si K est un corps de nombres, $\varepsilon = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}$, le ℓ -adique du groupe des unités $E = E_K$, $\varepsilon \simeq \mu \times \mathbb{Z}_\ell^{r+c-1}$. $U_\ell = \prod_{p|\ell} U_p$ le groupe des unités semi locales (avec $U_p = U_{K_p}^1$). Le sous groupe des unités infinitésimales est

$$\varepsilon^\infty = \ker(\varepsilon \rightarrow U_\ell),$$

et on a : $\varepsilon^\infty \simeq \mathbb{Z}_\ell^\delta$ où δ est le défaut de Leopoldt.

7.5.2 Preuve de l'assertion

Notons $\varepsilon_{K'_\infty}^\omega = \bigcup_{n \in \mathbb{N}} \varepsilon_{K'_n}^\omega$ le group de défaut en haut de la tour. Il s'agit de voir qu'il est de type fini sur $\mathbb{Z}_\ell$, ce qui montre que $\varepsilon_{K'_\infty}^\omega$ est ultimement constant.

Pour cela, introduisons l'extension kummerienne $K'_\omega[\mathfrak{C}_{K'_\infty}^\omega]$ avec $\mathfrak{C}_{K'_\infty}^\omega = (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \sqrt{\varepsilon_{K'_\infty}^\omega}$ et $\sqrt{\varepsilon_{K'_\infty}^\omega} = \mu_{K'_\infty}^{\text{loc}} = \{x \in R_{K_\infty} \mid x \in \prod_p \mu_{p_\infty}\}$.⁹

L'extension abélienne L'_∞/K'_∞ est localement triviale partout par construction, i.e. il est complètement décomposée en toutes ses places : elle est contenue dans l'extension H'_∞ abélienne maximale non ramifiée ℓ -décomposée de K'_∞ .

On a :

$$\text{Gal}(H'_\infty/K'_\infty) \simeq \varprojlim \text{Cl}'_{K'_n},$$

avec $\text{Cl}'_{K'_n} = \ell$ -groupe des ℓ -classes d'ideaux.

Les théorèmes de structure donnent donc

$$\begin{aligned} e' &\sim \bigoplus (\wedge/p_i) \oplus \left(\bigoplus \wedge/\ell^{\mu_i} \wedge \right) \\ &\simeq \mathbb{Z}_\ell^\lambda \oplus \text{module de torsion.} \end{aligned}$$

Or on a : $\mu_{K'_n}^{\text{loc}} \simeq \mu_{K'_n} \times \mathbb{Z}_\ell^{\delta_{K'_n}}$ d'où il suit $\delta_{K'_n} \leq \chi$, $\forall n \in \mathbb{N}$.

7.5.3 Enoncé des resultats en termes de caractères

On suppose K totalement réel et $K' = K[\zeta_\ell]$. Δ contient la conjugation complexe τ et on dit qu'un caractère ℓ -adique $\varphi \in \Delta^\times$ est

- réel quand on a $\varphi(\tau) = +1$
- imaginaire quand on a $\varphi(\tau) = -1$.

Pour tout $\mathbb{Z}_\ell[\Delta]$ -module $\mathfrak{M}$ on écrit

$$\begin{aligned} \mathfrak{M}^+ &= \bigoplus_{\varphi(\tau)=+1} \mathfrak{M}^{e_\varphi} = \mathfrak{M}^{\frac{1+\tau}{2}} \\ \mathfrak{M}^- &= \bigoplus_{\varphi(\tau)=-1} \mathfrak{M}^{e_\varphi} = \mathfrak{M}^{\frac{1-\tau}{2}} \end{aligned}$$

Remarque: Si φ est réel, son réflet $\varphi^* = \omega\varphi^{-1}$ est imaginaire et inversement.

7.5.4 Preuve des identités

On a obtenu les suites exactes courtes de $\mathbb{Z}_\ell[\Delta]$ -modules :

$$1 \rightarrow {}_\ell R/R_n / {}_\ell \mu \rightarrow {}_\ell \mathfrak{H}_{\mathfrak{M}_n}^S \rightarrow \text{Rad}_S^\top(K'_n) \rightarrow 1 \quad (6)$$

à droite les radicaux sont paramétrés par les caractères :

$$(\rho_T^S, \mu_T^S, \lambda_T^S)$$

9. On a $\mu_K^{\text{loc}} \simeq \mu_K \times \mathbb{Z}_\ell^{\delta_K}$.

à gauche $\ell^n \mu$ est paramétrée par $(0, 0, \omega)$

$$\ell^n \mathcal{U}_{T_n} = \left(\prod_{\mathfrak{p}'_n \in T, \mathfrak{p}'_n \nmid \ell} \ell^n \mu_{\mathfrak{p}'_n} \right) \left(\prod_{\mathfrak{p}'_n \in T, \mathfrak{p}'_n \mid \ell} \ell^n \mathcal{U}_{\mathfrak{p}'_n} \right)$$

où $\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}_n} \mathcal{U}_{\mathfrak{p}'_n} = \left(\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}} \mu_{\mathfrak{p}'_n} \right) \times \mathbb{Z}_\ell[\Delta/\Delta_{\mathfrak{p}_n}]$ et $\Delta_{\mathfrak{p}_n}$ est le sous groupe de décomposition de $\mathfrak{p}'_n$ dans K'_n/K_n , i.e. le sous groupe de décomposition de $\mathfrak{p} = \mathfrak{p}_0$ dans K'/K .

Notons $\chi_{\mathfrak{p}} = \text{Ind}_{\Delta_{\mathfrak{p}}}^{\Delta} s_{\Delta_{\mathfrak{p}}}$ le caractère du $\mathbb{Z}_\ell[\Lambda]$ -module $\mathbb{Z}_\ell[\Lambda/\Lambda_{\mathfrak{p}}]$ puis $\delta_T = \sum_{\mathfrak{p} \in T, \mathfrak{p} \mid \ell} (\deg_\ell T) \chi_{\mathfrak{p}}$ ¹⁰ et $\chi_T = \sum_{\mathfrak{p} \in T} \chi_{\mathfrak{p}}$.

En fin de compte, $\ell^n \mathcal{U}_{T_n}$ est paramétrée par les caractères $(\delta_T, 0, \omega \chi_T)$.

En resumé le groupe median est paramétrée par

$$(\rho_T^S, \mu_T^S, \lambda_T^S + \omega(\chi_T - 1))$$

Remarque: On a $\chi_{\mathfrak{p}}^{-1} = \chi_{\mathfrak{p}}$ (avec la convention $\chi_{\mathfrak{p}}^{-1}(\sigma) := \chi_{\mathfrak{p}}(\sigma^{-1})$) donc $\chi_T^{-1} = \chi_T$ et finalement

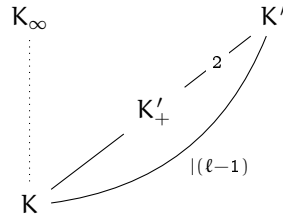
$$\omega(\chi_T - 1) = (\chi_T - 1)^*.$$

$$1 \rightarrow \ell^n \mathfrak{C}_{\mathfrak{M}_n}^S \rightarrow \ell^n \mathfrak{H}_{\mathfrak{M}_n}^S \rightarrow \ell^n \text{Gal}_T^S(K_n) \rightarrow 1 \quad (7)$$

Rappelons que $\ell^n \mathfrak{C}_{\mathfrak{M}_n}^S \simeq \ell^n (\varepsilon^S / \mu)$.

Le théorème de Herbrand donne le caractère du module ε^S / μ c'est $\sum_{\mathfrak{p} \mid S, \infty} \text{Ind}_{\Delta_{\mathfrak{p}}}^{\Delta} s_{\Delta_{\mathfrak{p}}}^{-1} = \underbrace{\chi_{\infty}}_{\deg C} + \underbrace{\chi_S}_{\deg S} - 1$,

avec $\chi_{\infty} = \sum_{\mathfrak{p} \mid \infty} \text{Ind}_{\Delta_{\mathfrak{p}}}^{\Delta} s_{\Delta_{\mathfrak{p}}}$.



Avec $\deg \chi_{\infty} = c$ et $\deg \chi_S = S$.

En résumé, les paramètres sont : $\begin{cases} \text{à gauche : } (\chi_{\infty}, 0, \chi_S - 1) \\ \text{à droite : } (\rho_T^S, \mu_T^S, \lambda_T^S) \end{cases}$

Au total $(\rho_T^S + \chi_{\infty}, \mu_T^S, \lambda_T^S + (\chi_S - 1))$.

7.5.5 Identités de dualité

En fin de compte on a :

(i) $\rho_T^S + \chi_{\infty} = \rho_S^T + \delta_T$

(ii) $\mu_T^S = \mu_S^T$

(iii) $\lambda_T^S + (\chi_S - 1) = (\lambda_S^T + (\chi_T - 1))^*$

¹⁰. $\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}_n} \mathcal{U}_{\mathfrak{p}'_n} \simeq \left(\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}_n} \mu_{\mathfrak{p}'_n} \right) \oplus \left(\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}_n} \mathcal{O}_{\mathfrak{p}'_n} \right)$ où $\bigoplus_{\mathfrak{p}'_n \mid \mathfrak{p}_n} \mathcal{O}_{\mathfrak{p}'_n} \approx \mathcal{O}_{\mathfrak{p}_n}[\Delta]$ caractère $[K_{\mathfrak{p}_n} : \mathbb{Q}_\ell] \chi_{\text{reg}}$, alors $\delta_T = \sum_{\mathfrak{p} \in T, \mathfrak{p} \mid \ell} (\deg_\ell T) \chi_{\mathfrak{p}}$ et $\deg_\ell T = \sum_{\mathfrak{p} \in T, \mathfrak{p} \mid \ell} [K_{\mathfrak{p}} : \mathbb{Q}_\ell]$.

Remarque: On peut écrire (i) sous forme symétrique en observant qu'on a $\chi_\infty + \chi_\omega^* = [K : \mathbb{Q}]_{\chi_{\text{reg}}} = \delta_T + \delta_S$. Ce qui donne :

$$(i)' \quad \rho_T^S + \frac{1}{2}(\chi_\omega + \delta_S) = (\rho_S^T + \frac{1}{2}(\chi_\omega + \delta_T))^*.$$

7.6 Détermination des invariants ρ

Corollaire 7.2. *On a $\rho_T^S = (\delta_T)^-$ pour l'extension S -décomposée T -ramifiée.*

Preuve : Cela résulte du fait que le défaut de Leopoldt est borné dans la tour.

On a vu qu'on a $\text{Gal}(M/H) \simeq \mu_\ell / s_\ell(\varepsilon)$ pour M ℓ -ramifiée maximale, H non ramifiée ℓ -décomposée maximale ($M = M_L^\emptyset$, $H = H_\emptyset^L$).

On a $\text{rg}_{\mathbb{Z}_\ell} \mu_\ell^+ = [K^+ : \mathbb{Q}] = c$ et $\text{rg}_{\mathbb{Z}_\ell} s_\ell(\varepsilon^+) = \text{rg}_\ell(\varepsilon) - \delta = c - 1 - \delta$ donc $\text{rg}_{\mathbb{Z}_\ell}(\text{Gal}(M/H)^+) \leq \delta + 1$

On conclut $(\rho_L^\emptyset)$ est nul, donc aussi ρ_T^S quelque soient S et T (vérifiant $S \cup T \supset L = \text{Pl}(\ell)$).

Il suit

$$\begin{aligned} \rho_T^S &= (\rho_T^S)^- \\ &= (\rho_T^S + \chi_\omega)^- \\ &= (\rho_S^T + \delta_T)^- \\ &= (\rho_S^T)^- + \delta_T^- \\ &= (\rho_S^T)^* + \delta_T^- \\ &= \delta_T^-. \end{aligned}$$

□

7.7 Détermination des invariants μ

On suppose toujours $\mu_\ell \subset K$ (ℓ impair) et $S \cup T \supset L = \text{Pl}_K(\ell)$. Il peut être intéressant de poser

$$S = S_\ell \cup S_0$$

$$T = T_\ell \cup T_0$$

avec $S_\ell = S \cap L$ (places ℓ -adiques dans S , dites *sauvages*) et $S \setminus S_\ell = S_0$ (places modérées dans S , dites *tame*).

Proposition 7.2. *On a $\mu_T^S = \mu_{T_\ell}^{S_\ell} = \mu_{T_\ell}^{\bar{T}_\ell}$ (avec $\bar{T}_\ell = L \setminus T_\ell$, puis qu'on a $S_\ell \cup T_\ell = L$).*

Preuve : On a vu déjà qu'on a :

$$\mu_T^S = \mu_{T_\ell}^{S_\ell}$$

car les sous groupes de décomposition des places de S_0 engendrent un $\mathbb{Z}_\ell$ -module de rang fini, donc sont sans conséquence sur l'invariant μ . Il suit :

$$\mu_T^S = \mu_{T_\ell}^{S_\ell} = (\mu_{S_\ell}^T)^* = (\mu_{S_\ell}^{T_\ell})^* = \mu_{T_\ell}^{S_\ell}.$$

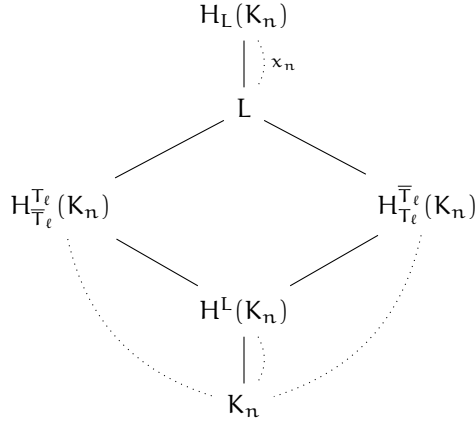
□

Proposition 7.3. *On a*

$$\mu_{T_\ell}^{\bar{T}_\ell} + \mu_{T_\ell}^{T_\ell} \leq \mu^L + \mu_L = \mu^L + (\mu^L)^*$$

Et la conjecture d'Iwasawa $\mu_\emptyset^\emptyset = 0$ implique donc $\mu_T^S = 0$, $\forall S, T$.

Preuve : Considerons le schema d'extensions :



Dans celui-ci, toutes les extensions relatives sont paramétrées (indiqué avec lignes pointillées).

On a

$$\rho^L = 0 \quad \text{et} \quad \rho_{T_\ell}^{T_\ell} + \rho_{T_\ell}^{\bar{T}_\ell} = \rho_L$$

par le calcul précédent.

On conclut $\chi_n(\rho) = 0$. Et, s'il n'est pas nul le terme dominant pour

$$\chi_n = \text{Gal}(H_L/H_{T_\ell}^{T_\ell} H_{T_\ell}^{\bar{T}_\ell})$$

est le terme en μ . On conclut

$$\mu_L \geq \mu_{T_\ell}^{T_\ell} + \mu_{T_\ell}^{\bar{T}_\ell} - \mu_L,$$

i.e.

$$\mu_{T_\ell}^{T_\ell} + \mu_{T_\ell}^{\bar{T}_\ell} \leq \mu_L + \mu^L = \mu^L + (\mu^L)^* \leq \mu_\emptyset^\emptyset + (\mu_\emptyset^\emptyset)^*.$$

□

En particulier c'est le cas dès que K est abélien sur $\mathbb{Q}$.

7.8 Détermination des invariants λ

Théorème 7.4. *Sur les hypothèses précédentes on a :*

$$\begin{aligned} \lambda_T^S &= \lambda_{T_\ell}^{S_\ell} + \chi_T^* \\ &= \lambda_{S_\ell}^{S_\ell} + \chi_T^* \end{aligned}$$

Preuve : On a vu qu'on a :

$$\lambda_T^S = \lambda_T^{S_\ell},$$

il suit :

$$\lambda_T^S + (\chi_S - 1) = \lambda_T^{S_\ell} + (\chi_{S_\ell} - 1) + \chi_{S_0}$$

puis qu'on a

$$\chi_S = \sum_{p \in S} \chi_p = \chi_{S_\ell} + \chi_{S_0}.$$

Par dualité, on obtient

$$\begin{aligned}
\lambda_T^S + (\chi_S - 1) &= (\lambda_{S_\ell}^T + (\chi_T - 1))^* + \chi_{S_0} \\
&= (\lambda_{S_\ell}^{T_\ell} + (\chi_{T_\ell} - 1) + \chi_{T_0})^* + \chi_{S_0} \\
&= \lambda_{T_\ell}^{S_\ell} + \chi_{T_0}^* + \underbrace{(\chi_{S_\ell} - 1) + \chi_{S_0}}_{=\chi_S - 1}
\end{aligned}$$

donc $\lambda_T^S = \lambda_{T_\ell}^{S_\ell} + \chi_{T_0}^*$.

□

Remarque:

1. Pour la partie imaginaire les places sauvages jouent librement dans $\lambda_{\bar{S}_\ell}^{S_\ell}$, ce qui donne

$$(\lambda_{\bar{S}_\ell}^{S_\ell})^- = (\lambda_{\bar{S}_\ell}^\emptyset)^- - (\chi_{S_\ell})^-.$$

Pour la partie réelle, la conjecture de Greenberg donne

$$(\lambda_{\bar{S}_\ell}^{S_\ell})^+ = (\lambda_{\bar{\emptyset}}^{S_\ell})^+.$$

2. Regardons la partie imaginaire des groupes de classes d'ideaux dans la tour

$$\begin{array}{c}
K_\infty \\
\vdots \\
K_{n+1} = K_n[\sqrt[\ell]{\zeta}] \\
\mid \\
K_n \\
\vdots \\
K
\end{array}$$

$\mathfrak{p}_n^{\ell^k} = (\alpha_n)$ principal.

Est-ce qu'on peut avoir

$$\mathfrak{p}_{n+1}^{\ell^k} = (\alpha_{n+1})$$

donc

$$(\alpha_{n+1})^\ell = (\alpha_n)$$

alors

$$\alpha_{n+1}^\ell = \alpha_n \zeta$$

avec ζ racine de l'unité.

Références

- [1] Emil Artin and John Tate. *Class field theory*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, second edition, 1990.
- [2] J.-F. Jaulent. *L'arithmétique des l-extensions*. Publications Mathématiques de la Faculté des Sciences de Besançon. [Mathematical Publications of the Faculty of Sciences of Besançon]. Université de Franche-Comté, Faculté des Sciences, Besançon, 1986. Dissertation, Université de Franche-Comté, Besançon, 1986, Théorie des nombres. Fasc. 1. 1984–1986 [Number theory. Part 1. 1984–1986].

- [3] J.-F. Jaulent. Théorie des nombres de base. PDF, Institute de Mathématiques de Bordeaux, Ecole Doctoral de Mathématiques de Bordeaux, 4 2014. 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. Transcrites par JIVG.