THEORIE DES NOMBRES

BESANCON

Années 1984/85-1985/86

Fascicule 2

GENRE DES CORPS SURCIRCULAIRES

Jean-François JAULENT

Genre des corps surcirculaires

Jean-François Jaulent

On sait, depuis les travaux essentiels d'Iwasawa sur les $\mathbb{Z}_\ell$-extensions des corps de nombres, que l'invariant λ associé aux ℓ-groupes de classes imaginaires dans une tour cyclotomique de corps à conjugaison complexe est, sous réserve de nullité de l'invariant μ, un bon analogue pour la théorie des nombres de la notion classique de genre attachée aux corps de fonctions d'une variable(*).

Un exemple particulièrement frappant de cette analogie est la formule, démontrée par Kida (cf. [20]), qui relie les invariants lambda associés aux ℓ-groupes de classes imaginaires dans une ℓ-extension finie quelconque de corps à conjugaison complexe, et joue dans la théorie d'Iwasawa le rôle de la formule de Riemann-Hurwitz dans celle des corps de fonctions d'une variable. De fait, une formule semblable avait été établie peu avant par Kuz'min (cf. [22]) pour les invariants lambda associés aux ℓ-groupes de ℓ-classes imaginaires de ces corps (i.e. aux quotients des ℓ-groupes de classes imaginaires de ces corps par leurs sous-groupes respectifs engendrés par les classes des idéaux premiers au-dessus de ℓ)(**). Ultérieurement, Wingberg [23] a montré qu'une formule identique vaut pour les invariants lambda associés aux ℓ-groupes de classes infinitésimales(***) dans une ℓ-extension de corps totalement réels. Plus récemment, des démonstrations simplifiées de ces résultats ont été données par D'Mello et Madan (cf. [2]), dans le cas étudié par Kida ; par Gold et Madan (cf. [5]), dans celui considéré par Kuz'min.

Auparavant, Iwasawa avait remarqué que la formule de Kida se généralisait en une identité entre représentations en tout point analogue à la formule de Chevalley-Weil pour les corps de fonctions (cf. [1]) ; il en déduisit une preuve cohomologique du résultat de Kida (cf. [13]), que Gold et Madan ont récemment simplifiée (cf. [6]).

(*) Une extension de corps imaginaires est dite admettre une conjugaison complexe lorsqu'elle provient d'une extension de même degré de leurs sous-corps réels.

(**) Le résultat de Kuz'min semble, aujourd'hui encore, curieusement méconnu. Il est vrai que la traduction anglaise de son long article aux Izvestija est légèrement postérieure au travail de Kida.

(***) En fait, Wingberg travaille sur des groupes de Galois. L'interprétation infinitésimale est celle de [16].

A ces démonstrations algébriques il convient d'ajouter, pour être complet, celles obtenues par voie analytique, qui utilisent la correspondance, démontrée par Iwasawa, entre les invariants λ et μ, et les fonctions L ℓ-adiques. La plus ancienne dans cette perspective est incontestablement la formule obtenue par Gras (cf. [9]) pour les corps abéliens à l'aide des fonctions L_ℓ de Kubota-Leopoldt. La preuve générale, due à Sinnott (cf. [23]), s'appuie sur la notion de pseudo-mesure ℓ-adique introduite par Serre. Tout récemment Gold et Madan ont montré que les méthodes de Sinnott s'appliquaient encore dans un cadre métacyclique où le degré des extensions n'est pas une puissance de ℓ. Les relations entre fonctions L qu'ils utilisent peuvent être regardées comme la version ℓ-adique des identités complexes étudiées par Brauer et Walter (cf. [15]).

Cela dit, l'objet de cet article est triple :

(i) En premier lieu, nous montrons que les multiples formules évoquées plus haut ne sont que les diverses formulations d'une seule et même identité arithmétique. L'argument essentiel est ici la correspondance, exposée dans [18] et établie dans [17], entre les invariants lambda associés aux différents groupes étudiés, qui affirme que tous les paramètres considérés se ramènent, au moins sous les conjectures de Leopoldt et de Gross, à l'un quelconque d'entre eux au moyen de formules standards.

(ii) Nous établissons ensuite que les deux expressions possibles de cette identité (en termes numériques ou bien en termes de représentations, c'est-à-dire de caractères) sont rigoureusement équivalentes. Ce point résulte d'un argument classique de Herbrand, qui ramène l'étude d'une représentation galoisienne à la détermination des restrictions de son caractère aux sous-groupes cycliques du groupe de Galois.

(iii) Enfin, nous prouvons que, par une heureuse coïncidence du vocabulaire, l'identité en question relève intégralement de la théorie habituelle des genres pour les corps de nombres. Nous en donnons deux démonstrations algébriques ; la première, écrite en termes de groupes de classes, s'obtient simplement par passage à la limite inductive à partir des suites exactes classiques de la théorie des genres ; la seconde, écrite en termes de groupes de Galois, s'obtient par passage à la limite projective. Nous renvoyons à [11] pour une théorie analytique des genres basée sur la notion de pseudo-mesure p-adique.

Dans la première partie, nous utilisons largement le formalisme général des groupes de S-classes T-infinitésimales introduit dans [19], dont le cadre très souple permet de rendre compte des diverses situations évoquées plus haut, qui correspondent simplement à des choix particuliers de S et de T. Nous renvoyons à [19] pour une démonstration des résultats techniques sur les groupes $C\ell$ que nous utilisons.

1. Description des paramètres lambda attachés à un corps surcirculaire :

a. Présentation des corps surcirculaires :

Le nombre premier ℓ étant supposé fixé une fois pour toutes, désignons par $\mathbb{Q}_\infty$ la $\mathbb{Z}_\ell$-extension cyclotomique du corps des rationnels. Les invariants que nous nous proposons d'étudier sont attachés à une catégorie bien particulière de corps, stable par extension finie :

Définition 1. Nous appelons corps surcirculaire (relativement au nombre premier ℓ) toute extension algébrique finie de la $\mathbb{Z}_\ell$-extension cyclotomique $\mathbb{Q}_\infty$ du corps des rationnels.

Remarque. Iwasawa appelle $\mathbb{Z}_\ell$-corps les extensions de $\mathbb{Q}$ obtenues comme $\mathbb{Z}_\ell$-extensions d'un corps de nombres de degré fini. Cette notion ne nous parait pas exactement adaptée au problème que nous considérons, puisque les résultats que nous avons en vue supposent explicitement que la $\mathbb{Z}_\ell$-extension étudiée soit la cyclotomique.

Tout corps surcirculaire K_∞ peut être regardé, d'une infinité de façons, comme la $\mathbb{Z}_\ell$- extension cyclotomique d'un corps de nombres K. Par exemple, si x est un élément primitif de K_∞ sur $\mathbb{Q}_\infty$, il est immédiat que $K = \mathbb{Q}(x)$ convient. Quoique non canonique, cette description des corps surcirculaires va nous être utile pour appliquer les théorèmes de structure de la théorie d'Iwasawa.

Notons auparavant qu'en vertu de la loi de décomposition des idéaux premiers dans une tour cyclotomique, le fait que tout corps surcirculaire K_∞ s'écrive $K.\mathbb{Q}_\infty$, pour un corps de nombre (de degré fini) convenable K, montre que les places ultramétriques de $\mathbb{Q}$ sont finiment décomposées dans $K_\infty/\mathbb{Q}$. Plus précisément, nous avons le résultat bien connu suivant :

Lemme 1. Soient K_∞ un corps surcirculaire, et K un corps de nombres vérifiant $K_\infty = K.\mathbb{Q}_\infty$.

(i) Les places de K au-dessus de ℓ sont presque totalement ramifiées dans K_∞/K ; c'est-à-dire qu'il existe une sous-extension K_{n_o} de K_∞, de degré fini ℓ^{n_o} sur K, telle que les places au-dessus de ℓ soient totalement ramifiées dans

K_∞/K_{n_o}.

(ii) Les autres places ultramétriques sont presque totalement inertes dans K_∞/K ; c'est-à-dire qu'il existe, pour chaque premier $\mathfrak{p}$ de K, une sous-extension $K_{n_\mathfrak{p}}$ de K_∞, de degré fini sur K, telle que les places au-dessus de $\mathfrak{p}$ soient inertes dans $K_\infty/K_{n_\mathfrak{p}}$.

(iii) Les places archimédiennes sont complètement décomposées dans K_∞/K.

Une conséquence élémentaire mais peu citée de l'assertion (ii) concerne les corps résiduels : si $\mathfrak{p}$ est une place de K au-dessus d'un premier p différent de ℓ, le corps résiduel $K_{\mathfrak{p}_\infty} = \mathcal{O}_\infty/\mathfrak{p}_\infty$ associé à l'une quelconque $\mathfrak{p}_\infty$ des places de K_∞ au-dessus de $\mathfrak{p}$ est la $\mathbb{Z}_\ell$-extension (cyclotomique) de $k_\mathfrak{p}$, c'est-à-dire la ℓ-extension (abélienne) maximale de $\mathbb{F}_\mathfrak{p}$. En particulier, dans une ℓ-extension de corps surcirculaires L_∞/K_∞, il ne peut y avoir inertie aux places ultramétriques étrangères à ℓ.

Enfin, il résulte du lemme que le groupe des diviseurs d'un corps surcirculaire peut se décrire comme suit :

(i) Les diviseurs construits sur les places au-dessus de ℓ forment un $\mathbb{Q}$-espace vectoriel de dimension finie :

$$D_{K_\infty}(\ell) = \bigoplus_{\mathfrak{p}_\infty | \ell} \mathfrak{p}_\infty^{\mathbb{Q}}$$

(ii) Les diviseurs construits sur les places au-dessus d'un premier $p \neq \ell$ forment un $\mathbb{Z}$-module libre de dimension finie :

$$D_{K_\infty}(p) = \bigoplus_{\mathfrak{p}_\infty | p} \mathfrak{p}_\infty^{\mathbb{Z}}$$

(iii) Les diviseurs construits sur les places archimédiennes forment un $\mathbb{F}_2$-espace vectoriel qui est soit nul (si K_∞ n'admet aucun plongement réel), soit infini dénombrable (si K_∞ admet un et donc une infinité de plongements réels).

$$D_{K_\infty}(\infty) = \bigoplus_{\mathfrak{p}_\infty | \infty} \mathfrak{p}_\infty^{\mathbb{Z}/2\mathbb{Z}}$$ [Le produit portant sur les places réelles de K_∞].

Il vient alors : $D_{K_\infty} = D_{K_\infty}(\ell) \oplus \left(\bigoplus_{p \neq \ell} D_{K_\infty}(p)\right) \oplus D_{K_\infty}(\infty)$.

b. <u>Les théorèmes de structure de la théorie d'Iwasawa</u> :

Reprenons la description des corps surcirculaires donnée plus haut. Supposons donné un corps de nombres K (de degré fini sur $\mathbb{Q}$) ; et considérons la $\mathbb{Z}_\ell$-extension cyclotomique K_∞ construite sur K. Notons $\Gamma = Gal(K_\infty/K)$ le groupe de Galois correspondant, identifié à $\mathbb{Z}_\ell$ par le choix d'un générateur topologique γ, puis $\Lambda = \mathbb{Z}_\ell[[\gamma-1]]$ l'algèbre d'Iwasawa associée. Ecrivons de même K_n l'unique sous-corps de K_∞ cyclique de degré ℓ^n sur K, et $\Gamma_n = Gal(K_\infty/K_n)$ le sous-groupe de Γ associé à K_n par la théorie de Galois.

Supposons choisis deux ensembles finis disjoints S et T de places de $\mathbb{Q}$, et considérons les ℓ-groupes $C\ell_T^S(K_n)$ de S-classes T-infinitésimales des corps K_n. La définition précise des groupes $C\ell_T^S(K_n)$ est sans importance ici, car nous ne serons intéressés que par des spécialisations très particulières de S et de T(*) ; disons simplement que $C\ell_T^S(K_n)$ est le ℓ-groupe de classes de diviseurs qui s'identifie canoniquement, via la théorie du corps de classes, au groupe de Galois $G_T^S(K_n)$ de la ℓ-extension abélienne maximale de K_n qui est T-ramifiée et S-décomposée (c'est-à-dire non ramifiée aux places étrangères à T, complètement décomposée aux places au-dessus de S, et maximale sous ces deux conditions).

Au sommet de la tour cependant, cet isomorphisme n'a plus lieu, et il importe de distinguer entre groupes de classes et groupes de Galois. C'est pourquoi nous poserons :

<u>Notation</u>. Etant donnés un corps surcirculaire $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$, et deux ensembles finis disjoints S et T de places de $\mathbb{Q}$, nous écrivons :

(i) $$\mathcal{C}_T^S(K_\infty) = \varprojlim C\ell_T^S(K_n)$$

la limite du système projectif des groupes $C\ell_T^S(K_n)$ pour les applications $N_{m/n}$ induites par la norme arithmétique. Le groupe $\mathcal{C}_T^S(K_\infty)$ est un Λ-module compact, canoniquement isomorphe au groupe de Galois $G_T^S(K_\infty)$ de la ℓ-extension abélienne maximale T-ramifiée et S-décomposée du corps K_∞.

(ii) $$C\ell_T^S(K_\infty) = \varinjlim C\ell_T^S(K_n)$$

la limite du système inductif des groupes $C\ell_T^S(K_n)$ pour les applications $j_{m/n}$ induites par l'extension des diviseurs. Nous disons que $C\ell_T^S(K_\infty)$ est le ℓ-groupe des S-classes T-infinitésimales du corps K_∞.

(*) Le lecteur intéressé par la définition et les principales propriétés des groupes $C\ell_T^S$ pourra se reporter au chapitre II, section 1, de [19].

Cela posé, les théorèmes de structure de la théorie d'Iwasawa affirment l'existence de trois invariants numériques ρ_T^S, μ_T^S, et λ_T^S, qui mesurent la croissance avec n des quotients d'exposant ℓ^n des groupes $C\ell_T^S(K_n)$; c'est-à-dire qu'il existe une constante ν_T^S (éventuellement négative), telle qu'on ait :

$$|{}^{\ell^n}C\ell_T^S(K_n)| = \ell^{x_n}\ , \text{ avec } x_n = \rho_T^S n \ell^n + \mu_T^S \ell^n + \lambda_T^S n + \nu_T^S,$$

pour tout n assez grand. Les valeurs exactes des paramètres ρ_T^S et μ_T^S, qui dépendent du choix du corps de base K, ne sont pas, à proprement parler, des invariants de K_∞. Il n'en est pas de même, en revanche, de l'invariant λ_T^S, qui est au coeur de notre étude.

Précisons tout cela :

<u>Proposition 1</u>. Le groupe $\mathcal{C}_T^S(K_\infty)$ est un Λ-module de torsion si et seulement si l'une ou l'autre des deux conditions suivantes est vérifiée :

(i) ou bien l'ensemble T ne contient pas la place ℓ.

(ii) ou bien l'ensemble T contient ℓ, et dans ce cas le corps K_∞ est totalement réel.

Dans tous les autres cas, le paramètre ρ_T^S associé au groupe $\mathcal{C}_T^S(K_\infty)$ est égal au nombre de places complexes du corps K.

Démonstration. Ce résultat étant essentiellement bien connu, nous nous contenterons d'une esquisse de sa démonstration.

(i) Si T ne contient pas ℓ, les groupes $C\ell_T^S(K_n)$ sont finis, et leur limite projective est un Λ-module de torsion par un argument classique de théorie d'Iwasawa.

(ii) Si T contient ℓ, les groupes $C\ell_T^S(K_n)$ sont infinis, et deux cas se présentent :

- Lorsque le corps K n'est pas totalement réel, il possède au moins un conjugué imaginaire, et le corps K_∞ admet alors une infinité de $\mathbb{Z}_\ell$-extensions qui sont non ramifiées en dehors de ℓ. Comme il ne peut y avoir inertie aux places ultramétriques étrangères à ℓ dans une ℓ-extension de K_∞, ces $\mathbb{Z}_\ell$-extensions sont S-décomposées ; et le groupe $\mathcal{C}_T^S(K_\infty)$ n'est donc pas un Λ-module de torsion.

- Lorsque, en revanche, K es totalement réel, le corps K_∞ n'admet qu'un nombre fini de $\mathbb{Z}_\ell$-extensions ℓ-ramifiées, en vertu de l'exactitude de la conjecture faible de Leopoldt dans les tours cyclotomiques (cf. [19], ch. IV, section 2). Les groupes $\mathcal{C}_{\{\ell\}}^S(K_\infty)$ sont ainsi des Λ-modules de torsion. Il en va de même pour les groupes $\mathcal{C}_T^S(K_\infty)$, puisque, les places de K_∞ au-dessus de T étant en nombre fini, le sous-module de $\mathcal{C}_T^S(K_\infty)$ engendré par les sous-groupes d'inertie associés est un $\mathbb{Z}_\ell$-module de type fini.

Dans les deux cas, le paramètre ρ_T^S est celui du groupe $\mathcal{C}_\ell(K_\infty) = \mathcal{C}_{\{\ell\}}^{\emptyset}(K_\infty)$, qui correspond à la ℓ-extension abélienne ℓ-ramifiée maximale du corps K_∞. Comme il est bien connu que celui-ci est égal au nombre de places complexes du corps K (*), la proposition est ainsi établie.

<u>Proposition 2</u>. Lorsque le corps K_∞ contient les racines 2ℓ-ièmes de l'unité, les groupes $\mathcal{C}_T^S(K_\infty)$ ont même paramètre mu, quels que soient les ensembles finis S et T de places de $\mathbb{Q}$. En particulier, la condition $\mu_T^S = 0$ a lieu, en dehors de toute autre hypothèse sur K_∞, dès que le groupe de Galois $G^\ell(K_\infty[\zeta_{2\ell}])$ associé à la ℓ-extension abélienne maximale non ramifiée et ℓ-décomposée du corps surcirculaire $K_\infty[\zeta_{2\ell}]$ est un $\mathbb{Z}_\ell$-module de torsion (**).

Démonstration. Les résultats de [17] montrent que les trois groupes $\mathcal{C}(K_\infty) = \mathcal{C}_\emptyset^\emptyset(K_\infty)$, $\mathcal{C}^\ell(K_\infty) = \mathcal{C}_\emptyset^{\{\ell\}}(K_\infty)$, et $\mathcal{C}_\ell(K_\infty) = \mathcal{C}_\ell^\emptyset(K_\infty)$, qui correspondent respectivement à la ℓ-extension abélienne maximale non-ramifiée de K_∞, à celle qui est non ramifiée et ℓ-décomposée, et à celle qui est ℓ-ramifiée, ont même paramètre mu, dès que le corps K_∞ contient toutes les racines d'ordre ℓ-primaire de l'unité (***). La proposition en résulte immédiatement, puisque les places de S et de T qui sont étrangères à ℓ sont sans influence sur le paramètre μ, les premières parce qu'il ne peut y avoir inertie dans une ℓ-extension de K_∞ en une place étrangère à ℓ, les secondes parce que le sous-groupe d'inertie d'une telle place dans une ℓ-extension de K_∞ est un $\mathbb{Z}_\ell$-module de type fini (****).

C'est une conjecture classique de la théorie d'Iwasawa que de supposer nul le paramètre mu associé aux ℓ-groupes de classes au sens ordinaire $\mathcal{C}\ell^{ord}(K_n)$ dans la $\mathbb{Z}_\ell$-extension cyclotomique $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ d'un corps de nombres (de degré fini) K. D'après la proposition 2, cela revient à supposer que l'on a

---

(*) Ce résultat $\rho_\ell = c_K$ est, en fait, équivalent à l'exactitude de la conjecture faible de Leopoldt dans K_∞/K.

(**) On ne connait pas de corps surcirculaire, ni même de $\mathbb{Z}_\ell$-corps, dans lequel cette condition est en défaut.

(***) On trouvera une autre démonstration de ce résultat dans le chapitre IV, section 2, de [19].

(****) Cet argument serait sans valeur dans un $\mathbb{Z}_\ell$-corps non surcirculaire, où les places de T étrangères à ℓ seraient susceptibles d'être infiniment décomposées.

$\mu_T^S(K_\infty)=0$, pour tout corps surcirculaire K_∞, quels que soient les ensembles finis S et T de places de $\mathbb{Q}$. Un résultat célèbre de Ferrero et Washington montre qu'il en est bien ainsi dès que le corps K_∞ est abélien sur $\mathbb{Q}$ (cf. [24], th.7.15). Bien entendu, ce n'est plus vrai en général pour les $\mathbb{Z}_\ell$-corps non surcirculaires (cf. [13]).

c. Le problème de la capitulation :

Nous avons dit plus haut que les valeurs exactes des paramètres ρ_T^S et μ_T^S attachés à un corps surcirculaire K_∞, peuvent dépendre du choix du corps de base K. Il n'en est pas de même, en revanche, des conditions $\rho_T^S = 0$ et $\mu_T^S = 0$.

(i) La première $\rho_T^S=0$ signifie en effet que le $\mathbb{Q}_\ell$-espace vectoriel $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{C}_T^S(K_\infty)$ construit sur le $\mathbb{Z}_\ell$-module $\mathcal{C}_T^S(K_\infty)$ est de dimension finie.

(ii) La seconde $\mu_T^S=0$ affirme, elle, que le sous-module de $\mathbb{Z}_\ell$-torsion $\mathrm{Tor}_T^S(K_\infty)$ de $\mathcal{C}_T^S(K_\infty)$ est un $\mathbb{Z}_\ell$-module fini.

Lorsqu'elles sont vérifiées, le groupe $\mathcal{C}_T^S(K_\infty)$ est ainsi un $\mathbb{Z}_\ell$-module de type fini, somme directe comme tel d'un $\mathbb{Z}_\ell$-module libre de dimension λ_T^S, et du sous-groupe fini $\mathrm{Tor}_T^S(K_\infty)$:

$$\mathcal{C}_T^S(K_\infty) \simeq \mathbb{Z}_\ell^{\lambda_T^S} \oplus \mathrm{Tor}_T^S(K_\infty).$$

Dans ce cas, les résultats de [8] interprètent le groupe $\mathrm{Tor}_T^S(K_\infty)$ comme limite projective des noyaux $\mathrm{Cap}_T^S(K_n)$ des applications naturelles j_n des ℓ-groupes de S-classes T-infinitésimales $C\ell_T^S(K_n)$ des corps K_n dans leur limite inductive $C\ell_T^S(K_\infty)$, qui est ici soit un $\mathbb{Z}_\ell$-module divisible de corang λ_T^S, soit, sous la conjecture de Leopoldt, somme directe d'un tel module et d'un exemplaire de $\mathbb{Z}_\ell$:

– Le premier cas $C\ell_T^S(K_\infty) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\lambda_T^S}$ se produit lorsque l'ensemble T ne contient pas la place ℓ ; les groupes $C\ell_T^S(K_n)$ sont alors finis, et les arguments de [8] donnent directement le résultat.

– Le second cas $C\ell_T^S(K_\infty) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\lambda_T^S} \oplus \mathbb{Z}_\ell$ a lieu lorsque T contient ℓ. Les hypothèses faites ($\rho_T^S = 0$) supposent ici que les corps K_n soient totalement réels, de sorte que les groupes $C\ell_T^S(K_n)$ s'écrivent, sous la conjecture de Leopoldt, comme sommes directes de leurs sous-modules de torsion respectifs

$Tor_T^S(K_n)$, et d'un $\mathbb{Z}_\ell$-module libre de rang 1, isomorphe à $Gal(K_\infty/K_n)$. Ce dernier module disparait, par passage à la limite projective, mais non par passage à la limite inductive, de sorte que $C\ell_T^S(K_\infty)$ est bien, comme annoncé, somme d'un $\mathbb{Z}_\ell$-module libre de rang 1, et du sous-groupe limite inductive des $Tor_T^S(K_n)$, qui est un $\mathbb{Z}_\ell$-module divisible de corang λ_T^S, par les mêmes arguments que plus haut.

Les groupes $Cap_T^S(K_n)$ mesurent ce qu'il est convenu d'appeler, depuis Hilbert, une capitulation ; en l'occurence la S-capitulation T-infinitésimale dans l'extension profinie K_∞/K_n. Avouons tout de suite qu'ils sont en général très mal connus, et que c'est là un des obstacles essentiels au calcul de l'invariant λ_T^S. La seule information directe que nous possédions sur eux provient de la suite exacte des classes ambiges de Chevalley, en fait de sa généralisation aux ℓ-groupes de S-classes T-infinitésimales (cf. [19], ch. 11, section 2), qui interprète la capitulation $Cap_T^S(K_n)$ comme un sous-groupe du premier groupe de cohomologie $H^1(\Gamma_n, E_T^S(K_\infty))$ construit sur les S-unités T-infinitésimales dans l'extension profinie K_∞/K_n. Faute de mieux, on est alors réduit à restreindre l'étude des invariants λ_T^S aux seuls cas où le groupe $H^1(\Gamma_n, E_T^S(K_\infty))$ est trivial pour des raisons évidentes.

- Lorsque l'ensemble T contient la place ℓ (auquel cas, les hypothèses faites impliquent que K_∞ soit totalement réel), l'exactitude de la conjecture faible de Leopoldt montre que les groupes $E_T^S(K_n)$ sont constants pour n assez grand(*), ce qui entraine évidemment $H^1(\Gamma_n, E_T^S(K_\infty)) = H^1(\Gamma_n, E_T^S(K_n)) = 1$; d'où $Cap_T^S(K_\infty) = 1$, comme attendu.

- Lorsque, en revanche, T ne contient pas ℓ, la cohomologie des groupes E_T^S n'est pas connue en général, ce qui oblige à faire des hypothèses restrictives sur le corps K_∞ ; en fait à se resteindre aux classes imaginaires :

<u>Définition 2</u>. Nous disons qu'une extension algébrique de $\mathbb{Q}$ admet une conjugaison complexe lorsque c'est une extension quadratique totalement imaginaire d'un corps totalement réel. Un corps surcirculaire à conjugaison complexe est donc une extension quadratique totalement imaginaire d'un corps surcirculaire totalement réel.

En présence d'une conjugaison complexe τ, il est naturel de dire qu'un module multiplicatif est réel lorsque τ opère trivialement dessus ; qu'il est imaginaire

(*) La conjecture faible de Leopoldt affirme que les groupes d'unités infinitésimales sont constants pour n assez grand dans une tour cyclotomique (cf. par exemple, [17]). L'extension de ce résultat pour S et T quelconques est sans malice.

lorsqu'elle opère par passage à l'inverse. Si le nombre premier ℓ est impair, tout $\mathbb{Z}_\ell$-module M s'écrit ainsi comme somme directe

$$M = M^+ \oplus M^- = M^{(1+\tau)/2} \oplus M^{(1-\tau)/2}$$

de ses composantes réelles et imaginaires. Cependant, si ℓ vaut 2, la même somme $M^+ + M^-$ peut n'être ni directe, ni totale. Cela n'interdit pas, bien sûr, de continuer à parler de composantes réelles ou imaginaires, mais requiert à l'occasion quelques précautions. C'est pourquoi nous supposerons dans ce qui suit que ℓ est impair, et nous réserverons pour plus tard le cas $\ell = 2$.

Cela dit, l'intérêt de se resteindre aux composantes imaginaires est que dans une tour cyclotomique de corps à conjugaison complexe, il n'est d'autres unités imaginaires que les racines de l'unité présentes dans la tour, lesquelles sont cohomologiquement triviales. Cela suffit à entraîner la nullité des groupes $H^1(\Gamma_n, E_T^S(K_\infty)^-)$ pour n assez grand, et donc celle de la composante imaginaire $\mathrm{Cap}_T^S(K_\infty)^-$ du sous-groupe de torsion de $\mathcal{C}_T^S(K_\infty)$.

Cette discussion peut donc, en fin de compte, se résumer comme suit :

<u>Proposition 3</u>. Supposons que ℓ soit impair, et que le corps surcirculaire K_∞ admette une conjugaison complexe.

(i) Si l'ensemble T contient la place ℓ, la composante réelle du groupe $\mathcal{C}_T^S(K_\infty)$ est, sous réserve de nullité de l'invariant mu, un $\mathbb{Z}_\ell$-module libre de dimension λ_T^{S+} :

$$\mathcal{C}_T^S(K_\infty)^+ \simeq \mathbb{Z}_\ell^{\lambda_T^{S+}} .$$

Lorsque, en outre, la conjecture de Leopoldt est vérifiée dans K_∞ (pour le nombre premier ℓ), la composante réelle du groupe $C\ell_T^S(K_\infty)$ est somme directe d'un exemplaire de $\mathbb{Z}_\ell$ et d'un $\mathbb{Z}_\ell$-module divisible de corang λ_T^{S+} :

$$C\ell_T^S(K_\infty)^+ \simeq \mathbb{Z}_\ell \oplus (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\lambda_T^{S+}} .$$

(ii) Si l'ensemble T ne contient pas la place ℓ, la composante imaginaire du groupe $\mathcal{C}_T^S(K_\infty)$ est, toujours sous réserve de nullité de l'invariant mu, un $\mathbb{Z}_\ell$-module libre de rang λ_T^{S-} :

$$\mathcal{C}_T^S(K_\infty)^- \simeq \mathbb{Z}_\ell^{\lambda_T^{S-}} .$$

Dans ce cas, la composante imaginaire du groupe $C\ell_T^S(K_\infty)$ est, elle, un $\mathbb{Z}_\ell$-module divisible de corang λ_T^{S-} :

$$C\ell_T^S(K_\infty)^- \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\lambda_T^{S-}} .$$

d. Correspondance entre les divers paramètres lambda :

Pour voir que les paramètres lambda correspondant aux divers choix de S et de T se ramènent tous à l'un quelconque d'entre eux par des formules standards, nous nous appuyerons sur les résultats de [19], qui montrent qu'il en est bien ainsi dans les trois cas fondamentaux évoqués plus haut :

(i) Le cas $S=\emptyset$, $T=\emptyset$ est celui considéré par Kida : le groupe $\mathcal{C}(K_\infty) = \mathcal{C}_\emptyset^\emptyset(K_\infty)$ s'identifie, en effet, au groupe de Galois de la ℓ-extension abélienne maximale non ramifiée de K_∞ ; et le groupe de classes associé $C\ell(K_\infty)=C\ell_\emptyset^\emptyset(K_\infty)$ n'est autre que le ℓ-groupe des classes de diviseurs, au sens ordinaire, du corps surcirculaire K_∞. Nous notons $\lambda=\lambda_\emptyset^\emptyset$ l'invariant lambda correspondant.

(ii) Le cas $S=\{\ell\}$, $T=\emptyset$ est celui considéré par Kuz'min : le groupe $\mathcal{C}^\ell(K_\infty)=\mathcal{C}_\emptyset^{\{\ell\}}(K_\infty)$ s'identifie au groupe de Galois de la ℓ-extension abélienne maximale non ramifiée et ℓ-décomposée de K_∞ ; et le groupe de classes associé $C\ell^\ell(K_\infty)=C\ell_\emptyset^{\{\ell\}}(K_\infty)$ n'est autre que le ℓ-groupe des ℓ-classes de diviseurs du corps surcirculaire K_∞. Nous notons $\lambda^\ell=\lambda_\emptyset^{\{\ell\}}$ l'invariant lambda correspondant.

(iii) Le cas $S=\emptyset$, $T=\{\ell\}$ est celui considéré par Wingberg : le groupe $\mathcal{C}_\ell(K_\infty)=\mathcal{C}_{\{\ell\}}^\emptyset(K_\infty)$ s'identifie au groupe de Galois de la ℓ-extension abélienne ℓ-ramifiée maximale de K_∞ ; et le groupe de classes associé $C\ell_\ell(K_\infty)=C\ell_{\{\ell\}}^\emptyset(K_\infty)$ est ce que nous appelons le ℓ-groupe des classes infinitésimales du corps surcirculaire K_∞. Nous notons $\lambda_\ell=\lambda_{\{\ell\}}^\emptyset$ l'invariant lambda correspondant.

La correspondance entre les divers paramètres lambda résulte d'arguments classiques de dualité qui font intervenir les groupes de racines d'ordre ℓ-primaire de l'unité. Le corps K_∞ étant supposé donné, nous serons donc amenés à raisonner dans l'extension cyclotomique $K'_\infty=K_\infty[\zeta_\ell]$, engendrée sur K_∞ par les racines ℓ-ièmes de l'unité. Les paramètres considérés seront donc ceux du corps K'_∞.

Du point de vue galoisien, la situation se présente donc comme suit :

- K_∞ est un corps surcirculaire à conjugaison complexe.
- K_∞^+ est son sous-corps réel maximal.
- K'_∞ est l'extension cyclotomique $K_\infty[\zeta_\ell]$.

Le groupe de Galois $\Delta=\mathrm{Gal}(K'_\infty/K_\infty^+)$ est donc un groupe abélien d'ordre d étranger à ℓ, et, plus précisément, d'exposant divisant $(\ell-1)$. Cette dernière condition implique que l'algèbre de groupe $\mathbb{Z}_\ell[\Delta]$ est une algèbre semi-locale, composée de d exemplaires de l'anneau $\mathbb{Z}_\ell$, indexés par les caractères ℓ-adiques irréductibles du groupe Δ. En particulier, les invariants attachés à K_∞ et à K_∞^+ s'interprètent comme ψ-parties des invariants attachés à K'_∞, pour un caractère ℓ-adique convenable ψ du groupe Δ. Par exemple, la composante réelle de K_∞ correspond au caractère unité 1 ; et la composante imaginaire, à l'unique caractère $\bar{1}$ de Δ, qui relève le caractère d'augmentation de $Gal(K_\infty/K_\infty^+)$.

Dans ce contexte, il est plus commode de regarder les invariants lambda, non plus comme des entiers, mais comme des caractères du groupe Δ :

<u>Convention</u>. Soient, comme plus haut, ℓ un nombre premier impair ; S et T deux ensembles finis disjoints de places de $\mathbb{Q}$; puis K_∞ un corps surcirculaire à conjugaison complexe, K_∞^+ son sous-corps réel maximal, K'_∞ l'extension cyclotomique $K_\infty[\zeta_\ell]$; et Δ le groupe de Galois de l'extension K'_∞/K_∞^+. Par λ_T^S nous entendons désormais le caractère ℓ-adique du groupe Δ construit sur les invariants lambda d'Iwasawa des φ-composantes du groupe $\mathcal{C}_T^S(K'_\infty)$; c'est-à-dire que pour chaque caractère ℓ-adique irréductible φ de Δ, l'invariant lambda habituel de la φ-composante du $\mathbb{Z}_\ell[\Delta]$-module $\mathcal{C}_T^S(K'_\infty)$ est donné par le produit scalaire $\langle\lambda_T^S, \varphi\rangle$.

Cela posé, convenons de dire qu'un caractère ℓ-adique irréductible de Δ est réel ou imaginaire suivant qu'il agit trivialement ou non sur la conjugaison complexe ; et écrivons :

$$\chi = \chi^+ + \chi^-$$

la décomposition d'un caractère ℓ-adique quelconque en ses composantes réelle et imaginaire. L'application

$$\varphi \longmapsto \varphi^* = \omega\varphi^{-1},$$

où φ^{-1} est le caractère conjugué de φ (défini par $\varphi^{-1}(\sigma) = \varphi(\sigma^{-1})$), et ω le caractère cyclotomique (i.e. le caractère de l'action de Δ sur les racines de l'unité) est une involution du groupe des caractères ℓ-adiques virtuels de Δ, qui échange caractères réels et imaginaires, connue, dans la tradition bisontine, sous le nom d'involution du miroir.

Avec ces notations, les résultats de dualité de [19] s'énoncent comme suit :

<u>Proposition 4</u>. Supposons que le corps K'_∞ satisfasse les conjectures de Leopoldt et de Gross. Alors les trois invariants λ, λ^ℓ, et λ_ℓ (associés respectivement au ℓ-groupes des classes au sens ordinaire $C\ell(K'_\infty)$, au ℓ-groupe des ℓ-classes $C\ell^\ell(K'_\infty)$, et au ℓ-groupe des classes infinitésimales $C\ell_\ell(K'_\infty)$), regardés comme caractères du groupe Δ, sont liés par les identités :

$$\lambda_\ell^* = \lambda + (\chi_\ell - 1)^+ \qquad \text{et} \qquad \lambda^\ell = \lambda - \chi_\ell^- ,$$

où $\chi_\ell = \sum_{p_\infty | \ell} \chi_{p_\infty}$ désigne la somme des induits à Δ des caractères unités des sous-groupes de décomposition dans K'_∞/K_∞^+ des places de K_∞^+ au-dessus de ℓ.

Plus précisément, nous avons ici :

<u>Théorème 1</u>. Soient S et T deux ensembles finis disjoints de places de $\mathbb{Q}$, ne contenant pas ℓ, puis $S^* = S \cup \{\ell\}$ et $T^* = T \cup \{\ell\}$. Avec les notations précédentes, et sous les conjectures de Leopoldt et de Gross, les paramètres lambda associés aux ℓ-groupes de S-classes T-infinitésimales du corps K'_∞, regardés comme caractères ℓ-adiques du groupe Δ, vérifient les identités :

$$\text{(i)}\ \lambda_T^{S-} = \lambda^- + \omega[(\sum_{p_\infty | T} \chi_{p_\infty} - 1)^+ \vee 0].$$

$$\text{(ii)}\ \lambda_T^{S^*-} = \lambda^{\ell -} + \omega(\sum_{p_\infty | T} \chi_{p_\infty} - 1)^+ = \lambda^- + \omega[(\sum_{p_\infty | T} \chi_{p_\infty} - 1)^+ \vee 0] - \sum_{p_\infty | \ell} \chi_{p_\infty}^- .$$

$$\text{(iii)}\ \lambda_{T^*}^{S+} = \lambda_\ell^+ + \omega \sum_{p_\infty | T} \chi_p^- = (\lambda^-)^* + \omega \sum_{p_\infty | T} \chi_p^- .$$

<u>Démonstration</u>. Nous avons supposé ici que ni S ni T ne contiennent ℓ. Il en résulte immédiatement que les places de S sont sans influence sur les paramètres lambda, puisque toute ℓ-extension de corps surcirculaires, non ramifiée au-dessus de S, est nécessairement S-décomposée. Reste à déterminer l'influence des places de T, c'est-à-dire la nature, dans chacun des trois groupes de Galois $\mathcal{C}_T^S(K'_\infty)$, $\mathcal{C}_T^{S^*}(K'_\infty)$, et $\mathcal{C}_{T^*}^S(K_\infty)$, du sous-module engendré par les groupes d'inertie attachés aux places de T. Nous nous appuyerons pour cela sur la théorie du corps de classes : pour chaque place p'_∞ de K'_∞ au-dessus de T, et tout n assez grand, le ℓ-groupe des unités principales de l'unique sous-corps K'_n de K'_∞ de degré ℓ^n sur $K' = K[\zeta_\ell]$ s'identifie au ℓ-sous-groupe de Sylow μ'_n du groupe des racines de l'unité du corps K'_n. La limite projective $U_{p'_\infty}$ de ces groupes est donc un $\mathbb{Z}_\ell$-module libre de rang 1, isomorphe au module de Tate

$$\mathbb{T}_\ell = \varprojlim \mu'_n$$

Maintenant, le groupe de Galois Δ permute transitivement les places de K'_∞ au-dessus d'une même place p_∞ de K^+_∞, et opère sur $\mathbb{T}_\ell$ par le caractère cyclotomique ω. Le produit :

$$U_{p_\infty} = \prod_{p'_\infty | p_\infty} U_{p'_\infty}$$

est donc un $\mathbb{Z}_\ell[\Delta]$-module projectif qui a pour caractère le translaté par ω de l'induit à Δ du caractère de la représentation unité du sous-groupe de décomposition de la place p_∞ dans l'extension abélienne K'_∞/K^+_∞ ; c'est encore le reflet $\chi^*_{p_\infty} = \omega\chi^{-1}_{p_\infty} = \omega\chi_{p_\infty}$ du caractère χ_{p_∞}.

Cela acquis, examinons successivement les trois cas fondamentaux.

(i) Le sous-module de $\mathcal{C}^S_T(K'_\infty)$ engendré par les sous-groupes d'inertie associés aux places au-dessus de T est le quotient du produit $U_T = \prod_{p_\infty | T} U_{p_\infty}$ par l'image de la limite projective des groupes d'unités des corps K'_n. Restreints à leur seule composante imaginaire, ces groupes se réduisent aux sous-groupes μ'_n, et leur limite projective n'est autre que le module de Tate $\mathbb{T}_\ell$. Le caractère cherché est donc la différence :

$$(\omega \sum_{p_\infty | T} \chi_{p_\infty})^- - \omega = \omega(\sum_{p_\infty | T} \chi^+_{p_\infty} - 1),$$

sous réserve, naturellement, de non-nullité du terme de gauche. Le cas opposé, $\sum_{p_\infty | T} \chi^+_{p_\infty} = 0$, ne se produit que lorsque T est vide. Le groupe U_{p_∞} est alors trivial, et le caractère cherché est le caractère nul, que nous pouvons encore écrire

$$\omega(\sum_{p_\infty | T} \chi^+_{p_\infty} - 1) \vee 0,$$

en convenant de désigner par $\alpha \vee \beta$ le plus petit caractère virtuel contenant à la fois α et β.

(ii) Le cas de $\mathcal{C}^{S^*}_T(K'_\infty)$ se traite de la même façon, à ceci près qu'il convient de remplacer les unités par les ℓ-unités. Mais comme, sous la conjecture de Gross, la composante imaginaire de la limite projective des groupes de ℓ-unités des corps K_n est la même que pour les unités (cf. [19], ch. IV, section 2), le caractère cherché est le même que plus haut.

(iii) Enfin, dans le cas de $\mathcal{C}^S_{T^*}(K'_\infty)$, ce sont les unités infinitésimales qui remplacent les unités. Sous la conjecture de Leopoldt, le sous-module cherché s'identifie donc au produit direct $U_T = \prod_{p_\infty | T} U_{p_\infty}$, dont la composante réelle a pour caractère le produit

$$(\omega \sum_{p_\infty | T} \chi_{p_\infty})^+ = \omega \sum_{p_\infty | T} \chi^-_{p_\infty} .$$

Compte tenu de la proposition 4, cela achève la démonstration.

<u>Remarque</u>. Le théorème 1 ci-dessus ne décrit que la moitié des relations entre les divers paramètres lambda. Il est clair cependant que l'identité (iii) vaut trivialement pour les composantes réelles, ce qui s'écrit :

$$(\lambda^S_{T^*}{}^-)^* = \lambda^+ + \sum_{p_\infty | T} \chi^+_p .$$

En revanche, la version réelle des identités (i) et (ii) n'a rien d'évident. C'est sans importance ici, compte tenu des restrictions énoncées dans la proposition 3.

2. <u>La formule des genres dans une ℓ-extension de corps surcirculaires</u> :

a. <u>Position du problème</u> :

Nous avons vu dans la section 1 que le choix de deux ensembles finis S et T de places de $\mathbb{Q}$ permet d'attacher à chaque corps surcirculaire à conjugaison complexe L_∞ un $\mathbb{Z}_\ell$-module libre, disons X_{L_∞}, de dimension finie x_{L_∞}, et un $\mathbb{Z}_\ell$-module divisible X'_{L_∞} de même codimension(*), à savoir respectivement la composante réelle ou imaginaire du groupe de Galois $\mathcal{C}^S_T(L_\infty)$ de la ℓ-extension abélienne maximale T-ramifiée et S-décomposée du corps L_∞, et celle du sous-module de $\mathbb{Z}_\ell$-torsion du ℓ-groupe $C\ell^S_T(L_\infty)$ des S-classes T-infinitésimales du corps L_∞.

Ces deux groupes sont canoniquement des modules galoisiens, c'est-à-dire que si L_∞ est une ℓ-extension galoisienne d'un sous-corps surcirculaire à conjugaison complexe K_∞, le groupe de Galois $G = \mathrm{Gal}(L_\infty/K_\infty)$ opère de façon naturelle sur X_{L_∞} comme sur X'_{L_∞}. Nous nous proposons de déterminer le caractère de cette opération. Nous allons voir qu'il suffit pour cela de le calculer dans un cas très particulier :

L'argument essentiel est ici l'existence de deux morphismes naturels entre les groupes X_{L_∞} et X_{K_∞} d'une part, X'_{L_∞} et X'_{K_∞} d'autre part. Le premier, j_{L_∞/K_∞} (respectivement j'_{L_∞/K_∞}) est induit par l'extension des diviseurs ; il correspond au transfert en termes galoisiens. Le second N_{L_∞/K_∞} (respective-

(*) La codimension d'un $\mathbb{Z}_\ell$-module divisible est la dimension sur $\mathbb{Z}_\ell$ de son dual de Pontrjagin.

ment $\mathcal{N}'_{L_\infty/K'_\infty}$) provient de la norme arithmétique ; il correspond à la restriction des groupes de Galois. L'identité entre opérateurs

$$\mathcal{N}_{L_\infty/K_\infty} \circ j_{L_\infty/K_\infty} = [L_\infty : K_\infty] \quad (\text{resp. } \mathcal{N}'_{L_\infty/K_\infty} \circ j'_{L_\infty/K_\infty} = [L_\infty : K_\infty])$$

montre que j_{L_∞/K_∞} (resp. j'_{L_∞/K_∞}) est un pseudo-isomorphisme de X_{K_∞} dans $X^G_{L_\infty}$ (resp. de X'_{K_∞} dans $X'^G_{L_\infty}$). Les identités qui s'ensuivent

$$\dim_{\mathbb{Z}_\ell} X^G_{L_\infty} = \dim_{\mathbb{Z}_\ell} X_{K_\infty} \quad \text{et} \quad \operatorname{codim}_{\mathbb{Z}_\ell} X'^G_{L_\infty} = \operatorname{codim}_{\mathbb{Z}_\ell} X'_{K_\infty}$$

vont nous permettre de dévisser la structure de X et de X'.

Distinguons trois étapes :

<u>1ère étape</u> : réduction au cas cyclique.

Pour établir que deux représentations galoisiennes sont isomorphes, il suffit de vérifier qu'elles ont le même caractère. Or l'égalité de deux caractères se teste sur les éléments du groupe de Galois. Et la valeur d'un caractère sur un élément est donnée par celle de la restriction de ce caractère au sous-groupe cyclique engendré par cet élément. Nous ne restreignons pas la généralité de la démonstration, si nous supposons que G est un ℓ-groupe cyclique.

<u>2ème étape</u> : réduction au calcul du rang.

Si $G = G_m$ est cyclique d'ordre ℓ^m, la décomposition de l'algèbre de groupe $\mathbb{Q}_\ell[G]$ s'écrit :

$$\mathbb{Q}_\ell[G] \simeq \bigoplus_{i=0}^{m} \mathbb{Q}_\ell[\zeta_{\ell^i}]$$

et celle du caractère régulier $\chi_{\text{rég}}$:

$$\chi_{\text{rég}} = \sum_{i=0}^{m} \psi_i, \quad \text{avec} \quad \begin{cases} \psi_o = 1, \text{ et} \\ \deg \psi_i = (\ell-1)\ell^{i-1}, \text{ pour } i = 1, \dots, m. \end{cases}$$

En particulier, tout caractère ℓ-adique χ du groupe G est alors de la forme

$$\chi = \sum_{i=0}^{m} n_i \psi_i, \quad \text{avec } (n_o, n_1, \dots, n_m) \in \mathbb{N}^{m-1} ;$$

c'est-à-dire qu'il est entièrement déterminé par la donnée des $(m+1)$ entiers $n_o, n_1, \dots, n_m$.

Cela étant, si M est un $\mathbb{Q}_\ell[G]$-module noethérien, et $M_o, \dots, M_m$ sont les sous-modules fixés par les $(m+1)$ sous-groupes G_i de G d'ordres respectifs ℓ^i, les relations

$$\dim_{\mathbb{Q}_\ell} M_k = \sum_{i=0}^{k} n_i \deg \psi_i$$

montrent que la détermination du caractère de M et le calcul des dimensions des M_i sont un seul et même problème.

3ème étape : réduction au cas cyclique élémentaire.
Ce point acquis, il est clair maintenant qu'il nous suffit de donner une démonstration dans le seul cas où le groupe G est cyclique d'ordre premier. En effet, tout ℓ-groupe étant résoluble, une ℓ-extension galoisienne quelconque de corps de nombres s'obtient toujours par empilement d'un nombre fini de ℓ-extensions cycliques élémentaires. Si donc nous venons à disposer d'une formule pour les rangs dans le cas cyclique de degré premier, nous tiendrons de ce fait une formule de rang valable dans toute ℓ-extension galoisienne, et donc, en fin de compte, une identité sur les caractères dans une telle extension.

Conclusion : schéma de démonstration.
Dans tout ce qui suit, nous supposerons que G est un ℓ-groupe cyclique de degré premier (impair), et nous raisonnerons directement sur les caractères des modules considérés. D'après ce qui précède, les formules que nous obtiendrons, démontrées dans ce cas particulier, vaudront en fait pour un ℓ-groupe quelconque. Les équations aux dimensions s'obtiendront simplement en prenant les degrés des caractères.

b. Etude algébrique du cas cyclique de degré premier :

Supposons donc le groupe G cyclique d'ordre ℓ ; notons $\chi_{\text{rég}}$ le caractère de la représentation régulière de G, et $\chi_{\text{aug}} = \chi_{\text{rég}} - 1$ celui de la représentation d'augmentation.
Distinguons deux cas, suivant que le $\mathbb{Z}_\ell[G]$-module étudié est libre ou bien divisible sur $\mathbb{Z}_\ell$.

1er cas : modules libres
Si χ est de type fini et sans $\mathbb{Z}_\ell$-torsion, sa description comme somme directe de $\mathbb{Z}_\ell[G]$-modules indécomposables est de la forme :

$$\chi \simeq \mathbb{Z}_\ell[G]^\alpha \oplus \mathbb{Z}_\ell[\zeta_\ell]^\beta \oplus \mathbb{Z}_\ell^\gamma ,$$

avec α, β, et γ dans $\mathbb{N}$. Le caractère qui lui correspond est donc :

$$\chi = \alpha\chi_{\text{rég}} + \beta\chi_{\text{aug}} + \gamma 1 = (\alpha+\gamma)\chi_{\text{rég}} - (\gamma-\beta)\chi_{\text{aug}}$$

de sorte que le rang de χ est donné par la formule :

$$X = \ell(\alpha+\gamma) - (\ell-1)(\gamma-\beta).$$

Dans l'identité obtenue, les indices $(\alpha+\gamma)$ et $(\gamma-\beta)$ ont une interprétation simple :

- Le premier $(\alpha+\gamma)$ est la dimension sur $\mathbb{Z}_\ell$ du module des points fixes de X :

$$\alpha+\gamma = \dim_{\mathbb{Z}_\ell} X^G$$

- Le second $(\gamma-\beta)$ n'est autre que le quotient de Herbrand dimensionnel du module X :

$$\gamma-\beta = h^2(X)-h^1(X) = q(X) \text{ , avec}$$

$$\gamma = h^2(X) = \dim_{\mathbb{F}_\ell} H^2(G,X) \quad \text{et} \quad \beta = h^1(X) = \dim_{\mathbb{F}_\ell} H^1(G,X).$$

Dans ce cas, nous obtenons donc :

Lemme 2. Si G est un groupe cyclique d'ordre ℓ, le caractère d'un $\mathbb{Z}_\ell[G]$-module noethérien et sans $\mathbb{Z}_\ell$-torsion est donné par la formule :

$$\chi = \dim X^G \cdot \chi_{\text{rég}} - q(X)\chi_{\text{aug}},$$

où $q(X)$ représente le quotient de Herbrand dimensionnel de X. En particulier, la dimension de X sur $\mathbb{Z}_\ell$ est ainsi :

$$x = \ell \dim X^G - (\ell-1)q(X).$$

2ème cas : modules divisibles

Si X' est de cotype fini et $\mathbb{Z}_\ell$-divisible, sa description comme somme directe de $\mathbb{Z}_\ell[G]$-modules indécomposables est de la forme :

$$X' \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)\otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell[G]^{\alpha'} \oplus [\mathbb{Q}_\ell[\zeta_\ell]/\mathbb{Z}_\ell[\zeta_\ell]]^{\beta'} \oplus (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\gamma'}$$

avec α', β', et γ' dans $\mathbb{N}$. Le caractère qui lui correspond est donc :

$$\chi' = \alpha'\chi_{\text{rég}} + \beta'\chi_{\text{aug}} + \gamma\ 1 = (\alpha'+\gamma')\chi_{\text{rég}} + (\beta'-\gamma')\chi_{\text{aug}},$$

de sorte que le corang de X' est donné par la formule :

$$x' = \ell(\alpha'+\gamma') + (\ell-1)\ (\beta'-\gamma').$$

Comme plus haut, les indices $(\alpha'+\gamma')$ et $(\beta'-\gamma')$ ont une interprétation simple.

- Le premier $(\alpha'+\gamma')$ est la codimension du sous-module des points fixes de X' :

$$\alpha'+\gamma' = \operatorname{codim}_{\mathbb{Z}_\ell} X'$$

- Le second $(\beta'-\gamma')$ n'est autre que le quotient de Herbrand dimensionnel du module X' :

$$\beta'-\gamma' = h^2(X')-h^1(X') = q(X'), \text{ avec}$$

$$\beta' = h^2(X') = \dim_{\mathbb{F}_\ell} H^2(G,X') \quad \text{et} \quad \gamma' = h^1(X') = \dim_{\mathbb{F}_\ell} H^1(G,X').$$

Dans ce cas, nous obtenons donc :

Lemme 3. Le groupe G étant cyclique d'ordre ℓ, le caractère d'un $\mathbb{Z}_\ell[G]$-module X' de cotype fini et $\mathbb{Z}_\ell$-divisible est donné par la formule :

$$\chi' = \dim X'^G . \chi_{rég} + q(X')\chi_{aug} ,$$

où $q(X')$ représente le quotient de Herbrand dimensionnel de X'. En particulier, la codimension de X' sur $\mathbb{Z}_\ell$ est ainsi :

$$x' = \ell . \operatorname{codim}_{\mathbb{Z}_\ell} X'^G + (\ell-1)\, q(X').$$

Nota. Dans les applications arithmétiques, nous aurons toujours $x = x'$, d'où $-q(X) = q(X')$, et finalement $\chi = \chi'$, de sorte que nous pourrons raisonner indifféremment sur X ou sur X'. Cela ne veut pas dire, en revanche, que nous aurons systématiquement $\beta = \beta'$ et $\gamma = \gamma'$, le groupe X n'étant pas, en général, isomorphe au dual de Pontrjagin de X' en tant que module galoisien ; l'égalité des caractères signifie seulement que cet isomorphisme a lieu après extension des scalaires à $\mathbb{Q}_\ell$.

Enoncé des résultats.

Dans la section précédente, nous avons convenu de regarder les paramètres λ_T^S associés aux groupes $\mathcal{C}_T^S$ ou $\mathcal{C}\ell_T^S$ attachés à un corps surcirculaire à conjugaison complexe non plus comme des entiers, mais comme des caractères ℓ-adiques d'un groupe abélien Δ d'exposant divisant $(\ell-1)$.

Pour reformuler dans le même contexte les lemmes 2 et 3, nous allons considérer la situation suivante :

- K_∞ est un corps surcirculaire à conjugaison complexe ; K_∞^+ son sous-corps réel maximal ; et $K_\infty' = K_\infty[\zeta_\ell]$ l'extension cyclotomique engendrée sur K_∞ par les racines ℓ-ièmes de l'unité.

- L_∞ est une ℓ-extension galoisienne de K_∞, qui provient par composition d'une ℓ-extension galoisienne totalement réelle L_∞^+ de K_∞^+ ; et L_∞' est l'extension cyclotomique $L_\infty[\zeta_\ell]$.

- G est le groupe de Galois de l'extension L_∞'/K_∞', identifié à $\mathrm{Gal}(L_\infty^+/K_\infty^+)$; et Δ est le groupe abélien $\mathrm{Gal}(L_\infty'/L_\infty^+) \simeq \mathrm{Gal}(K_\infty'/K_\infty^+)$.

- Les objets étudiés sont équipés d'une action naturelle de G et de Δ, c'est-à-dire que ce sont des $\mathbb{Z}_\ell[\Delta \times G]$-modules.

Cela posé, par application des arguments précédents à chaque composante Δ-isotypique de X et de X', nous obtenons immédiatement :

<u>Proposition 5</u>. Supposons que le groupe G soit cyclique d'ordre ℓ ; et soient comme plus haut, $\chi_{\text{rég}}$ le caractère de la représentation régulière de G, et $\chi_{\text{aug}}=\chi_{\text{rég}}-1$ celui de la représentation d'augmentation.

(i) Si X est un $\mathbb{Z}_\ell[\Delta\times G]$-module, de type fini et libre sur $\mathbb{Z}_\ell$, son caractère χ est donné par la formule :

$$\chi = \operatorname{car}_\Delta X^G.\chi_{\text{rég}} - q_\Delta(G,X).\chi_{\text{aug}},$$

où $\operatorname{car}_\Delta X^G$ est le caractère de X^G regardé comme $\mathbb{Z}_\ell[\Delta]$-module, et $q_\Delta(G,X)$ le Δ-quotient de Herbrand du G-module X, i.e. l'unique caractère virtuel du groupe Δ à valeurs dans $\mathbb{Z}_\ell$, qui relève la différence $h^1_\Delta(G,X)-h^2_\Delta(G,X)$ des caractères respectifs des $\mathbb{F}_\ell[\Delta]$-modules $H^1(G,X)$ et $H^2(G,X)$.

(ii) Si X' est un $\mathbb{Z}_\ell[\Delta\times G]$-module, de cotype fini et divisible sur $\mathbb{Z}_\ell$, son caractère χ' est donné par la formule :

$$\chi' = \operatorname{car}_\Delta X'^G.\chi_{\text{rég}} + q_\Delta(G,X').\chi_{\text{aug}},$$

où $\operatorname{car}_\Delta X'^G$ et $q_\Delta(G,X')$ sont définis comme plus haut.

c. <u>Etude arithmétique du cas cyclique de degré premier impair</u> :

Nous supposons désormais que ℓ est impair et que L_∞/K_∞ est une ℓ-extension cyclique élémentaire de corps surcirculaires à conjugaison complexe ; nous notons L'_∞/K'_∞ l'extension obtenue par adjonction des racines ℓ-ièmes de l'unité, et L^+_∞/K^+_∞ la sous-extension réelle maximale de L_∞/K_∞. Comme plus haut, Δ désigne le groupe abélien $\mathrm{Gal}(L'_\infty/L^+_\infty)\simeq\mathrm{Gal}(K'_\infty/K^+_\infty)$, et G le groupe cyclique $\mathrm{Gal}(L'_\infty/K'_\infty)\simeq\mathrm{Gal}(L_\infty/K_\infty)\simeq\mathrm{Gal}(L^+_\infty/K^+_\infty)$.

Le $\mathbb{Z}_\ell$-module libre considéré est (sous réserve de nullité de l'invariant μ) la composante imaginaire $X_{\ell'_\infty}=\mathcal{C}^-_{L'_\infty}$ du groupe de Galois de la ℓ-extension abélienne non ramifiée maximale de L'_∞ ; le $\mathbb{Z}_\ell$-module divisible qui lui correspond est la composante imaginaire $X'_{L'_\infty}=C\ell^-_{L'_\infty}$ du ℓ-groupe des classes de diviseur (au sens ordinaire) du corps surcirculaire L'_∞.

Comme plus haut, nous notons $\chi_{L'_\infty}$ le caractère de $X_{L'_\infty}$, et $\chi'_{L'_\infty}$ celui de $X'_{L'_\infty}$, l'un et l'autre regardés comme $\mathbb{Z}_\ell[\Delta\times G]$-modules. Nous réservons la notation $\lambda_{L'_\infty}$ pour désigner indifféremment le caractère de $X_{L'_\infty}$ régardé comme $\mathbb{Z}_\ell[\Delta]$-module, ou celui de $X'_{L'_\infty}$. L'invariant lambda traditionnel d'Iwasawa n'est autre que le degré de $\lambda_{L'_\infty}$; c'est aussi le degré commun de $\chi_{L'_\infty}$ et de $\chi'_{L'_\infty}$.

Cela posé, la proposition 5 nous dit que pour être en mesure d'exprimer $\chi_{L'_\infty}$ et $\chi'_{L'_\infty}$ à partir de $\chi_{K_\infty} = \chi'_{K'_\infty}$, il suffit de déterminer l'action de Δ sur les groupes de cohomologie $H^1(G, \mathcal{C}^-_{L'_\infty})$ et $H^2(G, \mathcal{C}^-_{L'_\infty})$, d'une part ; $H^1(G, C\ell^-_{L'_\infty})$ et $H^2(G, C\ell^-_{L'_\infty})$, d'autre part.

<u>1er cas : cohomologie des groupes de classes</u>

<u>Lemme 4</u>. Soient L_∞/K_∞ une ℓ-extension cyclique élémentaire de corps surcirculaires, et G son groupe de Galois. Alors :

(i) Le groupe multiplicatif $L^\times_\infty$ est cohomologiquement trivial ; autrement dit :

$$H^1(G, L^\times_\infty) = 1 \quad \text{et} \quad H^2(G, L^\times_\infty) = 1.$$

(ii) La cohomologie du groupe des diviseurs principaux P_{L_∞} est duale de celle du groupe des unités E_{L_∞} ; ce qui s'écrit :

$$H^1(G, P_{L_\infty}) \simeq H^2(G, E_{L_\infty}) \quad \text{et} \quad H^2(G, P_{L_\infty}) \simeq H^1(G, E_{L_\infty}).$$

(iii) La cohomologie du groupe des diviseurs D_{L_∞} est donnée par les formules :

$$H^1(G, D_{L_\infty}) = 1 \quad \text{et} \quad H^2(G, D_{L_\infty}) \simeq \mathrm{Ram}'_{L_\infty/K_\infty}.$$

Dans celle-ci, le groupe $\mathrm{Ram}'_{L_\infty/K_\infty}$, qui mesure la ramification en dehors de ℓ dans l'extension L_∞/K_∞ est la somme directe :

$$\mathrm{Ram}'_{L_\infty/K_\infty} \simeq \bigoplus_{\mathfrak{p} \nmid \ell} \mathbb{Z}/e_{\mathfrak{p}}\mathbb{Z},$$

où $\mathfrak{p}$ parcourt les places de K_∞, étrangères à ℓ, qui se ramifient dans L_∞/K_∞, et $e_{\mathfrak{p}}$ désigne l'indice de ramification correspondant (ici ℓ).

Démonstration. La trivialité des premiers groupes de cohomologie $H^1(G, L^\times_\infty)$ et $H^1(G, D_{L_\infty})$ est bien connue, du moins pour les corps de nombres, indépendamment de toute hypothèse sur le groupe fini G ; c'est ce qu'il est convenu d'appeler le théorème 90 de Hilbert (*). Son extension aux corps surcirculaires

(*) Bien entendu, dans son traité de 1913, Hilbert n'énoncait pas son résultat sous forme cohomologique, mais seulement dans le cas cyclique : D. Hilbert.- Traité des corps de nombres algébriques.- Ann. Fac. Toulouse (1909/10) ; Hermann, Paris (1913).

ne pose pas de difficulté : il suffit d'écrire L_∞/K_∞ comme limite inductive de sous-extensions relativement cycliques L_n/K_n, de degré fini sur $\mathbb{Q}$, et d'appliquer à ces extensions le théorème de Hilbert. Le cas des groupes $H^2(G, L_\infty^\times)$ et $H^2(G, D_{L_\infty})$ est, en revanche, plus surprenant, puisque, pour les corps de nombres, aucun de ces deux groupes n'est fini. Cela dit, examinons successivement les diverses assertions du lemme :

(i) L'identité $H^2(G, L_\infty^\times) = 1$ est signalée par Iwasawa (cf. [14], lemme 5), et vaut en fait pour tout ℓ-groupe G. Lorsque G est cyclique, elle signifie simplement que les éléments de $K_\infty^\times$ sont normes d'éléments de $L_\infty^\times$ (cf. [2], lemme 3) :

$$K_\infty^\times = N_{L_\infty/K_\infty}(L_\infty^\times).$$

Dans ce cas, d'après le principe de Hasse, il suffit pour l'établir de vérifier que tout élément de $K_\infty^\times$ est norme locale partout dans l'extension L_∞/K_∞. Ecrivons donc, pour ce faire, $L_\infty = \bigcup_{n\in\mathbb{N}} L_n$, et $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ comme réunion croissante de corps de nombres, avec L_n cyclique sur K_n de groupe G, et $[L_{n+1} : L_n] = [K_{n+1} : K_n] = \ell$. Puis, étant donnés x un élément de $K_\infty^\times$ et $\mathfrak{p}_\infty$ une place de K_∞, fixons n assez grand pour avoir $x \in K_n^\times$ et $\mathfrak{p}_\infty$ non décomposée dans K_∞/K_n. Formons alors les symboles de Hasse attachés aux places au-dessous de $\mathfrak{p}_\infty$; nous obtenons :

$$\left(\frac{x, L_{n+1}/K_{n+1}}{\mathfrak{p}_{n+1}}\right) = \left(\frac{N_{n+1/n}(x), L_n/K_n}{\mathfrak{p}_n}\right) = \left(\frac{x^\ell, L_n/K_n}{\mathfrak{p}_n}\right) = \left(\frac{x, L_n/K_n}{\mathfrak{p}_n}\right)^\ell = 1$$

ce qui prouve que x est norme locale en $\mathfrak{p}_{n+1}$ dans L_{n+1}/K_{n+1}, donc norme locale en $\mathfrak{p}_\infty$ dans L_∞/K_∞.

(ii) Le fait que les groupes d'unités E_{L_∞} et de diviseurs principaux P_{L_∞} soient en dualité cohomologique résulte immédiatement du résultat précédent. En effet, la suite exacte courte qui définit P_{L_∞}

$$1 \longrightarrow E_{L_\infty} \longrightarrow L_\infty^\times \longrightarrow P_{L_\infty} \longrightarrow 1$$

conduit à l'hexagone exact :