CHAPITRE II

INDÉPENDANCE ℓ-ADIQUE DE NOMBRES ALGÉBRIQUES

CALCUL INFINITÉSIMAL DANS UN CORPS DE NOMBRES ALGÉBRIQUES

SOMMAIRE

1.- INDÉPENDANCE ℓ-ADIQUE DE NOMBRES ALGÉBRIQUES.

2.- CALCUL INFINITÉSIMAL DANS UN CORPS DE NOMBRES ALGÉBRIQUES.

INDÉPENDANCE ℓ-ADIQUE DE NOMBRES ALGÉBRIQUES

Le problème de l'indépendance ℓ-adique de nombres algébriques s'est posé historiquement à l'occasion d'un calcul analytique : On sait depuis longtemps que la fonction zêta complexe d'un corps de nombres se prolonge en une fonction méromorphe sur le plan complexe avec un unique pôle , simple , au point 1 , et que l'expression du résidu en ce point fait intervenir le produit du nombre de classes de ce corps par le régulateur complexe du groupe de ses unités . De façon tout à fait semblable , on sait aujourd'hui que la fonction zêta ℓ-adique , qui est méromorphe sur le disque unité fermé du corps $\mathbb{C}_\ell$, admet un unique pôle éventuel au point 1 , avec pour résidu , outre un certain nombre de facteurs canoniques , le produit du nombre de classes par le régulateur ℓ-adique des unités , la non nullité de ce régulateur étant la condition de la présence effective du pôle (cf. [Se_2]) .

En fait, c'est en 1962 que Leopoldt, dans son étude sur l'arithmétique des corps abéliens (cf. [Le_2]) , introduit le régulateur ℓ-adique des unités , et suggéra sa fameuse conjecture sur l'égalité du rang ℓ-adique des unités et du nombre de Dirichlet $r_K + c_K - 1$. En 1965 , Ax (cf. [Ax]) , s'appuyant sur un analogue ℓ-adique dû à Mahler du théorème de Guel'fond-Schneider (*) , démontra cette conjecture dans un certain nombre de cas particuliers ; mais c'est Brumer , en 1967 , en généralisant au cadre ℓ-adique le récent résultat de Baker sur l'indépendance ℓ-adique de nombres algébriques (cf. [Br]) , qui établit finalement le résultat pour tous les corps abéliens . Dans les autres cas , cependant , la conjecture n'a guère avancé depuis : les méthodes algébriques , illustrées au Chapitre IV (cf. Ch.IV.2 , 3 § b) , donnent des résultats précis , mais qui ne permettent de conclure que pour des corps particuliers ; les méthodes transcendantes donnent seulement

(*) Il s'agit de la version ℓ-adique du septième problème de Hilbert .

des minorations du rang ℓ-adique : le résultat actuellement le plus fin , dû à Waldschmidt (cf. [Wa]) , et sur lequel nous reviendrons plus loin , permet ainsi d'affirmer que le rang ℓ-adique des unités est du moins la moitié du nombre de Dirichlet (*) . De ce fait , une démonstration de la conjecture de Schanuel ℓ-adique résoudrait complètement le problème .

D'un autre côté , la conjecture de Leopoldt sur la non nullité du régulateur ℓ-adique des unités et les relations attendues entre ce régulateur et le résidu au point 1 de la fonction zêta ℓ-adique ont été généralisées par Serre aux fonctions L d'Artin ℓ-adiques attachées à certaines représentations galoisiennes . Etudiant le comportement de ces mêmes fonctions au voisinage de 0 , Gross énonça une conjecture analogue à celle de Leopoldt (**) , mais faisant intervenir cette fois le régulateur ℓ-adique construit sur les ℓ-unités imaginaires d'un corps à conjugaison complexe, conjecture qu'il démontra dans le cas abélien , à l'aide du théorème de Baker - Brumer .

Le parallèle extrêmement intéressant entre ces deux conjec - tures appelle plusieurs commentaires : D'abord la différence, soulignée par plusieurs auteurs (***) , entre les régulateurs qui leur corres - pondent , est en grande partie factice : Leopoldt a introduit sa conjec - ture pour un corps totalement réel ; Gross pour un corps à conjugaison complexe (i.e. pour une extension quadratique totalement imaginaire d'un corps totalement réel) ; dans les deux cas , pour un type de corps dans lequel le comportement des places à l'infini est très particulier . En l'absence de conditions du même ordre sur les places au-dessus de ℓ , il n'y a pas lieu de s'étonner si réapparait dans le résultat la dissymé- trie introduite dans les hypothèses. De fait, l'étude synoptique du cha- pitre IV (cf. Ch. IV.2 , 3 § c) fait apparaitre une parfaite dualité entre les interprétations arithmétiques de ces deux conjectures , et fournit un même critère algébrique de leur validité . Enfin , et c'est ce qui

---

(*) On a même une conclusion sensiblement plus précise (cf. th. 15) .

(**) Il s'agit de la " première conjecture " de Gross . La " seconde conjecture " concerne les relations entre le régulateur des ℓ-unités et le coefficient dominant du développement Taylorien de la fonction L d'Artin au voisinage de l'origine. Pour plus de détails sur les conjec - tures de Gross , on pourra consulter le livre de Koblitz [Ko] .

(***) Ainsi [Ko] , [Fe_1] , ... : les deux régulateurs n'ont pas la même dimension .

nous intéresse plus particulièrement ici, les arguments de transcendance invoqués pour justifier l'une ou l'autre de ces conjectures ne prennent jamais en compte la nature arithmétique des éléments algébriques manipulés.

C'est pourquoi nous avançons ici une conjecture générale, contenant celles dûes à Leopoldt et à Gross, qui décrit le comportement ℓ-adique de n'importe quel sous-module noethérien du groupe multiplicatif des éléments non nuls d'un corps de nombres algébriques. Plus précisément, nous postulons que le rang ℓ-adique d'un tel module se lit sur le caractère de la représentation galoisienne qui lui est associée.

Avant d'énoncer cette conjecture, traçons d'abord le cadre général du problème :

1.- POSITION DU PROBLÈME ET ÉNONCÉ DE LA CONJECTURE.

a.- Les deux complétions multiplicatives d'un corps de nombres.

Un corps de nombres K étant donné, il existe deux façons (au moins) de construire un $\mathbb{Z}_\ell$-module à partir de son groupe multiplicatif :

- La plus simple consiste à former directement le produit tensoriel $\mathcal{R} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$. Le groupe obtenu est un $\mathbb{Z}_\ell$-module qui n'est ni de type fini, ni même compact pour la topologie des sous-modules d'indice fini, mais cependant réunion dénombrable de sous-modules compacts : Si $(S_n)_{n \in \mathbb{N}}$ est une suite croissante de parties qui recouvre l'ensemble Pl_K des places non complexes de K, le groupe $\mathcal{R}$ est la réunion croissante, lorsque n décrit $\mathbb{N}$, de ses sous-modules noethériens $\mathcal{E}^S$, où $\mathcal{E}^S = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E^S$ désigne le tensorisé ℓ-adique du groupe des S unités de K (i.e. la fermeture de l'image de E^S dans $\mathcal{R}$).

- Une autre façon de procéder consiste à introduire d'abord le complété semi-local de K pour les places au-dessus de ℓ, et à considérer ensuite le groupe multiplicatif $K_\ell^\times = (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} K)^\times$ de l'algèbre obtenue. Comme K_ℓ est la somme directe des complétés de K pour les places au-dessus de ℓ, le groupe $K_\ell^\times$ est le produit des groupes multiplicatifs des corps locaux K_I :

$$K_\ell^\times = \bigoplus_{\mathfrak{l}|\ell} K_\mathfrak{l}^\times = \bigoplus_{\mathfrak{l}|\ell} [\mu_\mathfrak{l}^\circ \cdot U_\mathfrak{l} \cdot \pi_\mathfrak{l}^{\mathbb{Z}}] .$$

Sa décomposition directe fait donc intervenir les groupes $\mu_\mathfrak{l}^\circ$ de racines locales de l'unité d'ordre étranger à ℓ , les groupes locaux d'unités principales $U_\mathfrak{l} = (1 + \mathfrak{l})$, et autant de $\mathbb{Z}$-modules libres de rang 1 associés à une uniformisante locale $\pi_\mathfrak{l}$ qu'il y a dans K de places au-dessus de ℓ. Le sous-groupe $\mathcal{U}_\ell = \bigoplus_{\mathfrak{l}|\ell} U_\mathfrak{l}$ étant déjà un $\mathbb{Z}_\ell$-module , la manière la plus économique de fabriquer un $\mathbb{Z}_\ell$-module à partir de $K_\ell^\times$ est de former le complété profini :

$$\mathcal{K}_\ell^\times = \varprojlim_k K_\ell^{\times \ell^k} = \bigoplus_{\mathfrak{l}|\ell} \varprojlim_k K_\mathfrak{l}^\times / K_\mathfrak{l}^{\times \ell^k} = \bigoplus_{\mathfrak{l}|\ell} U_\mathfrak{l} \cdot \pi_\mathfrak{l}^{\mathbb{Z}_\ell} .$$

Le groupe $\mathcal{K}_\ell^\times$ ainsi construit , produit direct des complétés profinis $\mathcal{K}_\mathfrak{l}^\times$ des groupes multiplicatifs des corps locaux $K_\mathfrak{l}$ est un $\mathbb{Z}_\ell$-module compact , et même noethérien .

Cela posé , l'injection naturelle de $K^\times$ dans $K_\ell^\times$ (i.e. l'application diagonale de $K^\times$ dans le produit $\bigoplus_{\mathfrak{l}|\ell} K_\mathfrak{l}^\times$) se prolonge de façon unique en un morphisme continu du tensorisé $\mathcal{R} = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$ dans le complété profini $\mathcal{K}_\ell^\times = \varprojlim_k K_\ell^\times / K_\ell^{\times \ell}$. Nous allons voir que cet homomorphisme est surjectif .

<u>THÉORÈME & DÉFINITION II.1.1.</u>- Etant donné un corps de nombres K , l'application naturelle s du tensorisé ℓ-adique $\mathcal{R} = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$ du groupe multiplicatif de K dans le complété profini $\mathcal{K}_\ell^\times = \varprojlim_k K_\ell^\times / K_\ell^{\times \ell}$ du groupe des éléments inversibles de l'algèbre semi-locale $K_\ell = \mathbb{Z}_\ell \otimes_\mathbb{Z} K$, est un épimorphisme continu appelé application de semi-localisation .

Démonstration : La surjectivité de l'application s repose sur deux arguments :

- D'une part , chaque classe d'idéaux d'un corps de nombres contient un idéal étranger à un nombre fini de places données. En particulier chacun des idéaux premiers $\mathfrak{l}$ de K au-dessus de ℓ est associé à un idéal $\mathfrak{a}_\mathfrak{l}$ étranger à ℓ. Ecrivant $\mathfrak{l} = x_\mathfrak{l}\, \mathfrak{a}_\mathfrak{l}$, nous voyons qu'il est donc toujours possible de trouver dans $K^{\times}$ une famille d'éléments $(x_{\mathfrak{l}})_{\mathfrak{l}|\ell}$ vérifiant les conditions de valuation :

(i) $x_{\mathfrak{l}}$ est une uniformisante locale pour la place $\mathfrak{l}$ (i.e. $v_{\mathfrak{l}}(x_{\mathfrak{l}}) = 1$) ;

(ii) $x_{\mathfrak{l}}$ est une unité locale pour les places $\mathfrak{l}'|\mathfrak{l}$ autres que $\mathfrak{l}$ (i.e. $v_{\mathfrak{l}'}(x_{\mathfrak{l}}) = 0$) .

– D'autre part, le corps K est dense dans le produit $K_{\ell} = \bigoplus_{\mathfrak{l}|\ell} K_{\mathfrak{l}}$ de ses complétés pour les places au-dessus de ℓ . Si donc $(u_i)_{i=1,\dots,n}$ est une famille génératrice du $\mathbb{Z}_{\ell}$-module $\mathcal{U}_{\ell} = \bigoplus_{\mathfrak{l}|\ell} U_{\mathfrak{l}}$, et m un entier naturel , il est encore possible de résoudre dans $K^{\times}$ les n systèmes de congruences :

(iii) $s(y_i) \equiv u_i \pmod{\mathfrak{l}^m}$, $\forall\, \mathfrak{l}|\ell$.

Cela étant , si m est choisi plus grand que le module d'hyper-primarité des places au-dessus de ℓ $\left(\text{i.e. si le produit } \bigoplus_{\mathfrak{l}|\ell}(1+\mathfrak{l}^m) \text{ est contenu dans } \mathcal{U}_{\ell}^{\ell}\right)$, le lemme de Nakayama montre que les éléments $(s(x_i))_{\mathfrak{l}|\ell}$ et $(s(y_i))_{i=1,\dots,n}$ engendrent conjointement le $\mathbb{Z}_{\ell}$-module $\mathcal{K}_{\ell}^{\times}$, ce qui établit le théorème .

Il est bien clair , en revanche , que l'application de semi-localisation s n'est jamais injective (comme sa " restriction " à $K^{\times}$) , le groupe $\mathcal{K}_{\ell}^{\times}$ étant un $\mathbb{Z}_{\ell}$-module de type fini , mais non le tensorisé $\mathcal{R}$. Le premier problème de l'indépendance ℓ-adique est donc le suivant :

<u>Problème 1</u>.- Etant donnés $x_1,\dots,x_n$ dans $K^{\times}$, à quelle condition la restriction de s au sous-module $\mathbb{Z}_{\ell}$-engendré par les images de ces éléments dans $\mathcal{R}$ est-elle injective ?

Posée sous cette forme , la question n'est cependant pas totalement satisfaisante , le rôle dans $\mathcal{K}_{\ell}^{\times}$ des places au-dessus de ℓ étant par trop particulier : il est clair , par exemple, que les images $s(x_i)$, pour $i = 1,\dots,n$, d'un nombre fini d'uniformisantes locales associées à des places distinctes au-dessus du premier ℓ sont trivialement indépendantes ; mais ce résultat est en défaut pour tout autre premier $p \neq \ell$. Pour lisser la situation , il est naturel de faire appel au logarithme ℓ-adique : L'application Log_{ℓ} , qui est définie sur le sous-groupe principal $\mathcal{U}_{\ell}$ de $\mathcal{K}_{\ell}^{\times}$ par son développement en série entière :

$$\mathrm{Log}_\ell\, u = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{(u-1)^k}{k},$$

se prolonge de façon unique à $\mathcal{K}_\ell^\times$ grâce à son équation fonctionnelle

$$\mathrm{Log}_\ell\, xy = \mathrm{Log}_\ell\, x + \mathrm{Log}_\ell\, y,$$

si l'on convient de poser $\mathrm{Log}_\ell\, \ell_{\mathfrak{l}} = 0$, pour chaque place de $\mathfrak{l}$ de K au-dessus de ℓ, en désignant par $\ell_{\mathfrak{l}}$ l'image dans $\mathcal{K}_{\mathfrak{l}}^\times$ du nombre premier ℓ. Il vient alors :

<u>LEMME II.1.2.</u>- Le logarithme d'Iwasawa Log_ℓ est un morphisme continu du groupe multiplicatif $\mathcal{K}_\ell^\times$ dans le groupe additif $K_\ell = \bigoplus_{\mathfrak{l}|\ell} K_{\mathfrak{l}}$. Son image $\mathrm{Log}_\ell\, \mathcal{K}_\ell^\times$ est un $\mathbb{Z}_\ell$-réseau de K_ℓ. Son noyau est le radical dans $\mathcal{K}_\ell^\times$ du $\mathbb{Z}_\ell$-module libre engendré par les images $\ell_{\mathfrak{l}}$ du nombre premier ℓ dans chacun des facteurs locaux $\mathcal{K}_{\mathfrak{l}}^\times$; en particulier, il contient le groupe $\mu_\ell = \bigoplus_{\mathfrak{l}|\ell} \mu_{\mathfrak{l}}$ des racines de l'unité dans $\mathcal{K}_\ell^\times$.

<u>DÉFINITION II.1.3.</u>- Nous notons $\log_\ell$ et nous appelons logarithme ℓ-adique l'homomorphisme naturel $\mathrm{Log}_\ell \circ s$ du tensorisé multiplicatif $\mathcal{R} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$ dans le tensorisé additif $K_\ell = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K$ composé du logarithme d'Iwasawa et de l'application de semi-localisation.

Cela posé, le problème fondamental de l'indépendance ℓ-adique peut s'énoncer comme suit :

<u>Problème 2</u>.- Etant donnés $x_1, \dots, x_n$ dans $K^\times$, à quelle condition la restriction du logarithme ℓ-adique $\log_\ell$ au sous-module de $\mathcal{R}$ qui est $\mathbb{Z}_\ell$ engendré par les images de ces éléments est-elle injective ?

b.- <u>Enoncé de la conjecture</u>.

La notion-clé de cette conjecture étant celle de représentation monogène, commençons par énoncer les principaux résultats sur les représentations qui nous seront utiles :

Etant donnés un groupe fini G et un corps F de caractéristique nulle, écrivons :

$$F[G] = \bigoplus_{i=1}^{r} F[G]\, e_i = \bigoplus_{i=1}^{r} A_i$$

la décomposition semi-simple de l'algèbre $F[G]$ associée aux idempotents centraux minimaux e_i de $F[G]$.
Chacune des algèbres simples $A_i = F[G]e_i$ s'écrit comme somme directe d'idéaux à gauche minimaux deux à deux isomorphes :

$$A_i = \bigoplus_{j=1}^{r_i} F[G]e_{ij} = \bigoplus_{j=1}^{r_i} V_{ij}$$

où les $(e_{ij})_{j=1,\ldots,r_i}$ sont un système complet d'idempotents primitifs (non centraux pour $r_i > 1$) au-dessus de e_i.

Le caractère régulier de $F[G]$ se décompose alors comme somme :

$$\chi_{\text{rég}} = \sum_{i=1}^{r} r_i \chi_i$$

des caractères χ_i attachés aux modules indécomposables $V_{ij} = F[G]e_{ij}$, avec les multiplicités r_i.

Considérons maintenant un $F[G]$- module $\mathcal{M}$, et écrivons $\chi = \sum_{i=1}^{r} m_i \chi_i$ la décomposition irréductible du caractère associé. Si $\mathcal{N} = F[G].x$ est un sous-module monogène de $\mathcal{M}$, le caractère $\chi_{\mathcal{N}}$ qui lui correspond est contenu à la fois dans $\chi_{\mathcal{M}}$ (puisque $\mathcal{N}$ est contenu dans $\mathcal{M}$) et dans $\chi_{\text{rég}}$ (puisque $\mathcal{N}$ s'identifie à un quotient de $F[G]$). Autrement dit, nous avons simultanément :

$$\chi_{\mathcal{N}} \leq \chi_{\mathcal{M}} \qquad \text{et} \qquad \chi_{\mathcal{N}} \leq \chi_{\text{rég}} ,$$

ce que nous pouvons encore écrire :

$$\chi_{\mathcal{N}} \leq \chi_{\mathcal{M}} \wedge \chi_{\text{rég}} ,$$

en convenant de noter $\chi_{\mathcal{M}} \wedge \chi_{\text{rég}} = \sum_{i=1}^{r} \min\{m_i, r_i\} \chi_i$ le plus grand caractère contenu à la fois dans $\chi_{\mathcal{M}}$ et dans $\chi_{\text{rég}}$. Nous allons voir que cette dernière inégalité caractérise les sous-modules monogènes de $\mathcal{M}$:

<u>THÉORÈME II.1.4.</u>- Pour qu'un $F[G]$-module noethérien soit monogène, il faut et il suffit que son caractère soit contenu dans le caractère régulier.

Démonstration : Soit $\mathcal{N}$ un $F[G]$-module noethérien dont le caractère $\chi_{\mathcal{N}} = \sum_{i=1}^{r} n_i \chi_i$ est contenu dans le caractère régulier. L'identité

$n_i \leq r_i$ pour $i = 1,\dots,r$, se traduit par l'existence d'un isomorphisme φ de N pour la somme directe :

$$N \simeq \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} V_{ij} \ .$$

Posons alors $x_{ij} = \varphi^{-1}(e_{ij})$, puis $x = \sum_{i=1}^{r} \sum_{j=1}^{n_i} x_{ij}$; et considérons le $F[G]$-module engendré par x. Nous obtenons sans peine, par orthogonalité des idempotents e_{ij} , la décomposition :

$$F[G]\,x = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} F[G]\,x_{ij} \simeq \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_i} V_{ij} \ .$$

Et $F[G]\,x$, sous-module de N de même caractère, ne peut être que N.

<u>COROLLAIRE II.1.5.</u>- Dans un $F[G]$-module noethérien M , les sous-modules monogènes maximaux sont ceux de caractère $\chi_M \wedge \chi_{rég}$. En particulier , ils sont deux à deux isomorphes .

Démonstration : D'après ce qui précède , il s'agit de vérifier que les sous-modules monogènes de caractère maximal sont exactement les sous-modules monogènes maximaux . Or , d'un côté, tout sous-module de caractère $\chi_M \wedge \chi_{rég}$ est monogène maximal , puisqu'il est monogène d'après le théorème , mais qu'aucun sous-module de M strictement plus grand ne peut l'être ; et , d'un autre côté , si N est un sous-module de M, de caractère $\chi_N < (\chi_M \wedge \chi_{rég})$, et χ_i un facteur irréductible de $(\chi_M \wedge \chi_{rég}) - \chi_N$, le quotient M/N contient un sous-module de caractère χ_i , dont l'image réciproque dans M est un sous-module contenant strictement N, de caractère $\chi_N + \chi_i \leq (\chi_M \wedge \chi_{rég})$, donc monogène.

Venons-en maintenant à notre sujet : Soit K une extension galoisienne finie du corps de rationnels ; notons G son groupe de Galois , et ℓ un nombre premier . Le corps K , regardé comme $\mathbb{Q}[G]$-module , étant libre et de rang 1 , son localisé $K_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} K$ est donc un $\mathbb{Q}_\ell[G]$-module libre et monogène , c'est-à-dire un $\mathbb{Q}_\ell[G]$-module de caractère $\chi_{rég}$. Considérons un sous-module noethérien M du groupe multiplicatif $K^\times$, et notons $M_\ell = \log_\ell(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$ le sous-module de K_ℓ $\mathbb{Z}_\ell$-engendré par les logarithmes des éléments de M. Si M est stable par G , il en est de même de $\mathcal{M}_\ell$ (puisque le logarithme commute à l'action de Galois) , et le caractère $\chi_{\mathcal{M}_\ell}$ du $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{M}_\ell = \mathbb{Q}_\ell \operatorname{Log}_\ell \mathcal{M}$ est contenu à la fois dans celui $\chi_{rég}$ du $\mathbb{Q}_\ell[G]$-module K_ℓ (puisque $\mathbb{Q}_\ell \log_\ell \mathcal{M}$ est un sous-module de K_ℓ) , et dans celui $\chi_{\mathcal{M}}$ du $\mathbb{Q}[G]$- module $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{M}$ (puisque $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{M}_\ell$ est l'image de $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{M}) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathcal{M}$ par le logarithme ℓ-adique)(*) . En particulier , l'égalité $\chi_{\mathcal{M}_\ell} = \chi_{\mathcal{M}}$ ne peut avoir lieu que si $\chi_{\mathcal{M}}$ est contenu dans $\chi_{rég}$, i.e. , d'après le théorème 4 ci-dessus , si le $\mathbb{Q}[G]$-module $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{M}$ est monogène .

Ce résultat nous amène à poser la conjecture suivante :

CONJECTURE II.1.6.- Soient K une extension galoisienne finie du corps des rationnels , G son groupe de Galois , et ℓ un nombre premier . Etant donné un sous-module noethérien $\mathcal{M}$ du groupe multiplicatif $K^\times$, stable pour l'action de G , la restriction du logarithme ℓ-adique $\log_\ell$ au $\mathbb{Z}_\ell[G]$-module $\mathfrak{M} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{M}$, engendré par l'image de $\mathcal{M}$ dans le tensorisé $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$, est injective si et seulement si les trois conditions suivantes sont réunies :

(i) Le groupe $\mathcal{M}$ ne contient pas les racines $\ell^{\text{ièmes}}$ de l'unité.

(ii) Le radical de $\mathcal{M}$ dans $K^\times$ ne contient pas ℓ , i.e. $\ell \notin \sqrt{\mathcal{M}}$.

(iii) Le $\mathbb{Q}[G]$-module $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{M}$ est monogène , i.e. $\chi_{\mathcal{M}} \leq \chi_{rég}$.

Les deux premières conditions sont évidemment nécessaires puisque les racines ℓ-primaires de l'unité (**) et le nombre premier ℓ sont contenus dans le noyau du logarithme ℓ-adique ; la troisième d'après la discussion qui précède. La conjecture énoncée postule donc que ces conditions sont également suffisantes . Avant de la discuter , tirons-en immédiatement une conséquence :

(*) Nous notons indifféremment $\chi_{\mathcal{M}}$ le caractère du $\mathbb{Q}[G]$-module $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{M}$ et celui du $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathcal{M}$.

(**) Le produit tensoriel par $\mathbb{Z}_\ell$ a tué les racines de l'unité d'ordre étranger à ℓ .

THÉORÈME II.1.7.- Sous la conjecture précédente, le caractère χ_{M_ℓ} du $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \operatorname{Log}_\ell M$, engendré dans K_ℓ par l'image $M_\ell = \log_\ell(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$ du tensorisé ℓ-adique de M, est donné, en fonction du caractère χ_M du $\mathbb{Q}[G]$-module $\mathbb{Q} \otimes_{\mathbb{Z}} M$, par la formule :

(i) $\chi_{M_\ell} = \chi_M \wedge \chi_{\text{rég}}$, si ℓ n'appartient pas au radical de M.

(ii) $\chi_{M_\ell} = (\chi_M - 1) \wedge \chi_{\text{rég}}$, dans le cas contraire.

Démonstration : Quittes à remplacer M par l'une de ses puissances M^n, nous pouvons toujours supposer que M ne contient d'autre racine de l'unité que 1. Cela étant, distinguons les deux éventualités :

(i) $\ell \notin \sqrt{M}$. Dans ce cas, nous avons évidemment $\chi_{M_\ell} \leq \chi_M$ et $\chi_{M_\ell} \leq \chi_{\text{rég}}$, comme vu plus haut, donc $\chi_{M_\ell} \leq (\chi_M \wedge \chi_{\text{rég}})$. Réciproquement, le corollaire 5 nous donne l'inégalité opposée $\chi_{M_\ell} \geq (\chi_M \wedge \chi_{\text{rég}})$, puisque, si $\overline{N}$ est un sous-module monogène maximal de $\mathbb{Q} \otimes_{\mathbb{Z}} M$, et $x \in M$ un générateur de $\overline{N}$ (*), la restriction du logarithme ℓ-adique du $\mathbb{Z}_\ell[G]$-module $x^{\mathbb{Z}_\ell[G]}$ est injective, en vertu de la conjecture.

(ii) $\ell \in \sqrt{M}$. Dans ce cas, il existe un naturel $m \geq 1$, et un sous-module N de M, de caractère $\chi_N = \chi_M - 1$, tel que la somme $N \oplus \ell^{m\mathbb{Z}}$ soit directe et d'indice fini dans M. L'argument précédent appliqué à N permet alors de conclure.

c.- Discussion de la conjecture énoncée.

DÉFINITION II.1.8.- Convenons de dire qu'un $\mathbb{Z}[G]$-module noethérien M est quasi-monogène lorsque le $\mathbb{Q}[G]$-module associé $\mathbb{Q} \otimes_{\mathbb{Z}} M$ est monogène. Un $\mathbb{Z}[G]$-module quasi-monogène est donc un sur-module d'indice fini d'un $\mathbb{Z}[G]$-module monogène.

PROPOSITION II.1.9.- La conjecture précédente est vraie pour les modules M dont tous les éléments sont étrangers à ℓ, sous la conjecture de Schanuel ℓ-adique (**).

(*) Le groupe M étant pris sans torsion, il est canoniquement un sous-module de son tensorisé $\mathbb{Q} \otimes_{\mathbb{Z}} M$.

(**) Sous la forme faible, la conjecture de Schanuel ℓ-adique postule que les logarithmes ℓ-adiques de nombres algébriques $\mathbb{Q}$-multiplicativement indépendants et étrangers à ℓ sont $\mathbb{Q}$-algébriquement indépendants.

Pour établir cette proposition , nous nous appuyerons sur le lemme :

LEMME II.1.10.- Tout sous-module quasi-monogène $\mathcal{M}$ du $\mathbb{Z}[G]$-module $K^{\times}$, dont tous les éléments sont étrangers à ℓ , est contenu dans un sous-module quasi-monogène $\mathcal{N}$ de $K^{\times}$ qui possède les trois propriétés suivantes :

(i) Les éléments de $\mathcal{N}$ sont étrangers à ℓ .

(ii) Le $\mathbb{Q}[G]$-module $\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{N}$ est libre et monogène .

(iii) $\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{M}$ est facteur direct de $\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{N}$.

Démonstration du lemme : Puisque $\mathcal{M}$ est de type fini , nous pouvons trouver un nombre premier p, étranger à ℓ et à tous les éléments de $\mathcal{M}$, qui se décompose complètement dans l'extension galoisienne $K/\mathbb{Q}$. Notons x un générateur d'une puissance principale d'un quelconque des idéaux premiers $\mathfrak{p}$ de K au-dessus de p . Par hypothèse , le groupe de Galois G opère fidèlement sur les places de K au-dessus de p ; le sous-module $x^{\mathbb{Z}[G]}$, engendré dans $K^{\times}$ par x et ses conjugués , est donc isomorphe à $\mathbb{Z}[G]$. Il est linéairement disjoint de $\mathcal{M}$, puisque p est étranger à tous les éléments de $\mathcal{M}$. Considérons le $\mathbb{Q}[G]$- module $\overline{\mathcal{P}} = \mathbb{Q}\otimes_{\mathbb{Z}}(\mathcal{M}\oplus x^{\mathbb{Z}[G]})$ engendré par $\mathcal{M}$ et x : Il contient la représentation régulière ; et le corollaire 5 nous assure donc que ses sous-modules monogènes maximaux sont tous isomorphes à $\mathbb{Q}[G]$. Choisissons-en un $\overline{\mathcal{N}}$, qui contienne $\overline{\mathcal{M}} = \mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{M}$; le sous-groupe $\mathcal{N}$ formé des éléments de $\mathcal{M}\oplus x^{\mathbb{Z}[G]}$ qui tombent dans $\overline{\mathcal{N}}$ convient .

Démonstration de la proposition : Il s'agit d'établir que, pour tout sous-module quasi-monogène et sans $\mathbb{Z}$-torsion $\mathcal{M}$ du $\mathbb{Z}[G]$-module $K^{\times}$, le rang ℓ-adique $\mathrm{rg}_{\mathbb{Z}_\ell}\, \log_\ell(\mathbb{Z}_\ell\otimes_{\mathbb{Z}}\mathcal{M})$ du $\mathbb{Z}_\ell$-module libre engendré par l'image logarithmique de $\mathcal{M}$ dans K_ℓ est égal au rang $\mathrm{rg}_{\mathbb{Z}}\,\mathcal{M}$ du $\mathbb{Z}$- module libre $\mathcal{M}$, dès lors que tous les éléments de $\mathcal{M}$ sont étrangers à ℓ . D'après le lemme , il suffit de faire la démonstration lorsque $\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{M}$ est la représentation régulière de $\mathbb{Q}[G]$. Cela étant , notons $x\in\mathcal{M}$ un générateur du $\mathbb{Q}[G]$-module $\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{M}$, et considérons la matrice ℓ-adique :

$$X_\ell = [\mathrm{Log}_\ell\, x^{\sigma\tau}]_{(\sigma,\tau)\in G\times G}\,.$$

Son déterminant est un polynôme en les logarithmes ℓ-adiques des conjugués de x , qui n'est pas le polynôme nul : En effet , les conjugués de x étant par hypothèse $\mathbb{Q}$-multiplicativement indépendants , la matrice réelle :

$$X = [\mathrm{Log}\,|x^{\sigma\tau}|\,]_{(\sigma,\tau)\in G\times G}$$

est régulière , puisque l'image de $\mathcal{M}$ dans $\mathbb{R}^{[K:\mathbb{Q}]}$ par le plongement logarithmique :

$$\prod_{\sigma\in G} x^{\alpha_\sigma \sigma} \longrightarrow \Big(\mathrm{Log}\,\Big|\prod_{\sigma\in G} x^{\alpha_\sigma \sigma\tau}\Big|\Big)_{\tau\in G}$$

est un réseau de $\mathbb{R}^{[K:\mathbb{Q}]}$, en vertu d'un argument classique de géométrie des nombres (cf. [Sa$_1$] , Ch. IV, § 4) . La conjecture de Schanuel permet alors d'affirmer que la matrice X_ℓ est également régulière , ce qui signifie que l'image de $\mathcal{M}$ dans $K_\ell^{[K:\mathbb{Q}]}$ par le plongement logarithmique :

$$\prod_{\sigma\in G} x^{\alpha_\sigma \sigma} \longrightarrow \Big(\mathrm{Log}_\ell\Big(\prod_{\sigma\in G} x^{\alpha_\sigma \sigma\tau}\Big)\Big)_{\tau\in G}$$

est un réseau de $K_\ell^{[K:\mathbb{Q}]}$, et implique en particulier que les nombres $(\mathrm{Log}_\ell\, x^\sigma)_{\sigma\in G}$ sont K_ℓ- linéairement indépendants .

Pour pouvoir appliquer au module $\mathcal{M}$ la conjecture de Schanuel , nous avons supposé que tous les éléments de $\mathcal{M}$ étaient étrangers à ℓ . De fait , la conjecture énoncée plus haut requiert seulement que $\mathcal{M}$ ne contienne aucune puissance de ℓ . Il parait donc raisonnable d'énoncer la conjecture de Schanuel ℓ-adique sous la forme faible plus générale suivante :

Conjecture de Schanuel modifiée .- Si les logarithmes ℓ-adiques de nombres algébriques sont $\mathbb{Q}$ - linéairement indépendants , ils sont $\mathbb{Q}$ - algébriquement indépendants .

Cela posé , la proposition 9 se généralise immédiatement sous la forme :

PROPOSITION II.1.11.- La conjecture énoncée est vraie sous la conjecture de Schanuel modifiée .

Ce dernier résultat est l'une des présomptions les plus fortes que nous ayons en faveur de la conjecture énoncée .

2.- MINORATIONS DU RANG ℓ- ADIQUE ET PREUVE DE LA CONJECTURE DANS LE CAS ABÉLIEN .

a.- Preuve de la conjecture dans le cas abélien .

Considérons un sous-module noethérien et sans torsion M du groupe multiplicatif $K^\times$; notons $r_M = \mathrm{rg}_{\mathbb{Z}}\, M$ son rang , et $r_{M_\ell} = \mathrm{rg}_{\mathbb{Z}_\ell}\, M_\ell$ celui du $\mathbb{Z}_\ell$-module libre $\log_\ell(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$. Si M est stable pour l'action de G , les entiers r_M et r_{M_ℓ} sont les degrés respectifs des représentations associées à M et à M_ℓ :

$$r_M = \deg \chi_M \qquad \text{et} \qquad r_{M_\ell} = \deg \chi_{M_\ell} \ .$$

En particulier , le rang conjectural du module M_ℓ est donné par les formules :

$$r_{M_\ell} = \begin{cases} \deg\,[(\chi_M - 1) \wedge \chi_{\text{rég}}] \ , & \text{si } \ell \in \sqrt{M} \ , \\ \deg\,[\chi_M \wedge \chi_{\text{rég}}] \ , & \text{sinon} \ , \end{cases}$$

ce qu'il est commode d'écrire de façon indifférenciée :

$$r_{M_\ell} = \deg\,[\chi'_M \wedge \chi_{\text{rég}}] \ , \quad \text{en posant } \chi'_M = \begin{cases} \chi_M - 1 \ , & \text{si } \ell \in \sqrt{M} \\ \chi_M \ , & \text{dans le cas contraire.} \end{cases}$$

Nous allons voir que la conjecture énoncée est vraie dès que le groupe G est abélien , ce qui nous donnera au passage une première minoration du rang ℓ- adique r_M .

THÉORÈME II.1.12.- Soient M un sous-module noethérien du groupe multiplicatif $K^\times$, stable pour l'action de $G = \mathrm{Gal}(K/\mathbb{Q})$, puis χ_M le caractère du $\mathbb{Q}[G]$- module $\mathbb{Q} \otimes_{\mathbb{Z}} M$, et χ_{M_ℓ} celui du $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_\ell$, engendré dans K_ℓ par l'image $M_\ell = \log_\ell(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$ du tensorisé ℓ-adique de M. Alors le caractère χ_{M_ℓ} contient chaque caractère ℓ-adique irréductible ψ représenté dans le caractère χ'_M défini par $\chi'_M = \chi_M - 1$, si $\ell = \sqrt{M}$; $\chi'_M = \chi_M$ sinon : (*)

$$\chi_{M_\ell} \geq \sum_{\psi \leqslant \chi'} \psi$$

En particulier, la conjecture énoncée est vraie dès que le groupe G est abélien, et, plus généralement, dès que l'algèbre $\mathbb{Q}_\ell[G]$ est un produit direct de corps.

Démonstration : Supposons d'abord que M ne contienne pas de puissance de ℓ. Pour chaque caractère rationnel irréductible χ représenté dans χ_M, nous pouvons trouver un x_χ dans M qui engendre un $\mathbb{Q}[G]$-module irréductible de caractère χ.

- Si χ est irréductible sur $\mathbb{Q}_\ell$, le $\mathbb{Q}_\ell[G]$-module engendré par $\mathrm{Log}_\ell\, x_\chi$ (qui est non nul, puisque M ne contient pas de puissance de ℓ) est encore irréductible de caractère χ ; et il n'y a rien à démontrer.

- Sinon χ s'écrit comme somme de caractères ψ, irréductibles sur $\mathbb{Q}_\ell$, à valeurs dans une extension cyclotomique de $\mathbb{Q}$. Faisons choix d'une base $(x^\sigma)_{\sigma \in H}$ du $\mathbb{Q}$-espace $x^{\mathbb{Q}[G]}$, formé de conjugués de x. Si l'un des caractères au-dessus de χ, disons ψ, n'était pas représenté dans le $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} M_\ell$, nous aurions simultanément :

$$\sum_{\sigma \in G} \psi(\sigma^{-1})\, \mathrm{Log}_\ell\, x^\sigma = 0$$

dans K_ℓ, mais :

$$x^{\sum_{\sigma \in G} \psi(\sigma^{-1})\sigma} \neq 1 \text{ , dans } \mathbb{Z}_\ell \otimes_{\mathbb{Z}} M \text{ ,}$$

donc, en exprimant les conjugués de x en fonction des seuls $(x^\sigma)_{\sigma \in H}$, une relation de dépendance linéaire non triviale, à coefficients algébriques, entre les logarithmes ℓ-adiques des $(x^\sigma)_{\sigma \in H}$, contrairement au théorème d'indépendance de Baker-Brumer (cf. [Br]).

(*) Cette inégalité peut être regardée comme une généralisation du théorème fondamental de [EKW] pour le module des unités.

Enfin, si M contient des puissances de ℓ, il suffit de remarquer que M contient un sous-module d'indice fini de la forme $\ell^{m\mathbb{Z}} \oplus N$, où N est un $\mathbb{Z}[G]$-module de caractère $\chi_N = \chi_M - 1 = \chi'_M$, et de raisonner sur N pour se ramener au cas précédent.

En résumé, la conjecture est ainsi établie dans tous les cas où les caractères ℓ-adiques irréductibles sont représentés une fois et une seule dans le caractère régulier, c'est-à-dire (cf. [My], prop. 3) lorsque l'algèbre de groupe $\mathbb{Q}_\ell[G]$ est un produit direct de corps.

COROLLAIRE II.1.13. - Le rang ℓ-adique d'un $\mathbb{Z}[G]$-module multiplicatif M est au moins la racine carrée de son rang conjectural $r^{conj}_{M_\ell} = \deg(\chi'_M \wedge \chi_{rég})$:

$$r_{M_\ell} \geq \sqrt{r^{conj}_{M_\ell}} .$$

Démonstration : Dans la décomposition $\chi_{rég} = \sum d_\varphi \varphi$ du caractère régulier comme somme de caractères absolument irréductibles (à valeurs dans une extension cyclotomique de $\mathbb{Q}$), les indices d_φ sont les degrés respectifs des caractères φ (cf. [Se$_1$], Ch. I, § 2.4). Comme, d'après le théorème 12 ci-dessus, chaque caractère absolument irréductible φ représenté dans χ'_M l'est encore dans χ_{M_ℓ}, il vient donc :

$$r_{M_\ell} \geq \sum_{\varphi | \chi'_M} \deg\varphi = \sum_{\varphi | \chi'_M} \sqrt{d_\varphi \deg\varphi} \leq \sqrt{\sum_{\varphi | \chi'_M} d_\varphi \deg\varphi} = \sqrt{\deg\Big(\sum_{\varphi|\chi'_M} d_\varphi \varphi\Big)}$$

$$\geq \sqrt{\deg \chi^{conj}_{M_\ell}} = \sqrt{r^{conj}_{M_\ell}} .$$

C'est le résultat démontré par Emsalem, Kisilevsky, et Wales (cf. [EKW]), lorsque M est le groupe des unités.

b.- Minoration du rang ℓ-adique.

La minoration du rang ℓ-adique donnée par le corollaire 13 peut être sensiblement améliorée à l'aide d'un résultat de transcendance, dû à Waldschmidt, sur les matrices à coefficients logarithmes de nombres algébriques. Il vient, en effet :

PROPOSITION II.1.14.- Le rang ℓ-adique $r_{M_\ell} = \deg \chi_{M_\ell}$ d'un sous-module noethérien M du $\mathbb{Z}[G]$-module $K^\times$ est au moins la moitié du rang conjectural $r_{M_\ell}^{conj} = \deg(\chi'_M \wedge \chi_{rég})$:

$$r_{M_\ell} \geq \frac{1}{2}\, r_{M_\ell}^{conj} .$$

Démonstration : Il suffit naturellement d'établir ce résultat lorsque M est un $\mathbb{Z}[G]$-module sans $\mathbb{Z}$-torsion ne contenant pas de puissances de ℓ. Cela étant, prenons un x dans M engendrant un sous-module monogène maximal du produit $\overline{M} = \mathbb{Q} \otimes_{\mathbb{Z}} M$; et posons $N = x^{\mathbb{Z}[G]}$. La proposition sera démontrée si nous prouvons l'inégalité $r_{N_\ell} \geq \frac{1}{2}\, r_N$. Considérons pour cela la matrice en les logarithmes réels des modules des conjugués de x :

$$X = [\,\mathrm{Log}\,|x^{\sigma\tau}|\,]_{(\sigma,\tau) \in G \times G} .$$

Par un argument de géométrie des nombres déjà invoqué (cf. [Sa_1], Ch. IV, §4), cette matrice a pour rang r_N. Le théorème de Waldschmidt (cf. [Wa_2], §1, th. 1.1) permet alors d'affirmer que la matrice en les logarithmes ℓ-adiques :

$$X_\ell = [\,\mathrm{Log}_\ell(x^{\sigma\tau})\,]_{(\sigma,\tau) \in G \times G}$$

a pour rang au moins $\frac{1}{2}\, r_N$ (*). L'inégalité annoncée en résulte.

Enoncé en termes de représentations, le théorème de Waldschmidt conduit même à un résultat sensiblement plus précis : Ecrivons $\chi_{rég} = \sum r_\chi \chi$ la décomposition du caractère régulier comme somme de caractères rationnels irréductibles. Nous avons :

(*) En fait, le théorème énoncé dans [Wa_2] suppose que les $x^{\sigma\tau}$ soient des unités ℓ-adiques. Cependant, cette condition n'est nullement indispensable : Dans les démonstrations techniques, en effet, le changement de variables $x = \exp(\ell^m\, \mathrm{Log}_\ell\, x)$, avec m grand, permet toujours de se ramener à des unités principales. Outre l'algébricité de x, seule est donc requise la validité de l'implication $\sum_{\sigma \in G} a_\sigma \mathrm{Log}_\ell\, x^\sigma = 0 \Rightarrow \sum_{\sigma \in G} a_\sigma \mathrm{Log}\,|x^\sigma| = 0$ (pour des (a_σ) dans $\mathbb{Z}$), c'est-à-dire le fait que le $\mathbb{Z}[G]$-module multiplicatif engendré par x ne contienne pas de puissance de ℓ.

THÉORÈME II.1.15.- Soient M un sous-module galoisien isotypique du groupe multiplicatif $K^{\times}$, ne contenant pas de puissances de ℓ, de caractère $\chi_M = m\chi$, et χ_{M_ℓ} le caractère du $\mathbb{Z}_\ell[G]$-module $\log_\ell(\mathbb{Z}_\ell \otimes_{\mathbb{Z}} M)$.

- Si le caractère rationnel irréductible χ ne se décompose pas sur $\mathbb{Q}_\ell$ (i.e. si χ est un multiple $s\psi$ d'un caractère ℓ-adique irréductible ψ), le caractère χ_{M_ℓ} vérifie les minorations :

$$\chi_{M_\ell} \geq \frac{m}{2}\chi = \frac{1}{2}\chi_M, \quad \text{si } \chi_M \text{ est contenu dans } \chi_{\text{rég}} \ (\text{i.e. si } m \leq r_\chi).$$

$$\chi_{M_\ell} \geq \frac{k}{k+1} r_\chi \chi = \frac{k}{k+1}(\chi_M \wedge \chi_{\text{rég}}),$$

$$\text{avec } k = \left[\frac{m}{r_\chi}\right], \text{ dans tous les autres cas.}$$

- Si le caractère rationnel irréductible χ se décompose sur $\mathbb{Q}_\ell$ (i.e. s'il existe au moins deux caractères ℓ-adiques irréductibles distincts représentés dans χ), les formules précédentes restent valables pour les degrés :

$$r_{M_\ell} \geq \frac{1}{2} r_{M_\ell}^{\text{conj}} = \frac{1}{2} r_M, \quad \text{si } \chi_M \text{ est contenu dans } \chi_{\text{rég}}.$$

$$r_{M_\ell} \geq \frac{k}{k+1} r_{M_\ell}^{\text{conj}}, \quad \text{avec } k = \left[\frac{m}{r_\chi}\right], \text{ dans tous les autres cas.}$$

Démonstration : Lorsque χ_M est contenu dans $\chi_{\text{rég}}$, l'inégalité $r_{M_\ell} \geq \frac{1}{2} r_M$ est donnée par la proposition 14. Si le caractère χ est un multiple $s\psi$ d'un caractère ℓ-adique irréductible ψ, le caractère χ_{M_ℓ} est lui-même un multiple de ψ (tout comme χ_M) et l'inégalité $r_{M_\ell} \geq \frac{1}{2} r_M$ s'écrit donc :

$$\chi_{M_\ell} \geq \frac{1}{2}\chi_M, \quad \text{comme annoncé.}$$

On notera que cette inégalité, qui s'écrit encore $\chi_{M_\ell} \geq \frac{sm}{2}\psi$, donne en fait $\chi_{M_\ell} \geq \left[\frac{sm+1}{2}\right]\psi$, puisque ψ est contenu un nombre entier de fois dans χ_{M_ℓ} (mais ce résultat pourrait être en défaut pour χ).

Supposons donc désormais $m \geq r_\chi$, et posons $k = \left[\frac{m}{r_\chi}\right]$. Par hypothèse, nous pouvons trouver dans M un sous-module N, somme directe de k sous-modules monogènes $x_i^{\mathbb{Z}[G]}$ (pour $i = 1, \dots, k$), isotypiques de caractère $r_\chi \chi$; et le théorème sera établi si nous prouvons l'inégalité $r_{M_\ell} \geq \frac{k}{k+1} r_\chi \deg \chi$. Pour cela, introduisons l'idempotent central e_χ de l'algèbre $\mathbb{Q}_\ell[G]$ attaché au caractère χ ; faisons choix d'une base $H \subset G$ du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[G]e_\chi$; et considérons le $\mathbb{Z}$-module X , de rang $k r_\chi \deg \chi$, engendré dans K_ℓ^H par les images $(\mathrm{Log}_\ell x_i^{\sigma\tau})_{\sigma \in H}$ des conjugués des x_i dans le plongement logarithmique de $\mathcal{M}$ dans K_ℓ^H . Nous pouvons naturellement l'écrire comme somme directe $X = \underset{i=1}{\oplus} X_i$ des $\mathbb{Z}$-modules associés à chacun des x_i , de sorte qu'en vertu d'un lemme d'Emsalem (cf. [E] , lemme 4) , le coefficient $\theta(X, K_\ell^H)$ défini par :

$$\theta(X, K_\ell^H) = \min_V \frac{\mathrm{corg}_{\mathbb{Z}}(V \cap X)}{\mathrm{codim}_{K_\ell} V} = \min_V \frac{\mathrm{rg}_{\mathbb{Z}} X - \mathrm{rg}_{\mathbb{Z}}(V \cap X)}{\dim_{K_\ell} K_\ell^H - \dim_{K_\ell} V}$$

(lorsque V parcourt les sous-espaces stricts de K_ℓ^H qui sont rationnels sur $\mathbb{Q}$) , vérifie la minoration :

$$\theta(X, K_\ell^H) \geq \sum_{i=1}^{k} \theta(X_i, K_\ell^H) = \sum_{i=1}^{k} 1 = k \; .$$

Le théorème principal de Waldschmidt (cf. [Wa_2] , ch.4 , th. 4.1) conduit alors à la minoration :

$$\mathrm{rg}_{\mathcal{N}_\ell} \geq \frac{k}{k+1} (r_\chi \deg \chi) \; ,$$

ce qui est le résultat attendu .

Remarque : Nous avons supposé , dans l'énoncé du théorème 15 , que le module $\mathcal{M}$ ne contenait pas de puissances de ℓ . De fait , lorsque $\mathcal{M}$ est isotypique , la condition $\ell \in \sqrt{\mathcal{M}}$ ne peut avoir lieu que si $\chi_{\mathcal{M}}$ est un multiple m 1 du caractère unité . Mais comme celui-ci n'est représenté qu'une fois dans le caractère régulier , le caractère $\chi_{\mathcal{M}_\ell} = (\chi_{\mathcal{M}} - 1) \wedge \chi_{\text{rég}}$ est alors égal à 0 ou à 1 suivant que χ contient une ou plusieurs fois le caractère unité . Dans le premier cas , $\chi_{\mathcal{M}_\ell}$ est trivialement nul ; dans le second , le module $\mathcal{M}$ contient un nombre algébrique $x \in K^\times$ qui n'est pas dans le noyau du logarithme Log_ℓ , et le caractère $\chi_{\mathcal{M}_\ell}$ n'est pas nul. Dans les deux cas, il vient donc directement $\chi_{\mathcal{M}_\ell} = \chi_{\mathcal{M}_\ell}^{\text{conj}} = (\chi_{\mathcal{M}} - 1) \wedge \chi_{\text{rég}}$, sans qu'il soit nécessaire de faire appel à un quelconque argument transcendant .

<u>COROLLAIRE II.1.16</u> (*) .- Le rang ℓ-adique r_{M_ℓ} d'un sous-module galoisien M de $K^\times$ est égal à son rang conjectural $r_{M_\ell}^{\text{conj}}$ dès que M est assez grand en un sens indépendant de ℓ. Plus précisément, si chaque caractère rationnel irréductible χ représenté dans χ_M l'est au moins $\frac{r_\chi}{s_\chi}$ fois, le caractère χ_{M_ℓ} a sa valeur conjecturale $\chi_{M_\ell}^{\text{conj}} = \chi_M^! \wedge \chi_{rég}$. Les entiers r_χ et s_χ sont définis par la représentation matricielle $\mathbb{Q}[G]\, e_\chi \simeq M_{r_\chi}(D_\chi)$ du facteur simple de l'algèbre $\mathbb{Q}[G]$ associé au caractère χ : le premier r_χ est le nombre de fois où χ est représenté dans le carac - tère régulier ; le second s_χ, égal au degré sur $\mathbb{Q}$ du centre du corps gauche D_χ, est l'indice de Schur du caractère χ.

Démonstration : Il suffit évidemment de faire la démonstration lorsque M est isotypique, i.e. quand χ_M est de la forme $m\chi$, pour un caractère rationnel irréductible χ. Si les caractères absolument irréductibles φ au-dessus de χ sont de degré 1, ils sont représentés une seule fois dans le caractère régulier, et le théorème 12 donne immédiatement $\chi_{M_\ell} = \chi_{M_\ell}^{\text{conj}}$. C'est le cas en particulier lorsque χ est le caractère unité 1. Dans tout ce qui suit, nous pouvons donc supposer $\chi \neq 1$, auquel cas M ne contient pas de puissances de ℓ. Cela étant, d'après le théorème 15, pour $m \geq r_\chi$ nous avons :

$$r_{M_\ell} \geq \frac{k}{k+1}\, r_\chi \deg \chi > r_\chi \deg \chi - \frac{r_\chi \deg \chi}{k}, \quad \text{avec } k = \left[\frac{m}{r_\chi}\right].$$

Ecrivons alors $\chi = s_\chi \sum_{\varphi \mid \chi} \varphi$ la décomposition absolument irréductible du caractère χ (de sorte que nous avons $r_\chi s_\chi = \deg \varphi$). Si le carac - tère χ était strictement inférieur à sa valeur conjecturale $\chi_{M_\ell}^{\text{conj}} = r_\chi \chi$, nous aurions : $\quad r_{M_\ell} \leq r_\chi \deg \chi - \deg \varphi$.

L'égalité $\chi_{M_\ell} = \chi_{M_\ell}^{\text{conj}}$ a donc lieu dès que la quantité $\frac{r_\chi \deg \chi}{k}$ est infé - rieure à $\deg \varphi$, c'est-à-dire pour

$$k \geq r_\chi \frac{\deg \chi}{\deg \varphi}, \quad \text{i.e. } m \geq r_\chi^2 \frac{\deg \chi}{\deg \varphi} = \frac{r_\chi}{s_\chi} \deg \chi .$$

(*) L'égalité $r_{M_\ell} = r_{M_\ell}^{\text{conj}}$ dès que M est assez grand, en un sens indé - pendant de ℓ, est dûe à Emsalem : C'est le résultat principal de [E]. La borne proposée ici est plus fine que celle de [E].

c.- Comparaison des résultats obtenus .

Donnons d'abord quelques exemples, qui illustrent les limites des résultats précédents :

Exemple 1 .- Si G est le groupe quaternonien H_8, l'algèbre $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{H}$ est composée de quatre exemplaires de $\mathbb{Q}$, et d'un du corps des quaternions sur $\mathbb{Q}$.

- Si ℓ vaut 2, le facteur simple $\mathbb{Q}_2 \otimes_{\mathbb{Q}} \mathbb{H}$ est le corps $\mathbb{H}_2$ des quaternions sur $\mathbb{Q}_2$; l'algèbre $\mathbb{Q}_2[G]$ est un produit direct de corps, et la conjecture est vraie en vertu du théorème 12.

- Dans tous les autres cas, le produit tensoriel $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathbb{H}$ est isomorphe à $\mathcal{M}_2(\mathbb{Q})$; le caractère rationnel ρ correspondant à H s'écrit $\rho = 2\pi$, pour un caractère ℓ-adique (absolument) irréductible π. Si donc $\mathcal{M}$ est un sous-module galoisien de $K^\times$, ne contenant pas de puissances de ℓ, ayant pour caractère le caractère régulier

$$\chi_{\mathcal{M}} = 1 + \chi_1 + \chi_2 + \chi_3 + \rho ,$$

le théorème 12 donne seulement :

$$\chi_{\mathcal{M}_\ell} \geq 1 + \chi_1 + \chi_2 + \chi_3 + \pi .$$

D'après le corollaire 16, en revanche, l'égalité $\chi_{\mathcal{M}_\ell} = \chi_{\mathcal{M}_\ell}^{\text{conj}}$ est assurée dès que $\chi_{\mathcal{M}}$ contient deux fois le caractère ρ :

$$\chi_{\mathcal{M}} \geq 1 + \chi_1 + \chi_2 + \chi_3 + 2\rho \Rightarrow \chi_{\mathcal{M}_\ell} = 1 + \chi_1 + \chi_2 + \chi_3 + \rho .$$

Exemple 2 .- Si G est le groupe métacyclique M_{21}, la décomposition semi-simple de l'algèbre $\mathbb{Q}[G]$ s'écrit :

$$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q}[\sqrt{-3}\,] \oplus {}_3(\mathbb{Q}[\sqrt{-7}\,]) .$$

L'écriture rationnelle irréductible $\chi_{\text{rég}} = 1 + \chi + 3\rho$ du caractère régulier fait donc intervenir un caractère χ de degré 2 (qui se décompose sur $\mathbb{Q}_\ell$ comme somme de deux caractères absolument irréductibles, lorsque (-3) est un carré dans $\mathbb{Q}_\ell$) et un caractère ρ de degré 6.

- Si (-7) n'est pas un carré dans $\mathbb{Q}_\ell$, le caractère ρ est irréductible sur $\mathbb{Q}_\ell$. Par suite, si $\mathcal{M}$ est un sous-module galoisien de $K^\times$, ne contenant pas de puissances de ℓ, ayant pour caractère le caractère régulier $\chi_{\mathcal{M}} = \chi_{\text{rég}}$, le théorème 12 donne $\chi_{\mathcal{M}_\ell} \geq 1 + \chi + \rho$, et le théorème 15 : $\chi_{\mathcal{M}_\ell} \geq 1 + \chi + 2\rho$. Enfin, d'après le corollaire 16, l'égalité $\chi_{\mathcal{M}_\ell} = \chi_{\mathcal{M}_\ell}^{\text{conj}}$ a lieu sous la condition suffisante $\chi_{\mathcal{M}} \geq 1 + \chi + 18\rho$.

- Si (-7) est un carré dans $\mathbb{Q}_\ell$, le caractère ρ se décompose comme somme $\rho_1 + \rho_2$ de deux caractères ℓ-adiques (absolument) irréductibles , de degré 3 . Si donc , comme plus haut , M est un sous-module galoisien de $K^\times$, ne contenant pas de puissances de ℓ , ayant pour caractère le caractère régulier $\chi_M = \chi_{\text{rég}}$, le théorème 12 donne toujours $\chi_{M_\ell} \geq 1 + \chi + \rho$, mais le théorème 15 permet seulement d'affirmer que l'inégalité est stricte , sans préciser celui des caractères ρ_i au-dessus de ρ qui figure au moins deux fois dans χ . Enfin , le corollaire 16 donne encore $\chi_{M_\ell} = \chi_{M_\ell}^{\text{conj}}$, sous la condition suffisante $\chi \geq 1 + \chi + 18\,\rho$.

<u>Exemple 3</u> .- Si G est le groupe symétrique $\mathfrak{S}_4$, la décomposition semi-simple de l'algèbre $\mathbb{Q}[G]$ s'écrit :

$$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_3(\mathbb{Q}) \oplus M_3(\mathbb{Q}) \ ,$$

et la décomposition du caractère régulier comme somme de caractères rationnels irréductibles

$$\chi_{\text{rég}} = 1 + \varepsilon + 2\,\theta + 3\,\psi + 3\,\varepsilon\psi \ ,$$

fait donc intervenir deux caractères de degré 1, un caractère de degré 2 , et deux caractères de degré 3 . Tous sont absolument irréductibles (*) . En particulier , si M est un sous-module galoisien de $K^\times$, ne contenant pas de puissances de ℓ , ayant pour caractère le caractère régulier $\chi_M = \chi_{\text{rég}}$, le théorème 12 donne l'inégalité $\chi_{M_\ell} \geq 1 + \varepsilon + \theta + \psi + \varepsilon\psi$, et le théorème 15 l'inégalité plus forte $\chi_{M_\ell} \geq 1 + \varepsilon + \theta + 2\,\psi + 2\,\varepsilon\psi$. Enfin , le corollaire 16 assure l'égalité $\chi_{M_\ell} = \chi_{M_\ell}^{\text{conj}}$, sous la condition suffisante $\chi_M \geq 1 + \varepsilon + 4\,\theta + 9\,\psi + 9\,\varepsilon\psi$.

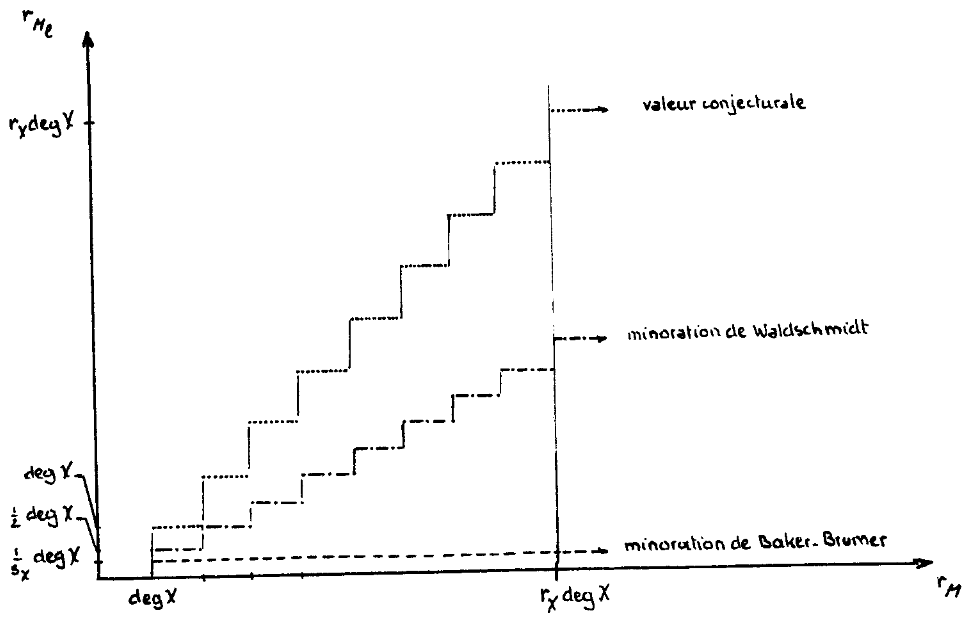
On voit sur ces exemples que le théorème 15 , s'il ne permet en aucun cas d'étendre le domaine de validité de la conjecture énoncée, conduit toujours néanmoins à des estimations du rang ℓ-adique sensiblement meilleures que celles résultant du théorème 12 . La différence

---

(*) Plus généralement , toutes les représentations de $\mathfrak{S}_n$ étant réalisables sur $\mathbb{Q}$, les caractères d'un tel groupe sont à valeurs rationnelles , et le théorème 12 vaut donc trivialement pour les groupes symétriques en l'abscence de tout argument transcendant .

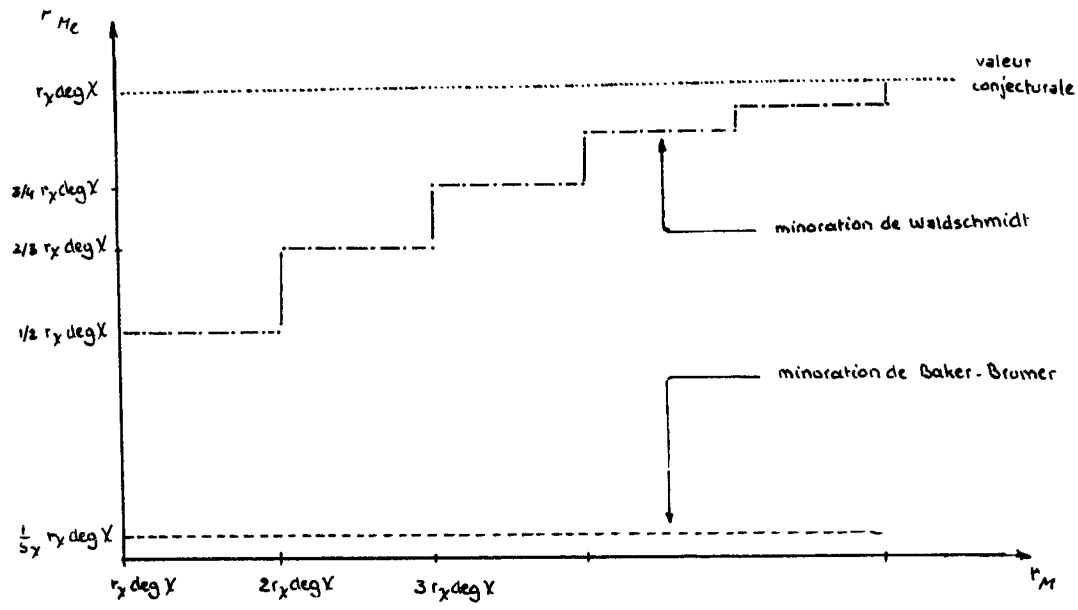
entre les minorations obtenues est d'ailleurs d'autant plus nette que les caractères irréductibles ont un indice élevé : Par exemple , si M est un sous-module isotypique de K^{χ} de caractère $\chi_M = m\,\chi$ (avec $\chi \neq 1$) , contenu dans le caractère régulier , le rang ℓ-adique r_{M_ℓ} est donné en fonction du rang r_M par le tableau suivant :

Tableau 1



Pour $m \geqslant r_\chi$, il vient de même :

Tableau 2



3.- APPLICATION AUX CONJECTURES DE LEOPOLDT ET DE GROSS.

a.- La conjecture de Leopoldt et le problème du rang ℓ-adique des S-unités.

Les sous-groupes de type fini de $K^\times$ les plus intéressants du point de vue de l'arithmétique sont naturellement les groupes de S-unités. Rappelons que, si S désigne un ensemble fini de places du corps des rationnels, contenant la place à l'infini, et S_K l'ensemble des places de K au-dessus de S, les S-unités du corps K sont les éléments inversibles de l'anneau $\mathcal{O}_K^S$ des S-entiers de K :

$$\mathcal{O}_K^S = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0, \quad \forall \mathfrak{p} \notin S_K\}.$$

Plus généralement :

DÉFINITION II.1.17.- Etant donné un ensemble fini quelconque $S = S_F$ de places d'un sous-corps F de K, nous appelons groupe des S-unités du corps de nombres K, et nous notons E_K^S, le noyau, dans le groupe multiplicatif $K^\times$, des valuations associées aux places de K au-dessus de S (*) :

$$E_K^S = \{x \in K^\times \mid v_{\mathfrak{p}}(x) = 0, \quad \forall \mathfrak{p} \notin S_K\}.$$

Les S-unités sont donc les S-unités au sens ordinaire qui sont positives en chaque place $\mathfrak{p}$ de K n'appartenant pas à S_K.

Comme les places complexes ne jouent aucun rôle dans la définition des groupes E_K^S, et que les carrés vérifient trivialement la condition de positivité aux places réelles, les groupes de S-unités ont la même dimension (**) qu'ils soient pris au sens ordinaire ou au sens de la définition précédente. Nous supposerons donc pour simplifier, dans tout ce qui suit, que l'ensemble S_K contient les places archimédiennes du corps K, auquel cas les deux définitions coïncident. Cela posé, lorsque le

---

(*) Pour une définition des valuations associées aux places d'un corps de nombres, voir Ch. III.1, § 1, a.

(**) Nous appelons dimension d'un $\mathbb{Z}$-module M, la dimension sur $\mathbb{Q}$ de l'espace vectoriel $\mathbb{Q} \otimes_{\mathbb{Z}} M$.

corps K est galoisien sur $\mathbb{Q}$, le groupe $\mathbb{Q} \otimes_{\mathbb{Z}} E_K^S$ est un module noethérien sur l'algèbre de Galois dont le caractère χ^S est connu depuis Herbrand :

PROPOSITION II.1.18.- Soient K/F une extension galoisienne de corps de nombres, $G = \mathrm{Gal}\,(K/F)$ son groupe de Galois, et S un ensemble fini de places de F, contenant les places archimédiennes. Pour chaque $\mathfrak{p}$ de S, désignons par $\chi_{\mathfrak{p}}$ l'induit à G du caractère de la représentation unité du sous-groupe de décomposition $D_{\mathfrak{P}}$ de l'une quelconque des places de K au-dessus de $\mathfrak{p}$; notons enfin χ_S la somme des $\chi_{\mathfrak{p}}$, lorsque $\mathfrak{p}$ décrit S. Le caractère du $\mathbb{Q}[G]$-module $\mathbb{Q} \otimes_{\mathbb{Z}} E_K^S$ construit sur les S-unités de K est donné par la formule :

$$\chi^S = \chi_S - 1 = \sum_{\mathfrak{p} \in S} \chi_{\mathfrak{p}} - 1.$$

Nous disons que χ^S est le caractère du groupe des S-unités dans l'extension K/F.

Démonstration : Le cas des unités, où S se réduit aux places archimédiennes, constitue le théorème de Herbrand proprement dit (cf. [He]). La proposition s'en déduit facilement, puisque, si S' est réunion de S et d'une place $\mathfrak{p}$, le quotient $E_K^{S'}/E_K^S$ s'identifie au sous-groupe principal du groupe $Id_K(\mathfrak{p})$ des idéaux de K construits sur les premiers au-dessus de $\mathfrak{p}$. Il vient donc :

$$\mathbb{Q} \otimes_{\mathbb{Z}} (E_K^{S'}/E_K^S) \simeq \mathbb{Q} \otimes_{\mathbb{Z}} Id_K(\mathfrak{p}) \simeq \mathbb{Q}[G/D_{\mathfrak{P}}],$$

puisque G opère transitivement sur les places de K au-dessus de $\mathfrak{p}$; d'où, comme attendu :

$$\chi^{S'} = \chi^S + \chi_{\mathfrak{p}}.$$

Introduisons maintenant le tensorisé ℓ-adique $\mathcal{E}_K^S = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K^S$ du groupe des S-unités. D'après le théorème 7, nous pouvons énoncer directement la proposition :

PROPOSITION II.1.19.- Soient $K/\mathbb{Q}$ une extension galoisienne du corps des rationnels, et S un ensemble fini de places de $\mathbb{Q}$ contenant la place à l'infini. Sous la conjecture énoncée plus haut, le caractère du $\mathbb{Z}_\ell$-module $\mathcal{L}og_\ell\, \mathcal{E}_K^S$ construit sur les S-unités du corps K (i.e. le caractère de l'action du groupe de Galois Gal $(K/\mathbb{Q})$ sur le $\mathbb{Q}_\ell$-espace vectoriel $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathcal{L}og_\ell\, \mathcal{E}_K^S$) est donné par la formule :

$$\chi_\ell^S = \chi^S \wedge \chi_{\text{rég}}, \quad \text{si } \ell \notin S ;$$

$$\chi_\ell^S = (\chi^S - 1) \wedge \chi_{\text{rég}}, \quad \text{si } \ell \in S.$$

<u>COROLLAIRE II.1.20</u>.- Lorsque l'ensemble S ne contient pas ℓ, le noyau $\mathcal{E}_{K,\infty}^S$ de l'application naturelle du groupe $\mathcal{E}_K^S = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K^S$ des S-unités généralisées dans le groupe $\mathcal{U}_\ell = \mathcal{U}_{K,\ell}$ des unités principales semi-locales du corps K, est un $\mathbb{Z}_\ell[G]$-module (*) dont le caractère χ_∞^S est donné, sous la conjecture précédente, par la formule :

$$\chi_\infty^S = \chi^S - (\chi^S \wedge \chi_{\text{rég}}).$$

<u>Remarque</u>.- Le corollaire 20 et la proposition précédente valent, indépendamment de la conjecture énoncée, dans deux cas particuliers importants :

(i) Si les sous-groupes de décomposition des places de S sont distingués et à quotient abélien : Dans ce cas, les caractères absolument irréductibles représentés dans χ^S le sont une fois et une seule dans le caractère régulier, et le théorème 12 assure la conclusion. De fait la condition requise sur les groupes de décomposition s'interprète comme suit : Il existe un sous-corps F de K, abélien sur $\mathbb{Q}$, tel que les places de S ne se décomposent pas dans l'extension relative K/F. Comme S contient par hypothèse les places archimédiennes, cela implique en particulier, que K est soit une extension abélienne de $\mathbb{Q}$, soit une extension quadratique totalement imaginaire d'un corps abélien réel.

(ii) Si l'ensemble S est assez grand ; ce qui peut s'entendre dans deux sens :

- En un sens arithmétique : Soit $u \in \mathcal{U}_\ell$ une unité semi-locale engendrant un $\mathbb{Z}_\ell[G]$-module $\mathcal{U}'$ d'indice fini dans $\mathcal{U}_\ell$; choisissons m

(*) Nous disons que $\mathcal{E}_{K,\infty}^S$ est le groupe des S-unités infinitésimales du corps K.