J. reine angew. Math. **404** (1990), 39—76

Journal für die reine und angewandte Mathematik

Étude heuristique des groupes de classes des corps de nombres

Par *Henri Cohen* et *Jacques Martinet* à Talence*)

§ 1. Introduction

Le problème de la répartition des nombres de classes et des groupes de classes d'idéaux de corps de nombres se pose depuis Gauss. Bien que l'on ait fait de remarquables découvertes dans ce domaine (par exemple le théorème de Brauer-Siegel et le théorème de Goldfeld-Gross-Zagier), on peut raisonnablement affirmer que l'on ne connait presque rien. Par exemple on ne sait pas s'il existe des groupes de classes de corps quadratiques imaginaires avec un p-rang arbitrairement grand (sauf bien sûr pour $p=2$), ou s'il existe une infinité de corps quadratiques réels de nombre de classes égal à 1.

En faisant certaines hypothèses heuristiques sur la répartition des groupes de classes, [C-L] donnent des résultats conjecturaux sur ces groupes, essentiellement dans le cas des corps quadratiques. Le but du présent article est de généraliser ces conjectures à des extensions quelconques de corps de nombres. Les résultats numériques correspondants pour tous les types d'extensions de degré inférieur ou égal à 4 de $\mathbb{Q}$ ont déjà été publiés dans [C-M 2].

Comme dans [C-L], pour formuler des conjectures raisonnables il est nécessaire d'enlever aux groupes considérés les p-composantes pour certains "mauvais" nombres premiers p. La situation est la suivante:

Soit L/K_0 une extension de corps de nombres de clôture galoisienne K/K_0 et de groupe de Galois $\Gamma=\mathrm{Gal}(K/K_0)$. Nous verrons qu'il est possible de comparer le groupe des classes relatives Cl_{L/K_0} avec le groupe $e\mathrm{Cl}_{K/K_0}$, où e est un idempotent de l'algèbre de groupe $\mathbb{Q}[\Gamma]$ lié à la représentation de permutation de Γ correspondant à L/K_0 (cf. § 7).

Une fois Cl_{K/K_0} débarassé de certaines "mauvaises" p-composantes, le groupe abélien fini $G=e\mathrm{Cl}_{K/K_0}$ peut être muni d'une structure de $\mathfrak{O}$-module, où $\mathfrak{O}$ est un ordre maximal de la $\mathbb{Q}$-algèbre semi-simple $A=e\mathbb{Q}[\Gamma]$ contenant $e\mathbb{Z}[\Gamma]$. On est alors ramené à une situation semblable à [C-L].

Le plan de l'article est le suivant: dans les paragraphes 2 à 5, nous développons les outils combinatoires et analytiques nécessaires à la généralisation des principes de [C-L]. Tous les résultats de ces paragraphes (ainsi que ceux du § 7) sont des théorèmes, et non des conjectures.

*) Unité de Recherche Associée du C.N.R.S. nº 226.

Il est intéressant de noter que, comme dans [C-L], la fonction analytique de base (que nous avons notée $Z(s)$) est intimement liée à la fonction zêta de l'algèbre semi-simple A. Nous renvoyons à [Deu] pour tout ce qui concerne les algèbres semi-simples et leur arithmétique.

Dans le paragraphe 6, nous énonçons l'hypothèse heuristique fondamentale qui généralise les deux hypothèses heuristiques de [C-L]. Il s'agit d'une égalité conjecturale entre la moyenne d'une fonction définie sur les groupes de classes d'une part, et la moyenne de cette fonction sur les $\mathfrak{O}$-modules finis relativement à une certaine "mesure" d'autre part (voir le paragraphe 6 pour un énoncé correct). Cette dernière moyenne est calculable analytiquement en pratique.

Dans le paragraphe 7 on montre comment relier les groupes Cl_{L/K_0} et $e\mathrm{Cl}_{K/K_0}$ et on discute la notion de "bonne" p-composante.

Enfin le paragraphe 8 regroupe un certain nombre de conséquences, commentaires et généralisations possibles.

Nous serons malheureusement obligés d'introduire de nombreuses notations. Nous utiliserons en particulier les deux notations suivantes (différentes de celles utilisées dans [C-L]):

* si E est un ensemble fini $|E|$ désigne le cardinal de E,

* si $q \neq 0$ on pose pour $n \in \mathbb{Z}$: $(n)_q = \prod_{1 \leqq k \leqq n} (1-q^{-k})$ si $n \geqq 0$,

$(n)_q = \infty$ si $n < 0$

(on peut en fait définir ce symbole pour $n \in \mathbb{C}$ quelconque mais nous n'en ferons pas usage).

Nous avons eu avec J.-F. Jaulent, G. Henniart, H. W. Lenstra, J. Oesterlé, J.-P. Serre et M. Taylor des discussions fructueuses qui nous ont beaucoup éclairées; nous les en remercions. Nous remercions également D. A. Buell, G. Fung, D. Shanks et H. C. Williams qui nous ont fourni ou fait connaître des données numériques très utiles.

§ 2. Dénombrement d'homomorphismes

Comme dans le paragraphe 1, A désigne une $\mathbb{Q}$-algèbre semisimple; on note $(e_i)_{1 \leqq i \leqq m}$ ses idempotents centraux irréducibles, et $A_i = Ae_i$ ses facteurs simples. L'algrèbre A s'identifie donc au produit $\prod_{i=1}^{m} A_i$, et chaque algèbre A_i est isomorphe à une algèbre de matrices $M_{l_i}(D_i)$ où D_i est un corps gauche de rang fini sur $\mathbb{Q}$ dont le centre est un corps de nombres K_i. On pose

$$d_i^2 = [D_i : K_i] \quad \text{et} \quad h_i^2 = [A_i : K_i]; \quad \text{donc,} \quad h_i = l_i d_i \quad \text{avec} \quad l_i \in \mathbb{Z}.$$

Le centre K de A est une algèbre étale qui s'identifie au produit des K_i. L'anneau $\mathbb{Z}_K$ des entiers de K s'identifie au produit des anneaux $\mathbb{Z}_{K_i}$, et ses idéaux maximaux sont en bijection avec les couples $(i, \mathfrak{p})$, où $i \in [1, m]$ et $\mathfrak{p}$ est un idéal maximal de $\mathbb{Z}_{K_i}$.

Etant donné un tel couple $(i, \mathfrak{p})$, la complétion de A en $(i, \mathfrak{p})$ (ou, ce qui revient au même, de A_i en $\mathfrak{p}$) est l'algèbre

$$A_{i,\mathfrak{p}} = K_{i,\mathfrak{p}} \otimes A_i,$$

où $K_{i,\mathfrak{p}}$ désigne le complété de K_i en $\mathfrak{p}$. C'est une $K_{i,\mathfrak{p}}$-algèbre centrale simple de rang h_i^2; elle est donc isomorphe à une algèbre de matrices $M_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}})$ où $D_{i,\mathfrak{p}}$ est un corps gauche de centre $K_{i,\mathfrak{p}}$. Comme dans la situation globale, on pose

$$d_{i,\mathfrak{p}}^2 = [D_{i,\mathfrak{p}} : K_{i,\mathfrak{p}}], \quad \text{donc} \quad h_i = l_{i,\mathfrak{p}}\, d_{i,\mathfrak{p}}.$$

Remarque 2. 1. Le corps gauche $D_{i,\mathfrak{p}}$ n'est pas nécessairement le complété de D_i en $\mathfrak{p}$, mais $D_i \otimes K_{i,\mathfrak{p}}$ peut être identifié à

$$M_{d_i/d_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}}).$$

Pour tout $\mathfrak{p}$, on a $d_{i,\mathfrak{p}} | d_i$ et $l_i | l_{i,\mathfrak{p}}$. D'autre part $d_{i,\mathfrak{p}} = 1$ (donc $l_{i,\mathfrak{p}} = h_i$) pour presque tout $\mathfrak{p}$, et d_i est le PPCM des $d_{i,\mathfrak{p}}$, donc l_i est le PGCD des $l_{i,\mathfrak{p}}$ (cf. [Deu]).

Donnons nous maintenant un ordre maximal $\mathfrak{O}$ de A (ou plus généralement un ordre maximal de A relativement à un localisé de $\mathbb{Z}$), et soient $\mathfrak{O}_i = \mathfrak{O} e_i$ ses composantes sur les facteurs simples de A. Si M est un $\mathfrak{O}$-module à gauche, on note encore $M_i = e_i M$ ses composantes sur les facteurs simples de A; chaque M_i est muni canoniquement d'une structure de $\mathfrak{O}_i$-module.

Par complétion, on associe à $\mathfrak{O}$ des ordres maximaux $\mathfrak{O}_{i,\mathfrak{p}}$ de $A_{i,\mathfrak{p}}$ (relativement au complété $B_{i,\mathfrak{p}}$ de $\mathbb{Z}_{K_i}$ en $\mathfrak{p}$), et à M des $\mathfrak{O}_{i,\mathfrak{p}}$-modules $M_{i,\mathfrak{p}}$. Le corps gauche $D_{i,\mathfrak{p}}$ contient un unique ordre maximal, noté $\mathfrak{o}_{i,\mathfrak{p}}$, et l'on peut choisir l'isomorphisme de $A_{i,\mathfrak{p}}$ sur $M_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}})$ de façon que $\mathfrak{O}_{i,\mathfrak{p}}$ ait pour image $M_{l_{i,\mathfrak{p}}}(\mathfrak{o}_{i,\mathfrak{p}})$. En outre, $\mathfrak{o}_{i,\mathfrak{p}}$ contient un unique idéal à gauche maximal, noté $\mathfrak{p}'$; c'est un idéal bilatère de $\mathfrak{o}_{i,\mathfrak{p}}$.

Notons que $\mathfrak{o}_{i,\mathfrak{p}}/\mathfrak{p}'$ est une extension de degré $d_{i,\mathfrak{p}}$ du corps fini $B_{i,\mathfrak{p}}/\mathfrak{p} B_{i,\mathfrak{p}}$ (où $B_{i,\mathfrak{p}}$ est comme ci-dessus le complété de $\mathbb{Z}_{K_i}$ en $\mathfrak{p}$), donc que

$$q = N\mathfrak{p}' = |\mathfrak{o}_{i,\mathfrak{p}}/\mathfrak{p}'| = |B_{i,\mathfrak{p}}/\mathfrak{p} B_{i,\mathfrak{p}}|^{d_{i,\mathfrak{p}}} = |\mathbb{Z}_{K_i}/\mathfrak{p}|^{d_{i,\mathfrak{p}}};$$

donc

$$q = N\mathfrak{q}' = (N\mathfrak{p})^{d_{i,\mathfrak{p}}}.$$

Ces notations étant introduites, nous pouvons en arriver au but de ce paragraphe: si P est un $\mathfrak{O}$-module (à gauche) projectif de type fini, et si G est un $\mathfrak{O}$-module fini, nous voulons calculer les cardinaux suivants:

$$|\mathrm{Hom}_{\mathfrak{O}}(P, G)|, \quad |\mathrm{Hom}_{\mathfrak{O}}^{s}(P, G)|, \quad |\mathrm{Aut}_{\mathfrak{O}}(G)|,$$

où $\mathrm{Hom}_{\mathfrak{O}}^{s}(P, G)$ est le sous-ensemble de $\mathrm{Hom}_{\mathfrak{O}}(P, G)$ formé des homomorphismes surjectifs. Pour cela, nous avons besoin des définitions suivantes:

Définition 2. 2. (i) Soit V un A-module de type fini. On appelle *rang de* V, et on note $\underline{u}(V)$, le m-uplet $(u_1(V_1), \ldots, u_m(V_m)) \in \mathbb{Q}^m$ où:

$$u_i(V_i) = \frac{1}{h_i^2} \dim_{K_i}(V_i).$$

(ii) Soit P un $\mathfrak{O}$-module projectif de type fini. On appelle *rang de* P, et on note encore $\underline{u}(P)$, le rang du A-module $\mathbb{Q} \otimes P$.

Définition 2. 3. Soit G un $\mathfrak{O}$-module fini, soient G_i ses composantes, et pour tout $\mathfrak{p}$ soit $G_{i,\mathfrak{p}}$ le sous-module de G_i formé des éléments dont l'annulateur est une puissance de $\mathfrak{p}$; $G_{i,\mathfrak{p}}$ est canoniquement muni d'une structure de $\mathfrak{o}_{i,\mathfrak{p}}$-module.

(i) On appelle $\mathfrak{p}'$-*rang de* G_i le nombre rationnel

$$r_{\mathfrak{p}'}(G_i) = \frac{1}{h_i^2} \dim_{\mathfrak{o}_{i,\mathfrak{p}}/\mathfrak{p}'}(G_{i,\mathfrak{p}}/\mathfrak{p}' G_{i,\mathfrak{p}}).$$

(ii) On appelle $\mathfrak{p}$-*rang de* G_i le nombre rationnel

$$r_{\mathfrak{p}}(G_i) = d_{i,\mathfrak{p}}^2 \, r_{\mathfrak{p}'}(G_i).$$

Remarque 2. 4. Lorsque le corps gauche D_i est réduit à son centre ($d_i = 1$), il est inutile de compléter pour la définition 2. 3: les $\mathfrak{p}$-rangs et $\mathfrak{p}'$-rangs coïncident et sont égaux à $\dim_{\mathbb{Z}_{K_i}/\mathfrak{p}}(G_i/\mathfrak{p} G_i)$.

Notons tout de suite la proposition suivante, qui résultera de la démonstration du théorème 2. 6.

Proposition 2. 5. (i) *On a* $l_i u_i(P) \in \mathbb{Z}$ (*donc* $h_i u_i(P) \in d_i \mathbb{Z}$).

(ii) *On a* $l_i r_{\mathfrak{p}}(G_i) \in \mathbb{Z}$ (*donc* $h_i r_{\mathfrak{p}}(G_i) \in d_i \mathbb{Z}$).

Nous pouvons maintenant énoncer:

Théorème 2. 6. *Avec les notations ci-dessus, on a*

$$|\mathrm{Hom}_{\mathfrak{O}}(P, G)| = \prod_{i=1}^{m} |G_i|^{u_i(P_i)}.$$

(*Nous noterons souvent* $|G|^{\underline{u}(P)}$ *cette dernière expression.*)

Démonstration. On se ramène immédiatement au cas où A est simple (i.e. $m = 1$) et où G est annulé par une puissance d'un idéal premier $\mathfrak{p}$ du centre K de A. Après complétion en $\mathfrak{p}$, on peut alors supposer que $\mathfrak{O}$ est un ordre au-dessus d'un anneau de valuation discrète B ayant pour corps des fractions K, et identifier A à une algèbre $M_l(D)$ (où D est un corps gauche de centre K) de façon que $\mathfrak{O}$ s'identifie à l'anneau $M_l(\mathfrak{o})$ des matrices carrées d'ordre l à coefficients dans l'unique ordre maximal $\mathfrak{o}$ de D. On note $\mathfrak{p}'$ l'idéal maximal de $\mathfrak{o}$.

Puisque P est projectif, l'application qui à

$$\varphi \in \mathrm{Hom}_{\mathfrak{O}}(P, G)$$

associe l'élément

$$\bar{\varphi} \in \mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P, G/\mathfrak{p}'G)$$

déduite de φ par passage au quotient, est surjective, et son noyau est clairement $\mathrm{Hom}_{\mathfrak{O}}(P, \mathfrak{p}'G)$. On a donc:

$$(1) \qquad |\mathrm{Hom}_{\mathfrak{O}}(P, G)| = |\mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P, G/\mathfrak{p}'G)|\,|\mathrm{Hom}_{\mathfrak{O}}(P, \mathfrak{p}'G)|.$$

Par récurrence, on en déduit que:

$$(2) \qquad |\mathrm{Hom}_{\mathfrak{O}}(P, G)| = \prod_{k \geqq 0} |\mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P, \mathfrak{p}'^{k}G/\mathfrak{p}'^{k+1}G)|.$$

Pour pouvoir continuer, il nous faut des renseignements sur les structures de $\mathfrak{O}$-modules de P et de G. Pour tout anneau R, notons $M_{l,c}(R)$ le $M_l(R)$-module à gauche formé des matrices à l lignes et c colonnes à coefficients dans R. On a alors:

Lemme 2. 7. (i) *Si P est un $\mathfrak{O}$-module projectif de type fini, alors P est $\mathfrak{O}$-isomorphe à $M_{l,v}(\mathfrak{o})$ avec $v = lu(P)$.*

(ii) *Si G est un $\mathfrak{O}$-module fini annulé par une puissance de $\mathfrak{p}$ (ou de $\mathfrak{p}'$, cela revient au même), alors G est $\mathfrak{O}$-isomorphe à $M_{l,n}(\mathfrak{o})/I$, où I est le sous-module de $M_{l,n}(\mathfrak{o})$ formé des matrices de la forme*

$$l \text{ lignes} \quad \begin{pmatrix} \mathfrak{p}'^{m_1} \cdots \mathfrak{p}'^{m_n} \\ \mathfrak{p}'^{m_1} \cdots \mathfrak{p}'^{m_n} \end{pmatrix} \quad (m_i \text{ entiers} > 0),$$

et on a $n = lr_{\mathfrak{p}}(G)$.

Démonstration. (i) Rappelons que $\mathfrak{O} = M_l(\mathfrak{o})$. En décomposant P en somme directe de modules irréductibles on voit que

$$P \cong \begin{pmatrix} \mathfrak{a}_1 \cdots \mathfrak{a}_v \\ \mathfrak{a}_1 \cdots \mathfrak{a}_v \end{pmatrix} \quad (l \text{ lignes}, \ \mathfrak{a}_i \neq 0)$$

où les $\mathfrak{a}_i$ sont des idéaux de $\mathfrak{o}$, donc principaux, d'où l'isomorphisme avec $M_{l,v}(\mathfrak{o})$. On a

$$u(P) = \frac{1}{h^2}\dim_K(\mathbb{Q} \otimes P) = \frac{1}{h^2}\dim_K(M_{l,v}(D))$$

$$= \frac{d^2 lv}{h^2} = \frac{v}{l},$$

d'où (i).

Puisque l_i est le PGCD des $l_{i,\mathfrak{p}}$, cela montre également le (i) de la proposition 2. 5 (qu'on aurait également pu obtenir directement par localisation, sans compléter).

(ii) L'isomorphisme avec un $M_{l,n}(\mathfrak{o})/I$ résulte de la structure énoncée ci-dessus pour les $\mathfrak{O}$-modules projectifs. Quant à la valeur de n, on a

$$r_{\mathfrak{p}}(G)=\frac{d^2}{h^2}\dim_{\mathfrak{o}/\mathfrak{p}'}(G/\mathfrak{p}'G)=\frac{d^2 ln}{h^2}=\frac{n}{l},$$

d'où le lemme.

Pour la suite, nous poserons

$$\mathbb{F}_q=\mathfrak{o}/\mathfrak{p}', \quad \text{où} \quad q=N\mathfrak{p}'.$$

Corollaire 2. 8. *En tant que $M_l(\mathbb{F}_q)$-modules à gauche, on a*

$$P/\mathfrak{p}'P\cong M_{l,v}(\mathbb{F}_q),$$
$$G/\mathfrak{p}'G\cong M_{l,n}(\mathbb{F}_q)$$

avec $v=lu(P)$, $n=lr_{\mathfrak{p}}(G)$.

Proposition 2. 9. *L' application*

$$M_{v,n}(\mathbb{F}_q)\to \mathrm{Hom}_{M_l(\mathbb{F}_q)}(M_{l,v}(\mathbb{F}_q), M_{l,n}(\mathbb{F}_q)),$$
$$m\mapsto (x\mapsto xm)$$

est un isomorphisme de $\mathbb{F}_q$-espaces vectoriels.

La démonstration de cette proposition est très facile et laissée au lecteur.

On déduit donc de ce qui précède que

$$|\mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P,\ G/\mathfrak{p}'G)|=|M_{v,n}(\mathbb{F}_q)|=q^{vlr_{\mathfrak{p}}(G)}.$$

Or, $lr_{\mathfrak{p}}(\mathfrak{p}'^kG)$ représente le nombre de $m_i>k$ dans le lemme 2. 7, et on a donc

$$\sum_{k\geqq 0} lr_{\mathfrak{p}}(\mathfrak{p}'^kG)=\sum_{i=1}^{n} m_i,$$

d'où:

$$|G|^{u(P)}=|G|^{v/l}=q^{v\sum_{i=1}^{n} m_i}=q^{\sum_{k\geqq 0} vlr_{\mathfrak{p}}(\mathfrak{p}'^kG)}$$
$$=\prod_{k\geqq 0}|\mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P,\ \mathfrak{p}'^kG/\mathfrak{p}'^{k+1}G)|$$
$$=|\mathrm{Hom}_{\mathfrak{O}}(P,\ G)|,$$

d'où le théorème 2. 6.

Théorème 2. 10. *Rappelons que l'on pose*:

$$(n)_q=\prod_{1\leqq k\leqq n}(1-q^{-k}) \quad \textit{pour} \quad n\geqq 0,\ (n)_q=\infty \quad \textit{si} \quad n<0.$$

Le nombre d'homomorphismes surjectifs de P dans G est donné par la formule

$$|\mathrm{Hom}^s_{\mathfrak{O}}(P, G)| = \prod_{i=1}^{m} \left[|G_i|^{u_i(P_i)} \prod_{\mathfrak{p} \subset \mathbb{Z}_{K_i}} (l_{i,\mathfrak{p}}\, u_i(P))_q / (l_{i,\mathfrak{p}}(u_i(P) - r_{\mathfrak{p}}(G_i)))_q \right]$$

où $q = N\mathfrak{p}^{d_{i,\mathfrak{p}}}$ et où $\mathfrak{p}$ parcourt les idéaux maximaux de $\mathbb{Z}_{K_i}$. Noter que ce produit est fini puisque $r_{\mathfrak{p}}(G_i) = 0$ pour presque tout $\mathfrak{p}$.

Démonstration. On suit pas à pas la démonstration du théorème 2. 6 en se limitant aux homomorphismes surjectifs. Les mêmes réductions étant faites, le lemme de Nakayama montre que $\varphi \in \mathrm{Hom}_{\mathfrak{O}}(P, G)$ est surjectif si et seulement si

$$\bar{\varphi} \in \mathrm{Hom}_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P, G/\mathfrak{p}'G)$$

est surjectif. L'analogue de la formule (1) est alors

$$(3) \qquad |\mathrm{Hom}^s_{\mathfrak{O}}(P, G)| = |\mathrm{Hom}^s_{\mathfrak{O}/\mathfrak{p}'\mathfrak{O}}(P/\mathfrak{p}'P, G/\mathfrak{p}'G)|\, |\mathrm{Hom}_{\mathfrak{O}}(P, \mathfrak{p}'G)|.$$

(Il n'y a *pas* de condition de surjectivité dans $\mathrm{Hom}_{\mathfrak{O}}(P, \mathfrak{p}'G)$.)

D'après le théorème 2. 6, on a

$$(4) \qquad |\mathrm{Hom}_{\mathfrak{O}}(P, \mathfrak{p}'G)| = |\mathfrak{p}'G|^{u(P)} = \left(\frac{|G|}{|G/\mathfrak{p}'G|}\right)^{u(P)}$$

$$= \left(\frac{|G|}{|M_{l,n}(\mathbb{F}_q)|}\right)^{u(P)} = \frac{|G|^{u(P)}}{q^{lnu(P)}} = \frac{|G|^{u(P)}}{q^{nv}}$$

d'après le corollaire 2. 8.

D'autre part en se ramenant au cas $l = 1$, il est facile de voir que les matrices $m \in M_{v,n}(\mathbb{F}_q)$ correspondant aux homomorphismes surjectifs par l'isomorphisme de la proposition 2. 9 sont celles qui définissent par multiplication à *droite* des applications surjectives de $\mathbb{F}_q^v$ sur $\mathbb{F}_q^n$, c'est-à-dire qui sont de rang n. Le nombre de telles matrices est évidemment égal à

$$(q^v - 1)(q^v - q) \cdots (q^v - q^{n-1}) = q^{nv}(v)_q / (v - n)_q$$

(même si $n > v$ puisqu'on a posé $(v - n)_q = \infty$ dans ce cas).

D'après (3) et (4), on a donc

$$|\mathrm{Hom}^s_{\mathfrak{O}}(P, G)| = |G|^{u(P)}(v)_q / (v - n)_q,$$

d'où le théorème 2. 10 puisque, d'après le lemme 2. 7,

$$v = lu(P),\ v - n = l(u(P) - r_{\mathfrak{p}}(G)).$$

Enfin nous avons:

Théorème 2. 11. *Soient* $\mathfrak{p} \subset \mathbb{Z}_{K_i}$ *un idéal maximal et* G *un* $\mathfrak{O}$*-module fini annulé par une puissance de* $\mathfrak{p}$. *Posons* $q = N\mathfrak{p}^{d_{i,\mathfrak{p}}}$. *Soient* $\mu_1, \ldots, \mu_t$ *les valeurs distinctes des* m_i *données par le lemme 2. 7, et* $k_1, \ldots, k_t$ *les multiplicités correspondantes (donc,* $\sum_{i=1}^{t} \mu_i k_i = \sum_{j=1}^{n} m_j$). *Alors,*

$$|\mathrm{Aut}_{\mathfrak{O}}(G)| = q^{\sum_{1 \leqq i,j \leqq t} \inf(\mu_i, \mu_j) k_i k_j} \prod_{i=1}^{t} (k_i)_q .$$

Remarque 2. 12. 1) Avec les notations du lemme 2. 7, l'exposant

$$\sum_{1 \leqq i,j \leqq t} \inf(\mu_i, \mu_j) k_i k_j$$

s'écrit aussi $\sum_{1 \leqq i,j \leqq n} \inf(m_i, m_j)$.

2) Si G est un $\mathfrak{O}$-module fini quelconque, il est clair que

$$|\mathrm{Aut}_{\mathfrak{O}}(G)| = \prod_{i=1}^{m} \prod_{\mathfrak{p} \subset \mathbb{Z}_{K_i}} |\mathrm{Aut}_{\mathfrak{O}}(G_{i,\mathfrak{p}})|$$

où $G_{i,\mathfrak{p}}$ désigne le sous-module de G_i formé par les éléments dont l'annulateur est une puissance de $\mathfrak{p}$, et donc le théorème 2. 11 fournit $|\mathrm{Aut}_{\mathfrak{O}}(G)|$ en toute généralité.

Démonstration. Reprenons les notations du lemme 2. 7 (ii). Comme dans la proposition 2. 9, on voit aisément que les homomorphismes de $M_{l,n}(\mathfrak{o})$ dans lui-même sont donnés par multiplication à droite avec une matrice $m \in M_n(\mathfrak{o})$.

Pour que cela induise un $\mathfrak{O}$-homomorphisme de G dans G par passage au quotient par I, il est nécessaire et suffisant que l'on ait $Im \subset I$ (puisque $M_{l,n}(\mathfrak{o})$ est projectif, noter que tout $\mathfrak{O}$-homomorphisme de G dans G s'obtient de cette façon). Si

$$m = (a_{ij})_{1 \leqq i,j \leqq n},$$

on voit que cette condition équivaut à

$$a_{ij} \in \mathfrak{p}'^{m_j - m_i} \quad \text{pour} \quad m_i < m_j .$$

Quitte à réordonner les m_i, on peut supposer que $m_1 \leqq \cdots \leqq m_n$.

On déduit immédiatement de ce qui précède que les $\mathfrak{O}$-homomorphismes de G dans G sont en $\mathfrak{o}$-isomorphisme avec le module quotient

$$(5) \qquad \begin{pmatrix} \mathfrak{o} & \mathfrak{p}'^{m_2 - m_1} & \cdots & \mathfrak{p}'^{m_n - m_1} \\ \mathfrak{o} & \mathfrak{o} & & \vdots \\ \vdots & \vdots & & \mathfrak{p}'^{m_n - m_{n-1}} \\ \mathfrak{o} & \mathfrak{o} & \cdots & \mathfrak{o} \end{pmatrix} \Big/ \begin{pmatrix} \mathfrak{p}'^{m_1} & \mathfrak{p}'^{m_2} & \cdots & \mathfrak{p}'^{m_n} \\ \vdots & \vdots & & \vdots \\ \mathfrak{p}'^{m_1} & \mathfrak{p}'^{m_2} & \cdots & \mathfrak{p}'^{m_n} \end{pmatrix}.$$

Les $\mathfrak{O}$-automorphismes correspondent aux classes modulo I de matrices dont le déterminant est inversible modulo $\mathfrak{p}'$. Avec les notations μ_i, k_i introduites dans l'énoncé, un représentant d'une telle classe, réduit modulo $\mathfrak{p}'$, est de la forme:

$$\begin{array}{c} \mathrm{k}_1 \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_1 \end{pmatrix} \\ \\ \mathrm{k}_t \begin{pmatrix} \mu_t \\ \vdots \\ \mu_t \end{pmatrix} \end{array} \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix} \quad .$$

$$\underbrace{\mu_1 \dots \mu_1}_{k_1} \quad \underbrace{\mu_2 \dots \mu_2}_{k_2} \quad \dots \quad \underbrace{\mu_t \dots \mu_t}_{k_t}$$

On en déduit que le nombre de telles matrices inversibles, modulo $\mathfrak{p}'$, vaut

$$q^{\sum_{1 \leqq i < j \leqq t} k_i k_j} \prod_{i=1}^{t} |\mathrm{GL}_{k_i}(\mathbb{F}_q)|$$

$$= q^{\sum_{1 \leqq i \leqq j \leqq t} k_i k_j} \prod_{i=1}^{t} (k_i)_q .$$

Or, le nombre d'éléments de $\mathfrak{o}/\mathfrak{p}'^{\mu_i}$ qui se réduisent modulo $\mathfrak{p}'$ en un élément donné de $\mathbb{F}_q = \mathfrak{o}/\mathfrak{p}'$ est égal à $q^{\mu_i - 1}$, et le nombre d'éléments de $\mathfrak{p}'^{\mu_j - \mu_i}/\mathfrak{p}'^{\mu_j}$ (pour $i < j$) qui se réduisent à 0 modulo $\mathfrak{p}'$ est égal à q^{μ_i}.

Il en résulte que le nombre de matrices dans le module quotient (5) qui modulo $\mathfrak{p}'$ se réduisent en une matrice donnée comme ci-dessus est égal à

$$q^{\sum_{1 \leqq i, j \leqq t} \inf(\mu_i, \mu_j) k_i k_j - \sum_{1 \leqq i \leqq j \leqq t} k_i k_j} .$$

Multipliant ceci par le nombre de matrices possibles modulo $\mathfrak{p}'$ fournit bien le théorème 2. 11.

§ 3. La fonction Z d'une $\mathbb{Q}$-algèbre semi-simple

Soient A une $\mathbb{Q}$-algèbre semi-simple, m le nombre de composantes simples de A. Dans ce paragraphe, nous allons associer à A une fonction $Z^A(\underline{s})$ de m variables complexes, qui s'exprime comme produit eulérien des fonctions locales associées aux algèbres simples sur les complétés des corps de nombres aux places finies. Ces diverses fonctions sont liées aux fonctions zêta correspondantes.

On conserve les notations du paragraphe 2. En particulier, $\mathfrak{O}$ est un ordre maximal de A, la lettre P désigne toujours un $\mathfrak{O}$-module projectif de type fini, et la lettre G un $\mathfrak{O}$-module fini. Si $\underline{u}, \underline{v} \in \mathbb{R}^m$, la notation "$\underline{u} > \underline{v}$" signifie que $\forall i, u_i > v_i$, et l'expression $\underline{u} \to \underline{\infty}$ signifie que $\forall i, u_i \to \infty$.

Nous avons vu (théorème 2. 10) que le nombre d'homomorphismes surjectifs de P dans G ne dépend de P qu'à travers son rang $\underline{u}(P)$. Cela justifie la définition suivante:

Definition 3. 1. (i) Soit $\underline{u}$ le rang d'un $\mathfrak{O}$-module projectif de type fini P. On pose

$$s_{\underline{u}}(G) = |\mathrm{Hom}^s_{\mathfrak{O}}(P, G)| \quad \text{et} \quad w_{\underline{u}}(G) = \frac{s_{\underline{u}}(G)}{|\mathrm{Aut}_{\mathfrak{O}}(G)|\,|G|^{\underline{u}}}.$$

(ii) On pose

$$w_{\underline{\infty}}(G) = w(G) = \frac{1}{|\mathrm{Aut}_{\mathfrak{O}}(G)|}.$$

Les rangs $\underline{u}$ de $\mathfrak{O}$-modules projectifs de type fini, ainsi que $\underline{\infty}$, seront appelés multi-indices *admissibles.*

Noter qu'il résulte encore du théorème 2. 10 que:

$$w_{\underline{\infty}}(G) = \lim_{\underline{u} \to \underline{\infty}} w_{\underline{u}}(G),$$

ce qui justifie la notation.

Proposition 3. 2. *Soient P un $\mathfrak{O}$-module projectif de rang $\underline{u}$ et G un $\mathfrak{O}$-module fini. Alors*

$$|\{Q \subset P : P/Q \cong G\}| = |G|^{\underline{u}} w_{\underline{u}}(G),$$

où la notation $Q \subset P$ signifie que Q est un sous-$\mathfrak{O}$-module de P, et où l'isomorphisme est un isomorphisme de $\mathfrak{O}$-modules.

Démonstration. L'ensemble des $Q \subset P$ tels que $P/Q \cong G$ est en bijection avec l'ensemble des noyaux des homomorphismes surjectifs de P dans G. Or, deux tels homomorphismes surjectifs φ_1 et φ_2 ont même noyau si et seulement si il existe un automorphisme σ de G tel que

$$\varphi_2 = \sigma \circ \varphi_1.$$

Le cardinal cherché vaut donc

$$s_{\underline{u}}(G)/|\mathrm{Aut}_{\mathfrak{O}}(G)|,$$

d'où la proposition.

Proposition 3. 3. *Soient G_1 et G_2 deux $\mathfrak{O}$-modules finis. Pour tout $\underline{u}$ admissible, on a:*

$$\sum_{G/\sim} w_{\underline{u}}(G)|\{H \subset G : H \cong G_1 \text{ et } G/H \cong G_2\}| = w_{\underline{u}}(G_1)\, w_{\underline{u}}(G_2).$$

(*La notation $G/\sim$ signifie que G est pris à $\mathfrak{O}$-isomorphisme près.*)

Démonstration. La somme étant finie, le cas $\underline{u} = \underline{\infty}$ résulte du cas $\underline{u} \neq \underline{\infty}$, par passage à la limite. Si $\underline{u} \neq \underline{\infty}$, soit P un $\mathfrak{O}$-module projectif de rang $\underline{u}$. Comme dans [C-L], théorème 3. 5, on compte de deux façons différentes le nombre de couples (P_1, P_2) de sous-modules de P avec

$$P/P_2 \cong G_2 \quad \text{et} \quad P_2/P_1 \cong G_1$$

en utilisant la proposition 3. 2.

Définition 3. 4. Pour tout multi-indice admissible $\underline{u}$ et tout idéal maximal $\mathfrak{p} \subset \mathbb{Z}_{K_i}$, on pose, sous réserve de convergence:

$$Z_{\underline{u}}^{A,\mathfrak{p}}(\underline{s}) = \sum_{G/\sim} w_{\underline{u}}(G)|G|^{-\underline{s}}$$

(où G parcourt les classes d'isomorphismes annulées par une puissance de $\mathfrak{p}$), et

$$Z_{\underline{u}}^{A}(\underline{s}) = \sum_{G/\sim} w_{\underline{u}}(G)|G|^{-\underline{s}}$$

où $\underline{s} \in \mathbb{C}^m$.

Remarque 3. 5. 1) A priori, on devrait écrire $Z_{\underline{u}}^{\mathfrak{O},\mathfrak{p}}$ et $Z_{\underline{u}}^{\mathfrak{O}}$ à la place de $Z_{\underline{u}}^{A,\mathfrak{p}}$ et $Z_{\underline{u}}^{A}$. Nous verrons ci-dessous que ces définitions ne dépendent pas de l'ordre maximal $\mathfrak{O}$ de A que l'on choisit, ce qui justifie les notations.

2) On écrira souvent $Z^{A,\mathfrak{p}}(\underline{s})$ et $Z^{A}(\underline{s})$ à la place de $Z_{\underline{\infty}}^{A,\mathfrak{p}}(\underline{s})$ et $Z_{\underline{\infty}}^{A}(\underline{s})$. De plus, si cela ne prête pas à confusion, nous omettrons l'indication de la $\mathbb{Q}$-algèbre A dans la notation.

Théorème 3. 6. *Sous les hypothèses de la définition* 3. 4 *on a:*

(i) $$Z_{\underline{u}}^{\mathfrak{p}}(\underline{s}) = \prod_{1 \leqq j \leqq l_{i,\mathfrak{p}} u_i} \left(1 - (N\mathfrak{p})^{-(h_i s_i + j d_{i,\mathfrak{p}})}\right)^{-1}.$$

(ii) $$Z_{\underline{u}}(\underline{s}) = \prod_{i=1}^{m} \prod_{\mathfrak{p} \subset \mathbb{Z}_{K_i}} Z_{\underline{u}}^{\mathfrak{p}}(\underline{s}) \quad \textit{pour } \mathrm{Re}(\underline{s}) > \underline{0}.$$

(iii) *Si $\underline{u}$ et $\underline{v}$ sont admissibles:*

$$Z_{\underline{u}+\underline{v}}^{\mathfrak{p}}(\underline{s}) = Z_{\underline{v}}^{\mathfrak{p}}(\underline{s}+\underline{u}) Z_{\underline{u}}^{\mathfrak{p}}(\underline{s}),$$

$$Z_{\underline{u}+\underline{v}}(\underline{s}) = Z_{\underline{v}}(\underline{s}+\underline{u}) Z_{\underline{u}}(\underline{s})$$

et en particulier

$$Z_{\underline{u}}(\underline{s}) = Z(\underline{s})/Z(\underline{s}+\underline{u}).$$

Démonstration. On peut procéder exactement comme dans le paragraphe 3 de [C-L]: on établit une formule pour $s_{\underline{u}+\underline{v}}(G)$ qui, combinée avec la proposition 3. 3, démontre (iii). Puis on calcule explicitement $Z^{\mathfrak{p}}_{1/l_{i,\mathfrak{p}}}(\underline{s})$, ce qui donne (i), et (ii) en résulte par linéarité.

Toutefois on peut raisonner tout à fait autrement: avec les notations du théorème 2. 11 on voit que la classe de $\mathfrak{O}$-isomorphisme de G est caractérisée par la donnée des couples $(\mu_j, k_j)_{1\leqq j\leqq t}$, et la donnée supplémentaire de $q=N\mathfrak{p}^{d_{i,\mathfrak{p}}}$ détermine $|\mathrm{Aut}_{\mathfrak{O}}(G)|$. D'autre part la formule pour le nombre $s_{\underline{u}}(G)$ ne fait intervenir que $\underline{u}$, $l_{i,\mathfrak{p}}$ et $l_{i,\mathfrak{p}}r_{\mathfrak{p}}(G)=n=\sum_{j=1}^{t} k_j$.

Enfin, $|G|=q^{(\sum k_j\mu_j)l_{i,\mathfrak{p}}}$. On a donc:

$$Z^{A,\mathfrak{p}}_{\underline{u}}(\underline{s})=F_{l_{i,\mathfrak{p}}u_i,\,l_{i,\mathfrak{p}}s_i}(q), \tag{6}$$

où

$$F_{v,s}(q)=\sum_{\substack{t\geqq 0\\ (\mu_j,k_j)_{1\leqq j\leqq t}}} \frac{(v)_q(v-\sum k_j)_q}{\prod_j (k_j)_q}\; q^{-\sum_{i,j}\inf(\mu_i,\mu_j)k_ik_j-s\sum_j k_j\mu_j}.$$

Posons $f(z)=F_{v,s}(1/z)$. Si $v>0$ et $\mathrm{Re}(s)>-1$, il est immédiat de vérifier que f est une fonction holomorphe de z dans le disque ouvert $|z|<1$ et que $f(0)=1$.

Or le corollaire 3. 7 de [C-L] nous dit que $Z^{\mathfrak{Q},\mathfrak{p}}_{v}(\underline{s})=f(1/p)=\prod_{1\leqq j\leqq v}(1-p^{-j-s})^{-1}$ pour p premier.

La fonction $g(z)=\prod_{1\leqq j\leqq v}(1-z^{j+s})^{-1}$ est clairement holomorphe pour $|z|<1$ si $v>0$ et Re $s>-1$, et égale à $f(z)$ sur l'ensemble non discret formé de 0 et des inverses des nombres premiers. Elle est donc égale à $f(z)$ pour tout $|z|<1$, ce qui donne

$$F_{v,s}(z)=\prod_{1\leqq j\leqq v}(1-z^{-j-s})^{-1}.$$

En remplaçant v, s, z par $l_{i,\mathfrak{p}}u_i$, $l_{i,\mathfrak{p}}s_i$ et $N\mathfrak{p}^{-d_{i,\mathfrak{p}}}$ on obtient le théorème 3. 6 (i), et le reste du théorème en découle aisément.

Remarque 3. 7. La démonstration ci-dessus permet également de ne pas se préoccuper de problèmes de convergence. Par exemple on voit aisément que

$$|Z^{A}_{\underline{u}}(\underline{s})|\leqq\prod_{i=1}^{m}|Z^{K_i}(h_i\,\mathrm{Re}\,(s_i))|.$$

Corollaire 3. 8. *Soient K un corps de nombres, et $u\in\frac{1}{h}\mathbb{N}$. Alors*

$$Z^{M_h(K)}_{u}(s)=Z^{K}_{hu}(hs),$$

et en particulier,

$$Z^{M_h(K)}(s)=Z^{K}(hs).$$

C'est une conséquence immédiate du théorème 3. 6 puisqu'on a ici $m=1$, $l_{\mathfrak{p}}=h$, $d_{\mathfrak{p}}=1$ pour tout $\mathfrak{p}$.

Corollaire 3. 9. *Posons* $\underline{1}=(1,\ldots,1)$

(i) $Z_{\underline{1}}^{A}(\underline{s}-\underline{1})=\zeta_A(\underline{s})$,

(ii) $Z^A(\underline{s})=\prod_{k\geq 1}\zeta_A(\underline{s}+k\underline{1})$

où par abus de notation on a écrit $\zeta_A(\underline{s})$ *à la place de* $\prod_{i=1}^{m}\zeta_{A_i}(s_i)$.

(*La fonction* $\zeta_A(s)$ *telle qu'elle est définie habituellement est une fonction d'une seule variable complexe s et vaut* $\zeta_A(s\cdot\underline{1})$ *avec nos notations.*)

Démonstration. En changeant j en $l_{i,\mathfrak{p}}-j$, on voit immédiatement que le facteur local $Z_{\underline{1}}^{A,\mathfrak{p}}(\underline{s}-\underline{1})$ vaut $\prod_{0\leq j\leq l_{i,\mathfrak{p}}-1}(1-(N\mathfrak{p})^{-(h_i s_i-jd_{i,\mathfrak{p}})})^{-1}$, ce qui est bien le facteur local de $\zeta_A(\underline{s})$ (voir [Deu]), d'où (i).

Pour (ii) on remarque que le théorème 3. 6 (iii) implique par récurrence que

$$Z^A(\underline{s})=\left(\prod_{k=0}^{r-1}Z_{\underline{1}}(\underline{s}+k\underline{1})\right)Z^A(\underline{s}+r\underline{1})$$

$$=\left(\prod_{k=1}^{r}\zeta_A(\underline{s}+k\underline{1})\right)Z^A(\underline{s}+r\underline{1}),$$

d'où (ii) puisque $\lim_{r\to\infty}Z^A(\underline{s}+r\underline{1})=1$. Remarquons d'ailleurs que la convergence absolue pour $\mathrm{Re}(\underline{s})>\underline{0}$ du produit infini $\prod_{k\geq 1}\zeta_A(\underline{s}+k\underline{1})$ provient du fait que

$$\zeta_A(\underline{s}+k\underline{1})=1+O(2^{-k}).$$

Proposition 3. 10. (i) *On a*

$$Z_{\underline{u}}^{A}(\underline{s})=\prod_{i=1}^{m}\left[\prod_{1\leq j\leq h_i u_i}\zeta_{K_i}(h_i s_i+j)E_i\right],$$

où

$$E_i=\prod_{\mathfrak{p}\subset K_i,\,d_{i,\mathfrak{p}}>1}\frac{\prod_{1\leq j\leq h_i u_i}(1-(N\mathfrak{p})^{-(h_i s_i+j)})}{\prod_{1\leq j\leq l_{i,\mathfrak{p}}u_i}(1-(N\mathfrak{p})^{-(h_i s_i+jd_{i,\mathfrak{p}})})}$$

(*le produit eulérien* E_i *est un produit fini*).

(ii) *Les fonctions $Z_{u_i}^{A_i}(s_i)$ possèdent un prolongement méromorphe à $\mathbb{C}$ tout entier. Leurs pôles sont parmi les rationnels négatifs ou nuls de dénominateur divisant h_i. En particulier le pôle en $s_i = 0$ est simple, de résidu*

$$C_{u_i}^{A_i} = \frac{1}{h_i} C_{h_i u_i}^{K_i} \prod_{\mathfrak{p} \subset K_i,\, d_{i,\mathfrak{p}} > 1} \frac{\prod_{1 \leqq j \leqq h_i u_i} (1 - (N\mathfrak{p})^{-j})}{\prod_{1 \leqq j \leqq l_{i,\mathfrak{p}} u_i} (1 - (N\mathfrak{p})^{-j d_{i,\mathfrak{p}}})}$$

avec $C_k^K = \operatorname{Res}_{s=1} \zeta_K(s) \prod_{2 \leqq j \leqq k} \zeta_K(j)$.

Démonstration. (i) résulte immédiatement du théorème 3. 6. Pour (ii), on remarque que l'énoncé est clairement vrai si $\underline{u} \neq \underline{\infty}$ d'après le prolongement analytique des fonctions ζ de Dedekind; pour $\underline{u} = \underline{\infty}$, il suffit d'utiliser le corollaire 3. 9 (ii) puisque le produit infini converge normalement sur tout compact inclus dans le complémentaire des pôles des fonctions $\zeta_{A_i}(s_i + k)$.

§ 4. Les fonctions $Z(f, s)$

On conserve les notations des paragraphes précédents.

Soit ψ une fonction définie sur l'ensemble des classes d'isomorphisme de $\mathfrak{O}$-modules finis G.

Définition 4. 1. On dira que ψ est de *type* w si ψ n'est pas identiquement nulle, et si pour tout couple (G_1, G_2) de $\mathfrak{O}$-modules finis on a

$$\sum_{G/\sim} \psi(G) |\{H \subset G : H \cong G_1 \text{ et } G/H \cong G_2\}| = \psi(G_1)\psi(G_2).$$

Par exemple, d'après la proposition 3. 3, les fonctions $w_{\underline{u}}$ pour $\underline{u}$ admissible, et en particulier la fonction $w = w_{\underline{\infty}}$, sont de type w, d'où l'appellation.

Définition 4. 2. Soit ψ de type w, et soit a une fonction définie sur les classes d'isomorphisme de $\mathfrak{O}$-modules finis. On appelle *ψ-série de Dirichlet associée à a* la série

$$Z_\psi(a, \underline{s}) = \sum_{G/\sim} \frac{\psi(G) a(G)}{|G|^{\underline{s}}}$$

sous réserve de convergence. En particulier on pose

$$Z_{\underline{u}}(a, s) = Z_{w_{\underline{u}}}(a, s) \quad \text{et} \quad Z(a, \underline{s}) = Z_{\underline{\infty}}(a, \underline{s}) = Z_w(a, \underline{s}).$$

Remarquons qu'en regroupant les $\mathfrak{O}$-modules de même cardinal on obtient une série de Dirichlet ordinaire. Toutefois, il est plus naturel de ne pas les regrouper (comme par exemple on ne regroupe pas les idéaux de même norme pour les fonctions zeta de Dedekind), mais de les considérer comme un type particulier de série de Dirichlet pour lequel il faut décrire des règles de calcul. La structure de $\mathbb{C}$-espace vectoriel est évidente mais la structure d'algèbre l'est un peu moins:

Définition 4. 3. Soient a et b deux fonctions définies sur les classes d'isomorphisme de $\mathfrak{O}$-modules finis. On appelle *$\mathfrak{O}$-convolution de a* et b, notée $a *_{\mathfrak{O}} b$, la fonction définie par:

$$(a *_{\mathfrak{O}} b)(G) = \sum_{\substack{G_1/\sim \\ G_2/\sim}} a(G_1)\, b(G_2) |\{H \subset G : H \cong G_1 \text{ et } G/H \cong G_2\}|.$$

On a alors:

Proposition 4. 4. *Soient ψ de type w et a et b deux fonctions définies sur les classes d'isomorphisme de $\mathfrak{O}$-modules finis. Sous réserve de convergence, on a*

$$Z_\psi(a *_{\mathfrak{O}} b, \underline{s}) = Z_\psi(a, \underline{s})\, Z_\psi(b, \underline{s}).$$

Démonstration immédiate.

On voit donc que le produit de ψ-séries de Dirichlet en est encore une de façon naturelle.

Exemples 4. 5. Soient ψ de type w, et G_1 et G_2 deux $\mathfrak{O}$-modules finis. Alors:

(i) Si $f(G) = |\{H \subset G : H \cong G_1 \text{ et } G/H \cong G_2\}|$, on a

$$Z_\psi(f, \underline{s}) = \frac{\psi(G_1)}{|G_1|^{\underline{s}}} \frac{\psi(G_2)}{|G_2|^{\underline{s}}}.$$

(ii) Si $f(G) = |\{H \subset G : H \cong G_1\}|$ ou $f(G) = |\{H \subset G : G/H \cong G_1\}|$, on a

$$Z_\psi(f, \underline{s}) = \frac{\psi(G_1)}{|G_1|^{\underline{s}}} Z_\psi(\underline{s}),$$

où l'on écrit $Z_\psi(\underline{s})$ à la place de $Z_\psi(1, \underline{s})$ (noter que la notation $Z_{\underline{u}}(\underline{s})$ est bien compatible avec celle donnée au paragraphe précédent).

(iii) Si $f(G) = |\{H \subset G\}|$,

$$Z_\psi(f, \underline{s}) = Z_\psi^2(\underline{s}).$$

Les démonstrations sont immédiates.

Le théorème suivant est important pour la suite.

Théorème 4. 6. *Soient ψ de type w, $\underline{u}$ un multi-indice admissible, P un $\mathfrak{O}$-module projectif de rang $\underline{u}$, et G_1 et G_2 deux $\mathfrak{O}$-modules finis.*

(i) *Sous réserve de convergence, on a*

$$\sum_{G/\sim} \frac{|\mathrm{Aut}_{\mathfrak{O}}(G)| w_{\underline{u}}(G)\, \psi(G)}{|G|^{\underline{s}}} = \frac{Z_\psi(\underline{s})}{Z_\psi(\underline{s} + \underline{u})}.$$

(ii) *Pour* $f(G)=|\{\varphi\in \mathrm{Hom}_{\mathfrak{D}}(P,G): G/\mathrm{Im}\,\varphi\cong G_1\}|$, *on a*

$$Z_\psi(f,\underline{s})=\frac{\psi(G_1)}{|G_1|^{\underline{s}}}\,\frac{Z_\psi(\underline{s}-\underline{u})}{Z_\psi(\underline{s})}.$$

(iii) *Pour* $f(G)=\sum_{\varphi\in \mathrm{Hom}_{\mathfrak{D}}(P,G)}|\{H\subset G/\mathrm{Im}\,\varphi: H\cong G_1 \text{ et } (G/\mathrm{Im}\,\varphi)/H\cong G_2\}|$ *on a*

$$Z_\psi(f,\underline{s})=\frac{\psi(G_1)}{|G_1|^{\underline{s}}}\,\frac{\psi(G_2)}{|G_2|^{\underline{s}}}\,\frac{Z_\psi(\underline{s}-\underline{u})}{Z_\psi(\underline{s})}.$$

(iv) *Pour* $f(G)=\sum_{\varphi\in \mathrm{Hom}_{\mathfrak{D}}(P,G)}|\{H\subset G/\mathrm{Im}\,\varphi: H\cong G_1\}|$, *on a*

$$Z_\psi(f,\underline{s})=\frac{\psi(G_1)}{|G_1|^{\underline{s}}}\,Z_\psi(\underline{s}-\underline{u}).$$

Démonstration. Posons provisoirement

$$Z_{\underline{u},\psi}(\underline{s})=\sum_{G/\sim}\frac{|\mathrm{Aut}_{\mathfrak{D}}(G)|\,w_{\underline{u}}(G)\,\psi(G)}{|G|^{s}}.$$

Nous allons démontrer (ii), (iii), (iv) avec $Z_{u,\psi}(\underline{s}-\underline{u})$ à la place de $Z_\psi(\underline{s}-\underline{u})/Z_\psi(\underline{s})$ (et donc $Z_\psi(\underline{s})Z_{\underline{u},\psi}(\underline{s}-\underline{u})$ à la place de $Z_\psi(\underline{s}-\underline{u})$ dans (iv)), puis nous en déduirons (i), ce qui fournira les formules finales du théorème. Pour montrer (ii), on effectue une sommation sur les φ d'image G' donnée à isomorphisme près. On obtient:

$$Z_\psi(f,\underline{s})=\sum_{G,\,G'/\sim}\frac{\psi(G)}{|G|^{\underline{s}}}\,s_{\underline{u}}(G')|\{H\subset G: H\cong G' \text{ et } G/H\cong G_1\}|,$$

et on conclut par 4. 5 (i).

Pour prouver (iii), on effectue une sommation sur les classes d'isomorphisme de quotients $G/\mathrm{Im}\,\varphi$. On obtient:

$$Z_\psi(f,\underline{s})=\sum_{G'/\sim}|\{H\subset G': H\cong G_1 \text{ et } G'/H\cong G_2\}|\sum_{G/\sim}\frac{\psi(G)}{|G|^{\underline{s}}}\,|\{\varphi: G/\mathrm{Im}\,\varphi\cong G\}|,$$

et on remplace la somme intérieure par sa valeur calculée en (ii), puis on utilise à nouveau l'exemple 4. 5 (i) (c'est-à-dire le fait que ψ est de type w). Enfin par sommation de (iii) sur les classes d'isomorphismes de G_2, on obtient (iv), sous la forme suivante:

$$Z_\psi(f_{G_1},\underline{s})=\frac{\psi(G_1)}{|G_1|^{\underline{s}}}\,Z_\psi(\underline{s})\,Z_{\underline{u},\psi}(\underline{s}-\underline{u})$$

avec

$$f_{G_1}(G)=\sum_{\varphi\in \mathrm{Hom}(P,G)}|\{H\subset G/\mathrm{Im}\,\varphi: H\cong G_1\}|.$$

Dans cette formule, prenons $G_1 = \{0\}$. D' après la définition 4. 1, on vérifie immédiatement que $\psi(\{0\}) = 1$. On a donc

$$Z_\psi(f_{\{0\}}, \underline{s}) = Z_\psi(\underline{s})\, Z_{\underline{u},\psi}(\underline{s} - \underline{u}).$$

Par ailleurs, il est clair que par définition,

$$f_{\{0\}}(G) = |\mathrm{Hom}(P, G)| = |G|^u \quad \text{(théorème 2. 6)},$$

donc que $Z_\psi(f_{\{0\}}, \underline{s}) = Z_\psi(\underline{s} - \underline{u})$, d'où (i) et le théorème 4. 6.

Remarque 4. 7. 1) On peut démontrer (i) directement sans difficulté.

2) La série $Z_{\underline{u},\psi}(\underline{s}) = \sum_{G/\sim} \dfrac{|\mathrm{Aut}_{\mathfrak{O}}(G)|\, w_{\underline{u}}(G)\, \psi(G)}{|G|^{\underline{s}}}$ est majorée en module par la série $Z_\psi(\underline{s})$. Il en résulte que si $Z_\psi(\underline{s})$ converge absolument pour $\mathrm{Re}(\underline{s}) > \underline{\sigma}$, il en est de même de $Z_{\underline{u},\psi}(\underline{s})$, et de plus que

$$\lim_{u \to \infty} Z_{\underline{u},\psi}(\underline{s}) = Z_{\underline{\infty},\psi}(\underline{s}) = Z_\psi(\underline{s}),$$

ce qui d'ailleurs est clair d'après (i). On en déduit en particulier:

Corollaire 4. 8. *Posons* $Z_{\underline{u},\underline{v}}(\underline{s}) = Z_{\underline{u},w}(\underline{s})$. *Alors, la série définisant* $Z_{\underline{u},\underline{v}}(\underline{s})$ *converge pour* $\mathrm{Re}(\underline{s}) > \underline{0}$ *et on a*

$$Z_{\underline{u},\underline{v}}(\underline{s}) = \frac{Z_{\underline{v}}(\underline{s})}{Z_{\underline{v}}(\underline{s} + \underline{u})} = \frac{Z_{\underline{u}}(\underline{s})}{Z_{\underline{u}}(\underline{s} + \underline{v})} = \frac{Z_{\underline{u}}(\underline{s})\, Z_{\underline{v}}(\underline{s})}{Z_{\underline{u}+\underline{v}}(\underline{s})}.$$

Démonstration. Nous venons de montrer l'assertion de convergence. La première égalité n'est autre que le théorème 4. 6 (i). La troisième résulte du théorème 3. 6 (iii), et la seconde par symétrie. Noter que cette symétrie n'est pas évidente à priori.

Pour terminer ce paragraphe nous démontrons un résultat qui, pour $f = 1$, se réduit au corollaire 3. 8.

Théorème 4. 9. *Soient K un corps de nombres et f une fonction définie sur les classes d'isomorphismes de* $\mathbb{Z}_K$*-modules finis; soit F la fonction analogue relative à l'ordre* $\mathfrak{O} = M_h(\mathbb{Z}_K)$ *qui, pour tout n-uple* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ *d'idéaux non nuls de* $\mathbb{Z}_K$ *est telle que*

$$F\left(M_{h,n}(\mathbb{Z}_K) \Big/ \begin{pmatrix} \mathfrak{a}_1 & \cdots & \mathfrak{a}_n \\ \cdot & & \cdot \\ \mathfrak{a}_1 & & \mathfrak{a}_n \end{pmatrix}\right) = f\left(\bigoplus_{i=1}^{n} \mathbb{Z}_K/\mathfrak{a}_i\right)$$

(*ceci a bien un sens puisque les* $\mathfrak{O}$*-modules finis sont décrits à isomorphisme près par des quotients de* $M_{h,n}(\mathbb{Z}_K)$). *Alors, pour tout u multiple de* $\dfrac{1}{h}$, *on a*

$$Z_u^{M_h(K)}(F, s) = Z_{hu}^K(f, hs).$$

Démonstration. Soient G un $\mathbb{Z}_K$-module fini, P un $\mathbb{Z}_K$ module projectif de rang $v=hu$. A G on peut associer un $\mathfrak{O}$-module fini $\mathfrak{G}$ comme ci-dessus et tout $\mathfrak{O}$-module fini s'obtient de cette façon. De même, si

$$P \cong \bigoplus_{i=1}^{v} \mathfrak{a}_i$$

on peut lui associer

$$\mathfrak{P} = \begin{pmatrix} \mathfrak{a}_1 & \cdots & \mathfrak{a}_v \\ \cdot & & \cdot \\ \mathfrak{a}_1 & \cdots & \mathfrak{a}_v \end{pmatrix} \quad (h \text{ lignes}).$$

Comme dans la proposition 2. 9 on vérifie que $\mathrm{Hom}^s_{\mathfrak{O}}(\mathfrak{P}, \mathfrak{G})$ est canoniquement isomorphe à $\mathrm{Hom}^s_{\mathbb{Z}_K}(P, G)$. Comme $u(\mathfrak{P}) = \dfrac{v}{h} = u$ et $|\mathfrak{G}| = |G|^h$, on obtient immédiatement le théorème 4. 9.

§ 5. Valeurs moyennes

Dans ce paragraphe, on conserve les notations des paragraphes précédents.

Définitions 5. 1. Soit f une fonction à valeurs complexes définie sur l'ensemble des classes d'isomorphisme de $\mathfrak{O}$-modules finis, soient $\underline{u}$ et $\underline{v}$ deux multi-indices admissibles, et soit P un $\mathfrak{O}$-module projectif de type fini de rang $\underline{u}$.

On appelle valeur moyenne de f (pour $\underline{u}$ et $\underline{v}$) la limite suivante, si elle existe:

$$M_{\underline{u},\underline{v}}(f) = \lim_{\underline{x} \to \underline{\infty}} \frac{\displaystyle\sum_{|G| \leqq \underline{x}} |G|^{-\underline{u}} \sum_{\varphi \in \mathrm{Hom}(P, G)} w_{\underline{v}}(G)\, f(G/\mathrm{Im}\,\varphi)}{\displaystyle\sum_{|G| \leqq \underline{x}} |G|^{-\underline{u}} \sum_{\varphi \in \mathrm{Hom}(P, G)} w_{\underline{v}}(G)}$$

(la notation $|G| \leqq \underline{x}$ signifie que pour tout i, $|G_i| \leqq x_i$). En particulier on pose

$$M_{\underline{u}}(f) = M_{\underline{u},\underline{\infty}}(f) \quad \text{(valeur moyenne de } f \text{ pour } \underline{u}).$$

On remarque que si f est constante, ces valeurs moyennes coïncident bien avec cette constante. D'autre part d'après le théorème 2. 6, le dénominateur peut s'écrire plus simplement

$$\sum_{|G| \leqq \underline{x}} w_{\underline{v}}(G).$$

Dans les applications, on aura toujours

$$M_{\underline{u}}(f) = \lim_{\underline{v} \to \underline{\infty}} M_{\underline{u},\underline{v}}(f).$$

En fait, seule la moyenne $M_{\underline{u}}(f)$ nous intéressera vraiment, et lorsqu'il s'agira de groupes de classes, $\underline{u}$ sera imposé (ce sera le rang d'un groupe d'unités).

Malgré l'absence d'additivité dénombrable, on convient de parler de "(u, v)-probabilité" lorsque f est la fonction caractéristique d'une certaine propriété.

Nous rappelons le lemme taubérien suivant (voir [C-L] pour une forme équivalente).

Lemme 5. 2. *On suppose que A est une algèbre* simple. *Soit c une fonction à valeurs réelles positives ou nulles, définie sur les classes d'isomorphisme de $\mathfrak{O}$-modules finis.*

Supposons que la série

$$D(s)=\sum_{G/\sim} c(G)|G|^{-s}$$

soit convergente pour $\mathrm{Re}(s)>0$, *et qu'il existe une constante* $C\in\mathbb{C}$ *telle que* $D(s)-C/s$ *possède un prolongement holomorphe sur un voisinage du demi-plan fermé* $\mathrm{Re}(s)\geqq 0$. *Alors, quand* $x\to\infty$,

$$\sum_{|G|\leqq x} c(G)\sim C\log x$$

(*si* $C=0$, *ceci signifie que* $\sum_{|G|\leqq x} c(G)=o(\log x)$).

Définition 5. 3. Pour tout multi-indice admissible $\underline{u}=(u_1,\ldots,u_m)$, on pose

$$C_{\underline{u}}^{A}=\prod_{i=1}^{m} C_{u_i}^{A_i}$$

où $C_{u_i}^{A_i}$ est le résidu en $s=0$ de la fonction $Z_{u_i}^{A_i}(s)$, donné par la proposition 3. 10 (ii).

Proposition 5. 4. *Quand* $\underline{x}\to\underline{\infty}$:

$$\sum_{|G|\leqq \underline{x}} w_{\underline{u}}(G)\sim C_{\underline{u}}^{A}\prod_{i=1}^{m}\log x_i.$$

En effet on se ramène au cas où A est simple, et dans ce cas la proposition résulte de la proposition 3. 10 et du lemme 5. 2.

Remarques 5. 5. 1) En raisonnant différement (i.e. sans utiliser de théorème taubérien), on peut obtenir un résultat avec reste et non un simple équivalent. Nous n'en aurons pas besoin ici.

2) Par définition, $|G|\leqq\underline{x}$ signifie que pour tout i, $|G_i|\leqq x_i$ donc, puisque $w_{\underline{u}}(G)$ est multiplicative sur les facteurs simples, la somme $\sum_{|G|\leqq\underline{x}} w_{\underline{u}}(G)$ est tout simplement le produit des sommes analogues sur les facteurs simples. Il en aurait été tout autrement si l'on avait écrit $\sum_{|G|\leqq x} w_{\underline{u}}(G)$ avec x à une seule variable.

Nous ne savons pas quel est l'équivalent dans ce cas.

Le théorème fondamental qui va nous permettre d'effectuer les calculs explicites qui interviennent dans les formules heuristiques décrivant le comportement asymptotique des groupes de classes est le suivant:

Théorème 5. 6. *Soit f une fonction définie sur les classes d'isomorphisme de $\mathfrak{O}$-modules finis, positives ou nulle, et multiplicative par rapport aux facteurs simples de l'algèbre (i.e. telle que $f(G)=\prod_{i=1}^{m} f(e_i G)$; on note $f_1, \ldots, f_m$ les fonctions attachées aux facteurs simples). Supposons que les séries $Z_{v_i}^{A_i}(f_i, s)$ convergent pour $\mathrm{Re}(s)>0$ et qu'il existe des constantes C_i telles que $Z_{v_i}^{A_i}(f_i, s)-C_i/s$ possèdent un prolongement holomorphe dans un voisinage du demi-plan $\mathrm{Re}(s)\geqq 0$. Alors:*

(i) *Quels que soient les multi-indices admissibles $\underline{u}$ et $\underline{v}$, on a*

$$M_{\underline{u},\underline{v}}(f)=\lim_{\underline{s}\to\underline{u}}\frac{Z_{\underline{v}}^{A}(f,\underline{s})}{Z_{\underline{v}}^{A}(\underline{s})},$$

et en particulier si pour tout i, $u_i>0$:

$$M_{\underline{u},\underline{v}}(f)=\frac{Z_{\underline{v}}^{A}(f,\underline{u})}{Z_{\underline{v}}^{A}(\underline{u})}.$$

(ii) *Quel que soit le multi-indice admissible $\underline{u}$, on a*

$$M_{\underline{u}}(f)=\lim_{\underline{s}\to\underline{u}}\frac{Z^{A}(f,\underline{s})}{Z^{A}(\underline{s})},$$

et en particulier si pour tout i, $u_i>0$:

$$M_{\underline{u}}(f)=\frac{Z^{A}(f,\underline{u})}{Z^{A}(\underline{u})}.$$

Démonstration. Toutes les assertions découlent trivialement de la première assertion de (i). Il est clair également qu'il suffit de se restreindre au cas où l'algèbre A est simple. Dans ce cas on peut écrire (cf. définition 5. 1):

$$M_{u,v}(f)=\lim_{x\to\infty}\frac{N(x)}{D(x)}.$$

Nous avons vu que $D(x)\sim C_v^A \log x$, où

$$C_v^A=\mathrm{Res}_{s=0}\, Z_v^A(s)=\lim_{s\to 0} s Z_v^A(s+u)\, Z_{u,v}^A(s)$$

d'après le théorème 3. 6.

D'autre part la série de Dirichlet associée au numérateur vaut

$$\begin{aligned}\varphi(s) &= \sum_{G/\sim} \sum_{\varphi} f(G/\mathrm{Im}\,\varphi)\, w_v(G)|G|^{-s-u} \\ &= \sum_{G_1/\sim} \sum_{G/\sim} |\{\varphi : G/\mathrm{Im}\,\varphi \cong G_1\}|\, w_v(G)|G|^{-s-u} \\ &= \Big(\sum_{G_1/\sim} f(G_1) w_v(G_1)|G_1|^{-s-u}\Big) Z^A_{u,v}(s)\end{aligned}$$

d'après le théorème 4. 6 (ii); donc, $\varphi(s) = Z^A_v(f, s+u)\, Z^A_{u,v}(s)$.

Or, on remarque que le lemme taubérien 5. 2 peut s'appliquer à la série $\varphi(s)$: en effet, si $u=0$, $Z^A_{u,v}(s)=1$, donc l'hypothèse du théorème équivaut à celle du lemme (i.e. on a un prolongement, mais surtout un pôle au plus *simple* en $s=0$), alors que, si $u>0$, $Z^A_v(f, u)$ existe, et $Z^A_{u,v}(s)$ a un pôle simple (si $v>0$). On a donc

$$N(x) \sim N \cdot \log x,$$

où

$$N = \mathrm{Res}_{s=0}\, \varphi(s) = \lim_{s \to 0} s Z^A_v(f, s+u)\, Z^A_{u,v}(s).$$

On en déduit immédiatement le théorème.

Ceci termine les longs préliminaires combinatoires et analytiques qui nous permettront de faire des calculs explicites utiles. Nous allons maintenant aborder la partie heuristique de cet article.

§ 6. L'hypothèse heuristique fondamentale

Nous allons montrer dans ce paragraphe comment on peut de façon naturelle généraliser les heuristiques de [C-L]. Rappelons celles-ci brièvement dans le cas d'une extension quadratique de $\mathbb{Q}$. On définit la moyenne d'une fonction f définie sur les classes d'isomorphisme de groupes abéliens finis par la formule:

$$\mathfrak{M}(f) = \lim_{x \to \infty} \frac{\sum_{|d_K| \leqq x} f(\mathrm{Cl}_K^{\{2\}})}{\sum_{|d_K| \leqq x} 1}$$

où $\mathrm{Cl}_K^{\{2\}}$ désigne la partie impaire du groupe des classes d'un corps quadratique K, les corps K parcourant soit l'ensemble des corps quadratiques imaginaires, soit l'ensemble des corps quadratiques réels (bien entendu les moyennes ainsi obtenues seront en général distinctes). Une reformulation des hypothèses heuristiques et des résultats de [C-L] est que $\mathfrak{M}(f) = M_u^{\{2\}}(f)$, où u est le rang du groupe des unités de K (0 dans le cas imaginaire, 1 dans le cas réel; voir la définition 5. 1 et l'hypothèse 6. 6 pour $M_u^{\{2\}}(f)$).

Nous allons généraliser ceci non seulement à des extensions quelconques de $\mathbb{Q}$ (galoisiennes ou non) au lieu d'extensions quadratiques, mais également au cas où le corps de base n'est plus $\mathbb{Q}$ mais un corps de nombres quelconque K_0. Dans ce cas, l'objet intéressant à étudier est le groupe des classes relatives Cl_{L/K_0} formé des classes d'idéaux de L dont la norme est triviale (i.e. principale) dans K_0.

Soit donc L/K_0 une extension finie de corps de nombres de degré n, de clôture galoisienne K/K_0. Posons $\Gamma=\mathrm{Gal}(K/K_0)$ et $\Gamma'=\mathrm{Gal}(K/L)$

$$\left.\begin{array}{l} K \\ | \quad)\Gamma' \\ L \\ n \mid \\ K_0 \end{array}\right\} \Gamma.$$

A l'extension L/K_0 est associée une représentation de permutation définie à isomorphisme près par son caractère $r_{\Gamma/\Gamma'}$. Ce caractère contient une fois exactement la représentation unité, et nous posons

$$a_{\Gamma/\Gamma'}=r_{\Gamma/\Gamma'}-1 \qquad \text{(caractère d'augmentation).}$$

D'autre part à tout caractère ψ de Γ, on associe un idempotent e_ψ par le procédé suivant:

Si χ est un caractère absolument irréductible, on pose $e_\chi=\dfrac{\chi(1)}{|\Gamma|}\sum_{s\in\Gamma}\chi(s^{-1})s$, puis $e_\psi=\sum_\chi e_\chi$, où la sommation porte sur les caractères absolument irréductibles contenus dans ψ. Cette définition sera appliquée en particulier dans le cas où ψ est le caractère d'augmentation $a_{\Gamma/\Gamma'}$.

Nous verrons au paragraphe suivant comment le groupe Cl_{L/K_0} est relié au groupe $e_{a_{\Gamma/\Gamma'}}\mathrm{Cl}_{K/K_0}$, expression qui n'a de sens que si l'on convient d'enlever de Cl_{K/K_0} les p-composantes correspondant aux p qui apparaissent dans le dénominateur de l'idempotent. Ceci permet de se ramener à une situation galoisienne, et nous allons donc généraliser les heuristiques de [C-L] à des groupes $e\mathrm{Cl}_{K/K_0}$ convenables. Ceci conduit aux définitions suivantes.

Nous nous donnons un groupe fini Γ, un idempotent e du centre de $A=\mathbb{Q}[\Gamma]$ et un corps de nombres K_0. Nous reprenons les notations du paragraphe 2; en particulier $\mathfrak{O}$ désigne un ordre maximal de A contenant $\mathbb{Z}[\Gamma]$. Pour p premier, nous notons $\mathbb{Z}_{(p)}$, $\mathfrak{O}_{(p)}$, ... les localisés en p de $\mathbb{Z}$, $\mathfrak{O}$, ...

Définition 6.1. On dit qu'un nombre premier p est *bon pour* e si, pour toute composante irréductible e' de e, on a:

(i) $e'\in\mathbb{Z}_{(p)}[\Gamma]$,

(ii) $e'\mathbb{Z}_{(p)}[\Gamma]$ est un ordre maximal de A relativement à $\mathbb{Z}_{(p)}$,

et qu'il est *mauvais pour* e dans le cas contraire.

On dit que p est *bon pour un caractère* χ s'il est bon pour l'idempotent e_χ associé à χ.

Définition 6. 2. Etant donnés un $\mathfrak{O}$-module fini G et un ensemble S de nombres premiers, on note G^S la partie de G première à S.

La condition (i) de 6. 1 permet de définir le produit $e \cdot x$ lorsque x est un élément de la p-composante d'un $\mathbb{Z}_{(p)}[\Gamma]$-module fini quelconque (par exemple, un groupe de classes). La condition (ii) permet d'utilisir les résultats combinatoires et analytiques des paragraphes précédents.

Soit maintenant K une extension galoisienne de K_0 de groupe de Galois Γ.

Convention 6. 3. Etant donnée une extension galoisienne comme ci-dessus, on convient, lorsque l'on considère un groupe $e\mathrm{Cl}^S_{K/K_0}$, que S contient les nombres premiers mauvais pour e.

Définition 6. 4. (i) On appelle *e-rang du groupe des unités de* K, et on note $\mathrm{rg}_e(K)$, le rang du $\mathfrak{O}$-module $e(\mathbb{Q} \otimes_{\mathbb{Z}} E_K)$, au sens de la définition 2. 2, où E_K est le groupe des unités de K; c'est donc un élément de $\mathbb{Q}^m$, où m est le nombre de composantes simples de A.

(ii) On dit qu'un élément $\underline{u}$ de $\mathbb{Q}^m$ est *admissible pour le triplet* (K_0, Γ, e) s'il existe une extension galoisienne K/K_0, de groupe de Galois isomorphe à Γ et telle que $\mathrm{rg}_e(K) = \underline{u}$.

Définition 6. 5. Soit $\underline{u}$ un multi-indice admissible et soit f une fonction définie sur l'ensemble des classes d'isomorphisme de $\mathfrak{O}$-modules finis. On définit la *moyenne de f relativement au quintuplet* $(K_0, \Gamma, e, \underline{u}, S)$ par

$$\mathfrak{M}^S_{\underline{u}}(f) = \lim_{x \to \infty} \frac{\sum_{|d_K| \leqq x} f(e\mathrm{Cl}^S_{K/K_0})}{\sum_{|d_K| \leqq x} 1},$$

où les sommations portent sur les extensions galoisiennes K/K_0 contenues dans une clôture algébrique donnée de K_0, ayant un groupe de Galois isomorphe à Γ et un e-rang égal à $\underline{u}$. Cette moyenne dépend bien sûr du choix de S, mais le plus souvent nous prendrons pour S l'ensemble des mauvais nombres premiers.

L'hypothèse heuristique fondamentale est alors la suivante:

Hypothèse 6. 6. Soit e un idempotent central de $\mathbb{Q}[\Gamma]$, orthogonal à l'idempotent $e_1 = \frac{1}{[\Gamma]} \sum_{s \in \Gamma} s$. Soit S un ensemble de nombres premiers contenant ceux qui sont mauvais pour e, et soit enfin $\underline{u}$ un multi-indice admissible. Alors, pour toute fonction f "raisonnable" définie sur l'ensemble des classes d'isomorphisme de $\mathfrak{O}_S$-modules finis, on a:

$$\mathfrak{M}^S_{\underline{u}}(f) = M^S_{\underline{u}}(f),$$

où $\mathfrak{M}^S_{\underline{u}}(f)$ est définie ci-dessus (définition 6. 5) et $M^S_{\underline{u}}(f) = M_{\underline{u}}(f_S)$, où $M_{\underline{u}}$ est définie en 5. 1 et f_S est la fonction définie par

$$f_S(G) = f(G^S).$$

(Il revient au même de restreindre G à des $\mathfrak{O}$-modules finis premiers à S dans les sommations de la définition 5. 1, cf. [C-L], proposition 5. 6 et 5. 7.)

Commentaires et remarques. (i) De même que dans [C-L], nous ne pouvons préciser la notion de fonction "raisonnable": il faut certainement se restreindre aux fonctions vérifiant le théorème taubérien 5. 6, ce qui est le cas des fonctions intéressantes en pratique.

(ii) La valeur, et même l'existence de la quantité $\mathfrak{M}_{\underline{u}}^{S}(f)$ figurant à gauche de l'égalité 6. 6, est inconnue pour presque toutes les fonctions. En revanche, le membre de droite est de nature combinatoire et analytique, et peut se calculer dans la pratique en utilisant les résultats des paragraphes précédents, exactement comme dans [C-L].

(iii) Comme les fonctions raisonnables au sens du théorème 5. 6 sont multiplicatives sur les facteurs simples, les calculs de moyennes se ramènent tout de suite au cas où e est irréductible. Il est clair que l'idempotent e_1 doit être exclu: en effet, les mauvais p sont alors exactement ceux qui divisent l'ordre de Γ, et le groupe $e_1 \mathrm{Cl}_{K/K_0}^{S}$ est réduit à l'élément neutre. (En général l'ensemble des mauvais p est seulement contenu dans l'ensemble des diviseurs de $|\Gamma|$, cf. proposition 7. 1; toutefois les bons p divisant $|\Gamma|$ posent des problèmes particuliers, cf. 8. a).

Dans la pratique, pour appliquer l'hypothèse heuristique fondamentale à une classe de corps donnée, on procède de la façon suivante:

1) Dans le cas où il s'agit d'une classe d'extensions non galoisiennes L/K_0, on essaie de comparer Cl_{L/K_0} à un groupe du type $e\mathrm{Cl}_{K/K_0}$ où K parcourt l'ensemble des clôtures galoisiennes des extensions de la classe considérée, en utilisant des méthodes décrites au paragraphe suivant. (Le groupe Γ est donné à isomorphisme près comme groupe de permutation, et l'on s'impose en outre les classes de conjugaison des Frobenius à l'infini.)

On s'occupe maintenant de tels groupes; le cas le plus intéressant est celui où e est irréductible dans $\mathbb{Q}[\Gamma]$ (ce qui rend inutile les multi-indices).

2) On détermine les p qui sont bons pour e, et on choisit un ensemble S contenant les mauvais p, le plus souvent l'ensemble des mauvais p lui-même.

3) Le choix de $\underline{u}$ est maintenant dicté par le comportement des places à l'infini dans les extensions considérées, grâce au théorème de Herbrand dont l'énoncé est le suivant (voir [A-T] pour une démonstration):

Théorème 6. 7 (Herbrand). *Soit K une extension galoisienne finie de K_0, de groupe de Galois Γ. Pour chaque place infinie v de K_0, soit Γ_v (défini à conjugaison près) le groupe de décomposition d'une place de K au dessus de v. Alors, le $\mathbb{Q}[\Gamma]$-module $\mathbb{Q} \otimes E_K$ a pour caractère*

$$\chi_E = -1 + \sum_v \mathrm{Ind}_{\Gamma_v}^{\Gamma}(1_{\Gamma_v}).$$

Soit alors χ un caractère de Γ irréductible sur $\mathbb{Q}$, et soit φ une composante absolument irréductible de χ. Le caractère du module $V=e_\chi(\mathbb{Q}\otimes E_K)$ est égal à

$$\sum_{\varphi|\chi}\langle\varphi,\chi_E\rangle\varphi=\langle\varphi,\chi_E\rangle\chi$$

(ceci est indépendant de φ). Identifions $e_\chi\mathbb{Q}[\Gamma]$ à une algèbre $M_h(D)$, où D est un corps gauche de centre K, de rang r^2 sur K. Soit K' un sous-corps commutatif maximal de D. On a:

$$\dim_{K'}(K'\otimes_{\mathbb{Q}}V)=hr\langle\chi_E,\varphi\rangle,$$

donc $\dim_K(K'\otimes_{\mathbb{Q}}V)=hr^2\langle\chi_E,\varphi\rangle$, d'où d'après la définition 2. 2:

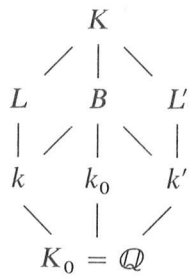
$$u=\frac{1}{h^2r^2}\dim_K(K'\otimes_{\mathbb{Q}}V)=\frac{1}{h}\langle\chi_E,\varphi\rangle$$

$$\left(=\frac{1}{h|\Gamma|}\sum_{s\in\Gamma}\chi_E(s)\varphi(s)\right).$$

4) Les résultats heuristiques obtenus sur $e\mathrm{Cl}_{K/K_0}$ ne sont en général pas suffisants pour obtenir ce que l'on cherche sur Cl_{L/K_0}. Nous devons faire une hypothèse supplémentaire d'indépendance de moyennes pour parvenir au résultat final.

L'exemple ci-dessous va clarifier ce que nous voulons dire.

Exemple 6. 8. *Corps quartiques totalement réels de type diédral.* Soit $L/\mathbb{Q}$ de degré 4, à clôture galoisienne K, de groupe de Galois Γ diédral (d'ordre 8); L est fixé par un sous-groupe $\Gamma'=\{1,\tau\}$ non distingué d'ordre 2, et contient un unique sous-corps quadratique, noté k; le diagramme ci-contre résume la situation (noter que L et L' ont un corps conjugué sur $\mathbb{Q}$ distinct d'eux-mêmes).



On écrit $\Gamma=\langle\sigma,\tau\rangle$ avec $\tau^2=\sigma^4=1$ et $\tau\sigma\tau^{-1}=\sigma^{-1}$.

Le caractère $a_{\Gamma/\Gamma'}$ est de degré 3, somme de deux caractères absolument irréductibles φ, de degré 1, et χ, de degré 2; l'idempotent e qui lui est associé est de la forme $\lambda/8$ avec $\lambda\in\mathbb{Z}[\Gamma]$, et 2 est l'unique nombre premier mauvais pour e (et il l'est effectivement pour e, e_φ et e_χ). On choisit $S\supset\{2\}$.

Si $K_0\subset k\subset L$ est une tour d'extensions, on montre immédiatement que l'on a la décomposition

$$\mathrm{Cl}^S_{L/K_0}=\mathrm{Cl}^S_{L/k}\oplus\mathrm{Cl}^S_{k/K_0}$$

dès que S contient les diviseurs premiers de $[L:k]$. Il en résulte que l'étude heuristique de Cl_L^S se ramène à celles de Cl_k^S et de $\mathrm{Cl}_{L/k}^S$. La première est classique ([C-L], § 9, II; [C-M 1], § 2, (1. 2)). Pour la seconde, on vérifie sans difficulté que le $\mathbb{Z}$-module $e_\chi \mathrm{Cl}_K^S$ est isomorphe au produit $\mathrm{Cl}_{L/k}^S \times \mathrm{Cl}_{L/k}^S$ (cf. § 7, ou utiliser l'application qui au couple $(\mathfrak{a}, \mathfrak{b})$ d'idéaux de L associe le produit $\mathfrak{a}\sigma\mathfrak{b}$ étendu à K).

L'algèbre $e_\chi \mathbb{Q}[\Gamma]$ est isomorphe à $M_2(\mathbb{Q})$. Posons $\mathfrak{o} = \mathbb{Z}\left[\frac{1}{2}\right]$ et $\mathfrak{O} = M_2(\mathfrak{o})$. Les groupes $e_\chi \mathrm{Cl}_K$ et $e_\chi(\mathfrak{O} \otimes_{\mathbb{Z}[\Gamma]} E_K)$ sont des $\mathfrak{O}$-modules, dont le dernier est de rang 1 d'après le théorème de Herbrand (on a $h=2$, $\chi_E = r_\Gamma - 1$, donc $\langle \chi_E, \varphi \rangle = \langle \chi_E, \chi \rangle = \chi(1) = 2$). Notre hypothèse heuristique fondamentale nous dit donc que si F est une fonction définie sur les classes d'isomorphismes de $\mathfrak{O}$-modules finis, on devrait avoir $\mathfrak{M}_1^S(F) = M_1^S(F)$ ("$\mathfrak{O}$-moyenne"). Or tout $\mathfrak{O}$-module G est de la forme $g \times g$ pour un $\mathfrak{o}$-module g convenable. Ainsi, pour $G = e_\chi \mathrm{Cl}_K^S$, on peut prendre $g = \mathrm{Cl}_{L/k}^S$, qui est justement le groupe que nous voulons étudier.

Comme dans le théorème 4. 9, à toute fonction F comme ci-dessus, on peut associer la fonction f définie sur l'ensemble des classes d'isomorphismes de $\mathfrak{o}$-modules par $f(g) = F(g \times g)$. D'après ce théorème, on a

$$M_1^S(F) = M_2^S(f).$$

Enfin, la quantité qui nous intéresse, que nous noterons $\mathfrak{M}^S(f)$ est égale à

$$\lim_{x \to \infty} \frac{\sum_{d_L \leqq x} f(\mathrm{Cl}_{L/k}^S)}{\sum_{d_L \leqq x} 1} = \lim_{x \to \infty} \frac{\sum_{d_L \leqq x} F(e_\chi \mathrm{Cl}_K^S)}{\sum_{d_L \leqq x} 1}$$

(K étant déterminé par L). Il est alors nécessaire de supposer que cette dernière limite est égale à

$$\mathfrak{M}_1^S(F) = \lim_{x \to \infty} \frac{\sum_{d_K \leqq x} F(e_\chi \mathrm{Cl}_K^S)}{\sum_{d_K \leqq x} 1}$$

(où on somme sur d_K au lieu de d_L). Ceci revient essentiellement à supposer que le comportement du groupe des classes relatives de L/k est indépendant du corps quadratique (réel) k choisi.

Dans ce cas précis, une justification est fournie par l'argument suivant: pour k fixé, les extensions quadratiques L/k telles que $L/\mathbb{Q}$ soit de type diédral sont de densité 1 parmi toutes les extensions quadratiques de k([B]). On peut donc appliquer l'hypothèse heuristique fondamentale directement à l'ensemble des extensions quadratiques totalement réelles de k.

La conclusion de cette discussion est donc que l'hypothèse heuristique raisonnable à faire pour les corps quartiques totalement réels de type diédral, est que

$$\mathfrak{M}^S(f) = M_2^S(f),$$

ce qui correspond bien à ce qui est annoncé dans [C-M 2], § 6. 4.

[On notera que les résultats sont les mêmes pour L/k et L'/k'. Il en est de même quand K est imaginaire, où l'on a l'une des deux situations suivantes: k et k' réels, L et L' totalement imaginaires, ou bien k et L imaginaires et k' réel et L' de signature mixte (à échange près de (k, L) et (k', L')). La discussion est analogue au cas totalement réel, sauf qu'ici le rang de E_K sur $M_2(\mathbb{Z})$ est 1/2 dans le premier cas et 0 dans le second. Des calculs de Lakein ([L]) lorsque k est imaginaire confirment nos conjectures.]

§ 7. Classes relatives et idempotents

Dans ce paragraphe, K désigne une extension galoisienne finie d'un corps de nombres K_0, Γ son groupe de galois, Γ' un sous-groupe de Γ, et L la sous-extension de K fixe par Γ'. On note e l'idempotent associé à la représentation d'augmentation $a_{\Gamma/\Gamma'}$, et l'on se donne un ensemble S de nombre premiers contenant ceux qui sont mauvais pour e.

Nous désirons comparer les groupes $e\mathrm{Cl}^S_{K/K_0}$ et Cl^S_{L/K_0}. Pour cela, nous comparons d'abord $e\mathrm{Cl}^S_{K/K_0}$ au groupe des classes "ambiges" $(\mathrm{Cl}^S_{K/K_0})^{\Gamma'}$, puis nous démontrons l'égalité entre Cl^S_{L/K_0} et $(\mathrm{Cl}^S_{k/K_0})^{\Gamma'}$ dans certains cas de produits semi-directs qui incluent en particulier tous les degrés $\leqq 4$ de [C-M 2] (l'égalité n'est pas vraie en général).

Auparavant, nous donnons quelques résultats concernant les bons p, justifiant les choix faits pour l'ensemble S dans tous les cas traités dans [C-L] et [C-M 2] (dans le cas du groupe symétrique S_3, on utilise 7. 1 (ii)).

Proposition 7. 1. *Soit χ un caractère de Γ à valeurs rationnelles et soit e_χ l'idempotent associé.*

(i) *Si p ne divise pas $|\Gamma|$, p est bon pour e_χ.*

(ii) *Si Γ est diédral d'ordre $2m$ avec m impair, et si χ ne contient pas de caractère de degré* 1, 2 *est bon pour e_χ.*

(iii) *Le nombre premier* 3 *est bon pour les caractères de degré* 3 *de A_4 et de S_4.*

Démonstration. Le calcul explicite de l'idempotent montre tout de suite que la condition $e_\chi \in \mathbb{Z}_{(p)}[\Gamma]$ est vérifiée dans chaque cas. Nous allons vérifier que $e_\chi \mathbb{Z}_{(p)}[\Gamma]$ est un ordre maximal en calculant des discriminants dans $\mathbb{Z}_{(p)}[\Gamma]$ pour la trace ou pour la trace réduite selon les cas. Posons $n = |\Gamma|$.

(i) Le discriminant (pour la trace) de la base canonique de $\mathbb{Z}[\Gamma]$ sur $\mathbb{Z}$ est égal à $\pm n^n$. Il est donc inversible dans $\mathbb{Z}_{(p)}$ si p ne divise pas n.

(ii) On a $n = 2m$; l'exposant de 2 dans le discriminant de $\mathbb{Z}[\Gamma]$ est donc égal à $2m$. Comme il y a $(m-1)/2$ caractères absolument irréductibles de degré 2, le passage de la trace à la trace réduite divise ce discriminant par $2^{4(m-1)/2} = 2^{n-2}$, et les caractères de degré 1 contribuent pour un facteur 2^2 (à cause de l'indice 2 de $\mathbb{Z}[g]$ dans l'ordre maximal, où g est le quotient d'ordre 2 de Γ). L'image de $\mathbb{Z}[\Gamma]$ dans le produit des facteurs simples non commutatifs de $\mathbb{Q}[\Gamma]$ a donc un discriminant impair pour la trace réduite, et est donc un ordre maximal.

(iii) On fait un calcul analogue à celui fait en (ii). Pour A_4, l'exposant 12 de 3 dans le discriminant de $\mathbb{Z}[\Gamma]$ se répartit ainsi dans la décomposition

$$\mathbb{Q}[\Gamma] \cong \mathbb{Q} \times \mathbb{Q}(\zeta_3) \times M_3(\mathbb{Q}):$$

2 pour l'indice de la partie commutative, 1 pour le discriminant de $\mathbb{Q}(\zeta_3)$, et 9 pour le passage de la trace réduite à la trace dans $M_3(\mathbb{Q})$.

Pour S_4, on a un exposant 24, décomposé en 6 provenant du quotient isomorphe à S_3 (calculé en (ii)) et en 2 fois 9 pour chaque facteur simple isomorphe à $M_3(\mathbb{Q})$, d'où la proposition.

Soit G un $\mathbb{Z}[\Gamma]$-module fini, et soit $\lambda \in \mathbb{Q}[\Gamma]$; écrivons $\lambda = \frac{1}{m} \sum_{s \in \Gamma} a(s)s$, où les $a(s)$ sont des entiers dont le PGCD avec m vaut 1. Pour $x \in G$, on définit le produit λx lorsque l'une des deux conditions suivantes est vérifiée:

(i) $\sum a(s)sx = 0$, et alors on pose $\lambda x = 0$;

(ii) m est premier à l'ordre de G.

Etant donné un caractère χ de $\mathbb{Q}[\Gamma]$, la χ-composante $G_\chi = e_\chi G$ de G est définie lorsque e_χ vérifie l'une des conditions ci-dessus. Lorsqu'il en est ainsi pour tous les caractères irréductibles, on a l'égalité

$$G = \bigoplus_\chi G_\chi \tag{7. 2}$$

(somme sur l'ensemble des caractères irréductibles de G).

Nous pouvons maintenant comparer les groupes $(\mathrm{Cl}^S_{K/K_0})^{\Gamma'}$ et Cl^S_{K/K_0} (où e est l'idempotent associé au caractère d'augmentation $a_{\Gamma/\Gamma'}$). Il suffit d'appliquer le théorème suivant au groupe Cl^S_{K/K_0}:

Théorème 7. 3. *Soit G un $\mathbb{Z}[\Gamma]$-module fini, verifiant les conditions suivantes:*

(i) *La composante p-primaire de G est nulle pour tout nombre premier p mauvais pour e.*

(ii) *La composante de G sur le caractère unité est nulle.*

(iii) *Si χ est un caractère irréductible orthogonal à $a_{\Gamma/\Gamma'}$ et si p divise l'ordre de Γ, la composante p-primaire de G_χ est nulle.*

Alors il existe un $\mathbb{Z}[\Gamma]$-module fini H tel que les groupes $(eG)_\chi$ et $G_\chi^{\Gamma'}$ soient isomorphes respectivement à

$$H_\chi^{\langle \chi, a_\Gamma \rangle} \quad \text{et} \quad H_\chi^{\langle \chi, a_{\Gamma/\Gamma'} \rangle} \quad \text{en tant que } \mathbb{Z}\text{-modules}$$

pour tout caractère irréductible χ de Γ. (a_Γ désigne le caractère d'augmentation de Γ lui-même, égal à $a_{\Gamma/\{1\}}$.)

Remarque 7. 4. La condition (iii) est conséquence des conditions (i) et (ii) si Γ est diédral et Γ' d'ordre 2, ou si Γ est isomorphe à A_4 et Γ' fixe une lettre.

Démonstration du théorème. Il s'agit de construire pour tout caractère irréductible χ de G un groupe H_χ égal à sa χ-composante et vérifiant les propriétés du théorème. En décomposant G en la somme de ses composantes p-primaires, on est tout de suite ramené au cas où G est un p-groupe abélien. Traitons d'abord le cas où G est annulé par p.

G est alors un $\mathbb{F}_p[\Gamma]$-module (une "représentation de Γ sur $\mathbb{F}_p$"). Lorsque p ne divise pas $|\Gamma|$, on effectue un calcul de dimensions à l'aide des caractères. Si V désigne un $\mathbb{F}_p[\Gamma]$-module de caractère χ, on a $\dim V^\Delta = \langle \mathrm{Res}^\Delta_\Gamma(\chi), 1\rangle_\Delta$ pour tout sous-groupe Δ de Γ, d'où $\dim V^{\Gamma'} = \langle \mathrm{Res}^{\Gamma'}_\Gamma(\chi), 1\rangle_{\Gamma'} = \langle \chi, \mathrm{Ind}^\Gamma_{\Gamma'}(1)\rangle_\Gamma = \langle \chi, r_{\Gamma/\Gamma'}\rangle_\Gamma = \langle \chi, 1\rangle_\Gamma + \langle \chi, a_{\Gamma/\Gamma'}\rangle_\Gamma$. Comme $V^\Gamma = (0)$ on a $\langle \chi, 1\rangle = 0$, d'où l'égalité $\dim V^{\Gamma'} = \langle \chi, a_{\Gamma/\Gamma'}\rangle$.

Appliquons ce calcul en prenant pour V une composante irréductible de G. Si χ n'est pas contenu dans $a_{\Gamma/\Gamma'}$, on a $(eV)_\chi = (0) = V^{\Gamma'}$, et on peut prendre $H_\chi = (0)$. Sinon, on a $(eV)_\chi = V_\chi$, et $\dim V_\chi(1) = \langle \chi, a_\Gamma\rangle$. En regroupant les composantes isotypiques, on obtient le résultat cherché.

Il faut maintenant généraliser ce calcul au cas ou p est seulement supposé bon pour $a_{\Gamma/\Gamma'}$. Or, le fait que $e\mathbb{Z}_{(p)}[\Gamma]$ soit un ordre maximal fait que eV se relève en un module projectif sur $\mathbb{Z}_{(p)}[\Gamma]$. On est alors dans la situation qui est l'objet de la proposition 46 du § 16. 4 de [Ser], où il est encore possible d'identifier les caractères de $e\mathbb{Z}_p[\Gamma]$ avec des relèvements dans $\mathbb{Q}[\Gamma]$. Lorsque χ est contenu dans $a_{\Gamma/\Gamma'}$, on a encore $\dim V_\chi = \chi(1)$, et la dimension de $V^{\Gamma'}$, qui se calcule à l'aide du caractère modulaire correspondant (ibid., § 18. 1, (ix)) est aussi donnée par la même formule, vu que χ est nul sur les éléments p-singuliers de Γ (ibid., cor. à la proposition 46). Lorsque χ est orthogonal à $a_{\Gamma/\Gamma'}$, $(eV)_\chi = (e_\chi e)\,V$ est réduit à (0), et $V^{\Gamma'}$ l'est aussi par hypothèse.

Nous devons maintenant revenir au cas général où l'on suppose seulement G annulé par une puissance de p. Lorsque la χ-composante de G est nulle, il n'y a pas de problème puisqu'il suffit de prendre $H_\chi = (0)$. On peut donc se limiter aux caractères χ contenus dans $a_{\Gamma/\Gamma'}$. En outre, G étant un module de type fini sur $e\mathbb{Z}_{(p)}[\Gamma]$, il existe une suite exacte

$$0 \to P \to L \to G \to 0$$

où L est libre de type fini sur $e\mathbb{Z}_{(p)}[\Gamma]$. Notant G_i le sous-groupe de G annulé par p^i, on en déduit pour tout i des suites exactes

$$0 \to P_i \to L_i \to G_i \to 0$$

dans lesquelles P_i et L_i sont sans torsion, donc projectifs sur $e\mathbb{Z}_{(p)}[\Gamma]$ puisque $e\mathbb{Z}_{(p)}[\Gamma]$ est un ordre maximal, et même projectifs sur $\mathbb{Z}_{(p)}[\Gamma]$ puisque $e\mathbb{Z}_{(p)}[\Gamma]$ est facteur direct dans $\mathbb{Z}_{(p)}[\Gamma]$. Il en résulte que pour tout i, G_i est un Γ-module cohomologiquement trivial, ce qui montre en utilisant la suite exacte

$$0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0$$

que la suite

$$0 \to G_i^{\Gamma'} \to G_{i+1}^{\Gamma'} \to (G_{i+1}/G_i)^{\Gamma'} \to 0$$

est également exacte, ce qui permet enfin d'identifier les groupes $(G_{i+1}/G_i)^{\Gamma'}$ et $G_{i+1}^{\Gamma'}/G_i^{\Gamma'}$.

De l'étude faite pour les Γ-modules annulés par p, il résulte que pour tout $i \geqq 0$ les nombres des facteurs invariants de eG et de $G^{\Gamma'}$ annulés par p^i sont dans le rapport $\langle \chi, a_\Gamma \rangle / \langle \chi, a_{\Gamma/\Gamma'} \rangle$ (ou sont tous deux nuls), ce qui assure l'existence de H_χ, d'où le théorème.

Remarque 7. 5. Soit M un $e\mathbb{Z}[\Gamma]$-module fini; pour tout p premier, tout entier $i>0$ et tout χ irréductible, notons $M_{p^i,\chi}$ le sous-module de la χ-composante de M annulé par p^i. La connaissance des facteurs invariants des $M_{p^i,\chi}$ caractérise M à isomorphisme près en tant que $e\mathbb{Z}[\Gamma]$-module. En particulier, la classe d'isomorphisme de H_χ en tant que $e_\chi\mathbb{Z}[\Gamma]$-module est déterminée par le théorème 7. 3. Par exemple, dans le cas d'un groupe Γ diédral d'ordre $2m$, $m \geqq 3$, les groupes $(eG)_\chi$ et $(G^{\Gamma'})_\chi$ (Γ' d'ordre 2) portent des structures de module sur $\mathbb{Z}[\zeta_d + \zeta_d^{-1}]$ pour un diviseur $d>1$ convenable de m, et H_χ est déterminé en tant que module sur $\mathbb{Z}[\zeta_d + \zeta_d^{-1}]$.

Il reste maintenant à comparer les groupes $(\mathrm{Cl}^S_{K/K_0})^{\Gamma'}$ et Cl^S_{L/K_0}. Les cas où S contient tous les diviseurs premiers de l'ordre de Γ' est facile et bien connu (cf. prop. 7. 6 ci-dessous et son corollaire). Des cas moins triviaux ont été traités par J.-F. Jaulent (non publié; cf. th. 7. 8).

L'injection $i: I_L \to I_K$ et la norme $n: I_K \to I_L$ induisent, par passage aux classes, des homomorphismes

$$i^* : \mathrm{Cl}_L \to \mathrm{Cl}_K \quad \text{et} \quad n^* : \mathrm{Cl}_K \to \mathrm{Cl}_L.$$

Théorème 7. 6. *Soit $m = [K : L]$. Le noyau (resp. le conoyau) de*

$$i^* : \mathrm{Cl}_L \to \mathrm{Cl}_K^{\Gamma'} \quad \textit{est annulé par } m \textit{ (resp. } m^2\textit{)}.$$

Corollaire 7. 7. *Si S contient tous les diviseurs premiers de Γ', l'homomorphisme*

$$i^* : \mathrm{Cl}^S_{L/K_0} \to (\mathrm{Cl}^S_{K/K_0})^{\Gamma'} \quad \textit{est un isomorphisme}.$$

Démonstration de 7. 6. Comme $n^* \circ i^*$ est l'application $c \to c^m$, $(\mathrm{Ker}\, i^*)^m$ est réduit à l'élément neutre. Pour étudier Coker i^*, nous introduisons, en suivant Hilbert, le sous-groupe $\mathrm{Cl}'_{K/L}$ de $\mathrm{Cl}^{\Gamma'}_{K/L}$ formé des classes de K qui contiennent un idéal invariant. Si $c \in \mathrm{Cl}'_{K/L}$ est représentée par l'idéal invariant $\mathfrak{a}$ de K, c^m est représenté par

$$\mathfrak{a}^m = i \circ n(\mathfrak{a}) \in \mathrm{Im}\, i,$$

donc m annule le conoyau de i^* dans $\mathrm{Cl}'_{K/L}$. Soit maintenant $c \in \mathrm{Cl}^{\Gamma'}_{K/L}$ représentée par un idéal $\mathfrak{a}$. Pour tout $s \in \Gamma'$, il existe $a_s \in K^*$ tel que $s\mathfrak{a} = a_s\mathfrak{a}$. L'application $s \mapsto (a_s)$ est un 1-cocycle de Γ' à valeurs dans le groupe P_K des idéaux principaux de K. Comme $H^1(\Gamma', P_K)$ est annulé par m, il existe un élément $a \in K^*$ tel que pour tout $s \in \Gamma'$, $(a_s^m) = (a \cdot sa^{-1})$; l'idéal $(a\mathfrak{a})$ est donc invariant et représente c; donc $\mathrm{Cl}^{\Gamma'}_{K/L}/\mathrm{Cl}'_{K/L}$ est un groupe annulé par m, ce qui démontre le théorème.

La structure de $\mathrm{Ker}\, i^*$ (la "capitulation") est mal connue. Toutefois, on a:

Théorème 7. 8 (Jaulent). *Supposons que Γ soit produit semi-direct de Γ' par un sous-groupe distingué Δ sur lequel Γ' opère fidèlement. Notons M le sous-corps de K fixe par Δ. Alors l'homomorphisme*

$$i^* : \mathrm{Cl}_{L/K_0} \to \mathrm{Cl}_{K/M}^{\Gamma'} \quad \textit{est un isomorphisme.}$$

(*La restriction aux classes relatives à K_0 est indispensable ici: il est en effet facile de donner des exemples dans lesquels Cl_L contient des classes non triviales provenant d'une classe de K_0 qui capitule dans M.*)

Démonstration. Soient $v = \sum_{s \in \Delta} s$ et $v' = \sum_{s \in \Gamma'} s$ les normes dans les algèbres $\mathbb{Z}[\Delta]$ et $\mathbb{Z}[\Gamma']$. Soit R l'algèbre $\mathbb{Z}[\Gamma']/v\mathbb{Z}[\Gamma']$ (noter que v est dans le centre de $\mathbb{Z}[\Gamma']$) et soit R' la sous-algèbre $\sum_{s \in \Gamma'} R(s-1) + v'R$ de R.

Le théorème résulte évidemment de la conjonction des deux assertions suivantes:

Lemme 7. 9. (i) *L'égalité $R' = R$ entraîne la conclusion du théorème* 7. 8.

(ii) *Sous les hypothèses de* 7. 8, *on a $R' = R$.*

Démonstration du lemme. (i) Si $R = R'$, il existe dans $\mathbb{Z}[\Gamma]$ des éléments a_s ($s \in \Gamma'$), b, c tels que

$$1 = \sum_{s \in \Gamma'} a_s(s-1) + v'b + vc.$$

Si $\mathfrak{a}$ est un idéal de L qui devient principal dans K, l'identité ci-dessus montre que, modulo le groupe engendré par les idéaux de K_0, $\mathfrak{a}$ est équivalent à l'idéal $N_{K/L}(b\mathfrak{a})$, qui est principal dans K, d'où l'injectivité de i^* (et la surjectivité de la norme de $\mathrm{Cl}_{K/M}$ vers Cl_{L/K_0}).

Si c est une classe invariante de $\mathrm{Cl}_{K/M'}$ le même calcul montre que cette classe est représentée par $i^* \circ n^*(bc)$, d'où la surjectivité de i^*.

(ii) Les orbites de Γ' opérant sur Δ-$\{1\}$ sont équipotentes à Γ'. Soit $\delta \subset \Delta$ un système de représentants de ces orbites. On a dans $\mathbb{Z}[\Gamma]$, $\sum_{s \in \Gamma'} \sum_{t \in \delta} sts^{-1} = v - 1$, identité qui s'écrit encore $1 = v \cdot 1 - \sum_{t \in \delta} \sum_{s \in \Gamma'} st(s^{-1} - 1) - \sum_{t \in \delta} \sum_{s \in \Gamma'} st$ et est donc de la forme $1 = \sum_{s \in \Gamma'} a_s(s-1) + v'b + vc$ en posant $a_s = \sum_{t \in \delta} s^{-1}t$, $b = \sum_{t \in \delta} t$ et $c = 1$, d'où le lemme et le théorème 7. 8.

La conjonction des théorèmes 7. 3, 7. 6 et 7. 8 donne des identifications de $\mathrm{Cl}_{K/M}$ à un produit de copies de Cl_{L/K_0} dans tous les cas considérés dans [C-M 2] (il s'agit bien de produits semi-directs). On peut obtenir des démonstrations directes à partir d'identités convenables, ce qui a été fait en 6. 8 pour le groupe diédral d'ordre 8. C'est ainsi qu'initialement nous avons étudié les groupes diédraux et le groupe A_4.

§ 8. Commentaires et remarques diverses

a) Sur la notion de bons nombres premiers. A priori, il semble raisonnable d'appliquer les calculs heuristiques de moyennes à des sous-familles restreintes d'extensions dont le comportement à l'infini est donné: par exemple, s'il s'agit de discriminants premiers, ou congrus à $-1 \pmod 3$, ou les deux, ou encore s'il s'agit de corps cubiques non galoisiens, se limiter à ceux qui sont associés à un corps quadratique donné.

La discussion qui est faite dans [C-M 2], § 3, à propos des calculs de Shanks et Williams sur les corps cubiques purs $\mathbb{Q}(\sqrt[3]{p})$, $p \equiv -1 \pmod 3$, montre qu'il faut être extrêmement prudent lorsque l'on n'exclut pas le nombre premier 2, qui est bon au sens de la définition 6. 1, mais qui divise le degré de la clôture galoisienne. (Rappelons que le comportement de la 2-composante du groupe des classes semble très différent selon que $p \equiv -1 \pmod 9$, ou que $p \equiv 2$ ou $5 \pmod 9$.) Quant aux mauvais nombres premiers, ils offrent aussi des possibilités d'interprétations heuristiques, comme le montre le résultat de Gerth ([G]), signalé dans [C-M 2], 3. 6, relatif au 4-rang du groupe des classes des corps quadratiques. Là aussi, la plus grande prudence est de rigueur comme le montre un exemple de Lenstra concernant la 2-composante des groupes des classes des corps quadratiques (communication privée). On observera que le comportement à l'infini d'une famille d'extensions galoisiennes K/K_0 à groupe de Galois isomorphe à un groupe Γ donné, se fixe en imposant pour toute place réelle de K_0 que le Frobenius à l'infini correspondant définisse une classe de conjugaison donnée de Γ d'ordre 1 ou 2 (à un automorphisme extérieur près de Γ).

Il semble raisonnable de supposer que l'on peut, sans changer le comportement statistique des groupes Cl^S_{K/K_0} pour S contenant les diviseurs premiers de $[K : K_0]$, imposer que les Frobenius en un nombre fini de places finies de K_0 soient dans des classes de conjugaison données de Γ, sauf peut-être en des places au dessus de 2 lorsque K/K_0 est de degré pair, à cause du "phénomène de Grünwald-Wang" (cf. [A-T], Ch. 10).

Signalons enfin des calculs en cours de G. Fung et H. Williams sur les corps cubiques de discriminants négatifs qui montrent que les "bons" nombres premiers qui divisent le degré de la clôture galoisienne ne sont pas aussi bons que nous l'espérions.

b) Sur les multi-indices admissibles. Dans l'égalité de l'hypothèse heuristique fondamentale 6. 6, le membre de gauche a la valeur 0 lorsque $\underline{u}$ n'est pas admissible, alors que le membre de droite est en général non nul. Par exemple lorsque K parcourt l'ensemble des corps quadratiques imaginaires, seule la valeur $u = 0$ est autorisée pour l'indice.

Fixons alors un nombre premier l, limitons nous aux corps pour lesquels l se décompose, et remplaçons l'anneau des entiers de K par celui des éléments de K qui sont entiers en dehors de l'un des facteurs de l. Le rang du groupe des unités est 1, et l'on constate sur les tables que le comportement du groupe des classes du nouvel anneau est tout à fait comparable à celui des anneaux d'entiers de corps quadratiques *réels*. Bien sûr, rendre inversible les deux idéaux premiers au dessus de l ou des idéaux premiers non décomposés ne changerait rien.

Nous conjecturons que, lorsque l'on rend inversible des nombres premiers $p_1, \ldots, p_k$ décomposés, il faut prendre $u = k$ pour faire l'étude heuristique, et nous laissons au lecteur le soin de généraliser cette conjecture à des situations autres que celles des corps quadratiques imaginaires.

c) Interprétation de caractères. Au paragraphe 7, nous avons concentré notre attention sur les idempotents e_χ pour lesquels χ est le caractère d'augmentation d'une représentation de permutation, situation particulièrement importante à cause de l'interprétation de $e_\chi \mathrm{Cl}_{K/K_0}$ à l'aide d'un groupe de classes relatif Cl_{L/K_0}.

Il est possible d'interpréter d'autres caractères en utilisant des extensions intermédiaires. Voici l'exemple d'une extension K/K_0 à groupe de Galois Γ isomorphe à S_4. Les caractères de Γ sont $\varepsilon_0, \varepsilon$ (la signature), φ de degré 2 provenant du quotient de Γ isomorphe à S_3, et deux caractères χ et $\varphi = \varepsilon\chi$ de degré 3, χ provenant de l'augmentation attachée aux permutations de S_4/S_3. Le groupe $e_\chi \mathrm{Cl}^S_{K/K_0}$ (pour $S \supset \{2, 3\}$) s'interprète à l'aide du groupe $\mathrm{Cl}^S_{K_4/K_0}$ (cf. § 7), où K_4 est une sous-extension de degré 4 de K/K_0. On peut de même relier $e_\varphi \mathrm{Cl}^S_{K/K_0}$ à $\mathrm{Cl}^S_{K_8/K_4}$, où $K_8 = K_4 K_2$, K_2 désignant la sous-extension quadratique de K/K_0.

Une autre interprétation possible des groupes précédents est la suivante: soit K_3 une sous-extension cubique de K/K_0 (résolvante cubique); on lui associe canoniquement deux sous-extensions K_6 et K_6' de K/K_0, non galoisiennes sur K_0, et telles que le discriminant de K_6/K_3 dans K_3^*/K_3^{*2} ait une norme triviale sur K_0.

Les groupes $e_\chi \mathrm{Cl}^S_{K/K_0}$ et $e_\varphi \mathrm{Cl}^S_{K/K_0}$ sont alors également reliés respectivement aux groupes Cl_{K_6/K_3} et $\mathrm{Cl}_{K'_6/K_3}$.

d) Le "Spiegelungssatz". Le cas particulier dû à Scholz du théorème de symétrie de Leopoldt indique qu'entre les 3-rangs des groupes de classes r de $k = \mathbb{Q}(\sqrt{m})$ et $\tilde{r}$ de $\tilde{k} = \mathbb{Q}(\sqrt{-3m})$, $m > 0$ on a la double inégalité $r \leqq \tilde{r} \leqq r+1$, l'égalité $r = \tilde{r}$ ayant lieu chaque fois que l'unité fondamentale de k n'est pas un cube modulo l'idéal $\mathfrak{f}$ de k, égal à (3^2) si 3 n'est pas ramifié dans k, et à $\mathfrak{p}^3$ si $(3) = \mathfrak{p}^2$ dans k. En faisant une hypothèse très raisonnable sur les classes de k modulo $\mathfrak{f}$ (cf. g) ci-après), on peut déduire les résultats heuristiques sur la valeur de r des résultats correspondants concernant $\tilde{r}$ (ou réciproquement); ce travail a été fait par Dutartre ([Du]) et concorde avec les prédictions. L'étude d'autres cas du Spiegelungssatz donnerait sans doute d'autres résultats confirmant la consistence interne de nos conjectures.

e) Le théorème de Brauer-Siegel. Soit K_0 un corps totalement réel. Considérons l'ensemble $\mathscr{E}$ des extensions quadratiques totalement imaginaires de K_0. Le rang relatif du groupe des unités de K étant nul, les résultats heuristiques de cet article prévoient que pour chaque entier impair m, l'ensemble des $K \in \mathscr{E}$ tels que h_{K/K_0} soit égal à m à une puissance de 2 près est de densité nulle. Ce résultat ne semble pas connu. Bien entendu, si l'on se limite à des extensions K/K_0 dans lesquelles un seul idéal premier est ramifié (dans ce cas, h_K est impair), le théorème de Brauer-Siegel précise alors le résultat: il n'y a qu'un nombre fini de corps $K \in \mathscr{E}$ tels que $h_K = m$.

f) Une moyenne liée aux discriminants cubiques. Soit p un nombre premier impair. Soit K_0 un corps de nombres, et soit $\mathscr{E}_\varrho$ l'ensemble des extensions quadratiques de K_0 dans lesquelles ϱ places réelles de K_0 sont ramifiées. Pour $K \in \mathscr{E}_\varrho$, soit r le p-rang du groupe Cl_{K/K_0}. On s'intéresse à la moyenne de la fonction p^r sur $\mathscr{E}_\varrho$.

Considérons sur l'ensemble des groupes abéliens finis (à isomorphisme près) la fonction définie par

$$f(G) = |\{H \subset G : H \cong \mathbb{Z}/p\mathbb{Z}\}|.$$

Si $r(G)$ désigne le p-rang de G on a $f(G)=\dfrac{p^{r(G)}-1}{p-1}$, donc

$$M(p^{r(G)})=(p-1)\,M(f)+1.$$

Avec les notations du § 5, on a

$$M_u(f)=\frac{Z(f,u)}{Z(u)},$$

où

$$Z(f,s)=\sum_G \frac{f(G)}{|\mathrm{Aut}\,G|\,|G|^s}=\sum_{n\geqq 1}\frac{1}{n^s}\sum_{|G|=n}\frac{f(G)}{|\mathrm{Aut}\,G|},$$

et

$$Z(s)=Z(1,s).$$

Or, d'après [C-L], prop. 4. 1, on a l'égalité

$$\sum_{|G|=n}\frac{1}{|\mathrm{Aut}\,G|}\,|\{G_1\subset G : G_1\cong H\}|=w\left(\frac{n}{|H|}\right)\frac{1}{|\mathrm{Aut}\,H|}$$

valable pour tout groupe abélien fini H, $w(m)$ étant nul lorsque m n'est pas entier, et égal à $\displaystyle\sum_{|G|=m}\frac{1}{|\mathrm{Aut}\,G|}$ sinon. En utilisant cette égalité avec $H=\mathbb{Z}/p\mathbb{Z}$ on obtient:

$$Z(f,s)=\frac{1}{p-1}\sum_{n\geqq 1}\frac{1}{n^s}\,w\left(\frac{n}{p}\right)=\frac{1}{p^s(p-1)}\sum_{m\geqq 1}\frac{w(m)}{m^s}=\frac{Z(s)}{p^s(p-1)},$$

d'où, en appliquant l'hypothèse heuristique fondamentale, $M(p^{r(G)})=1+\dfrac{1}{p^u}$, u désignant la différence des rangs des unités de K et de K_0. En notant (r_1, r_2) la signature de K_0 et ϱ le nombre de places réelles de K_0 ramifiées dans K/K_0, on voit que la signature de K est $(2r_1-2\varrho,\ \varrho+2r_2)$, d'où

$$M(p^{r(G)})=1+\frac{1}{p^{r_1+r_2-\varrho}}.$$

Or, pour $p=3$, cette moyenne a été étudiée (en liaison avec l'étude du nombre d'extensions cubiques de K_0 ayant un discriminant de norme donnée) par Datskowski et Wright ([D-W], th. I. 3), et la formule ci-dessus est un théorème pour $p=3$ (qui généralise un résultat ancien de Davenport-Heilbronn pour les cas où $K_0=\mathbb{Q}$; cf. [C-L], § 9, I, (C5) et II, (C0)).

Pour $p>3$ la moyenne de $p^{r(G)}$ est liée aux discriminants des extensions de degré p de K_0 à clôture galoisienne diédrale; on ne possède pas de théorème statistique sur ces discriminants.

g) Classes modulo un conducteur. Soit L un corps de nombres, et soit $\mathfrak{f}$ un "module" (ou "idéal généralisé") de L. Rappelons que $\mathfrak{f}$ est le produit formel d'un idéal entier $\mathfrak{f}_0$ de L et d'une famille finie $\mathfrak{f}_\infty$ de places réelles de L, que le groupe $(\mathbb{Z}_L/\mathfrak{f})^*$ est le produit $(\mathbb{Z}_L/\mathfrak{f}_0)^* \times \{\pm 1\}^{\mathfrak{f}_\infty}$. Le groupe $\mathrm{Cl}_{L,\mathfrak{f}}$ est le quotient $I_{L,\mathfrak{f}}/P_{L,\mathfrak{f}}$ du groupe des idéaux de L premiers à $\mathfrak{f}$ par son sous-groupe formé des idéaux principaux possédant un générateur α tel que $v_\mathfrak{p}(\alpha-1) \geqq v_\mathfrak{p}(\mathfrak{f}_0)$ pour tout $\mathfrak{p}$ premier divisant $\mathfrak{f}_0$ et tel que α soit positif aux places de $\mathfrak{f}_\infty$. On a alors une suite exacte:

$$0 \to (\mathbb{Z}_L/\mathfrak{f})^*/\mathrm{Im}\, E_L \to \mathrm{Cl}_{L,\mathfrak{f}} \to \mathrm{Cl}_L \to 0.$$

En outre, si L est une extension d'un corps K_0, et si $\mathfrak{f}$ provient d'un idéal f_0 de K_0, la norme de L à K_0 envoie $I_{L,\mathfrak{f}}$ dans $I_{K_0,\mathfrak{f}}$ et $P_{L,\mathfrak{f}}$ dans $P_{K_0,\mathfrak{f}}$, et l'on obtient un homomorphisme $N: \mathrm{Cl}_{L,\mathfrak{f}} \to \mathrm{Cl}_{K_0,\mathfrak{f}}$ compatible avec la suite exacte ci-dessus.

Il est naturel de chercher le comportement heuristique des groupes de classes modulo $\mathfrak{f}$ comme nous l'avons fait précédemment pour les cas $\mathfrak{f}=1$, l'interprétation par la théorie du corps de classes consistant à remplacer de corps de classes de Hilbert de K par le corps de classes de rayon $\mathfrak{f}$. On doit alors s'imposer la façon dont les diviseurs premiers de $\mathfrak{f}_0$ se décomposent dans L, et, plus précisément, se donner pour toutes les places finies ou non qui interviennent dans $\mathfrak{f}$ les classes de conjugaison de Frobenius dans $\mathrm{Gal}(K/K_0)$, K désignant une clôture galoisienne de L sur K_0. L'étude heuristique de $\mathrm{Cl}_{L,\mathfrak{f}}$ se divise en deux parties: (i) étude de $(\mathbb{Z}_L/\mathfrak{f})^*/\mathrm{Im}\, E_L$; (ii) étude des sections de l'application $\mathrm{Cl}_{L,\mathfrak{f}} \to \mathrm{Cl}_L$. Nous allons examiner brièvement quelques exemples dans lesquels $K_0=\mathbb{Q}$. Le cas où $\mathfrak{f}$ est réduit à la place infinie de $\mathbb{Q}$ est particulièrement intéressant: $\mathrm{Cl}_{L,\mathfrak{f}}$, noté Cl_L^+, est le groupe des classes au sens restreint de L.

Une relation de "Spiegelungssatz non semi-simple" existe sur le groupe $\mathrm{Cl}_{L,(4)\infty}$, qui entraîne des limitations quant aux structures possibles de Cl_L^+: les 2-rangs des groupes Cl_L^+ et Cl_L et le nombre r_1 de places réelles de L sont liés par l'inégalité $d_2(\mathrm{Cl}_L^+) - d_2(\mathrm{Cl}_L) \leqq \frac{r_1}{2}$, cf. [O]. Ainsi, si L est cubique réel, et si $d_2(\mathrm{Cl}_L^+/\mathrm{Cl}_L)$ atteint sa valeur maximale, égale à 2, Cl_L est d'ordre pair, et la suite exacte $\mathrm{Cl}_L^+ \to \mathrm{Cl}_L \to 1$ n'est pas scindée. Dans le cas où $L/\mathbb{Q}$ est cyclique, on a un résultat plus précis: Cl_L^+ et Cl_L ont même 2-rang, et cela bien que $L/\mathbb{Q}$ soit galoisienne de degré impair. Nous conjecturons toutefois que, quelque soit $\mathfrak{f}$ soumis aux condition que nous avons énoncées, pour une proportion définie de corps, les groupes $(\mathbb{Z}_L/\mathfrak{f})^*/\mathrm{Im}\, E_L$ et $\mathrm{Cl}_{L,\mathfrak{f}}$ ont une structure donnée. Nous n'avons cependant pas dans le cas général de valeurs à proposer pour ces densités. Les tables étendues de Ennola et Turunen de corps cubiques totalement réels [E-T] plaident en faveur d'une telle conjecture, avec des pourcentages respectifs de l'ordre de 55% et 0,50% pour la proportion de corps cubiques avec $\mathrm{Cl}_L^+/\mathrm{Cl}_L$ d'ordre 2 ou 4.

Lorsque $(\mathbb{Z}_L/\mathfrak{f})^*$ est d'ordre impair, la situation semble plus claire. On se limite bien sûr toujours aux bonnes composantes. En ce qui concerne le quotient $(E_L/\mathfrak{f})^*/\mathrm{Im}\, E_L$, nous pensons que l'image de E_L est un sous-groupe "au-hasard" de $(E_L/\mathfrak{f})^*$, remarque qui est à la base des heuristiques sur les groupes de classes (cf. [C-L], dernière ligne de la première page, mais l'idée n'est pas explicitée). Ainsi, si L parcourt les corps quadratiques de discriminant $d \equiv 5$ modulo 8, et que nous prenons $\mathfrak{f}=(2)$, le groupe $(\mathbb{Z}_L/\mathfrak{f})^*$ est d'ordre 3. Il n'y a rien à dire si d est <0, le groupe quotient par l'image de

E_L étant d'ordre 3 pour $d \neq -3$ et trivial pour $d=-3$. En revanche, dans le cas réel, nous conjecturons que ce groupe quotient est d'ordre 3 pour 1 corps sur 3, résultat en bon accord avec les calculs faits par Stephens et Williams dans [St-W] (noter que l'image de E_L est triviale dans $(\mathbb{Z}_L/(2))^*$ si et seulement si l'unité fondamentale de L est dans $\mathbb{Z}[\sqrt{d}]$). Si nous rendons inversible un facteur d'un nombre premier impair décomposé de L de façon à rendre E_L de rang 2 (cf. 8.b), nous pensons que $(\mathbb{Z}_L/(2))^*/\mathrm{Im}\, E_L$ est d'ordre 3 pour seulement 1 corps sur 9, ... En ce qui concerne le rang de la 3-composante de $\mathrm{Cl}_{L,(2)}$, nous devons tenir compte de la probabilité que nous estimons être correcte pour qu'une suite exacte $0 \to H \to E \to G \to 0$ soit scindée lorsque H est un groupe d'ordre 3, que G est un groupe de type $(3, 3, \ldots, 3)$ de rang t et que l'on impose à E d'être abélien. De façon générale, lorsque H et G sont des groupes abélien, et que G opère trivialement sur H, l'ensemble $H^2_{ab}(G, H)$ des éléments de $H^2(G, H)$ correspondant à une extension de H par G qui est un groupe abélien, constitue un sous-groupe de $H^2(G, H)$ qui s'identifie à $\mathrm{Ext}^1_{\mathbb{Z}}(G, H)$. Il est possible que la proportion de groupes $\mathrm{Cl}^S_{L,\mathfrak{f}}$ ($\mathfrak{f}$ étranger à (2) et aux places infinies, et S contenant les mauvais nombres premiers) ayant une structure donnée compatible avec des structures données pour $(\mathbb{Z}_L/\mathfrak{f})^*/\mathrm{Im}\, E_L$ et pour Cl_L, soit proportionnelle au nombre d'éléments de $H^2_{ab}(G, H)$ donnant naissance à cette structure.

h) Application aux discriminants. Le but de ce sous-paragraphe est d'indiquer une approche heuristique de certains problèmes de densité de discriminants. On montre facilement que le nombre de corps quadratiques, dans le cas réel comme dans le cas imaginaire, dont la valeur absolue du discriminant est $\leqq x$, est équivalent à $\frac{3}{\pi^2}x$ (la même constante $\frac{3}{\pi^2}=\frac{1}{2\zeta(2)}$).

On montre difficilement (Davenport et Heilbronn, cf. [D-W]) que, dans le cas cubique, le nombre de corps K avec $|d_K| \leqq x$ est équivalent à $\frac{x}{4\zeta(3)}$ dans le cas non réel et à $\frac{x}{12\zeta(3)}$ dans le cas réel. Que l'on ait des estimations proportionnelles à x est une conséquence des diverses conjectures que nous avons faites, si l'on veut bien admettre qu'il existe des termes de reste assez bons pour permettre certaines sommations infinies. On écrit un discriminant cubique D sous la forme df^2, où d est un discriminant quadratique (ou $d=1$) et f un entier $\geqq 1$, sans facteur carré autre que 9. Pour $f=1$, le nombre de discriminants D est $\frac{3^r-1}{2}$, où r est le 3-rang du groupe des classes de $Q(\sqrt{d})$, soit en moyenne 2 pour $d<0$ et $\frac{4}{3}$ pour $d>0$, cf. g). Passons à $f=2$, ce qui impose $d \equiv 5$ modulo 8. Si $r_3=0$, le nombre de discriminants D égaux à $4d$ est égal à 1 si $d<-3$, mais seulement à $\frac{1}{3}$ en moyenne si d est >0. Si $r_3>0$, on n'a aucun discriminant si la suite exacte de 8.g) est non scindée, mais $\frac{3^r-1}{2}$ dans la cas contraire si d est <-3, et $\frac{1}{3}\frac{3^r-1}{2}$ en moyenne si d est >0. On traite de façon analogue les cas où f est premier ou égal à 3^2. Dans le cas général, le nombre de diviseurs premiers de f intervient mais ce nombre est petit par rapport à f. Finalement, le nombre de

discriminants D à considérer s'obtient au moyen d'une sommation $\sum \frac{N(d,f)}{f^2}$, où $N(d,f)$, à d fixé, est assez petit pour que la série soit convergente. L'estimation en constante $\times x$ du cas quadratique doit donc s'étendre au cas cubique. Il serait du reste intéressant de préciser, pour d fixé, le nombre de discriminants cubiques de la forme $D=df^2$ pour $|D|\leqq x$, en cherchant un équivalent de la forme $\lambda(d)\sqrt{x}$, avec si possible un terme de reste; le cas $d=1$ a été examiné par Cohn ([Cohn]). Le passage du cas cubique non abélien au cas quartique de type S_4 est analogue: on cherche les discriminants quartiques Δ sous la forme $\Delta=Dg^2$ où D est un discriminant cubique, (et l'on fait de même pour le type A_4 en prenant pour D un discriminant de corps cubique cyclique). On connait les équivalents pour les cas cycliques et bicycliques (respectivement $cx^{1/2}$ et $c'x^{1/2}\log^2 x$ pour des constantes c et c' convenables), et Bailey ([B]) donne pour le cas diédral un encadrement $c_1 x\leqq N(x,\Delta)\leqq c_2 x$ où c_1 et c_2 sont des constantes et $N(x,\Delta)$ est le nombre de corps de type diédral avec $|\Delta|\leqq x$ (il y a bien sûr des constantes c, c', c_1, c_2, pour chaque signature).

h. 1) Conjecture. *Pour chacune des signatures à priori possibles, le nombre de corps quartiques de discriminant Δ avec $|\Delta|\leqq x$ possède un équivalent de la forme $c\,x$ dans le cas diédral comme dans le cas symétrique, et de la forme $c\sqrt{x}$ dans le cas alterné, pour des constantes c convenables.*

Des calculs récents de Buchmann et Ford ([B-F]) concernant les corps totalement réels de discriminant $\leqq 10^6$ sont en bon accord avec la conjecture ci-dessus pour les corps diédraux et symétriques, et confirment l'extrême rareté des corps alternés.

h. 2) Remarque. Des arguments fondés sur des dénombrements de polynômes ont conduit à conjecturer que, pour chaque degré n et chaque signature (r_1, r_2) avec $r_1+2r_2=n$, presque tout corps de degré n est à clôture galoisienne de groupe de galois isomorphe à S_n. La conjecture h. 1) entraîne que le degré 4 est une exception.

Ces méthodes heuristiques, faisant usage de la théorie du corps de classes, ne peuvent être adaptées à A_n ni à S_n pour $n\geqq 5$. Toutefois, les corps résolubles de degré 5 ou 7 pourraient être examinés comme les corps cubiques, et, au prix d'un certain effort, il devrait être possible de trouver (conjecturalement) un équivalent du nombre de corps dont la valeur absolue du discriminants est inférieure ou égale à x.

i) Vitesse de convergence. Posons:

$$R_u^S(f,x)=\frac{\sum\limits_{\substack{|D_K|\leqq x\\ K\text{ de type }u}} f(\mathrm{Cl}_K^S)}{\sum\limits_{\text{idem}} 1}-\mathfrak{M}_u(f).$$

Par définition, $R_u^S(f,x)$ tend vers 0 quand $x\to\infty$; on peut se poser la question de trouver un équivalent. En effet les tables semblent montrer, pour les fonctions f intéressantes, un comportement à peu près régulier et monotone.

Notre hypothèse heuristique fondamentale affirme que l'on doit avoir

$$\mathfrak{M}_u(f)=M_u^S(f).$$

Il n'est pas raisonnable d'émettre une conjecture au sujet de $R_u^S(f, x)$, mais après un examen empirique des tables, nous posons la question suivante: existe-t-il une fonction universelle $k(x)$ tendant (lentement) vers $+\infty$ et telle que lorsque $x \to \infty$:

$$R_u^S(f, x) \sim \frac{\sum_{|G| \leq \sqrt{x},\, \varphi} |G|^{-u} f(G/\mathrm{Im}\,\varphi) w_{k(x)}(G)}{\sum_{\text{idem}} |G|^{-u} w_{k(x)}(G)} - M_u^S(f)$$

(la condition $|G| \leqq \sqrt{x}$ dans la sommation (avec $|G|$ premier à S) est suggérée par le théorème de Brauer-Siegel). Des choix possibles pour $k(x)$ pourraient être $C_1(\log x)^\alpha$ (peut-être avec $\alpha = 1/2$), ou encore $C_2(\log\log x)^\beta$.

Si la réponse à cette question est positive, au moins en un sens assez faible, on peut en déduire par exemple le *sens* de la monotonie en moyenne de la convergence et il est bien en accord avec celui observé dans les tables, par exemple la croissance de la proportion de corps quadratiques imaginaires de nombre de classes divisible par 3, ou la décroissance de la proportion de corps quadratiques réels de discriminant premier et de nombre de classe égal à 1.

Bibliographie

[A-T] *E. Artin, J. Tate*, Class Field Theory, Harvard 1954.

[B] *A. M. Baily*, On the density of discriminants of quartic fields, J. reine angew. Math. **315** (1980), 190—210.

[B-F] *J. Buchmann, D. Ford*, On the Computation of Totally Real Quartic Fields of Small Discriminant, Math. Comp. **185** (1989), 161—174.

[C-L] *H. Cohen, H. W. Lenstra*, Heuristics on class groups of number fields, Lect. Notes in Math. **1068** (1984), 33—62.

[C-M] *H. Cohen, J. Martinet*, Ein heuristisches Studium der Klassengruppen, Graz 1986.

[C-M 2] *H. Cohen, J. Martinet*, Class Groups of Number Fields: Numerical Heuristics, Math. Comp. **48** (1987), 123—137.

[Cohn] *H. Cohn*, The density of Abelian cubic fields, Proc. Amer. Math. Soc. **5** (1954), 476—477.

[Deu] *M. Deuring*, Algebren, 2ième éd., Berlin 1968.

[Du] *Ph. Dutarte*, Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes, Diplôme, Université de Besançon 1984.

[D-W] *B. Datskowsky, D. J. Wright*, Density of discriminants of cubic extensions, J. reine angew. Math. **386** (1988), 116—138.

[E-T] *V. Ennola, R. Turunen*, On Totally Real Cubic Fields, Math. Comp. **44** (1985), 495—518.

[G] *F. Gerth III*, The 4-class ranks of quadratic fields, Invent. Math. **77** (1984), 489—515.

[L] *R. B. Lakein*, Computation of the Ideal Class Group of Certain Complex Quartic Fields II, Math. Comp. **29** (1975), 137—144.

[O] *B. Oriat*, Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres, Bull. Soc. Math. France **104** (1976), 301—307.

[Ser] *J.-P. Serre*, Représentations linéaires des groupes finis, 2ième éd., Paris 1971.

[S-W] *D. Shanks, H. C. Williams*, A Note on Class-Number One in Pure Cubic Fields, Math. Comp. **33** (1979), 1317—1320.

[St-W] *A. J. Stephens, H. C. Williams*, Computation of Real Quadratic Fields with Class Number One, Math. Comp. **184** (1988), 809—824.

Centre de Recherche en Mathématiques, Université de Bordeaux I, 351, cours de la Libération, 33405 Talence, France

Eingegangen 5. Dezember 1988